

# Chapter 1

## SETS

One concept that pervades almost the whole of mathematics and many other disciplines is the notion of sets. George Cantor is considered the founder of set theory. In this chapter we study set theory and follow Cantor's original intuitive approach but also build it axiomatically at times. So our approach is a fine blend of intuitive ideas and the theory built on axioms.

### 1.1. Preliminaries

Intuitively speaking, a set is a well-defined collection of objects. For example, the collection of all the students of B.Tech/M.Tech computer engineering in the college is a set. There is one thing inherent in the statement, 'well-defined collection of objects' in the definition of a set. By this we mean that, given a set and some object, we should be able to decide whether the object is a member of the set under consideration, or not. Objects which form the set are all distinct (some authors do not insist on this but we shall do so). For example, all the chairs lying in this room do not form a set, for if we take chairs out and place them among other chairs, we cannot identify the chairs lying in this room. Objects in the set are called **members** or **elements** of the set. Now we will give a more formal definition of a set. Let  $P$  be a given property. A **set** is a collection of objects having the given property  $P$ . Sets are normally denoted by capital letters such as  $S, T, U, X, Y, A, B, C$  etc. and elements or objects or members of a set are denoted by lower case letters. If  $S$  is a set and  $x$  is an object in  $S$ , we write  $x \in S$  while if  $x$  is not an element of  $S$  we write it as  $x \notin S$ . We may describe a set  $S$  by writing all the elements of  $S$ , if it were possible, and

to enclose these within brackets. For example, (a) {Ram, Rahim, Krishan, Uma} is a set consisting of Ram, Rahim, Krishan and Uma; (b) {1, 3, 5, 7, 9} is the set consisting of the odd integers 1, 3, 5, 7 and 9; (c) {1, 2, 3, . . . , 99, 100} is the set consisting of the integers from 1 to 100. Here the ellipsis after 3, and before 99 indicates the integers beyond 3 and up to 98; (d) {1, 3, 5, . . . ,  $2n + 1$ , . . .} is the set consisting of all odd positive integers; (e) {2, 4, 6, . . . ,  $2n, \dots$ } is the set of all even positive integers. The sets in examples (b) to (e) above may also be expressed in the set builder notation or in a more formal manner as

- (b)  $\{n|n \text{ is an odd positive integer less than } 10\}$   
 $= \{n|n \text{ is an integer, it is odd and } 1 \leq n \leq 10\}$
- (c)  $\{n|n \text{ is a positive integer less than } 101\}$   
 $= \{n|n \text{ is an integer and } 1 \leq n \leq 100\}$
- (d)  $\{n|n \text{ is an odd positive integer}\}$   
 $= \{2n + 1|n \text{ is a non-negative integer}\}$   
 $= \{m|m = 2n + 1, n \text{ a nonnegative integer}\}$
- (e)  $\{n|n \text{ is an even positive integer}\}$   
 $= \{2n|n \text{ is a positive integer}\}$   
 $= \{m|m = 2n, n \text{ a positive integer}\}.$

A set which has no elements is called an **empty set** or a **null set** and is denoted by  $\{\}$  or  $\varphi$ . Empty sets may be obtained more formally by using a property  $P$  which is self-contradictory. For example, the set of all positive integers less than 0 or the set of all odd integers which are divisible by 2 or the set of all real numbers which are the roots of the polynomial  $x^2 + 1$ . In the set builder notation we may describe these sets as

$$\begin{aligned} &\{n|n \text{ is a positive integer and } n < 0\} \\ &\{n|n \text{ is an odd integer and } 2 \text{ divides } n\} \\ &\{a|a \text{ is a real number and } a^2 + 1 = 0\}. \end{aligned}$$

We have not placed any restriction on the elements of a set. For example, we may have sets like

{Ram, Rahim, London, New Delhi, New York, 1, 2, 3}; or  
 $\{\{a, b, c\}, 1, 2, 3, 4, x, y, z\}$  in which one of the elements is  $\{a, b, c\}$ , which itself is a set; or  $\{\varphi, \{\varphi\}, \{1, 2, 3\}, 1, 2, 3\}$ . Observe that  $\{\varphi\}$  is not an empty set but is a set having one element which is  $\varphi$  the empty set. Or  $\{a, \{a\}, \{\{a\}\}, \{\{\{a\}\}\}, b, \{b\}, \{\{b\}\}\}$ .

Recall that while defining a set we have not placed any order in which the elements of a set are listed. Thus  $\{1, 2, 3\}$ ,  $\{1, 3, 2\}$  and  $\{2, 1, 3\}$

all represent the same set, the elements of which are 1, 2 and 3. Sets in which elements are written in a particular order are called ordered sets and will be studied later. We next establish notations for some well-known sets. Throughout, we write

$N$  = The set of all natural numbers =  $\{1, 2, 3, \dots, n, \dots\}$ ;  
which is also called the set of counting numbers;

$Z^+$  = The set of all non-negative integers =  $\{0, 1, 2, 3, \dots, n, \dots\}$ ;  
which is the same as the set  $N$  of natural numbers together with the number 0;

$Z$  = The set of all integers =  $\{0, \pm 1, \pm 2, \pm 3, \dots\}$ ;

$Q$  = The set of all rational numbers =  $\{p/q \mid p, q \text{ integers, } q \neq 0\}$ ;

$Q^*$  = The set of non-zero rational numbers  
=  $\{p/q \mid p, q \text{ integers, } p \cdot q \neq 0\}$ .

There are infinitely many numbers which are not rational numbers. Examples of such numbers are  $\sqrt{2}$ ,  $\sqrt{3}$ ,  $\sqrt{5}$ ,  $3\sqrt{2}$ ,  $\pi$  etc. These are real numbers, none of which is a rational number. Numbers which can be represented as points on the real line are called **real numbers**. There is a deep theorem in mathematics which says that between every two rational numbers there are infinitely many real numbers. We do not go into details about these numbers but we introduce the notations:

$R$  = The set of all real numbers;

$R^*$  = The set of all non-zero real numbers;

$C$  = The set of all complex numbers =  $\{a + ib \mid a, b \in R \text{ and } i = \sqrt{-1}\}$ ;

$C^*$  = The set of all non-zero complex numbers  
=  $\{a + ib \mid a, b \in R, i = \sqrt{-1} \text{ and } a \neq 0 \text{ or } b \neq 0\}$ .

Corresponding to every complex number there is a point in the plane and corresponding to every point in the plane there is a complex number.

The number of elements in a set  $S$  is called the **order of the set** and is denoted by  $o(S)$  or  $|S|$ . If the order of  $S$  is finite, we call  $S$  a **finite set** and otherwise we call it an **infinite set**. Also in this case we say that  $S$  is an infinite set. Observe that all sets  $N$ ,  $Z$ ,  $Q$ ,  $R$  and  $C$  are infinite sets. The set of all the roots of the cubic  $x^3 + 3x^2 + 8$  is a finite set of order 3. This is so because every polynomial of degree  $n$  has  $n$  roots. Given two sets  $A$  and  $B$ , we say that  $A$  is a **subset** of  $B$  if every element of  $A$  is in  $B$  and we express it by writing  $A \subseteq B$ . If  $A$  is a subset of  $B$  and there is an element  $b \in B$  which is not in  $A$ , then  $A$  is called a **proper subset** of  $B$  and this situation is expressed by  $A \subset B$ . Two sets  $A$  and  $B$  are said to be equal and written as  $A = B$  if  $A$  is a subset of  $B$  and  $B$  is a subset of  $A$ . It is

clear that if  $A$  is a subset of  $B$  and  $B$  is a subset of  $C$ , then  $A$  is a subset of  $C$ . Also, every set is a subset of itself. Following are some examples.

1. The set of B.Tech computer engineering second-year students in this college is a subset of the set of all B.Tech second-year students in the college.
2. The set of all second-year engineering students in this college is a subset of the set of all engineering students in the college.
3. The set of all people in Delhi is a subset of the set of all people in India.
4. The set  $\{1, 3, 5, 7, 9\}$  is a subset of the set  $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ .
5. The set of all odd integers is a subset of the set of all integers.
6. The set of all even integers is a subset of the set of all integers.
7. The set of all integers which are multiples of 3 is not a subset of the set of all odd integers as 6 is a multiple of 3 but is not an odd integer.
8. The set  $N$  of all natural numbers is a subset of the set of all integers, the set  $Z$  of all integers is a subset of the set of all rational numbers, the set  $Q$  of all rational numbers is a subset of the set of all real numbers, the set of all real numbers is a subset of the set of all complex numbers.
9. Let  $n$  be a positive integer. The set  $S = \{e^{2\pi ik/n} | 0 \leq k < n\}$  of all  $n$ th roots of unity is a subset of the set  $C$  of all complex numbers. Observe that, if for  $k < l < n$ ,  $e^{2\pi ik/n} = e^{2\pi il/n}$  then  $e^{2\pi i(l-k)/n} = 1$  or  $\cos 2\pi(l-k)/n + i \sin 2\pi(l-k)/n = 1$ , which is possible only if  $2\pi(l-k)/n$  is a multiple of  $2\pi$ . However, this is not possible as  $1 \leq l-k < n$ . This proves that the set  $S$  has order  $n$ . We shall consider this set again when we discuss groups. Observe that  $S$  is a subset of the set  $R$  of all real numbers only when  $n = 1$  or  $2$ .
10. The set  $\{1, -1\}$  is a subset of the set  $\{1, -1, i, -i\}$  where  $i = \sqrt{-1}$ .
11. Let  $M_2(R)$  denote the set of all square matrices of order 2 with real entries,  $M_2(R)^*$  be the set of all nonsingular square matrices of order 2 with real entries and  $M_2(R)^{**}$  be the set of all square matrices of order 2 with real entries which have determinant 1. Then  $M_2(R)^{**}$  is a subset of  $M_2(R)^*$  and  $M_2(R)^*$  is a subset of  $M_2(R)$ .
12. The set of vowels in the English alphabet is a subset of the set of all English alphabets.

## 1.2. Algebra of Sets

Sets that we study are subsets of a certain larger set. This larger set of which every set under study is a subset is called the **universal set**. The universal set may change with context. For example, if we talk of sets of

numbers, we may take the set  $C$  of complex numbers as the universal set. It may sometimes be enough to consider the set  $R$  of real numbers as the universal set. When we talked of students of B.Tech computer engineering second year in this college we take the set of all engineering students in the college as the universal set. For the set of all the people in Bombay, we may take the set of all people in India as the universal set. For the sets under consideration we will write  $X$  or  $E$  or  $U$  for the universal set. Let  $A, B$  be two sets. We define  $A \setminus B$  or  $A - B$  by  $A \setminus B = \{x \in A | x \notin B\}$  which clearly is a subset of  $A$ . The set  $X \setminus A = \{x \in X | x \notin A\}$  where  $X$  is the universal set is called the **complement** of  $A$  and is denoted by  $A'$  or  $A^c$  or  $\bar{A}$ .

We define **union**  $A \cup B$  and **intersection**  $A \cap B$  of two sets  $A, B$  by  $A \cup B = \{x \in X | x \in A \text{ or } x \in B\}$ ,  $A \cap B = \{x \in X | x \in A \text{ and } x \in B\}$ .

It is clear from the definitions that  $A, B$  are subsets of  $A \cup B$  while  $A \cap B$  is a subset of  $A$  as well as  $B$ . The following are then clear:

- (a)  $\varphi' = X$ ,  $X' = \varphi$                       (b)  $(A')' = A$   
 (c) If  $A \subseteq B$ , then  $B' \subseteq A'$       (d)  $A \cap A' = \varphi$ ,  $A \cup A' = X$ .

Moreover,

$$A \cup B = B \cup A, \quad A \cap B = B \cap A, \quad A \cup A = A, \quad A \cap A = A, \\ A \cup X = X \text{ and } A \cap X = A.$$

Also, if  $A$  is a subset of  $B$ , then  $A \cup B = B$  and  $A \cap B = A$ . The converse is also true and we can have:

**Theorem 1.1.** For sets  $A$  and  $B$ , (a)  $A \cup B = B$  if and only if  $A \subseteq B$ ;  
 (b)  $A \cap B = A$  if and only if  $A \subseteq B$ .

**Proof.** Suppose that  $A \subseteq B$ . Let  $x \in A \cup B$ . Then  $x \in A$  or  $x \in B$ . As  $A \subseteq B$ ,  $x \in A$  implies that  $x \in B$ . Then  $x \in B$  or  $x \in B$  i.e.  $x \in B$ . Hence  $A \cup B \subseteq B$ . Also  $B \subseteq A \cup B$ . Therefore  $A \cup B = B$ . On the other hand, if  $A \cup B = B$ , as  $A \subseteq A \cup B$ , we have  $A \subseteq B$ . Proof of (b) follows on similar lines.

Union and intersection of sets are related through laws known as distributive laws.

**Theorem 1.2.** For any sets  $A, B, C$ ,

- (a)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;  
 (b)  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ .

**Proof.** (a) Let  $x \in A \cap (B \cup C)$ . Then  $x \in A$  and  $x \in B \cup C$  or  $x \in A$  and ( $x \in B$  or  $x \in C$ ). This means that ( $x \in A$  and  $x \in B$ ) or ( $x \in A$  and

$x \in C$ ) i.e.  $x \in A \cap B$  or  $x \in A \cap C$ . Thus  $x \in (A \cap B) \cup (A \cap C)$ . This proves that

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C). \quad (1.1)$$

Next, let  $x \in (A \cap B) \cup (A \cap C)$ . Then  $x \in A \cap B$  or  $x \in A \cap C$  i.e. ( $x \in A$  and  $x \in B$ ) or ( $x \in A$  and  $x \in C$ ).

This is equivalent to saying that  $x \in A$  and ( $x \in B$  or  $x \in C$ ). i.e.  $x \in A$  and  $x \in B \cup C$ . Therefore  $x \in A \cap (B \cup C)$ . This proves that

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C). \quad (1.2)$$

Combining (1.1) and (1.2) gives

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

(b) Since  $B \cap C \subseteq B$  and  $B \cap C \subseteq C$ ,

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

Combining these we get

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

For the reverse inclusion, let  $x \in (A \cup B) \cap (A \cup C)$ . Then

$$x \in A \cup B \quad \text{and} \quad x \in A \cup C$$

or

$$(x \in A \text{ or } x \in B) \quad \text{and} \quad (x \in A \text{ or } x \in C).$$

This implies that  $x \in A$  or  $\{x \in B \text{ and } x \in C\}$  i.e.  $x \in A$  or  $x \in B \cap C$  which together imply that  $x \in A \cup (B \cap C)$ . This proves that

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

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

**Theorem 1.3.** For any sets  $A$  and  $B$ ,

$$(a) A \setminus B = A \cap B', \quad (b) (A \cup B)' = A' \cap B', \quad (c) (A \cap B)' = A' \cup B'.$$

**Proof.** (a)  $A \setminus B = \{x \in A \mid x \notin B\} = \{x \in A \mid x \in B'\} = A \cap B'$ .

(b) Let  $x \in (A \cup B)'$ . Then  $x \notin A \cup B$  and so  $x \notin A$  and  $x \notin B$  which is the same thing as saying that  $x \in A'$  and  $x \in B'$ . This shows that  $x \in A' \cap B'$ . Thus  $(A \cup B)' \subseteq A' \cap B'$ .

Next, let  $x \in A' \cap B'$ . Then  $x \in A'$  and  $x \in B'$  which is equivalent to saying that  $x \notin A$  and  $x \notin B$ . Therefore  $x \notin A \cup B$  or that  $x \in (A \cup B)'$ . Hence  $A' \cap B' \subseteq (A \cup B)'$ .

Combining the two inclusions, we get  $(A \cup B)' = A' \cap B'$ .

(c) Let  $x \in (A \cap B)'$ . Then  $x \notin A \cap B$ . Therefore either  $x \notin A$  or  $x \notin B$  which implies that  $x \in A'$  or  $x \in B'$  i.e.  $x \in A' \cup B'$ . Thus  $(A \cap B)' \subseteq A' \cup B'$ . On the other hand, if  $x \in A' \cup B'$ , then  $x \in A'$  or  $x \in B'$  i.e.  $x \notin A$  or  $x \notin B$ . This shows that  $x \notin A \cap B$  or that  $x \in (A \cap B)'$ . This proves that  $A' \cup B' \subseteq (A \cap B)'$ . Combining it with the reverse inclusion already proved, we get  $(A \cap B)' = A' \cup B'$ .

The two results as at (b) and (c) above are called **De Morgan's Laws**.

**Example 1.1.** For any sets  $A, B, C$  prove that

- (a)  $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$ ,
- (b)  $A \cup (B \setminus C) = (A \cup B) \setminus (C \setminus A)$ ,
- (c)  $A \setminus B \subseteq B'$ ,
- (d)  $(A \setminus B) \setminus C = A \setminus (B \cup C)$ .

**Solution.** Since  $A \setminus B = A \cap B'$  (c) follows.

- (a)  $(A \cap B) \setminus (A \cap C) = (A \cap B) \cap (A \cap C)'$ 

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

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

$$= A \cap B \cap C'$$

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

$$= A \cap (B \setminus C).$$
- (b)  $(A \cup B) \setminus (C \setminus A) = (A \cup B) \setminus (C \cap A')$ 

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

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

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

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

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

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

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

which completes the proof of (b).

$$\begin{aligned} \text{(d)} \quad (A \setminus B) \setminus C &= (A \setminus B) \cap C' = (A \cap B') \cap C' = A \cap (B' \cap C') \\ &= A \cap (B \cup C)' = A \setminus (B \cup C). \end{aligned}$$

Let  $A, B$  be two sets. By the **symmetric difference** of the sets  $A, B$  we mean the set  $(A \setminus B) \cup (B \setminus A)$  and it is denoted by  $A \sim B$  or  $A \oplus B$ . Now

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

Thus the symmetric difference  $A \oplus B$  consists of all elements which are in  $A$  or in  $B$  but not in both.

Two sets  $A$  and  $B$  are said to be **mutually disjoint** or **mutually exclusive** if they do not have any element in common, i.e. if  $A \cap B = \varphi$ . Observe that if  $A, B$  are mutually exclusive sets, then the symmetric difference  $A \oplus B$  is just  $A \cup B$ . On the other hand if  $A \subseteq B$ , then  $A \setminus B = \phi$  and  $A \oplus B = (A \cup B) \setminus (A \cap B) = B \setminus A = B \cap A'$ .

**Example 1.2.** For any sets  $A, B, C$ ,  $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$ .

**Solution.**

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

**Example 1.3.** Let  $A, B, C$  be any sets. Given that  $A \cap C \subseteq B \cap C$  and  $A \cap C' \subseteq B \cap C'$ , prove that  $A \subseteq B$ .

**Solution.** Let  $X$  be the universal set. It follows from the definition of the complement of a set that  $X = C \cup C'$ . Now

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

Thus,  $A \subseteq B$ .

Using the above we can deduce that if  $A, B, C$  are sets with  $A \cap B = A \cap C$  and  $A' \cap B = A' \cap C$ , then  $B = C$ .

**Exercise 1.1.** We have used in some of the proofs earlier that if  $A, B, C, D$  are sets such that  $A \subseteq B$  and  $C \subseteq D$ , then  $A \cap C \subseteq B \cap D$ . Give a formal proof of this observation.

In view of the above, if  $A, B, C$  and  $D$  are sets such that  $A \subsetneq B$  and  $C \subsetneq D$ , then  $A \cap C \subseteq B \cap D$  and  $A \cup C \subseteq B \cup D$ . It is not essential that  $A \cap C \subsetneq B \cap D$  and  $A \cup C \subsetneq B \cup D$ .

For example, let  $A = \{1, 2, 3\}, B = \{1, 2, 3, 5, 7\}, C = \{1, 2, 4\}$  and  $D = \{1, 2, 4, 6\}$ . Then  $A \subsetneq B, C \subsetneq D$  but  $A \cap C = \{1, 2\} = B \cap D$ .

This example also shows that  $A \cap C = B \cap C$  but  $A \neq B$ .

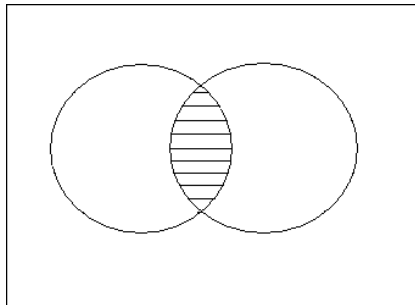
For the observation about union, we take  $A = \{1, 2, 3\}, B = \{1, 2, 3, 4\}, C = \{1, 2, 4\}$  and  $D = B$ . Then  $A \subsetneq B, C \subsetneq D$  and  $A \cup C = \{1, 2, 3, 4\} = B \cup D$ . This example also shows that  $A \cup B = A \cup C$  while  $B \neq C$ .

### 1.3. Venn Diagrams

Sometimes it is convenient to visualize results about unions, intersections, complementation and their combinations using two-dimensional figures or diagrams. In this pictorial representation, universal set is represented by a rectangle and sets are represented by circular, elliptic or any curved regions. If  $A, B$  are any two sets then their intersection and union are represented by the shaded region in Figs. 1.1 and 1.2 below while the complement  $A'$  of  $A$  is given by the shaded region in Fig. 1.3,  $A \setminus B$  is given by Fig. 1.4 and the symmetric difference  $A \sim B = A \oplus B$  is given by Fig. 1.5.

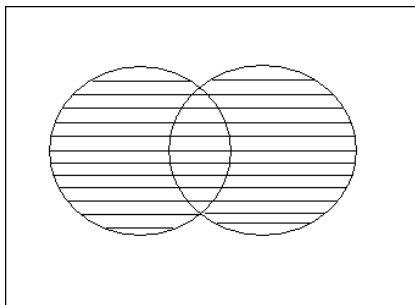
**Exercise 1.2.** If  $A, B, C$  are any sets indicate using Venn diagrams the proofs of the distributive laws

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



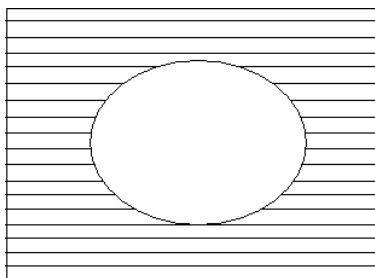
$$A \cap B$$

Fig. 1.1.



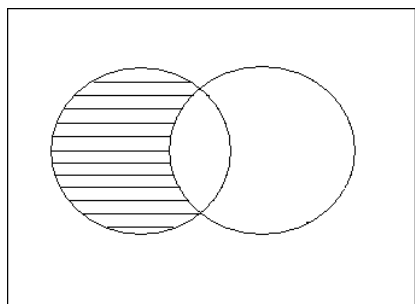
$$A \cup B$$

Fig. 1.2.



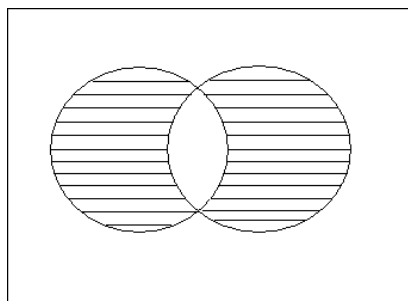
$$A'$$

Fig. 1.3.



$$A - B$$

Fig. 1.4.



$$A \oplus B$$

Fig. 1.5.

#### 1.4. Power Set

We will now consider power set of a set and binary relations on sets. Let  $S$  be a non-empty set. The collection of all subsets of  $S$  is called the **power set** of  $S$  and is denoted by  $\mathfrak{P}(S)$ . For example, if

- (a)  $S = \{1\}$ , then  $\mathfrak{P}(S) = \{\phi, S\}$ ;
- (b)  $S = \{1, 2\}$ , then  $\mathfrak{P}(S) = \{\phi, \{1\}, \{2\}, S\}$ ;
- (c)  $S = \{1, 2, 3\}$ , then

$$\mathfrak{P}(S) = \{\phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, S\}.$$

In case (a) the number of elements in  $\mathfrak{P}(S)$  is  $2 = 2^1$ ; in case (b) the number of elements in  $\mathfrak{P}(S)$  is  $4 = 2^2$ ; and in case (c), the number of elements in  $\mathfrak{P}(S)$  is  $8 = 2^3$ .

We shall prove later that if  $S$  is a finite set of order  $n$ , then  $o(\mathfrak{P}(S)) = 2^n$ . Binary relations on sets shall also be considered later.

### 1.5. Countable Sets

Let  $A, B$  be two non-empty sets. By a **map**  $f$  from  $A$  to  $B$  written as  $f: A \rightarrow B$  we mean a rule or a law which associates to every element of  $A$  a unique element of  $B$ . The unique element of  $B$  which is associated with an element  $a$  of  $A$  is denoted by  $f(a)$  and is called the  $f$ -image of  $a$  or the image of  $a$  under  $f$ . For example, if  $A = B = R$ , the set of real numbers, we may define  $f: R \rightarrow R$  by  $f(a) = |a|$ ,  $a \in R$ , where  $|a|$  denotes the magnitude of  $a$ . Recall that  $|a| = a$  if  $a \geq 0$  and  $|a| = -a$  if  $a < 0$ .

We may consider some other maps  $f: R \rightarrow R$  as

- (a)  $f(a) = -a, a \in R$ ,
- (b)  $f(a) = a^2, a \in R$ ,
- (c)  $f(a) = e^a, a \in R$ ,
- (d)  $f(a) = 2a + 3, a \in R$ .

Observe that we have not defined any map like  $f(a) = 1/a + 2$  or  $1/a - 1$  etc. because in the first case the right-hand side is not defined for  $a = -2$  while it is not defined for  $a = 1$  in the second case. We have also not considered things like  $f(a) = \sqrt{a}$  for if  $a < 0$ , then  $\sqrt{a}$  is not a real number. However, (e) if  $A$  is the set of all positive real numbers and  $B$  is the set of all real numbers in the interval  $(0, 1)$ , we may define  $f(a) = 1/a + 2$ ,  $a \in A$ . (f) Let  $A = \{1, 2, 3\}$ ,  $B = \{a, b\}$ . Then the assignments in Figs. 1.6–1.8 below are maps while those in Figs. 1.9 and 1.10 below are not maps.

- (g) Let  $N$  be the set of all natural numbers and  $Z$  be the set of all integers. Then

- (i)  $f: N \rightarrow N$  given by  $f(n) = 2n$ ,  $n \in N$ ;
- (ii)  $f: Z \rightarrow Z$  given by  $f(n) = 2n$ ,  $n \in Z$

are maps.

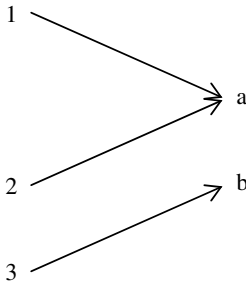


Fig. 1.6.

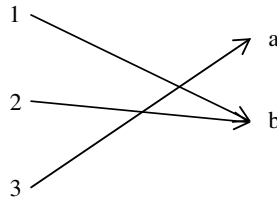


Fig. 1.7.

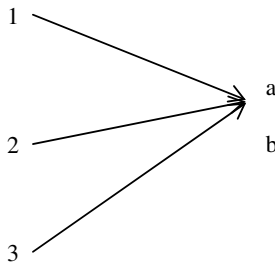


Fig. 1.8.

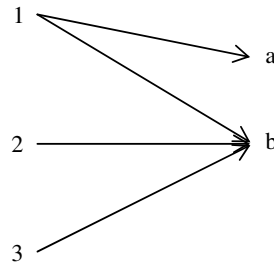


Fig. 1.9.

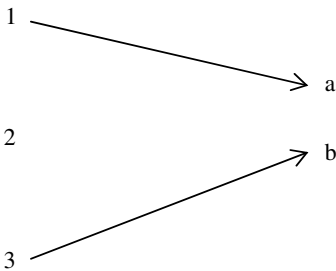


Fig. 1.10.

- (h)  $f : C \rightarrow R$  given by  $f(a + ib) = a^2 + b^2$ ,  $a, b \in R$ , is a map.
- (i) Let  $M_2(R)$  be the set of all square matrices of order 2 over  $R$ . Then  $f : M_2(R) \rightarrow R$  defined by  $f(A) = \det A$ ,  $A \in M_2(R)$  is a map.
- (j)  $f : R \rightarrow C$  defined by  $f(\alpha) = e^{i\alpha} = \cos \alpha + i \sin \alpha$ ,  $\alpha \in R$ , is also a map.

Let  $A, B$  be non-empty sets. A map  $f : A \rightarrow B$  is called

- (1) **injective** or **one-one** or **monomorphic** if for  $a_1, a_2 \in A, a_1 \neq a_2$  implies  $f(a_1) \neq f(a_2)$ . Equivalently, if  $f(a_1) = f(a_2), a_1, a_2 \in A$ , then  $a_1 = a_2$ ;

- (2) **surjective** or **onto** or **epimorphic** if for every  $b \in B$ , there exists an  $a \in A$  such that  $f(a) = b$  i.e. every element of  $B$  is the image of an element of  $A$ ;
- (3) **bijective** or **isomorphic** if  $f$  is both one-one and onto.

**Example 1.4.** The maps in examples (a), (d), (e) above are bijective, the maps in examples (c), (g)((i) and (ii)) are injective but not surjective while the maps in (b), (h), (j) are neither injective nor surjective. The map in (i) is surjective but not injective.

**Example 1.5.** Define a map  $f : N \rightarrow Z$  by  $f(2k + 1) = k + 1, k \geq 0$  and  $f(2k) = -k, k \geq 0$ . Since  $f(2k + 1) > 0$  while  $f(2k) \leq 0$ , for no  $k$  and  $l$ ,  $f(2k + 1) = f(2l)$ . Also  $f(2k + 1) = f(2l + 1)$  implies that  $k + 1 = l + 1$  which gives  $k = l$  and  $f(2k) = f(2l)$  shows that  $-k = -l$  or that  $k = l$ . Thus the map  $f$  defined is one-one. For any positive integer  $k, k = f(2k - 1)$  and  $-k = f(2k)$ . Hence the map  $f$  is onto as well. Thus the map  $f$  is bijective.

**Definition.** Given two sets  $P$  and  $Q$ , we say that there is a **one-to-one correspondence** between the elements of  $P$  and the elements of  $Q$  if it is possible to pair off the elements in  $P$  and  $Q$  such that every element in  $P$  is paired off with a distinct element of  $Q$  and vice versa, i.e. every element of  $P$  is associated with a unique element of  $Q$  and every element of  $Q$  is associated with exactly one element of  $P$ . This is equivalent to saying (in precise formal language) that there exists a map  $f : P \rightarrow Q$  which is bijective.

**Definition.** A set  $S$  is said to be **countable** if it is finite or the elements of  $S$  are in one-to-one correspondence with the elements of  $N$  — the set of natural numbers. Sometimes a set  $S$ , the elements of which are in one-to-one correspondence with the elements of  $N$ , is called **denumerable**. Then a set  $S$  is countable if either it is finite or denumerable. Thus for infinite sets there is no difference between denumerable and countable sets. A set which is not countable is called **uncountable**.

**Theorem 1.4.** Every infinite subset of a denumerable set is denumerable.

**Proof.** Let  $A$  be a denumerable set and  $B$  be an infinite subset of  $A$ . Let  $f : N \rightarrow A$  be a map which is one-one and onto. Then the elements of  $A$  are  $f(1), f(2), f(3), \dots$  and, therefore, the elements of  $B$  look like  $f(i_1), f(i_2), \dots$  for  $i_1 < i_2 < i_3 < \dots$ . Define a map  $g : N \rightarrow B$  by  $g(n) = f(i_n), n \in N$ . By the very definition  $g$  is onto. Suppose that  $g(n) = g(m)$ .

Then  $f(i_m) = f(i_n)$  which implies that  $i_m = i_n$ , the map  $f$  being one-one. However, for  $m \neq n, i_m \neq i_n$ , by our choice. Therefore  $i_m = i_n$  implies that  $m = n$ . Hence the map  $g$  is one-one as well. This proves that  $B$  is denumerable.

**Theorem 1.5.** The set  $Z^+ \times Z^+ = \{(m, n) | m, n \in Z^+\}$  of all ordered pairs  $(m, n), m, n \in Z^+$  is denumerable.

**Proof.** Observe that a set is denumerable if the elements of the set can be listed in a row so that the elements can be called the first, the second, the third, etc. Keeping this in mind, we list the elements of  $Z^+ \times Z^+$  as follows:

$$(0, 0), (0, 1), (1, 0), (0, 2), (1, 1), (2, 0), (0, 3), (1, 2), \\ (2, 1), (3, 0), (0, 4), (1, 3), (2, 2), (3, 1), (4, 0), \dots$$

i.e. we first list the pair  $(0, 0)$ , then all pairs the sum of the entries of which is 1 starting with the pair having first entry 0, then all pairs  $(a, b)$  with  $a + b = 2$ , starting with  $(0, 2)$ , then all pairs  $(a, b)$  with  $a + b = 3$ , then  $a + b = 4$ , and so on every time the first pair being  $(0, a + b)$ . The above fashion lists all the elements of  $Z^+ \times Z^+$  showing that the set  $Z^+ \times Z^+$  is denumerable.

A careful examination of the first few terms of the above listing of elements of  $Z^+ \times Z^+$  suggests that there may be defined a map  $f : Z^+ \times Z^+ \rightarrow N$  by  $f(m, n) = (1/2)(m + n)(m + n + 1) + m + 1, m, n \in Z^+$  which gives the above listing.

**Exercise 1.3.** Prove that the map  $f : Z^+ \times Z^+ \rightarrow N$  defined above is injective. (Hint: Let  $(a, b), (c, d) \in Z^+ \times Z^+$  and suppose that  $f(a, b) = f(c, d)$ . Consider four possible cases, namely:

- (a)  $a \neq c, b \neq d, a + b \neq c + d$ .
- (b)  $a \neq c, b \neq d$  but  $a + b = c + d$ .
- (c)  $a = c, b \neq d$ .
- (d)  $a \neq c, b = d$ .

Now  $f(a, b) = f(c, d)$  implies that  $(a + b)^2 + 3a + b = (c + d)^2 + 3c + d$  which ultimately leads to  $(a + b + c + d + 1)(a - c + b - d) + 2(a - c) = 0$ .

This implies that  $a - c = km$  and  $a - c + b - d = -k$  or  $-2k$  for some positive integer  $k$ . The second alternative leads to  $a + b + c + d + 1 = m < a - c + 1$  which is obviously not possible. In the case of first alternative,  $a + b + c + d + 1 = 2(a - c)/k$ . For  $k > 1$ , this again leads to an obvious

contradiction, while for  $k = 1$ , this leads to  $a = b + 3c + d + 1$  which again can be shown to lead to a contradiction. In case  $(b - d)/(a - c)$  is an integer, we must have  $1 + (b - d)/(a - c) = -1$  and  $a + b + c + d + 1 = 2$ . This implies that three of  $a, b, c, d$  are zero and one of these is 1. This is a contradiction to case (i). Therefore, in case (i) it follows that  $f(a, b) = f(c, d)$  cannot happen (Cases (ii), (iii) and (iv) are much simpler than this case).

As a consequence of this result it follows that  $Z^+ \times Z^+$  may be identified with a subset of  $N$  and so is denumerable. Also the set  $N \times N$  being an infinite subset of the denumerable set  $Z^+ \times Z^+$  is denumerable. The set  $Z^+$  is also denumerable in view of the map  $f : Z^+ \rightarrow \mathbb{N}$  given by  $f(a) = a + 1$ ,  $a \in Z^+$  being bijective.

**Theorem 1.6.** The set  $Q$  of all rational numbers is denumerable.

**Proof.** We can prove this result in a few steps.

1. Consider the subset  $A = \{(m, n) \mid m, n \in N \text{ and } g.c.d(m, n) = 1\}$ . This is an infinite subset of the set  $N \times N$ . Since  $N \times N$  is denumerable,  $A$  is denumerable. Let  $Q^+$  be the set of all positive rational numbers. Define a map  $f : A \rightarrow Q^+$  by  $f(m, n) = m/n$ ,  $(m, n) \in N \times N$ . Since every positive rational number is of the form  $p/q$ , where  $p, q$  are positive integers and  $g.c.d(p, q) = 1$ , therefore  $p/q = f(p, q)$ . Thus  $f$  is onto. In fact, every positive rational number can be uniquely expressed in the form  $p/q$ ,  $p, q$  positive integers with  $g.c.d(p, q) = 1$ , the map  $f$  is one-one as well. Hence  $Q^+$  is denumerable.
2. We have proved in Example 1.5 that the map  $f : N \rightarrow Z$  given by  $f(m) = -m/2$  if  $m$  is even and  $(m + 1)/2$  if  $m$  is odd is bijective. Therefore, the set  $Z$  of integers is denumerable.

Define a map  $g : N \times N \rightarrow Z \times Z$  by  $g(m, n) = (f(m), f(n))$ ,  $m, n \in N$ . Let  $m, n, m', n' \in N$  and suppose that  $g(m, n) = g(m', n')$ . Then  $(f(m), f(n)) = (f(m'), f(n'))$  which implies that  $f(m) = f(m')$  and  $f(n) = f(n')$ . The map  $f$  being injective, it follows that  $m = m'$ ,  $n = n'$  or that  $(m, n) = (m', n')$ . Hence  $g$  is one-one. Let  $a, b \in Z$ . The map  $f$  being onto, there exist  $m, n \in N$  such that  $a = f(m)$  and  $b = f(n)$ . Then  $(a, b) = ((f(m), f(n)) = g(m, n)$ . Hence  $g$  is onto as well. Thus  $g$  is a bijective map. The set  $N \times N$  being denumerable, it follows that  $Z \times Z$  is denumerable.

3. Let  $B = \{(m, n) \mid m, n \in Z, n \neq 0 \text{ and } g.c.d(m, n) = 1\}$ . Then  $B$  is an infinite subset of the denumerable set  $Z \times Z$  and, so  $B$  is denumerable. Now define a map  $h : B \rightarrow Q$ , where  $Q$  is the set of all



**Proof.** If the set  $R$  of real numbers is denumerable, then every infinite subset of  $R$  is denumerable. However, we prove that the set of all real numbers in the interval  $(1, 2)$  is not denumerable. From this it will then follow that the set of real numbers is uncountable. We prove by contradiction that the set of real numbers in the interval  $(1, 2)$  is uncountable. So, suppose that the set of all real numbers in  $(1, 2)$  is denumerable. Let these numbers be listed as  $a_1, a_2, a_3, \dots, a_i, \dots$ .

Let the decimal representations of these numbers be

$$\begin{array}{cccccc} a_1 = 1.a_{11} & a_{12} & a_{13} & a_{14} & \dots & \\ a_2 = 1.a_{21} & a_{22} & a_{23} & a_{24} & \dots & \\ a_3 = 1.a_{31} & a_{32} & a_{33} & a_{34} & \dots & \\ \dots & \dots & \dots & & & \\ a_i = 1.a_{i1} & a_{i2} & a_{i3} & a_{i4} & \dots & \\ \dots & \dots & \dots & & & \end{array}$$

Then  $a_{ij}$  all belong to the set  $\{0, 1, 2, \dots, 9\}$ . Consider a real number  $b$  with decimal representation  $b = 1.b_1 b_2 b_3 \dots$  where the decimal digits  $b_1, b_2, b_3, \dots$  are defined by  $b_i = 3$ , if  $a_{ii} \neq 3$  i.e.

$$a_{ii} \in \{0, 1, 2, 4, 5, 6, 7, 8, 9\} \quad \text{and} \quad b_i = 4 \text{ if } a_{ii} = 3.$$

Thus  $b_i \neq a_{ii}$  for any  $i$  or  $b_i$  is not the  $i$ th decimal digit of  $a_i$  for any  $i$ . Two numbers are equal if and only if the corresponding entries in the decimal representations of the two are equal. It follows that the number  $b$  does not appear in the above listing of the real numbers in the interval  $(1, 2)$ . However,  $1 < b < 2$  so that  $b \in (1, 2)$ . This is a contradiction and it follows that the set of real numbers in the interval  $(1, 2)$  is not denumerable and, hence,  $R$  is uncountable.

**Remark:** The procedure given for proving that the set of positive rational numbers is denumerable can also be used to prove that *a denumerable union of denumerable sets is denumerable*.

## 1.6. Some Special Maps (Functions)

In this section we give a brief description of some functions defined on real numbers which are quite useful and may appear frequently. These include, among others, polynomial functions, logarithmic functions and exponential functions. In a polynomial function every real number  $x$  is associated with a polynomial in  $x$  such as  $f(x) = 2x + 1$ ,  $f(x) = x^2 + x + 1$ ,  $f(x) =$

$1/2x^2 - x + 1$  etc. In general, a polynomial function may neither be one-one, nor onto. However, a linear polynomial function such as  $f(x) = ax + b$ , where  $a, b$  are fixed real numbers, is always one-one as well as onto. Observe that in a linear polynomial function  $f(x) = ax + b$ ,  $x \in R$ ,  $a$  is non-zero. In case  $a$  is zero, this function no longer remains a linear function and becomes a constant function which associates the fixed real number  $b$  to every real number  $x$ . The function  $f(x) = x^2$ ,  $x \in R$  is neither one-one, nor onto as there is no real number  $x$  for which  $x^2 = -1$  and  $f(1) = 1^2 = (-1)^2 = f(-1)$ .

In **logarithmic function**  $f(x) = \log^x$  to every real number  $x$  is associated the unique real number  $a$  such that  $x = 2^a$ . Observe that for every real number  $a$ ,  $2^a > 0$ . Thus the logarithmic function is defined on the set of positive real numbers. We have used the notation  $\log^x$  for the logarithm of  $x$  to the base 2. Logarithmic functions may be defined to any base  $b$ . In that case we write  $\log_b^x$  to mean the number  $a$  such that  $x = b^a$  and call  $\log_b^x$  to be the logarithm of  $x$  to the base  $b$ . When the base of logarithm is the number 10, we call such a logarithm as natural logarithm and we write  $\log_{10}^x$  as  $\ln x$ .

Another function that is defined on the set  $N$  of natural numbers and called the **factorial function** is defined for every natural number  $n$  as  $f(n) = n! = n(n-1) \dots 1$  (i.e. the product of the first  $n$  natural numbers) and is called factorial  $n$ . We define  $0! = 1$ . Observe that  $3! = 3 \times 2 \times 1 = 6$ ,  $5! = 5 \times 4 \times 3 \times 2 \times 1 = 120$  and  $7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 5040$ .

We next define two other functions from the set of all real numbers to the set of integers.

**Definition.** The **floor function** denoted by  $\lfloor \ ]$  is the function:  $R \rightarrow Z$  which assigns to the real number  $x$  the largest integer which is less than or equal to  $x$ . Thus  $\lfloor x \rfloor$  denotes the largest integer  $\leq x$ . On the other hand we define the **ceiling function** denoted by  $\lceil \ ]$ :  $R \rightarrow Z$  to be the function which associates to the real number  $x$  the smallest integer which is greater than or equal to the real number  $x$ . Thus  $\lceil x \rceil$  is the smallest integer  $\geq x$ . Observe that

- (a)  $\lfloor x \rfloor = \lceil x \rceil$  for every integer  $x$ ;
- (b) both the floor function  $\lfloor \ ]$  and the ceiling function  $\lceil \ ]$  are onto;
- (c) neither of the functions  $\lfloor \ ]$  and  $\lceil \ ]$  is one-one.

The floor function is also sometimes called **the greatest integer function** and analogously the ceiling function may be called **the least integer function**.

In analysis both floor function and the ceiling function are cited as functions which have infinitely many discontinuities. These functions are in fact discontinuous for every  $x \in \mathbb{Z}$ . To fix up our ideas about these functions, note that

$$\begin{aligned} \lfloor 1/3 \rfloor &= 0; & \lceil 1/3 \rceil &= 1; & \lfloor -1/3 \rfloor &= -1; & \lceil -1/3 \rceil &= 0; & \lfloor 2.3 \rfloor &= 2; \\ \lceil 2.3 \rceil &= 3; & \lfloor \sqrt{5} \rfloor &= 2; & \lceil \sqrt{5} \rceil &= 3. \end{aligned}$$

The following properties of the floor and the ceiling function are clear from their definitions. If  $n$  is an integer, then

- (a)  $\lfloor x \rfloor = n$  if and only if  $n \leq x < n + 1$ ;
- (b)  $\lceil x \rceil = n$  if and only if  $x - 1 < n \leq x$ ;
- (c)  $\lfloor x \rfloor = n$  if and only if  $n - 1 < x \leq n$ ;
- (d)  $\lceil x \rceil = n$  if and only if  $x \leq n < x + 1$ .

Combining (b) and (d) above, we also have

$$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1.$$

The floor and the ceiling functions for  $x$  and  $-x$  are related by

- (e)  $\lfloor -x \rfloor = -\lceil x \rceil$ ; (f)  $\lceil -x \rceil = -\lfloor x \rfloor$ .

For (e), let  $\lceil x \rceil = n$ . Then by (d) above  $x \leq n < x + 1$ . This leads to  $-x \geq -n > -x - 1$  or  $-x - 1 < -n \leq -x$  which by (b) implies that  $-n = \lfloor -x \rfloor$ . Hence  $\lfloor -x \rfloor = -\lceil x \rceil$ . The result (f) may be proved on similar lines by using (a) and (c).

**Theorem 1.8.** For any integer  $n$  and real number  $x$ ,

- (a)  $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ ; (b)  $\lceil x + n \rceil = \lceil x \rceil + n$ .

**Proof.** Suppose that  $\lfloor x \rfloor = m$ , where  $m$  is an integer. Then by (c) above  $m - 1 < x \leq m$ . Adding  $n$  to the numbers in this inequality, we have  $m + n - 1 < n + x \leq m + n$  in which  $m + n$  is again an integer. By (c) again,  $\lfloor n + x \rfloor = m + n = \lfloor x \rfloor + n$ . This proves (b) above. The result (a) may be proved on similar lines.

**Theorem 1.9.** For any real number  $x$ , prove that

$$\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor.$$

**Proof.** Let  $x = n + \epsilon$ , where  $n$  is an integer and  $\epsilon$  is a real number with  $0 \leq \epsilon < 1$ . Then by the definition of the floor function  $\lfloor x \rfloor = n$ . We consider two cases:  $\epsilon < 1/2$  and  $\epsilon \geq 1/2$ .

Case (a)  $0 \leq \epsilon < 1/2$ . Then  $0 \leq 2\epsilon < 1$ . Therefore  $2x = 2n + 2\epsilon$  where  $2n$  is an integer and  $0 \leq 2\epsilon < 1$ . Hence  $\lfloor 2x \rfloor = 2n$ . Also  $x + 1/2 = n + \epsilon + 1/2$  and  $0 \leq \epsilon + 1/2 < 1$ . Therefore  $\lfloor x + 1/2 \rfloor = n$ . Hence

$$\lfloor 2x \rfloor = 2n = n + n = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor.$$

Case (b)  $1/2 \leq \epsilon < 1$ . Then  $1 \leq 2\epsilon < 2$  or  $0 \leq 2\epsilon - 1 < 1$ . Now  $2x = 2n + 2\epsilon = 2n + 1 + (2\epsilon - 1)$ , with  $0 \leq 2\epsilon - 1 < 1$ , so that  $\lfloor 2x \rfloor = 2n + 1$ . Also  $x + 1/2 = n + \epsilon + 1/2 = n + 1 + (\epsilon - 1/2)$ , with  $0 \leq \epsilon - 1/2 < 1/2$ . Therefore  $\lfloor x + 1/2 \rfloor = n + 1$ . Thus  $\lfloor 2x \rfloor = 2n + 1 = n + n + 1 = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor$ .

**Example 1.6.** Data stored on a computer disc or transmitted over a data network are usually expressed as strings of bytes. Each byte is made up of 8 bits. How many bytes are required to encode 125 bits of data?

**Solution.** To determine the number of bytes needed, we need to divide 125 by 8. The quotient which is 15 is such that 15 bytes will be able to store  $15 \times 8 = 120$  bits of data. We are still left with 5 bits of data for which another byte will be used. Then the number of bytes needed is 16 which equals  $\lceil 125/8 \rceil$  i.e. the smallest integer which is  $\geq 125/8$ .

**Example 1.7.** In asynchronous transfer mode (ATM) (which is a communications protocol used on backbone networks), data are organized into cells of 53 bytes. How many ATM cells can be transmitted in one minute over a connection that transmits data at the rate of 128 kilobits per second?

**Solution.** In one minute, this connection can transmit  $128000 \times 60 = 7680000$  bits. Each ATM cell is 53 bytes long i.e. it is  $53 \times 8 = 424$  bits long. Then the number of cells that can be transmitted in 1 minute is  $\leq 7680000/424$  and it has to be a whole number i.e. an integer. This means that  $\lfloor 7680000/424 \rfloor = \lfloor 18113 + 11/53 \rfloor = 18113$  ATM cells can be transmitted in 1 minute over a 128 kilobits per second connection.

**Exercise 1.4.** How many ATM cells as described in the above example can be transmitted in 10 seconds over a link operating at the rate of

- (a) 300 kilobits per second?
- (b) 500 kilobits per second?
- (c) 1 megabit per second (1 megabit = 1,000,000 bits)?

### 1.6.1. The characteristic function

Let  $U$  be a universal set. For any subset  $A$  of  $U$ , we can define a map  $f_A : U \rightarrow B = \{0, 1\}$  by  $f_A(x) = 0$  if  $x \notin A$  and  $1$  if  $x \in A$ .

The map  $f_A$  is called the **characteristic function of  $A$** . The characteristic functions of the subsets of the universal set  $U$  have the following properties:

**Theorem 1.10.** Let  $A, B$  be subsets of  $U$ . Then, for every  $x \in U$ ,

- (a)  $f_{A \cap B}(x) = f_A(x)f_B(x)$ ;
- (b)  $f_{A \cup B}(x) = f_A(x) + f_B(x) - f_A(x)f_B(x)$ ;
- (c)  $f_{A'}(x) = 1 - f_A(x)$ ;
- (d)  $f_{A \oplus B}(x) = f_A(x) + f_B(x) - 2f_A(x)f_B(x)$ .

**Proof.** (a) If  $x \in A \cap B$ , then  $x \in A$  and  $x \in B$  so that  $f_{A \cap B}(x) = 1 = f_A(x)f_B(x)$ . If  $x \notin A \cap B$ , then either  $x \notin A$  or  $x \notin B$  and we have  $f_A(x) = 0$  or  $f_B(x) = 0$  and  $f_{A \cap B}(x) = f_A(x)f_B(x)$ .

(b) If  $x \in A \cup B$ , then either  $x$  belongs to both  $A$  and  $B$  or  $x$  belongs to one of  $A, B$  and not the other. In the first case

$$1 = f_{A \cup B}(x) = f_A(x) + f_B(x) - f_A(x)f_B(x)$$

while in the other case one of  $f_A(x), f_B(x)$  is zero and the other is 1.

Therefore,  $f_A(x) + f_B(x) - f_A(x)f_B(x) = 1 = f_{A \cup B}(x)$ .

If  $x \notin A \cup B$ , then  $x \notin A$  and  $x \notin B$  so all three of  $f_{A \cup B}(x), f_A(x)$  and  $f_B(x)$  are 0 and, so,  $f_{A \cup B}(x) = f_A(x) + f_B(x) - f_A(x)f_B(x)$ .

(c)  $x \in A'$  if and only if  $x \notin A$ . Therefore one of  $f_A(x), f_{A'}(x)$  is 0 and the other is 1. It then follows that  $f_{A'}(x) = 1 - f_A(x)$ .

(d) Recall that  $A \oplus B = (A - B) \cup (B - A) = A \cup B - A \cap B$ . If  $x \in A \oplus B$ , then  $x \in A \cup B$  but  $x \notin A \cap B$  and one of  $f_A(x), f_B(x)$  is 1 and the other is 0 but  $f_{A \cap B}(x) = 0$ . Therefore

$$1 = f_{A \oplus B}(x) = f_A(x) + f_B(x) - 2f_A(x)f_B(x).$$

On the other hand, if  $x \notin A \oplus B$ , then  $x \notin A \cup B - A \cap B$ . This means that either  $x \in A \cap B$  or  $x \notin A$  and  $x \notin B$  i.e. either  $x$  is in both  $A$  and  $B$  or  $x$  is in neither of  $A, B$ . In the first case  $f_A(x) + f_B(x) - 2f_A(x)f_B(x) = 1 + 1 - 2 \cdot 1 = 0$  while in the second case  $f_A(x) + f_B(x) - 2f_A(x)f_B(x) = 0$ . Thus in both the cases  $f_{A \oplus B}(x) = 0 = f_A(x) + f_B(x) - 2f_A(x)f_B(x)$ .

Consider the universal set  $U$  and the power set  $\wp(U)$  of  $U$  i.e. the set of all subsets of  $U$ . To every subset  $A$  of  $U$  corresponds a function  $f_A : U \rightarrow \mathbb{B}$ . Thus we obtain a collection of maps (**characteristic maps**) the elements

of which are in one-to-one correspondence with the subsets of  $U$ . This set or collection of maps is denoted by  $B^U$  i.e.

$$B^U = \{f_A : U \rightarrow B \mid A \in \wp(U)\}.$$

### 1.7. Partitions of Sets

**Definition.** Let  $A$  be non-empty set. A collection or set  $\{A_i, i \in K$ , of subsets  $A_i$  of  $A$ , where  $K$  is an index set is called a partition of  $A$  if

- (a)  $A_i \neq \emptyset$  for every  $i \in K$ ;
- (b)  $A_i \cap A_j = \emptyset$  for  $i, j \in K$  and  $i \neq j$ ,
- (c)  $A = \cup A_i$ , where  $i$  runs over all the elements of  $K$ .

Each subset  $A_i$  of  $A$  appearing in the partition is called a **block** of the partition.

Partitions of sets appear in a natural way in the study of groups and rings. In fact the collection of all left cosets of a subgroup  $H$  of a group  $G$  provides a partition of the set  $G$ . We shall consider this problem later while studying groups. Another situation where partitions appear naturally arises while studying equivalence relations on sets. Indeed, equivalence classes determined by an equivalence relation on a set provide a partition of the set. We study these also later in the book. A set can have many partitions.

**Example 1.8.** If  $A = \{1, 2, 3\}$ , then  $P_1 = \{\{1\}, \{2\}, \{3\}\}$ ,  $P_2 = \{\{1, 2\}, \{3\}\}$ ,  $P_3 = \{\{1\}, \{2, 3\}\}$ ,  $P_4 = \{\{2\}, \{1, 3\}\}$  are partitions of  $A$ .

**Example 1.9.** If  $A = \{1, 2, 3, 4\}$ , then

$$\begin{aligned} P_1 &= \{\{1\}, \{2\}, \{3\}, \{4\}\}, & P_2 &= \{\{1\}, \{2\}, \{3, 4\}\}, \\ P_3 &= \{\{1\}, \{3\}, \{2, 4\}\}, & P_4 &= \{\{1\}, \{4\}, \{2, 3\}\}, \\ P_5 &= \{\{2\}, \{3\}, \{1, 4\}\}, & P_6 &= \{\{2\}, \{4\}, \{1, 3\}\}, \\ P_7 &= \{\{3\}, \{4\}, \{1, 2\}\}, & P_8 &= \{\{1, 2\}, \{3, 4\}\}, \\ P_9 &= \{\{1, 3\}, \{2, 4\}\}, & P_{10} &= \{\{1, 4\}, \{2, 3\}\}, \\ P_{11} &= \{\{1\}, \{2, 3, 4\}\}, & P_{12} &= \{\{2\}, \{1, 3, 4\}\}, \\ P_{13} &= \{\{3\}, \{1, 2, 4\}\}, & P_{14} &= \{\{4\}, \{1, 2, 3\}\} \end{aligned}$$

are some partitions of  $A$ . However,  $\{\{1\}, \{2, 3\}, \{1, 2\}\}$  is not a partition of the set  $\{1, 2, 3\}$  nor is  $\{\{1, 2\}, \{2, 3\}\}$  a partition of this set. Similarly  $\{\{1, 2\}, \{2, 3, 4\}\}$ ,  $\{\{1, 2\}, \{2, 3\}, \{4\}\}$ ,  $\{\{1, 4\}, \{2, 3\}, \{4\}\}$  are not partitions of the set  $\{1, 2, 3, 4\}$ .

**Example 1.10.** The collection  $\{2Z, 2Z + 1\}$ , where  $2Z$  is the set of all even integers and  $2Z + 1$  is the set of all odd integers, is a partition of the set of all integers. Another partition of  $Z$  is  $\{3Z, 3Z + 1, 3Z + 2\}$ , where  $3Z + i, 0 \leq i \leq 2$  is the set of integers which on division by 3 leave the remainder  $i$ .

**Example 1.11.** Recall that a complex number  $a + ib$ , where  $a, b$  are real numbers, is called pure imaginary if  $a = 0$  but  $b \neq 0$ . Let  $iR^*$  denote the set of all pure imaginary numbers, with  $i = \sqrt{-1}$ . Then the collection  $\{R, iR^*\}$  is a partition of the set  $C$  of complex numbers.

**Example 1.12.** Consider the set  $A$  of the English alphabet,  $V$  the set of vowels and  $C$  the set of consonants in  $A$ . Then  $\{V, C\}$  is a partition of the set  $A$ .

For a set  $A$ , the collection  $\{A\}$  has only one element, namely the set  $A$  itself also provides a partition of the set  $A$ . Such a partition is called **trivial partition**. It is only non-trivial partitions which are of interest.

For obtaining partitions of a subset  $B$  of a set  $A$  from a given partition of the set  $A$ , we have

**Theorem 1.11.** Let  $A$  be a non-empty set,  $B$  be a non-empty subset of  $A$  and  $\{A_i\}, i \in K$  be a partition of  $A$ . Then  $\{A_i \cap B | i \in K \text{ with } A_i \cap B \neq \varphi\}$  is a partition of  $B$ .

**Proof.** Let  $J$  be a subset of  $K$  consisting of all  $j \in K$  for which  $A_j \cap B \neq \varphi$ . Let  $b \in B$ . Then  $b \in A = \cup A_i, i \in K$ . Thus, there exists a  $j \in K$  such that  $b \in A_j$ . Then  $b \in A_j \cap B$  and  $A_j \cap B \neq \varphi$ . This proves that  $j \in J$  and, so,  $J \neq \varphi$ . The above also proves that  $B \subseteq \cup(A_j \cap B)$  where  $j$  runs over all the elements of  $J$ . As  $A_j \cap B \subseteq B$  for every  $j \in J$ ,  $\cup(A_j \cap B) \subseteq B$ . Hence  $B = \cup(A_j \cap B)$ .

Consider  $A_i \cap B$  and  $A_j \cap B$ , where  $i, j \in J$  and  $i \neq j$ . Then  $A_i \cap A_j = \varphi$  and  $(A_i \cap B) \cap (A_j \cap B) = (A_i \cap A_j) \cap B = \varphi \cap B = \varphi$ . This completes the proof that  $\{A_j \cap B | j \in J\}$  is a partition of  $B$ .

**Definition.** A partition  $\varphi = \{B_i | i \in L\}$  of a set  $A$  is called a **refinement of a partition**  $\Pi = \{A_i | i \in K\}$  of  $A$  if for every  $i \in L, B_i$  is a subset of  $A_j$  for some  $j \in K$ . If for some  $i \in L, B_i$  is a proper subset of some  $A_j, j \in K$ , then  $\varphi$  is called a **proper refinement** of  $\Pi$ . Every partition  $\Pi$  of  $A$  is a refinement of itself.

Consider a partition  $\Pi = \{\{1\}, \{2, 3\}, \{4, 5\}\}$  of the set  $A = \{1, 2, 3, 4, 5\}$ . Then  $\Pi_1 = \{\{1\}, \{2\}, \{3\}, \{4, 5\}\}$ ,  $\Pi_2 = \{\{1\}, \{2, 3\}, \{4\}, \{5\}\}$  and

$\Pi_3 = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}$  are refinements of  $\Pi$  but  $\{\{1, 2\}, \{3\}, \{4, 5\}\}$  is not a refinement of  $\Pi$ . Observe that  $\Pi, \Pi_1, \Pi_2, \Pi_3$  are the only possible refinements of  $\Pi$ .

### Exercise 1.5.

1. Find all possible nontrivial partitions of the set  $A = \{1, 2, 3, 4, 5\}$ .
2. If  $A = \{1, 2\}$  there is one nontrivial partition of  $A$ , namely  $\{\{1\}, \{2\}\}$ . For  $A = \{1, 2, 3\}$ , we have calculated all the possible partitions of  $A$  and these are 4 in number. For a set having 4 elements, we have obtained 14 nontrivial partitions which are all the possible ones. For a set having 5 elements, prove or disprove that the number of nontrivial partitions is 66. If this number is not 66, find the correct number.
3. For a set having 5 elements, find the number of partitions having two blocks each.
4. For a set having 6 elements, find the number of partitions having (i) two blocks each; (ii) three blocks each.
5. Among the partitions  $P_1, P_2, P_3, P_4$  of  $A = \{1, 2, 3\}$  obtained in Example 1.8, decide the partitions which are refinements of some other partitions.
6. Among the partitions  $P_1$  to  $P_{14}$  of  $A = \{1, 2, 3, 4\}$  obtained in Example 1.9, determine the partitions which are refinements of some other partitions.
7. Prove that every refinement  $P_1$  of a partition  $P$  of a non-empty set  $A$ ,  $P_1 \neq P$ , is a proper refinement of  $P$ .

### 1.8. The Minset and Maxset Normal Forms

Let  $X$  be a universal set and  $\{A_i\}, 1 \leq i \leq r$  be a collection of subsets of  $X$ . A set obtained from  $\varphi, X$  and  $A_1, A_2, \dots, A_r$  by the use of set operations (complementation),  $\cup$  and  $\cap$  is called a set generated by  $A_1, A_2, \dots, A_r$ . Consider, for example, two subsets  $A, B$  of  $X$ . Then

$$\begin{aligned} &\varphi, X, A, B, A', B', A \cap B, A \cap B', A' \cap B, A' \cap B', A \cup B, A \cup B', \\ &A' \cup B \quad \text{and} \quad A' \cup B' \end{aligned} \tag{1.3}$$

are some of the sets generated by  $A, B$ .

**Example 1.13.** Consider sets generated by  $A, B$  which involve three of the sets  $A, A', B, B'$ . Such sets are of the form

$$(A^* \cup B^*) \cup C, \quad (A^* \cup B^*) \cap C, \quad (A^* \cap B^*) \cup C, \quad (A^* \cap B^*) \cap C \tag{1.4}$$

where  $A^*$  is  $A$  or  $A'$ ,  $B^*$  is  $B$  or  $B'$  and  $C$  is either  $A$  or  $A'$  or  $B$  or  $B'$ .

We consider the case when  $C$  is either  $A$  or  $A'$ . Observe that

$$\begin{aligned}
 (A^* \cup B^*) \cup C &= A^* \cup B^* && \text{if } C = A^* \\
 &= X && \text{if } C \neq A^*; \\
 (A^* \cup B^*) \cap C &= (A^* \cap C) \cup (B^* \cap C) \\
 &= A^* && \text{if } C = A^* \\
 &= B^* \cap C && \text{if } C \neq A^*; \\
 (A^* \cap B^*) \cup C &= (A^* \cup C) \cap (B^* \cup C) \\
 &= A^* && \text{if } C = A^* \\
 &= B^* \cup C && \text{if } C \neq A^*; \\
 (A^* \cap B^*) \cap C &= A^* \cap B^* && \text{if } C = A^* \\
 &= \varphi && \text{if } C \neq A^*.
 \end{aligned}$$

Thus the sets in (1.4) are sets generated by  $A, B$  involving two of  $A, B, A', B'$ . Interchanging  $A$  and  $B$  in the above argument, we can prove that the sets in (1.4) when  $C$  is either  $B$  or  $B'$  are also sets generated by  $A, B$  involving at most two of  $A, B, A', B'$ . By using iteration or a simple induction argument, we can prove that the sets in (1.3) are all the possible sets generated by  $A, B$ . An argument similar to the above also gives

**Theorem 1.12.** Every set generated by a collection  $\{A_i\}$ ,  $1 \leq i \leq r$  of subsets of  $X$  involves at most  $r$  of the sets  $A_1, \dots, A_r, A'_1, \dots, A'_r$ .

Let  $\{A_i\}$ ,  $1 \leq i \leq r$ , be a collection (or set) of subsets of a universal set  $X$ . A set of the form  $\cap A_i^*$ ,  $1 \leq i \leq r$ , where each  $A_i^*$  is either  $A_i$  or  $A'_i$  is called a **minset** or **minterm generated by**  $A_1, A_2, \dots, A_r$ . Since every  $A_i^*$  has two choices, there are  $2^r$  such minsets.

For example, if we consider a set

- (a)  $\{A_1, A_2\}$  of two subsets of  $X$ , the minsets generated by  $A_1, A_2$  are

$$A_1 \cap A_2, A_1 \cap A'_2, A'_1 \cap A_2, \quad \text{and} \quad A'_1 \cap A'_2.$$

- (b)  $\{A_1, A_2, A_3\}$  of three subsets of  $X$ , then the minsets generated by  $A_1, A_2, A_3$  are

$$\begin{aligned}
 &A_1 \cap A_2 \cap A_3, \quad A_1 \cap A_2 \cap A'_3, \quad A_1 \cap A'_2 \cap A_3, \quad A'_1 \cap A_2 \cap A_3, \\
 &A_1 \cap A'_2 \cap A'_3, \quad A'_1 \cap A'_2 \cap A_3, \quad A'_1 \cap A_2 \cap A'_3 \quad \text{and} \quad A'_1 \cap A'_2 \cap A'_3.
 \end{aligned}$$

All minsets need not be non-empty. Consider for example,

$$X = \{1, 2, \dots, 9\}, A_1 = \{1, 2\} \text{ and } A_2 = \{3, 4\}.$$

One of the minsets in this case is  $A_1 \cap A_2$  which is the empty set. In general, if we take  $r$  subsets  $A_i$ ,  $1 \leq i \leq r$  of  $X$  such that  $\cap A_i = \varphi$ , then one of the minsets is the empty set. Also, if one of the subsets  $A_1, A_2, \dots, A_r$ , say  $A_r$ , is the universal set  $X$  itself, then all minsets in which  $A_r$  appears are the empty set. This situation may be avoided by taking all the subsets  $A_1, A_2, \dots, A_r$  proper.

The concept of minsets is related to the partitions of a set and this relationship is provided by

**Theorem 1.13.** The set of all non-empty minsets generated by  $A_1, A_2, \dots, A_r$  constitutes a partition of the set  $X$ .

**Proof.** It is enough to prove that every  $x \in X$  belongs to one and only one minset. Let  $x \in X$ . For any  $i$ ,  $1 \leq i \leq r$ ,  $x \in A_i$  or  $x \in A'_i$ . Thus there exists a minset  $\cap A_i^*$ ,  $1 \leq i \leq r$ , to which  $x$  belongs. If possible, suppose that  $x$  belongs to two distinct minsets, say,  $\cap B_i$  and  $\cap D_i$ , where for every  $i$ ,  $B_i = A_i$  or  $A'_i$  and for every  $j$ ,  $D_j = A_j$  or  $A'_j$ . The two minsets being distinct, there exists an  $i$ ,  $1 \leq i \leq r$ , such that  $B_i \neq D_i$ . But  $B_i$  being either  $A_i$  or  $A'_i$  and similarly for  $D_i$ , in one of the minsets  $A_i$  appears while in the other  $A'_i$  appears. But  $\cap B_j \subseteq B_i$  and  $\cap D_j \subseteq D_i$ . Therefore  $x \in B_i \cap D_i = A_i \cap A'_i = \varphi$  — which is a contradiction. Thus every  $x \in X$  belongs to one and only one minset.

Observe that later half of the above proof amounts to proving that *every two distinct minsets are disjoint*.

For the sake of convenience a minset  $\cap A_i^*$ ,  $1 \leq i \leq r$ , is denoted by  $M_{\delta_1 \delta_2 \dots \delta_r}$  where each  $\delta_i$  is either 0 or 1 according to the rule that  $\delta_i = 0$  if  $A_i^* = A'_i$  and  $\delta_i = 1$  if  $A_i^* = A_i$ . For example, if  $A, B, C$  are three subsets of  $X$  and we think of  $A$  as  $A_1, B$  as  $A_2$  and  $C$  as  $A_3$ , then

$$\begin{aligned} M_{111} &= A \cap B \cap C, & M_{110} &= A \cap B \cap C', & M_{101} &= A \cap B' \cap C, \\ M_{011} &= A' \cap B \cap C, & M_{100} &= A \cap B' \cap C', & M_{010} &= A' \cap B \cap C', \\ M_{001} &= A' \cap B' \cap C, & M_{000} &= A' \cap B' \cap C'. \end{aligned}$$

**Example 1.14.** Consider subsets  $A, B$  of  $X$ . As already seen, all the sets generated by  $A, B$  are given in (1.3). Moreover, all the minsets generated by  $A, B$  are

$$A \cap B, \quad A \cap B', \quad A' \cap B, \quad A' \cap B'.$$

By Theorem 1.13.,

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

Then

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

Similarly,

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

Also then

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

Thus all non-empty sets generated by  $A, B$  have been expressed as union of some minsets generated by  $A, B$ . This result is true in general and we have

**Theorem 1.14.** Every set generated by  $A_1, A_2, \dots, A_r$  is either  $\varphi$  or is equal to a union of distinct minsets generated  $A_1, A_2, \dots, A_r$ .

When a set is  $\varphi$  or is expressed as a union of distinct minsets, it is said to be in **minset normal form** or **minset canonical form**.

**Example 1.15.** Consider three subsets  $A, B, C$  of a universal set  $X$ . The minsets generated by  $A, B, C$  are

$$\begin{aligned} A \cap B \cap C, \quad A \cap B \cap C', \quad A \cap B' \cap C, \quad A' \cap B \cap C, \quad A \cap B' \cap C', \\ A' \cap B \cap C', \quad A' \cap B' \cap C \quad \text{and} \quad A' \cap B' \cap C'. \end{aligned}$$

Then, proceeding as in Example 1.14, we get

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

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

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

and  $A', B', C'$  can be obtained from the expressions for  $A, B, C$  by changing  $A$  to  $A', B$  to  $B'$  and  $C$  to  $C'$  respectively. Thus

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

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

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

Once these are obtained, any non-empty set generated by  $A, B, C$  can then be expressed as union of distinct minsets by substituting for  $A, B, C, A', B', C'$  from above. For example,

$$\begin{aligned} & (A \cap B') \cup (B \cap (A \cup C')) \\ &= (A \cap B') \cup ((B \cap A) \cup (B \cap C')) \\ &= ((A \cap B') \cup (A \cap B)) \cup (B \cap C') \\ &= (A \cap (B' \cup B)) \cup (B \cap C') \\ &= (A \cap X) \cup (B \cap C') \\ &= A \cup (B \cap C') \\ &= (A \cup B) \cap (A \cup C') \\ &= (A \cup (A' \cap B \cap C) \cup (A' \cap B \cap C')) \cap ((A \cup (A' \cap B \cap C')) \\ &\quad \cup (A' \cap B' \cap C')) \\ &= ((A \cup (A' \cap B \cap C')) \cup (A' \cap B \cap C)) \cap ((A \cup (A' \cap B \cap C')) \\ &\quad \cup (A' \cap B' \cap C')) \\ &= (A \cup (A' \cap B \cap C')) \cup ((A' \cap B \cap C) \cap (A' \cap B' \cap C')) \\ &= (A \cup (A' \cap B \cap C)) \cup \varphi \\ &= A \cup (A' \cap B \cap C') \\ &= (A \cap B \cap C) \cup (A \cap B \cap C') \cup (A \cap B' \cap C) \cup (A \cap B' \cap C') \\ &\quad \cup (A' \cap B \cap C'). \end{aligned}$$

**Exercise 1.6.** Find the minimal normal form of  $((A \cup D') \cap (B' \cup C')) \cup (A \cap B \cap D)$  generated by  $A, B, C, D$ .

**Definition.** Let  $\{A_i\}$ ,  $1 \leq i \leq r$ , be a collection of subsets of a universal set  $X$ . Then a set of the form  $\cup A_i^*$ ,  $1 \leq i \leq r$ , where for every  $i$ ,  $1 \leq i \leq r$ ,  $A_i^*$  is either  $A_i$  or  $A'_i$ , is called a **maxset** generated by  $A_1, A_2, \dots, A_r$ . As in the case of minsets, there are  $2^r$  maxsets generated by  $A_1, A_2, \dots, A_r$ .

Observe that  $(\cup A_i^*)' = \cap (A_i^*)'$  and for every  $i$ ,  $1 \leq i \leq r$ ,  $(A_i^*)'$  is either  $A_i$  or  $A'_i$ . Thus every maxset generated by  $A_1, A_2, \dots, A_r$  is the complement of a minset generated by  $A_1, A_2, \dots, A_r$  and conversely. Similar to the expression for minsets, a maxset  $\cup A_i^*$  generated by  $A_1, A_2, \dots, A_r$  is denoted by  $\tilde{M}_{\delta_1 \delta_2 \dots \delta_r}$ , where every  $\delta_i$  is either 0 or 1 with  $\delta_i = 0$  if  $A_i^* = A_i$  and  $\delta_i = 1$  if  $A_i^* = A'_i$ . Writing  $A$  as  $A_1, B$  as  $A_2$  and  $C$  as  $A_3$ , we observe that the maxset  $A' \cup B \cup C'$  is  $\tilde{M}_{101}$ . However  $A' \cup B \cup C' = (A \cap B' \cap C) = M'_{101}$ . In general (it is clear from the definition of minset and maxset) that  $\tilde{M}_{\delta_1 \delta_2 \dots \delta_r} = M'_{\delta_1 \delta_2 \dots \delta_r}$ . In view of this relationship between minsets and maxsets and Theorem 1.14 we have

**Theorem 1.15.** Every set generated by  $A_1, A_2, \dots, A_r$  is either  $X$  or is an intersection of distinct maxsets generated by  $A_1, A_2, \dots, A_r$ .

When a set generated by  $A_1, A_2, \dots, A_r$  is expressed as  $X$  or as an intersection of distinct maxsets, it is said to be in a **maxset normal form** or **maxset canonical form**.

**Example 1.16.** Consider subsets  $A, B$  of the universal set  $X$ . The maxsets generated by  $A, B$  are  $A \cup B, A \cup B', A' \cup B$  and  $A' \cup B'$ .

Then

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

Similarly

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

**Example 1.17.** Consider the case of three subsets  $A, B, C$  of  $X$ . The maxsets generated by  $A, B, C$  are

$$\begin{aligned} A \cup B \cup C, \quad A \cup B' \cup C, \quad A \cup B \cup C', \quad A' \cup B \cup C, \quad A \cup B' \cup C', \\ A' \cup B \cup C', \quad A' \cup B' \cup C \quad \text{and} \quad A' \cup B' \cup C'. \end{aligned}$$

In this case

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

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

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

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

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

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

We next obtain a maxset normal form of  $(A \cap B) \cup (A' \cap C)$ .

Using the values of  $A, A'$  etc. obtained above

$$A \cap B = \{(A \cup B \cup C) \cap (A \cup B' \cup C) \cap (A \cup B \cup C') \cap (A \cup B' \cup C') \\ \cap (A' \cup B \cup C) \cap (A' \cup B \cup C')\}$$

and

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

Set

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

Then  $A \cap B = L \cap (A \cup B' \cup C') \cap (A \cup B \cup C')$  and

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

Now

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

and

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

Therefore

$$(A \cap B) \cup (A' \cap C) = (L \cap (A \cup C')) \cup (L \cap (A' \cup B')) \\ = L \cap (A \cup C' \cup A' \cup B') \\ = L \cap (A \cup A' \cup C' \cup B') \\ = L \cap X = L.$$

Hence

$$(A \cap B) \cup (A' \cap C) = \{(A \cup B \cup C) \cap (A \cup B' \cup C) \cap (A' \cup B \cup C) \cap (A' \cup B \cup C')\}$$

is the required maxset normal form representation of  $(A \cap B) \cup (A' \cap C)$ .

Unlike the set of all minsets generated by  $A_1, A_2, \dots, A_r$ , the set of all maxsets generated by  $A_1, A_2, \dots, A_r$  does not provide a partition of the set  $X$ . In fact every two distinct maxsets need not be disjoint. For example,  $A_1 \cup A_2 \cup \dots \cup A_r$  and  $A'_1 \cup A_2 \cup \dots \cup A_r$  are distinct maxsets and  $(A_1 \cup A_2 \cup \dots \cup A_r) \cap (A'_1 \cup A_2 \cup \dots \cup A_r) = (A_1 \cap A'_1) \cup (A_2 \cup \dots \cup A_r) = A_2 \cup A_3 \cup \dots \cup A_r$  which is not an empty set.

We end this section with the following

**Theorem 1.16.** Minset normal form (or maxset normal form) of a set  $S$  generated by  $A_1, A_2, \dots, A_r$  is unique except for the order of minsets (or maxsets).

As an immediate corollary of this we have

**Corollary.** Two sets  $S$  and  $T$  generated by  $A_1, A_2, \dots, A_r$  are equal if and only if  $S$  and  $T$  have identical minset canonical form (maxset canonical form).

**Exercise 1.7.**

1. Prove Theorem 1.14.
2. Prove Theorem 1.16.
3. Find the minset and maxset normal forms of the sets
  - (i)  $B' \cap C$ , (ii)  $A \cup (B \cap C')$ , (iii)  $(A' \cap B) \cup (B' \cap (A \cup C))$  generated by  $A, B, C$ .
4. Use the minset and maxset normal forms to prove that the complement of  $(A \cap B') \cup (A' \cap (B \cup C'))$  is  $(A' \cup B) \cap (A \cup (B' \cap C))$ .
5. Let  $A = \{1, 2, \dots, 9\}$  and set  $A_1 = \{5, 6, 7\}$ ,  $A_2 = \{2, 4, 5, 9\}$ ,  $A_3 = \{3, 4, 5, 6, 8, 9\}$ .
  - (i) Find all minsets generated by  $A_1, A_2, A_3$ .
  - (ii) Find all maxsets generated by  $A_1, A_2, A_3$ .
  - (iii) Express the sets  $A'_1$ ,  $A_1 \cup A_2$  and  $A'_2 \cup A'_3$  in the minset normal form and maxset normal form.

## 1.9. Multisets

A sub-branch of a bank applied to be upgraded to a regular branch. For this the sub-branch was asked to supply the monthly lists of all bank account

numbers for which there were transactions during the last three months. For a particular account, there could be more than one transaction during a month; some of these may be debit entries and some credit entries. For all these transactions the sub-branch could not list that account only once, for otherwise the branch would lose credit for the remaining transactions of this account number. The lists of these account numbers are not sets as it may contain the same account number more than once. Each of these three lists is called a multiset. Thus a multiset is a collection of objects not necessarily all distinct. A second example of a multiset is the collection of names of all students who appeared in the university examination for discrete mathematics in a particular year. Yet another example of a multiset is the collection of all names in the telephone directory of a town.

We may list some other multisets as:

$$A = \{a, a, a, b, b, c, c, d, d, d, e\}$$

$$B = \{a, a, b, b, b, c, c, c, d, e, e, e\}$$

$$C = \{a, a, b, c, d, d\}$$

$$D = \{1, 1, 2, 2, 2, 2, 3, 3, 4, 4, 4, 4, 5, 5\}$$

$$E = \{1, 1, 2, 2, 3, 4, 4, 4, 5, 5\}$$

$$F = \{1, 1, 2, 2, 3, 4, 4, 5, 5, 5, 6\}$$

$$G = \{1, 1, 2, 2, 3, 4, 4, 5, 5, 5\}.$$

The **multiplicity** of an element of a multiset is defined to be the number of times the element occurs in the multiset. For example, in the multiset  $A$ , the multiplicity of  $a$  is 3, multiplicity of  $b$  is 2, multiplicity of  $c$  is 2, multiplicity of  $d$  is 3 while that of  $e$  is 1. In the multiset  $B$ , multiplicity of  $a$  is 2, of  $b$  it is 3, of  $c$  it is 3, of  $d$  it is 1 and that of  $e$  is 3. By ignoring or removing multiplicities of different elements of a multiset, we get a set — the underlying set of the multiset. The set corresponding to the multisets  $A$  and  $B$  is  $\{a, b, c, d, e\}$ , that corresponding to the multiset  $C$  is  $\{a, b, c, d\}$ , the set corresponding to the multisets  $D, E$  and  $G$  is  $\{1, 2, 3, 4, 5\}$  while the set corresponding to the multiset  $F$  is  $\{1, 2, 3, 4, 5, 6\}$ . The **order** or the **cardinality** of a multiset is defined to be the order or cardinality of the corresponding (or underlying) set. Thus the order of each of the multisets  $A, B, D, E, G$  is 5, the order of  $C$  is 4 and that of  $F$  is 6.

A multiset  $X$  is called a **submultiset** of a multiset  $Y$  if the multiplicity of every  $x \in X$  is less than or equal to the multiplicity of  $x$  as an element of

$Y$ . For example,  $C$  is a submultiset of  $A$ ,  $E$  is a submultiset of  $D$ , and  $G$  is a submultiset of  $F$ .

Observe that every set is always a multiset with the multiplicity of every element being 1. We will now define union, intersection and difference of multisets. These are to be so defined that these are in conformity with union, intersection and difference respectively of sets or that these do not contradict the corresponding definitions for sets.

Let  $P, Q$  be multisets. Then

- (a) the **intersection**  $P \cap Q$  of  $P$  and  $Q$  is the multiset in which the multiplicity of an element  $x$  is the minimum of the multiplicities of  $x$  as an element of  $P$  and as an element of  $Q$ ;
- (b) the **union**  $P \cup Q$  of  $P$  and  $Q$  is the multiset in which the multiplicity of an element  $x$  is equal to the maximum of the multiplicities of  $x$  as an element of  $P$  and as an element of  $Q$ ;
- (c) the **difference**  $P - Q$  of  $P$  and  $Q$  is the multiset in which the multiplicity of an element  $x$  is the multiplicity of  $x$  as an element of  $P$  minus the multiplicity of  $x$  as an element of  $Q$ . If this difference of multiplicities of  $x$  is  $\leq 0$ , then  $x$  does not appear in  $P - Q$ .

It is fairly easy to see that  $P \cap Q$  is a submultiset of  $P$  as well as of  $Q$ , both  $P$  and  $Q$  are submultisets of  $P \cup Q$  and  $P - Q$  is a submultiset of  $P$ .

**Example 1.18.** For the multisets  $A$  to  $G$  as above

- (a)  $A \cap B = \{a, a, b, b, c, c, d, e\}$   
 $A \cup B = \{a, a, a, b, b, b, c, c, c, d, d, d, e, e, e\}$   
 $A - B = \{a, d, d\}, B - A = \{b, c, e, e\}$
- (b)  $A \cap C = C, A \cup C = A, A - C = \{a, b, c, d, e\}, C - A = \varnothing$
- (c)  $B \cap C = \{a, a, b, c, d\}$   
 $B \cup C = \{a, a, b, b, b, c, c, c, d, d, e, e, e\}$   
 $B - C = \{b, b, c, c, e, e, e\}, C - B = \{d\}$
- (d)  $D \cap E = E, D \cup E = D, D - E = \{2, 2, 3, 4\}, E - D = \varnothing$
- (e)  $D \cap F = \{1, 1, 2, 2, 3, 4, 4, 5, 5\}$   
 $D \cup F = \{1, 1, 2, 2, 2, 2, 3, 3, 4, 4, 4, 4, 5, 5, 5, 6\}$   
 $D - F = \{2, 2, 3, 4, 4\}, F - D = \{5, 6\}$
- (f)  $D \cap G = \{1, 1, 2, 2, 3, 4, 4, 5, 5\}$

$$D \cup G = \{1, 1, 2, 2, 2, 2, 3, 3, 4, 4, 4, 4, 5, 5, 5\}$$

$$D - G = \{2, 2, 3, 4, 4\}, G - D = \{5\}$$

$$(g) E \cap F = \{1, 1, 2, 2, 3, 4, 4, 5, 5\}$$

$$E \cup F = \{1, 1, 2, 2, 3, 4, 4, 4, 5, 5, 5, 6\}$$

$$E - F = \{4\}, F - E = \{5, 6\}$$

$$(h) E \cap G = \{1, 1, 2, 2, 3, 4, 4, 5, 5\}$$

$$E \cup G = \{1, 1, 2, 2, 3, 4, 4, 4, 5, 5, 5\}$$

$$E - G = \{4\}, G - E = \{5\}$$

$$(i) F \cap G = G, F \cup G = F, F - G = \{6\}, G - F = \varnothing.$$

We next define the symmetric difference of two multisets. This again needs to be consistent with the definition of symmetric difference of two sets. Recall that the symmetric difference of two sets  $P$  and  $Q$  is defined to be  $(P - Q) \cup (Q - P)$  and it has been shown to be equal to  $(P \cup Q) - (P \cap Q)$ . Let  $P, Q$  be two multisets. As in the case of sets, we define the **symmetric difference**  $P \oplus Q$  of  $P$  and  $Q$  by

$$P \oplus Q = (P - Q) \cup (Q - P).$$

**Theorem 1.17.** For multisets  $P$  and  $Q$ ,  $P \oplus Q = (P \cup Q) - (P \cap Q)$ .

**Proof.** Let  $x \in P \oplus Q$  be an element of multiplicity  $\geq 1$ . Then multiplicity of  $x = \max\{\text{multiplicity of } x \text{ in } P - Q, \text{ multiplicity of } x \text{ in } Q - P\}$

$$= \max\{((\text{multiplicity of } x \text{ in } P) - (\text{multiplicity of } x \text{ in } Q)), \\ ((\text{multiplicity of } x \text{ in } Q) - (\text{multiplicity of } x \text{ in } P))\}.$$

Observe that one of

$(\text{multiplicity of } x \text{ in } P) - (\text{multiplicity of } x \text{ in } Q)$  and

$(\text{multiplicity of } x \text{ in } Q) - (\text{multiplicity of } x \text{ in } P)$  is positive and the other is negative. Therefore multiplicity of  $x$  equals

$[(\text{multiplicity of } x \text{ in } P) - (\text{multiplicity of } x \text{ in } Q)]$  or

$[(\text{multiplicity of } x \text{ in } Q) - (\text{multiplicity of } x \text{ in } P)],$

whichever is positive. If multiplicity of  $x$  in  $P >$  multiplicity of  $x$  in  $Q$ , then

$$\begin{aligned} & (\text{multiplicity of } x \text{ in } P) - (\text{multiplicity of } x \text{ in } Q) = \\ & (\text{multiplicity of } x \text{ in } P \cup Q) - (\text{multiplicity of } x \text{ in } P \cap Q). \end{aligned}$$

Similarly, if multiplicity of  $x$  in  $Q >$  multiplicity of  $x$  in  $P$ , then

$$\begin{aligned} & (\text{multiplicity of } x \text{ in } Q) - (\text{multiplicity of } x \text{ in } P) = \\ & (\text{multiplicity of } x \text{ in } P \cup Q) - (\text{multiplicity of } x \text{ in } P \cap Q). \end{aligned}$$

Thus in either case multiplicity of  $x$  equals

$$(\text{multiplicity of } x \text{ in } P \cup Q) - (\text{multiplicity of } x \text{ in } P \cap Q).$$

Thus  $P \oplus Q$  is a submultiset of  $P \cup Q - P \cap Q$ .

On the other hand, let  $x$  be in  $P \cup Q - P \cap Q$ . Then, multiplicity of

$$\begin{aligned} x &= (\text{multiplicity of } x \text{ in } P \cup Q) - (\text{multiplicity of } x \text{ in } P \cap Q) = \\ & (\text{multiplicity of } x \text{ in } P) - (\text{multiplicity of } x \text{ in } Q) \end{aligned}$$

or

$$= (\text{multiplicity of } x \text{ in } Q) - (\text{multiplicity of } x \text{ in } P) \text{ whichever is positive.}$$

Therefore,

$$\begin{aligned} \text{multiplicity of } x &= \text{multiplicity of } x \text{ in } P - Q \text{ or multiplicity of } x \text{ in } Q - P \\ &= \text{multiplicity of } x \text{ in } (P - Q) \cup (Q - P) = P \oplus Q. \end{aligned}$$

Hence,  $(P \cup Q) - (Q \cap P)$  is a submultiset of  $P \oplus Q$ .

$$\text{Therefore, } P \oplus Q = (P \cup Q) - (Q \cap P).$$

**Example 1.19.** We have computed  $P - Q$  and  $Q - P$  as also  $P \cup Q$  and  $P \cap Q$  for the multisets  $A$  to  $G$  as in Example 1.18. We now compute the symmetric difference for pairs of multisets  $A$  to  $G$  for which  $P - Q$  and  $Q - P$  have already been obtained.

1.  $A \oplus B = \{a, d, d\} \cup \{b, c, e, e\} = \{a, b, c, d, d, e, e\}$ .
2.  $A \oplus C = (A - C) \cup (C - A) = (A - C) \cup \varnothing = A - C = \{a, b, c, d, e\}$  and

$$(A \cup C) - (A \cap C) = A - C = A \oplus C.$$

3.  $B \oplus C = (B - C) \cup (C - B) = \{b, b, c, c, e, e, e\} \cup \{d\} = \{b, b, c, c, d, e, e, e\}$ .

Also

$$\begin{aligned} B \cup C - B \cap C &= \{a, a, b, b, b, c, c, d, d, e, e, e\} - \{a, a, b, c, d\} \\ &= \{b, b, c, c, d, e, e, e\} = B \oplus C. \end{aligned}$$

4.  $D \oplus E = (D - E) \cup (E - D) = (D - E) \cup \varnothing = D - E = \{2, 2, 3, 4\}$

and

$$(D \cup E) - (D \cap E) = D - E = \{2, 2, 3, 4\} = D \oplus E.$$

5.  $D \oplus F = (D - F) \cup (F - D) = \{2, 2, 3, 4, 4\} \cup \{5, 6\} = \{2, 2, 3, 4, 4, 5, 6\}$   
and

$$\begin{aligned} (D \cup F) - (D \cap F) &= \{1, 1, 2, 2, 2, 2, 3, 3, 4, 4, 4, 4, 5, 5, 5, 6\} \\ &\quad - \{1, 1, 2, 2, 3, 4, 4, 5, 5\} \\ &= \{2, 2, 3, 4, 4, 5, 6\} = D \oplus F. \end{aligned}$$

6.  $D \oplus G = (D - G) \cup (G - D) = \{2, 2, 3, 4, 4\} \cup \{5\} = \{2, 2, 3, 4, 4, 5\}$   
and

$$\begin{aligned} D \cup G - D \cap G &= \{1, 1, 2, 2, 2, 2, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5\} \\ &\quad - \{1, 1, 2, 2, 3, 4, 4, 5, 5, \} \\ &= \{2, 2, 3, 4, 4, 5\} = D \oplus G. \end{aligned}$$

7.  $E \oplus F = (E - F) \cup (F - E) = \{4\} \cup \{5, 6\} = \{4, 5, 6\}$   
and

$$\begin{aligned} (E \cup F) - (E \cap F) &= \{1, 1, 2, 2, 3, 4, 4, 4, 5, 5, 5, 6\} \\ &\quad - \{1, 1, 2, 2, 3, 4, 4, 5, 5\} \\ &= \{4, 5, 6\} = E \oplus F. \end{aligned}$$

8.  $E \oplus G = (E - G) \cup (G - E) = \{4\} \cup \{5\} = \{4, 5\}$   
and

$$\begin{aligned} (E \cup G) - (E \cap G) &= \{1, 1, 2, 2, 3, 4, 4, 4, 5, 5, 5\} \\ &\quad - \{1, 1, 2, 2, 3, 4, 4, 5, 5\} \\ &= \{4, 5\} = E \oplus G. \end{aligned}$$

9.  $F \oplus G = (F - G) \cup (G - F) = \{6\} \cup \varnothing = \{6\}$   
and

$$\begin{aligned} (F \cup G) - (F \cap G) &= F - G = \{1, 1, 2, 2, 3, 4, 4, 5, 5, 5, 6\} \\ &\quad - \{1, 1, 2, 2, 3, 4, 4, 5, 5, 5\} \\ &= \{6\} = F \oplus G. \end{aligned}$$

Observe that the result of Theorem 1.17 stands verified in all cases in the above example. Also observe that if  $Q$  is a submultiset of  $P$ , then  $P \oplus Q = P - Q$ . In particular, if  $Q$  is the empty set (= multiset), then  $P \oplus Q = P$ .

**Exercise 1.8.**

1. For sets  $A$ ,  $B$  and  $C$ , show that

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

where for a set  $K$ ,  $K'$  denotes the complement of  $K$ .

2. Let  $A = \{0, 2, 4, 6, 8\}$ ,  $B = \{0, 1, 2, 3, 4\}$  and  $C = \{0, 3, 6, 9\}$ , find

$$A \cup B \cup C \quad \text{and} \quad A \cap B \cap C.$$

3. Let  $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{0, 3, 6\}$  and  $C = \{0, 3, 6, 9\}$ . Find  
 (a)  $A \cup B$ ; (b)  $A \cap B$ ; (c)  $A \cap C$ ; (d)  $A \cup C$ ; (e)  $A - B$ ; (f)  $B - A$ ;  
 (g)  $A - C$ ; (h)  $B - C$ ; (i)  $C - A$ ; (j)  $C - B$ .
4. For any sets  $A$  and  $B$  show that  
 (a)  $A \cup (A \cap B) = A$ ; (b)  $A \cap (A \cup B) = A$ .
5. Find sets  $A$  and  $B$  if  $A - B = \{1, 5, 7, 8\}$  and  $B - A = \{2, 10\}$ .
6. List the elements of the set  
 (a)  $\{n \in Z \mid n^2 - 10n - 24 < 0 \text{ and } 4 < n < 16\}$ ;  
 (b) of prime numbers less than 25;  
 (c)  $\{q \in Q \mid q^2 - 1 = 15 \text{ and } q^3 = 60\}$ .
7. Find the power set of  $A$  when  
 (a)  $A = \{\varphi\}$ ; (b)  $A = \{\varphi, a, \{a\}\}$ ; (c)  $A = \wp(\{a\})$ .
8. For  $A = \{a, b, \{a, c\}, \phi\}$ , determine the following sets:  
 (a)  $A \setminus \{a\}$ ; (b)  $A \setminus \phi$ ; (c)  $A \setminus \{\phi\}$ ; (d)  $A \setminus \{a, b\}$ ; (e)  $\{a\} \setminus A$ .
9. If  $A$  is a subset of the universal set  $X$ , prove that  
 (a)  $A \oplus A' = X$ ; (b)  $A \oplus \varphi = A$ ; (c)  $A \oplus X = A'$ .
10. For any sets  $A$ ,  $B$  show that  $(A \oplus B) \oplus B = A$ .
11. For sets  $A$ ,  $B$ ,  $C$ , if  $A \oplus C = B \oplus C$ , does it necessarily imply that  $B = C$ ?
12. Give an example to show that intersection of two countable infinite sets is (a) finite; (b) again countable and infinite.
13. If  $A$  is a finite set having  $n$  elements, prove that  $A$  has exactly  $2^n$  distinct subsets.  
 (Refer to the section on mathematical induction in Chapter 3.)

14. Let  $S$  be a non-empty set and  $\wp(S)$  be the power set of  $S$ . In  $\wp(S)$  define addition and multiplication as follows: For  $A, B \in \wp(S)$ , define
- $A + B = (A - B) \cup (B - A)$  (= the symmetric difference  $A \oplus B$ );
  - $AB = A \cap B$ .

For subsets  $A, B, C$  of  $S$ , prove the following relations.

- $(A + B) + C = A + (B + C)$ ;
  - $A(B + C) = AB + AC$ ;
  - $AA = A$ ;
  - $A + A = \varnothing$ ;
  - If  $A + B = A + C$ , then  $B = C$ .
- (Also refer to Question 11 above.)
15. Given sets  $A = \{1, 2, 3\}$ ,  $B = \{3, 5, 7\}$ , find  $A - B$  and  $B - A$ . Also find  $A \times B$  and  $B \times A$ .
16. For any sets  $A, B, C$ , prove that
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$ ;
  - $A \times (B \cup C) = (A \times B) \cup (A \times C)$ ;
  - $(A \times B) - (A \times C) = A \times (B - C)$ .
17. If  $A, B$  are two sets, prove that  $\wp(A \cap B) = \wp(A) \cap \wp(B)$ .
18. Give an example to show that
- $\wp(A \cup B) \neq \wp(A) \cup \wp(B)$ ;
  - $\wp(A - B) \neq \wp(A) - \wp(B)$ .

19. Show that the set  $A$  does not exist when

$$A = \{S \mid S \text{ is a set such that } S \notin S\} \text{ (Russell's paradox).}$$

20. If  $S$  is a finite set, prove that any map:  $S \rightarrow S$  which is one-one is onto and any map:  $S \rightarrow S$  which is onto is one-one.
21. Give an example to show that the two results in Question 20 are not true if  $S$  is an infinite set.
22. Give an example to show that if  $\sigma : A \rightarrow B$ ,  $\tau : B \rightarrow C$  are maps such that
- $\tau \circ \sigma : A \rightarrow C$  is onto, it is not necessary that  $\sigma$  and  $\tau$  are onto;
  - $\tau \circ \sigma : A \rightarrow C$  is one-one, it is not necessary that  $\sigma$  and  $\tau$  are one-one.
23. For the set  $\mathbb{Z}$  of integers, prove that the map  $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  defined by  $f(m, n) = m + n$ ,  $m, n \in \mathbb{Z}$ , is onto but is not one-one.

24. Prove that the map  $f : \mathbb{R} \rightarrow \mathbb{R}$  defined by  $f(x) = e^x$ ,  $x \in \mathbb{R}$ , is one-one. Is it onto? Justify.
25. Let  $f : X \rightarrow Y$  be a map. Prove that  $f(A \cap B) = f(A) \cap f(B)$  for all subsets  $A, B$  of  $X$  if and only if  $f$  is one-one.
26. Prove or disprove that  $\lceil x+y \rceil = \lceil x \rceil + \lceil y \rceil$  for all real numbers  $x$  and  $y$ .
27. Prove or disprove that  $\lfloor x+y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$  for all real numbers  $x$  and  $y$ .
28. For the functions  $f$  and  $g$  from  $\mathbb{R}$  to  $\mathbb{R}$  defined by  $f(x) = x^2 + 1$  and  $g(x) = x + 2$ ,  $x \in \mathbb{R}$ , find  $f \circ g$  and  $g \circ f$ . Also find  $f + g$  and  $fg$ .
29. If  $f, g$  are functions such that  $f$  and  $f \circ g$  are both one-one, is  $g$  necessarily one-one? Justify.
30. If  $f, g$  are functions such that  $f$  and  $f \circ g$  are both onto, is  $g$  necessarily onto? Justify.
31. Consider the functions  $f, g$  where  $f(x) = ax + b$ ,  $g(x) = cx + d$  with  $a, b, c, d$  real constants. Find the values of the constants  $a, b, c, d$  so that  $f \circ g = g \circ f$ .
32. Determine the number of bytes required to encode  $n$  bits of data when  $n$  equals  
(i) 5; (ii) 10; (iii) 501; (iv) 2999; (v) 3000; (vi) 6; (vii) 16; (viii) 166;  
(ix) 29900; (x) 999; (xi) 1002.
33. Data are transmitted over a particular network in blocks of 1500 octets (blocks of 8 bits). Determine the number of blocks required to transmit the amounts of data over this Network. (Note that here a byte is a synonym for an octet, a kilobyte is 1,000 bytes and a megabyte is 1,000,000 bytes.)  
(i) 149 kilobytes of data, (ii) 150 kilobytes of data,  
(iii) 274 kilobytes of data, (iv) 384 kilobytes of data,  
(v) 1455 megabytes of data, (vi) 43.6 megabytes of data.