UNIT 1 SETS, FUNCTIONS AND FIELDS

Structure

1.1 INTRODUCTION

This unit seeks to introduce you to the pre-requisites of linear algebra. We recall the concepts of sets, relations and functions here. These are fundamental to the study of any branch of mathematics. In particular, we study binary operations on a set, since this concept is necessary for the study of **algebra.** We conclude with defining a field, which is a very important algebraic structure, and give some examples of it.

Objectives

After studying this unit, you should be able to

- identify and work with sets, relations, functions and binary operations;
- recognise a field;
- give examples of finite and infinite fields.

1.2 SETS

We shall recall that the term **set** is used to describe any **well defined** collection of objects, that is, every set should be so described that given any object it should be clear whether the given object belongs to the set or not.
For instance,

a) the collection **N** of all natural numbers, and
b) the collection of all positive integers which divide 48 (namely, the integers 1,2,3,4,6,8,12,16,24 and 48) are well defined, and hence, are sets.

But the collection of all rich people is not a set, because there is no way of deciding whether a human being is rich or not.

If S is a set, an object a in the collection S is called an **element** of S. This fact is expressed in symbols as $a \in S$ (read "a is in S" or "a belongs to S"). If a is not in S, we write $a \notin S$. For example, $3 \in \mathbf{R}$, the set of real numbers. But $\sqrt{-1} \notin \mathbf{R}$.

The Greek letter epsilon, ϵ, denotes 'belongs to'

There are usually two ways of describing a set (1) Roster Method, and (2) Set Builder Method.

Roster Method: In this method, we list all the elements of the set within braces. For instance, as we have mentioned above, the collection of all positive divisors of 48 contains 1,2,3,4,6,8,12,16,24 and 48 as its **elements. So this set may be written as** {1,2,3,4,6,8,12,16,24,48}.

In this description of a set, the following two conventions are followed :

Convention 1: The order in which the elements of the set are listed is not important.

Convention 2: No element is written more than once: that is, every element must be written exactly once.

For example, consider the set S of all integers between $1\frac{1}{2}$ and $4\frac{1}{4}$. Obviously, these integers are 2,3 and 4. So we may write

$S = \{2,3,4\}$.

We may also write $S = \{3,2,4\}$, but we must not write $S = \{2,3,2,4\}$. Why? Isn't this what Convention 2 says?

The roster method is sometimes used to list the elements of a large set also. In this case we may not want to list all the elements of the set. We list some and give an indication of the rest of the elements. For example, the set of integers lying between 0 and 100 is $\{0,1,2,\ldots,100\}$.
Another method that we can use for describing a set is the

Set Builder Method: In this method we first try to find a property which characterises the elements of the set, that is, a property P which all elements of the set possess, and which no other objects possess. Then we describe the set as

$\{x \mid x \text{ has property P}\}$, or as

$\{x : x \text{ has property P}\}$.

This is to be read as "the set of all x such that x has property P".

For example, the set S of all integers lying between $1\frac{1}{2}$ and $4\frac{1}{4}$ can also be written as $S = \{x : x \text{ is an integer and } 1\frac{1}{2} < x < 1\frac{1}{4}\}$.

Example 1: Write the set N by the set builder method and the roster method.

Solution: By the set builder method we have the set
$N = \{x \mid x \text{ is a natural number}\}$.
By the roster method we have $N = \{1,2,3,\ldots\}$.

E E1) Write the following sets by the roster method.

$A = \{x \mid x \text{ is an integer and } 10 < x < 15\}$

$B = \{x \mid x \text{ is an even integer and } 10 < x < 15\}$

$C = \{x \mid x \text{ is a positive divisor of } 20\}$

$D = \{p/q \mid p,q \text{ integers and } 1 \leq p < q \leq 3\}$

E E2) Write the following sets by the set builder method.

$P = \{7,8,9\}$; $Q = \{1,2,3,5,7,11\}$; $R = \{3,6,9,\ldots\}$.

Let us now look at some sets that can be obtained from given sets.

1.2.1 Subsets, Unions, Intersections

Consider the sets $A = \{1,3,4\}$ and $B = \{1,4\}$. Here every element of B is also an element of A. In such a case, that is, when every element of B is an element of A, we say that **B is a subset of A, and we write $B \subseteq A$.**

It is obvious that if A is any set, then every element of A is certainly an element of A. So, for every set A, $A \subseteq A$.

Consider the sets $Q = \{1,3,5,15\}$ and $S = \{2,3,5,7\}$. Is $Q \subseteq S$? No, because not every element of Q is in S; for example, $1 \in Q$ but $1 \notin S$. Is $S \subseteq Q$? No, because, for example, $2 \in S$ but $2 \notin Q$. Therefore, there do exist pairs of sets, A and B, such that neither of them is contained in the other. This is written as $A \not\subseteq B$ and $B \not\subseteq A$ ('$\not\subseteq$' denotes 'is not a subset of'.)

∃ denotes 'there exists

Note that if B is not a subset of A, there must be an element of B which is not an element of A. In mathematical notation this can be written as '$\exists\, x \in B$ such that $x \notin A$'.

We can now say that two sets **A and B are equal** (i.e., have precisely the same elements) **if and only if $A \subseteq B$ and $B \subseteq A$.**

E E3) Which of the following statements are true?

a) $N \subseteq Z$ b) $Z \subseteq N$ c) $\{0\} \subseteq \{1,2,3\}$ d) $\{2,4,6\} \not\subseteq \{2,4,8\}$

We now give one way of obtaining a new set from two or more given sets.

Union: If we have two sets A and B, we can collect the elements of both to get a new set. This set is called their union. Formally, we define the **union of A and B** to be the set of all those elements which are in A or in B or in both A and B. The union of A and B is denoted by **$A \cup B$.** Thus,
$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.

Example 2: Find $A \cup B$ when
a) $A = \{1,2\}$ and $B = \{4,6,7\}$.
b) $A = \{1,2,3,4\}$ and $B = \{2,4,6,8\}$.

Solution: a) $A \cup B = \{1,2,4,6,7\}$.
b) $A \cup B = \{1,2,3,4,6,8\}$. Observe that 2 and 4 are in both A and B, but when we write $A \cup B$, we write these elements only once, in accordance with Convention 2 given earlier.

Can you see that, for any set A, $A \cup A = A$?

E E4) Show that, if $A \subseteq C$ and $B \subseteq C$, then $A \cup B \subseteq C$.

The definition of union can be immediately extended to define the union of more than two sets. If $A_1, A_2, \ldots, A_k$ are k sets, their union $A_1 \cup A_2 \cup \ldots\ldots \cup A_k$ is the set of elements which belong to at least one of these sets. That is,

$A_1 \cup A_2 \cup \ldots\ldots \cup A_k = \{x \mid x \in A_i \text{ for some } i,\ i = 1,2,\ldots,k\}$

The expression $A_1 \cup A_2 \cup \ldots\ldots \cup A_k$ is often abbreviated to $\bigcup_{i=1}^{k} A_i$.

Now let us look at another way of obtaining a new set from two or more given sets.

Intersection: If A and B are two sets, then the **intersection of A and B** (denoted by $A \cap B$) is the set of elements common to A and B. So,

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

Thus, if $P = \{1,2,3,4\}$ and $Q = \{2,4,6,8\}$, then $P \cap Q = \{2,4\}$.

Can you see that, for any set A, $A \cap A = A$?

A set having no elements is called an empty set or null set, and is denoted by ϕ, the Greek letter phi.

Now suppose $A = \{1,2\}$ and $B = \{4,6,7\}$. Then what is $A \cap B$? We observe that, in this case, A and B have no common elements, and so $A \cap B = \phi$, the empty set.

When the intersection of two sets is ϕ, we say that the two sets are **disjoint** (or **mutually disjoint**). For example, the two sets $\{1,4\}$ and $\{0,5,7,14\}$ are disjoint.

The definition of intersection can be extended to any number of sets. Thus, the intersection of k sets $A_1, A_2, \ldots, A_k$ is

$A_1 \cap A_2 \cap \ldots \cap A_k = \{x \mid x \in A_i \text{ for each } i = 1,2,\ldots,k\}$.

The expression $A_1 \cap A_2 \cap \ldots \cap A_k$ is abbreviated to $\bigcap_{i=1}^{k} A_i$.

Example 3: If $A \subseteq B$, what is $A \cap B$?

Solution: Since $A \subseteq B$, we know that every element of A is an element of B. Then

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

Example 4: For every set A, show that $\phi \subseteq A$.

Solution: We have already made the remark that if B is not a subset of A, there must be an element of B which is not an element of A. So if ϕ is not a subset of A, we should be able to produce an element in ϕ which is not in A. Can we do so? Obviously not! Because ϕ has no elements at all. We are therefore forced to the conclusion that $\phi \subseteq A$.

E E5) For every set A, show that $\phi \cup A = A$ and $\phi \cap A = \phi$.

E E6) State whether the following are true or false.

a) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

b) If $A \not\subseteq B$ and $B \not\subseteq A$, then A and B are disjoint.

c) $A \not\subseteq (A \cup B)$

d) $B \subseteq (A \cup B)$

e) If $A \cup B = \phi$, then $A = B = \phi$.

E E7) Suppose $A = \{a,b,c\}$, $B = \{a,b,p,q\}$ and $C = \{a,p,r,s\}$. Find the following sets:

a) $A \cup B$, b) $B \cap C$, c) $(A \cup B) \cap C$, d) $(A \cap C) \cup (B \cap C)$.

What do you guess from your answers to (c) and (d)?

Is $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$? Check your guess by making your own choice for A, B and C.

Apart from the operations of unions and intersections, there is another operation on sets, namely, the operation of taking complements.

Complements: When we are working with elements and subsets of a single set X, we say that the set X is the **universal set.** Suppose X is the universal set and $A \subseteq X$, then the set of all elements of X which are not in A is called the **complement of A** and is denoted by

A', A^c or $X \setminus A$. Thus,

$A^c = \{x \mid x \in X, x \notin A\}$.

If $X = \{a,b,p,q,r\}$ and $A = \{a,p,q\}$, then clearly $A^c = \{b,r\}$.

E8) Why are the following statements true?

a) A and A^c are disjoint, i.e., $A \cap A^c = \phi$.

b) $A \cup A^c = X$, where X is the universal set.

c) $(A^c)^c = A$

Certain properties of the complements of sets have been stated as **De Morgan's Laws.** We give them as a theorem.

Theorem 1: If A and B are subsets of X, then

a) $(A \cup B)^c = A^c \cap B^c$

b) $(A \cap B)^c = A^c \cup B^c$

(In words, 'complement of union is intersection of complements' and 'complement of intersection is union of complements'.)

Proof: a) Two sets P and Q are equal, if and only if $P \subseteq Q$ and $Q \subseteq P$, that is, if and only if $x \in P \Rightarrow x \in Q$ and $x \in Q \Rightarrow x \in P$.

'$\Rightarrow$' denotes 'implies'

Thus, to prove (a), we must prove that

$x \in (A \cup B)^c \Rightarrow x \in A^c \cap B^c$ and $x \in A^c \cap B^c \Rightarrow x \in (A \cup B)^c$.

Now

$$x \in (A \cup B)^c \Rightarrow x \notin A \cup B$$
$$\Rightarrow x \notin A \text{ and } x \notin B$$
$$\Rightarrow x \in A^c \text{ and } x \in B^c$$
$$\Rightarrow x \in A^c \cap B^c$$

Conversely,

$$x \in A^c \cap B^c \Rightarrow x \in A^c \text{ and } x \in B^c$$
$$\Rightarrow x \notin A \text{ and } x \notin B$$
$$\Rightarrow x \notin A \cup B$$
$$\Rightarrow x \in (A \cup B)^c$$

Note that in both parts of the proof, the various steps are the same but only in reverse order. When this is the case, both parts can be combined as follows.

'$\Leftrightarrow$' denotes 'implies and is implied by' or 'if and only if'.

$$x \in (A \cup B)^c \Leftrightarrow x \notin A \cup B$$
$$\Leftrightarrow x \notin A \text{ and } x \notin B$$
$$\Leftrightarrow x \in A^c \text{ and } x \in B^c$$
$$\Leftrightarrow x \in A^c \cap B^c$$

E E9) Try and prove (b) (of Theorem 1) now.

So far we have looked at sets algebraically. Now let us look at them pictorially.

1.2.2 Venn Diagrams

Some results about sets can be easily understood and visualised by using Venn diagrams, named after the English logician John Venn (1834-1923). In a Venn diagram the universal set is usually represented by a rectangle and its subsets by circles or other closed figures in its interior. For example, if A, B and C are subsets of X, this fact is represented by the following diagram (Fig. 1).

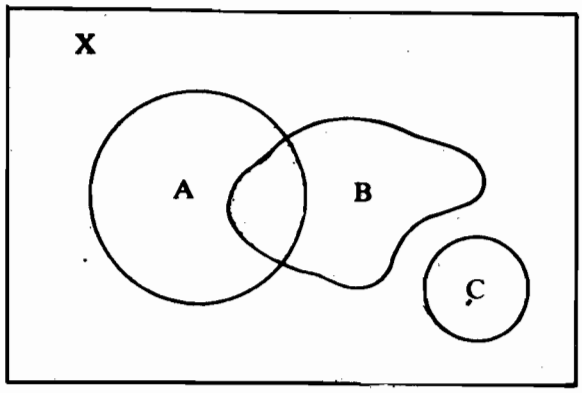


Fig. 1

The idea is that points in the interior of the rectangle represent the elements of X and the points in the interior of the closed figures, A, B and C represent the elements of A, B and C, respectively. Notice that the subsets of X can be of any shape.

If X = {a,b,c,p,q,r,s}, A = {a,b,p,r} and B = {p,q,r}, then this can be represented by the following Venn diagram (Fig. 2).

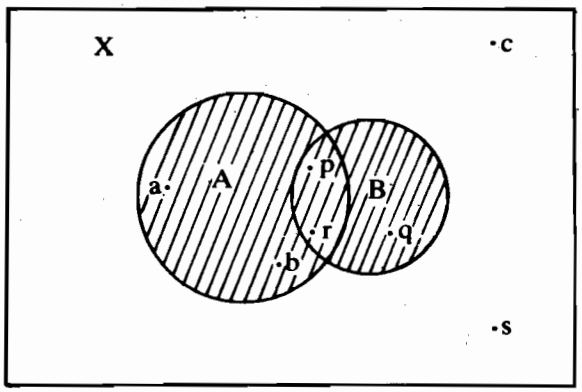


Fig. 2

Then, $A \cup B$ is the shaded portion in Fig. 2, and $(A \cup B)^c$ is the unshaded portion of the diagram.

E E10) Use Venn diagrams to demonstrate the truth of the following results. Here A,B,C are subsets of X.

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

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

We will now talk of the product of sets, of which the coordinate system is a special case.

1.3 CARTESIAN PRODUCT OF SETS

An interesting set that can be formed from two given sets is their **Cartesian product,** named after the French philosopher and mathematician René Descartes (1596 – 1650) He also invented the Cartesian coordinate system.

Rene Descartes

Let A and B be two sets. Consider the pair (a,b), in which the first element is from A and the second from B. Then (a,b) is called an **ordered pair.** In an ordered pair, the order in which the two elements are written is important. Thus, **(a,b) and (b,a) are different ordered pairs.** Two ordered pairs **(a,b) and (c,d) are said to be equal,** or same, if **$a = c$ and $b = d$.**

Definition: The **Cartesian product $A \times B$,** of the sets A and B, is the set of all possible ordered pairs (a,b), where $a \in A$, $b \in B$.

That is, $A \times B = \{(a,b) : a \in A, b \in B\}$.

For example, if $A = \{1,2,3\}$, $B = \{4,6\}$, then

$A \times B = \{(1,4), (1,6), (2,4), (2,6), (3,4), (3,6)\}$

Also note that

$B \times A = \{(4,1), (4,2), (4,3), (6,1), (6,2), (6,3)\}$, and $A \times B \neq B \times A$.

We can also define the Cartesian product of more than two sets in a similar way. Thus, if $\mathbf{R}$ is the set of all real numbers, then

$\mathbf{R} \times \mathbf{R} = \{(a_1, a_2) : a_1 \in \mathbf{R}, a_2 \in \mathbf{R}\}$,

$\mathbf{R} \times \mathbf{R} \times \mathbf{R} = \{(a_1, a_2, a_3) : a_i \in \mathbf{R}\}$,

and so on. It is customary to write $\mathbf{R}^2$ for $\mathbf{R} \times \mathbf{R}$ and $\mathbf{R}^n$ for $\mathbf{R} \times \ldots\ldots\ldots \times \mathbf{R}$ (n times).

Since every point in a plane has two coordinates, x and y, and every ordered pair (x,y) of real numbers defines the coordinates of a point in the plane, we say $\mathbf{R}^2$ represents a plane. Thus, $\mathbf{R}^2$ is the Cartesian product of the x-axis and the y-axis. In the same way $\mathbf{R}^3$ represents three-dimensional space, and $\mathbf{R}^n$ represents n-dimensional space, for any $n \geq 1$. Note that $\mathbf{R}$ represents a line.

E E11) If $A = \{2,5\}$, $B = \{2,3\}$, find $A \times B$, $B \times A$, $A \times A$.

E E12) If $A \times B = \{(7,2), (7,3), (7,4), (2,2), (2,3), (2,4)\}$, determine A and B.

E E13) Prove that $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

Let us now look at subsets of certain Cartesian products.

1.4 RELATIONS

You are already familiar with the concept of a relationship between people. For example, a parent-child relationship exists between A and B if and only if A is a parent of B or B is a parent of A.

In mathematics, a relation R on a set S is a relationship between the elements of S. If $a \in S$ is related to $b \in S$ by means of this relation, we write a R b, or $(a,b) \in R$. From the latter notation we see that $R \subseteq S \times S$. And this is exactly how a (binary) relation on a set is defined.

Definition: A **relation** R on a set S is a subset of S×S.

For example, if N is the set of natural numbers and R is the relation 'is a multiple of', then 15R5, but not 5R15. That is, $(15,5) \in R$ but $(5,15) \notin R$. Here $R \subseteq N \times N$.

Again, if Q is the set of all rational numbers and R is the relation 'is greater than', then 3R2 (because $3 > 2$). In fact, for any number **$n>1$, $nR(n-1)$.**

E E14) Let N be the set of all natural numbers and R the relation 'is a divisor of' on the set N. State whether the following are true or false.

a) 2 R 3

b) n R n, $\forall\, n \in N$

c) n R m and m R n $\Rightarrow$ m = n

We now look at some particular kinds of relations.

Definition: A relation R defined on a set S is said to be

i) **reflexive** if we have a R a $\forall$ a $\in$ S.

ii) **symmetric** if a R b $\Rightarrow$ b R a $\forall$ a, b $\in$ S.

iii) **transitive** if a R b and b R c $\Rightarrow$ a R c $\forall$ a,b,c $\in$ S.

To get used to these concepts, consider the following examples.

Example 5: Let N be the set of all natural numbers. We define the relation R on N as follows:

a R b if and only if $a > b$.

Determine whether R is reflexive, symmetric and transitive.

Solution: Since $a > a$ is not true, so a R a is not true. Hence, R is not reflexive.

If $a > b$ then certainly $b > a$ is not true. That is, a R b **does not** imply b R a. Hence, R is not symmetric.

Since $a > b$ and $b > c$ implies **$a > c$,** we find that a R b, b R c implies a R c. Thus, R is transitive.

E E15) The relation $R \subseteq N \times N$ is defined by $(a,b) \in R$ iff 5 divides $(a-b)$. Is R reflexive, symmetric or transitive?

The relationship in E 15 is reflexive, symmetric and transitive. Such a relation is called an **equivalence relation.**

A very important property of an equivalence relation on a set S is that it divides S into a number of mutually disjoint subsets, that is, it **partitions** S. Let us see how this happens.

Let R be an equivalence relation on the set S. Let $a \in S$. Then the set $S_a = \{b \mid b \in S, aRb\}$ is called the **equivalence class** of a in S. It is just the set of elements in S which are related to a. For instance, for R given in E15, what is the equivalence class of 1?

This is

$N_1 = \{n \mid 1Rn, n \in N\}$

$= \{n \mid n \in N \text{ and 5 divides } 1-n\}$

$= \{n \mid n \in N \text{ and 5 divides } n-1\}$

$= \{1,6,11,16,21,\ldots\}$

Similarly,

$N_2 = \{n \mid n \in N \text{ and 5 divides } n-2\}$
$= \{2,7,12,17,22,.....\}$
$N_3 = \{3,8,13,18,23,....\}$
$N_4 = \{4,9,14,19,24,....\}$
$N_5 = \{5,10,15,20,25,....\}$
$N_6 = \{1,6,11,16,21,....\}$
$N_7 = \{2,7,12,17,22,....\}$,etc.

Note that

i) $N = N_1 \cup N_2 \cup N_3 \cup N_4 \cup N_5$, and the sets on the right hand side are mutually disjoint.

ii) N_1 and N_6 are not disjoint. In fact, $N_1 = N_6$. Similarly $N_2 = N_7$, and so on.

These observations will be proved in general in the following theorem.

Theorem 2: Let R be an equivalence relation on a set S. For $a \in S$, let S_a denote the equivalence class of a. Then,

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

b) If $a,b \in S$ then $S_a \cap S_b = \phi$ or $S_a = S_b$

Proof: a) Since $S_a \subseteq S \forall a \in S$, $\bigcup_{a \in S} S_a \subseteq S$ (see E 4).

Conversely, let $x \in S$. Then, $x \in S_x$ (as x R x is true.) And S_x is one of the sets in the collection $\{S_a \mid a \in S\}$, whose union is $\bigcup_{a \in S} S_a$.

Hence, $x \in \bigcup_{a \in S} S_a$. So $S \subseteq \bigcup_{a \in S} S_a$

Thus, $S \subseteq \bigcup_{a \in S} S_a$ and $\bigcup_{a \in S} S_a \subseteq S$, proving (a).

b) Suppose $S_a \cap S_b \neq \phi$. Let $x \in S_a \cap S_b$.

Then, $x \in S_a$ and $x \in S_b$.

$\Rightarrow$ aRx and bRx

$\Rightarrow$ aRx and xRb (since R is symmetric)

$\Rightarrow$ aRb (since R is transitive)

Using this we shall prove that $S_a = S_b$. For this, take $y \in S_a$. Then aRy, which is the same as yRa. We have also shown that aRb. This gives us yRb, since R is transitive That is, bRy, which means that $y \in S_b$. Thus, $S_a \subseteq S_b$. Similarly, it can be proved that $S_b \subseteq S_a$. Thus, $S_a = S_b$, and (b) is proved.

Note that, in the above theorem, because of (b), distinct sets on the right hand side of (a) are all disjoint from one another. Therefore, (a) expresses S as a union of mutually disjoint subsets of S; that is we have a partition of S into equivalence classes.

E E16) Show that 'aRb if and only if a = b' is an equivalence relation on **Z**. What is Z_1?

E17) Let $S = A \cup B \cup C$, where A,B,C are mutually disjoint, and R is the relation defined on S by:
aRb if whenever $a \in A, b \in A$ or whenever $a \in B$, $b \in B$, or whenever $a \in C$, $b \in C$.

Prove that R is an equivalence relation on S. For $b \in B$, what is S_b?

In the next section we discuss a familiar concept that also leads to some relations.

1.5 FUNCTIONS

Recall that a function f from a set A to a set B is a rule which associates with every element of A exactly one element of B. This is written as $f : A \to B$. If f associates with $a \in A$, the element b of B, we write $f(a) = b$. A is called the **domain** of f and the set $\{f(a) \mid a \in A\}$ is called the **range** of f. The range of f is a subset of B. B is called the **co-domain** of f.

Note that
i) For **each** element of A, we associate some element of B.
ii) For each element of A, we associate **only one** element of B.
iii) Two or more elements of A could be associated with the same element of B.

For example, let $A = \{1,2,3\}$, $B = \{1,2,3,4,5,6,7,8,9,10\}$. Define $f : A \to B$ by $f(1) = 1, f(2) = 4, f(3) = 9$. Then f is a function. In this case we can also write $f(x) = x^2$ for each $x \in A$. The domain of f is A and the range is $\{1,4,9\}$.

We could also have written the definition of f as $f : A \to B : f(x) = x^2$. We will often use this notation for defining any function.

If we define $g : A \to B$ by $g(1) = 1, g(2) = 1, g(3) = 4$, then g is also a function. The domain of g remains the same, namely, A. The range of g is $\{1,4\}$.

A function $f : A \to B$ is said to be **one-one** (or **injective**) if different elements of A are associated with different elements of B, i.e., if $a_1, a_2 \in A$ and $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$. In the foregoing examples, the function f is one-one. The function g is not one-one because 1 and 2 are distinct elements of A, but $g(1) = g(2)$.

'f is one-one' can also be written as 'f is 1–1'

Now consider another example of sets and functions.
Let $A = \{1,2,3\}$, $B = \{p,q,r\}$. Let $f:A \to B$ be defined by $f(1) = q, f(2) = r, f(3) = p$. Then f is a function. Here the range of f = B = co-domain of f. This is an example of an onto function, as you shall see.

Definition: A function $f:A \to B$ is said to be **onto** (or **surjective**) if the range of f is B, i.e., if, for **each** $b \in B$, there is an $a \in A$ such that $f(a) = b$.

If a function is both one-one and onto it is called **bijective.** The example of an onto function given above is also 1-1, and hence, bijective.

E E18) Let $f:\mathbf{N} \to \mathbf{N}$ be defined by $f(n) = n+5$. Prove that f is one-one but not onto.

E E19) Let $f:\mathbf{Z} \to \mathbf{Z}$ be defined by $f(n) = n+5$. Prove that f is both one-one and onto.

E E20) Let $A = \{1,-1,2,3\}$. If $f:A \to \mathbf{R}$ is defined by $f(x) = x^2-5x+6$, find the range of f.

Two functions that you will often come across are

i) the **identity function** $I_A:A \to A: I_A(a) = a \; \forall \; a \in A$,

ii) the **constant function** $f:A \to B$: $f(a) = c \; \forall \; a \in A$, where c is a fixed element of B.

E E21) a) Can you show that the identity function is bijective?

b) What must X be like for the constant function $f:X \to \{c\}$ to be injective?

Now let us see what we mean by the composition of two or more functions.

1.5.1 Composition of Functions

If $f:A \to B$ and $g:C \to D$ are functions and if the range of f is a subset of C, there is a natural way of combining g and f to yield a new function $h:A \to D$. For each $x \in A$, h(x) is defined by the formula $h(x) = g(f(x))$. (Note that f(x) is in the range of f, so that $f(x) \in C$. Therefore, $g(f(x))$ is defined and is an element of D.) This function h is called the **composition of g and f** and is written as **gof**. The domain of gof is A and its codomain is D.

Example 6: Let $f : \mathbf{R} \to \mathbf{R}$ and $g:\mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x^2$ and $g(x) = x+1$. What is gof? What is fog?

$f: A \to B$ and
$g: C \to D$ are **equal** if $A = C$ and $f(a) = g(a)$ $\forall$ $a \in A$.

Solution: We observe that the range of f is a subset of **R**, the domain of g. Therefore, gof is defined. By definition, $\forall$ $x \in \mathbf{R}$,

$gof(x) = g(f(x)) = f(x) + 1 = x^2 + 1$.
Now, let us find fog. Again, it is easy to see that fog is defined.
$\forall$ $x \in \mathbf{R}$, $fog(x) = f(g(x)) = (g(x))^2 = (x+1)^2$.
Thus, gof $\neq$ fog.

Example 7: Let $A = \{1,2,3\}$, $B = \{p,q,r\}$ and $C = \{x,y\}$. Let $f: A \to B$ be defined by $f(1) = p$, $f(2) = p$, $f(3) = r$. Let $g: B \to C$ be defined by $g(p) = x$, $g(q) = y$, $g(r) = y$. Determine if fog and gof can be defined.

Solution: For fog to be defined, it is necessary that the range of g should be a subset of the domain of f. In this case, the range of g is C and the domain of f is A. As C is not a subset of A, fog cannot be defined.

Since the range of f, which is $\{p,r\}$, is a subset of B, the domain of g, we see that gof is defined.

Also $gof: A \to C$ is such that

$gof(1) = g(f(1)) = g(p) = x$

$gof(2) = g(f(2)) = g(p) = x$

$gof(3) = g(f(3)) = g(r) = y$

In this example note that g is surjective, and so is gof.

E E22) In each of the following questions, both f and g are functions from **R** to **R**. Define fog and gof, wherever meaningful.

a) $f(x) = 5x$, $g(x) = x + 5$

b) $f(x) = 5x$, $g(x) = x/5$

c) $f(x) = x^3$, $g(x) = \sin x + 3$

d) $f(x) = |x|$, $g(x) = x^2$.

Remark: Functions can lead to relations. How can this happen? Given a function $f: A \to B$, can you define a relation? What about $R \subseteq A \times B$, where $(a,b) \in R$ iff $b = f(a)$? This is a relation that arises from f.

We now come to a theorem which shows us that the identity function behaves like the number $1 \in \mathbf{R}$ does for multiplication. That is, if we take the composition of any function f with the suitable identity function, we get the same function f.

Theorem 3: For every function $f:A \to A$, we have $fol_A = f$ and $I_A of = f$.

Proof: Since both f and I_A are defined from A to A, both the compositions fol_A and $I_A of$ are defined. Moreover, $\forall x \in A$,

$fol_A(x) = f(I_A(x)) = f(x)$, so $fol_A = f$.

Also, $\forall x \in A$,

$I_A of(x) = I_A(f(x)) = f(x)$, so $I_A of = f$.

On the lines of this theorem you can try the next exercise.

E E23) If B is any set and $g:B \to A$, prove that $I_A og = g$ and $gol_B = g$.

In the case of real numbers, you know that given any real number $x \neq 0$, $\exists y \neq 0$ such that $xy = 1$. y is called the inverse of x. Similarly, we define an inverse function for a given function.

Definition: Let $f:A \to B$ be a given function. If there exists a function $g:B \to A$ such that $fog = I_B$ and $gof = I_A$, then we say that g is the **inverse** of f, and we write $g = f^{-1}$.
For example, consider $f:\mathbf{R} \to \mathbf{R}$ defined by $f(x) = x+3$. If we define $g:\mathbf{R} \to \mathbf{R}$ by $g(x) = x-3$, then $fog(x) = f(g(x)) = g(x)+3 = (x-3)+3 = x \; \forall x \in \mathbf{R}$. Hence, $fog = I_{\mathbf{R}}$. Similarly, $gof = I_{\mathbf{R}}$ (verify). So $g=f^{-1}$

Note that, in the above example, f adds 3 to x and g does the opposite—it subtracts 3 form x. Thus, the key to finding the inverse of a given function is : try to retrieve x from (x).

For example let $f:\mathbf{R} \to \mathbf{R}$ be defined by $f(x) = 3x + 5$. How can we retrieve x from $3x + 5$? The answer is "first subtract 5 and then divide by 3". So we try $g(x) = \frac{x-5}{3}$. And we find

$$gof(x) = g(f(x)) = \frac{f(x)-5}{3} = \frac{(3x+5)-5}{3} = x$$

Also, $fog(x) = 3(g(x)) + 5 = 3\frac{(x-5)}{3} + 5 = x \; \forall x \in \mathbf{R}$.

E E24) What is the inverse of $f:\mathbf{R} \to \mathbf{R}$: $f(x) = \frac{x}{3}$?

Do all functions have an inverse? No, as the following example shows.

Example 8: Let $f: \mathbf{R} \to \mathbf{R}$ be given by $f(x) = 1 \; \forall x \in \mathbf{R}$. What is the inverse of f?

Solution: If f has an inverse $g:\mathbf{R} \to \mathbf{R}$ we have $fog = I_{\mathbf{R}}$, i.e., $\forall x \in \mathbf{R}$, $fog(x) = x$. Now take $x = 5$. We should have $fog(5) = 5$, i.e., $f(g(5)) = 5$. But $f(g(5)) = 1$, since $f(x) = 1 \; \forall x$. We reach a contradiction. Therefore, f has no inverse.

In view of this example, we naturally ask for necessary and sufficient conditions for f to have an inverse. The answer is given by the following theorem.

Theorem 4: A function $f:A \to B$ has an inverse if and only if f is bijective.

Proof: First suppose f is bijective. We shall define a function $g:B \to A$ and then prove that $g = f^{-1}$.

Let $b \in B$. Since f is onto, there is some $a \in A$ such that $f(a) = b$, and, as f is one-one, there is only one such $a \in A$. We take this unique element a of A as g(b). That is, given $b \in B$, we define $g(b) = a$, where $f(a) = b$.

Note that, since f is onto, $B = \{f(a) | a \in A\}$. Then, we are simply defining $g:B \to A$ by $g(f(a)) = a$. This automatically ensures that $gof = I_A$.

Now, for this g, we prove that $g = f^{-1}$. Let $a \in A$. Then $gof(a) = g(f(a)) = a$, by the definition of g, so that $gof = I_A$.

Next, let $b \in B$. Then, if $g(b) = a$, we must have
$f(a) = b$ (by the definition of g), so $fog(b) = f(g(b)) = f(a) = b$.

Hence, $fog = I_B$.
This proves that $g = f^{-1}$.

Conversely, suppose f has an inverse and let $g = f^{-1}$ We must prove that f is one-one and onto.

Suppose $f(a_1) = f(a_2)$ then $g(f(a_1)) = g(f(a_2))$.
$\Rightarrow gof(a_1) = gof(a_2)$
$\Rightarrow a_1 = a_2$, because $gof = I_A$.
So f is one-one.

Finally, given $b \in B$, we have $fog = I_B$, so that $fog(b) = I_B(b) = b$, i.e., $f(g(b)) = b$. So, given $b \in B$, there is $g(b) \in A$ such that $f(g(b)) = b$. That is, f is onto.

Hence the theorem is proved.

E E25) Consider the following functions from **R** to **R**. For each determine whether it has an inverse and, when the inverse exists, find it.

a) $f(x) = x^2$

b) $f(x) = 0$

c) $f(x) = 11x + 7$

We now come to a particular kind of function, namely, a binary operation.

1.5.2 Binary Operation

You are familiar with the operations of addition and multiplication on the set of real numbers. Addition is a function which associates with $(a,b) \in \mathbf{R}^2$ the element $a + b$ of **R**. So, it is a function from $\mathbf{R} \times \mathbf{R}$ to **R**. Can you see that multiplication is also a function from $\mathbf{R} \times \mathbf{R}$ to **R**? These functions can be performed on any two elements of **R**. They are examples of binary operations, which we now define.

Definition: A binary operation on a non-empty set S is a function from $S \times S$ to S.

Thus, a binary operation on S associates a unique element in S to each pair of elements in S. The word 'binary' means involving pairs. It is customary to denote a binary operation by a symbol such as $+, ., 0, *$, etc.

As mentioned earlier, + and × are binary operations on **R**.
Another example is $* : \mathbf{R} \times \mathbf{R} \to \mathbf{R}: a * b = \frac{a+b}{2}$

Some binary operations can have special properties which we now define.

Definition: A binary operation $*$ on a set S is said to be
a) **closed** on a subset T of S if $t_1 * t_2 \in T \; \forall \; t_1, t_2 \in T$.
b) **commutative** if $a * b = b * a \; \forall \; a, b \in S$.
c) **associative** if $(a*b)* c = a*(b*c) \; \forall \; a,b,c \in S$.

For example, the operations of addition and multiplication on **R** are commutative as well as associative. But, subtraction is neither commutative nor associative on **R**. Why? Is $a-b = b-a$, or $(a-b)-c = a-(b-c) \; \forall \; a,b,c \in \mathbf{R}$? No. For example, $1-2 \neq 2-1$ and $(1-2)-3 \neq 1-(2-3)$. Also subtraction is not closed on $\mathbf{N} \subseteq \mathbf{R}$, because $1 \in \mathbf{N}, 2 \in \mathbf{N}$ but $1-2 \notin \mathbf{N}$.

Note that a binary operation on S is always closed on S, but may not be closed on a subset of S.

In calculations you must have often used the fact that $a(b+c) = ab + ac$ and $(b+c)a = ba + ca \; \forall \; a,b,c \in \mathbf{R}$. We say that multiplication distributes over addition in **R**. In general, we have the following definition.

Definition: If o and $*$ are two binary operations on a set S, we say that $*$ **is distributive over** o if $\forall \; a,b,c \in S$, we have
$a*(boc) = (a* b)o(a*c)$, and $(boc)*a = (b*a)o(c*a)$.

Example 9: Let $a*b = \frac{a+b}{2} \; \forall \; a,b \in \mathbf{R}$. Prove that the operation of multiplication in **R** distributes over $*$.

Solution: We have to see whether $a(b*c) = ab * ac$ and $(b*c)a = ba * ca$.

Now $a(b*c) = a\frac{(b+c)}{2} = \frac{ab+ac}{2} = ab * ac$.

Also $(b*c)a = \frac{(b+c)}{2}a = \frac{ba+ca}{2} = ba * ca$.

Hence, multiplication is distributive over $*$.

Now, go back to E10. What does it say? It says that the intersection of sets distributes over the union of sets and the union of sets distributes over the intersection of sets.

Let us now look deeper at some binary operations. You know that, for any $a \in \mathbf{R}, a + 0 = a$ and $0+a = a$ and $a+(-a) = (-a)+a = 0$. We say that 0 is the identity element for addition and $(-a)$ is the negative, or additive inverse, of a. In general, we have the following definition.

Definition: Let $*$ be a binary operation on a set S. If there is an element $e \in S$ such that $\forall \; a \in S$, $a * e = a$ and $e * a = a$, then e is called **an identity element** for $*$.

For $a \in S$, we say that $b \in S$ is an **inverse** of a, if $a * b = e$ and $b * a = e$. In this case, we usually write $b = a^{-1}$

In the following theorem we will prove the uniqueness of the identity element for $*$, and the uniqueness of the inverse of an element with respect to $*$, if it exists.

Theorem 5: Let $*$ be a binary operation on a set S. Then
a) if $*$ has an identity element, it must be unique.
b) if $*$ is associative and $s \in S$ has an inverse with respect to $*$, it must be unique.

Proof: a) Suppose e and e′ are both identity elements for $*$.
Then $e = e * e'$, since e′ is an identity element
$= e'$, since e is an identity element.
That is, $e = e'$. Hence, the identity element is unique.

b) Suppose there exist $a, b \in S$ such that $s * a = e = a * s$ and $s * b = e = b * s$, e being the identity element for $*$. Then

$$a = a*e = a*(s*b)$$
$$= (a*s) * b, \text{ since } * \text{ is associative}$$
$$= e*b = b$$

That is, $a = b$.
Hence, the inverse of s is unique.

This theorem allows us to use the identity element and the inverse, henceforth.

Example 10: If the binary operation $\oplus: \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ is defined by $a \oplus b = a+b-1$, prove that $\oplus$ has an identity. If $x \in \mathbf{R}$, determine the inverse of x with respect to $\oplus$, if it exists.

Solution: We are looking for some $e \in \mathbf{R}$ such that $a \oplus e = a = e \oplus a \; \forall \; a \in \mathbf{R}$. Now, $a \oplus e = a + e - 1$. So we want $e \in \mathbf{R}$ such that $a+e-1 = a \; \forall \; a \in \mathbf{R}$.
Obviously, $e = 1$ will satisfy this. Also, $1 \oplus a = a \; \forall \; a \in \mathbf{R}$. Hence, 1 is the identity element of $\oplus$.

For $x \in \mathbf{R}$, if b is the inverse of x, we should have $b \oplus x = 1$,
i.e., $b + x - 1 = 1$, so $b = 2-x$.
Indeed, $(2-x) \oplus x = (2-x) + x - 1 = 1$, and $x \oplus (2-x) = x+2-x-1=1$.
So $x^{-1} = 2-x$.

E E26) For the following binary operations defined on **R**, determine whether they are commutative, associative or have identity elements.

a) $x \oplus y = x + y - 5$.

b) $x * y = 2(x + y)$

c) $x \triangle y = \frac{x-y}{2}$

Now that you are familiar with sets and binary operations we will study sets with particular types of operations. This course is built on such sets.

1.6 FIELDS

You must be familiar with the sets
Q, of all rational numbers
R, of all real numbers
C, of all complex numbers.

In this section you will discover that these sets are examples of fields. **Q** and **R** were known to Euclid, way back in 300 B.C. The complex number field, **C**, is relatively new. It was developed in the 18th century.

All fields need not be infinite sets. You will also come across fields with only a finite number of elements. These finite fields were studied by Gauss in his book Disquisitiones Arithmeticae.

In the following definition we will talk of properties of the binary operations denoted by '+' and '·'. Do not confuse these with the usual addition and multiplication in **R** (though these operations in **R** do satisfy the properties given, as you can check for yourself as we go along).

Definition: Let + and · be two binary operations on a non-empty set **F**. The set **F** is called a field if the following 9 properties hold $\forall$ a,b,c $\in$ **F**.

A1) + is associative: (a+b)+c = a+(b+c)

A2) $\exists$ an identity element with respect to +, denoted by 0:
a+0 = 0+a = (0 is called the **zero element**).

A set F for which A1–A3 hold is called a group with respect to +

A3) Every element of **F** has an inverse with respect to +: for any a $\in$ **F**, $\exists$ b $\in$ **F** such that a+b = 0 = b+a. b is written as (−a) and is called the inverse of a with respect to +.

A4) + is commutative: a + b = b + a.

M1) · is associative: (a·b)·c = a·(b·c)

M2) $\exists$ an identity element with respect to; denoted by e:
a·e = e·a = a.

F is called a ring with respect to + and · if it satisfies A1–A4, M1 and D.

M3) Every element of **F** \ {0} has an inverse with respect to : : for any a $\in$ **F**\{0}
$\exists$ b $\in$ **F** \ {0} such that a.b = e = b·a. (b is written as a^{-1})

M4) · is commutative: a·b = b·a

D) · distributes over + :
(a+b)·c = a·c + b·c and a·(b+c) = a·b + a·c

The operation that satisfies A1−A4 is called **addition,** and its inverse operation is called subtraction. The other binary operation is called **multiplication,** and its inverse operation is called division. Thus, subtraction and division are defined by
a − b = a+(−b), and a÷ b = a·b^{-1} for b ≠ 0.
Note that a field is closed under the basic operations of addition, subtraction and multiplication. The set of non-zero elements of a field are closed under division. Can you see that both **Q** and **R** are fields? You just need to check that they satisfy the 9 properties for the usual operations of addition and multiplication. The system **Z** is not a field because, for example, 2 $\in$ **Z** does not have a multiplicative inverse in **Z.** This violates property M3.

E E27) Show that the system **C** of complex numbers is also a field, the operations being given by
(a+ib) + (c+id) = (a+c) + i(b+d), and
(a+ib) · (c+id) = ac − bd + i (bc+ad) $\forall$ a,b,c,d $\in$ **R.** ($i = \sqrt{-1}$.)

An important property of every field is expressed in the following result.

Theorem 6: If **F** is a field, then $\forall$ a $\in$ **F**, a·0 = 0.

Proof: Let a·0 = b.

Then b = a·0 = a(0 + 0) (because 0 + 0 = 0)

= a·0 + a·0 (distributive property)

= b + b

That is, b = b + b

Hence 0 = b + (−b) = (b+b) + (−b)

= b+(b+(−b)) (Associative property)

= b + 0

= b

Thus, b = 0, i.e., a·0 = 0

So far we have only given examples of infinite fields. Now we give an example of a finite field.

Example 11: On the set $\mathbf{Z}_3 = \{0,1,2\}$ we define the binary operations $\oplus$ and $\odot$ as follows:

$x \oplus y$ = remainder left on dividing x + y by 3.

$x \odot y$ = remainder left on dividing x · y by 3.

$\forall$ x, y $\in \mathbf{Z}_3$.

Show that $\mathbf{Z}_3$ is a field. It is called the **field of integers modulo 3.**

Solution: It can be easily verified that both the operations are commutative and associative. 0 and 1 are the additive and multiplicative identities respectively. The additive inverse of 0,1,2, are 0,2 and 1, respectively. The multiplicative inverses of 1 and 2 are 1 and 2, respectively. You can also verify that multiplication is distributive over addition. So $\mathbf{Z}_3$ is a field. Note that $\mathbf{Z}_3$ is a finite field since it only has 3 elements.

In general, given any prime number p, we get a finite field $\mathbf{Z}_p$. The underlying set of $\mathbf{Z}_p$ is {0,1,2,..,p−1}. The binary operations on $\mathbf{Z}_p$ are $\oplus$ and $\odot$ defined as follows:

$x \oplus y$ = remainder left on dividing x + y by p.

$x \odot y$ = remainder left on dividing x·y by p.

$\forall$ x,y $\in \mathbf{Z}_p$.

These fields are called **prime fields.**

E E28) If R = {a / b | a,b $\in$ **Z**, b odd}, is R a field?

Before ending this section we will define an important trait of a field, namely, its characteristic.

Definition: If, for a field **F**, $\exists$n $\in$ **N** such that na = 0 $\forall$ a $\in$ **F**, then the least such positive integer n is called the **characteristic** of the Field **F.**

If no such positive integer exists we say that the field is of **characteristic** 0.

Example 12: What are the characteristics of

a) **Q, R, C**?

b) the prime field $\mathbf{Z}_p$, for any prime number p?

Solution: a) For any $n \in \mathbf{N}$ and $x \in \mathbf{Q}$, $nx = 0 \Rightarrow x = 0$. $\therefore$, the characteristic of **Q** is zero. Similarly, the characteristics of **R** and **C** are zero.

b) The characteristic of any prime field $\mathbf{Z}_p$ is p. Why? Well, what happens if you take an element $x \in \mathbf{Z}_p$, and divide px by p? The remainder is zero. That is, $p \odot x = 0$, for any $x \in \mathbf{Z}_p$. Also, if you take any natural number m, $0 < m < p$, then $m \odot 1 = m \neq 0$. Therefore, p is the least positive integer such that $p \odot x = 0 \; \forall \; x \in \mathbf{Z}_p$. This tells us that the characteristic of $\mathbf{Z}_p$ is p.

It can be proved that if a **field is not of characteristic zero then its characteristic has to be a prime number.**

When you go to the next unit you will realise how important it is to be thoroughly familiar with fields. Do make sure that you are quite at ease with this section. Now let us briefly go through the points brought up in this unit.

1.7 SUMMARY

We conclude by summarising what we have covered in this unit. We have

1) studied the concepts of sets, subsets, complements, unions and intersections of sets.
2) shown you how to represent sets by Venn diagrams.
3) defined the Cartesian product of sets, as well as relations and equivalence relations on a set.
4) defined the notions of a function, composition of functions and inverse functions.
5) studied the possible properties of binary operations on a set.
6) defined and seen many examples of fields, both infinite and finite.
7) defined the characteristic of a field.

1.8 SOLUTIONS/ANSWERS

E1) $A = \{11,12,13,14\}$ $\quad C = \{1,2,4,5,10,20\}$

$B = \{12,14\}$ $\quad D = \{1/2, 1/3, 2/3\}$

E2) $P = \{x \mid x \text{ is an integer and } 6 < x < 10\}$

$= \{x \mid x \text{ is an integer and } 7 \leq x \leq 9\}$

$Q = \{x \mid x = 1 \text{ or } x \text{ is a prime number less than } 12\}$

(A prime number is a number whose only factors are 1 or itself.)

$R = \{x \mid x \text{ is a multiple of } 3\}$

E3) (a) and (d)

E4) For $x \in A \cup B$, we have $x \in A$ or $x \in B$. In either case $x \in C$. Therefore, $A \cup B \subseteq C$.

E5) $\phi \cup A = \{x \mid x \in \phi \text{ or } x \in A\}$

$= \{x \mid x \in A\}$, since ϕ has no elements.

$= A$

$\phi \cap A = \phi$, since $\phi \subseteq A$.

E6) a) True b) False c) False d) True e) True

E7) a) {a,b,c,p,q} b) {a,p} c) {a,p} d) {a,p}

$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ always, as you will see in E10.

E8) a) Since $x \in A$ if and only if $x \notin A^c$, we find that A and A^c are disjoint.

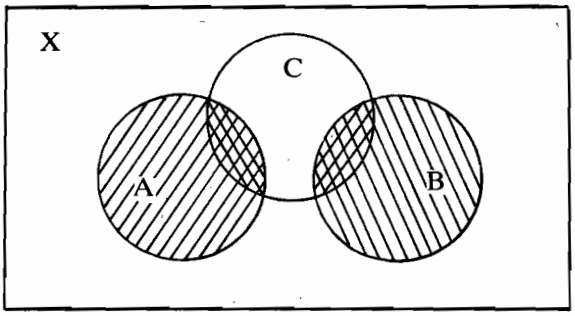
b) For any $x \in X$, $x \in A$ or $x \in A^c$. Therefore, $A \cup A^c = X$.

c) Let $x \in (A^c)^c$. Then $x \notin A^c$, so that $x \in A$. Thus, $(A^c)^c \subseteq A$. On the other hand, if $x \in A$, then $x \notin A^c$.

Hence, $x \in (A^c)^c$. $\therefore A \subseteq (A^c)^c$. $\therefore$, by the definition of equality of sets we find $(A^c)^c = A$.

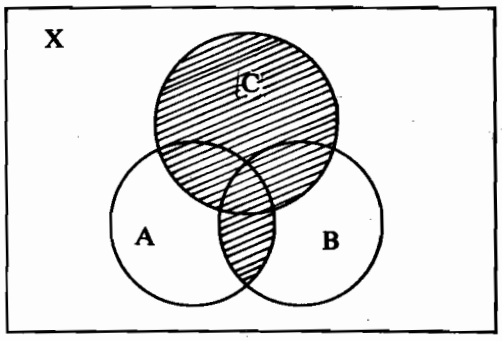
E9) $x \in (A \cap B)^c \iff x \notin A \cap B \iff x \notin A$ or $x \notin B \iff x \in A^c$ or $x \in B^c$
$\iff x \in A^c \cup B^c$.

E10) a)



$A \cup B$ is all the shaded portion. $(A \cup B) \cap C$ is the double shaded portion. As you can see from the figure, this is the same as the union of $A \cap C$ (the double shaded portion in A) and $B \cap C$ (the double shaded portion in B).

b)



$(A \cap B) \cup C$ is the shaded portion. From the figure you can see that it is the same as the set $(A \cup C) \cap (B \cup C)$.

E11) $A \times B = \{(2,2), (5,2), (2,3), (5,3)\}$
$B \times A = \{(2,2), (2,5), (3,2), (3,5)\}$
$A \times A = \{(2,2), (2,5), (5,2), (5,5)\}$

E12) Since the first element in each pair has to be in A, we get $A = \{7,2\}$. Similarly, $B = \{2,3,4\}$.

E13) $(x,y) \in (A \cup B) \times C \iff x \in A \cup B$ and $y \in C$
$\iff x \in A$ or $x \in B$ and $y \in C$
$\iff (x,y) \in A \times C$ or $(x,y) \in B \times C$
$\iff (x,y) \in (A \times C) \cup (B \times C)$

E14) a) F b) T c) T

E15) R is reflexive since $5 \mid a - a = 0$, for any $a \in \mathbf{N}$.
R is symmetric because, if $5 \mid a-b$, then $5 \mid b-a$, for any $a,b \in \mathbf{N}$.
R is transitive because, if $5 \mid a-b$ and $5 \mid b-c$, then
$5 \mid (a-b) + (b-c)$, that is, $5 \mid a-c$, for any $a,b,c \in \mathbf{N}$.

E16) R is reflexive, since $a \mathrel{R} a \; \forall \; a \in \mathbf{Z}$.
R is symmetric, since $a \mathrel{R} b \Rightarrow b \mathrel{R} a \; \forall \; a,b \in \mathbf{Z}$.
R is transitive, since $a \mathrel{R} b$, $b \mathrel{R} c \Rightarrow a \mathrel{R} c \; \forall \; a,b,c \in \mathbf{Z}$
$\mathbf{Z}_1 = \{x \in \mathbf{Z} \mid x \mathrel{R} 1\} = \{1\}$

E17) R is clearly reflexive and symmetric.
Now, if a R b and $a \in A$, then $b \in A$. Again, if b R c, then, since $b \in A$, we get $c \in A$. So we find that whenever $a \in A$, $c \in A$. Similarly, if $a \in B$, $c \in B$ and if $a \in C$, $c \in C$. Thus aRb, bRc $\Rightarrow$ a R c. That is, R is transitive.
For $b \in B$, $S_b = \{x \in S \mid x\ R\ b\} = \{x \in S \mid x \in B\} = B$.

E18) Let $m, n \in \mathbf{N}$ such that $f(m) = f(n)$. Then $m+5 = n+5$. Therefore, $m = n$. This means that $m \neq n \Rightarrow f(m) \neq f(n)$. Therefore, f is $1-1$. f is not onto because there is no $n \in \mathbf{N}$ such that $f(n) = 1$. Why? Well, if $f(n) = 1$, then $n+5 = 1$, and hence, $n = -4 \notin \mathbf{N}$.

E19) f is $1-1$, just as shown in E18.
Now f is onto because given any $z \in \mathbf{Z}$, $\exists\ z-5 \in \mathbf{Z}$ such that $f(z-5) = z$.

E20) The range of f $= \{f(x) \mid x \in A\}$
$= \{f(1), f(-1), f(2), f(3)\}$
$= \{2, 12, 0\}$

E21) a) $I_A: A \to A$ is $1-1$ (since $a_1 \neq a_2 \Rightarrow I_A(a_1) \neq I_A(a_2)$), and is onto (since the range of I_A is A).
b) Suppose X has at least two elements, say x and y. Then $f(x) = c = f(y)$, but $x \neq y$. This means that f is not $1-1$, which is a contradiction. Therefore, X also has to be a singleton, that is, have only one element, if f is to be $1-1$.

E22) a) Both fog and gof can be defined.
$fog\ (x) = f(g(x)) = 5g(x) = 5(x+5)\ \forall\ x \in \mathbf{R}$.
$gof\ (x) = g(f(x)) = f(x) + 5 = 5x + 5\ \forall\ x \in \mathbf{R}$.
Note that $fog \neq gof$.
b) $(fog)\ (x) = 5(x/5) = x\ \forall\ x \in \mathbf{R}$.
$(gof)\ (x) = 5x/5 = x\ \forall\ x \in \mathbf{R}$.
In this case $fog = gof$.
c) $(fog)\ (x) = (\sin x + 3)^3$ and $(gof)\ (x) = \sin x^3 + 3$.
d) $(fog)\ (x) = |x|^2$ and $(gof)\ (x) = |x|^2$.
In this case $fog = gof$.

E23) Since $I_A: A \to A$, $I_A \circ g$ is defined. Similarly, $g \circ I_B$ is defined. Now, $(I_A \circ g)\ (b) = I_A(g(b)) = g(b)\ \forall\ b \in B$.
$\therefore, I_A \circ g = g$.
Similarly, $g \circ I_B = g$.

E24) Define $g: \mathbf{R} \to \mathbf{R}: g(x) = 3x$. Then $fog = I_{\mathbf{R}} = gof$.

E25) a) f is not $1-1$ since $f(-1) = f(1)$. $\therefore$, f is not bijective and f^{-1} does not exist.
b) f is not onto, and hence f^{-1} does not exist.
c) f is bijective, and hence f^{-1} exists. In fact $f^{-1}: \mathbf{R} \to \mathbf{R}: f^{-1}(x) = \frac{x-7}{11}$

E26) a) Since $x \oplus y = y \oplus x$ for any $x, y \in \mathbf{R}$, $\oplus$ is commutative.
Since $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ for any $x, y, z \in \mathbf{R}$, $\oplus$ is associative.
Since $x \oplus 5 = 5 \oplus x = x$, we get 5 to be the identity element for $\oplus$.
b) $*$ is commutative, not associative and has no identity element.
c) $\triangle$ is neither commutative nor associative, and has no identity element.

E27) C is a field because '+' satisfies A1 – A4, the zero being $0 + i0 = 0$, and the inverse of $a + ib$ being $(-a) + i(-b)$. '$\cdot$' satisfies M1 – M4, the identity being $1 + i0 = 1$ and the inverse of $(a + ib)$ being $\frac{a - ib}{a^2 + b^2}$. D is also satisfied.

E28) Over here + and $\cdot$ are the usual + and $\cdot$ in **Q**. Therefore, A1 – A4 are satisfied, the zero being 0/1 (or 0/b for any odd b!). M1, M2, M4 and D are also satisfied, the multiplicative identity being 1/1. But M3 is not satisfied, since 2/1 has no inverse in **R**.