$\Rightarrow (A \cup B) \cup C \subseteq A \cup (B \cup C)$ ...(2)

By using equations (1) and (2) we get,

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

(*iii*) ***Distributive laws:*** For three given sets A, B and C to prove that,

(*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: Let $a \in A \cap (B \cup C)$,

Here $a \in A \cap (B \cup C)$

$\Rightarrow a \in A$ and $a \in B \cup C$

$\Rightarrow a \in A$ and ($a \in B$ or $a \in C$)

$\Rightarrow$ ($a \in A$ and $x \in B$) or ($a \in A$) or $a \in C$)

$\Rightarrow a \in A \cap B$ or $a \in A \cap C$

$\Rightarrow a \in (A \cap B) \cup (A \cap C)$

Hence,

$A \cup (B \cup C) \subset (A \cap B) \cup (A \cap C)$ ...(1)

Conversely let $b \in (A \cap B) \cup (A \cap C)$

Here, $b \in (A \cap B) \cup (A \cap C) \Rightarrow b \in A \cap B$ or $b \in A \cap C$

$\Rightarrow$ ($b \in A$ and $b \in B$) or ($b \in A$ and $b \in C$)

$\Rightarrow$ ($b \in A$ and $b \in B$) or ($b \in C$)

$\Rightarrow$ ($b \in A$ and $b \in B \cup C$)

$\Rightarrow$ ($b \in A \cap (B \cup C)$

$\therefore (A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ ...(2)

By using equations (1) and (2) we get,

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

Number of Elements in the Union of two Or more Sets

Let A, B and C be three finite sets and let $n(A)$, $n(B)$, $n(C)$ respectively denote the number of elements in these sets . Then we see that,

$$n(A \cup B) = n(A) + n(B) - n(A \cap B) \quad \text{...(1)}$$

In case A and B are disjoint sets then, $A \cap B = \phi$ and $n(A \cap B) = n(\phi) = 0$

i.e., for disjoint sets A and B

$$n(A \cup B) = n(A) + n(B)$$

Similarly we can show that,

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(A \cap C) + n(A \cap B \cap C) \quad ...(2)$$

Solved Example

Example 10: In a group of 1000 people, there are 750 who can speak Hindi and 400 who can speak Bengali. How many people can speak Hindi only? How many people can speak Bengali only? How many people can speak both Hindi and Bengali?

Solution: Let H and B denote the sets of those people. Who can speak Hindi and Bengali respectively.

Given:

$$n(H \cup B) = 1000,\ n(H) = 750,\ n(B) = 400$$

Now

$$n(H \cap B) = n(H) + n(B) - n(H \cup B)$$
$$= 750 + 400 - 1000$$

$$\Rightarrow \quad n(H \cap B) = 150$$

Hence 150 people can speak both Hindi and Bengali. Now we have to find those people who can speak Hindi only, that is, $n(H \cap B')$

But $$n(H \cap B') = n(H) - n(H \cap B) = 750 - 150 = 600$$

So, 600 people can speak Hindi only.

Similarly:

$$n(B \cap H') = n(B) - n(B \cap H) = 400 - 150 = 250$$

So, 250 people can speak Bengali only.

Example 11: In a survey of 200 students of a higher secondary school, it was found that 120 studied mathematics; 90 studied physics; and 70 studied chemistry; 40 studied mathematics and physics; 30 studied physics and chemistry; 50 studied chemistry and mathematics, and 20 studied none of these subjects. Find the number of students who studied all the three subjects.

Solution: Given,

$$n\,(U) = 200,\ n\,(M) = 120,\ n\,(P) = 90,\ n\,(C) = 70$$
$$n\,(M \cap P) = 40,\ n\,(P \cap C) = 30,\ n\,(C \cap M) = 50,\ n\,(M \cup P \cup C)' = 20$$

Now

$$n\,(M \cup P \cup C)' = n\,(U) - n\,(M \cup P \cup C)$$

$$\Rightarrow \quad 20 = 200 - n\,(M \cup P \cup C)$$

$$\Rightarrow \quad n\,(M \cup P \cup C) = 200 - 20 = 180$$

and;

$$= n(M) + n\,(P) + n\,(C) - n\,(M \cap P) - n\,(P \cap C)$$

$$n(M \cup P \cup C) - n(C \cap M) + n(M \cap P \cap C)$$

$$180 = 120 + 90 + 70\ 40 - 30 - 50 + n(M \cap P \cap C)$$

$$\Rightarrow \quad n(M \cap P \cap C) = 180 + 120 - 280 = 20$$

Hence 20 students studied all the three subjects.

Example 12: In a survey of population of 450 people, It is found that 205 can speak English, 210 people can speak Hindi and 120 people can speak Tamil. If 100 people can speak both English and Hindi, 80 can speak both English and Tamil, 35 people can speak Hindi and Tamil, and 20 people all the three languages. Find the numbers of people who can speak. English but not Hindi or Tamil. Find also the number of people who can speak neither English nor Hindi nor Tamil.

Solution: Let F, H and T denote the sets of those people who can speak English, Hindi and Tamil respectively.

Given,

$$n(U) = 450,\ n(E) = 205,\ n(H) = 210, \text{ and } n(T) = 120$$

$$n(H \cap T)\ 35,\ n(H \cap E) = 100,\ n(E \cap T) = 80,$$

$$n(H \cap T \cap E) = 20$$

Now, we have to find the human of people who can English but not Hindi or Tamil.

$$n(H \cap E' \cap T') = n(H) - n(H \cap E) - H(H \cap T) + n(H \cap E \cap T)$$

$$= 210 - 100 - 35 + 20$$

$$= 95$$

Now,

$$n(H \cup E \cup T) = n(H) + n(E) + n(T) - n(H \cap E) - n(E \cap T)$$

$$- n(H \cap T) + n(H \cap E \cap T)$$

$$= 250 + 210 + 120 - 35 - 100 - 80$$

$$= 320$$

Now we have to find the number of people who can speak neither English nor Hindi nor Tamil.

$$n(H \cup E \cup T)' = n(\cup) - (H \cup E \cup T)$$

$$= 450 - 320$$

$$= 130$$

So, 130 people cannot speak Hindi, English or Tamil.

Example 13: At a certain conference of 100 people there are 29 Indian women and 23 Indian men of these Indian people 4 are doctors and 24 are either men or doctors. There are no foreign doctors. How many foreigners are attending the conference? How many women doctors are attending the conference?

Solution: Let E denote the set of all Indian people attending the conference. Then E' will denote the set of all foreigners attending the conference. Also let W, M and D denote the set of Indian women, Indian men and Indian doctors respectively.

Given:

$$n(E \cup E') = 100,\ n(W) = 29,\ n(M) = 23,\ n(B) = 4,\ (M \cup D) = 243$$

Clearly

$$W \cap H = \phi \text{ and } W \cup M = E$$

So, $$n(E) = n(W) + n(M) = 29 + 23 = 52$$

Also $n(E \cup E')$ 100, or $n(E) + n(E') = 100$

$\therefore$ $$52 + n(E') = 100$$

or $$n(E') = 100 - 52 = 48$$

So, 48 foreigners are attending the conference since there are no foreign doctors there can be no foreign women doctors. Hence in order to find out women doctors, we simply find Indian women doctors,

i.e., $$n(W \cap D)$$

Now we have,

$$n(M \cup D) = n(M) + n(D) - n(M \cap D)$$

or $$24 = 23 + 4 - n(M \cap D)$$

i.e., $$n(M \cap D) = 3$$

Thus the number of male Indian doctors is 3 since there are all 4 Indian doctors.

The number of Indian women doctors = 4 – 3 = 1

Hence

$$n(W \cap D) = 1$$

Example 14: An analysis of 100 personnel injury claims made upon a motor insurance company revealed that loss or injury in respect of an eye, an arm or a leg occurred in 30, 50 and 70 cases respectively, claims involved this loss or injury to two of these member numbered 44. How many claims involved loss or injury to all the three, we must assume that one or another of the three members was mentioned in each of the 100 claims.

Solution: Let E, A and L denote the sets of people having injuries in eyes arms or legs respectively.

Given,

$$n(E \cup A \cup L) = 100,\ n(E) = 30,\ n(A) = 50,\ n(L) = 70$$

Also,

$$n(E \cap A \cap L') \cup (A \cap L \cap E') \cup (L \cap E \cap A')] = 44 \qquad ...(1)$$

Now,

$$n(E \cup A \cup L) = n(E) + n(A) + n(L) - n(E \cap A) - n(A \cap L) - n(L \cap E) + n(E \cap A \cap L)$$

$$100 = 30 + 50 + 70 - n(E \cap A) - n(A \cap L) - n(L \cap E) + n(E \cap A \cap L)$$

$$\Rightarrow n(E \cap A) + n(A \cap L) + n(L \cap E) - n(E \cap A \cap L) = 30 + 50 + 70 - 100 = 50 \quad \ldots(2)$$

Since: $(E \cap A \cap L')$, $(A \cap L \cap E')$, $(L \cap E \cap A')$ are disjoints

So by equation (1), we get

$n(E \cap A \cap L') + n(A \cap L \cap E) + n(L \cap E \cap A') = 44$

or $(E \cap A) - n(E \cap A \cap L) + n(A \cap L) - n(A \cap L \cap E) + n(L \cap E) - n(L \cap E \cap A) = 44$

or $n(E \cap A) + n(A \cap L) + n(L \cap E) - 3n(E \cap A \cap L) = 44 \quad \ldots(3)$

$\Rightarrow$ (2) - (3) We get,

$$2n(E \cap A \cap L) = 6$$

or

$$n(E \cap A \cap L) = 3$$

Example 15: De Morgan's Laws: To prove that

(*a*) $(A \cup B)' = A' \cap B'$

(*b*) $(A \cap B)' = A' \cup B'$

(*c*) $A - (B \cup C) = (A - B) \cap (A - C)$

(*d*) $A - (B \cap C) = (A - B) \cup (A - C)$

Solution: (*a*) Let $x \in (A \cup B)'$

But $x \in (A \cup B)' \Rightarrow x \in A \cup B$

$\Rightarrow$ $x \in A$ and $x \notin B$

$\Rightarrow$ $x \in A'$ and $x \notin B'$

$\Rightarrow$ $x \in A' \cap B'$

i.e., $(A \cup B)' \subseteq A' \cap B' \quad \ldots(1)$

Conversely, let

$y \in A' \cap B'$

$\Rightarrow$ $y \in A'$ and $\in B'$

$\Rightarrow$ $y \notin A'$ and $y \notin B$

$\Rightarrow$ $y \notin A \cup B$

$\Rightarrow$ $y \in (A \cup B)'$

i.e., $A' \cap B' \subseteq (A \cup B)'$ ...(2)

By using equations (1) and (2) we get,

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

(*b*) Let $a \in (A \cup B)'$

But $a \in (A \cap B)' \Rightarrow a \notin (A \cap B)$

$\Rightarrow$ $a \notin A$ or $a \notin B$

$\Rightarrow$ $a \in A'$ or $a \in B'$

$\Rightarrow$ $a \in A' \cup B'$

i.e., $(A \cap B)' \subseteq A' \cup B'$ ...(1)

Conversely, let $b \in A' \cup B'$

But $b \in A' \cup B' \Rightarrow b \in A'$ or $b \in B'$

$\Rightarrow$ $b \notin A$ or $b \notin B$

$\Rightarrow$ $b \notin A \cap B$

$\Rightarrow$ $b \in (A \cap B)'$

i.e., $A' \cup B' \subseteq (A \cap B)'$ ...(2)

By using equations (1) and (2) we get,

$$(A \cap B)' = A' \cup B' \quad \text{...(}b\text{)}$$

(*c*) Let $x \in A - (B \cup C)$

But $x \in A - (B \cup C)$ $\Rightarrow x \in A$ and $x \notin B \cup C$

$\Rightarrow x \in A$ and $[x \notin B$ and $x \notin C]$

$\Rightarrow [x \in A$ and $x \notin B]$ and $[x \in A$ and $x \notin C]$

$\Rightarrow x \in (A - B)$ and $x \in (A - C)$

$\Rightarrow x \in (A - B) \cap (A - C)$

i.e., $A - (B \cup C) \subseteq (A - B)\ (A - C)$ ...(1)

Conversely let

$b \in (A - B) \cap (A - C) \Rightarrow b \in (A - B)$ and $b \in (A - C)$

$\Rightarrow b \in A$ but $b \in B$ and $b \in A$ but $b \in C$

$\Rightarrow b \in A$ but $b \notin B$ and $b \notin C$

$\Rightarrow b \in A$ but $b \in B \cup C$

$\Rightarrow b \in A - (B \cup C)$

i.e., $(A - B)\ (A - C) \subseteq A - (B \cup C)$ ...(2)

By using equations (1) and (2) we get,

$$A - (B \cup C) = (A - B) \cap (A - C) \quad \ldots(c)$$

(*c*) Here, $A - (B \cap C) = A \cap (B \cap C)'$

$= A \cap (B' \cup C')$ by equation (*b*)

$= (A \cap B') \cup (A \cap C')$ by distributive law

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

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

Example 25: Prove that,

(*i*) $A \cap (B - C) = (A \cap B) - (A \cap C)$

(*ii*) $(A - B) \cup B = A$ iff $B \subset A$

Solution:

(*i*) $A \cap (B - C) = A \cap B - A \cap C$

Let $a \in A \cap C\ (B - C)$

But $a \in A \cap (B - C) \Rightarrow a \in A$ and $a \in (B - C)$

$\Rightarrow a \in A$ and $a \in B$ but $a \notin C$

$\Rightarrow (a \in A$ and $a \in B)$ but $a \notin A \cap C$

$\Rightarrow a \in (A \cap B)$ but $a \notin A \cap C$

$\Rightarrow a \in (A \cap B) - (A \cap C)$

i.e., $A \cap (B - C) \subseteq (A \cap B) - (A \cap C) \quad \ldots(1)$

Now let $b \in (A \cap B) - (A \cap C)$

$\therefore\ b \in (A \cap B) - (A \cap C) \Rightarrow b \in A \cap B, b \notin A \cap C$

$\Rightarrow b \in A$ and $b \in B$ and $b \in A$ but $b \notin C$

$\Rightarrow b \in A$ and $b \in B$ but $b \notin C$

$\Rightarrow b \in A, b \in B - C$

$\Rightarrow b \in A \cap (B - C) \quad \ldots(2)$

By using equations (1) and (2) we get,

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

(*ii*) $(A - B) \cup B\ A$ iff $B \subset A$

$(A\text{-}B) \cup B = A \Leftrightarrow (A \cap B') \cup B = A$

$\Leftrightarrow (A \cup B) \cap (B' \cup B) = A$ (by distributive law)

$\Rightarrow \Leftrightarrow (A \cup B) \cap S = A\ (\because B' \cup B = S$ universal law)

$\Rightarrow \Leftrightarrow A \cup B\ A\ (\because A \cap S = A)$

$\Rightarrow$ all elements of B are in A

$\Rightarrow$ $B \subset A$

Hence $(A - B) \cup B \Rightarrow B \subseteq A$

Example 17: Prove that,

(*a*) $(A - B) \cup (B - A) = (A \cup B) - A \cap B)$

(*b*) $(A - B) = \phi$ iff $A \subseteq B$

Solution: (*a*) We have to prove that $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$

(*a*) Hence, $(A - B) \cup (B - A) = (A \cap B') \cup (B \cap A')$

$\therefore$ $A - B = A \cap B'$

$= [(A \cap B') \cup B] \cap [(A \cap B') \cup A']$ ...by distributive law

$= [(A \cup B) \cap (B' \cup B)] \cap [(A \cup A') \cap (B' \cup A')]$

...by distributive law

$= [(A \cup B) \cap S] \cap [S \cap (B' \cup A')]$... $\therefore$ $B' \cup B = S$

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

$= (A \cup B) \cap (B \cap A)'$ ... by De Morgan's law

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

Hence,

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

(*b*) Here, $A - B = \phi \Rightarrow A \cap B' = \phi \therefore (A - B) = A \cap B'$

$\Rightarrow$ A and B' are disjoint

$\Rightarrow$ all elements of A belongs to B

$\Rightarrow A \subseteq B$

Conversely,

$A \subseteq B$ there is no elements in A which does not belongs to B

$\Rightarrow$ $A - B = \phi$

Hence $A - B = \phi \Rightarrow A \subset B$

Example 18: If $A = [1, 2, 3\}$, $B = \{2, 4, 6\}$, $C = \{4, 6, 8, 10\}$ and $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ find A' B' and C' prove that,

(*i*) $(A \cup B)' = A' \cap B'$

(*ii*) $(A \cap B)' = A' \cup B'$ where U is taken as universal set.

Solution: $A = \{1, 2, 3\}$ $B = \{2, 4, 6\}$ and $C = \{4, 6, 8, 10\}$

$$U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$A' = \{4, 5, 6, 7, 8, 9, 10\}$$

$$B' = \{1, 3, 5, 7, 8, 9, 10\}$$

$$C' = \{1, 2, 3, 5, 7, 9\}$$

Now (*i*) $A \cup B = \{1, 2, 3, 4, 6\}$

$$(A \cup B)' = \{7, 8, 9, 10\}$$

$$A' \cap B' = \{5, 7, 8, 9, 10\}$$

Hence,

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

(*ii*) $A \cap B = \{2\}$

$$(A \cap B)' = \{1, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$A' \cup B' = \{1, 3, 4, 5, 6, 7, 8, 9, 10\}$$

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

Example 19: Of the members of there athletic teams a certain schools, 21 are on the basketball team, 26 on hockey team and 29 on the football team 14 play hockey and basketball, 15 play hockey and football, 12 play football and basketball and 8 play all the three games. How many members are there in all.

Solution: We can solve this problem by using formula and venn diagram.

By Formula: Let B, H, and F denote the sets of members who are on the basket-ball team, hockey team and football team respectively.

So, we are given

$$n(B) = 21, n(H)\ 26, n(F) = 29,$$

$$n(H \cap F) = 15, n(F \cap B) = 12$$

and $n(B \cap H \cap F) = 8$

$n(B \cup H \cap F) = ?$

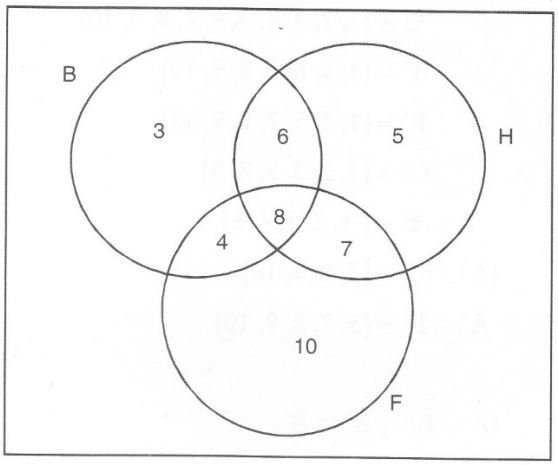
We know that,

$$n(B \cup H\,F) = n(B) + n(H) + n(F) - n(B \cap H) - (H \cap F) - n(F \cap B) + n(B \cap H \cap F)$$

$$= 21 + 26 + 29 - 14 - 15 - 12 + 8 = 43$$

Hence, there are 43 members in all.

By venn diagrams: 8 play all the three games.



Since 14 play hockey and basketball of which 8 are already written in $B \cap H \cap F$, we write 6 in the remaining part of $H \cap B$. Similarly we write 7 and 4 in the remaining parts of $H \cap F$ and $F \cap B$. Finally there are 21 members on the basketball of which $6 + 8 + 4 = 18$ have already been written, So we write 3 in the remaining part of B. Similarly we write 5 and 10 in the remaining parts of H and F respectively.

So,

Total Number = $3 + 6 + 5 + 4 + 8 + 7 + 10 = 43$.

Check Your Progress

1. What is Infinite set? Give example.
2. What is empty set? Give example.

2.7 LET US SUM UP

A set is a collection of definite distinguishable objects such that, given a set and an Object, we can ascertain whether or not the specified object is included in the set. A set is a well-defined collection of distinct objects. By a 'well defined' collection of objects, we mean that there is a rule (s) by means of which it is possible to say that without ambiguity, whether a particular object belongs to the collection or not. Each object belonging to a set is called an element (or a member) of the set.

The most common method of describing the sets are Roster method or listing method or Tabular method and Set Builder method or property method or Rule method.

2.8 KEYWORDS

Sets: A set is a well-defined collection of distinct objects.

Singleton Set: If a set consists of only one element, it is called a singleton set.

Finite Set: A set consisting of a natural number of objects.

Disjoint Sets: Two sets are said to be disjoint.

2.9 QUESTIONS FOR DISCUSSION

1. Find the smallest set A such as, $A \cup \{1, 2, 3\} = \{1, 2, 3, 4, 5, 6, 7, 8\}$
2. Let $A = \{a, b, c, d\}$, $B = \{b, c, d, e, f\}$, $C = \{e, f, g, h, i\}$? Find $A \cup B$, $B \cap C$, $A - B$, $B - A$, $A \cap (B \cup C)$, $A \cup (B \cap C)$ and $A \cup B \cup C$.
3. If $x = \{2, 4, 6, 8, 10\}$ $y = \{6, 8, 10, 12, 14\}$ $z = \{10, 12, 14, 15, 16\}$ and $U = \{1, 2, 3, 4, 6, 8, 10, 12, 14, 16\}$ then find x', $(x \cup y)'$, $(x \cap y)'$ and $(x - y)'$
4. If $x = \{a, b, c, d, e, f\}$, $y = \{e, f, g, h\}$ and $z = \{g\ h, i, j\}$, Find $(x \cup y) \cap (x \cup z)$ and $(x \cap y) \cup (x \cap z)$.
5. If $x = \{1, 2, 3\}$ then find all subsets of x.

Check Your Progress: Modal Answers

1. If number of elements in a set is infinite, the set is called infinite set.

   For Example: Set of natural numbers.

   $N = \{1, 2, 3, 4, ...\}$ is an infinite set.
2. If a set consists of no elements, it is called the empty sector null set or void set and is represented by ϕ.

2.10 SUGGESTED READINGS

Anuranjan Misra, *Discrete Mathematics*, Acme Learning pvt ltd.

Richard Johnsonbaugh, *Discrete Mathematics*, Prentice Hall

V. K. Balakrishnan, *Introductory Discrete Mathematics*, Courier Dover Publications,

R. C. Penner, *Discrete Mathematics: Proof Techniques and Mathematical Structures*, World Scientific, 1999

Mike Piff, *Discrete Mathematics: An Introduction for Software Engineers*, Cambridge University Press, 1991

LESSON

3

RELATIONS

CONTENTS

3.0 AIMS AND OBJECTIVES

After studying this lesson, you will be able to:

- Understand the concept of relations
- Discuss operations on relations
- Discuss types of relations and equivalence relations

3.1 INTRODUCTION: RELATION

A relation between two sets A and B is a subset of A × B. *Symbolically, we can write:*

R is a relation from A to B iff $R \subset A \times B$.

If A = B, then we say that R is a relation on A. We can write aRb iff $(a, b) \in R$ and say that a is R-related to b or that b is a R-relation of a.

We can write $a(\sim R)b$. If a is not R-related to b. We can say that A relation, binds together two-objects of a partition class according to some rule.

When we say that, an ordered pair (x, y) satisfies or belongs to a relation R, *we can write:*

$(x, y) \in R$.

Example: Let X = {2, 3, 6, 9, 18, 27} and R stand for "is thrice of".

Here 6R2, 9R3, 18R6, 27R9. Hence obtained ordered pairs are (6, 2), (9, 3), (18, 6), (27, 9).

Hence, R is defined as the set of ordered pairs:

$$= \{(6, 2), (9, 3), (18, 6), (27, 9)\}$$

3.2 RANGE AND IMAGE

As usual, the pair (a, b) of the relation R has two element. First element a and second element b and a, $b \in R$. If collect first elements from each pairs. i.e. all first element (a) together to form a set and also collect all second elements (b) to form another set, we get two sets each being a subset of A.

The set of all first elements a for which there is a. Corresponding b given by $(a, b) \in R$ and $a, b \in A$ is called the Domain of R.

The set of all b's to which there is some corresponding a such that $(a, b) \in R$ and $a, b \in A$ is called the range or image of R.

Example: Consider the relation $R = \{(x, y) : y = 4x^2,\ x \in N\}$

Here, N = {1, 2, 3, 4, ...}.

$y = 4x^2$, gives the domain of R = and the range of R = {4, 16, 36, ...}.

So, R = {(1, 4), (2, 16), (3, 36)....}.

Binary Relation

A relation R between pairs of elements of a given set is called a binary relation.

3.3 OPERATIONS ON RELATIONS

3.3.1 Inverse of a Relation

The inverse of a relation R is the set of all reversed pairs of R and is denoted by R^{-1}.

So if $R = \{(x, y) : xRy \text{ and } x, y \in R\}$

then $R^{-1} = \{(y, x) : x, y \in R\}$

i.e. $xRy \Leftrightarrow yR^{-1}x$

Example: (*i*) If A = {a, b, c}, B = {1, 2, 3}

Let a relation R such that

$$R = \{(a, 1), (b, 2), (c, 3)\}$$

So here domain of $R = (a, b, c)$

and Range of $R = (1, 2, 3)$

and $R^{-1} = \{(1, a), (2, b), (3, c)\}$

Domain of $R^{-1} = (1, 2, 3)$

and Range of $R^{-1} = (a, b, c)$.

Example: (ii) The inverse of relation "is greater than" is the relation "is less than" *i.e.* $x > y \Leftrightarrow y < x$.

3.3.2 Identity Relation

A relation R in a set A is said to be identity relation denoted by I_A if

$$I_A = \{(a, b) : (a, b) \in A \text{ and } a = b\}$$

This relation is also called Equality relation.

Example: Let A = {*a*, *b*, *c*}

I_A = {(a, a), (b, b), (c, c) is an identity or equality relation in A.

3.3.3 Void Relation

A relation R in a set A is said to be a void relation. If $R = \phi$.

Example: Let A = (1,2,3) and R is a relation defined by *a*R*b*. Iff *a* divides *b* then $R = \phi \subset [A \times A]$ is a void relation.

3.3.4 Universal Relation

A relation R in a set A is said to be universal relation, if R coincide with A × A.

i.e. R is universal relation. iff R = A × A.

Example: A = {1, 2, 3} then

R = A × A = {(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)} is a universal relation.

3.4 COMPOSITE RELATION

Let R_1 and R_2 be the relations from the sets A to B and B to C respectively then the composite of R_1 and R_2 is a relation from A to C denoted by R_2 o R_1

$$R_2 \text{ o } R_1 = [(a, c) \exists b \in B \text{ such that } (a, b) \in R_1 \text{ and } (b, c) \in R_2]$$

$\Rightarrow (a, b) \in R_1,\ (b, c) \in R_2$

$\Rightarrow (a, c) \in R_2 \circ R_1$

Example: If two relations R_1 and R_2 are such that:

$$R_1 = [(a, c), (b, a), (c, d)]$$

and $$R_2 = [(a, b), (b, c), (c, d)]$$

then calculate $R_2 \circ R_1$

Domain $(R_2 \circ R_1)$ = dom (R_1)

$(a, c) \in R_1$ and $(c, d) \in R_2 \Rightarrow (a, d) \in R_2 \circ R_1$

$(b, a) \in R_1$ and $(a, b) \in R_2 \Rightarrow (b, b) \in R_2 \circ R_1$

$(c, d) \in R_1$ and $(d, c) \in R_2 \Rightarrow (c, c) \in R_2 \circ R_1$

Hence, $R_2 \circ R_1 = [(a, d), (b, b), (c, c)]$

3.5 PROPERTIES OF BINARY RELATION

3.5.1 Reflexive

A relation R on a set A is said to be reflexive, if each member $a \in A$ is R-related to itself.

i.e. $aRa \ \forall \ a \in A$

or a relation R in a set A is said to be reflexive if every element of A is related to itself *i.e.* aRa is true for all $a \in A$

or

R is reflexive if $(a, a) \in R \ \forall \ a \in A$.

Example 1: Let A be the set of all triangles (coplanar) and R stand for "equal in area to". Now any triangle $a \in A$ is equal in area to itself, *i.e.* $aRa \ \forall \ a \in R$. Hence R is reflexive.

Example 2: Let A be the set of all lines and R stand for "is parallel to". Now any line $a \in A$ is parallel to itself i.e. $aRa \ \forall \ a \in R$. Hence, R is reflexive.

Example 3: Let A be the set of all members of a family. Let R be defined by "is wife of". Clearly any wife is not "the wife of" itself *i.e.* a is not R-related to a, $\forall \ a \in R$. Hence, R is not reflexive.

Example 4: (a) If $R_1 = \{(a, a), (a, b), (a, c), (b, b), (b, c)\}$ be a relation on $A = \{a, b, c\}$, then R_1 is reflexive relation since for every $a \in A$, $(a, a) \in R_1$.

(*b*) If $R_2 = \{(a, a), (a, b), (a, c), (b, c)\}$ be a relation on $A = \{a, b, c\}$ then R_2 is not a reflexive relation since for $b \in A$, $(b, b) \notin R_2$.

3.5.2 Symmetric

A relation R is called symmetric if the second element is also related with first element in the same manner as the first element is relation with second element of each pair.

R is symmetric if $(a, b) \in R \Rightarrow (b, a) \in R$, $a, b \in A$

or A relation R on a set A is defined as symmetric if $aRb \Rightarrow bRa$, whenever $a, b \in A$

Example 5: Consider a set A of all students studying in a given college. Let R stand for "is a class-mate of" on the set A.

Clearly, if $a, b \in A$ and a "is a class-mate of" b, i.e. if aRb, then definitely b "is a class-mate of" *a i.e.* bRa.

So, $aRb \Rightarrow bRa$.

Hence, Relation R on set A is symmetric.

Example 6: Consider a set A of integers. Let R stand for "is equal to" on set A.

Definitely if $(a, b) \in R$ and $a = b \Rightarrow b = a$.

So, $aRb \Rightarrow bRa$.

So, Relation R on set A is symmetric.

Example 7: Let $R_1 = \{(a, a), (a, b), (a, c), (b, b), (b, a), (c, a)\}$ on $A = \{a, b, c\}$ is a symmetric relation.

Example 8: Let A be the set of lines in a plane. Then the relation "is parallel to" is a symmetric relation.

Let $a, b \in R$ because if $a \,||\, b \Rightarrow b \,||\, a$ on $aRb \Rightarrow bRa$.

Example 9: Let A be the set of lines in a plane. Then the relation "is perpendicular to" is a symmetric relation. Let $a, b \in A$

and of $a \perp b$ definitely $b \perp a$.

$aRb \Rightarrow bRa$.

So, Relation R on set A is symmetric.

3.5.3 Asymmetric Relation

A relation R on a set A is asymmetric if whenever $(a, b) \in R$ then $(b, a) \notin R$ for $a \neq b$ *i.e.* If $aRb \Rightarrow bRa$. It means that the presence of (a, b) in R excludes the possibility of presence of (b, a) in R. For example: The Relation

$R_1 = \{(a, a), (a, b), (b, c), (c, a)\}$ on $A = \{a, b, c\}$ is an asymmetric relation.

3.5.4 Antisymmetric Relation

A relation R on a set A is antisymmetric. If for all. $a, b \in A$ (aRb and bRa) $\Rightarrow a = b$.

Example 10: Let R standing for " $>$ " be defined on the set N of all natural numbers.

Clearly, if $n_1, n_2 \in N$ and of n_1Rn_2, then n_2 not related to n_1.

i.e. $n_1 > n_2$ then $n_2 \not> n_1$.

So Relation R on set N is antisymmetric.

Example 11: Let $R_1 = \{(x, y) \in R^2 \mid x \leq y\}$ is an antisymmetric relation on R since $x \leq y$ and $y \leq x$ is only possible. When $x = y$, then $(x, y) \in R$ and $(y, x) \in R$ implies $x = y$.

Example 12: Let $R = \{(x, y) \in N \mid x$ is a division of $y\}$ is an antisymmetric relation. Since x divides y and y divides x implies $x = y$.

Example 13: Let $R_1 = \{(a, b), (b, b), (b, c)\}$ on $A = \{1, 2, 3\}$ is an antisymmetric relation.

3.5.5 Transitive Relation

A relation R on a set A is called transitive if whenever aRb and bRc then aRc for $a, b, c \in A$.

i.e. aRb and $bRc \Rightarrow aRc$ for $a, b, c \in A$.

Example 14: The relation 'is parallel to' on the set of lines in a plane is transitive, because if a line x is parallel to the line y and if y is parallel to the line z then x is parallel to z.

Example 15: The relation 'is perpendicular to' on the set of lines in a plane is not transitive, because if a line x perpendicular to y and if y is perpendicular to the line z.

3.6 EQUIVALENCE RELATION

A relation R on a set A is called an equivalence relation on A, if it is reflexive, symmetric and transitive.

Existence of equivalence relation is denoted by the symbol $\cong$.

i.e. If $a, b, c \in A$ and if R be an equivalence relation on A then R is an equivalence relation. If

(*i*) $aRa, \forall a \in A$ (Reflexive)

(*ii*) $aRb \Rightarrow bRa$, where $a, b \in A$ (Symmetry)

(*iii*) $aRb, bRc \Rightarrow aRc$ (Transitivity)

Since a relation R is also regarded as a subset of $A \times A$, alternative conditions in that order are as follows:

(*i*) $(a, a) \in R, \forall a \in A$

(*ii*) $(a, b), (b, a) \in R$ or $(a, b) \in R \Rightarrow (b, a) \in R$

(*iii*) $(a, b), (b, c), (c, a) \in R$ or $(a, b), (b, c) \in R \Rightarrow (a, c) \in R$

Smallest Equivalence Relation

An equivalence relation R on a set A is called the smallest equivalence relation. If R is smallest subset of $A \times A$.

Clearly $A \times A$ contains n^2 elements, n elements are provided by reflexivity property in R. If no elements are provided in the set R by symmetric and transitive properties, then this is the smallest set.

Now 'is equal to' is an equivalence relation. For this R, reflexivity, symmetry and transitivity produce the same ordered pairs (a, a) $\forall a \in A$. Hence, it yields the minimum number of ordered pairs.

Largest Equivalence Relation

Since R on A is a subset of A × A, the largest subset of A × A is A × A itself. Hence A × A is the largest equivalence relation on A.

Theorem: Prove that 'congruence modulo m' is an equivalence relation on the set of all integers.

Proof: Let I be the set of all integers and let R defined on I stand for "congruence modulo m".

Thus aRb stands for

$$a \equiv b \pmod{m}, \quad a, b \in \mathrm{I} \text{ i.e. } m \mid (a - b)$$

(*i*) *Reflexivity*: Let $a \in \mathrm{I}$

$\because$ $a - a = 0$ and 0 is divisible by m,

$a \equiv a \pmod{m}$, $\forall\, a \in \mathrm{I}$

Hence, R is reflexive.

(*ii*) *Symmetric*: Let $a, b \in \mathrm{I}$

$$\therefore \quad a\,\mathrm{R}b \Rightarrow a \equiv b \pmod{m}$$
$$\Rightarrow m \mid (a - b)$$
$$\Rightarrow m \mid (b - a) \text{ because } a - b = -(b - a)$$
$$\Rightarrow b \equiv a \pmod{m}$$
$$\Rightarrow b\mathrm{R}a$$

Hence, R is symmetric.

(*iii*) *Transitivity*: Let $a, b, c \in \mathrm{I}$. Also let aRb and bRc

$$a\mathrm{R}b \Rightarrow m \mid (a - b) \text{ and } b\mathrm{R}c \Rightarrow m \mid (b - c)$$
$$a\mathrm{R}b, b\mathrm{R}c \Rightarrow m \mid (a - b), m \mid (b - c)$$
$$\Rightarrow m \mid [(a - b) + (b - c)]$$
$$\Rightarrow m \mid (a - c)$$
$$\Rightarrow a\mathrm{R}c$$

i.e., $a \equiv b \pmod{m}$ $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

Hence, R is transitive.

Example 16: Show that "is similar to" on the set T of all coplanar triangles is an equivalence relation.

Solution: Let R stands for "is similar to".

(*i*) *Reflexivity*: Let $t \in \mathrm{T}$. Hence, tRt, $\forall\, t \in \mathrm{T}$

$\therefore$ Every triangle t is similar to itself.

Thus R is reflexive.

(*ii*) *Symmetry*: Let $t_1, t_2 \in T$, then $t_1 R t_2 \Rightarrow t_2 R t_1$ for

If triangle t_1 is similar to t_2 then triangle t_2 is also similar to t_1.

Hence, R is symmetric.

(*iii*) *Transitivity*: Let $t_1, t_2, t_3 \in T$, now if t_1 'is similar to' to t_2 and t_2 'is similar to' t_3 then we have t_1 'is similar to' t_3.

Hence, R is transitive.

Since R is reflexive, symmetric and transitive, hence R is an equivalence relation.

Example 17: If R and R′ be equivalence relations on a set A, prove that $R \cap R'$ is an equivalence relation on A.

Solution: Let R and R′ are defined on A.

$\therefore$ $R \subset A \quad A$ and $R' \subset A \quad A$

Hence, $R \cap R' \subset A \quad A$

Now let $a, b, c \in A$

(*i*) *Reflexivity*: Since R and R′ are equivalence relations,

$\therefore$ $aRa, aR'a \; \forall \; a \in A$

$\therefore$ $(a, a) \in R$ and $(a, a) \in R', \forall \; a \in A$

Hence, $(a, a) \in R \cap R', \forall \; a \in A$

$\therefore$ $R \cap R'$ is reflexive on A.

(*ii*) *Symmetry*: Let $(a, b) \in R \cap R'$ when $a, b \in A$

$(a, b) \in R \cap R' \Rightarrow (a, b) \in R$ and $(a, b) \in R'$

$\Rightarrow (b, a) \in R$ and $(b, a) \in R'$, ($\because$ R and R′ are symmetric)

$\Rightarrow (b, a) \in R \cap R'$

$\therefore$ $R \cap R'$ is symmetric.

(*iii*) *Transitivity*: Let $(a, b), (b, c) \in R \cap R'$

$\therefore$ $(a, b), (b, c) \in R \cap R' \Rightarrow (a, b), (b, c) \in R$ and $(a, b), (b, c) \in R'$

$\Rightarrow (a, c) \in R$ and $(a, c) \in R'$

$\because$ R, R′ are transitive.

$\Rightarrow (a, c) \in R \cap R'$

(*ii*) *Symmetry*: Let $t_1, t_2 \in T$, then $t_1 R t_2 \Rightarrow t_2 R t_1$ for

If triangle t_1 is similar to t_2 then triangle t_2 is also similar to t_1.

Hence, R is symmetric.

(*iii*) *Transitivity*: Let $t_1, t_2, t_3 \in T$, now if t_1 'is similar to' to t_2 and t_2 'is similar to' t_3 then we have t_1 'is similar to' t_3.

Hence, R is transitive.

Since R is reflexive, symmetric and transitive, hence R is an equivalence relation.

Example 17: If R and R′ be equivalence relations on a set A, prove that $R \cap R'$ is an equivalence relation on A.

Solution: Let R and R′ are defined on A.

$\therefore$ $R \subset A \quad A$ and $R' \subset A \quad A$

Hence, $R \cap R' \subset A \quad A$

Now let $a, b, c \in A$

(*i*) *Reflexivity*: Since R and R′ are equivalence relations,

$\therefore$ $aRa, aR'a \; \forall \; a \in A$

$\therefore$ $(a, a) \in R$ and $(a, a) \in R', \forall \; a \in A$

Hence, $(a, a) \in R \cap R', \forall \; a \in A$

$\therefore$ $R \cap R'$ is reflexive on A.

(*ii*) *Symmetry*: Let $(a, b) \in R \cap R'$ when $a, b \in A$

$(a, b) \in R \cap R' \Rightarrow (a, b) \in R$ and $(a, b) \in R'$

$\Rightarrow (b, a) \in R$ and $(b, a) \in R'$, ($\because$ R and R′ are symmetric)

$\Rightarrow (b, a) \in R \cap R'$

$\therefore$ $R \cap R'$ is symmetric.

(*iii*) *Transitivity*: Let $(a, b), (b, c) \in R \cap R'$

$\therefore$ $(a, b), (b, c) \in R \cap R' \Rightarrow (a, b), (b, c) \in R$ and $(a, b), (b, c) \in R'$

$\Rightarrow (a, c) \in R$ and $(a, c) \in R'$

$\because$ R, R′ are transitive.

$\Rightarrow (a, c) \in R \cap R'$

$x \in [a] \Rightarrow xRa, \ \forall x \in [a]$

Also $b \in [a]$ $\Rightarrow bRa$

$\Rightarrow aRb$, for R is symmetric

$\Rightarrow a \in [b]$

but xRa and aRb $\Rightarrow xRb$ by transitivity of R

$\Rightarrow x \in [b], \ \forall x \in [a]$

$\therefore [a] \subseteq [b]$

Hence, $[a] = [b]$

(*iii*) Since $[a] \cap [b] \neq \phi$, let $[a] \cap [b] = [l, m, n]$

Clearly $l \in [a]$ and $l \in [b]$. Since $l \in [a]$, we have $[l] = [a]$ we have $[l] = [a]$ by (ii) property.

Similarly $[l] = [b]$

Hence from transitivity of relation "=" we have $[a] = [b]$.

Check Your Progress

Fill in the blanks:

1. The inverse of a relation R is the set of all reversed pairs of R and is denoted by..... .
2. A relation R is called .....if the second element is also related with first element in the same manner as the first element is relation with second element of each pair.

3.8 LET US SUM UP

A relation between two sets A and B is a subset of A × B. If A = B, then we say that R is a relation on A. We can write aRb iff $(a, b) \in R$ and say that a is R-related to b or that b is a R-relation of a.

The set of all first elements a for which there is a. Corresponding b given by $(a, b) \in R$ and $a, b \in A$ is called the Domain of R.

The set of all b's to which there is some corresponding a such that $(a, b) \in R$ and $a, b \in A$ is called the range or image of R.

The inverse of a relation R is the set of all reversed pairs of R and is denoted by R^{-1}.

A relation R in a set A is said to be a void relation. If $R = \phi$.

A relation R in a set A is said to be universal relation, if R coincide with A × A.

3.9 KEYWORDS

Identity Relation: A relation R in a set A is said to be identity relation denoted by I_A if $I_A = \{(a, b): \text{and } a = b\}$

Void Relation: A relation R in a set A is said to be a void relation. If $R = \phi$.

Universal Relation: A relation R in a set A is said to be universal relation, if R coincide with A × A.

Symmetric: A relation R is called symmetric if the second element is also related with first element in the same manner as the first element is relation with second element of each pair.

3.10 QUESTIONS FOR DISCUSSION

1. Prove that the relation "=" on the set of all real numbers is an equivalence relation.
2. Let L be the set of all straight lines of the Eulerian plane, verify whether parallelism between two straight lines is an equivalence relation on L.
3. Let n be a fixed positive integer. Define a relation R on the set of all integers I as follows:

   aRb iff $n/(a-b)$ that is $(a-b)$ is divisible by n. Show that R is an equivalence relation on I.
4. m is said to be related to n if m and n are integers and $m-n$ is divisible by 13. Does this defines an equivalence relation?
5. A relation R on I (the set of integers) is defined as
   (a) R =
   (b) Show that R is an equivalence relation on I.
6. Let I be the set of integers. Let a relation aRb be defined if $a-b$ is an even integer. Show that R is an equivalence relation.
7. N is the set of natural numbers. The relation R is defined on N × N as follows:
   (a) (a, b) R (c, d) $a + d = b + c$
   (b) Prove that R is an equivalence relation.
8. N is the set of positive integers and ~ be a relation on N × N defined by
   (a) $(a, b) \sim (c, a)$ iff $ad = bc$
   (b) Check the relation for being an equivalence relation.
9. A relation R on the set of complex numbers is defined by $z_1 R z_2$ if and only if $(z_1 - z_2)/(z_1 + z_2)$ is real. Show that R is an equivalence relation.
10. Which of the following are equivalence relations?
    (a) "Is the square of" for the set of natural numbers?
    (b) "Has the same radius as" for the set of all circles in a plane?
    (c) "" for the set of sets {A, B, C, ...}.
    (d) The set of real numbers : xRy, if $x = \pm y$.
    (e) The set of straight lines in the plane in which xRy if x is perpendicular to y.
    (f) The set of straight line in the plane in which xRy if x is parallel to y.
    (g) "" for the set of real numbers.
    (h) on which (a, b) R (c, d) $b - d = a - c$.
    (i) 'a is less than or equal to b if there exist a non-negative c such that $a + c = b$' on the set R.
11. If R stands for "is at the same distance from the origin as" and is a relation on the set of all coplanar points, prove that R is an equivalence relation.

12. Show that the relation aRb defined by $|a| = |b|$, in the set of all real numbers, is an equivalence relation. Further show that the relation aRb defined by $|a| \geq |b|$ is an equivalence relation.
13. If R is a relation in the natural numbers N, defined by the open set "$x - y$ is divisible by 5" that is
    (a) R =
    (b) Prove that R is an equivalence relation.
14. Discuss the R-relation "$2x + 3y = 12$" defined on the set N of natural numbers, such that .
15. If are relations on a set A, test the truth of the following:
    (a) If R is an equivalence relation then:

        xRy, xRz yRz,

    (b) If R is reflexive
    (c) If are transitive, then is transitive.
16. Construct examples on the following R-relations.
    (a) R neither symmetric non-transitive but reflexive.
    (b) R neither reflexive non-transitive but symmetric.
    (c) R reflexive and symmetric but not transitive.
    (d) R neither reflexive non-symmetric but transitive.
    (e) R reflexive and transitive but not symmetric.
    (f) R symmetric and transitive but not reflexive.
17. Test the reflexivity, symmetry, transitivity of the following R-relations :
    (a) When R stands for "is twice the are of" and is defined on all coplanar triangles.
    (b) When R on the set N is defined by xRy, if , .
    (c) When R = {(1, 3), (3, 5), (5, 3), (5, 7)} on the set A = {1, 3, 5, 7}.

Check Your Progress: Modal Answers

1. R^{-1}
2. Symmetric

3.11 SUGGESTED READINGS

Anuranjan Misra, *Discrete Mathematics*, Acme Learning pvt ltd.

Richard Johnsonbaugh, *Discrete Mathematics*, Prentice Hall

V. K. Balakrishnan, *Introductory Discrete Mathematics*, Courier Dover Publications,

R. C. Penner, *Discrete Mathematics: Proof Techniques and Mathematical Structures*, World Scientific, 1999

Mike Piff, *Discrete Mathematics: An Introduction for Software Engineers*, Cambridge University Press, 1991

LESSON

4

FUNCTIONS

CONTENTS

4.0 AIMS AND OBJECTIVES

After studying this lesson, you will be able to:

- Understand concept of functions
- Discuss types of functions and classification of functions
- Discuss examplrs on functions

4.1 INTRODUCTION

Let X and Y be two given sets. If y be any given rule or operation there corresponds to each element x $\in$ X, a unique element y $\in$ Y, then this correspondence denoted by f, is called mapping of X into Y or f is called function of X to Y.

4.2 CORRESPONDENCE

Let us consider the set A = $\{a_1, a_2, a_3 \ldots\ldots a_{n3}\}$ of all authors who have written the books which from the set B = $\{b_1, b_2, b_3 \ldots\ldots b_n\}$. Let us concern ourselves here, with the natural association of each book of the set B with authors of Set A.

This process of associating an element of B with an element of A may result in associating b_1 with a_2, b_2 with a_3, b_5 with a_2, b_7 with a_1, ..., b_3 with a_5. This association of the elementary one set B with the elements of another set A, is called correspondence.

4.3 TYPES OF CORRESPONDENCE

4.3.1 One to One Correspondence

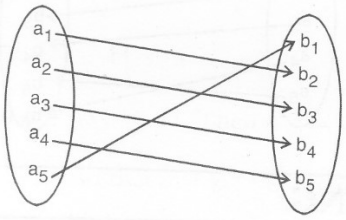
If each element of A corresponds to one and only one element of another set B, and each element of B corresponds to one and only one element of A, we say there is one to one correspondence between the elements of A and the elements of B.

Let, A = $\{a_1, a_2, a_3, a_4, a_5\}$

B = $\{b_1, b_2, b_3, b_4, b_5\}$

Let,

$a_1 \to b_2$, $a_2 \to b_3$, $a_3 \to b_4$, $a_4 \to b_5$, $a_5 \to b_1$ or graphically we can show:



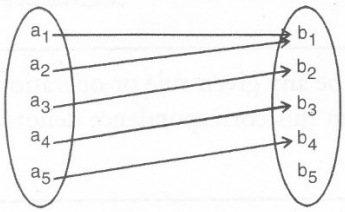
So there is a one to one correspondence between elements of set A and elements of set B.

4.3.2 Many to One Correspondence

If at least two elements of set A correspond to only one element of set, then there is many to one correspond between set A and set B.

We can see it graphically as:

Let, A = $\{a_1, a_2, a_3, a_4, a_5\}$ and B = $\{b_1, b_2, b_3, b_4, b_5\}$

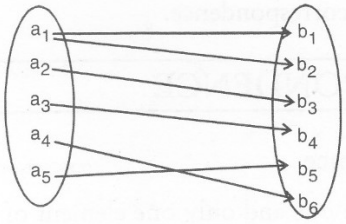


4.3.3 One to Many Correspondence

If some elements of A correspond to more than one element of another set B, then this type of correspondence is called one to many correspondence.

Let, A = $\{a_1, a_2, a_3, a_4, a_5\}$ B = $\{b_1, b_2, b_3, b_4, b_5\}$

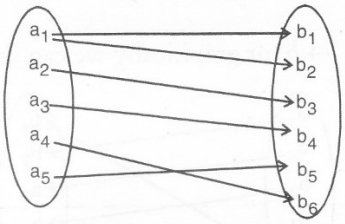
Figure below shows one to many correspondence:



4.3.4 Many to Many Correspondence

If one or more elements of A corresponds to one or more elements of B, then this type of correspondence is called many to many correspondence.

Figure below show many to many correspondence:



4.4 FUNCTIONS MAPPING

Let X and Y be two given sets. If y be any given rule or operation there corresponds to each element $x \in X$, a unique element $y \in Y$, then this correspondence denoted by f, is called mapping of X into Y or f is called function of X to Y.

f-image: The element $y \in Y$, which due to mapping f, corresponds to an element $x \in X$ is denoted by the symbol f(x), i.e. y = f(x).

f(x) is called the f-image of x or the value of the function for x.

f-set: The set of all f-images of the element of X, is called image set and is denoted by f (X) or {f(x)}.

The statement "the mapping f of X to Y is denoted by $f : X \rightarrow Y$.

4.4.1 Types of Mapping (Functions)

There are two types of mapping:

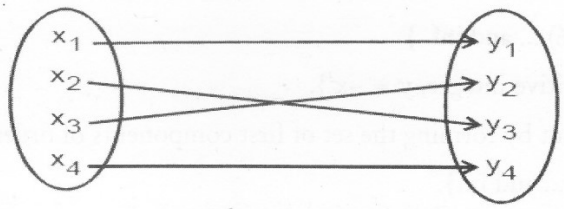
Onto or Surjective Mapping: In this mapping, every element of Y is an f-image of some of $x \in X$, i.e., there is no element in Y which has no correspondence with any element of X such a correspondence is called the mapping of X onto Y.

Hence, the mapping f: $X \to Y$ is said to be onto mapping if,

$$\text{f-set } \{f(x)\} = Y, \forall\ x \in x$$

Let $X = \{x_1, x_2, x_3, x_4\}$; $Y = \{y_1, y_2, y_3, y_4\}$

Then figure shows onto mapping



Into or Injective Mapping: In this mapping at least one element Y is not anf-Image of any $x \in X$. Such a correspondence is called mapping of X into Y.

Hence, the mapping f: $X \to Y$ is called mapping of X into Y if $\{f(x)\} \subset y$, $\forall\ x \in X$.

Let, $X = \{x_1, x_2, x_3, x_4, x_5\}$ $Y = \{y_1, y_2, y_3, y_4, y_5, y_6, y_7\}$

Equivalent sets: Two sets whose element can be placed in one to one correspondence are called equivalent set or cardinally equivalent sets.

Countable or denumerable sets: If one to one correspondence exists between a set A and the set N of all natural numbers the set A is called countable or denumerable set.

Domain and Co-domain: In any mapping f: $X \to Y$, the set X is called the domain and Y is called the co-domain of mapping f.

Range of mapping: The f-set is called the range of f.

4.4.2 Classification of Function

Constant mapping or constant function: The function f or mapping f defined on a set x, such that $f(x) = a$ $\forall\ x \in X$ is called a constant function on X.

i.e. every element of X is mapped onto the same single element 'a' of another given set.

Identity mapping: If every element of a set X is mapped onto itself then the mapping is called identity mapping i.e. x: $X \to X$ is defined by $f(x) = x$, $\forall\ x \in X$.

Transformation: A mapping f: $x \to x$, i.e. mapping of a set into is called a transformation, i.e. mapping f is called transformation if domain of f - co-domain of f.

Inclusion mapping: A mapping $f : X \to Y$; defined by $f(x) = x$; if $X \subseteq Y$ is called Inclusion map of X to Y.

4.5 SOLVED FUNCTIONS

Example 1: For a mapping $f : X \to Y$; defined by $f(x) = x - 2$, $\forall\ x \in X$, find f-image of $x = 0, 3, 5, -1, -2 \in X$.

Solution: By putting $x = 0, 3, 5, -1, 2$ in $f(x) = x - 2$ we get

$f(0) = 0 - 2 = -2$; $f(3) = 3 - 2 = 1$; $f(5) = 5 - 2 = 3$; $f(-1) = -1 - 2 = -3$

$f(-2) = -2 - 2 = -4$

Hence, Images are $-2, 1, 3, -3 - 4$, respectively.

Example 2: For each mapping defined by the following set of ordered pairs, find out domain and the range.

(i) {(1, 1), (2, 4) (3, 9) (4, 16) ... and inf. }

(ii) $f = \{(x, y) : x$ is the positive integer, $y = -x^2\}$.

Solution: Domain is found out by forming the set of first components of ordered pairs.

Hence domain = {1, 2, 3, 4 ... and inf}.

Range is find out by forming the set of 2^{nd} component of ordered pairs.

$\therefore$ Range = {1, 4, 9, 16 ...}.

(ii) Hence x is first component of ordered pairs and each x is positive integer. Hence domain is the set of all positive integers.

$\therefore$ Domain = {1, 2, 3, 4, ... and inf.}

By putting $x = 1, 2, 3...$ in $y = -x^2$ we get $y = -1, -4, -9, ...$

These are second component of orders pairs.

Hence, range = {- 1, - 4, - 9, ... an inf}.

Example 3: Given A = {2, 3, 4}, B = {2, 5, 6, 7} construct an example of each of the following.

(i) An injective mapping from A to B.

(ii) A mapping from A to B which is not injective

(iii) A mapping from B to A.

Solution: (i) An injective (i.e. one-one) mapping A to B may be defined as:

$f = \{(2,5), (3,7), (4,6)\}$.

(ii) A mapping from A to B which is not injective may be defined as:

$g = \{(2, 2), (3, 5), (4, 2)\}$

(iii) A mapping from B to A may be defined as:

$h = \{(2, 2), (5, 3), (6\ 4), (7, 4)\}$

Example 4: If X = {1, 2, 3, 4, 5} and Y = {1, 3, 5, 7, 9} Find $X \cap Y$ and $(X - Y) \cup (Y - X)$. Determine which of the following sets are (i) mappings (ii) relations (iii) neither; of X to Y.

(i) $F = \{\{x, y\} : y = x + 2, x \in X, y \in Y\}$

(ii) $F = \{(1, 1)\} (2, 1), (3, 3) (4, 3) (5, 5)\}$

(iii) $F = \{(1, 1)\} (1, 3), (3, 5) (3, 7) (5, 7)\}$

(iv) $F = \{(1, 3)\} (2, 5), (4, 7) (5, 9) (3, 1)\}$

Solution: $X \cap Y = \{1, 3, 5\}$

$(X - Y) \cup (Y - X) = \{2, 4\} \cup (7, 9) = \{2, 4, 7, 9\}$

(i) We rewrite F as follows:

$\therefore$ $1 \in x$ and $y = x + 2 = 1 + 2 = 3 \in Y$

$\therefore$ $(1, 3) \in F$

$\therefore$ $2 \in X$ but $y = 2 + 2 = 4 \notin Y$, we have $(2, 4) \notin F$

$\therefore$ $3 \in X$ and $y = 3 + 2 = 5 \in Y$, we have $(3, 5) \in F$

$\therefore$ $4 \in X$ and $y = 4 + 2 = 6 \notin$ we have $(4, 5) \notin F$.

Finally since $5 \in X$ and $y = 5 + 2 = 7 \in X$, we have $(5, 7) \in F$.

Hence, $F = \{1, 3\}, (3,5), (5, 7)\}$.

Hence, F is a relation from X to X, since $F \subset X * Y$ but it is not a mapping since the elements 2 and 4 of the domain X have no image in Y under F.

(ii) Hence, F is a mapping from X to Y since each element of X has a unique image in Y under F. So F is a relation from X to Y.

Hence, F is a many one into mapping.

(iii) Here, F is a relation from X to Y. Since $F \subset X. Y$ but F is not a mapping since the element $1 \in X$ has two images 1 and 3 in X so that the image is not unique.

Example 5: Suppose f is the collection of the ordered pairs of real numbers and $x = 6$ is the first element of some ordered pair in f. Suppose the vertical line through $x = 6$ intersects the graph of f twice. Is f a function? Why or why not?

Solution: f is not a function. The graph of the function f consists of points represented by the ordered pairs of the form (x, f(x)).

If the vertical line through $x = 6$ is cut by the graph of f twice, then it means that the element 6 of the domain of f has two images. Hence f is not a function as for t to be a function each element of the domain must have unique image.

Example 6: Given $A = \{x: \pi/6 \leq x \leq \pi/3\}$ and $f(x = \cos x - x (1 + x)$; find $f(A)$

Solution: We know that as x increases from 0 to $\pi/2$, cos x decreases from 1 to 0. Therefore,

$\pi/6 \leq x \leq \pi/3 \Rightarrow \cos(\pi/6) \geq \cos x \geq \cos(\pi/3)$

$\Rightarrow$ $1/2 \leq \cos x \leq \sqrt{3}/2$ ...(1)

Again since $\pi/6 \leq x < \pi/3$ ...(2)

$\therefore \quad 1 + \pi/6 \leq 1 + x \leq 1 + \pi/3$ ... (3)

Multiplying (2) and (3) we get ....

$\pi/6 * (1 + \pi/6) \leq x (1 + x) \leq \pi/3 (1 + \pi/3)$

or $-\pi/6 (1+\pi/6) \geq -x (1 +x) \geq -\pi/3 (1+\pi/3)$

or $-\pi/3 (1 + \pi/3) \leq -x (1+x) \leq -\pi/6 (1+\pi/6)$ ... (4)

By Adding (1) and (4), we get

$1/2 - \pi/3 (1+\pi/3) \leq \cos x - (1 + x) \leq \sqrt{3}/2 - \pi/6 (1 + \pi/6)$

i.e. $1/2 - \pi/3 (1+\pi/3) \leq f(x) \leq \sqrt{3}/2 - \pi/6 (1 + \pi/6)$

Hence,

$$f(A) = \{y : 1/2 - \pi/3 (1 + \pi/3) \leq y \leq \sqrt{3}/2 - \pi/6 (1+\pi/6)\}$$

Example 7: Let A and B be two sets each with a finite number of elements. Assume that there is injective mapping form A to B and that there is an injective mapping from B to A. Prove that there is a bijective mapping from A to B.

Solution: Let f be an injective mapping from A to B. Since f is one-one; number of elements in A is less than or equal to the number of elements in B, that is $n(A) \leq n(B)$. Similarly sine there exists in injective mapping.

$g: B \rightarrow A$, we have $n(B) \leq n(A)$

Hence, $n(A) = n(B)$

Since the number of elements in A and B is the same, we can define a bijective mapping from A to B.

For if $A = \{a_1, a_2 .... a_n\}$

and, $B = \{b_1, b_2 ... b_n\}$

Then one such bijective mapping is–

$$h = \{(a_1, b_1), (a_2, b_2) .... (a_n, b_n)\}$$

In fact, we can define many such bijective mapping from A to B.

Check Your Progress

1. Let f be a one-one function with domain (x, y, z) and range {1, 2, 3). It is given that exactly one of the following statement is true and the remaining two are false. $f(x) = 1$, $f(g) \neq 1$, $f(z) \neq 2$. Determine $f^{-1}(1)$.
2. Is $g = \{(1, 1) (2, 3), (3, 5) (4, 7)$ a function? If this is described by the formula $2(x) = \alpha x + \beta$, then what should be assigned to α and β?

4.6 LET US SUM UP

If each element of A corresponds to one and only one element of another set B, and each element of B corresponds to one and only one element of A, we say there is one to one correspondence.

If at least two elements of set A correspond to only one element of set, then there is many to one correspond between set A and set B.

If some elements of A correspond to more than one element of another set B, then this type of correspondence is called one to many correspondence.

If one or more elements of A corresponds to one or more elements of B, then this type of correspondence is called many to many correspondence.

The function f or mapping f defined on a set x, such that $f(x) = a \ \forall \ x \in X$ is called a constant function on X.

If every element of a set X is mapped onto itself then the mapping is called identity mapping.

A mapping f: $x \rightarrow x$, i.e. mapping of a set into is called a transformation.

4.7 KEYWORDS

Correspondence: This association of the elementary one set B with the elements of another set A, is called correspondence.

Mapping: Let X and Y be two given sets. If y be any given rule or operation there corresponds to each element $x \in X$, a unique element $y \in Y$, then this correspondence denoted by f, is called mapping of X into Y

Surjective Mapping: In this mapping, every element of Y is an f-image of some of $x \in X$

Injective Mapping: In this mapping at least one element Y is not anf-Image of any $x \in X$.

Equivalent Sets: Two sets whose element can be placed in one to one correspondence are called equivalent set

Denumerable Sets: If one to one correspondence exists between a set A and the set N of all natural numbers the set A is called countable or denumerable set.

Domain and Co-domain: In any mapping f: $X \rightarrow Y$, the set X is called the domain and Y is called the co-domain of mapping f.

4.8 QUESTIONS FOR DISCUSSION

1. What is correspondence? What are different types of correspondence?
2. What is function mapping? Discuss different types of mapping.
3. Discuss classification of functions.

Check Your Progress: Modal Answers

1. There are three possibilities:
   (a) The statement $f(a) = 1$ is true the statement $f(y) \neq 1$, $f(z) \neq 2$ are both false.
   (b) The statement $f(y) \neq 1$ is true and the statement $f(x) = 1$, $f(z) \neq 2$ are false.

Contd...

(c) The statement $f(z) \neq 1, f(y) \neq 1$ are false.

In case (a), the true statement are:

$$f(x) = 1, f(y) = 1, f(z) = 2.$$

If then, f is not a one-one mapping which is a contradiction so this possibility is true out.

In case (b) the true statement must be:

$$f(x) = 2 \text{ or } 3, f(y) = 2 \text{ or } 3, f(z) = 2.$$

So, in the case also f cannot be a one-one mapping since in this case two elements x,y,z must have the same image.

In case (c), the true statement are:

$$f(x) \ 2 \text{ or } 3, f(y) = 1, f(z) = 1 \text{ or } 3$$

Hence, $f^{-1}(1) = \{y\}$

2. Here g is a function since the image of every element of the domain {1, 2, 3, 4} is unique. If x is any element of the domain, then clearly its image is, given by $g(x) = 2x - 1$.

Hence, $\alpha = 2$ and $\beta = -1$

4.9 SUGGESTED READINGS

Anuranjan Misra, *Discrete Mathematics*, Acme Learning pvt ltd.

Richard Johnsonbaugh, *Discrete Mathematics*, Prentice Hall

V. K. Balakrishnan, *Introductory Discrete Mathematics*, Courier Dover Publications,

R. C. Penner, *Discrete Mathematics: Proof Techniques and Mathematical Structures*, World Scientific, 1999

Mike Piff, *Discrete Mathematics: An Introduction for Software* Engineers, Cambridge University Press, 1991

UNIT III

LESSON

5

ALGEBRAIC STRUCTURES

CONTENTS

5.0 AIMS AND OBJECTIVES

After studying this lesson, you will be able to:

- Understand the concept of groups and subgroups with examples
- Discuss semigroups and monoids
- Understand the concept of homomorphisms
- Discuss permutation groups and normal subgroups
- Discuss cosets and lagrange's theorm
- Understand the algebraic manipulation
- Discuss ring and its types

5.1 INTRODUCTION

A non-empty set together with one or more binary operations defined on the set is called a Algebraic Structure or Mathematical Structure. Arithmetic operations combine two elements of the set of real numbers to give another element of the same set. Such operations are called 'binary operations.

5.2 BINARY OPERATION

We are aware with arithmetic operations like addition, subtraction, multiplication and division. Wherein these operations on any two real numbers yield another real number.

Arithmetic operations combine two elements of the set of real numbers to give another element of the same set. Such operations are called 'binary operations or binary compositions'.

Let $x, y \in R$ then $x + y \in R$, $x - y \in R$, $x * y \in R$, and $\frac{x}{y} \in R$. So a binary operation is a rule, defined on a given set S, which assigns to any elements a unique third element in S. It is denoted by the symbol '$\circ$'.

'$\circ$' assigns to any two elements $a, b \in S$, a unique third element $a \circ b \in S$.

An operation '$\circ$' on a non-empty set S which is a mapping that associates with each ordered pair (a, b). When $a, b \in S$, a uniquely defined element $a \circ b$ of S, is called a binary operation.

In other words, a binary operation '$\circ$' on a set S, is a mapping of $S \times S$ into S.

Example 1: Let the operation '$\circ$' be ordinary addition '+' defined on the set N. Let $a, b \in N$. Hence $a \circ b = a + b =$ + ve (integer)

i.e. $(a+b) \in N$. Hence '+' is a binary operation.

Example 2: Consider a set S of all odd integers, on which the operation. '+' is defined. Clearly if $a, b \in S$, then $a + b$ is an even number. Thus $(a+b) \notin S$. Hence '+' on S is not a binary operation.

Example 3: Let '$\circ$' stand for ordinary division '$\div$' defined on the set S of all non-zero integers. Let $a, b \in S$.

Clearly $a \circ b = a \div b$. But $a \div b$ may not be an integer. Hence $a \div b$ may not belong to S. Hence '$\div$' on S is not a binary operation.

5.3 TYPES OF BINARY OPERATIONS

Commutative

If binary operation '$\circ$' on a set S is such that $a \circ b = b \circ a, \ \forall a, b \in S$, then operation '$\circ$' is called Commutative.

Example 4: Let R be the set of all real numbers and '$\circ$' stand for ordinary '+'. If $a, b \in R$ then

$$a + b = b + a, \ \forall a, b \in R.$$

Hence '+' on R is commutative.

But if $\circ$ stands for $\div$ than $a \circ b = a \div b$ and $b \circ a = b \div a$ definitely $a/b \neq b/a$ except when $a = \pm b$.

Hence '$\div$' on R is not a commutative operation.

Associative

An operation '$\circ$' on a set S is said to be associative if, $\forall a, b, c \in S, \ a \circ (b \circ c) = (a \circ b) \circ c$.

Example 5: Ordinary '+' and '$\cdot$' defined on the set of all real numbers or complex numbers or all integers on all rational numbers are associative, *i.e.*

$$a + (b + c) = (a + b) + c \qquad \forall a, b, c \in S$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad \forall a, b, c \in S$$

But 'subtraction' and 'division' are not associative on the sets mentioned above, *e.g.*

$a - (b - c) = a - b + c$, while $(a - b) - c = a - b - c$

$a - (b - c) \neq (a - b) - c$

Example 6: Let binary operation '$\circ$' on the set R of all real numbers be taken by $a \circ b = a + 3b, \ \forall a, b \in R$.

Now let $a, b, c \in R$

$\therefore \quad a \circ (b \circ c) = a \circ (b + 3c) = a + 3(b + 3c) = a + 3b + 9c.$

and $\quad (a \circ b) \circ c = (a + 3b) \circ c = (a + 3b) + 3c = a + 3b + 3c$

Hence, $\quad a \circ (b \circ c) \neq (a \circ b) \circ c$

Hence, '$\circ$' on R is not associative.

Distributive

Let '$\circ$' and $\oplus$ be two binary operations defined on a given set S. Let $a, b, c \in S$.

If $a \circ (b \oplus c) = (a \circ b) \oplus (a \circ c)$

Operation '$\circ$' is said to be left distribution with respect to $\oplus$.

If $(b \oplus c) \circ a = (b \circ a) \oplus (c \circ a)$, then '$\circ$' is said to be right distributive with respect to '$\oplus$'.

If an operation is left as well as right distributive we simply say it is distributive.

Example 7: Let I be the set of all integers. If $x, y, z \in I$ then let $x \circ y = x + 2y$ and $x \oplus y = 2xy$.

Clearly $x \circ (y \oplus z) = x \circ (2yz) = x + 2(yz) = x + 2yz;$

$x \circ y = x + 2y; = x + 2z$

$(x \circ y) \oplus (x \circ z) = (x + 2y) \oplus (x + 2z)$

$= 2(x + 2y)(x + 2z)$

$x \circ (y \oplus z) \neq (x \circ y) \oplus (x \circ z)$

Hence '$\circ$' is not left distributive with respect to

Again $(y \oplus z) \circ x = 2yz \circ x = 2yz + 2x$

Now $(y \circ x) \oplus (z \circ x) = 2(y + 2x)(z + 2x)$

Clearly $(y \circ x) \oplus (z \circ x) \neq (y \circ x) \oplus (z \circ x)$

Hence '$\circ$' is not right distributive with respect to $\oplus$.

But $x \oplus (y \circ z) = x \oplus (y + 2z) = 2x(y + 2z) = 2xy + 4xz$

$= (x \oplus y) \circ (x \oplus z).$

Hence $\oplus$ is left distributive with respect to $\circ$.

Also $(y \circ z) \oplus x = (y + 2z) \oplus x = 2(y + 2z)x$

$= 2yx + 4zx = (y \oplus x) \circ (z \oplus x).$

Hence $\oplus$ is also right distributive over $\circ$.

Identity of the operation: Let '$\circ$' be the operation defined. On a set A. If there exists the element $e \in A$, such that

$$e \circ a = a, \ \forall \ a \in A$$

then e is called left identity with respect to operation '$\circ$'.

But if $e \circ a = a, \ \forall \ a \in A$

then e is called right identity w.r.t operation '$\circ$'.

Increase with respect to the operation: Let '$\circ$' be the operation defined on the set A. If there exists an element $b \in A$ corresponding to $a \in A$. Such that

$$b \circ a = e$$

then b is left inverse of a in A with respect to operation '$\circ$'.

Similarly, if $a \circ b = e$, then b is called right inverse of a with respect to operation '$\circ$' in A.

Inverse of a is denoted by the symbol a^{-1}.

5.4 ALGEBRAIC STRUCTURE

A non-empty set together with one or more binary operations defined on the set is called a Algebraic Structure or Mathematical Structure.

Or we can say an algebraic structure is a set together with closed operation defined over the set.

It G is a non-empty set and '$\circ$' is a binary operation on it then Algebraic structure formed by them is denoted by $(G, \circ)$.

Isomorphic

A homomorphic which is injective (one-to-one) is called a monomorphism, a homomorphism which is surjective (on to) is called an epimorphism and when the homomorphism is a bijection then it is called an isomorphism. If there exists an isomorphism between two structures then they are said to be isomorphic.

The word isomorphic means 'same shape' and so it seems reasonable to expect that isomorphisms should be able to partition the set of all algebraic structure into equivalence classes.

Example 8: The two structures $(\{\phi, S\}, \cap, \cup)$ and $(\{0,1\}, \wedge, \vee)$ (as defined in the below given table) are Isomorphic.

$\vee$	0	1	2	3	4
0	0	1	2	3	4
1	1	1	2	3	4
2	2	2	2	3	4
3	3	3	3	3	4
4	4	4	4	4	4

$\wedge$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	1	1	1
2	0	1	2	2	2
3	0	1	2	3	3
4	0	1	2	3	4

$a \vee b$ = the maximum of a and b.

$a \wedge b$ = the minimum of a and b.

Solution: Let $\phi(\phi) = 0$ and $\phi(S) = 1$. Clearly ϕ is a bijection. Also $\phi(\phi \cap \phi) = \phi(\phi) = 0 = 0 \wedge 0 = \phi(\phi) \wedge \phi(\phi)$.

Group

Consider a mathematical system consisting of a non-empty set S and an operation $*$ defined on set S. The system is a group under the following group axioms:

(G_1) Closure axiom: G is closed under the binary operation $*$.

Thus if $a, b \in G$, we have

$$a * b \in G, \ \forall\, a, b \in G;$$

i.e., $a * b$ is an element of G. This means '$*$' is a binary operation.

(G_2) Associative axiom: The operation '$*$' on G is associative.

Thus if $a, b, c \in G$ we have

$$a * (b * c) = (a * b) * c \ \ \forall\, a, b, c \in G$$

(G_3) Identity axiom: These exists the element $e \in G$ such that:

$$a * e = e * a = a \quad \forall\, a \in G$$

e is called the identity element of G, for the operation '$*$'.

(G_4) Inverse axiom: Every element belonging to G has its inverse.

Thus $\forall\, a \in G$, there exists a^{-1}, such that

$$a * a^{-1} = a^{-1} * a = e,\ a^{-1} \in G$$

5.5 SOME DEFINITIONS

(*i*) ***Finite Group:*** If a group consists of a finite number of elements, it is called a finite group.

(*ii*) ***Infinite Group:*** If a group contains an infinite number of elements, it is called an infinite group.

(*iii*) ***Order of a Group:*** The number of elements in a finite group is called the order of the group.

Let a group consists of m elements, it is called a group of mth order.

(*iv*) ***Abelian Group or Commutative Group:*** It is addition to group axioms, operation is also commutative, it is called Abelian Group or Commutative Group.

Thus for an abelian group with composition '$*$' defined in it, we must have

$$a * b = b * a \quad \forall\, a, b, \in G.$$

or we can say

A mathematical system consisting of a set S and a binary operation $*$ forms a commutative group. If it exhibits the following properties:

- Closure Property
- Associative Property
- Identity Property
- Inverse Property
- Commutative Property

Example 9: Prove that the set of cube roots of unity is abelian finite group with respect to multiplication.

Solution: Let 1, ω, ω^2 be cube roots of unity so that $\omega^3 = 1$. Let us form the composition table for the set $G = \{1, \omega, \omega^2\}$ with respect to multiplication.

$*$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Here $\omega^3 = 1$ and $\omega^4 = \omega^3.\omega = \omega$.

1. Since all elements in the composition table belong to G, hence G is closed under binary operation $*$.
2. Since multiplication of complex number is associative therefore multiplication is associative in G.
3. It is clear from first row of the table that 1 is the identity element in G.
4. Inverse of 1, ω, ω^2 are 1, ω^2, ω respectively and they all belong to G.

Hence G is a multiplication group and it contains. Finite number of elements $\Rightarrow$ hence it is a finite group.

Example 10: The table given below defines a certain binary operation $\oplus$ on the Set A = $\{a, b, c, d, e\}$. Show that the set A forms a group with respect to the binary operation $\oplus$ and find the inverse of each element.

$\oplus$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

Solution:

1. Since all elements in the composition table belong to A. Hence A is closed under binary operation $\oplus$.

   Since $(a \oplus b) \oplus c = b \oplus c = d$

   $a \oplus (b \oplus c) = a \oplus d = d$
2. So $\oplus$ is associative in A.
3. Since

   $a \oplus a = a,\ b \oplus a = a \oplus b = b,\ c \oplus a = a \oplus c = c,$

   $d \oplus a = a \oplus d = d,\ e \oplus a = a \oplus e = e.$

   So, 'a' is the identity element in A.
4. Inverse:

   Here $d \oplus c = a$ (left identity) and $c \oplus d = a$ (Right identity)

   $\Rightarrow c$ is the inverse of d.

   Similarly d is the inverse of c

   and since $e \oplus b = a$ and $b \oplus e = a$ so e is the inverse of b and b is the inverse of e. Inverse of a is a.

   Since (A, $\oplus$) has all four properties of group. Hence the system (A, $\oplus$) forms a group.

Example 11: Does $\{1, -1\}$ forms a group under multiplication.

Solution: First we make the composition table

Let $A = \{1, -1\}$

$*$	1	-1
1	1	-1
-1	-1	1

1. Since all element of the composition table belong to A. So A is closed under the binary operation $*$.
2. Since multiplication of integers is associative, so A is associative under the operation $*$.
3. The identity element for multiplication is 1 which is in the Group A.
4. Since $1*1 = 1$ so inverse of 1 is 1
5. $-1*-1 = 1$ inverse of -1 is -1

Hence, $(A, *)$ has all four properties of a Group.

Hence the system $(A, *)$ forms a Group.

Example 12: Prove that the set of all integers (including zero) with additive, binary operation is an infinite abelian group.

Solution: Let I be the set of all integers and $x, y, z \in I$.

(*i*) ***Closure:*** $x, y \in I \Rightarrow x, y$ are integers.

$\Rightarrow x + y$ is an integer.

$\Rightarrow (x + y) \in I$

Hence the group I is closed under the operation $+$.

(*ii*) ***Associative Property:*** We know that the addition of integers x, y, z is associative.

i.e., if $x, y, z \in I$ then $x + (y + z) = (x + y) + z$.

Hence, addition in I is associative.

(*iii*) ***Existence of Intensity:*** Let $x \in I$, also $0 \in I$.

Here $0 + x = x + 0, \forall x \in I$

Hence, 0 is additive identity in I.

(*iv*) ***Existence of Inverse:*** Here $x \in I \Rightarrow -x \in I$.

But $(-x) + x = 0 \quad \forall x \in I$

Hence, $-x$ is inverse of x, $\forall x \in I$.

Hence inverse of each element in I belongs to I.

It is clear that number of elements in I is infinite.

$\Rightarrow$ I is a infinite group.

(*v*) ***Commutative Property:*** Since addition of integers is commutative.

i.e., $x + y = y + x, \forall x, y \in I.$

Since I contains all five properties of an abelian group under the operation +.

So I is an infinite abelian group.

Example 13: Prove that the set of all non-singular square matrices of order n with real elements is a group with respect to matrix multiplication. Is it an abelian group?

Solution: Set G be the set of all $n \times n$ non-singular matrices over the set of real numbers. Let matrices $A, B, C \in G$.

(*i*) ***Closure:*** Since produce of two square matrices of the same order is a square matrices of the same order.

$\therefore AB \in G, \forall A, B \in G$

Hence G is closed under the operation multiplication.

(*ii*) ***Associative Property:*** We know that product of three matrices A, B, C ∈ G is associative, *i.e.* A(BC) = (AB)C by the theory of matrices.

Hence G is associative under this operation.

(*iii*) ***Identity Element:*** Let I denote the unit matrix of order n. Hence $I \in G$.

Also $IA = A \ \forall A \in G$.

Hence, I is multiplicative identity.

(*iv*) ***Inverse Elements:*** By theory of matrices every non-singular square matrix A possesses a non singular square matrix A^{-1} as its inverse. Such that

$$A^{-1}A = I \ \forall A \in G.$$

Hence, G is a group with this composition.

(*v*) ***Commutative Property:*** Since the product of two matrices is not commutative.

i.e., $AB \neq BA$

Hence G is a non-abelian group.

Example 14: Determine whether the following sets form a group for the operation defined in the set.

(*i*) $K = \{...., -4, -2, 0, 2, 4, ...\}$ with the operation of addition.

(*ii*) Z = set of integers including zero with the operation $*$ defined as:

$a * b = a - b; \ a, b \in Z.$

Example 15: A set of 2×2 real matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}_{2\times 2}$ with binary multiplication is a group. When $ad - bc \neq 0$.

Solution: Let G be the group of 2×2 real matrices.

(*i*) ***Closure:*** Let $A, B \in G$

and $$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \; B = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

$$A * B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

$$= \begin{bmatrix} ab + br & aq + rs \\ cp + dr & cq + ds \end{bmatrix}$$

$$= (ab + br)(cq + ds) - (cp + dr)(aq + rs)$$

$$= abcq + apds + prcq + brds - cpaq - cpbs - draq - drbs.$$

$$= ps(ad - bc) + rq(cb - ad)$$

$$= (ad - bc)(ps - rq)$$

$$\neq 0$$

So $A * B \in G$

Hence, Group G is closed under the operation multiplication.

(*ii*) ***Associative Property:*** We know that in matrix operation

$$(AB)C = A(BC)$$

Hence multiplication is associative in G.

(*iii*) ***Identity:*** Let e be the identity.

So $$\begin{bmatrix} a & b \\ c & d \end{bmatrix} e = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Hence, identity exists in G.

(*iv*) ***Inverse:*** $$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Example 16: Show that the set of all odd integers with addition is not a group.

Solution: Let Set $A = \{1, 3, 5, 7, 9, ...\}$

Closure: Here $1, 3 \in A$

But $1 + 3 = 4 \notin A$

So Set A is not closed under the operation '+'.

Hence, it is not a group.

Example 17: Prove that set of zero and even integers with addition is an abelian group.

Solution: Let the Set A = $\{0, 2, 4, 6, 8, ...\}$

Let $x, y, z \in A$ and A be the set of zero and even integers.

(*i*) ***Closure:*** $x, y \in A$, since x, y are even integers.

$\Rightarrow$ $x + y$ is an even integer.

$\Rightarrow$ $x + y \in A$

Hence closure property Holds.

(*ii*) ***Associative Property:*** We know that the addition of integers is associative.

If $x, y, z \in A$ then

$$x + (y + z) = (x + y) + z$$

Hence, addition in A is associative.

(*iii*) ***Existence of Identity:*** Let $x \in A$, also $0 \in A$

Hence, $0 + x = x + 0 \ \forall x \in A$

Hence, 0 is additive identity in A.

(*iv*) ***Existence of Inverse:*** Here $x \in A \Rightarrow -x \in A$

But $(-x) + x = 0 \ \forall x \in A$

So $-x$ is inverse of $x \ \forall x \in A$.

Hence inverse of each element in A belongs to A.

(*v*) ***Existence of Abelian:*** Here $x, y \in A$

and $x \circ y = y \circ x \ \forall x, y$

Also addition of integers is commutative.

i.e. $x + y = y + x$

$\forall x, y \in A$

Hence, it is an infinite abelian group.

Example 18: Show that the set $\{0 \pm n, \pm 2n, ... \pm kn ....\}$ is an additive group, n being a fixed integer.

Solution: Set A = $\{0 \pm n, \pm 2n, ... \pm kn ....\}$ and also let $x, y, z \in A$.

(*i*) ***Closure:*** $x, y \ x, y \in A$ are integers.

$\Rightarrow$ $x + y$ is an integer. (because $0 \pm n = \pm kn \in A$)

$\Rightarrow$ $(x + y) \in A$

Hence closure property holds.

(*ii*) ***Associative Property:*** We know that addition of integers x, y, z is associative i.e. if $x, y, z \in A$ then

$$x + (y + z) = (x + y) + z$$

(*iii*) ***Existence of Identity:*** Let $x \in A$. Also $0 \in A$

Hence $0 + x = x + 0 \ \forall x \in A$

Hence 0 is additive identity in A.

(*iv*) ***Existence of Inverse:*** Here $x \in A, -x \in A$. But

$$(-x) + (x) = 0 \ \forall x \in A.$$

Hence, $-x$ is inverse of $x \ \forall x \in A$.

Thus, A forms an additive group in which number of element is infinite. Hence it is an additive group.

Example 19: Prove that the set $\{1, -1, i, -i\}$ is an abelian multiplication finite group of order 4.

Solution:

(*i*) ***Closure:*** $1, -1 \in A$ and also $x, y, z \in A$

$-1 * -1 = -1 \in A$

$i \times i = i^2 = -1 \in A$

$i \times i = 1 \in A$

$-i \times i = -1 \in A$

Hence closure property holds.

(*ii*) ***Associative Property:*** Let $x, y, z \in A$.

Now $x \times (y \times z) = z \times (x \times y)$

Since $1 \times (-1 \times i) = -i$

$i \times (1 \times -i) = -i$

Hence associative property holds.

(*iii*) ***Existence of Identity:*** Let $1 \in A$. Also $-1 \in A$.

But $1 \times -1 = -1 \ \forall x \in A$.

Hence, -1 is the multiplication identity.

(*iv*) ***Existence of Inverse:*** Here $x \in A \Rightarrow -x \in A$.

But $1 \times -1 = -1 \ \forall x \in A$.

Hence, -1 is inverse of $1 \ \forall 1 \in A$.

Hence, inverse of each element in A belongs to A.

Thus A forms an multiplication group in which numbers is 4. Hence it is finite group of order 4.

(*v*) ***Existence of Abelian:*** Also multiplication of integers is commutative.

i.e. $x \times y = y \times x \ \forall\, x, y \in A$.

Hence it is an finite abelian group of order 4.

Example 20: Show that the set {1} forms a group with respect to multiplication.

Solution: Let Set A = {1} and $x, y, z \in A$

where $x = 1, y = 1, z = 1$.

(*i*) ***Closure:*** $1, 1 \in A$

$\Rightarrow 1 \times 1$ is an integer.

$\Rightarrow 1 \in A$. Hence closure property holds.

(*ii*) ***Associative Property:*** We know that multiplication of integers 1, 1, 1 is associative i.e. if $1, 1, 1 \in A$ then

$$x \times (y \times x) = (x \times y) \times x$$

Hence multiplication in A is associative.

(*iii*) ***Existence of Identity:*** Let $x \in A$ and $1 \in I$.

Hence $1 \times x = x \times 1 \ \forall\, x \in 1$.

Hence, 1 is additive identity in A.

(*iv*) ***Existence of Inverse:*** Here $x \in A \Rightarrow \frac{1}{x}$

But $x \times \frac{1}{x} = 1 \qquad \forall\, x \in A$

Hence $\frac{1}{x}$ is inverse of $x \ \forall\, x \in A$

Hence, inverse of each element in A belongs to A.

Thus, A forms an multiplication group.

Example 21: Show that the set of integers with respect to multiplication is not a group.

Solution: Let A = Set of integers and $x, y, z \in A$.

Where x, y, z are integers.

(*i*) ***Closure:*** Let $x, y \in A$

$\Rightarrow x \times y$ is an integer.

$x \times y \in A$

Hence, closure property holds.

(*ii*) ***Associative Property:*** We know that multiplication of integers x, y, z is associative *i.e.*, if $x, y, z \in$ A then

$$x \times (y \times z) = (x \times y) \times z$$

Hence, addition in A is associative.

(*iii*) ***Existence of Identity:*** Let $x \in$ A also $1 \in$ A

Hence $1 \times x = x \times 1 = x \quad \forall x \in$ A

Hence 1 is the multiplication identity.

(*iv*) ***Existence of Inverse:*** Here $x \in$ A

But $\frac{1}{x}$ is not a integer

So $\frac{1}{x} \notin$ A For example Let $x = 2$

$$\frac{1}{2} \notin \text{A}$$

Hence, inverse does not exist.

Hence, A is not a group with respect to multiplication.

Example 22: Show that the set of vectors with vector multiplication as composition is not a group.

Solution: Let V be the set of all vectors and let '$*$' denote vector multiplication. Also let $v_1, v_2, v_3 \in$ V.

(*i*) ***Closure Property:*** $v_1, v_2 \in$ V, then $v_1 \times v_2$ is a vector.

$\therefore \quad v_1 \times v_2 \in$ V, $\forall\, v_1, v_2 \in$ V

Hence, closure property holds.

(*ii*) ***Associative Property:*** Now $a \times (b \times c) = (a \cdot c)b - (a \cdot b) \cdot c$

and $(a \times b) \times c = (a \cdot c)b - (b \cdot c) \cdot a$

Clearly $(a \times b) \times c = (a \times b) \times c$

Hence $*$ is not associative.

Hence V is not a group for the operation '$*$'.

Example 23: Prove that n, nth roots of unity from a multiplicative abelian group.

Solution: Let $x^n = 1 = \cos(2r\pi) + i \sin(2r\pi)$

$$x = \cos\frac{2r\pi}{n} + i \sin\frac{2r\pi}{n}, \; r = 0, 1, 2, \ldots n-1$$

$$= e^{2r\pi i/n}, \; r = 0, 1, 2, \ldots n-1$$

Hence the set of n, nth root of unity is given by

$$\text{A} = \left\{ e^{2r\pi i/n} : r = 0, 1, 2, \ldots n-1 \right\}$$

(*i*) ***Closure Property:*** Let $a, b \in A$ and $a = e^{2\pi r_1 i/n}$, $b = e^{2\pi r_2 i/n}$

where $0 < r_1, r_2 < n - 1$.

$\therefore \quad ab = e^{2\pi r_1 i/n} . e^{2\pi r_2 i/n} = e^{2\pi i(r_1 + r_2)/n} \in A$ if $(r_1 + r_2) < n - 1$

But if $r_1 + r_2 > n - 1$, let $r_1 + r_2 = n + P$ where $0 \le P \le n - 2$.

$$ab = e^{2\pi r(n+P)/n} = e^{2\pi i} . e^{2\pi Pi/n} = e^{2\pi Pi/n} \in A$$

For $0 \le P \le n - 2$.

Hence $a, b \in A \Rightarrow ab \in A, \ \forall a, b \in A$.

Hence closure property holds.

(*ii*) ***Associative Properties:*** Since n, nth roots of unity are complex numbers, and multiplication of complex numbers is associative, hence product of roots is associative.

or $e^{2\pi r_1 i/n} (e^{2\pi r_2 i/n} . e^{2\pi r_3 i/n}) = e^{2\pi i(r_1 + r_2 + r_3)/n}$

$$= (e^{2\pi r_1 i/n} . e^{2\pi r_2 i/n}) e^{2\pi r_3 i/n}$$

Hence Associative property holds.

(*iii*) ***Existence of Identity:*** Putting $r = 0$ in $e^{2r\pi i/n}$

We get $e^{2r\pi i/n} = e^0 = 1$

$\therefore 1 \in A$. Also $1 . e^{2\pi ri/n} = e^{2\pi ri/n}, \ \forall e^{2\pi ri/n} \in A$.

Hence, 1 is identity and $1 \in A$.

(*iv*) ***Existence of Inverse:*** Let $a = e^{2\pi ir/n}$ and $b = e^{2\pi(n-r)i/n}$.

Hence, $ab = e^{2\pi ri/n} . e^{2\pi(n-r)i/n} = e^{2\pi i} = 1, . \ \forall a \in A$

Hence, $e^{2\pi(n-r)i/n}$ is inverse of $e^{2\pi ri/n}$.

Also $e^{2\pi(n-r)i/n} \in A$.

Hence, inverses of elements of A belong to A.

Also $a \cdot b = b \cdot a$.

Hence, A is abelian group with respect to multiplication.

Example 24: Verify that the totality of all positive rationals form as group under the composition defined by

$$a * b = ab/2$$

Solution: Let Q^+ be the set of all positive rationals and let $a, b, c \in Q^+$.

(*i*) ***Closure Property:*** Here $a * b = \frac{ab}{2}$ a rational.

$\therefore \quad ab \in Q^+, \ \forall a, b \in Q^+$.

Hence, closure property holds.

(*ii*) ***Associative Property:*** Now $a * (b * c) = a * \left(\frac{bc}{2}\right)$

by definition

$$= \frac{abc}{4} = \frac{ab}{2} \cdot \frac{c}{2}$$

$$= (a * b) * \frac{c}{2} = (a * b) * c$$

Hence associative property holds.

(*iii*) ***Existence of Identity:*** Let e be the left identity.

$\therefore \quad e * a = a \Rightarrow \frac{ea}{2} = a$

$\Rightarrow \quad e = 2. \qquad$ Also $2 \in Q^+$

Hence 2 is identity and $2 \in Q^+$.

(*iv*) ***Existence of Inverse:*** Let b be left inverse of a.

$\Rightarrow \qquad b * a = a = 2$

$\Rightarrow \qquad \frac{ba}{2} = 2$

$\Rightarrow \qquad b = \frac{4}{a} \in Q^+ \qquad \because \quad a \in Q^+$

Hence inverse of $\forall a \in Q^+, \in Q^+$.

Thus $(Q^+, *)$ is a group.

(*v*) ***Commutative Law:*** Clearly $(a * b) = \frac{ab}{2} = \frac{ba}{2} = b * a$

Hence $*$ is commutative and $(Q^+, *)$ is an abelian group.

5.6 SEMIGROUPS

Let us consider, an algebraic system (A,*) where * is a binary operation on A. Then the system (A,*) is said to be a semi-group if it satisfies the following properties:

1. The operation * is a closed operation on set A.
2. The operation * is an associative operation.

Example 25: Consider an algebraic system (A,*), where A={1,3,5,7,.....}, the set of all positive odd integers and * is a binary operation means multiplication. Determine whether (A,*) is a semi-group.

Solution:

Closure Property: The operation * is a closed operation because multiplication of two odd integers is a +ve odd integer.

Associative Property: The operation * is an associative operation on set A. Since for every (a,b,c) belongs to A, we have

$$(a*b)*c=a*(b*c)$$

Hence the algebraic system (A,*) is a semi-group.

5.7 MONOIDS

Let us consider, an algebraic system (A,*) where * is a binary operation on A. Then the system (A,o) is said to be a monoid if it satisfies the following properties.

(i) The operation o is a closed operation on set A.

(ii) The operation o is an associative operation.

(iii) There exists an identity element w.r.t the operation o.

Example 26: Consider an algebraic system (N,+), where the set N={0,1,2,3,4,.....}the set of natural numbers and + is an addition operation. Determine whether (N,+) is a monoid.

Solution:

Closure Property: The operation + is closed since sum of two numbers is a natural number.

Associative Property: The operation + is an associative property since we have

$$(a+b)+c=a+(b+c) \text{ foe all a,b,c belong to N}$$

Identity: The element 0 is an identity element w.r.t the operation +.

Hence the algebraic system(N,+) is a monoid.

5.8 ALTERNATIVE DEFINITION OF A GROUP

Theorem: A set G with a binary composition denoted multiplicatively is a group iff

(*i*) the composition is associative and (*ii*) $\forall\, a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solution in G.

Proof:

Necessary Conditions: Let $(G, *)$ be the group.

Hence from group axioms, composition is binary as well as associative. Also let a^{-1} be the inverse of a, where $a \in G$.

Then $ax = b \Rightarrow a^{-1}(ax) = a^{-1}b$

$\Rightarrow (a^{-1}a)x \Rightarrow a^{-1}b$ (By Associative Property)