BLOCK I:
DISCRETE MATHEMATICAL STRUCTURES AND MATHEMATICAL LOGIC

UNIT 1: CONGRUENCE, PERMUTATION AND COMBINATION WITH REPETITION

Space for learners:

Unit Structure:

1.1 INTRODUCTION

Space for learners:

In this unit, you will learn about a useful way of comparing the remainder of two integers, called congruence. You will also learn various properties of congruence with their proof like Addition rule of congruence, Multiplication rule of congruence, Power rule of congruence and Cancellation rule of congruence. You will also learn how Power rule can be used to check the divisibility of certain large numbers. Again, you will learn the concept of Least Residues and Modular Arithmetic with some examples.

In the middle part, you will learn a very familiar concept of Mathematics, Permutation, i.e., how a number of objects can be arranged in a definite order taking some or all at a time. You will learn Factorial Notation with some examples, which is mostly used in Permutation as well as Combination. Again, the concept of Fundamental principle of Counting is explained here with some examples. We can also learn how we arrange n different objects taking r at a time if some objects repeats, i.e., Permutation with repetition with some examples. You will also learn how n objects can be arranged if the objects are distinct objects. Again, you will learn the arrangement of n distinct objects around a fix circle where Clockwise and Anticlockwise orders are different as well as same with some examples. Again, you can see the how certain restrictions can be imposed on Permutation, i.e., Restricted Permutation and some examples of it.

In the latter part, you will learn another very familiar concept of Mathematics, called Combination, i.e., the selection of all or part of a set of objects without regard to the order in which objects are selected with various examples. You will again learn the concept of Restricted Combination, i.e., how Combination can be made if there are certain restriction.

1.2 UNIT OBJECTIVES

After going through this unit, you will be able to:

- Understand the concept of Congruence
- Know the Properties of Congruence
- Know the concept of Least Residues

- Know Modular Arithmetic
- Define Permutation
- Understand the Concept of Factorial Notation
- Know the fundamental concept of Counting
- Learn Permutation with repetition
- Learn Permutation of n objects if the objects are distinct
- Learn the concept of Circular Permutation
- Learn the concept of Restricted Permutation
- Learn the concept of Combination
- Learn the concept of Restricted Combination

Space for learners:

1.3 CONGRUENCE

Definition1: Let n be a positive integer. Two integers a and b are congruent modulo n if they each have the same remainder on division by n. If a and b are congruent modulo n, then it is written symbolically as

$$a \equiv b \pmod{n}.$$

For example, 19 and 12 are congruent modulo 7; that is,

$19 \equiv 12 \pmod{7}$

because 19 and 12 each have remainder 5 on division by 7.

Also, −8 and 10 are congruent modulo 6; that is,

$-8 \equiv 10 \pmod{6}$,

because −8 and 10 each have remainder 4 on division by 6.

Definition2: Let n be a fixed integer. Two integers a and b are said to be congruent modulo n if $n \mid a-b$ i.e., if a-b is divisible by n.

For example, 3 and 24 are said to be congruent modulo 7, because (3-24) = -21, which is divisible by 7.

Therefore, $3 \equiv 24 \pmod{7}$.

Again, if a and b are not congruent modulo n, then the difference between a and b is not an integer multiple of n; that is, $a - b$ is not divisible by n.

For example, 4 and 6 are not congruent modulo 5, because 4-6=-2, which is not divisible by 5.

Illustrative Example:

List all integers x in the range $1 < x < 100$ that satisfy $x \equiv 3 \pmod 7$.

Solution:

Given,

$$x \equiv 3 \pmod 7$$

i.e. $7 \mid x-3$

i.e. $x-3= 7k, k \in Z$

i.e. $x=3+7k$ ……………… (1)

Therefore,

$$1 < 3+7k < 100$$

$$-2 < 7k < 97.$$

From this we obtain the values of k as,

0,1,2,3,4,5,6,7,8,9,10,11,12,13.

Now, putting the values of k in equation (1), we get the values of

x=3,10,17,24,31,38,45,52,57,66,73,80,87 and 94.

1.4 PROPERTIES OF CONGRUENCE

1.$a \equiv a \pmod n$

2. if $a \equiv b \pmod n$ then $b \equiv a \pmod n$

3. if $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$

4. Addition Law of Congruence

If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $a + c \equiv b + d \pmod n$

5. Multiplication Law of Congruence

If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $ac \equiv bd \pmod n$.

6. For any integers a, b, and c

(a) If $a \equiv b \pmod n$, then $a + c \equiv b + c \pmod n$.

(b) If $a \equiv b \pmod n$, then $ca \equiv cb \pmod n$.

Space for learners:

Proof (1): For any integer a and any fixed positive integer n,

We have a-a=0, which is divisible by n

Therefore, $n \mid (a-a)$, since 0 is divisible by any integer.

Therefore $a \equiv a \bmod n$.

For example, $5 \equiv 5 \pmod 7$, because 5-5=0 is divisible by 7.

Proof (2): Let, $a \equiv b \pmod n$, then, $n|(a - b)$.

Therefore, $n|(-1)(a - b)$

Or, $n|(b - a)$.

Therefore, $b \equiv a \pmod n$.

So, if $a \equiv b \pmod n$ then $b \equiv a \pmod n$.

For example, if $3 \equiv 18 \pmod 5$, then $18 \equiv 3 \pmod 5$, because 3-18=-15 and 18-3=15,both -15 and 15 are divisible by 5.

Proof (3): Let $a \equiv b \pmod n$.

Then,

$$n|(a-b)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Again,

Let, $b \equiv c \pmod n$.

Then,

$$n|(b-c)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

From equation (1) & (2), we get,

$n|(a - b + b- c)$ [by Linear Combination Theorem]

or $n|(a - c)$.

Thus, $a \equiv c \bmod n$.

Therefore, if $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$

For example, we consider

$7 \equiv 12 \pmod 5$ [Because 7-12=-5,which is divisible by 5]

and $12 \equiv 22 \pmod 5$ [Because 12-22=-10,which is divisible by 5]

Now, clearly we can say that

$7 \equiv 22 \pmod 5$ [Because 7-22=-15,Which is divisible by 5]

Space for learners:

Proof (4): Let, $a \equiv b \pmod{n}$.

Then,

a-b is divisible by n ……………………(1)

And, $c \equiv d \pmod{n}$.

Then, $c - d$ are divisible by n …………………(2)

From equation (1) & (2) we get,

$(a - b) + (c - d)$ is divisible by n.

But, $(a - b) + (c - d) = (a + c) - (b + d)$.

So, $(a + c) - (b + d)$ is divisible by n.

Therefore, $a + c \equiv b + d \pmod{n}$.

So, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.

For example,

We know that,

$19 \equiv 1 \pmod{18}$ and $37 \equiv 1 \pmod{18}$,

so, by the addition rule of congruence,

$19 + 37 \equiv 1 + 1 \equiv 2 \pmod{18}$.

Or $56 \equiv 2 \pmod{18}$.

Proof (5): Let, $a \equiv b \pmod{n}$.

Then, a-b is divisible by n

Then, (a-b)c is also divisible by n……………………(1)

And $c \equiv d \pmod{n}$.

Then, c-d is divisible by n

Then, (c-d)b is also divisible by n………………..… .(2)

From equation (1) & (2),

(a-b)c+(c-d)b is also divisible by n

But, $(a - b)c + (c - d)b = ac - bd$.

So, $ac - bd$ is divisible by n.

Hence, $ac \equiv bd \pmod{n}$.

Hence, If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Space for learners:

For Example,

$17 \equiv -2 \pmod{19}$

and $14 \equiv -5 \pmod{19}$.

Therefore,

$17 \times 14 \equiv (-2) \times (-5) \equiv 10 \pmod{19}$ [By Multiplication rule of Congruence]

Or , $238 \equiv 10 \pmod{19}$.

1.4.1 Power Rule for Congruences

If $a \equiv b \pmod{n}$, and m is a positive integer, then $a^m \equiv b^m \pmod{n}$.

For example, suppose you wish to find the least residue(remainder) of 19^5 modulo 9. Since $19 \equiv 1 \pmod 9$, it follows that $195 \equiv 1^5 \equiv 1 \pmod 9$, so the least residue is 1. This is a particularly simple application of the power rule.

1.4.2 Cancellation Rule of Congruence

If, $ca \equiv cb \pmod{n}$ then $a \equiv b \pmod{n/d}$ where $d = \gcd(c,n)$

For example,

Consider, $33 \equiv 15 \pmod 9$

Now, $3*11 \equiv 3*5 \pmod 9$

$11 \equiv 5 \pmod 3$,by cancellation law of congruence.[since, gcd of 3 and 9 is 3]

Again, by same law we can write $-35 \equiv 45 \pmod 8$, as $-7 \equiv 9 \pmod 8$

1.5 LEAST RESIDUES

The least residue of a modulo n is the remainder r that you obtain when you divide a by n. The integer r is one of the numbers 0, 1, . . . , n − 1, and it satisfies $a \equiv r \pmod{n}$.

For example, the least residue of −33 modulo 7 is 2

Because, $-33 = 7 \times (-5) + 2$

Space for learners:

1.6 MODULAR ARITHMETIC

Modular arithmetic is the application of the usual arithmetic operations – namely addition, subtraction, multiplication and division – for congruences. Addition, subtraction and multiplication are often simpler to carry out in modular arithmetic than they are normally, because you can use congruences to reduce large numbers to small numbers.

Examples:

1. Find the least residue of 67+68 modulo 6
2. Find the least residue of 17*14 modulo 19

Solution1: We know that,

$67 \equiv 1 \pmod 6$ [Because 67-1=66,is divisible by 6]………(1)

$68 \equiv 2 \pmod 6$ [Because 68-2=66,is divisible by6]………(2)

From equation (1) & (2),

$67+68 \equiv 1+2 \pmod 6$ [By Addition rule of congruence]

Or $135 \equiv 3 \pmod 6$ [135-3=132,is divisible by 6].

Therefore, the least residue of 67+68 modulo 6 is 3

Solution2: We know that,

$17 \equiv -2 \pmod{19}$ [Because 17-(-2)=19,is divisible by 19]………(1)

$14 \equiv -5 \pmod{19}$ [Because 14-(-5)=19,is divisible by 19]………(2)

From equation (1) & (2),

$17*14 \equiv (-2)*(-5) \equiv 10 \pmod{19}$ [By Multiplication Law of congruence].

Therefore, the least residue of 17*14 modulo 19 is 10.

Space for learners:

1.7 APPLICATION OF POWER LAW OF CONGRUENCE

Example1: Find the remainder when $25^{100} + 11^{500}$ is divided by 3.

Solution 1:

We know that, $25 \equiv 1 \pmod 3$.

Therefore, $25^{100} \equiv 1^{100} \pmod 3$ [By Power rule of Congruence]

Therefore, $25^{100} \equiv 1 \pmod 3$……………………….(1)

Again, $11 \equiv -1 \pmod 3$.

Therefore, $11^{500} \equiv (-1)^{500} (\text{mod } 3)$ [By Power rule of Congruence]

Therefore, $11^{500} \equiv 1 \pmod 3$……………………….(2)

From equation (1) & (2),

$25^{100} + 11^{500} \equiv 2 \pmod 3$ [By addition law of Congruence]

Therefore, the remainder is 2.

Example 2: Show that $3^{1000} + 3$ is divisible by 28.

Solution 2: We know that, $3^3 = 27 \equiv -1 \pmod{28}$.

Therefore, $(3^3)^{333} \equiv (-1)^{333} \pmod{28}$ [By power rule of Congruence]

Therefore, $3^{999} \equiv -1 \pmod{28}$.

$3^{1000} = 3^{999}.3 \equiv -1.3 \pmod{28}$ [By Properties 6(b)]

Therefore, $3^{1000} \equiv -3 (\text{ mod } 28)$ ……………………….(1)

Again, $3 \equiv 3 (\text{ mod } 28)$ ……………………………….(2)

From equation (1) & (2),

$3^{1000} + 3 \equiv -3+3 \equiv 0 (\text{ mod } 28)$ [By addition rule of Congruence]

Therefore, $3^{1000} + 3 \equiv 0 \pmod{28}$.

So, the remainder, when we divide $3^{1000}+3$ by 28, is 0.

Hence, we can say that $3^{1000} +3$ is divisible by 28.

CHECK YOUR PROGRESS-I

1. Which of the following congruences are true?
(a) $11 \equiv 26 \pmod 5$ (b) $9 \equiv -9 \pmod 5$
(c) $28 \equiv 0 \pmod 7$ (d) $-4 \equiv -18 \pmod 7$
(e) $-8 \equiv 5 \pmod{13}$ (f) $38 \equiv 0$ (mod 13

(2). Determine the integers in between 50 and 100 which are congruent to 1 modulo 4.

(3). List all integers x in the range $1 \le x \le 100$ that satisfy $x \equiv 7$ (mod 17).

(4). Find the least residues of the following integers modulo 10.
(a) 17 (b) 50 (c) 6 (d) −1 (e) −38

(5). Find the least residues of the following integers modulo 7.
(a) 3×6 (b) 22×29 (c) 51×74

(6).Show that 2^{20}-1 is divisible by 41

(7). What is the remainder when 3^{5555} is divided by 80?

Space for learners:

1.8 PERMUTATION

A permutation is an arrangement in a definite order of a number of objects taken some or all at a time.

The number of permutations of n different objects taken r at a time, where $0 < r \leq n$ and the objects do not repeat is n (n – 1) (n – 2) . . . (n – r + 1), which is denoted by ^nP_rorP(n,r)

$^np_r = \frac{n!}{(n-r)!}$where $0 \leq r \leq n$

Space for learners:

1.8.1 Factorial Representation

The notation n! represents the product of first n natural numbers, i.e., the product $1 \times 2 \times 3 \times . . . \times (n - 1) \times n$ is denoted as n!. We read this symbol as 'n factorial'.

Thus, $1 \times 2 \times 3 \times 4 . . . \times (n - 1) \times n = n!$

$1 = 1!$

$1 \times 2 = 2!$

$1\times 2 \times 3 = 3!$

$1 \times 2 \times 3 \times 4 = 4!$

We define $0! = 1$

Again,

$5! = 5 \times 4! = 5 \times 4 \times 3! = 5 \times 4 \times 3 \times 2! = 5 \times 4 \times 3 \times 2 \times 1!$

Example 1. Evaluate (a) 3! (b) 2! + 4! (c) 2! ×3!

Solution:

(a) $3! = 3\times2\times1= 6$

(b) $2! = 2\times1 = 2$

$4! = 4\times3\times 2\times1 = 24$

Therefore, $2! + 4! = 2 + 24 = 26$

(c) $2! \times 3! =2 \times6= 12$

Example2: Find the value of (a)$^np_0$ (b)$^np_1$ (c) ^np_n (d)$^6p_3$

Solution 2 (a)

We know that

$^np_r = \frac{n!}{(n-r)!}$

Therefore,

$^np_0 = \frac{n!}{(n-0)!}$

$= \frac{n!}{(n)!}$

$=1$

So, $^np_0 = 1$. Similarly $^5p_0 = {}^7p_0 = 1$.

2. (b) We know that,

$^np_r = \frac{n!}{(n-r)!}$

$\Rightarrow {}^np_1 = \frac{n!}{(n-1)!}$

$= \frac{n*(n-1)!}{(n-1)!}$

$=n$

So, $^np_1 = n$, similarly $5p_1 = 5$, $^6p_1 = 6$.

2(c) We know that

$^np_r = \frac{n!}{(n-r)!}$

$^np_n = \frac{n!}{(n-n)!}$

$= \frac{n!}{0!}$

$= n!$ [since, $0! = 1$]

Therefore, $^np_n = n!$. Similarly, $^5p_5 = 5!$, $^7p_7 = 7!$

2 (d) We know that,

$^np_r = \frac{n!}{(n-r)!}$

Space for learners:

$So,\quad {}^6p_3 = \frac{6!}{(6-3)!}$

$= \frac{6!}{3!}$

$= \frac{6\times5\times4\times3!}{3!}$

$=6\times5\times4$

$=120$

Example 3:

(a) Prove that ${}^np_r = {}^{n-1}p_r + r.{}^{n-1}p_{r-1}$

(b) Find the value of n, if ${}^np_7 = 42\times {}^np_5$

(c) *Find the valueof n if* ${}^np_5 : {}^np_3 = 2:1$

Solution 3(a):

$RHS = {}^{n-1}p_r + r.{}^{n-1}p_{r-1}$

$= \frac{(n-1)!}{(n-1-r)!} + r\times\frac{(n-1)!}{\{(n-1)-(r-1)\}!}$ [Since, ${}^np_r = \frac{n!}{(n-r)!}$]

$= \frac{(n-1)!}{(n-r-1)!} + r\times\frac{(n-1)!}{(n-r)!}$

$= \frac{(n-1)!}{(n-r-1)!} + r\times\frac{(n-1)!}{(n-r)\times(n-r-1)!}$ [Since, $n!=n\times(n-1)!$]

$= \frac{(n-1)!}{(n-r-1)!}\left(1+\frac{r}{n-r}\right)$

$= \frac{(n-1)!}{(n-r-1)!} \times \frac{n}{n-r}$

$= \frac{n!}{(n-r)!}$

$= {}^np_r$

$=$L.H.S

Hence, ${}^np_r = {}^{n-1}p_r + r.{}^{n-1}p_{r-1}$

3(b):

Given,

${}^np_7 = 42\times {}^np_5$

$\Rightarrow \frac{n!}{(n-7)!} = 42\times\frac{n!}{(n-5)!}$

$\Rightarrow \frac{1}{(n-7)!} = \frac{42}{(n-5)!}$

$\Rightarrow (n-5)! = 42\times(n-7)!$

Space for learners:

$\Rightarrow$ (n-5)$(n-6)(n-7)! = 42 \times (n-7)!$

$\Rightarrow$ (n-5)(n-6)= 42

$\Rightarrow$ (n-5)(n-6)=7×6

$\Rightarrow$ (n-5)=7 or (n-6)=6

$\Rightarrow$ n=12

The required value of n is 12

3(c):

Given,

$^np_5 : {}^np_3 = 2:1$

$\Rightarrow \frac{n!}{(n-5)!} : \frac{n!}{(n-3)!} = 2:1$

$\Rightarrow \frac{\frac{n!}{(n-5)!}}{\frac{n!}{(n-3)!}} = \frac{2}{1}$

$\Rightarrow \frac{n!}{(n-5)!} \times \frac{(n-3)}{n!} = \frac{2}{1}$

$\Rightarrow \frac{(n-3)!}{(n-5)!} = 2$

$\Rightarrow \frac{(n-3)(n-4)(n-5)!}{(n-5)!} = 2$

$\Rightarrow$ (n-3)(n-4)=2

$\Rightarrow$ (n-3)(n-4)=2×1

$\Rightarrow$ n-3=2 or n-4 =1

$\Rightarrow$ n=5

1.8.2 Fundamental Principle of Counting (Multiplication Principle)

"If an event can occur in m different ways, following which another event can occur in n different ways, then the total number of occurrences of the events in the given order is m×n."

Space for learners:

Example 1: How many 3-digit numbers can be formed with the digits 1,4,7,8 and 9 if the digits are not repeated?

Solution 1:

Three-digit numbers will have units, ten's and hundred's place.

Out of 5 given digits any one can take the unit's place.

This can be done in 5 ways. ... (i)

After filling the unit's place, any of the four remaining digits can take the ten's place.

This can be done in 4 ways. ... (ii)

After filling in ten's place, hundred's place can be filled from any of the three remaining digits.

This can be done in 3 ways. ... (iii)

∴ By counting principle, the number of 3 digit numbers = $5 \times 4 \times 3 = 60$

Example2: There are 4 books on fairy tales, 5 novels and 3 plays. In how many ways can you arrange these so that books on fairy tales are together, novels are together and plays are together and, in the order, books on fairy tales, novels and plays.

Solution 2:

There are 4 books on fairy tales and they have to be put together.

They can be arranged in 4! ways.

Similarly, there are 5 novels.

They can be arranged in 5! ways.

And there are 3 plays.

They can be arranged in 3! ways.

So, by the counting principle all of them together can be arranged in $4! \times 5! \times 3!$ ways = 17280 ways.

Space for learners:

CHECK YOUR PROGRESS-II

8 (a) Evaluate:

(i) 6! (ii) 7! (iii) 7! + 3! (iv) 6! × 4!

(b) Which of the following statements are true?

(i) 2!× 3! = 6! (ii) 2! + 4! = 6! (iii) 4! - 2! = 2!

9.Find the value of

(a) ${}^{15}p_4$ (b) ${}^{11}p_5$ (c) ${}^{9}p_0$

10.Find the value of n if 2* ${}^{9}p_n = {}^{10}p_n$

11. $Find\ the Value\ of\ r\ if$ ${}^{18}p_{r-1}:{}^{17}p_{r-1}$ =9:7

12. Find the value of r if 5*${}^{4}p_r$ =6 *${}^{5}p_{r-1}$

13.How many words of 4 letters with or without meaning can be formed from the letters of the word RICE.

14.Without repetition how many 4 digits numbers can be formed with the digits 1,3,5,7,9.

Space for learners:

1.6.3 Permutation with Repetition

The number of permutations of n different objects taken r at a time, where repetition is allowed, is n^r.

Example 1: Find the number of 4 digit numbers that can be formed using the digits 1, 2, 4, 5, 7, 8 when repetition is allowed.

Solution1:

The number of 4 digit numbers that can be formed using the digits 1, 2, 4, 5, 7, 8 when repetition is allowed = 6^4 = 1296

Example 2: Ten different letters of an alphabet are given. Words with 5 letters are formed from these letters. Find the number of words which have at least one letter repeated.

Solution 2:

The number of 5 letter words using ten different letters when repetition is allowed = 10^5

Again,

The number of 5 letter words using ten different letters when repetition is not allowed=${}^{10}p_5$

$Therefore, the$number of 5 letter words using ten different letters in which at least one

letter repeated = $10^5 - {}^{10}p_5 = 100000 - 30240 = 69760$

Example 3: How many numbers lying between 100 and 1000 can be formed with the digits 0, 1, 2, 3, 4, 5, if the repetition of the digits is not allowed?

Solution 3:

Every number between 100 and 1000 is a 3-digit number. We, first, have to count the permutations of 6 digits taken 3 at a time.

This number would be ${}^6p_3$.

But, these permutations will include those also where 0 is at the 100's place. For example, 092, 042. . .etc. are such numbers which are actually 2-digit numbers and hence the number of such numbers has to be subtracted from ${}^6p_3$ to get the required number. To get the number of such numbers, we fix 0 at the 100's place and rearrange the remaining 5 digits taking 2 at a time. This number is ${}^5p_2$.

So, the required number is = ${}^6p_3 - {}^5p_2$

$$= 100$$

1.8.4 Permutations when all the Objects are Not Distinct Objects

The number of permutations of n objects, where p1 objects are of one kind, p2 are of second kind, ..., pk are of kth kind and the rest, if any, are of different kind is $\frac{n!}{p1!\,p2!\ldots\ldots pk!}$

Example 1: How many words can be formed with the letters of the words COMMITTEE?

Solution1:

Here, there are 9 objects (letters) of which there are 2M's, 2 T's, 2 E's and rest are all different.

Therefore, the required number of arrangements $=\frac{9!}{2!2!2!} = \frac{9\times8\times7\times6\times5\times4\times3\times2\times1}{2\times2\times2}$

$=9\times 7\times 6\times 5\times 4\times 3\times 2\times 1$

=45360

Space for learners:

Example 2: In how many ways can 4 red, 3 yellow and 2 green balls be arranged in a row if the balls of the same colour are indistinguishable?

Solution 2:

Total no of balls=9

So, out of 9 balls, 4 balls are red, 3 balls are yellow and 2 balls are green.

Therefore, the total no of arrangements=$\frac{9!}{4!\,3!\,2!}$

$=\frac{9\times8\times7\times6\times5\times4!}{4!\times6\times2}$

$=\frac{9\times8\times7\times5}{2}$

$=9\times4\times7\times5$

=1260

1.8.5 Circular Permutation

Circular Permutation is the total number of ways in which n distinct objects can be arranged around a fix circle.

It is of two types

Case1- Clockwise and Anticlockwise orders are different.

Here, the number of circular permutations of n dissimilar things is $(n-1)!$

Case2- Clockwise and Anticlockwise orders are same.

Here, the number of circular permutations of n things is $\frac{1}{2}[(n-1)!]$

Example 1: Find the number of ways of arranging 7 persons around a circle.

Solution1:

Number of persons, n = 7

∴The number of ways of arranging 7 persons around a circle = $(n-1)! = 6! = 720$

Space for learners:

Example 2: Find the number of ways of arranging 6 boys and 6 girls around a circular table so that (i) all the girls sit together (ii) no two girls sit together iii) boys and girls sit alternatively

Space for learners:

Solution2:

(i) Treat all the 6 girls as one unit. Then we have 6 boys and 1 unit of girls. They can be arranged around a circular table in 6! Ways. Now, the 6 girls can be arranged among themselves in 6! Ways.

∴The number of required arrangements = $6! \times 6! = 720 \times 720 = 5{,}18{,}400$

(ii) First arrange the 6 boys around a circular table in 5! ways. Then we can find 6 gaps between them. The 6 girls can be arranged in these 6 gaps in 6! ways.

∴The number of required arrangements = $5! \times 6! = 120 \times 720 = 86{,}400$

(iii) The arrangements of boys and girls sit alternatively in same as the arrangements of no two girls sit together or arrangements of no two boys sit together.

First arrange the 6 girls around a circle table in 5! ways.

Then we can find 6 gaps between them.

The 6 boys can be arranged in these 6 gaps in 6! ways.

∴The number of required arrangements = $5! \times 6! = 120 \times 720 = 86{,}400$

Example 3: Find the number of ways of arranging 6 red roses and 3 yellow roses of different sizes into a garland. In how many of them (i) all the yellow roses are together (ii) no two yellow roses are together

Solution 3:

Total number of roses = 6 + 3 = 9

∴ The number of ways of arranging 6 red roses and 3 yellow roses of different sizes into a garland

$$= \frac{1}{2}[(9-1)!$$

$=\frac{1}{2}(8!)$

$=\frac{1}{2}\times 40320$

$=20160$

(i) Treat all the 3 yellow roses as one unit. Then we have 6 red roses and one unit of yellow roses.

They can be arranged in garland form in (7 - 1)! = 6! ways.

Now, the 3 yellow roses can be arranged among themselves in 3! ways. But in the case of garlands, clockwise arrangements look alike.

∴The number of required arrangements $=\frac{1}{2}\times 6!\times 3!$

$=\frac{1}{2}\times 720\times 6$

$=2160$

(ii) First, arrange the 6 red roses in garland form in 5! ways.

(iii) Then we can find 6 gaps between them. The 3 yellow roses can be arranged in these 6 gaps in ${}^6p_3$ ways. But in the case of garlands, clock-wise and anti-clockwise arrangements look alike.

∴The number of required arrangements$=\frac{1}{2}\times 5!\times {}^6p_3$

$=\frac{1}{2}\times 120\times 6\times 5\times 4$

$=7200$

1.8.6 Restricted Permutation

Permutation with some specific restrictions is called restricted permutations. Following are some Permutation corresponding to some common restrictions.

The number of permutation of n different things taken r of them at a time in which k particular things

(a) Never Occur is = ${}^{n-k}p_r$

Space for learners:

(b) Always occur is $^{n-k}p_{r-k} \times {}^{r}p_{k}$

(c) Are placed in some specific places in $^{n-k}p_{r-k}$

Example1: How many words can be formed with the letters of the word EQUATION taking 5 at a time if

(a) None of words contains Q,U and T

(b) A and O occur In each word

Solution 1:

(a) There are 8 letters in the word EQUATION. If none of the words contain the 3 letters Q,U and T, then there will be remain 8-3=5 letters.

So, the permutation will be the arrangement of these 5 letters.

Therefore, the required no of words = $^{5}p_{5} = 120$

(b) Since, A and O are always present, So any two of the 5 gaps are to be filled up by the two letters A and O, Which can be done in 5p2 ways. After filling 2 of the 5 gaps, the remaining 5-2=3 gaps can be filled up by the 3 letters from the remaining 8-2=6 letters, which will be filled in 6p3 ways.

Therefore, the required no of words=6p3 ×5p2 =2400

Example 2: How many arrangements of the letters of the word 'BENGALI' can be made (i) if the vowels are never together. (ii) if the vowels are to occupy only odd places.

Solution 2:

(i) Considering vowels a, e, i as one letter, we can arrange 4+1 letters in 5! Ways in each of which vowels are together.

These 3 vowels can be arranged among themselves in 3! ways.

∴ Total number of words = 5! × 3! = 120 × 6 = 720

(ii) There are 4 odd places and 3 even places.

3 vowels can occupy 4 odd places in $^{4}p_{3}$ ways

And 4 constants can be arranged in $^{4}p_{4}$ ways.

∴Required number of words $= {}^{4}p_{3} \times {}^{4}p_{4}$

$=24\times24$

$=576$

Space for learners:

1.9 COMBINATION

A combination is a selection of all or part of a set of object without regard to the order in which objects are selected.

The number of combinations of n things taken r at a time is denoted by ${}^nC_r$ and it is defined by ${}^nC_r = \frac{n!}{(n-r)!\,r!}$ For $0 \leq r \leq n$

1.9.1 Restricted Combination

If there are certain restrictions on Combination like a particular object occurring always and occurring never, then it is called Restricted Combination.

The numbers of Combinations of n different things taking r of them at a time if x particular things are

(i) Always included is ${}^{n-x}C_{r-x}$

(ii) Always excluded is ${}^{n-x}C_r$

Example 1:

Show That

(a) ${}^nC_0=1$

(b) ${}^nc_r= {}^np_r/r!$

(c) ${}^nc_1=n$

(d) ${}^nc_r={}^nc_{n-r}$

(e) ${}^nc_r+{}^nc_{r-1}={}^{n+1}c_r$

Solution:

(a) LHS= ${}^nC_0$

$=\frac{n!}{(n-0)!\,0!}$ $[{}^nC_r = \frac{n!}{(n-r)!\,r!}]$

$=\frac{n!}{n!\,1}$ $[0!=1]$

=1

=RHS

(b) LHS=${}^nC_r$

$=\frac{n!}{(n-r)!\,r!}$

Space for learners:

$={}^{n}p_r/r!$ [Since, ${}^{n}P_r = \frac{n!}{(n-r)!}$]

=RHS

(c) LHS= nC1

$=\frac{n!}{(n-1)!\times 1!}$ [since, ${}^{n}C_r=\frac{n!}{(n-r)!\, r!}$]

$=\frac{n\times(n-1)!}{(n-1)!\times 1}$

=n

=RHS

(d) LHS= ${}^{n}C_r$

$=\frac{n!}{(n-r)!\times r!}$

$=\frac{n!}{(n-r)!\times(n-(n-r))!}$

$={}^{n}C_{n-r}$

=RHS

(e) LHS= ${}^{n}C_r+{}^{n}C_{r-1}$

$=\frac{n!}{(n-r)!\, r!}+\frac{n!}{(n-r+1)!(r-1)!}$

$=\frac{n!}{(n-r)!\, r(r-1)!}+\frac{n!}{(n-r+1)(n-r)!(r-1)!}$

$=\frac{n!}{(n-r)!\,(r-1)!}\left(\frac{1}{r}+\frac{1}{n-r+1}\right)$

$=\frac{n!}{(n-r)!\,(r-1)!}\left(\frac{n-r+1+r}{r(n-r+1)}\right)$

$=\frac{(n+1)\times n!}{r\times(r-1)!(n-r+1)\times(n-r)!}$

$=\frac{(n+1)!}{r!\times(n-r+1)!}$

$=\frac{(n+1)!}{r!\times(n+1-r)!}$

$={}^{n+1}C_r$

=RHS

Example 2:

(a) Find the value of ${}^{9}C_7$

(b) If ${}^{12}C_r = {}^{12}C_{r+2}$ find the value of r

(c) If ${}^{n}C_3 \div {}^{n}C_2 = 8$,find the value of n.

(d) If ${}^{n}P_r = 110$ and ${}^{n}C_r=55$,find the value of r

Space for learners:

Solution:

(a) $^9C_7$

$=\frac{9!}{(9-7)!\times 7!}$

$=\frac{9!}{2!\times 7!}$

$=\frac{9\times8\times7!}{2\times7!}$

$=\frac{9\times8}{2}$

$=36$

(b) Given

$^{12}C_r={}^{12}C_{r+2}$

$\Rightarrow {}^{12}C_{12-r}={}^{12}C_{r+2}$ $[Since, {}^nc_r={}^nc_{n-r}]$

$\Rightarrow 12-r = r+2[if\ {}^nc_r={}^nc_s\ then\ r=s]\ \Rightarrow 2r=10$

$\Rightarrow r=5$

(c) Given,

$^nC_3\div{}^nC_2=8$

$\Rightarrow \frac{n!}{(n-3)!\times3!}\div\frac{n!}{(n-2)!\times2!}=8\Rightarrow\frac{n!}{(n-3)!\times3!}\times\frac{(n-2)!\times2!}{n!}=8\Rightarrow\frac{(n-2)!\times2!}{(n-3)!\times3!}=8$

$\Rightarrow \frac{(n-2)\times(n-3)!\times2}{(n-3)!\times6}=8\Rightarrow\frac{(n-2)}{3}=8$

$\Rightarrow (n-2)=24\Rightarrow n=26$

(d)

Given,

$^nP_r=110$

Again, $^nC_r=55$

We know that,

$^nP_r={}^nC_r\times r!$

$\Rightarrow 110=55*r!$

$\Rightarrow r!=\frac{110}{55}$

Space for learners:

$\Rightarrow r! = 2$

$Therefore, r = 2$

CHECK YOUR PROGRESS-II

15. Find the value of n if $^{n}p_4 = 30 * {}^{n}c_5$

16. If $^{n}C_6 : {}^{n-3}C_3 = 91 : 4$, find the value of n?

17. If $^{n}C_9 = {}^{n}C_8$, find $^{n}C_{17}$.

18. Verify each of the following statements:

(i) $^{5}c_2 = {}^{5}c_3$

(ii) $^{4}C_3 \times {}^{3}c_2 = {}^{12}c_6$

(iii) $^{4}C_2 + {}^{4}C_3 = {}^{8}c_5$

(iv) $^{10}c_2 + {}^{10}c_3 = {}^{11}c_3$

Example 3: A group consists of 4 girls and 7 boys. In how many ways can a team of 5 members be selected if the team has (i) no girl? (ii) at least one boy and one girl? (iii) at least 3 girls?

Solution:

(i) Since, the team will not include any girl, therefore, only boys are to be selected. 5 boys out of 7 boys can be selected in $^{7}C_5$ ways.

Therefore, the required number of ways $= {}^{7}C_5$

$$= \frac{7!}{(7-5)! \times 5!} = \frac{7!}{2! \times 5!}$$

$$= \frac{7 \times 6 \times 5!}{2 \times 5!}$$

$$= \frac{7 \times 6}{2} = 21$$

(ii) Since, at least one boy and one girl are to be there in every team. Therefore, the team can consist of

(a) 1 boy and 4 girls (b) 2 boys and 3 girls

(c) 3 boys and 2 girls (d) 4 boys and 1 girl.

1 boy and 4 girls can be selected in $^{7}C_1 \times {}^{4}C_4$ ways.

Space for learners:

2 boys and 3 girls can be selected in ${}^{7}C_2 \times {}^{4}C_3$ ways.

3 boys and 2 girls can be selected in ${}^{7}C_3 \times {}^{4}C_2$ ways.

4 boys and 1 girl can be selected in ${}^{7}C_4 \times {}^{4}C_1$ ways.

Therefore, the required number of ways = ${}^{7}C_1 \times {}^{4}C_4 + {}^{7}C_2 \times {}^{4}C_3 + {}^{7}C_3 \times {}^{4}C_2 + {}^{7}C_4 \times {}^{4}C_1$

$= 7 + 84 + 210 + 140$

$= 441$

(iii) Since, the team has to consist of at least 3 girls, the team can consist of

(a) 3 girls and 2 boys. Or (b) 4 girls and 1 boy.

Note that the team cannot have all 5 girls, because, the group has only 4 girls

3 girls and 2 boys can be selected in ${}^{4}C_3 \times {}^{7}C_2$ ways.

4 girls and 1 boy can be selected in ${}^{4}C_4 \times {}^{7}C_1$ ways

Therefore, the required number of ways = ${}^{4}C_3 \times {}^{7}C_2 + {}^{4}C_4 \times {}^{7}C_1$

= 84+7

= 91

***Example* 4**: A question paper consists of 10 questions divided into two parts A and B. Each part contains five questions. A candidate is required to attempt 6 questions in all of which at least 2 should be from part A and at least 2 from part B. In how many ways can the candidate select the questions if he can answer all questions equally well?

Solution: The candidate has to select six questions in all of which at least two should be from Part A and two should be from Part B. He can select questions in any of the following ways:

	Part A	Part B
(i)	2	4
(ii)	3	3

Space for learners:

(iii) 4 2

If the candidate follows choice (i), the number of ways in which he can do so is

$$^5C_2 \times {}^5C_4 = 10 \times 5 = 50$$

If the candidate follows choice (ii), the number of ways in which he can do so is

$$^5C_3 \times {}^5C_3 = 10 \times 10 = 100$$

Similarly, if the candidate follows choice (iii), then the number of ways in which he can do so is

$$^5C_4 \times {}^5C_2 = 5 \times 10 = 50$$

Therefore, the candidate can select the question in

$$50 + 100 + 50 = 200 \text{ ways}$$

Example5:

In how many ways can a selection of 4 persons be made from 10 persons such that one particular person is always (i) included (ii) excluded

Solution: This is the example of Restricted Combination.

(i) The number of ways of selecting 4 persons from 10 persons such that a particular person is always included is $= {}^9C_3$

$$= \frac{9!}{6! \times 3!} = \frac{9 \times 8 \times 7 \times 6!}{6! \times 6} = 84$$

(ii) The number of ways of selecting 4 persons from 10 persons such that a particular person is always excluded is $= {}^9C_4$

$$= \frac{9!}{5! \times 4!} = \frac{9 \times 8 \times 7 \times 6 \times 5!}{5! \times 4 \times 3 \times 2 \times 1} = 126$$

Example6: A committee of 5 members is to be formed from 6 male teachers and 4 female teachers. How many ways the committee be formed if there be at least one female teacher in the committee?

Solution:

The possible selections are as follows:

Space for learners:

1. $4c1 \times 6C4$

2. $4c2 \times 6C3$

3. $4c3 \times 6C2$

4. $4c4 \times 6C1$

Therefore, the total no of Selections

$^4c_1 \times {}^6C_4 + {}^4c_2 \times {}^6C_3 + {}^4c_3 \times {}^6C_2 + {}^4c_4 \times {}^6C_1$

$= \frac{4!}{3! \times 1!} \times \frac{6!}{4! \times 2!} + \frac{4!}{2! \times 2!} \times \frac{6!}{3! \times 3!} + \frac{4!}{1! \times 3!} \times \frac{6!}{4! \times 2!} + \frac{4!}{0! \times 4!} \times \frac{6!}{5! \times 1!}$

$= 4 \times \frac{6 \times 5}{2} + \frac{4 \times 3}{2} \times \frac{6 \times 5 \times 4}{3 \times 2 \times 1} + 4 \times \frac{6 \times 5}{2} + 1 \times 6 = 60 + 6 \times 20 +$

$60 + 6 = 246$

1.10 SUMMING UP

- Two integers a and b are congruent modulo n if they each have the same remainder on division by n.
- If $a \equiv b \pmod{n}$, and m is a positive integer, then $a^m \equiv b^m \pmod{n}$ can be termed as the power rule of congruence.
- The least residue of a modulo n is the remainder r that you obtain when you divide a by n.
- Addition, subtraction and multiplication are often simpler to carry out in modular arithmetic than they are normally, because you can use congruences to reduce large numbers to small numbers.
- Permutation is an arrangement in a definite order of a number of objects taken some or all at a time.
- The number of permutations of n different objects taken r at a time, where repetition is allowed, is n^r
- Circular Permutation is the total number of ways in which n distinct objects can be arranged around a fix circle.
- Permutation with some specific restrictions is called restricted permutations.

Space for learners:

- A combination is a selection of all or part of a set of object without regard to the order in which objects are selected. If there are certain restrictions on Combination like a particular object occurring always and occurring never, then it is called Restricted Combination.

Space for learners:

1.11 ANSWERS TO CHECK YOUR PROGRESS

1. $(a) True$

$(b) False$

$(c) True$

(d) True

(e) True

(f) False

2. n-=52, 56, 60,……….. .96

3. X=7, 24, 41,58,75,92

4. (a) Since, $17 = 1 \times 10 + 7$, the least residue is 7.

(b) Since, $50 = 5 \times 10 + 0$, the least residue is 0.

(c) Since, $6 = 0 \times 10 + 6$, the least residue is 6.

(d) Since, $-1 = (-1) \times 10 + 9$, the least residue is 9.

(e) Since, $-38 = (-4) \times 10 + 2$, the least residue is 2.

5. (a) $3 \times 6 \equiv 18 \equiv 4 \pmod 7$ So the least residue is 4.

(b) $22 \times 29 \equiv 1 \times 1 \equiv 1 \pmod 7$,So the least residue is 1

(c) $51 \times 74 \equiv 2 \times 4 \equiv 8 \equiv 1 \pmod 7$,so least residue is 1

6. We have, $32 \equiv -9 \pmod{41}$

$\Rightarrow 2^5 \equiv -9 (mod\ 41)$

$\Rightarrow (2^5)^2 \equiv (-9)^2 (mod\ 41)$ $[By\ Power\ rule] Again,\quad (-9)2 = 81 \equiv -1\ (mod\ 41)$

$i.e., (2^5)^2 \equiv (-1)(mod\ 41)$

$Similarly, \{(2^5)^2\}^2 \equiv (-1)^2 (mod\ 41)[By\ power\ rule]$

$i.e., 2^{20} \equiv 1(mod\ 41)$

7. We notice that $3^4 = 81 \equiv 1 \pmod{80}$.

   That is, we have $3^4 \equiv 1 \pmod{80}$

By power rule of Congruence,

$(3^4)^{1388} \equiv 1 \pmod{80}$. [$since$, $3^{5555} = (3^4)^{1388} . 3^3$]

Therefore, $(3^4)^{1388} . 3^3 \equiv 3^3 \pmod{80}$.

Therefore, $3^{5555} \equiv 27 \pmod{80}$.

So, the required remainder is 27

8. (a) (i) 720

   (ii) 5040

   (iii) 5046

   (iv) 17280

8. (b) (i) False

   (ii) False

   (iii) False

9. (a) 32760

   (b) 55440

   (c) 1

10. n=5

11. r=5

12. r=8, 3

13.24

14. 120

Space for learners:

15. 8

16. 15

17. 1

18. (i) True

    (ii) False

    (iii) False

    (iv) True

Space for learners:

1.12 POSSIBLE QUESTIONS

1. Find the least residue of 1492 (mod 4), (mod 10) .
2. Does $33x \equiv 12 \pmod 6$ imply $11x \equiv 4 \pmod 6$?Why ?
3. What is the remainder when 2^{50} *is divided by* 7?
4. Find the least residue of 11^6 modulo 9.
5. Check whether 4 and 6 are congruent modulo 5 or not?
6. Every integer a is congruent modulo 1 to every integer b. State True or False.
7. If ${}^nP_r = {}^nP_{r+1}$ and ${}^nC_r = {}^nC_{r-1}$,find the value of n and r.
8. If ${}^nC_{r-1} = 36, {}^nC_r = 84$ and ${}^nC_{r+1} = 126$,find the value of n and r?
9. How many numbers less than 1000 can be formed using the digits 0,1,2,3,4,5,6 if repetition of digits being allowed?
10. In how many ways can 3 boys and 4 girls be arranged so that no two boys will be side by side?
11. Find the number of numbers greater than 4000 which can be formed using the digits 0, 2, 4, 6, 8 without repetition.
12. 9 different letters of an alphabet are given. Find the number of 4 letter words that can be formed using these 9 letters which have (i) no letter repeated (ii) at least one letter repeated.
13. Find the number of ways of arranging the letters of the word.

(a) INDEPENDENCE (b) MATHEMATICS

14. In how many ways 6 books be put into 5 bags?
15. How many ways 3 students can be selected from 50 students?
16. In how many ways can the letters in the word ENGINEERING is arranged such that no two E's are together?
17. A cricket team consisting of 11 players is to be selected from 6 bowlers and 8 batsmen including at least 4 bowlers. In how many ways can this be done?
18. There are 5 black and 6 red balls in a bag. How many selections can be made taking 2 black and 3 red balls?

1.12 REFERENCES AND SUGGESTED READINGS

- Permutation and Combination by Ramesh Chandra
- http:// www.wikipedia.org
- http://mathworld.wolfram.com

Space for learners:

UNIT 2: SETS

Space for learners:

Unit Structure:

2.1 INTRODUCTION

In mathematics, a set is a collection of elements. The elements that make up a set can be any kind of mathematical objects: numbers, symbols, points in space, lines, other geometrical shapes, variables, or even other sets. The set with no element is the empty set; a set with a single element is a singleton. A set may have a finite number of elements or be an infinite set. Two sets are equal if and only if they have precisely the same elements.

Sets are ubiquitous in modern mathematics. Indeed, set theory, more specifically Zermelo–Fraenkel set theory, has been the standard way to provide rigorous foundations for all branches of mathematics since the first half of the 20th century.

The concept of a set emerged in mathematics at the end of the 19th century. The German word for set, Menge, was coined by Bernard Bolzano in his work Paradoxes of the Infinite.

A set is a gathering together into a whole of definite, distinct objects of our perception or our thought—which are called elements of the set.

Bertrand Russell called a set a class: "When mathematicians deal with what they call a manifold, aggregate, Menge, ensemble, or some equivalent name, it is common, especially where the number of terms involved is finite, to regard the object in question (which is in fact a class) as defined by the enumeration of its terms, and as consisting possibly of a single term, which is in that case is the class."

Space for learners:

2.2 UNIT OBJECTIVES

After going through this unit, you will be able to:

- idea of set
- definition of sets
- representation sets
- operations of sets
- questions and answers for your progress

2.3 DEFINITIONS OF SETS

Set - Definition

A set is an unordered collection of different elements. A set can be written explicitly by listing its elements using set bracket. If the order of the elements is changed or any element of a set is repeated, it does not make any changes in the set.

Some Example of Sets

- A set of all positive integers
- A set of all the planets in the solar system
- A set of all the states in India
- A set of all the lowercase letters of the alphabet

Representation of a Set

Sets can be represented in two ways −

- Roster or Tabular Form
- Set Builder Notation

Roster or Tabular Form

The set is represented by listing all the elements comprising it. The elements are enclosed within braces and separated by commas.

Space for learners:

Example 1 Set of vowels in English alphabet, A={a,e,i,o,u}.

Example 2 Set of odd numbers less than 10, B={1,3,5,7,9}.

Set Builder Notation

The set is defined by specifying a property that elements of the set have in common. The set is described as A={x:p(x)}A={x:p(x)}

Example 1 The set {a,e,i,o,u}{a,e,i,o,u} is written as

A={x:x is a vowel in English alphabet}.

Example 2 The set {1,3,5,7,9} is written as

B={x:1≤x<10 and (x%2)≠0}.

If an element x is a member of any set S, it is denoted by x∈S and if an element y is not a member of set S, it is denoted by y∉S.

Example If S={1,1.2,1.7,2},1∈S, but 1.5∉S.

Some Important Sets

N − the set of all natural numbers = {1,2,3,4,.....}

Z − the set of all integers = {.....,−3,−2,−1,0,1,2,3,.....}

Z+ − the set of all positive integers

Q − the set of all rational numbers

R − the set of all real numbers

W − the set of all whole numbers

Cardinality of a Set

Cardinality of a set S, denoted by |S|, is the number of elements of the set. The number is also referred as the cardinal number. If a set has an infinite number of elements, its cardinality is ∞.

Example − |{1,4,3,5}|=4,|{1,2,3,4,5,…}|=∞|. If there are two sets X and Y,

- |X|=|Y| denotes two sets X and Y having same cardinality. It occurs when the number of elements in X is exactly equal to the number of elements in Y. In this case, there exists a bijective function 'f' from X to Y.
- |X|≤|Y| denotes that set X's cardinality is less than or equal to set Y's cardinality. It occurs when number of elements in X is

less than or equal to that of Y. Here, there exists an injective function ‘f’ from X to Y.

- $|X|<|Y|$ denotes that set X’s cardinality is less than set Y’s cardinality. It occurs when number of elements in X is less than that of Y. Here, the function ‘f’ from X to Y is injective function but not bijective.
- If $|X|\leq|Y|$ and $|X|\geq|Y|$ then $|X|=|Y|$. The sets X and Y are commonly referred as equivalent sets.

Types of Sets

Sets can be classified into many types. Some of which are finite, infinite, subset, universal, proper, singleton set, etc.

Finite Set

A set which contains a definite number of elements is called a finite set.

Example − $S=\{x|x\in N \text{ and } 70>x>50\}$

Infinite Set

A set which contains infinite number of elements is called an infinite set.

Example − $S=\{x|x\in N \text{ and } x>10\}$

Subset

A set X is a subset of set Y (Written as $X\subseteq Y$) if every element of X is an element of set Y.

Example 1 Let, $X=\{1,2,3,4,5,6\}$ and $Y=\{1,2\}$. Here set Y is a subset of set X as all the elements of set Y is in set X. Hence, we can write $Y\subseteq X$.

Example 2 − Let, $X=\{1,2,3\}$ and $Y=\{1,2,3\}$. Here set Y is a subset (Not a proper subset) of set X as all the elements of set Y is in set X. Hence, we can write $Y\subseteq X$.

Proper Subset

The term “proper subset” can be defined as “subset of but not equal to”. A Set X is a proper subset of set Y (Written as $X\subset Y$) if every element of X is an element of set Y and $|X|<|Y|$.

Space for learners:

Example − Let, $X=\{1,2,3,4,5,6\}$ and $Y=\{1,2\}$. Here set $Y \subset X$ since all elements in Y are contained in X too and X has at least one element is more than set Y.

Universal Set

It is a collection of all elements in a particular context or application. All the sets in that context or application are essentially subsets of this universal set. Universal sets are represented as U.

Example: We may define U as the set of all animals on earth. In this case, set of all mammals is a subset of U, set of all fishes is a subset of U, set of all insects is a subset of U, and so on.

Empty Set or Null Set

An empty set contains no elements. It is denoted by $\emptyset$. As the number of elements in an empty set is finite, empty set is a finite set. The cardinality of empty set or null set is zero.

Example − $S=\{x|x \in NS=\{x|x \in N \text{ and } 7<x<8\}=\emptyset$

Singleton Set or Unit Set

Singleton set or unit set contains only one element. A singleton set is denoted by $\{s\}$.

Example − $S=\{x|x \in N, 7<x<9\}= \{8\}$

Equal Set

If two sets contain the same elements they are said to be equal.

Example − If $A=\{1,2,6\}$ and $B=\{6,1,2\}$, they are equal as every element of set A is an element of set B and every element of set B is an element of set A.

Equivalent Set

If the cardinalities of two sets are same, they are called equivalent sets.

Example If $A=\{1,2,6\}$ and $B=\{16,17,22\}$, they are equivalent as cardinality of A is equal to the cardinality of B. i.e. $|A|=|B|=3$.

Disjoint Set

Two sets A and B are called disjoint sets if they do not have even one element in common. Therefore, disjoint sets have the following properties –

Space for learners:

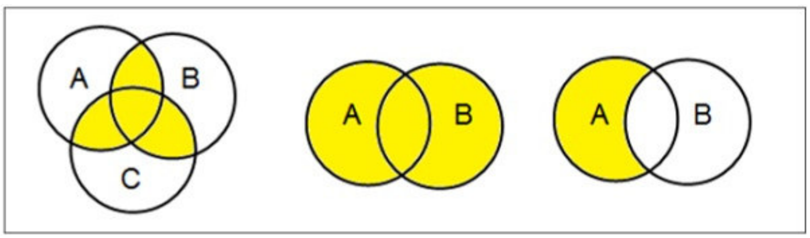
- $n(A \cap B) = \emptyset$
- $n(A \cup B) = n(A) + n(B)$

Example Let, A={1,2,6} and B={7,9,14}, there is not a single common element, hence these sets are overlapping sets.

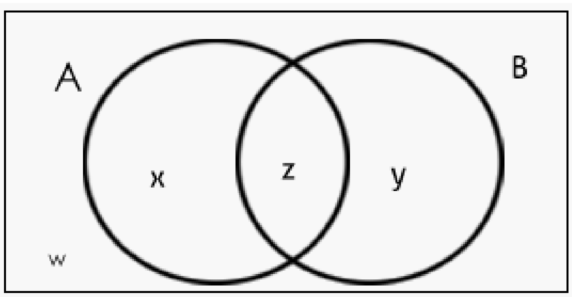
Venn Diagrams

Venn diagram, invented in 1880 by John Venn, is a schematic diagram that shows all possible logical relations between different mathematical sets.

Examples



Venn Diagram in case of two elements



Where;

X = number of elements that belong to set A only
Y = number of elements that belong to set B only
Z = number of elements that belong to set A and B both $(A \cap B)$
W = number of elements that belong to none of the sets A or B

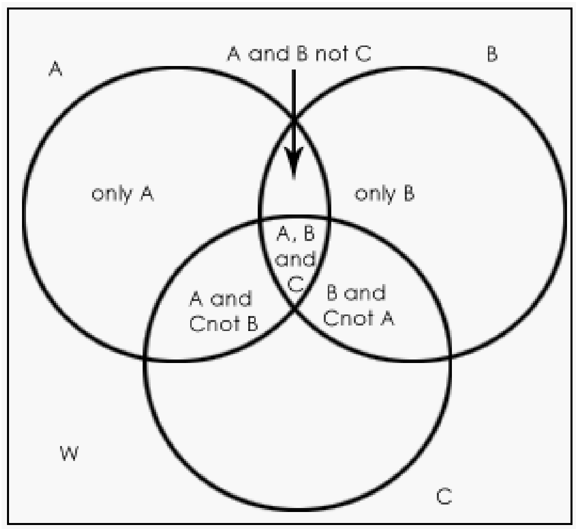
From the above figure, it is clear that

$n(A) = x + z$;
$n(B) = y + z$;
$n(A \cap B) = z$;
$n(A \cup B) = x + y + z$.

Total number of elements = $x + y + z + w$

Space for learners:

Venn Diagram in case of three elements



Where,

W = number of elements that belong to none of the sets A, B or C

Example 1: In a college, 200 students are randomly selected. 140 like tea, 120 like coffee and 80 like both tea and coffee.

How many students like only tea?

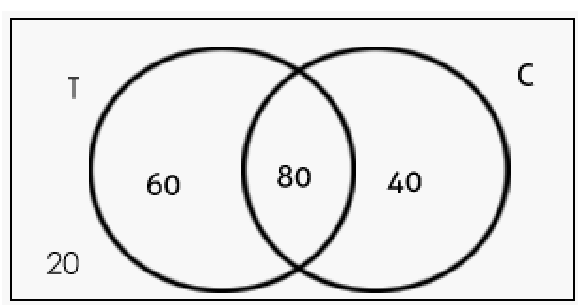
How many students like only coffee?

How many students like neither tea nor coffee?

How many students like only one of tea or coffee?

How many students like at least one of the beverages?

Solution: The given information may be represented by the following Venn diagram, where T = tea and C = coffee.



Number of students who like only tea = 60

Space for learners:

Number of students who like only coffee = 40

Number of students who like neither tea nor coffee = 20

Number of students who like only one of tea or coffee = 60 + 40 = 100

Number of students who like at least one of tea or coffee = n (only Tea) + n (only coffee) + n (both Tea & coffee) = 60 + 40 + 80 = 180

Example 2: In a survey of 500 students of a college, it was found that 49% liked watching football, 53% liked watching hockey and 62% liked watching basketball. Also, 27% liked watching football and hockey both, 29% liked watching basketball and hockey both and 28% liked watching football and basket ball both. 5% liked watching none of these games.

How many students like watching all the three games?

Find the ratio of number of students who like watching only football to those who like watching only hockey.

Find the number of students who like watching only one of the three given games.

Find the number of students who like watching at least two of the given games.

Solution:

n(F) = percentage of students who like watching football = 49%

n(H) = percentage of students who like watching hockey = 53%

n(B)= percentage of students who like watching basketball = 62%

$n(F \cap H) = 27\%$; $n(B \cap H) = 29\%$; $n(F \cap B) = 28\%$

Since 5% like watching none of the given games so, $n(F \cup H \cup B) = 95\%$.

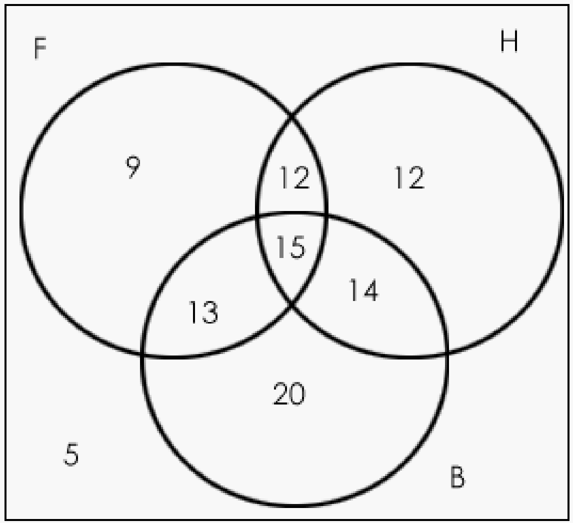
Now applying the basic formula,

$95\% = 49\% + 53\% + 62\% - 27\% - 29\% - 28\% + n(F \cap H \cap B)$

Solving, you get $n(F \cap H \cap B) = 15\%$.

Now, make the Venn diagram as per the information given.

Space for learners:



Space for learners:

Note: All values in the Venn diagram are in percentage.

Number of students who like watching all the three games = 15 % of 500 = 75.

Ratio of the number of students who like only football to those who like only hockey = (9% of 500)/(12% of 500) = 9/12 = 3:4.

The number of students who like watching only one of the three given games = (9% + 12% + 20%) of 500 = 205

The number of students who like watching at least two of the given games=(number of students who like watching only two of the games) +(number of students who like watching all the three games)= (12 + 13 + 14 + 15)% i.e. 54% of 500 = 270.

CHECK YOUR PROGRESS-I

Q1 :Which of the following are sets? Justify our answer.

(i) The collection of all months of a year beginning with the letter J.

(ii) The collection of ten most talented writers of India.

(iii) A team of eleven best-cricket batsmen of the world.

(iv) The collection of all boys in your class.

(v) The collection of all natural numbers less than 100.

(vi) A collection of novels written by the writer Munshi Prem Chand.

(vii) The collection of all even integers.

(viii) The collection of questions in this Chapter.

(ix) A collection of most dangerous animals of the world.

Q2. Let A = {1, 2, 3, 4, 5, 6}. Insert the appropriate symbol or in the blank spaces:

(i) 5…A (ii) 8…A (iii) 0…A

(iv) 4…A (v) 2…A (vi) 10…A

Q3 :Write the following sets in the set-builder form:

(i) (3, 6, 9, 12) (ii) {2, 4, 8, 16, 32}

(iii) {5, 25, 125, 625} (iv) {2, 4, 6 …}

(v) {1, 4, 9 … 100}

Q4. Which of the following are examples of the null set

(i) Set of odd natural numbers divisible by 2

(ii) Set of even prime numbers

(iii) {x:x is a natural numbers, $x < 5$ and $x > 7$ }

(iv) {y:y is a point common to any two parallel lines}

Q5. Which of the following sets are finite or infinite

(i) The set of months of a year

(ii) {1, 2, 3 ...}

(iii) {1, 2, 3 ... 99, 100}

(iv) The set of positive integers greater than 100

(v) The set of prime numbers less than 99

Q6. State whether each of the following set is finite or infinite:

(i) The set of lines which are parallel to the x-axis

(ii) The set of letters in the English alphabet

(iii) The set of numbers which are multiple of 5

(iv) The set of animals living on the earth

(v) The set of circles passing through the origin (0, 0)

Space for learners:

Q7. In the following, state whether A = B or not:

(i) A = {a, b, c, d}; B = {d, c, b, a}

(ii) A = {4, 8, 12, 16}; B = {8, 4, 16, 18}

(iii) A = {2, 4, 6, 8, 10}; B = {x: x is positive even integer and x ≤ 10} (iv) A = {x: x is a multiple of 10}; B

= {10, 15, 20, 25, 30 ...}

Q8. Are the following pair of sets equal? Give reasons.

(i) A = {2, 3}; B = {x: x is solution of $x^2 + 5x + 6 = 0$}

(ii) A = {x: x is a letter in the word FOLLOW}; B = {y: y is a letter in the word WOLF}

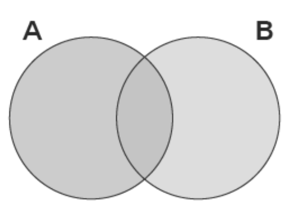
Space for learners:

2.4 OPERATIONS OF SETS

A set is defined as a collection of objects. Each object inside a set is called an 'Element'. A set can be represented in three forms. They are statement form, roster form, and set builder form. Set operations are the operations that are applied on two more sets to develop a relationship between them. There are four main kinds of set operations which are:

1. Union of sets
2. Intersection of sets
3. Complement of a set
4. Difference between sets/Relative Complement

Before we move on to discuss the various set operations, let us recall the concept of Venn diagrams as it is important in understanding the operations on sets. A Venn diagram is a logical diagram that shows the possible relationship between different finite sets. It looks as shown below.



Basic Set Operations:

Space for learners:

Now that we know the concept of a set and Venn diagram, let us discuss each set operation one by one in detail. The various set operations are:

Union of Sets

For two given sets A and B, $A \cup B$ (read as A union B) is the set of distinct elements that belong to set A and B or both. The number of elements in $A \cup B$ is given by $n(A \cup B) = n(A) + n(B) - n(A \cap B)$, where $n(X)$ is the number of elements in set X. To understand this set operation of the union of sets better, let us consider an example: If $A = \{1, 2, 3, 4\}$ and $B = \{4, 5, 6, 7\}$, then the union of A and B is given by $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$.

Intersection of Sets

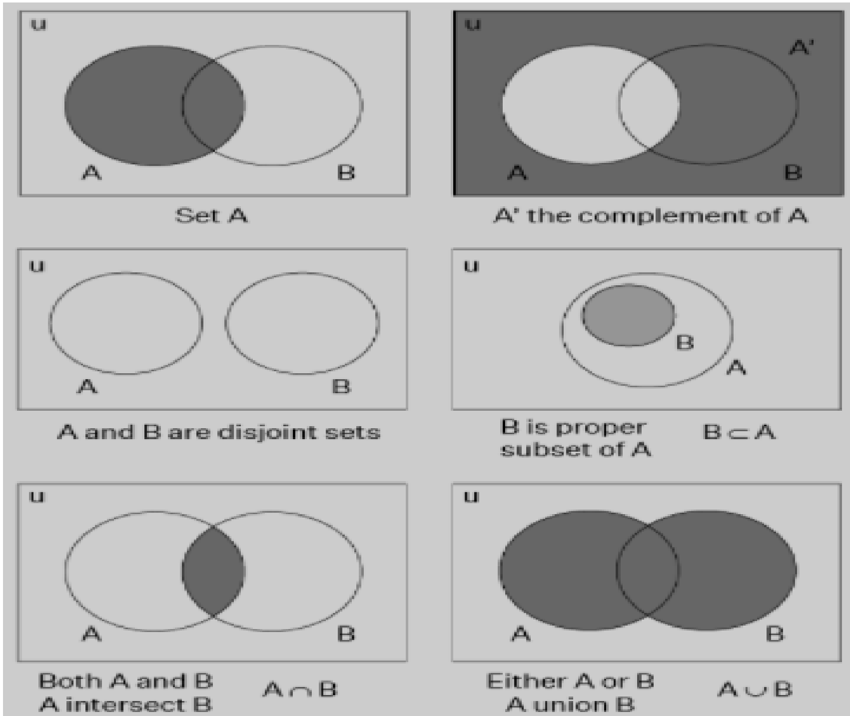
For two given sets A and B, $A \cap B$ (read as A intersection B) is the set of common elements that belong to set A and B. The number of elements in $A \cap B$ is given by $n(A \cap B) = n(A)+n(B)-n(A \cup B)$, where $n(X)$ is the number of elements in set X. To understand this set operation of the intersection of sets better, let us consider an example: If $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 7\}$, then the intersection of A and B is given by $A \cap B = \{3, 4\}$.

Set Difference

The set operation difference between sets implies subtracting the elements from a set which is similar to the concept of the difference between numbers. The difference between sets A and B denoted as $A - B$ lists all the elements that are in set A but not in set B. To understand this set operation of set difference better, let us consider an example: If $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 7\}$, then the difference between sets A and B is given by $A - B = \{1, 2\}$.

Complement of Sets

The complement of a set A denoted as A' or Ac (read as A complement) is defined as the set of all the elements in the given universal set(U) that are not present in set A. To understand this set operation of complement of sets better, let us consider an example: If $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and $A = \{1, 2, 3, 4\}$, then the complement of set A is given by $A' = \{5, 6, 7, 8, 9\}$.



The above image shows various set operations with the help of Venn diagrams which makes it clearer. When the elements of one set B completely lie in the other set A, then B is said to be a proper subset of A. When two sets have no elements in common, then they are said to be disjoint sets. Now, let us explore the properties of the set operations that we discussed.

Properties of Set Operations:

The properties of set operations are similar to the properties of fundamental operations on numbers. The important properties on set operations are stated below:

Commutative Law - For any two given sets A and B, the commutative property is defined as,

$A \cup B = B \cup A$

This means that the set operation union of two sets is commutative.

$A \cap B = B \cap A$

This means that the set operation intersection of two sets is commutative.

Associative Law - For any three given sets A, B and C the associative property is defined as,

Space for learners:

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

This means the set operation union of sets is associative.

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

This means the set operation intersection of sets is associative.

De-Morgan's Law - The law states that for any two sets A and B, we have $(A \cup B)' = A' \cap B'$ and $(A \cap B)' = A' \cup B'$

$A \cup A = A$

$A \cap A = A$

$A \cap \emptyset = \emptyset$

$A \cup \emptyset = A$

$A \cap B \subseteq A$

$A \cup B \subseteq A$

Important Notes on Set Operations:

Set operation formula for union of sets is $n(A \cup B) = n(A) + n(B) - n(A \cap B)$ and set operation formula for intersection of sets is $n(A \cap B) = n(A)+n(B)-n(A \cup B)$.

The union of any set with the universal set gives the universal set and the intersection of any set A with the universal set gives the set A.

Union, intersection, difference, and complement are the various operations on sets.

The complement of a universal set is an empty set $U' = \phi$. The complement of an empty set is a universal set $\phi' = U$.

CHECK YOUR PROGRESS-II

9. Let A={1,2,3,4} and let B={3,4,5,6} . Then: find $A \cap B$, $A \cup B$ $A-B$ and A^C

10. Let A={y,z} and let B={x,y,z} . Then: find $A \cap B$, $A \cup B$, $A-B$, and A^C

11. If A = {2, 3, 4, 5} B = {4, 5, 6, 7} C = {6, 7, 8, 9} D = {8, 9, 10, 11}, find

Space for learners:

(a) $A \cup B$

(b) $A \cup C$

(c) $B \cup C$

(d) $B \cup D$

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

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

(g) $B \cup (C \cup D)$

12. If $A = \{4, 7, 10, 13, 16, 19, 22\}$ $B = \{5, 9, 13, 17, 20\}$

$C = \{3, 5, 7, 9, 11, 13, 15, 17\}$ $D = \{6, 11, 16, 21\}$ then find

(a) A - C

(b) D - A

(c) D - B

(d) A - D

(e) B - C

(f) C - D

(g) B - A

(h) B - D

(i) D - C

(j) A - B

(k) C - B

(l) C - A

Space for learners:

2.5 SUMMING UP

- A set can be written explicitly by listing its elements using set bracket. If the order of the elements is changed or any element of a set is repeated, it does not make any changes in the set.
- Sets can be represented in two ways − Roster or Tabular Form, Set Builder Notation

- Cardinality of a set S, denoted by |S|, is the number of elements (cardinal number) of the set. If a set has an infinite number of elements, its cardinality is ∞.
- A set which contains a definite number of elements is called a finite set. A set which contains infinite number of elements is called an infinite set.
- A set X is a subset of set Y (Written as X⊆Y) if every element of X is an element of set Y. A Set X is a proper subset of set Y (Written as X⊂Y) if every element of X is an element of set Y and |X|<|Y|.
- Universal set is a collection of all elements in a particular context or application. The cardinality of empty set or null set is zero. Singleton set or unit set contains only one element.
- If two sets contain the same elements, they are said to be equal. If the cardinalities of two sets are same, they are called equivalent sets. Disjoint sets do not have even one element in common.

5. Set operations are the operations applied on two more sets to develop a relationship between them. There are four main kinds of set operations: Union of sets, Intersection of sets, Complement of a set, Difference between sets/Relative Complement.

2.6 ANSWERS TO CHECK YOUR PROGRESS

Answer 1:

(i) The collection of all months of a year beginning with the letter J is a well-defined collection of objects

because one can definitely identify a month that belongs to this collection.

Hence, this collection is a set.

(ii) The collection of ten most talented writers of India is not a well-defined collection because the criteria for

determining a writer's talent may vary from person to person.

Hence, this collection is not a set.

Space for learners:

(iii) A team of eleven best cricket batsmen of the world is not a well-defined collection because the criteria for

determining a batsman's talent may vary from person to person.

Hence, this collection is not a set.

(iv) The collection of all boys in your class is a well-defined collection because you can definitely identify a boy

who belongs to this collection.

Hence, this collection is a set.

(v) The collection of all natural numbers less than 100 is a well-defined collection because one can definitely

identify a number that belongs to this collection.

Hence, this collection is a set.

(vi) A collection of novels written by the writer Munshi Prem Chand is a well-defined collection because one can

definitely identify a book that belongs to this collection.

Hence, this collection is a set.

(vii) The collection of all even integers is a well-defined collection because one can definitely identify an even

integer that belongs to this collection.

Hence, this collection is a set.

(viii) The collection of questions in this chapter is a well-defined collection because one can definitely identify a

question that belongs to this chapter.

Hence, this collection is a set.

(ix) The collection of most dangerous animals of the world is not a well-defined collection because the criteria

for determining the dangerousness of an animal can vary from person to person.

Hence, this collection is not a set.

Answer 2:

(i) 5 A

(ii) 8 A

Space for learners:

(iii) 0 A

(iv) 4 A

(v) 2 A

(vi) 10 A

Answer 3:

(i) {3, 6, 9, 12} = {x: x = 3n, n N and 1 ≤ n ≤ 4}

(ii) {2, 4, 8, 16, 32}

It can be seen that 2 = 21, 4 = 22, 8 = 23, 16 = 24, and 32 = 25.

{2, 4, 8, 16, 32} = {x: x = 2n, n N and 1 ≤ n ≤ 5}

(iii) {5, 25, 125, 625}

It can be seen that 5 = 51, 25 = 52, 125 = 53, and 625 = 54.

{5, 25, 125, 625} = {x: x = 5n, n N and 1 ≤ n ≤ 4}

(iv) {2, 4, 6 …}

It is a set of all even natural numbers.

{2, 4, 6 …} = {x: x is an even natural number}

(v) {1, 4, 9 … 100}

It can be seen that 1 = 12, 4 = 22, 9 = 32 …100 = 102.

{1, 4, 9… 100} = {x: x = n2, n N and 1 ≤ n ≤ 10}

Answer 4:

(i) A set of odd natural numbers divisible by 2 is a null set because no odd number is divisible by 2.

(ii) A set of even prime numbers is not a null set because 2 is an even prime number.

(iii) {x: x is a natural number, x < 5 and x > 7} is a null set because a number cannot be simultaneously less

than 5 and greater than 7.

(iv) {y: y is a point common to any two parallel lines} is a null set because parallel lines do not intersect. Hence,

they have no common point.

<u>Space for learners:</u>

Answer 5:

(i) The set of months of a year is a finite set because it has 12 elements.

(ii) {1, 2, 3 …} is an infinite set as it has infinite number of natural numbers.

(iii) {1, 2, 3 …99, 100} is a finite set because the numbers from 1 to 100 are finite in number.

(iv) The set of positive integers greater than 100 is an infinite set because positive integers greater than 100 are

infinite in number.

(v) The set of prime numbers less than 99 is a finite set because prime numbers less than 99 are finite in number.

Answer 6:

(i) The set of lines which are parallel to the x-axis is an infinite set because lines parallel to the x-axis are infinite

in number.

(ii) The set of letters in the English alphabet is a finite set because it has 26 elements.

(iii) The set of numbers which are multiple of 5 is an infinite set because multiples of 5 are infinite in number.

(iv) The set of animals living on the earth is a finite set because the number of animals living on the earth is finite

(although it is quite a big number).

(v) The set of circles passing through the origin (0, 0) is an infinite set because infinite number of circles can pass

through the origin.

Answer 7:

(i) A = {a, b, c, d}; B = {d, c, b, a}

The order in which the elements of a set are listed is not significant.

A = B

(ii) A = {4, 8, 12, 16}; B = {8, 4, 16, 18} It can be seen that 12 A but 12 B.

A ≠ B

Space for learners:

(iii) $A = \{2, 4, 6, 8, 10\}$

$B = \{x: x$ is a positive even integer and $x \leq 10\}$

$= \{2, 4, 6, 8, 10\}$

Therefore, $A = B$

Answer 8:

(i) $A = \{2, 3\}$; $B = \{x: x$ is a solution of $x2 + 5x + 6 = 0\}$

The equation $x2 + 5x + 6 = 0$ can be solved as:

$x(x + 3) + 2(x + 3) = 0$ $(x + 2)(x + 3) = 0$

$x = -2$ or $x = -3$

$A = \{2, 3\}$; $B = \{-2, -3\}$

$A \neq B$

(ii) $A = \{x: x$ is a letter in the word FOLLOW$\} = \{F, O, L, W\}$

$B = \{y: y$ is a letter in the word WOLF$\} = \{W, O, L, F\}$

The order in which the elements of a set are listed is not significant.

$A = B$

Answer 9:

$A \cap B=\{3,4\}$

$A \cup B=\{1,2,3,4,5,6\}$

$A-B=\{1,2\}$

$A^C=\{$all real numbers except 1,2,3 and 4$\}$

Answer 10: $A \cap B=\{y,z\}$ $A \cup B=\{x,y,z\}$ $A-B=\emptyset$ $A^c=\{$everything except y and z$\}$

Answer 11:

(a) {2, 3, 4, 5, 6, 7}

(b) {2, 3, 4, 5, 6, 7, 8, 9}

(c) {4, 5, 6, 7, 8, 9}

(d) {4, 5, 6, 7, 8, 9, 10, 11}

(e) {2, 3, 4, 5, 6, 7, 8, 9}

(f) {2, 3, 4, 5, 6, 7, 8, 9}

(g) {4, 5, 6, 7, 8, 9, 10, 11}

Space for learners:

Answer 12:

(a) {4, 10, 16, 19, 22}

(b) {6, 11, 21}

(c) {6, 11, 16, 21}

(d) {4, 7, 10, 13, 19, 22}

(e) {20}

(f) {3, 5, 7, 9, 13, 15, 17}

(g) {5, 19, 17, 20}

(h) {5, 9, 13, 17, 20}

(i) {6, 16, 21}

(j) {4, 7, 10, 16, 19, 22}

(k) {3, 7, 11, 15}

(l) {3, 5, 9 11, 15, 17}

2.7 POSSIBLE QUESTIONS

1. If A = {2, 3, 4, 5} B = {4, 5, 6, 7} C = {6, 7, 8, 9}

D = {8, 9, 10, 11}, find

(a) $A \cup B$

(b) $A \cup C$

(c) $B \cup C$

(d) $B \cup D$

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

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

(g) $B \cup (C \cup D)$

2. If A = {4, 6, 8, 10, 12} B = {8, 10, 12, 14} C = {12, 14, 16} D = {16, 18}, find

(a) $A \cap B$

(b) $B \cap C$

(c) $A \cap (C \cap D)$

(d) $A \cap C$

Space for learners:

(e) $B \cap D$

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

(g) $A \cap (B \cup D)$

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

(i) $(A \cup D) \cap (B \cup C)$

3. If $A = \{4, 7, 10, 13, 16, 19, 22\}$ $B = \{5, 9, 13, 17, 20\}$

$C = \{3, 5, 7, 9, 11, 13, 15, 17\}$ $D = \{6, 11, 16, 21\}$ then find

(a) A - C

(b) D - A

(c) D - B

(d) A - D

(e) B - C

(f) C - D

(g) B - A

(h) B - D

(i) D - C

(j) A - B

(k) C - B

(l) C - A

4. If A and B are two sets such that $A \subset B$, then what is $A \cup B$?

5. Find the union, intersection and the difference (A - B) of the following pairs of sets.

(a) A = The set of all letters of the word FEAST

B = The set of all letters of the word TASTE

(b) $A = \{x : x \in W, 0 < x \leq 7\}$

$B = \{x : x \in W, 4 < x < 9\}$

(c) $A = \{x \mid x \in N, x \text{ is a factor of } 12\}$

$B = \{x \mid x \in N, x \text{ is a multiple of } 2, x < 12\}$

(d) A = The set of all even numbers less than 12

Space for learners:

B = The set of all odd numbers less than 11

(e) A = {x : x ∈ I, -2 < x < 2}

B = {x : x ∈ I, -1 < x < 4}

(f) A = {a, l, m, n, p}

B = {q, r, l, a, s, n}

6. Let X = {2, 4, 5, 6}   Y = {3, 4, 7, 8}   Z = {5, 6, 7, 8}, find

(a) (X - Y) ∪ (Y - X)

(b) (X - Y) ∩ (Y - X)

(c) (Y - Z) ∪ (Z - Y)

(d) (Y - Z) ∩ (Z - Y)

7. Let ξ = {1, 2, 3, 4, 5, 6, 7} and A = {1, 2, 3, 4, 5} B = {2, 5, 7} show that

(a) (A ∪ B)' = A' ∩ B'

(b) (A ∩ B)' = A' ∪ B'

(c) (A ∩ B) = B ∩ A

(d) (A ∪ B) = B ∪ A

8. Let P = {a, b, c, d}   Q = {b, d, f}   R = {a, c, e} verify that

(a) (P ∪ Q) ∪ R = P ∪ (Q ∪ R)

(b) (P ∩ Q) ∩ R = P ∩ (Q ∩ R)

2.8 REFERENCES AND SUGGESTED READINGS

- Descriptive Set Theory by David Marker.
- Set Theory by Burak Kaya
- Set Theory Some Basics and A Glimpse Of Some Advanced Techniques
- Lectures On Set Theory
- Set Theory by Anush Tserunyan
- An Introduction To Set Theory
- Set Theory for Computer Science
- The Axioms of Set Theory.

Space for learners:

UNIT 3: RELATIONS

Space for learners:

Unit Structure:

3.1 INTRODUCTION

In mathematics, a binary relation over sets X and Y is a subset of the Cartesian product X × Y; that is, it is a set of ordered pairs (x, y) consisting of elements x in X and y in Y. It encodes the common concept of relation: an element x is related to an element y, if and only if the pair (x, y) belongs to the set of ordered pairs that defines the binary relation. A binary relation is the most studied special case n = 2 of an n-ary relation over sets X_1, ..., X_n, which is a subset of the Cartesian product $X_1 \times ... \times X_n$.[1][2]

An example of a binary relation is the "divides" relation over the set of prime numbers {\displaystyle \mathbb {P} }\mathbb {P} and the set of integers {\displaystyle \mathbb {Z} }\mathbb {Z} , in which each prime p is related to each integer z that is a multiple of p, but not to an integer that is not a multiple of p. In this relation, for instance, the prime number 2 is related to numbers such as −4, 0, 6, 10, but not to 1 or 9, just as the prime number 3 is related to 0, 6, and 9, but not to 4 or 13.

Binary relations are used in many branches of mathematics to model a wide variety of concepts. These include, among others:

the "is greater than", "is equal to", and "divides" relations in arithmetic;

the "is congruent to" relation in geometry;

the "is adjacent to" relation in graph theory;

the "is orthogonal to" relation in linear algebra.

A function may be defined as a special kind of binary relation. Binary relations are also heavily used in computer science.

A binary relation over sets X and Y is an element of the power set of $X \times Y$. Since the latter set is ordered by inclusion ($\subseteq$), each relation has a place in the lattice of subsets of $X \times Y$. A binary relation is either a homogeneous relation or a heterogeneous relation depending on whether $X = Y$ or not.

Since relations are sets, they can be manipulated using set operations, including union, intersection, and complementation, and satisfying the laws of an algebra of sets. Beyond that, operations like the converse of a relation and the composition of relations are available, satisfying the laws of a calculus of relations, for which there are textbooks by Ernst Schröder,[4] Clarence Lewis, and Gunther Schmidt. A deeper analysis of relations involves decomposing them into subsets called concepts, and placing them in a complete lattice.

In some systems of axiomatic set theory, relations are extended to classes, which are generalizations of sets. This extension is needed for, among other things, modeling the concepts of "is an element of" or "is a subset of" in set theory, without running into logical inconsistencies such as Russell's paradox.

The terms correspondence, dyadic relation and two-place relation are synonyms for binary relation, though some authors use the term "binary relation" for any subset of a Cartesian product $X \times Y$ without reference to X and Y, and reserve the term "correspondence" for a binary relation with reference to X and Y.

3.2 UNIT OBJECTIVES

In going through this unit, you will be able to:

- learn about the relations.
- learn types of relations

Space for learners:

- understand closure properties of relations
- know the equivalence and partial order of relations
- know the basis of functions.

Space for learners:

3.3 TYPES OF RELATION

Binary Relation

Let P and Q be two non- empty sets. A binary relation R is defined to be a subset of P x Q from a set P to Q. If (a, b) ∈ R and R ⊆ P x Q then a is related to b by R i.e., aRb. If sets P and Q are equal, then we say R ⊆ P x P is a relation on P e.g.

(i) Let A = {a, b, c}

B = {r, s, t}

Then R = {(a, r), (b, r), (b, t), (c, s)} is a relation from A to B.

(ii) Let A = {1, 2, 3} and B = A

R = {(1, 1), (2, 2), (3, 3)} is a relation (equal) on A.

Example: If a set has n elements, how many relations are there from A to A.

Solution: If a set A has n elements, A x A has n^2 elements. So, there are 2^{n2} relations from A to A.

Example: If a set A = {1, 2}. Determine all relations from A to A.

Solution: There are 2^2= 4 elements i.e., {(1, 2), (2, 1), (1, 1), (2, 2)} in A x A. So, there are 2^4= 16 relations from A to A. i.e.

1. {(1, 2), (2, 1), (1, 1), (2, 2)}, {(1, 2), (2, 1)}, {(1, 2), (1, 1)}, {(1, 2), (2, 2)},
2. {(2, 1), (1, 1)},{(2,1), (2, 2)}, {(1, 1),(2, 2)},{(1, 2), (2, 1), (1 , 1)}, {(1, 2), (1, 1),
3. (2, 2)}, {(2,1), (1, 1), (2, 2)}, {(1, 2), (2, 1), (2, 2)}, {(1, 2), (2, 1), (1, 1), (2, 2)} and ∅.

Domain and Range of Relation

Domain of Relation: The Domain of relation R is the set of elements in P which are related to some elements in Q, or it is the set of all first entries of the ordered pairs in R. It is denoted by DOM (R).

Range of Relation: The range of relation R is the set of elements in Q which are related to some element in P, or it is the set of all second entries of the ordered pairs in R. It is denoted by RAN (R).

Space for learners:

Example:

1. Let A = {1, 2, 3, 4}
2. B = {a, b, c, d}
3. R = {(1, a), (1, b), (1, c), (2, b), (2, c), (2, d)}.

Solution:

DOM (R) = {1, 2}

RAN (R) = {a, b, c, d}

Complement of a Relation

Consider a relation R from a set A to set B. The complement of relation R denoted by R is a relation from A to B such that

R = {(a, b): {a, b) $\notin$ R}.

Example:

1. Consider the relation R from X to Y
2. X = {1, 2, 3}
3. Y = {8, 9}
4. R = {(1, 8) (2, 8) (1, 9) (3, 9)}

Q. Find the complement relation of R.

Solution:

X x Y = {(1, 8), (2, 8), (3, 8), (1, 9), (2, 9), (3, 9)}

Now we find the complement relation R from X x Y

R = {(3, 8), (2, 9)}

Representation of Relations

Relations can be represented in many ways. Some of which are as follows:

1. Relation as a Matrix: Let P = $[a_1,a_2,a_3,.......a_m]$ and Q = $[b_1,b_2,b_3......b_n]$ are finite sets, containing m and n number of elements respectively. R is a relation from P to Q. The relation R can be represented by m x n matrix M = $[M_{ij}]$, defined as

$$M_{ij} = \begin{cases} 0, \text{ if } (a_i, b_i) \notin R \\ 1, \text{ if } (a_i, b_i) \in R \end{cases}$$

Example

1. Let P = {1, 2, 3, 4}, Q = {a, b, c, d} and R = {(1, a), (1, b), (1, c), (2, b), (2, c), (2, d)}.

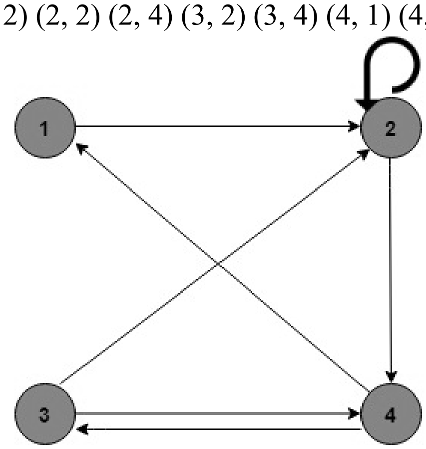
The matrix of relation R is shown as fig:

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \left\{ \begin{array}{cccc} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right\} \end{array}$$

2. Relation as a Directed Graph: There is another way of picturing a relation R when R is a relation from a finite set to itself.

Example

1. A = {1, 2, 3, 4}
2. R = {(1, 2) (2, 2) (2, 4) (3, 2) (3, 4) (4, 1) (4, 3)}



3. Relation as an Arrow Diagram: If P and Q are finite sets and R is a relation from P to Q. Relation R can be represented as an arrow diagram as follows.

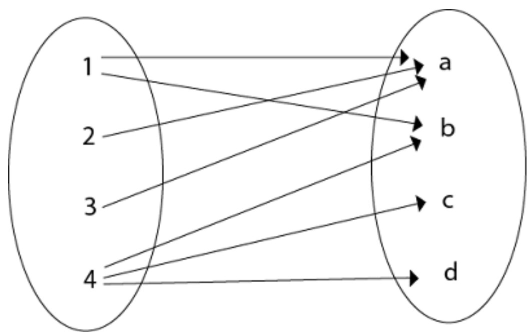
Draw two ellipses for the sets P and Q. Write down the elements of P and elements of Q column-wise in three ellipses. Then draw an arrow from the first ellipse to the second ellipse if a is related to b and a ∈ P and b ∈ Q.

Space for learners:

Example

1. Let P = {1, 2, 3, 4}
2. Q = {a, b, c, d}
3. R = {(1, a), (2, a), (3, a), (1, b), (4, b), (4, c), (4, d)

The arrow diagram of relation R is shown in fig:



4. Relation as a Table: If P and Q are finite sets and R is a relation from P to Q. Relation R can be represented in tabular form.

Make the table which contains rows equivalent to an element of P and columns equivalent to the element of Q. Then place a cross (X) in the boxes which represent relations of elements on set P to set Q.

Example

1. Let P = {1, 2, 3, 4}
2. Q = {x, y, z, k}
3. R = {(1, x), (1, y), (2, z), (3, z), (4, k)}.

The tabular form of relation as shown in fig:

	x	y	z	k
1	x	x		
2			x	
3			x	
4				x

Composition of Relations

Let A, B, and C be sets, and let R be a relation from A to B and let S be a relation from B to C. That is, R is a subset of A × B and S is a

Space for learners:

subset of B × C. Then R and S give rise to a relation from A to C indicated by R◦S and defined by:

1. a (R◦S)c **if for** some b ∈ B we have aRb and bSc.   is,
2. R ◦ S = {(a, c)| there exists b ∈ B **for** which (a, b) ∈ R and (b, c) ∈ S}

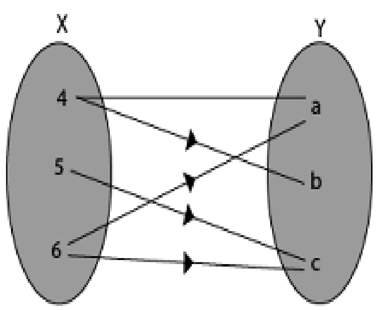
The relation R◦S is known the composition of R and S; it is sometimes denoted simply by RS.

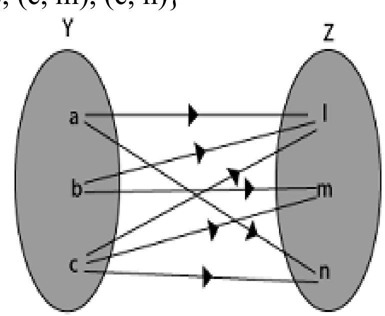
Let R is a relation on a set A, that is, R is a relation from a set A to itself. Then R◦R, the composition of R with itself, is always represented. Also, R◦R is sometimes denoted by R^2. Similarly, $R^3 = R^2 \circ R = R \circ R \circ R$, and so on. Thus, R^n is defined for all positive n.

Example: Let X = {4, 5, 6}, Y = {a, b, c} and Z = {l, m, n}. Consider the relation R_1 from X to Y and R_2 from Y to Z.

R_1 = {(4, a), (4, b), (5, c), (6, a), (6, c)}

R_2 = {(a, l), (a, n), (b, l), (b, m), (c, l), (c, m), (c, n)}

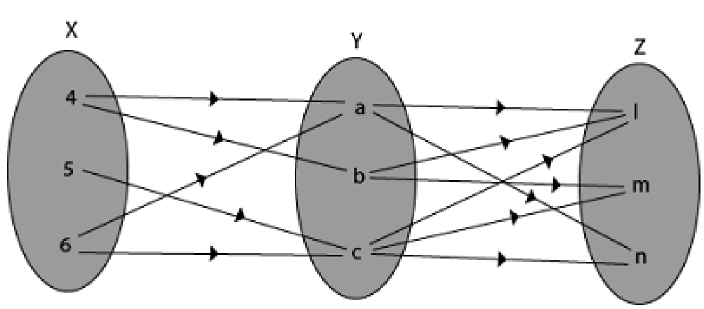




Find the composition of relation **(i)** R_1 o R_2 **(ii)** R_1o R_1^{-1}

Solution:

(i) The composition relation R_1 o R_2 as shown in fig:

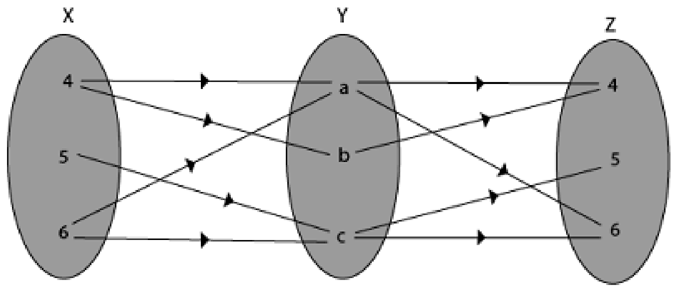


R_1 o R_2

__Space for learners:__

R_1 o R_2 = {(4, l), (4, n), (4, m), (5, l), (5, m), (5, n), (6, l), (6, m), (6, n)}

(ii) The composition relation $R_1 o R_1^{-1}$ as shown in fig:



$R_1 \text{ o } R_1^{-1}$

Composition of Relations and Matrices

There is another way of finding R∘S. Let M_R and M_S denote respectively the matrix representations of the relations R and S. Then

Example

Let P = {2, 3, 4, 5}. Consider the relation R and S on P defined by R = {(2, 2), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5), (5, 3)}

S = {(2, 3), (2, 5), (3, 4), (3, 5), (4, 2), (4, 3), (4, 5), (5, 2), (5, 5)}.

1. Find the matrices of the above relations.
2. Use matrices to find the following composition of the relatio n R and S.
3. (i)RoS (ii)RoR (iii)SoR

Solution: The matrices of the relation R and S are a shown in fig:

$$M_R = \begin{array}{c} \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{cccc} 2 & 3 & 4 & 5 \end{array} \\ \left\{ \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{array} \right\} \end{array} \quad \text{and} \quad M_S = \begin{array}{c} \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{cccc} 2 & 3 & 4 & 5 \end{array} \\ \left\{ \begin{array}{cccc} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{array} \right\} \end{array}$$

(i) To obtain the composition of relation R and S. First multiply M_R with M_S to obtain the matrix M_R x M_S as shown in fig:

__Space for learners:__

The non zero entries in the matrix M_R x M_S tells the elements related in RoS. So,

$$M_R \times M_S = \begin{array}{c} \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{cccc} 2 & 3 & 4 & 5 \end{array} \\ \begin{Bmatrix} 2 & 2 & 1 & 4 \\ 2 & 1 & 0 & 2 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{Bmatrix} \end{array}$$

Hence the composition R o S of the relation R and S is

R o S = {(2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (4, 2), (4, 5), (5, 2), (5, 3), (5, 4), (5, 5)}.

(ii) First, multiply the matrix M_R by itself, as shown in fig

$$M_R \times M_R = \begin{array}{c} \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{cccc} 2 & 3 & 4 & 5 \end{array} \\ \begin{Bmatrix} 1 & 2 & 2 & 3 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{Bmatrix} \end{array}$$

Hence the composition R o R of the relation R and S is

R o R = {(2, 2), (3, 2), (3, 3), (3, 4), (4, 2), (4, 5), (5, 2), (5, 3), (5, 5) }

(iii) Multiply the matrix M_S with M_R to obtain the matrix M_S x M_R as shown in fig:

$$M_S \times M_R = \begin{array}{c} \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{cccc} 2 & 3 & 4 & 5 \end{array} \\ \begin{Bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 \end{Bmatrix} \end{array}$$

The non-zero entries in matrix M_S x M_R tells the elements related in S o R.

Space for learners:

Hence the composition S o R of the relation S and R is

S o R = {(2, 4) , (2, 5), (3, 3), (3, 4), (3, 5), (4, 2), (4, 4), (4, 5), (5, 2) , (5, 3), (5, 4), (5, 5)}.

More on Types of Relations

1. Reflexive Relation: A relation R on set A is said to be a reflexive if **(a, a) ∈ R** for every **a** ∈ A.

Example: If A = {1, 2, 3, 4} then R = {(1, 1) (2, 2), (1, 3), (2, 4), (3, 3), (3, 4), (4, 4)}. Is a relation reflexive?

Solution: The relation is reflexive as for every a ∈ A. (a, a) ∈ R, i.e. (1, 1), (2, 2), (3, 3), (4, 4) ∈ R.

2. Irreflexive Relation: A relation R on set A is said to be **irreflexive if (a, a) ∉ R** for every **a ∈ A**.

Example: Let A = {1, 2, 3} and R = {(1, 2), (2, 2), (3, 1), (1, 3)}. Is the relation R reflexive or irreflexive?

Solution: The relation R is not reflexive as for every a ∈ A, (a, a) ∉ R, i.e., (1, 1) and (3, 3) ∉ R. The relation R is not irreflexive as (a, a) ∉ R, for some a ∈ A, i.e., (2, 2) ∈ R.

3. Symmetric Relation: A relation R on set A is said to be symmetric iff (a, b) ∈ R ⟺ (b, a) ∈ R.

Example: Let A = {1, 2, 3} and R = {(1, 1), (2, 2), (1, 2), (2, 1), (2, 3), (3, 2)}. Is a relation R symmetric or not?

Solution: The relation is symmetric as for every (a, b) ∈ R, we have (b, a) ∈ R, i.e., (1, 2), (2, 1), (2, 3), (3, 2) ∈ R but not reflexive because (3, 3) ∉ R.

Example of Symmetric Relation:

1. Relation ⊥r is symmetric since a line a is ⊥r to b, then b is ⊥r to a.
2. Also, Parallel is symmetric, since if a line a is ∥ to b then b is also ∥ to a.

Antisymmetric Relation: A relation R on a set A is antisymmetric if (a, b) ∈ R and (b, a) ∈ R then a = b.

Example: Let A = {1, 2, 3} and R = {(1, 1), (2, 2)}. Is the relation R antisymmetric?

Space for learners:

Solution: The relation R is antisymmetric as a = b when (a, b) and (b, a) both belong to R.

Space for learners:

Example: Let A = {4, 5, 6} and R = {(4, 4), (4, 5), (5, 4), (5, 6), (4, 6)}. Is the relation R antisymmetric?

Solution: The relation R is not antisymmetric as $4 \neq 5$ but (4, 5) and (5, 4) both belong to R.

5. Asymmetric Relation: A relation R on a set A is called an Asymmetric Relation if for every (a, b) ∈ R implies that (b, a) does not belong to R.

6. Transitive Relations: A Relation R on set A is said to be transitive iff (a, b) ∈ R and (b, c) ∈ R ⟺ (a, c) ∈ R.

Example: Let A = {1, 2, 3} and R = {(1, 2), (2, 1), (1, 1), (2, 2)}. Is the relation transitive?

Solution: The relation R is transitive as for every (a, b) (b, c) belong to R, we have (a, c) ∈ R i.e, (1, 2) (2, 1) ∈ R ⇒ (1, 1) ∈ R.

Note 1: The Relation ≤, ⊆ and / are transitive, i.e., a ≤ b, b ≤ c then a ≤ c

(ii) Let a ⊆ b, b ⊆ c then a ⊆ c

(iii) Let a/b, b/c then a/c.

Note 2: ⊥r is not transitive since a ⊥r b, b ⊥r c then it is not true that a ⊥r c. Since no line is ∥ to itself, we can have a ∥ b, b ∥ a but a ∦ a.

Thus ∥ is not transitive, but it will be transitive in the plane.

7. Identity Relation: Identity relation I on set A is reflexive, transitive and symmetric. So identity relation I is an Equivalence Relation.

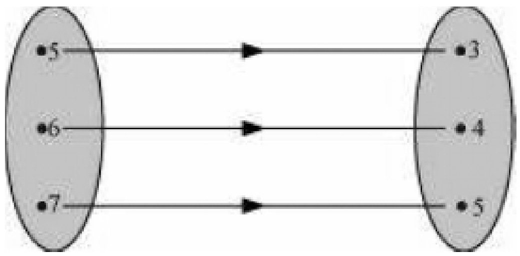
Example: A= {1, 2, 3} = {(1, 1), (2, 2), (3, 3)}

8. Void Relation: It is given by R: A →B such that R = ∅ (⊆ A x B) is a null relation. Void Relation R = ∅ is symmetric and transitive but not reflexive.

9. Universal Relation: A relation R: A →B such that R = A x B (⊆ A x B) is a universal relation. Universal Relation from A →B is reflexive, symmetric and transitive. So this is an equivalence relation.

CHECK YOUR PROGRESS

1. The given figure shows a relationship between the sets P and Q. write this relation



(i) in set-builder form (ii) in roster form. What is its domain and range?

2. Let A = {1, 2, 3, 4, 6}. Let R be the relation on A defined by

{(a, b): a, b ∈A, bis exactly divisible by a}.

(i) Write R in roster form

(ii) (ii) Find the domain of R

(iii) (iii) Find the range of R.

3. Determine the domain and range of the relation R defined by R = {(x, x+ 5): x ∈{0, 1, 2, 3, 4, 5}}.

4. Which of the following relations are functions? Give reasons. If it is a function, determine its domain and range.

(i) {(2, 1), (5, 1), (8, 1), (11, 1), (14, 1), (17, 1)}

(ii) {(2, 1), (4, 2), (6, 3), (8, 4), (10, 5), (12, 6), (14, 7)}

(iii) {(1, 3), (1, 5), (2, 5)}

3.4 CLOSURE PROPERTIES OF RELATIONS

Consider a given set A, and the collection of all relations on A. Let P be a property of such relations, such as being symmetric or being transitive. A relation with property P will be called a P-relation. The P-closure of an arbitrary relation R on A, indicated P (R), is a P-relation such that

$$R \subseteq P(R) \subseteq S$$

Space for learners:

(1) Reflexive and Symmetric Closures: The next theorem tells us how to obtain the reflexive and symmetric closures of a relation easily.

Theorem: Let R be a relation on a set A. Then:

- $R \cup \Delta_A$ is the reflexive closure of R
- $R \cup R^{-1}$ is the symmetric closure of R.

Example:

Let A = {k, l, m}. Let R is a relation on A defined by R = {(k, k), (k , l), (l, m), (m, k)}.

Find the reflexive closure of R.

Solution: $R \cup \Delta$ is the smallest relation having reflexive property, Hence,

RF = R ∪ Δ = {(k, k), (k, l), (l, l), (l, m), (m, m), (m, k)}.

Example: Consider the relation R on A = {4, 5, 6, 7} defined by

R = {(4, 5), (5, 5), (5, 6), (6, 7), (7, 4), (7, 7)}

Find the symmetric closure of R.

Solution: The smallest relation containing R having the symmetric property is $R \cup R^{-1}$,i.e.

RS = R ∪ R-1 = {(4, 5), (5, 4), (5, 5), (5, 6), (6, 5), (6, 7), (7, 6), (7, 4), (4, 7), (7, 7)}.

(2) Transitive Closures: Consider a relation R on a set A. The transitive closure R of a relation R of a relation R is the smallest transitive relation containing R.

Recall that $R^2 = R \circ R$ and $R^n = R^{n-1} \circ R$. We define

$$\boxed{R^* = \bigcup_{i=1}^{\infty} R^i}$$

The following Theorem applies:

Theorem1: R^* is the transitive closure of R.

Suppose A is a finite set with n elements.

$$R^* = R \cup R^2 \cup \ldots\ldots \cup R^n$$

Space for learners:

Theorem 2: Let R be a relation on a set A with n elements. Then

$$\text{Transitive }(R) = R \cup R^2 \cup \ldots\ldots \cup R^n$$

Example: Consider the relation R = {(1, 2), (2, 3), (3, 3)} on A = {1, 2, 3}.

Then $R^2 = R \circ R$ = {(1, 3), (2, 3), (3, 3)} and

$R^3 = R^2 \circ R$ = {(1, 3), (2, 3), (3, 3)} Accordingly,
Transitive (R) = {(1, 2), (2, 3), (3, 3), (1, 3)}

Example: Let A = {4, 6, 8, 10} and R = {(4, 4), (4, 10), (6, 6), (6, 8), (8, 10)} is a relation on set A. Determine transitive closure of R.

Solution: The matrix of relation R is shown in fig:

$$M_R = \begin{array}{c} \\ 4 \\ 6 \\ 8 \\ 10 \end{array} \begin{array}{c} \begin{array}{cccc} 4 & 6 & 8 & 10 \end{array} \\ \left\{ \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right\} \end{array}$$

Now, find the powers of M_R as in fig:

$$M_{R^2} = \begin{array}{c} \\ 4 \\ 6 \\ 8 \\ 10 \end{array} \begin{array}{c} \begin{array}{cccc} 4 & 6 & 8 & 10 \end{array} \\ \left\{ \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right\} \end{array} \qquad M_{R^3} = \begin{array}{c} \\ 4 \\ 6 \\ 8 \\ 10 \end{array} \begin{array}{c} \begin{array}{cccc} 4 & 6 & 8 & 10 \end{array} \\ \left\{ \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right\} \end{array}$$

$$M_{R^4} = \begin{array}{c} \\ 4 \\ 6 \\ 8 \\ 10 \end{array} \begin{array}{c} \begin{array}{cccc} 4 & 6 & 8 & 10 \end{array} \\ \left\{ \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right\} \end{array}$$

Hence, the transitive closure of M_R is M_R^* as shown in Fig (where M_R^* is the ORing of a power of M_R).

Space for learners:

$$M_{R^*} = M_R \vee M_{R^2} \vee M_{R^3} \vee M_{R^4}; \quad M_{R^*} = \begin{array}{c|cccc} & 4 & 6 & 8 & 10 \\ \hline 4 & 1 & 0 & 0 & 1 \\ 6 & 0 & 1 & 1 & 1 \\ 8 & 0 & 0 & 0 & 0 \\ 10 & 0 & 0 & 0 & 0 \end{array}$$

Thus, R^* = {(4, 4), (4, 10), (6, 8), (6, 6), (6, 10), (8, 10)}.

Note: While ORing the power of the matrix R, we can eliminate MRn because it is equal to MR* if n is even and is equal to MR3 if n is odd.

3.5 EQUIVALENCE OF RELATIONS

Equivalence Relations:

A relation R on a set A is called an equivalence relation if it satisfies following three properties:

1. Relation R is Reflexive, i.e., aRa ∀ a∈A.
2. Relation R is Symmetric, i.e., aRb ⟹ bRa
3. Relation R is transitive, i.e., aRb and bRc ⟹ aRc.

Example: Let A = {1, 2, 3, 4} and R = {(1, 1), (1, 3), (2, 2), (2, 4), (3, 1), (3, 3), (4, 2), (4, 4)}.

Show that R is an Equivalence Relation.

Solution:

Reflexive: Relation R is reflexive as (1, 1), (2, 2), (3, 3) and (4, 4) ∈ R.

Symmetric: Relation R is symmetric because whenever (a, b) ∈ R, (b, a) also belongs to R.

Example: (2, 4) ∈ R ⟹ (4, 2) ∈ R.

Transitive: Relation R is transitive because whenever (a, b) and (b, c) belongs to R, (a, c) also belongs to R.

Example: (3, 1) ∈ R and (1, 3) ∈ R ⟹ (3, 3) ∈ R.

So, as R is reflexive, symmetric and transitive, hence, R is an Equivalence Relation.

Space for learners:

Note1: If R_1 and R_2 are equivalence relation then $R_1 \cap R_2$ is also an equivalence relation.

Space for learners:

Example: A = {1, 2, 3}

R_1 = {(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)}

R_2 = {(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)}

$R_1 \cap R_2$ = {(1, 1), (2, 2), (3, 3)}

Note2: If R_1 and R_2 are equivalence relation then $R_1 \cup R_2$ may or may not be an equivalence relation.

Example: A = {1, 2, 3}

R_1 = {(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)}

R_2 = {(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)}

$R_1 \cup R_2$= {(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)}

Hence, Reflexive or Symmetric are Equivalence Relation but transitive may or may not be an equivalence relation.

Inverse Relation

Let R be any relation from set A to set B. The inverse of R denoted by R^{-1} is the relations from B to A which consist of those ordered pairs which when reversed belong to R that is:

R^{-1} = {(b, a): (a, b) ∈ R}

Example: A = {1, 2, 3}

B = {x, y, z}

Solution: R = {(1, y), (1, z), (3, y)

R^{-1} = {(y, 1), (z, 1), (y, 3)}

Clearly $(R^{-1})^{-1}$ = R

Note1: Domain and Range of R^{-1} is equal to range and domain of R.

Example: R = {(1, 1), (2, 2), (3, 3), (1, 2), (2, 3), (3, 2)}

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

Note2: If R is an Equivalence relation, then R^{-1} is always an Equivalence relation.

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

R = {(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)}

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

R^{-1} is a Equivalence Relation.

Note3: If R is a Symmetric Relation, then R^{-1}=R and vice-versa.

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

R = {(1, 1), (2, 2), (1, 2), (2, 1), (2, 3), (3, 2)}

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

Note 4: Reverse Order of Law

$(S \circ T)^{-1} = T^{-1}S^{-1}$ $(R \circ S \circ T)^{-1} = T^{-1} \circ S^{-1} \circ R^{-1}$.

3.5 PARTIAL ORDER OF RELATIONS

A relation R on a set A is called a partial order relation if it satisfies the following three properties:

1. Relation R is Reflexive, i.e. aRa ∀ a∈A.
2. Relation R is Antisymmetric, i.e., aRb and bRa ⟹ a = b.
3. Relation R is transitive, i.e., aRb and bRc ⟹ aRc.

Example: Show whether the relation (x, y) ∈ R, if, x ≥ y defined on the set of +ve integers is a partial order relation.

Solution: Consider the set A = {1, 2, 3, 4} containing four +ve integers. Find the relation for this set such as R = {(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3), (1, 1), (2, 2), (3, 3), (4, 4)}.

Reflexive: The relation is reflexive as for every a ∈ A. (a, a) ∈ R, i.e. (1, 1), (2, 2), (3, 3), (4, 4) ∈ R.

Antisymmetric: The relation is antisymmetric as whenever (a, b) and (b, a) ∈ R, we have a = b.

Transitive: The relation is transitive as whenever (a, b) and (b, c) ∈ R, we have (a, c) ∈ R.

Example: (4, 2) ∈ R and (2, 1) ∈ R, implies (4, 1) ∈ R.

Space for learners:

As the relation is reflexive, antisymmetric and transitive. Hence, it is a partial order relation.

Example: Show that the relation 'Divides' defined on N is a partial order relation.

Solution:

Reflexive: We have a divides a, ∀ a∈N. Therefore, relation 'Divides' is reflexive.

Antisymmetric: Let a, b, c ∈N, such that a divides b. It implies b divides a if a = b. So, the relation is antisymmetric.

Transitive: Let a, b, c ∈N, such that a divides b and b divides c.

Then a divides c. Hence the relation is transitive. Thus, the relation being reflexive, antisymmetric and transitive, the relation 'divides' is a partial order relation.

Example: (a) The relation ⊆ of a set of inclusion is a partial ordering or any collection of sets since set inclusion has three desired properties:

1. A ⊆ A for any set A.

2. If A ⊆ B and B ⊆ A then B = A.

3. If A ⊆ B and B ⊆ C then A ⊆ C

(b) The relation ≤ on the set R of real no that is Reflexive, Antisymmetric and transitive.

(c) Relation ≤ is a Partial Order Relation.

n-Ary Relations

By an n-ary relation, we mean a set of ordered n-tuples. For any set S, a subset of the product set Sn is called an n-ary relation on S. In particular, a subset of S3 is called a ternary relation on S.

Partial Order Set (POSET):

The set A together with a partial order relation R on the set A and is denoted by (A, R) is called partial orders set or POSET.

Total Order Relation

Consider the relation R on the set A. If it is also called the case that for all, a, b ∈ A, we have either (a, b) ∈ R or (b, a) ∈ R or a = b, then the relation R is known total order relation on set A.

Space for learners:

Example: Show that the relation '<' (less than) defined on N, the set of +ve integers is neither an equivalence relation nor partially ordered relation but is a total order relation.

Solution:

Reflexive: Let a ∈ N, then a < a

⟹ '<' is not reflexive.

As, the relation '<' (less than) is not reflexive, it is neither an equivalence relation nor the partial order relation.

But, as ∀ a, b ∈ N, we have either a < b or b < a or a = b. So, the relation is a total order relation.

Equivalence Class

Consider, an equivalence relation R on a set A. The equivalence class of an element a ∈ A, is the set of elements of A to which element a is related. It is denoted by [a].

Example: Let R be an equivalence relation on the set A = {4, 5, 6, 7} defined by

R = {(4, 4), (5, 5), (6, 6), (7, 7), (4, 6), (6, 4)}.

Determine its equivalence classes.

Solution: The equivalence classes are as follows:

{4} = {6} = {4, 6}

{5} = {5}

{7} = {7}.

Circular Relation

Consider a binary relation R on a set A. Relation R is called circular if (a, b) ∈ R and (b, c) ∈ R implies (c, a) ∈ R.

Example: Consider R is an equivalence relation. Show that R is reflexive and circular.

Solution: Reflexive: As, the relation, R is an equivalence relation. So, reflexivity is the property of an equivalence relation. Hence, R is reflexive.

Circular: Let (a, b) ∈ R and (b, c) ∈ R

⇒ (a, c) ∈ R (∵ R is transitive)

⇒ (c, a) ∈ R (∵ R is symmetric)

Space for learners:

Thus, R is Circular.

Compatible Relation

A binary relation R on a set A that is Reflexive and symmetric is called Compatible Relation.

Every Equivalence Relation is compatible, but every compatible relation need not be an equivalence.

Example: Set of a friend is compatible but may not be an equivalence relation.

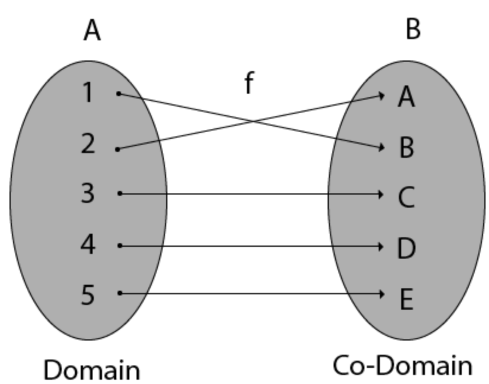
Friend   Friend

$a \rightarrow b$, $b \rightarrow c$ but possible that a and c are not friends.

3.6 INTRODUCTION TO FUNCTION

Functions

It is a mapping in which every element of set A is uniquely associated at the element with set B. The set of A is called Domain of a function and set of B is called Co domain.



Domain, Co-Domain, and Range of a Function:

Domain of a Function: Let f be a function from P to Q. The set P is called the domain of the function f.

Co-Domain of a Function: Let f be a function from P to Q. The set Q is called Co-domain of the function f.

Range of a Function: The range of a function is the set of picture of its domain. In other words, we can say it is a subset of its co-domain. It is denoted as f (domain).

Space for learners:

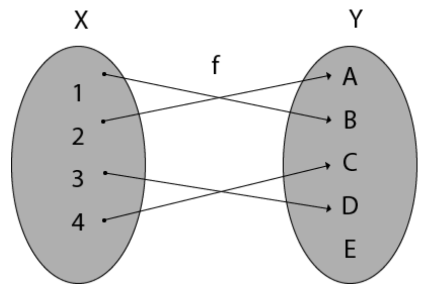
1. If f: P → Q, then f (P) = {f(x): x ∈ P} = {y: y ∈ Q | ∃ x ∈ P, such that f (x) = y}.

Example: Find the Domain, Co-Domain, and Range of function.

1. Let x = {1, 2, 3, 4}

2. y = {a, b, c, d, e}

3. f = {(1, b), (2, a), (3, d), (4, c) }



Solution:

Domain of function: {1, 2, 3, 4}

Range of function: {a, b, c, d}

Co-Domain of function: {a, b, c, d, e}

Functions as a Set

If P and Q are two non-empty sets, then a function f from P to Q is a subset of P x Q, with two important restrictions

1. ∀ a ∈ P, (a, b) ∈ f for some b ∈ Q

2. If (a, b) ∈ f and (a, c) ∈ f then b = c.

Note1: There may be some elements of the Q which are not related to any element of set P.

2. Every element of P must be related with at least one element of Q.

Example: If a set A has n elements, how many functions are there from A to A?

Solution: If a set A has n elements, then there are nn functions from A to A.

Representation of a Function

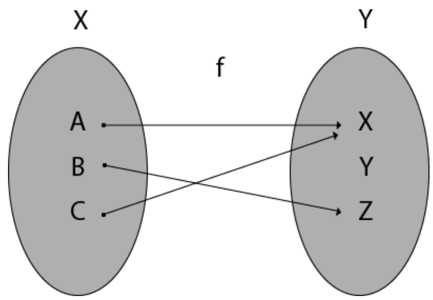
The two sets P and Q are represented by two circles. The function f: P → Q is represented by a collection of arrows joining the points which represent the elements of P and corresponds elements of Q

Space for learners:

Example: Let, X = {a, b, c} and Y = {x, y, z} and f: X → Y such that

f= {(a, x), (b, z), (c, x)}

Then f can be represented diagrammatically as follows



Example: Let X = {x, y, z, k} and Y = {1, 2, 3, 4}. Determine which of the following functions. Give reasons if it is not. Find range if it is a function.

a. f = {(x, 1), (y, 2), (z, 3), (k, 4)

b. g = {(x, 1), (y, 1), (k, 4)

c. h = {(x, 1), (x, 2), (x, 3), (x, 4)

d. l = {(x, 1), (y, 1), (z, 1), (k, 1)}

e. d = {(x, 1), (y, 2), (y, 3), (z, 4), (z, 4)}

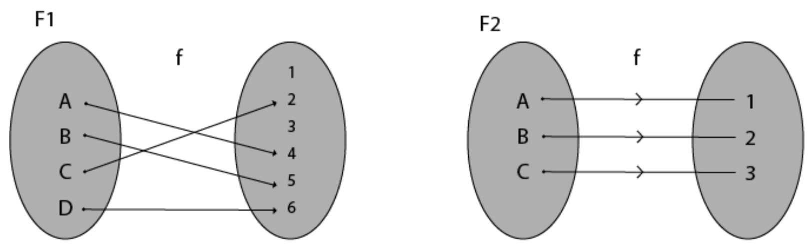
Solution:

1. It is a function. Range (f) = {1, 2, 3, 4}
2. It is not a function because every element of X does not relate with some element of Y i.e., Z is not related with any element of Y.
3. h is not a function because h (x) = {1, 2, 3, 4} i.e., element x has more than one image in set Y.
4. d is not a function because d (y) = {2, 3} i.e., element y has more than image in set Y.

Types of Functions

Injective (One-to-One) Functions: A function in which one element of Domain Set is connected to one element of Co-Domain Set.

Space for learners:

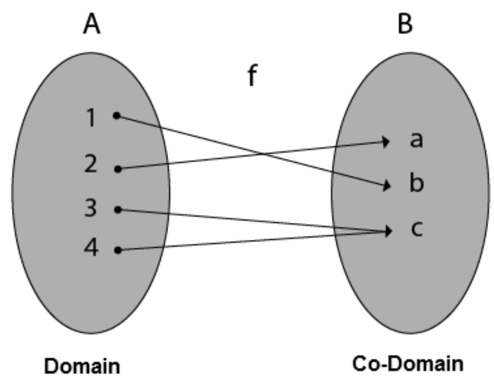


F1 and F2 show one to one Function

Surjective (Onto) Functions: A function in which every element of Co-Domain Set has one pre-image.

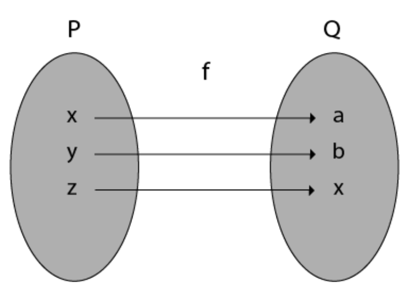
Example: Consider, A = {1, 2, 3, 4}, B = {a, b, c} and f = {(1, b), (2, a), (3, c), (4, c)}.

It is a Surjective Function, as every element of B is the image of some A



Note: In an Onto Function, Range is equal to Co-Domain.

Bijective (One-to-One Onto) Functions: A function which is both injective (one to - one) and surjective (onto) is called bijective (One-to-One Onto) Function.



Example: Consider P = {x, y, z} Q = {a, b, c} and f: P → Q such that

f = {(x, a), (y, b), (z, c)}

Space for learners:

The f is a one-to-one function and also it is onto. So it is a bijective function.

Into Functions: A function in which there must be an element of co-domain Y does not have a pre-image in domain X.

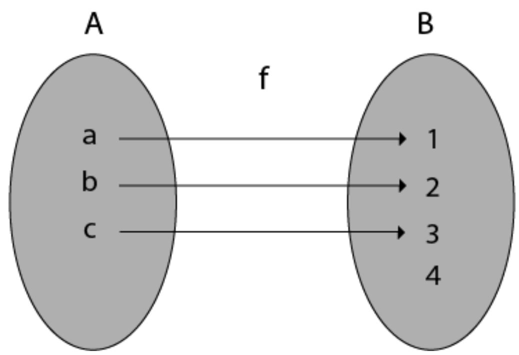
Example: Consider, A = {a, b, c}

B = {1, 2, 3, 4}   and f: A → B such that

f = {(a, 1), (b, 2), (c, 3)}

In the function f, the range i.e., {1, 2, 3} ≠ co-domain of Y i.e., {1, 2, 3, 4}

Therefore, it is an into function

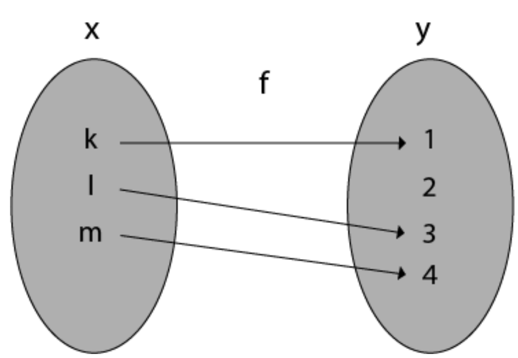


One-One into Functions: Let f: X → Y. The function f is called one-one into function if different elements of X have different unique images of Y.

Example: Consider, X = {k, l, m}   Y = {1, 2, 3, 4} and f: X → Y such that

f = {(k, 1), (l, 3), (m, 4)}

The function f is a one-one into function



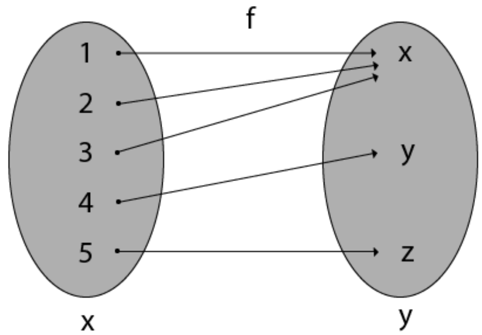
Space for learners:

Many-One Functions: Let f: X → Y. The function f is said to be many-one functions if there exist two or more than two different elements in X having the same image in Y.

Example: Consider X = {1, 2, 3, 4, 5}   Y = {x, y, z} and f: X → Y such that

f = {(1, x), (2, x), (3, x), (4, y), (5, z)}

The function f is a many-one function

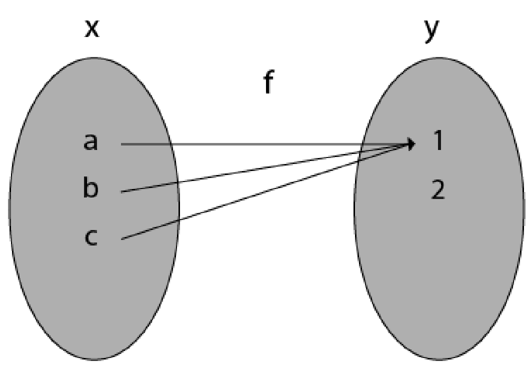


Many-One into Functions: Let f: X → Y. The function f is called many-one function if and only if is both many one and into function.

Example: Consider X = {a, b, c}   Y = {1, 2} and f: X → Y such that

f = {(a, 1), (b, 1), (c, 1)}

As the function f is a many-one and into, so it is a many-one into function.



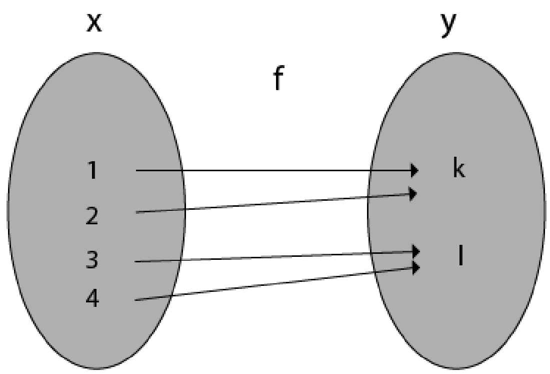
Many-One onto Functions: Let f: X → Y. The function f is called many-one onto function if and only if is both many one and onto.

Example: Consider X = {1, 2, 3, 4} Y = {k, l} and f: X → Y such that

f = {(1, k), (2, k), (3, l), (4, l)}

Space for learners:

The function f is a many-one (as the two elements have the same image in Y) and it is onto (as every element of Y is the image of some element X). So, it is many-one onto function



Identity Functions

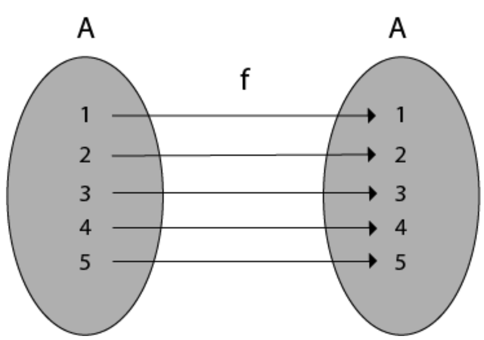
The function f is called the identity function if each element of set A has an image on itself i.e., f (a) = a ∀ a ∈ A.

It is denoted by I.

Example: Consider, A = {1, 2, 3, 4, 5} and f: A → A such that

f = {(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)}.

The function f is an identity function as each element of A is mapped onto itself. The function f is a one-one and onto



Invertible (Inverse) Functions

A function f: X → Y is invertible if and only if it is a bijective function.

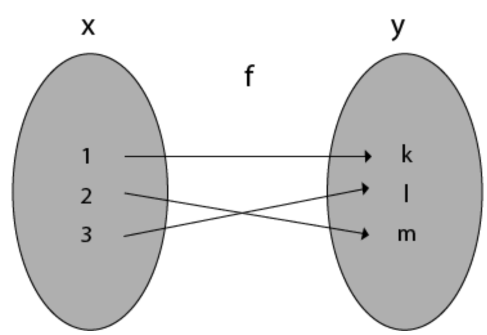
Consider the bijective (one to one onto) function f: X → Y. As f is a one to one, therefore, each element of X corresponds to a distinct element of Y. As f is onto, there is no element of Y which is not the image of any element of X, i.e., range = co-domain Y.

The inverse function for f exists if f-1 is a function from Y to X.

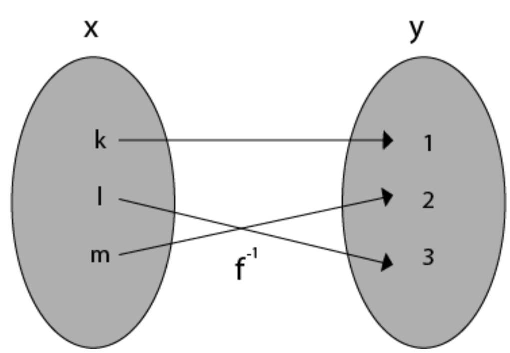
Space for learners:

Example: Consider, X = {1, 2, 3}

Y = {k, l, m} and f: X→Y such that f = {(1, k), (2, m), (3, l)



The inverse function of f is shown in fig:



Compositions of Functions

Consider functions, f: A → B and g: B → C. The composition of f with g is a function from A into C defined by (gof) (x) = g [f(x)] and is defined by gof.

To find the composition of f and g, first find the image of x under f and then find the image of f (x) under g.

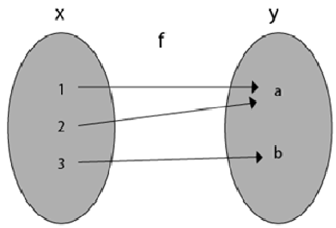
Example: Let X = {1, 2, 3}

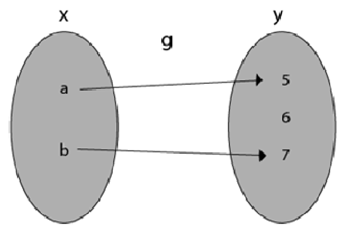
Y = {a, b}

. Z = {5, 6, 7}.

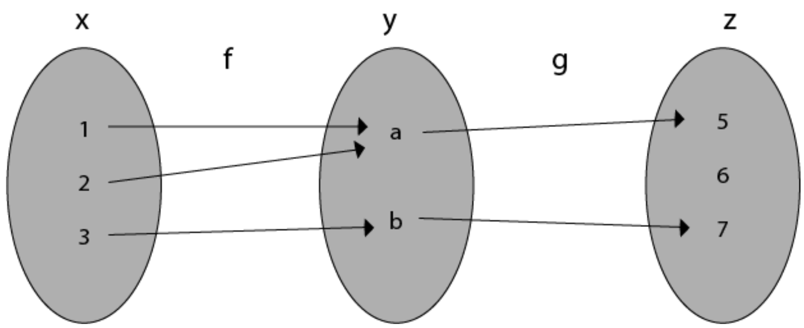
Consider the function f = {(1, a), (2, a), (3, b)} and g = {(a, 5), (b, 7)} as in figure. Find the composition of gof.

Space for learners:





Solution: The composition function gof is shown in fig below:



(gof) (1) = g [f (1)] = g (a) = 5, (gof) (2) = g [f (2)] = g (a) = 5

(gof) (3) = g [f (3)] = g (b) = 7.

Example: Consider f, g and h, all functions on the integers, by f (n) =n2, g (n) = n + 1 and h (n) = n - 1.

Determine (i) hofog (ii) gofoh (iii) fogoh.

Solution:

(i) hofog (n) = n + 1,

hofog (n + 1) = (n+1)2

h [(n+1)2] = (n+1)2 - 1 = n2 + 1 + 2n - 1 = n2 + 2n.

(ii) gofoh (n) = n - 1, gof (n - 1) = (n-1)2

g [(n-1)2] = (n-1)2 + 1 = n2 + 1 - 2n + 1 = n2 - 2n + 2.

(iii) fogoh (n) = n - 1

fog (n - 1) = (n - 1) + 1

f (n) = n2.

Note:

- If f and g are one-to-one, then the function (gof) (gof) is also one-to-one.
- If f and g are onto then the function (gof) (gof) is also onto.

Space for learners:

- o Composition consistently holds associative property but does not hold commutative property.

Space for learners:

3.7 SUMMING UP

- A binary relation R between two non-empty sets P and Q is defined to be a subset of P x Q from a set P to Q.
- Domain of relation R is the set of elements in P which are related to some elements in Q, or it is the set of all first entries of the ordered pairs in R. Range of relation R is the set of elements in Q which are related to some element in P, or it is the set of all second entries of the ordered pairs in R.
- Relations can be represented in terms of matrix, Directed Graph, Table or Arrow Diagram.
- Relations may be of type reflexive, irreflexive, symmetric, asymmetric or transitive relations.
- A relation R on a set A is called an equivalence relation if R is reflexive, symmetric and transitive.
- A relation R on a set A is called a partial order relation if R is Reflexive, Antisymmetric and transitive.
- The set A together with a partial order relation R on the set A and is denoted by (A, R) is called a partial order set or POSET.
- A binary relation R on a set A is called circular if $(a, b) \in R$ and $(b, c) \in R$ implies $(c, a) \in R$.
- A mapping in which every element of set A is uniquely associated with the element of set B is called function. The set of A is called Domain of a function and set of B is called Co domain.
- Functions are of types injective, surjective, bijective and into and many more.

3.8 ANSWERS TO CHECK YOUR PROGRESS

Answer 1:

According to the given figure, P = {5, 6, 7}, Q = {3, 4, 5}

(i) $R = \{(x, y): y = x- 2; x \in P\}$ or $R = \{(x, y): y = x- 2$ for $x= 5, 6, 7\}$

(ii) $R = \{(5, 3), (6, 4), (7, 5)\}$

Domain of $R = \{5, 6, 7\}$

Range of $R = \{3, 4, 5\}$

Answer 2:

$A = \{1, 2, 3, 4, 6\}$, $R = \{(a, b): a, b \in A$, bis exactly divisible by $a\}$

(i) $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 6), (2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (6, 6)\}$

(ii) Domain of $R = \{1, 2, 3, 4, 6\}$

(iii) Range of $R = \{1, 2, 3, 4, 6\}$

Answer 3:

$R = \{(x, x+ 5): x \in \{0, 1, 2, 3, 4, 5\}\}$

$\therefore R = \{(0, 5), (1, 6), (2, 7), (3, 8), (4, 9), (5, 10)\}$

$\therefore$Domain of $R = \{0, 1, 2, 3, 4, 5\}$

Range of $R = \{5, 6, 7, 8, 9, 10\}$

Answer 4:

(i) $\{(2, 1), (5, 1), (8, 1), (11, 1), (14, 1), (17, 1)\}$

Since 2, 5, 8, 11, 14, and 17 are the elements of the domain of the given relation having their unique images, this

relation is a function.

Here, domain = $\{2, 5, 8, 11, 14, 17\}$ and range = $\{1\}$

(ii) $\{(2, 1), (4, 2), (6, 3), (8, 4), (10, 5), (12, 6), (14, 7)\}$

Since 2, 4, 6, 8, 10, 12, and 14 are the elements of the domain of the given relation having their unique images, this

relation is a function.

Here, domain = $\{2, 4, 6, 8, 10, 12, 14\}$ and range = $\{1, 2, 3, 4, 5, 6, 7\}$

Space for learners:

(iii) {(1, 3), (1, 5), (2, 5)}

Since the same first element i.e., 1 corresponds to two different images i.e., 3 and 5, this relation is not a function.

Space for learners:

3.9 POSSIBLE QUESTIONS

Short answer type questions:

1. Which of these is not a type of relation?

    a) Reflexive

    b) Subjective

    c) Symmetric

    d) Transitive

2. An Equivalence relation is always symmetric.

    a) True

    b) False

3. Which of the following relations is symmetric but neither reflexive nor transitive for a set A = {1, 2, 3}.

    a) R = {(1, 2), (1, 3), (1, 4)}

    b) R = {(1, 2), (2, 1)}

    c) R = {(1, 1), (2, 2), (3, 3)}

    d) R = {(1, 1), (1, 2), (2, 3)}

4. Which of the following relations is transitive but not reflexive for the set S={3, 4, 6}?

    a) R = {(3, 4), (4, 6), (3, 6)}

    b) R = {(1, 2), (1, 3), (1, 4)}

    c) R = {(3, 3), (4, 4), (6, 6)}

    d) R = {(3, 4), (4, 3)}

5. Let R be a relation in the set N given by R={(a,b): a+b=5, b>1}. Which of the following will satisfy the given relation?

   a) (2,3) ∈ R

   b) (4,2) ∈ R

   c) (2,1) ∈ R

   d) (5,0) ∈ R

6. Which of the following relations is reflexive but not transitive for the set T = {7, 8, 9}?

   a) R = {(7, 7), (8, 8), (9, 9)}

   b) R = {(7, 8), (8, 7), (8, 9)}

   c) R = {0}

   d) R = {(7, 8), (8, 8), (8, 9)}

7. Let I be a set of all lines in a XY plane and R be a relation in I defined as R = {(I1, I2):I1 is parallel to I2}. What is the type of given relation?

   a) Reflexive relation

   b) Transitive relation

   c) Symmetric relation

   d) Equivalence relation

8. Which of the following relations is symmetric and transitive but not reflexive for the set I = {4, 5}?

   a) R = {(4, 4), (5, 4), (5, 5)}

   b) R = {(4, 4), (5, 5)}

   c) R = {(4, 5), (5, 4)}

   d) R = {(4, 5), (5, 4), (4, 4)}

9. (a,a) ∈ R, for every a ∈ A. This condition is for which of the following relations?

   a) Reflexive relation

Space for learners:

b) Symmetric relation

c) Equivalence relation

d) Transitive relation

10. $(a_1, a_2) \in R$ implies that $(a_2, a_1) \in R$, for all $a_1, a_2 \in A$. This condition is for which of the following relations?

a) Equivalence relation

b) Reflexive relation

c) Symmetric relation

d) Universal relation

Long answer type questions:

1. Let A = {1, 3, 5, 7} and B = {p, q, r}. Let R be a relation from A into B defined by R = {(1, p), (3, r), (5, q), (7, p), (7, q)} find the domain and range of R.
2. Let A = {2, 4, 6} and B = {x, y, z}.

State which of the following are relation from A into B

(i) R_1 = {(2, x), (y, 4), (6, z)}

(ii) R_2 = {(4, y) (y, 4)}

(iii) R_3 = {(2, x) (4, y) (6, z)}

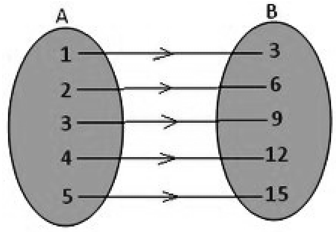
3. Let A = {3, 4, 5, 6} B = {1, 2, 3, 4, 5, 6} Let R = {(a, b) : a ∈ A, b ∈ B and a < b}.

Write R in the roster form. Find its domain and range.

4. Let A = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10} Let R be A relation on A defined by R = {a, b} : a ∈ A, b ∈ A, a is a multiple of b}. Find R, domain of R, range of R.
5. Determine the range and domains of the relation R defined by R = {(x - 1), (x + 2) : x ∈ (2, 3, 4, 5)}
6. Let A = {1, 2, 3, 4, 5, 6} Define a relation R from A to A by R {(x, y) : y = x + 2}
   - Depict this relation using an arrow diagram.
   - Write down the domain and range of R

Space for learners:

7. The adjoining figure shows a relation between the set A and B. Write this relation in find domain and range



(i) Set builder form.

(ii) Roster form.

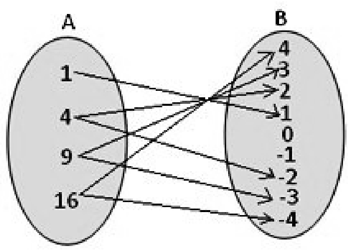
(iii) Find domain and range.

8. If A = {1, 4, 9, 16} and B = {1, 2, 3} Let R be a relation 'is square of' from A to B.

Find R domain and range of R.

9. Let A = {3, 4, 5} and B = {6, 8, 9, 10, 12}. Let R be the relation 'is a factor of' from A to B. Find R.

10. Adjoining figure shows relation between A and B. Write relation in



Range of a set

(i) Set builder form.

(ii) Roster form.

(iii) Find domain and range of R.

3.10 REFERENCES AND SUGGESTED READINGS

- Sets Relations Functions – by Gunther Gedia.
- Sets Relations Functions A programmed unit in modern mathematics – by Myra McFadden.
- Concrete on the relation and function – by Jane Tennitope.
- Set theory – Charles C Printer.
- Naïve set theory – Paul Halmour.

Space for learners:

UNIT4: BOOLEAN ALGEBRA

Space for learners:

Unit Structure:

4.1 INTRODUCTION

Space for learners:

In this unit we will learn Boolean algebra which was developed by George Boole (1815-1864) a logician, to examine a given set of propositions (statements) with a view to checking their logical consistency and simplifying them by removing redundant statements or clauses. He used symbols to represent simple propositions. Compound propositions were expressed in terms of these symbols and connectives. Again, we will learn various properties of Boolean algebra with their proof. We will learn Boolean expression and Principle of Duality, how we can convert one Boolean expression to another. We will learn how we can simplify various Boolean expressions by using the Boolean properties.

We will learn Boolean function, literals, Minterms and Maxterm. Again, we will learn the truth table of Conjunction and Disjunction operation. we will learn the two most important canonical forms of Boolean algebra, Sum of Minterms (SOM) and Product of Maxterm (POM). We will learn how to write the simplified output expression of an Boolean function in SOM and POM form by using Boolean Identities as well as truth table. And finally we will learn the application of Boolean Algebra.

4.2 UNIT OBJECTIVES

After going through this unit, you will be able to:

- define Boolean algebra
- know about duality principle of Boolean algebra
- know various properties of Boolean algebra with proof
- define Boolean expression and how to simplify it
- define literal, Minterm and Maxterm.
- define Boolean function
- define Conjunction, Disjunction and Complement operation
- define the canonical form SOM and POM
- know how to convert output expression into SOM and POM
- know the application of Boolean Algebra

4.3 BOOLEAN ALGEBRA

Space for learners:

Definitions: A non-empty set B with two binary operations $\vee$ and $\wedge$, a unary operation $'$, and two distinct elements 0 and I is called a Boolean Algebra if the following axioms holds for any elements a, b, c $\in$ B

[B1]: Commutative Laws:

$a \vee b = b \vee a$ and $a \wedge b = b \wedge a$

[B2]: Distributive Law:

$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ and $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

[B3]: Identity Laws:

$a \vee 0 = a$ and $a \wedge I = a$

[B4]: Complement Laws:

$a \vee a' = I$ and $a \wedge a' = 0$

We shall call 0 as zero element, 1 as unit element and a' the complement of a.

We denote a Boolean Algebra by $(B, \vee, \wedge, \sim, 0, I)$

Example 1. Let, $D_6 = \{1, 2, 3, 6\}$ has four elements. Define $\vee$, $\wedge$ and $'$ on D_6 by $a \vee b = \text{lcm}(a, b)$, $a \wedge b = \gcd(a, b)$ and $a' = 6/a$. Then D_6 is a Boolean Algebra with 1 as the zero element and 6 as the unit element.

Solution:

We prepare the following tables for the operations $\vee, \wedge, '$

Table for operation ($\vee$)

$\vee$	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

Table for operation ($\wedge$)

$\wedge$	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

Table for operation (')

'	1	2	3	6
	6	3	2	1

we observe that all the entries in the tables are element of D_6. Therefore '$\vee$' and '$\wedge$' are binary operations on set D_6. Also, ' ' ' is a unary operation on D_6 .

we observe the following properties -

Commutativity:

The entries in the composition tables for $\vee$ and $\wedge$ are symmetric about the diagonal starting from the upper left corner. Therefore, $\vee$ and $\wedge$ are commutative binary operations on D_6.

Distributivity:

From the composition tables of $\vee$ and $\wedge$, we have

$$1\vee (2 \wedge 3) = 1 \vee 1 = 1 \text{ and } (1\vee 2) \wedge (1\vee 3) = 2 \wedge 3 = 1$$

$$\therefore\ 1 \vee (2\wedge 3) = (1\vee 2) \wedge (1 \vee 3)$$

Similarly,

$$1 \vee (2\wedge 6) = (1 \vee 2) \wedge (1\vee 6)$$

$$1 \vee (3\wedge 6) = (1\vee 3) \wedge (1\vee 6)$$

$$2\vee (3\wedge 6)= (2\vee 3) \wedge (2\vee 6) \text{etc.}$$

Thus, $\vee$ is distributive over $\wedge$

Also,

$$1 \wedge(2 \vee 3) = 1 \wedge 6 = 1 \text{ and } (1\wedge 2) \vee (1 \wedge 3) = 2 \wedge 3 = 1$$

$$\therefore\ 1 \wedge(2\vee 3) = (1\wedge 2) \vee (1 \wedge 3)$$

Similarly,

$$1 \wedge(2\vee 6) = (1 \wedge 2) \vee (1\wedge 6)$$

$$1 \wedge (3\vee 6) = (1\vee 3) \wedge(1\vee 6)$$

$$2\wedge (3\vee 6)= (2\wedge 3)\vee (2\wedge 6)\text{etc.}$$

Thus, $\wedge$ is distributive over $\vee$.

Existence of identity elements:

For binary operation '$\vee$', we observe that the first row of the composition table coincides with the top most row and the first column coincides with the left most column. These two intersect at

Space for learners:

1. so, 1 is the identity element for ‘∨’. Similarly, 6 is the identity element for ‘∧ ‘.

Thus, 1 and 6 are respectively the zero and unit element.

Complement laws:

We have,

$1\vee 1' = 1 \vee 6 = 6$, $2 \vee 2' = 2 \vee 3 = 6$, $3\vee 3' = 3\vee 2 = 6$, $6\vee 6' = 6\vee 1 = 6$
$1\wedge 1' = 1\wedge 6 = 1$, $2\wedge 2' = 2\wedge 3 = 1$, $3\wedge 3' = 3\wedge 2 = 1$, $6\wedge 6' = 6\wedge 1 = 1$

$\therefore\ 1' = 6/1 = 6$, $2' = 6/2 = 3$, $3' = 6/3 = 2$, $6' = 6/6 = 1$

Thus, the set D_6 with the given binary operations and a unary operation satisfies all the axioms of Boolean algebra. Hence, (D_6, ‘∨’, ‘∧’, ‘ ‘ ‘) is a Boolean algebra .

4.4 PRINCIPLE OF DUALITY

By the dual of a proposition concerning a Boolean algebra B, we mean the proposition obtained by substituting ∨ for ∧, ∧for V, 0 for 1, and 1 for 0, i.e., by exchanging ∧ and V, and exchanging 0 and. Any pair of expression satisfying this property is called Dual expression. Again, this characteristic of Boolean algebra is called the Principle of Duality.

For example, the dual of $x\wedge(y\vee z) = (x\wedge Y) \vee (x\wedge Z)$ is $x\vee (y\wedge Z) = (x\vee Y) \wedge (x\vee Z)$, and vice versa.

4.5 PROPERTIES OF A BOOLEAN ALGEBRA

1. Idempotent Laws:

(i) $a \vee a = a$ (ii) $a \wedge a = a$

2. Boundedness Laws:

(i) $a \vee I = I$ (ii) $a \wedge 0 = 0$

3. Absorption Laws:

(i) $a \vee (a \wedge b) = a$ (ii) $a \wedge (a \vee b) = a$

4. Associative Laws:

(i) $(a \vee b) \vee c = a \vee (b \vee c)$ (ii) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

Space for learners:

5.De Morgan's Law:

(i) $(a \vee b)' = a' \wedge b'$ (ii) $(a \wedge b)' = a' \vee b'$.

6.(i) $(a \vee b) = (a' \wedge b')'$ (ii) $(a \wedge b) = (a' \vee b')'$

7. (i) $a \wedge (a' \vee b) = (a \wedge b)$ (ii) $a \vee (a' \wedge b) = (a \vee b)$

Proof: It is sufficient to prove first part of each law since second part follows from the first by principle of duality.

1. (i). We have

$a = a \vee 0$ (by identity law in a Boolean algebra)

$= a \vee (a \wedge a')$ (by complement law)

$= (a \vee a) \wedge (a \vee a')$ (by distributive law)

$= (a \vee a) \wedge I$ (complement law)

$= a \vee a$ (identity law),

1(ii). We know that,

$a = a \wedge 1$(by identity law in a Boolean algebra)

$= a \wedge (a \vee a')$ (by complement law)

$= (a \wedge a) \vee (a \wedge a')$ (by distributive law)

$= (a \wedge a) \vee 0$ (complement law)

$= (a \wedge a)$ (identity law)

2(i). We have

$a \vee I = (a \vee I) \wedge I$ (identity law)

$= (a \vee I) \wedge (a \vee a')$ (complement law)

$= a \vee (I \wedge a')$ (Distributive law)

$= a \vee a'$ (identity law)

$= I$ (complement law).

2(ii). it is the dual of 2(i)

Space for learners:

3(i). we note that

$a \vee (a \wedge b) = (a \wedge I) \vee (a \wedge b)$ (identity law)

$= a \wedge (I \vee b)$ (distributive law)

$= a \wedge (b \vee I)$ (commutativity)

$= a \wedge I$ (Identity law)

$= a$ (identity law)

3(ii). it is the dual of 3(i)

4(i).

Let,

$L = (a \vee b) \vee c$ $\qquad$ $R = a \vee (b \vee c)$

Then $a \wedge L = a \wedge [(a \vee b) \vee c]$

$= [a \wedge (a \vee b)] \vee (a \wedge c)$ (distributive Law)

$= a \vee (a \wedge c)$ (absorption law)

$= a$ (absorption law)

And

$a \wedge R = a \wedge [a \vee (b \vee c)]$

$= (a \wedge a) \vee (a \wedge (b \vee c)]$ (distributive law)

$= a \vee (a \wedge (b \vee c)]$ (idempotent law)

$= a$ (absorption Law)

Thus, $a\wedge L = a \wedge R$ and so, by duality, $a \vee L = a \vee R$.

Further, $a' \wedge L = a' \wedge [(a \vee b) \vee c]$

$= [a' \wedge (a \vee b)] \vee (a' \wedge c)$ (distributive law)

$= [(a' \wedge a) \vee (a' \wedge b)] \vee (a' \wedge c)$ (distributive law)

$= [0\vee (a' \wedge b)] \vee (a' \wedge c)$ (complement Law)

$= (a' \wedge b)] \vee (a' \wedge c)$ (Identity law)

$= a' \wedge (b \vee c)$ (distributive law)

Space for learners:

On the other hand

$a' \wedge R \;\; = a' \wedge [a \vee (b \vee c)]$

$= (a' \wedge a) \vee [a' \wedge (b \vee c)]$ (distributive law)

$= 0 \vee [a' \wedge (b \vee c)]$ (complement law)

$= a' \wedge (b \vee c)]$ (identity law)

Hence,

$a' \wedge L = a' \wedge R$ and so by duality $a' \vee L = a' \vee R$

Therefore,

$L = (a \vee b) \vee c$

$= 0 \vee [(a \vee b) \vee c] = 0 \vee L$ (identity law)

$= (a \wedge a') \vee [(a \vee b) \vee c]$

$= (a \wedge a') \vee L$ (complement law)

$= (a \vee L) \wedge (a' \vee L)$ (distributive law)

$= (a \vee R) \wedge (a' \vee R)$ (using $A \vee L = a \vee R$ and $a' \vee L = a' \vee R$]

$= (a \wedge a') \vee R$ (distributive law)

$= 0 \vee R$ (complement law)

$= R$ (identity law)

Hence, $(a \vee b) \vee c = a \vee (b \vee c)$

4(ii). It is the dual of 4(i)

5(i). We have,

$(a \vee b) \vee (a' \wedge b') = (b \vee a) \vee (a' \wedge b')$ (commutative)

$= b \vee (a \vee (a' \wedge b'))$ (associative)

$= b \vee [(a \vee a' \wedge (a \vee b')]$ (distributive)

$= b \vee [I \wedge (a \vee b')$ (complement)

$= b \vee (a \vee b')$ (identity)

$= b \vee (b' \vee a)$ (commutative)

$= (b \vee b') \vee a$ (associative law)

$= I \vee a$ (complement law)

$= I$ (Identity law)

Space for learners:

Also, $(a \vee b) \wedge (a' \wedge b') = [(a \vee b) \wedge a'] \wedge b'$ (associativity)

$= [a \wedge a') \vee (b \wedge a')] \wedge b'$ (distributive law)

$= [0 \vee (b \wedge a')] \wedge b'$ (complement)

$= (b \wedge a') \wedge b'$ (identity)

$= b \wedge b' \wedge a'$

$= 0 \wedge a'$

$= 0$

Hence, $a' \wedge b'$ is complement of $a \vee b$,

i.e. $(a \vee b)' = a' \wedge b'$.

5(ii). It is the dual of 5(i)

6(i). We know that,

$(a \vee b)' = a' \wedge b'$ [By De Morgan's Law]

$(a \vee b)'' = (a' \wedge b')'$. [Taking Complement on both sides]

$(a \vee b) = (a' \wedge b')'$[Since, $a'' = a$]

6(ii). It is the dual of 6(i)

7(i). LHS= $a \wedge (a' \vee b)$

$= (a \wedge a') \vee (a \vee b)$ [By Distributive Law]

$= 0 \vee (a \vee b)$ [By Complement Law]

$= (a \vee b)$ [Since, $0 \vee x = x$]

=RHS

7(ii). is the dual of 7(i)

4.5.1 Theorem

Uniqueness of the complement: If $x \vee y=1$ and $x \wedge y=0$, then $y=x'$.

Proof:

We know that,

$y = y \vee 0$ [Since, $x \vee 0=x$]

$= y \vee (X \wedge X')$ [by Complement law B4]

Space for learners:

$= (y \vee x) \wedge (y \vee x')$ [by Distributive law B2]

$= (x \vee y) \wedge (y \vee x')$ [by Commutative Laws B1]

$= 1 \wedge (y \vee x')$ [by hypothesis]

$= (y \vee x') \wedge 1$ [by Commutative Laws B1]

$= y \vee x'$ [Since, $x \wedge 1 = x$]

Again, $x' = x' \vee 0$ [Since, $x \vee 0 = x$]

$= x' \vee (x \wedge y)$ [by hypothesis]

$= (x' \vee x) \wedge (x' \vee y)$ [by Distributive law B2]

$= (x \vee x') \wedge (x' \vee y)$ [by Commutative Laws B1]

$= 1 \wedge (x' \vee y)$ [by Complement law B4]

$= (x' \vee y) \wedge 1$ [By Complement law B4]

$= (x' \vee y)$ [since, $x \wedge 1 = x$]

$= (y \vee x')$ [by Commutative Laws B1]

$= y$[Already proved that $y = y \vee x'$]

Hence, If $x \vee y = 1$ and $x \wedge y = 0$, then $y = x'$.

CHECK YOUR PROGRESS-I

1.Find the duals of the following Boolean Expression

(a) $x \vee y$ (b) $(a \vee b) \vee c = a \vee (b \vee c)$ (c) $a \wedge (a' \vee b) = (a \wedge b)$

(d) $(a \wedge b)' = a' \vee b'$

2. Let $D_{30} = \{ 1, 2, 3, 5, 6, 10, 15, 30 \}$ be the set of all divisors of 30 and let $\vee$ and $\wedge$ be two operations on B as defined below : $a \vee b$ = L C M of a and b ,$a \wedge b$ = GCD of a and b. Also , for each $a \in B$, let us define $a' = 30/a$ Then , show that (D_{30} , $\vee$, $\wedge$, ') is a Boolean algebra.

Space for learners:

4.6 BOOLEAN EXPRESSION

Space for learners:

Let, (A, ∧, ∨,') be a Boolean algebra. Then expression involving members of A and the operations ∧, ∨ and complementation are called Boolean expression or Boolean Polynomials.

Let x_1, x_2,…, x_n be a set of n variables (or letters or symbols). A Boolean Polynomial (Boolean expression, Boolean form or Boolean formula) $p(x_1, x_2, \ldots, x_n)$ in the variables $x_1, x_2, \ldots, x_n$ is defined recursively as follows:

1. The symbols 0 to 1 are Boolean polynomials
2. $x_1, x_2, \ldots, x_n$ are all Boolean polynomials
3. if $p(x_1, x_2, \ldots, x_n)$ and $q(x_1, x_2, \ldots, x_n)$ are two Boolean polynomials, then

   $p(x_1, x_2, \ldots, x_n) \vee q(x_1, x_2, \ldots, x_n)$ and $p(x_1, x_2, \ldots, x_n) \wedge q(x_1, x_2, \ldots, x_n)$ are also Boolean polynomials.
4. If $p(x_1, x_2, \ldots, x_n)$ is a Boolean polynomial, then

   $(p(x_1, x_2, \ldots, x_n))'$ is also Boolean polynomials
5. There are no Boolean polynomials in the variables $x_1, x_2, \ldots, x_n$ other than those obtained in accordance with rules 1 to 4.

For example, for variables x, y and z, the expressions

$p1(x, y, z) = (x \vee y) \wedge z$

$p2\ (x, y, z) = (x \vee y') \vee (y \wedge 1)$

$p3(x, y, z) = (x \vee (y' \wedge z)) \vee (x \wedge (y \wedge 1))$ are Boolean expressions.

Note: A Boolean expression of n variables, there may or may not contain all the n variables.

4.6.1 Minimization of Boolean Expression

1.Simplify the following Boolean Expression

(a)$(A'\wedge B'\wedge C') \vee (A'\wedge B\wedge C')\vee (A\wedge B'\wedge C')\vee(A\wedge B\wedge C')$

(b) $(A\wedge B) \vee (A\wedge C)' \vee [(A\wedge B'\wedge C) \wedge (A\wedge B)\vee C]$

Solutions:

1.(a) $(A'\wedge B'\wedge C') \vee (A'\wedge B\wedge C')\vee (A\wedge B'\wedge C')\vee(A\wedge B\wedge C')$

$= [(A' \wedge C') \wedge(B' \vee B)] \vee [(A \wedge C') \wedge (B' \vee B)]$ [Distributive law]

$= [(A' \wedge C') \wedge 1] \vee [(A \wedge C') \wedge 1]$ [Since, $B' \vee B =1$]

$= (A' \wedge C') \vee (A \wedge C')$ [Since $A \wedge 1= A$]

$= C' \wedge(A' \vee A)$ [Distributive law]

$= C' \wedge 1$ [Since, $B' \vee B =1$]

$= C'$ [Since $A \wedge 1= A$]

1. (b) $(A\wedge B) \vee (A\wedge C)' \vee [(A\wedge B'\wedge C) \wedge (A\wedge B)\vee C]$

$= (A\wedge B) \vee (A\wedge C)' \vee (A\wedge B'\wedge C \wedge A\wedge B)\vee (A\wedge B'\wedge C\wedge C)$

$= (A\wedge B) \vee (A' \vee C') \vee 0 \vee (A\wedge B'\wedge C)$ [By De Morgans law and $B\wedge B'=0, C\wedge C=C$]

$=(A\wedge B) \vee (A' \vee C') \vee (A\wedge B'\wedge C)$

$= (A\wedge B) \vee (A' \vee C') \vee(B'\wedge C)$ [Since, $A\vee (A\wedge B)=A\vee B$]

$= A' \vee (A\wedge B) \vee C' \vee(C \wedge B')$

$= A' \vee B \vee C' \vee B'$

$= A' \vee C' \vee 1$ [since, $B \vee B'=1$]

$= A' \vee 1$ [Since, $C' \vee 1 =1$]

$=1$

4.7 BOOLEAN FUNCTION

Each Boolean expression represents a Boolean function. Any function specifying a Boolean expression is called a Boolean function.

Let, $B=\{0,1\}$.Then $B_n=\{ (x_1,x_2,\ldots\ldots x_n)| x_i\in B \text{ for } 1\leq i \leq n \}$ is the set of all possible n-tuples of 0s and 1s.The variable x is called a Boolean variable if it assumes values only from B,that is,if its only possible values are 0 and 1. A function from B_n to B is called a Boolean function of degree n.

Thus if $f(x,y) = x\wedge y$, then f is the Boolean function and $x\wedge y$ is the boolean expression (or the value of the function f).

Space for learners:

4.8 CONJUNCTION (∧) OPERATION

The Conjunction or Boolean product of two variables x and y, which is denoted by xy or x∧y gives a value 1 when both x and y have the value 1 and the value 0 otherwise.

X	y	x∧y
0	0	0
0	1	0
1	0	0
1	1	1

4.9 DISJUNCTION (∨) OPERATION

The Disjunction or Boolean sum of two variables x and y, which is denoted by x+y or x∨y gives a value 1 when either x or y or both has the value 1 and the value 0 otherwise

X	y	x∨y
0	0	0
0	1	1
1	0	1
1	1	1

4.10 COMPLEMENTATION(′)

It is an expression with the value 1 when x has the value 0 and the value 0 when x has the value 1.

Examples1:Find the values of Boolean function f(x,y)=x∧y′

Examples2: Find the values of Boolean function f(x, y, z)=(x∧y) ∨ z′

Solution1:It is a Boolean function of two variables. The values are displayed in the table given below

X	y	y′	f(x,y)= x∧y′
1	1	0	0
1	0	1	1
0	1	0	0
1	1	O	0

Space for learners:

Solution2: It is a Boolean function of 3 variables. The values are displayed in the table given below:

X	y	z	$x \wedge y$	z'	$f(x,y,z)=(x \wedge y) \vee z'$
1	1	1	1	0	1
1	1	0	1	1	1
1	0	1	0	0	0
1	0	0	0	1	1
0	1	1	0	0	0
0	1	0	0	1	1
0	0	1	0	0	0
0	0	0	0	1	1

4.11 DEFINITION OF LITERAL

A literal is a Boolean variable or complemented variable such as x, x′, y, y′, and so on.

4.12 FUNDAMENTAL PRODUCT OR MINTERM

A fundamental product is a literal or a product of two or more literal in which no two literals involve the same variable. Fundamental product is also called a minterm or complete product.

A minterm in n variables is a product of n literals in which each variable is represented by the variable itself or its complement.

A minterm of the Boolean variables x_1, x_2, … x_n is a Boolean product $y_1 \wedge y_2 \wedge y_3 \dots \wedge y_n$, where $y_i=x_i$ or $y_i=x'_i$

For example, for a 3 variable Boolean function there are 8 nos of possible minterms, which are

$x \wedge y \wedge z$, $x' \wedge y \wedge z$, $x \wedge y' \wedge z$, $x \wedge y \wedge z'$

$x \wedge y' \wedge z'$ $x' \wedge y \wedge z'$ $x' \wedge y' \wedge z$ $x' \wedge y' \wedge z'$

4.13 DEFINITION OF MAXTERM

A maxterm in n variable is a sum of n literals in which each variable is represented by the variable itself or its complement.

A maxterm of the Boolean variables x_1, x_2,… x_n is a Boolean sum $y_1 \vee y_2 \vee y_3 \dots \vee y_n$, where $y_i=x_i$ or $y_i=x'_i$

Space for learners:

For example, for a 3 variable Boolean function there are 8 nos of possible maxterms, which are

$x \vee y \vee z$, $x' \vee y \vee z$, $x \vee y' \vee z$, $x \vee y \vee z'$

$x \vee y' \vee z'$ $x' \vee y \vee z'$ $x' \vee y' \vee z$ $x' \vee y' \vee z'$

4.14 CANONICAL FORM OR NORMAL FORM

A Boolean function can be uniquely described by its truth table or in one of the canonical forms. Two dual canonical forms are:

(1) The sum of Minterms (SOM) or Sum of Product (SOP) or Disjunctive normal form (DNF)

(2) The Product of Maxterm or Product of Sum (POS) or Conjunctive Normal form (CNF)

4.14.1 Sum of Minterms (SOM) /Sum of Products (SOP) / Disjunctive Normal Form (DNF)

A Boolean function(expression) is said to be in Disjunctive normal form in n variables $x_1, x_2, \ldots\ldots x_n$ if it can be written as join(Sum) of terms of the type $f_1(x_1) \wedge f_2(x_2) \wedge \ldots\ldots f_n(x_n)$ where $f_i(x_i)$ or x'_i for all i=1,2,….n and no two terms are same. Also 1 and 0 are said to be in disjunctive normal form.

Here, $f_1(x_1) \wedge f_2(x_2) \wedge \ldots\ldots f_n(x_n)$ are called minterms or minimal polynomials.

For example, $(x \wedge y \wedge z') \vee (x \wedge y' \wedge z') \vee (x' \wedge y \wedge z')$ is a Boolean expression in SOM form.

4.14.2 Rules for Converting Output Expression into SOM

There are two ways by which we can convert the output expression in SOM form-

First Way

(a) Examine each term in the given logic function. Retain if it is a minterm; continue to examine the next term in the same manner.

Space for learners:

(b) Check for variables that are missing in each product, which is not a minterm. Multiply (∧) the product by ($x \vee x'$) term, for each variable x that is missing.

(c) Multiply (∧) all the products and eliminate the redundant term.

Second Way: Procedure for obtaining the output expression in SOM from a truth table:

1. Give a product term for each input combination in the table, containing an output value of 1.

2. Each product term contains its input variables in either complemented or uncomplemented form.

3. All the product terms are Summed (∨)together in order to produce the final SOM expression of the output.

Example: *Find the SOM expansion for the function* $f(x, y, z) = (x \vee y) \wedge z'$

Space for learners:

Solution: We will find the SOM expansion of $f(x,y,z) = (x \vee y) \wedge z'$ in two ways.

First way: By using Boolean identities

Given, $f(x,y,z) = (x \vee y) \wedge z'$

$= (x \wedge z') \vee (y \wedge z')$ [Distributive law]

$= (x \wedge 1 \wedge z') \vee (1 \wedge y \wedge z')$ [Identity law]

$= [x \wedge (y \vee y') \wedge z')] \vee [(x \vee x') \wedge y \wedge z')]$ [complement law]

$= (x \wedge y \wedge z') \vee (x \wedge y' \wedge z') \vee (x \wedge y \wedge z') \vee (x' \wedge y \wedge z')$ [Distributive law]

$= (x \wedge y \wedge z') \vee (x \wedge y' \wedge z') \vee (x' \wedge y \wedge z')$ [By idempotent law]

Second Way:

we can construct the sum of Minterm expansion by determining the values of for all possible values of the variables x,y and z.

Now, the Sum of Product expansion of f is the Boolean Sum(∨) of the three minterms corresponding to the three rows of the table that give the value 1 for the function.

X	Y	Z	$x \vee y$	z'	$f(x,y,z)=(x \vee y) \wedge z'$	Minterm
1	1	1	1	0	0	
1	1	0	1	1	1	$x \wedge y \wedge z'$
1	0	1	1	0	0	
1	0	0	1	1	1	$x \wedge y' \wedge z'$
0	1	1	1	0	0	
0	1	0	1	1	1	$x' \wedge y \wedge z'$
0	0	1	0	0	0	
0	0	0	0	1	0	

Therefore, $f(x,y,z)= (x \wedge y \wedge z') \vee (x \wedge y' \wedge z') \vee (x' \wedge y \wedge z')$

Example1. Convert the function into SOM form $[(x\wedge y') \vee z'] \wedge (x'\vee z)'$

Solution:

$[(x\wedge y') \vee z'] \wedge (x'\vee z)'$

$= [(x'\vee y'') \vee z'] \wedge (x'\vee z)'$ [By De Morgan's Law]

$= [(x'\vee y \vee z'] \wedge (x'\vee z)'$ [Since, $y''=y$]

$= [(x'\vee y \vee z'] \wedge (z\vee x')'$ [By Commutative law]

$= [(x'\vee y \vee z'] \wedge (z'\wedge x'')$ [By De Morgan's Law]

$= [(x'\vee y \vee z'] \wedge (z'\wedge x)$ [since $x''=x$]

$= (x'\wedge z'\wedge x) \vee (y \wedge z'\wedge x) \vee (z'\wedge z'\wedge x)$ [By distributive law]

$= 0 \vee (y \wedge z'\wedge x) \vee (z'\wedge z'\wedge x)$ [since $x \wedge x'=0$]

$=0 \vee (y \wedge z'\wedge x) \vee (z'\wedge x)$ [Since $z'\wedge z' = z'$, Idempotent Laws]

$= (x \wedge y \wedge z') \vee (z'\wedge x)$ [Since $0 \vee a=a$]

$= (x \wedge y \wedge z') \vee[(z'\wedge x) \wedge 1]$ [Since, $a \wedge 1=1$]

$=(x \wedge y\wedge z') \vee [(z'\wedge x)\wedge (y \vee y')]$ [Since, $a \vee a'= 1$]

$= (X\wedge y\wedge z') \vee[(z'\wedge x\wedge y) \vee (z'\wedge x\wedge y')]$ [By distributive law]

$= (x \wedge y \wedge z') \vee[(x\wedge z'\wedge y) \vee (x\wedge z'\wedge y')]$

$=(x \wedge y \wedge z') \vee (x\wedge y'\wedge z')$

Space for learners:

4.14.3 Product of Maxterms (POM) / Product of Sums (POS) / Conjunctive Normal Form (CNF)

Space for learners:

A Boolean function(expression) is said to be in Conjunctive normal form in n variables $x_1, x_2, \ldots\ldots x_n$ if it can be written as meet(Product) of terms of the type $f_1(x_1) \vee f_2(x_2) \vee \ldots\ldots f_n(x_n)$ where $f_i(x_i)$ or x'_i for all i=1,2,….n and no two terms are same. Also 1 and 0 are said to be in disjunctive normal form.

Here, $f_1(x_1) \vee f_2(x_2) \vee \ldots\ldots f_n(x_n)$ are called Maxterms or maximal polynomials

For example,

$(x \vee y \vee z') \wedge (x \vee y' \vee z') \wedge (x' \vee y \vee z')$ is a boolaen expression in POM form

4.14.4 Rules for Converting the Output Expression into POM

There are two ways by which we can convert the output expression in POM form

First Way

(a) Examine each term in the given logic function. Retain if it is a Maxterm; continue to examine the next term in the same manner.

(b) Check for variables that are missing in each sum, which is not a maxterm. Add $(x \wedge x')$ to the sum term, for each variable x that is missing.

(c) Expand the expression using the distributive property and eliminate the redundant term.

Second Way

The procedure for obtaining the output expression of a Boolean function in POM form from a truth table.

(a) Give a sum term for each input combination in the table, which has an output value 0.

(b) Each sum terms contains all its input variables in complemented or uncomplemented form. If the input variable is 0, then it appears in an uncomplemented form; if the input variable is 1, it appears in the complemented form.

(c) All the sum terms are AND operated ($\wedge$) together to obtain the final POM expression.

Example: Convert the function in POM form

$$Y = A \vee (B' \wedge C)$$

Solution:

First way:

Here,

$Y = A \vee (B' \wedge C)$

$= (A \vee B') \wedge (A \vee C)$ [By Distributive law]

$= (A \vee B' \vee 0) \wedge (A \vee C \vee 0)$ [Since $a \vee 0 = a$]

$= [A \vee B' \vee (C \wedge C')] \wedge [A \vee C \vee (B \wedge B')]$ [Since, $a \wedge a' = 0$]

$= (A \vee B' \vee C) \wedge (A \vee B' \vee C') \wedge (A \vee C \vee B) \wedge (A \vee C \vee B')$ [Distributive law]

$= (A \vee B \vee C) \wedge (A \vee B' \vee C) \wedge (A \vee B' \vee C')$ [Since, $A \wedge A = A$]

Second Way:

A	B	C	B'	$B' \wedge C$	$Y = A \vee (B' \wedge C)$	Maxterm
0	0	0	1	0	0	$(A \vee B \vee C)$
0	0	1	1	1	1	
0	1	0	0	0	0	$(A \vee B' \vee C)$
0	1	1	0	0	0	$(A \vee B' \vee C')$
1	0	0	1	0	1	
1	0	1	1	1	1	
1	1	0	0	0	1	
1	1	1	0	0	1	

From the truth table, we have seen that for the given 3-input function we find the Y value is 0 for the input combinations 000,010 and 011 and their corresponding Maxterms are $(A \vee B \vee C)$, $(A \vee B' \vee C)$ and $(A \vee B' \vee C')$

Therefore, the required POM form is,

$(A \vee B \vee C) \wedge (A \vee B' \vee C) \wedge (A \vee B' \vee C')$

Space for learners:

CHECK YOUR PROGRESS-II

4.Simplify the following Boolean Expression

(a) $(A\vee B\vee C)\wedge(A\vee B'\vee C')\wedge(A\vee B\vee C')\wedge(A\vee B'\vee C)$

(b) $(A\wedge B)\vee(B\wedge B)\vee C\vee B'$

(c) $A\vee(A'\wedge B)\vee(A'\wedge B'\wedge C)\vee(A'\wedge B'\wedge C'\wedge D)$

5. Obtain the Canonical SOM expression for the function $Y(A,B)=A\vee B$

6. Obtain the Canonical SOM expression for the function $Y(A,B,C)=A\vee(B\wedge C)$

7. Obtain the Canonical POM expression for the function

$Y(A,B,C)=(A\vee B')\wedge(B\vee C)\wedge(A\vee C')$

Space for learners:

4.15 APPLICATION OF BOOLEAN ALGEBRA

Boolean algebra is useful in designing switching circuits. Subsequently we will use Boolean algebra to design logic circuits for logical and arithmetic operations performed by processors.

Boolean Algebra of Switching circuits:

Let B = {0 ,1}, where 0 and 1 denote the two mutually exclusive states, off and on, of a switch respectively.

Let the operations of connecting the switches in parallel and connecting the switches in series be denoted by + and. respectively.

Let $0'=1$ and $1'=0$. Then, [B, ∨, ∧, ‘] is a Boolean algebra, known as the Boolean algebra of switching circuits

The composition tables for the above operations are given below:

∨	0	1
0	0	1
1	1	1

∧	0	1
0	0	1
1	1	1

'	
0	1
1	0

Boolean switching circuit: An arrangement of wires and switches formed by the repeated use of a combination of switches in parallel and series is called a Boolean switching circuit.

Equivalent switching circuits: Two switching circuits A and B, are said to be equivalent, denoted by A ~B if both are in the same state for the same states of their constituent switches. Thus, two switching circuits are said to be equivalent if and only if their corresponding Boolean functions are equal. This happens when their Boolean function have the same value, o or 1, for every possible assignment of the values o and 1 to their variables

4.16 SUMMING UP

- A non-empty set B with two binary operations ∨ and ∧, a unary operation ′, and two distinct elements 0 and 1 is called a Boolean Algebra if commutative, distributive, identity and complement properties hold for any elements a, b, c ∈ B.
- By the dual of a proposition concerning a Boolean algebra B, we mean the proposition obtained by substituting ∨ for ∧, ∧for V, 0 for 1, and 1 for 0, i.e., by exchanging ∧ and V, and exchanging 0 and. Any pair of expression satisfying this property is called Dual expression.
- Let (A, ∧, ∨,') be a Boolean algebra. Then expression involving members of A and the operations ∧, ∨ and complementation are called Boolean expression or Boolean Polynomials.
- Any function specifying a Boolean expression is called a Boolean function. A literal is a Boolean variable or complemented variable such as x, x′, y, y′, and so on.

Space for learners:

- A minterm in n variable is a product of n literals in which each variable is represented by the variable itself or its complement. A maxterm in n variable is a sum of n literals in which each variable is represented by the variable itself or its complement.
- Boolean algebra is useful in designing switching circuits. Subsequently we will use Boolean algebra to design logic circuits for logical and arithmetic operations performed by processors.

Space for learners:

4.17 ANSWERS TO CHECK YOUR PROGRESS

1.(a) $x \wedge y$ (b) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

(c) $a \vee (a' \wedge b) = (a \vee b)$

(d) $(a \vee b)' = a' \wedge b'$

2. The given operations on D_{30} satisfy the following properties:

(a) Closure properties:

Let, a and b be any two arbitrary elements of D_{30}. Then, each one of a and b is a divisor of 30, that means LCM of a and b is a divisor of 30 and HCF of a and b is a divisor of 30.

So, for all a and b,

$(a \vee b) \in D_{30}$ and $(a \wedge b) \in D_{30}$.

So, D_{30} is closed for each of the operations $\vee$ and $\wedge$

(b) Commutative laws:

Let, a and b be any two arbitrary elements of D_{30}

Then, LCM of a and b= LCM of b and a

So, for all $a, b \in D_{30}, a \vee b = b \vee a$, and,

HCF of a and b=HCF of b and a

So, for all $a, b \in D_{30}, a \wedge b = b \wedge a$,

Hence, the given Boolean algebra follows Commutative law

(c). Associative laws:

Let a,b, c be arbitrary elements of B.

(i) LCM [{LCM (a, b)} and c] = LCM [a and {LCM (b, c)}]

$\Rightarrow (a \vee b) \vee c = a \vee (b \vee c)$ for all $a, b, c \in D_{30}$

(ii) HCF [{HCF (a, b)} and c] = HCF [a and {HCF (b, c)}]

$\Rightarrow (a \wedge b) \wedge c = a \wedge (b \wedge c)$ for all a, b, c $\in D_{30}$

So, it follows the Associative law

(d). Distributive laws:

Let a and b be any two arbitrary elements of D_{30}

Then, we know that HCF is distributive over LCM, and LCM is distributive over HCF

(i) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ for all a, b, c $\in D_{30}$. [Distributive law of HCF over LCM]

(ii) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ [distributive law of LCM over HCF]

(e). Existence of identity elements

Clearly, $1 \in D_{30}$ and $30 \in D_{30}$

Such that (i) $a \vee 1$ = LCM (a and 1) = a for all $a \in D_{30}$

(ii) $a \wedge 30$=HCF(a and 30)=a for all $\in D_{30}$

This shows that 1 is the identity element for $\vee$ and 30is the identity element for $\wedge$

(f). Existence of complement

For each $a \in D_{30}$

Let us define its complement $a' = 30/a$

Then, we have (i) $(a \vee a')$=LCM (a, 30/a) =30

(ii) $a \wedge a'$ =HCF(a, 30/a)=1

Now,

{1′= 30 and 30′= 1};{2′= 15 and 15′= 2}; { 3′= 10 and 10′= 3};{5′= 6 and 6′= 5}.

Thus, each $a \in D_{30}$ has its complement a' in B.

Hence,

$(D_{30}, \vee, \wedge, ')$ is a Boolean algebra.

3. (a) A

3. (b) 1

3. (c) $A \vee B \vee C \vee D$

Space for learners:

4. $(A \wedge B) \vee (A \wedge B') \vee (A' \wedge B)$

5. $(A \wedge B \wedge C) \vee (A \wedge B \wedge C') \vee (A \wedge B' \wedge C') \vee (A' \wedge B \wedge C)$

6. $(A \vee B' \vee C) \wedge (A \vee B' \vee C') \wedge (A \vee B \vee C) \wedge (A' \vee B \vee C) \wedge (A \vee B \vee C')$

7. $(X \vee Y \vee Z') \wedge (X \vee Y' \vee Z) \wedge (X' \vee Y \vee Z) \wedge (X' \vee Y \vee Z')$

4.18 POSSIBLE QUESTIONS

1. Find a Boolean product of the variables x, y and z or their complement that has the value 1 if and only if

(a) $x=y=0, z=1$ (b) $x=0, y=1, z=0$ (c) $x=0, y=z=1$ (d) $x=y=z=0$

2. Find the sum of product expansion of the function $f(x,y,z)=x$

3. With the values of truth table express the values of the following Boolean Function

(a) $F(x,y,z)=(x \wedge y') \vee (xyz)'$ (b) $F(x,y,z)=(x' \wedge y) \vee (y' \wedge z)$

4. With the help of the truth table of Conjunction and Disjunction Operation verify De Morgan's Laws.

5. Using identities of Boolean algebra show that

$(x \wedge y') \vee (y \wedge z') \vee (x' \wedge z) = (x' \wedge y) \vee (y' \wedge z) \vee (x \wedge z')$

4.19 REFERENECS AND SUGGESTED READINGS

- Lattices and Boolean Algebra first concept, Second Edition By Vijay K Khanna
- Discrete Mathematical Structures with Application to Computer Science by J.P Tremblay & R. Manohar.

Space for learners:

UNIT 5: ALGEBRAIC STRUCTURES

Space for learners:

Unit Structure:

5.1 INTRODUCTION

An algebraic structure consists of a non-empty set together with one or more binary compositions which satisfies some postulates. An Algebraic structure is the collection of any particular models of a given set of axioms. If$*$ is a binary operation on G. Then $(G, *)$ is an algebraic structure. $(R, +, .)$ is an algebraic structure equipped with two operations

5.2 UNIT OBJECTIVES

After going through this unit, you will be able to:

- understand the basics of group and its various properties.
- know the cancellation laws of groups
- define subgroups and various operations on subgroups
- understand the Lagrange's Theorem
- understand ring and its operations
- give the definition of field
- understand the vector space

5.3 GROUP: THEOREM AND PROPERTIES

Group: A non-empty set G, together with a binary composition '$*$' (star) is said to form a group, if it satisfies the following postulates

(i) Closure property:

$a * b \in G$, for all $a, b \in G$

(ii) Associativity:

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

(iii) Existence of identity:

There exists a unique element $e \in G$, called the identity element of G such that

$$a * e = a = e * a \text{, for all } a \in G$$

Space for learners:

(the element e is called the identity element)

(iv) Existence of inverse:

For every $\in G$, there exist $a' \in G$(depending upon a) such that

$$a * a' = e = a' * a.$$

Note: (i) The group G with the binary operation $*$ is sometimes denoted by $<G ,*>$

(ii) In particular the group $< G , +>$ is called an addition group, the binary operation being addition.

(iii) In particular the group $< G , . >$ is called a multiplication group, the binary operation being multiplication.

1. Theorem: The identity element in a group is unique.

Proof: Let G be a group. If possible, let e and e' be two identity elements of a group G.

We have, $ee' = e$ if e' is the identity and $ee' = e'$ if e is the identity. But ee' is a unique element of G.

$\therefore ee' = e$ and $ee' = e \quad => e = e'$

Hence the identity element is unique.

2. Theorem: The inverse of each element of a group is unique.

Proof: Let a be any element of a group G and let e be the identity element. Suppose b and c are two inverses of a i.e.

$$ba = e = ab \ldots\ldots\ldots\ldots\ldots..(i) \text{ and}$$

$$ca = e = ac \ldots\ldots\ldots\ldots\ldots\ldots(ii)$$

We have, $(ba)c = ec \ (\therefore ba = e)$

$= c(iii)(\therefore eisidentity)$

Also, $b(ac) = b(e) \ (\therefore ac = e)$

$= be = b(iv)$

But in a group composition is associative

$\therefore b(ac) = (ba)c => b = c$

Hence, inverse of an element of a group is unique.

3. Theorem: The inverse of product of two elements of a group is the product of the inverse taken in the reverse order.

OR

Prove that $(ab)^{-1} = b^{-1}a^{-1} \forall a , b \in G$, where $G$is a group.

Space for learners:

Space for learners:

Proof: Let a and b be elements of G.

If a^{-1} and b^{-1} are inverse of a and b respectively.

Then $aa^{-1} = e = a^{-1}a$ and $bb^{-1} = e = b^{-1}b$, where e is the identity element.

Now,

$$(ab)(b^{-1}a^{-1}) = [(ab)b^{-1}]a^{-1} \left(\begin{matrix}\because compositionisan \\ associative\end{matrix}\right)$$

$$= [a(bb^{-1})]a^{-1}(byassociativity)$$

$$= [ae]a^{-1}(\because bb^{-1} = e)$$

$$= aa^{-1}(\because ae = a)$$

$$= e$$

Also,

$(b^{-1}a^{-1})(ab) = b^{-1}[a^{-1}(ab)]$, by associativity

$$= b^{-1}[(a^{-1}a)b]$$

$$= b^{-1}(eb)(\because a^{-1}a = e)$$

$$= b^{-1}b$$

$$= e \quad (\because b^{-1}b = e)$$

Thus, we have $(ab)(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})(ab)$

$\therefore$by definition of inverse, we have $(ab)^{-1} = b^{-1}a^{-1}$

Example: Show that the set N of all natural numbers N is not a group with respect to addition.

Solution:

(i) Closure: Property:

We know that sum of two natural number is natural number.

$\therefore$ N is closed with respect to addition.

(ii) Associativity:

Also, addition of natural number is an associative composition.

(iii) Existence of identity:

But there exist no natural number $e \in N$ such that $e + a = a = a + e \;\forall a \in N$

For addition, 0 is the identity but $0 \notin N$

Hence, condition of existence of identity is not satisfied.

$\therefore$ N is not a group w.r.t. addition.

$\therefore < N , + >$ is not a group.

5.4 BASIC TERMS AND THEIR DEFINITION

Space for learners:

Commutative group (or Abelian group):

A commutative group is an order pair $(G\ ,\ *)$ where G is a non-empty set and $*$ is a binary operation defined on G such that the following properties hold.

(i) Closure property:

$a * b \in G$, for all $a\ , b \in G$

(ii) Associativity:

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

(iii) Existence of identity:

There exists an element $\in G$, called the identity element of G such that $a * e = a = e * a\ , \forall a \in G$.

(iv) Existence of inverse:

For any $\in G$, $\exists$ an element $a' \in G($ depending on a) such that $a * e' = e = e' * a$, where a' is called inverse of a.

(v) Commutativity:

The binary composition $*$ is commutative i.e.,

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

Semi-Group: A non-empty set G together with binary composition $(.)$ is called a semi-group if

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

Note: Every group is a semi-group.

Monoid: A non-empty set G together with binary composition which is associative and identity element exists is said to be a monoid.

Finite group and Infinite group:

If in a group, the set G has a finite number of distinct elements is known as a finite group and if the number of elements of the set are infinite then it is known as an infinite group.

Order of a group:

The number of elements in a finite group is called the order of the group and is denoted by $O(G)$ or $|G|$. E.g., In the group

$G = \{1\ , -1\ , i\ , -i\}$

The order of group is $O(G) = 4$.

Space for learners:

Order of an element in a group (Period):

The order of an element a in a group G is the least positive integer $n(if exist)$ such that $a^n = e$, the identity element of G and we write $O(a) = n$.

If $a^n \neq e \forall$ positive integer n then a is said to be of infinite order or of zero order.

Example 1: Show that the set of integers, I is a group with respect to the operation of addition.

Solution:

(i) Closure property:
We know that sum of two integer is also an integer i.e.

$$a + b \in I \ , \ \forall a , b \in I$$

Thus I is closed with respect to addition.
(ii) Associativity:
We know that addition of integers is an associative composition.

$$\therefore a + (b + c) = (a + b) + c \forall a , b , c \in I$$

(iii) Existence of identity:
The number $0 \in I$, also we have

$$0 + a = a = a + 0 \ \forall a \in I$$

$\therefore$the integer 0 is an identity.
(iv) Existence of inverse:
For any $a \in I$, then $-a \in I$
$\therefore a + (-a) = 0 = (-a) + a$
$\therefore I$is a group with respect to addition
i.e.$< I , + >$is a group.

5.5 CANCELLATION LAWS

If a , b , c are any elements of G then
(i) $ab = ac => b = c$ (Left cancellation law)
(ii) $ba = ca => b = c$ (Right cancellation law)

Proof: Let e be the identity

Since, $a \in G$ =>there exist $a^{-1} \in G$ such that $a^{-1}a = e = aa^{-1}$

Now, $ab = ac$

$=> a^{-1}(ab) = a^{-1}(ac)$ *(multiplying both sides on left by* a^{-1} *)*

$=> (a^{-1}a)b = (a^{-1}a)c$ *, by associativity*

$=> eb = ec(\because\ a^{-1}a = e)$

$=> b = c$ *(* $\because$ *e is the identity)*

$\therefore ab = ac => b = c$

Example 1: Show that the cancellation laws do not hold in a semi-group.

Solution: Consider the set M of all 2×2 matrices over integers under matrix multiplication, which forms a semi-group.

If we consider $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}$ and $C = \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix} \in M$

Then, $AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

& $AC = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$\therefore AB = AC$

But, $B \neq C$

$\therefore$ the cancellation laws do not hold in a semi-group

Example 2: Prove that if for every element a in a group G , $a^2 = e$ where e is the identity element of G then show that G is abelian.

Solution: Let G be a group such that $a^2 = e \forall a \in G$ where e is the identity element of G.

We are to show that G is abelian.

Let $a, b \in G$ then $ab \in G$ and so

$(ab)^2 = e$

$=> (ab)(ab) = e$

$=> (ab)(ab)b^{-1} = eb^{-1}$ $\qquad [\ \because b^{-1} \in G]$

$=> (ab)a(bb^{-1})a^{-1} = b^{-1}a^{-1}$ $\qquad [\because a^{-1} \in G\ ]$

$=> (ab)(aea^{-1}) = b^{-1}a^{-1}$

$=> abe = b^{-1}a^{-1}$

$=> ab = b^{-1}a^{-1}$ …………………… (i)

Also, $a \in G => a^2 = e$, by hypothesis

Space for learners:

$=> ae = e$

$=> (aa)a^{-1} = ea^{-1} [\because a^{-1} \in G]$

$=> a(aa^{-1}) = a^{-1}$

$\therefore a = a^{-1}$ .... (ii)

Similarly, $b \in G => b^2 = e$

$=> b = b^{-1}$ .... (iii)

Using (ii) and (iii) we get from (i)

$ab = ba$

Thus ,a , $b \in G => ab = ba$

So $G$is abelian.

5.5.1 Permutation Group

Let A be a finite set (may be finite or infinite) and $f: A \to A$ is bijective mapping then S is called permutation group i.e.

$$P(A) = \{f: A \to A: f \text{ is bijective mapping}\}$$

The number of elements in the finite set S is known as the degree of permutation.

Cycle or circular permutation:

Let $\propto \in S_n$, then α is called a cycle or circular permutation if there exists

$\{i_1, i_2, \dots\dots, i_r\}$ such that $\alpha(i_1) = i_2$,

$\alpha(i_2) = i_3, \dots\dots\dots\dots, \alpha(i_{r-1}) = i_r$,

$\alpha(i_r) = i_1$ then permutation is represented by $\alpha = (i_1 i_2 \dots\dots\dots\dots i_r)$ and $\alpha(i) = i$ for all other $i \in S_n$

5.6 SUBGROUP

Sub group: Let $< G ,*>$ be a group and H be a non-empty subset of G. Then H is called a subgroup G. Then H is called a subgroup G if and only if H itself is a group under the binary composition '$*$' defined on G.

The above definition can be written in full as follows:

Space for learners:

Let $< G ,*>$ be a group and $\subseteq G$, $H \neq \phi$. Then H is called a subgroup of G if

(i) H is closed w.r.t. the binary composition '$*$' i.e. $a * b \in H$ $\forall a \ , b \in H$.

(ii) '$*$' is associative in H(which is obvious since G is group).

(iii) $e \in H$, where e is the identity element of G .

(iv) $\forall a \in H$ there exist $a^{-1} \in H$ such that $a * a^{-1} = e = a^{-1} * a$.

Example 1: Show that a non-empty subset H of a group G is a subgroup of G if and only $, b \in H => ab^{-1} \in H$.

Solution: Let G be a group and H be a non empty subset of G.

We assume, H be a subgroup of G then H itself a group w.r.t. the binary composition defined on G. We show that $a , b \in H => ab^{-1} \in H$

Let $, b \in H$, since H is a group.

$b \in H => b^{-1} \in H$

Thus, $a , b \in H => a , b^{-1} \in H$

$=> ab^{-1} \in H$ [since H is a group, so using closure property in H]

$\therefore a \ , b \in H => ab^{-1} \in H$

Conversely let H be such that $a , b \in H => ab^{-1} \in H$ .... (i)

We show that H is a subgroup of G.

(I) Existence of identity:

Let e be the identity element of G.

Since, H is nonempty so there exists $a \in H$

Taking $b = a$ in (i) , we see that $aa^{-1} \in H => e \in H$

$\therefore$ This shows the existence of identity in H

(II) Existence of inverse:

Let $a \in H$, by (I) ,$e \in H$

$\therefore e \in H , a \in H => ea^{-1} \in H$(using(i))

$=> a^{-1} \in H$

Thus, $a \in H => a^{-1} \in H$

This shows the existence of the inverse of every element in H.

(III) Closure property:

Let $a , b \in H$.

Space for learners:

Space for learners:

Then by (II), $b^{-1} \in H$

Thus, a,b$\in H => a(b^{-1})^{-1} \in H$ [by using (i)]

$=> ab \in H$

Thus, $a , b \in H => ab \in H$

Which shows that H is closed with respect to the composition G.

(IV) Associativity:

Let $a , b , c \in H$

Since, $\subseteq G$, $a , b , c \in G$

Since, G is a group , we have $(ab)c = a(bc)$

Hence, associativity holds in H.

From (I) to (IV), it follows that H itself a group with respect to composition G.

So, H is a subgroup of G .

Intersections of subgroups:

Theorem1. If H and K are two subgroups of a group G then $H \cap K$ is a subgroup.

Proof: Let H and Kbe two subgroups of a group G.

We are to show that $H \cap K$ is a subgroup of G.

Since, H and K are subgroups of G .

We have, $H \subseteq G$, $K \subseteq G$, $e \in H$, $e \in K$, where e is the identity element of G.

$=> H \cap K \subseteq G$ and $e \in H \cap K$

$=> H \cap K \subseteq G$ ....(i)

& $H \cap K \neq \phi$ ....(ii)

Finally, let $x , y \in H \cap K$ then,

$x , y \in H and x , y \in K$

Since, H is a subgroup of G,

$x , y \in H => xy^{-1} \in H$

Similarly, $x , y \in K => xy^{-1} \in K$

$\therefore xy^{-1} \in H$ & $xy^{-1} \in K$

$=> xy^{-1} \in H \cap K$

Thus, $x , y \in H \cap K => xy^{-1} \in H \cap K$ ....(iii)

From (i), (ii) and (iii) we see that

$\therefore H \cap K$ is a subgroup of G.

Give an example to show that union of two subgroup of a group may not be a subgroup of the group.

Solution: we consider the additive group $< I , +>$ of all integers. Let $H = \{2a / a \in I\}$ and $K = \{3a \;/\; a \in J\}$ then

$H \subseteq I \;, K \subseteq I$ and $H \neq \phi \;, K \neq \phi$ ....(i)

Also, $x , y \in H => x = 2a \,, \; y = 2b$, where $a , b \in I$

$=> x - y = 2(a - b) = 2c$, where $c = a - b \in I$

$=> x - y \in H$ .... (ii)

Similarly, $x \;, y \in K => x - y \in K$ ....(iii)

From (i), (ii) & (iii) we see that

$\therefore H$ and $K$are subgroups of I.

Now, $2 \in H \subseteq H \cup K \& 3 \in K \subseteq H \cup K$

$=> 2 , 3 \in H \cup K$

But $2 + 3 = 5 \notin H \& 2 + 3 = 5 \notin K$

$=> 2 + 3 = 5 \notin H \cup K$

Hence, $H \cup K$ is not closed with respect to addition and

consequently $H \cup K$ is not a subgroup of I .

Definition:

Coset: Let H be a subgroup of a group G. If $a \in G$ then the set $Ha = \{ha : h \in H\}$ is called the right coset of H in G generated by a.

Let H be a subgroup of a group. If $a \in G$ then the set

$aH = \{ah : h \in H\}$ is called the left coset of H in G generated by a.

Note: Any two right (left) cosets of a subgroup are either disjoint or

Identical.

Lagrange's Theorem:

Statement: The order of each subgroup of a finite group is a divisor of the order of the group.

Proof: Let G be a finite group and $o(G) = n$. Let H be a subgroup of G then H is obviously finite. Let $o(H) = m$.

We first show that $o(aH) = m \forall a \in G$

We define $f : H \to H$ by $f(h) = ah \forall h \in H$

Then, $h_1 , h_2 \in H \,, \; f(h_1) = f(h_2) => ah_1 = ah_2$

Space for learners:

$=> h_1 = h_2$, by left cancellation law.

$\therefore f$ is one-one.

Also, for an arbitrary element $ah \in aH$, we find $h \in H$ such that $f(h) = ah$ and so f is onto.

Thus, $f: H \rightarrow aH$ is bijection and consequently

$$o(aH) = o(H) = m \quad , \forall a \in G \ldots \ldots \ldots \ldots (i)$$

Next, let $C = \{aH: a \in G\}$

Since, G is finite, C is clearly a finite family.

Also, two distinct elements of G may produce the same left

coset. So, if $(C) = k$, then $1 \leq k \leq m$.

Let, $C = \{a_1H , a_2H , \ldots \ldots \ldots \ldots \ldots \ldots , a_kH\}$, where $a_1 , a_2 , \ldots \ldots \ldots , a_k \in G$

Clearly, $a_iH \subseteq G$ for $i = 1 , 2 , \ldots \ldots , k$

$$=> \cup_{i=1}^{k} a_iH \subseteq G \ldots \ldots \ldots \ldots \ldots \ldots \ldots (ii)$$

Further, $x \in G => xH = a_jH$, for some j , $1 \leq j \leq k$

$$=> x \in xH = a_jH \subseteq \cup_{i=1}^{k} a_iH$$

$$=> x \in \cup_{i=1}^{k} a_iH$$

$$\therefore G \subseteq \bigcup_{i=1}^{k} a_iH \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots (iii)$$

From (ii) & (ii) we get,

$$G = \cup_{i=1}^{k} a_iH \ldots \ldots \ldots \ldots (iv)$$

Also, $1 \leq i \leq k$, $1 \leq j \leq k$, $i \neq j => a_iH \neq a_jH$

$$=> a_iH \cap a_j = \phi \text{ ....(v)}$$

Hence, the coset $a_1H , a_2H , \ldots \ldots \ldots \ldots , a_nH$ are mutually disjoint.

From (iv) we get,

$$n = o(G) = o\left(\cup_{i=1}^{k} a_iH\right)$$

$$= o(a_1H) + o(a_2H) + \ldots \ldots \ldots + o(a_kH)$$

$$= m + m + \ldots \ldots \ldots \ldots \ldots \ldots \text{upto } k \text{ times (by (i))}$$

$$= km$$

$$=> \frac{n}{m} = k$$

$$=> \frac{o(G)}{o(H)} = k$$, where k is positive integers.

Space for learners:

$=> o(H)$is a divisor of $o(G)$.

Cyclic group: Let a group G is said to be cyclic if there exist an element $a \in G$ such that every element $x \in G$ is of the form $= a^n$, where n is an integer. The element a is then called the generator of G and we can write $G =< a >$.

e.g., $G = \{1 , -1 , \ i , -i\}$

$= \{i^4 , \quad i^2 , \quad i^1 , i^3\}$

$\therefore G =< i >$ is a cyclic group under multiplication.

Example 2: Show that every cyclic group is abelian.

Solution: Let $G =< G >$ be a cyclic group generated by $a \in G$.

Let $x , y \in G$ be any elements.

Then $x = a^r$, $y = a^s$ for some integer $r \& s$

$\therefore xy = a^r a^s$

$= a^{r+s}$

$= a^{s+r} = a^s a^r = yx$

$\therefore xy = yx$

$\therefore G$ is abelian.

Example 3: Show that a subgroup f a cyclic group is cyclic.

Solution: Let $G =< a >$ be a cyclic group generated by $a \in G$ and H is any subgroup of G.

If $H = \{e\} =< e >$ then clearly H is a cyclic group

Let, $H \neq \{e\}$ and

$x \in H$ be any non-identity element.

$=> x \in G$, since H is a subgroup of G

$=> x = a^n$ for some integer

$=> x^{-1} = a^{-n}$

$\therefore a^n , a^{-n} \in H$

Let, m be the least positive integer such that $a^m \in H$. We shall show that $H =< a^m >$ is a cyclic group generated by a^m

Let, $x \in H$

$=> x \in G$, since H is a subgroup of G

$=> x = a^n$, for some integer

By division algorithm there exists integer q and r such that

Space for learners:

$n = mq + r$, where $0 \leq r < |m|$ .... (i)

$=> r = n - mq$

$=> a^r = a^{n-mq}$

$=> a^r = a^n a^{-mq}$

$=> a^r = a^n (a^m)^{-q}$

$\therefore a^r \in H$

$\therefore r = 0$, since m is the least positive integer such that $a^m \in H$

From (i)

$=> n = mq$

$=> a^n = a^{mq}$

$=> a^n = (a^m)^q$

$=> x = (a^m)^q$

$\therefore H =< a^m >$ is a cyclic subgroup.

CHECK YOUR PROGRESS-I

1. State whether true or false

(a) A non-empty subset H of a group G, which is closed under the binary composition in G is a subgroup of G.

(b) If G is a group and H is a non-empty subset of G, then H will be a subgroup of G if $H^2 = H$.

2. Every group of prime order is … … … … … … … ….(Even/Cyclic)

3. Union of two subgroup is a ....

5.7 RING AND THEIR PROPERTIES

Ring: A ring is an order triples$< R , + , \ . >$ where R is a nonempty set and $+ , \ .$ are two binary operation on R satisfying the following axioms .

[R_1] Closure property for addition:

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

Space for learners:

$[R_2]$ *Associativity for addition:*

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

$[R_3]$ *Existence of identity w.r.t. addition:*

There exists an element $0 \in R$, called the zero element of R such that

$$a + 0 = a = 0 + a\forall a \in R$$

$[R_4]$ *Existence of inverse w.r.t. addition:*

For all $\in R$, there exist an element $-a \in R$ such that

$$a + (-a) = 0 = (-a) + a$$

$[R_5]$ Commutative property for addition:

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

$[R_6]$ Closure property for (.):

$$a.b \in R\ , \qquad \forall a\ ,b \in R$$

$[R_7]$*Associative property for* (.):

$$(a.b).c = a.(b.c)\ ,\forall a\ ,b\ ,c \in R$$

$[R_8]$*Distributive laws of* (.) *and* (+):

$$(a + b).c = a.c + b.c$$

$$c.(a + b) = c.a + c.b\forall a\ ,b\ ,c \in R$$

Example 1: Give two examples of ring.

Solution:

(i) We consider the set R of real numbers equipped with two binary composition addition (+) and multiplication (.), then it is easy to verify that $< R\ ,+\ ,\ \ .>$ is a ring.

(ii) Let M_2 denotes the set of all 2×2 matrices of real numbers. In M_2 we consider two binary operations, viz. addition (+) of matrices and multiplication (.) of matrices then it is easy to verify that $(M_2\ ,+\ ,\ \ .)$ is a ring.

Example 2: Prove that the set of matrices M_2 of order 2×2 form a ring with respect to addition and multiplication.

Solution: Let A and $B \in M_2$. Then A and B are two 2×2 matrices and so $A + B$& AB are also 2×2 matrices.

$$\therefore A + B \in M_2 \& AB \in M_2$$

This shows that M_2 is closed with respect to addition and multiplication of matrices .... (i)

Space for learners:

Since both addition and multiplication of matrices are associative, we see that both the composition in M_2 are associative. ......(ii)

Also there exists 2×2 null matrix

$O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ such that for any 2×2 matrix $A \in M_2$,

$A + 0 = A = 0 + A$

This shows that 0 is the zero element of M_2 ....(iii)

Further, if $A \in M_2$ where $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$

Then there exists a matrix

$-A = \begin{bmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{bmatrix} \in M_2$ such that

$$A + (-A) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

Similarly, $(-A) + A = 0$

Therefore, $A + (-A) = 0 = (-A) + A$

This shows that $-A$ is the inverse of A in M_2.

Thus, every element of M_2 has inverse ....(iv)

Further addition of matrices is commutative and so the composition in M_2 is commutative ....(v)

Finally, by the distributive property of multiplication of matrices over addition we have,

$$\left.\begin{aligned} A(B + C) &= AB + AC \\ (B + C)A &= BA + CA \end{aligned}\right\}$$

$\forall A, B, C \in M_2$ .... (vi)

From (i) to (vi) we see that M_2 is a ring with respect to addition and multiplication of matrices .

Note: The ring R with two binary compositions $(+)$ and $(\,.\,)$ is sometimes denoted by $(R\ ,+\ ,\ .)$.

Commutative Ring:

A ring $(R\,, +\,,\ .)$ is called a commutative ring if and only if for all $a, b \in R$, $a.b = b.a$.

Ring with unity:

If in a ring R there exists an element $1 \in R$ such that

$\mathbf{1}.a = a = a.1 \quad \forall a \in R$ then R is called a ring with unity element.

Space for learners:

The element 1 is called the unity element of the ring.

Space for learners:

2. Theorem: In a ring, the following results hold

(i) $a.0 = 0 = 0.a \forall a \in R$

(ii) $a.(-b) = (-a).b = -a.b \forall a, b \in R$

(iii) $(-a).(-b) = a.b$

(iv) $a.(b-c) = a.b - a.c$

(v) $(b-c).a = b.a - c.a$

Proof:

(i) We have,

$a.0 = a(0+0)[\because \quad 0 = 0+0]$

$=> a.0 = a.0 + a.0 \quad [by left distributive law]$

$=> 0 + a.0 = a.0 + a.0$ [since $0.a \in R$and $0 + a.0 = a.0$]

$=> 0 = a.0$ [sincr R is a group w.r.t. $+$,therefore applying right cancellation law for addition in R]

Similarly, we have

$0.a = (0+0).a = 0.a + 0.a$ [by right distributive law]

$=> 0 + 0.a = 0.a + 0.a[\because 0 + 0.a = 0.a]$

$=> 0 = 0.a$ [using R.C.L. w.r.t.$+$ in the group $< R, + >$]

$\therefore a.0 = 0.a = 0$

(ii) From the existence of inverse, it follows that

$b + (-b) = 0$

$=> a.[b + (-b)] = a.0$

$=> a.b + a.(-b) = 0$ [by the left distributive law and $a.0 = 0$]

$=> -a.b + [a.b + a.(-b)] = -a.b + 0$ [adding $-a.b$ on the left of both sides]

$=> [-a.b + a.b] + a.(-b) = -a.b$ [by associative law]

$=> 0 + a.(-b) = -a.b$

$=> a.(-b) = -a.b$

Similarly, we can prove

$(-a).b = -ab$

$\therefore a.(-b) = (-a).b = -a.b$

(iii) We know that

$$a.(-b) = -.(ab) \ldots \ldots \ldots . . (1)$$

Writing $-a$ for a in (1) , we get

$(-a).(-b) = -[(-a).b]$

$= -[-(a.b)]$, since $(-a).b = -a.b$

$= a.b$ [$\therefore R$ is a group and inverse of the inverse of an element is the element itself. $-(-a = a)$]

$\therefore (-a).(-b) = a.b$

(iv) we have ,$a.(b-c) = a.[b+(-c)]$

$= a.b + a.(-c)$[by left distributive law]

$= a.b + [-a.c][\therefore a.(-c) = (-a).c = -a.c]$

$= a.b - a.c$

(v) we have ,$(b-c).a = [b-c].a$

$= b.a + (-c).a$(by right distributive law)

$= b.a + (-c.a) \because [(-c).a = -c.a]$

$= b.a - c.a$

Theorem: A commutative ring is an integral domain if and only if the cancellation law with respect to multiplication hold on it.

Proof: Let R be a commutative ring. First, we assume that R is an integral domain We are to show that the cancellation laws hold in R.

Let, $ab = ac$, where $a, b, c \in R$, $a \neq 0$

$=> ab - ac = 0$

$=> a(b-c) = 0$

$\therefore$ either $a = 0$ or $b - c = 0$ [$\because$ $R$is an integral domain]

But $a \neq 0$, $b - c = 0$

$=> b = c$

$\therefore ab = ac => b = c$, which shows that left cancellationlaw

with respect to multiplication.

Similarly, $a \neq 0$, $b, c \in R$, $ba = ca => b = c$, which shows the right cancellation law with respect to multiplication.

$\therefore$ The cancellation law holds in R .

Conversely, suppose that the cancellation law with respect to multiplication hold in R. We are to show that R is an integral domain.

Space for learners:

Let, $a, b \in R$ such that $ab = 0$

Now,

$a \neq 0$, $ab = 0$

$=> ab = a0$

$=> b = 0$ [by left cancellation law w.r.t. multiplication hold in R]

Similarly,

$b \neq$, $ab = 0$

$=> ab = 0b$ [by right cancellation law w.r.t. multiplication]

$=> a = 0$

Hence, $a, b \in R$, $ab = 0 =>$ either $a = 0$ or $b = 0$

So, $R$is an integral domain. Hence, commutative ring is an integral domain if and only if the cancellation law with respect to multiplication hold on it.

Example 3: Give an example of ring.

Solution: We consider the set of real number equipped with two binary composition addition (+) and multiplication (.) then it is easy to verify that $(R, +, .)$ is a ring.

Example 4: If R is a ring such that $a^2 = a \forall a \in R$, prove that

(i) $a + a = 0 \; \forall a \in R$

(ii) $a + b = 0 => a = b$

(iii) R is commutative.

Solution:

(i) Let $a \in R$ such that $a^2 = a$ then by closure property,

$a + a \in R$

$=> (a + a)^2 = a + a$ [by hypothesis]

$=> (a + a)(a + a) = a + a$

$=> (a + a)a + (a + a)a = a + a$

$=> (a^2 + a^2) + (a^2 + a^2) = a + a$ [by right distributive law]

$=> (a + a) + (a + a) = a + a (\because a^2 = a)$

$=> (a + a) + (a + a) = (a + a) + 0$

$=> a + a = 0$ [by right distributive law]

Space for learners:

(ii) Let $a\ , b \in R$ such that $a + b = 0$ then using (i)

$a + b = 0 = a + a$

$=> b = a$ [by left cancellation law]

$\therefore a = b$

$\therefore a + b = 0 => a = b$

(iii) Let, $a , b , c \in R$ then $a + b \in R$ and so, by hypothesis,

$(a + b)^2 = a + b$

$=> (a + b)(a + b) = a + b$

$=> (a + b)a + (a + b)b = a + b$

$=> a^2 + ba + ab + b^2 = a + b$ [by right distributive law]

$=> a + ba + ab + b = a + b$

$=> ba + ab + b = b$ [by LCL]

$=> ba + ab = 0$ [by RCL]

$=> ba = ab$[by result (ii)]

$\therefore ab = ba \forall a , b \in R$

$\therefore R$ is commutative.

Zero divisor in a ring:

A non-zero element ' a' in a ring R is called a (proper) zero divisor if there exist another non zero elements 'b' in Rsuch that $ab = 0$.

Example 5: Give an example of a ring with zero divisor.

Solution: We consider a ring M_2 of all 2×2 matrix over real numbers.

Let $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} \in M_2$

Then $A \neq 0 \quad , B \neq 0$

$AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$

$\therefore M_2$is a proper zero divisor

Integral domain:

A commutative ring R without proper zero divisor is called an integral domain

i.e., $ab = 0\ \forall a , b \in R$

$=> a = 0$ or $b = 0$

Space for learners:

Example 6: Give an example of a ring which is not an integral domain.

Solution: Let M_2 denote the set of all 2×2 matrices of real numbers then it is easy to verify that M_2 is a ring under matrix addition and multiplication.

Now, let $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Then $A \neq 0$, $B \neq 0$

But $AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$

$\therefore M_2$ is not an integral domain

Example 7: When is a ring said to be an integral domain?

Solution: A ring $< R \ , + \ , \ . >$is said to be an integral domain if the following two properties are satisfied in.

(i) Commutative property of multiplicativity

$$ab = ba \forall a , b \in R$$

(ii) Non-existence of zero divisor:

$a , b \in R$, $ab = 0$ =>either $a = 0$ or $b = 0$

5.8 FIELD AND ITS THEOREM

Definition: A field is an order triple $< F \ , + \ , \ . >$ where F is a set containing at least two elements and $(+) , (.)$ are two binary composition in F satisfying the following axioms:

(i) Closure property for addition:

$$a + b \in F \forall a \ , b \in F$$

(ii) Associativity for addition:

$$a + (b + c) = (a + b) + c \forall a \ , \quad b \ , c \in F$$

(iii) Existence of identity:

There exists an element $0 \in F$ called the zero element of F such that

$$a + 0 = a = 0 + a \forall a \in F$$

(iv) Existence of additive inverse:

For all $a \in F$ there exist an element $-a \in F$ such that

$$a + (-a) = (-a) + a$$

Space for learners:

(v) Commutativity for addition:

$a + b = b + a \forall a , b \in F$

(vi) Closure property for multiplication:

$a.b \in F \forall a , b \in F$

(vii) Associativity for multiplication:

$a.(b.c) = (a.b).c \forall a , b , c \in F$

(viii) Distribution property of multiplication over addition:

$a.(b + c) = a.b + a.c$

$(b + c).a = b.a + b.c \forall a , b , c \in F$

(ix) Existence of multiplicative identity:

There exists an element $1 \in F$, called the unit element of F such that $a.1 = a = 1.a \forall a \in F$

(x) Existence of multiplicative inverse for non-zero elements of F: For every non zero element $a \in F$ there exist an element $a^{-1} \in F$ such that $a.a^{-1} = 1 = a^{-1}.a$

(xi) Commutativity for multiplication:

$a.b = b.a \forall a , b \in F$

Alternate definition of Field:

A commutative ring with unity (having at least two elements) in which every non zero element has its multiplicative inverse (i.e., the set of non-zero element form a group under multiplication) is called a field.

Example 1: Show that every field is an integral domain but converse is not true (i.e., integral domain may not be a field).

Solution: Let F be a field i.e., F is a commutative ring with unity '1' in which every non-zero element has its multiplicative inverse.

To show that F is an integral domain.

Let, $a , b \in F$ such that $ab = 0$

We first assume that $a \neq 0$ since F is a field, a^{-1} exists i.e $a^{-1} \in F$ such that $aa^{-1} = 1 = a^{-1}a$

So, $ab = 0$

$=> a^{-1}(ab) = a^{-1}(0) = 0$

$=> (a^{-1}a)b = 0$

$=> 1\, b = 0$ [1 being the unity element in F]

Space for learners:

$=> b = 0$

Next, we assume that $b \neq 0$ then b^{-1} exists and so

$ab = 0$

$=> (ab)b^{-1} = (0)b^{-1}$

$=> a(bb^{-1}) = (0)b^{-1}$

$=> a(1) = 0$ [$\therefore$1 being the unit element of F]

$=> a = 0$

Thus, $a , b \in F$, $ab = 0 =>$ either $a = 0$ or $b = 0$

This shows that F is an integral domain. Hence every field is an integral domain.

Example 2: Show that every integral domain may not be a field.

Solution: We consider the ring $< I , + , . >$ of integers with usual addition and multiplication is an integral domain which is not a field. Since, the non-zero elements except ± 1 have no multiplicative inverse in I.

Now, $2 \in I$ and $2 \neq 0$ but there exist no $\frac{1}{2} \in I$ such that $2 . \frac{1}{2} = 1 = \frac{1}{2} . 2$

$\therefore$t he non-zero element $2 \in I$ has no multiplicative inverse .

So ,$< I , + , . >$is not a field .

5.9 HOMOMORPHISM

5.9.1 Homomorphism of Group

A mapping $f: G \rightarrow G'$is said to be a homomorphism of G into G' if

$f(ab) = f(a)f(b) \ \forall \ a , b \ \in G$

5.9.2 Kernel of a Homomorphism

If f is a homomorphism of a group G into a group G', then the set K of all those elements of Gwhich are mapped by f.

Space for learners:

5.10 VECTOR SPACE AND ITS PROPERTIES

Space for learners:

Let $(F, +, .)$ be field. The element of F is called scalars. The element of V(any non-empty set) is called vectors. Then V is a space over the field F if

(I) $(V, +)$is abelian group

(II) External Composition in V over F i.e $\alpha a \in V \quad , a \in V \quad , \alpha \in F$

(III) The two compositions $(+ , .)$ satisfy the following conditions:

(a) $\alpha(a+b) = \alpha a + \alpha b \quad \forall \ a, b \in V$

(b) $(\alpha + \beta)a = \alpha a + \beta a \quad \forall \ \alpha \in F$

(IV) $(\alpha\beta)a = \alpha(\beta a) \quad \forall \ a \in V \ , \ \alpha, \beta \in V$

(V)$1a = a$,1 is unity element of F

The V is a vector space over the field, e.g., $\mathbb{C}$ is a field of complex number and $\mathbb{R}$ is a field of real number.

(i) $\mathbb{C}(\mathbb{R})$ is vector space, since $\mathbb{R} \subseteq \mathbb{C}$.

(ii) $\mathbb{R}(\mathbb{C})$ is not vector space.

5.10.1 Linear Dependence and Linear Independence of Vectors

Let $V(F)$ be a vector space. A finite set $\{\alpha_1, \ \alpha_2, \dots \dots \dots \dots .., \alpha_n\}$ of vectors of V is said to be linearly dependent if there exist scalars $c_1, c_2 , \dots \dots \dots .. \ \ , c_n \in F$not all of them zero (some of them may be zero) such that $c_1\alpha_1 + c_2\alpha_2 + \ \dots \dots \dots \dots \dots . + c_n\alpha_n = 0$

$i.e$

$\sum_{i=0}^{n} c_i\alpha_i = 0$ atleast one $\alpha_i \neq 0$.

Some Important Result:

1. If two vectors are linearly dependent then one of them is a scalar multiple of other the other

2. A system consisting of a single non-zero vector is always linearly dependent.

5.10.2 Vector Subspaces

Let V be a vector space over the field F and let $W \subseteq V$. Then $W$is called a subspace of V if W itself is a vector space over F with respect to the operations of vector addition and scalar multiplication in V.

Result:

1. A subset $W$of a vector space $V(F)$ is a subspace of V, if and only if $\forall\ \alpha, \beta \in W$ and $a, b \in F => a\alpha + b\beta \in W$.

5.11 BASIS AND DIMENSION

Let V be a vector space over a field F. Then a subset B of V is called a basis of V if B is linearly independent over F and $V =< B >$ Number of elements in basis is called dimensions of vector space.

Linear Span

If $S = \{\alpha_1, \alpha_2, \alpha_3, \dots\dots\dots\dots, \alpha_n\}$ from (F) . Set of all liner combination of vectors of S is known as linear span of S.

Finite dimensional vector space

A vector space V_F is said to be finite dimensional vector space if there exist a finite subset S of F such that $=< B >$.

If $\mathbb{R}^2(\mathbb{R})$ is finite dimensional vector space. It is generated

by a finite set $B = \{(0,1), (1,0)\}$ then $dim\big(\mathbb{R}^2(\mathbb{R})\big) = 2$

Example 1:

Consider the vector space $\mathbb{C}(\mathbb{R})$, find the basis and dimension.

Solution:

Let, $\mathbb{C} = \{\alpha + i\beta : \alpha,\ \beta \in \mathbb{R}\}$

$$2 + 3i = \alpha.1 + \beta.i(Linear\ combination\ of\ basis)$$

$$= 2.1 + 3.i$$

$\therefore dim\big(\mathbb{C}(\mathbb{R})\big) = 2$

Space for learners:

Example 2: What is the dimension of $\mathbb{R}(\mathbb{Q})$?

Solution: $Dim\mathbb{R}(\mathbb{Q}) = \infty$

5.12 SUMMING UP

- A non-empty set, together with a binary composition '$*$' (star) is said to form a group, if it satisfies closure property, Associativity property, existence of identity and existence of inverse properties.
- A commutative group is an ordered pair $(G, *)$ having the additional Commutativity property in addition to all four properties of a group.
- If G be a group and H be a non-empty subset of G. Then H is called a subgroup G if and only if H itself is a group under the binary composition '$*$' defined on G.
- A ring is an order triples $< R, +, . >$ where R is a nonemptyset and $+, .$ are two binary operation on R satisfying the closure property for addition, associativity for addition, existence of identity w.r.t. addition, existence of inverse w.r.t. addition, commutative property for addition, closure property for $(.)$, Associative property for $(.)$ and Distributive laws of $(.)$ and $(+)$
- A non-zero element 'a' in a ring R is called a (proper) zero divisor if there exist another non zero elements 'b' in Rsuch that $ab = 0$.
- A commutative ring R without proper zero divisor is called an integral domain

5.13 ANSWERS TO CHECK YOUR PROGRESS

1.(a) False

(b) False

2. Cyclic

3. Sub-group

Space for learners:

5.14 POSSIBLE QUESTIONS

Space for learners:

Short Answer type Questions:

1. Define semi-group.
2. Give an example of a semi group which is not group.
3. Define zero divisor of a ring.
4. Give an example of a ring which is not an integral domain
5. Define basis of a vector space.
6. Define linearly independent of the vector space.
7. Define order of a permutation group.
8. Under what condition a ring is said to be an integral domain.

Long Answer type Question:

1. Show that identity element in a group is Unique.
2. Show that the set of all positive rational numbers forms an abelian group under the composition defined by $a * b = (ab/2)$
3. Show that every group of prime order is cyclic.
4. Show that union of two subspace may not be a subspace.
5. Show that intersection of two subgroup is again a subgroup.
6. Prove that two vectors are linearly independent then one of them is scalar multiple of the other.
7. Show that the vectors $(1,1,0,0)$, $(0,1,-1,0)$, $(0,0,0,3)$ in $\mathbb{R}^4(\mathbb{R})$are linearly independent.
8. Give an example of a ring which is not a field.
9. Show that every transposition is always an odd permutation.
10. Show that every field is an integral domain.

5.15REFERENCES AND SUGGESTED READINGS

- Modern Algebra by. Vasistha, A. R., Krishna Publication, India 2018

UNIT 6: PROPOSITIONAL CALCULUS-I

Space for learners:

Unit Structure:

6.1 INTRODUCTION

Mathematical logic is the science of reasons. Greek philosopher Aristotle (381-322 BC) first introduced the concept of logical reasoning. The mathematical logic compromise of two branches:(a) Propositional calculus, (b) Predicate calculus. But in this course, our discussion will restrict only propositional calculus. The branch of logic that deals with propositions is called propositional calculus. Propositional calculus is the study of the logical relationship between propositions. Propositional calculus forms the basis of all mathematical reasoning and it has many applications in computer science like design of computing machines, artificial intelligence, data structures for programming language etc.

6.2 UNIT OBJECTIVES

After going through this unit, you will be able to:

- define propositions and examples of propositions
- define truth tables about different propositions
- know about negation of a proposition
- know about conjunction, disjunction, conditional and bi-conditional of two propositions

Space for learners:

6.3 PROPOSITION

Definition:

A proposition (or statement) is a declarative sentence which is either true or false but not both.

The truth or falsity of a proposition is called its truth value.

Notations:

(a) If a proposition is true then its truth value is denoted by T

(b) If a proposition is false then its truth value is denoted by F

We now define Simple propositions and Compound propositions.

A simple proposition is a statement or assertion that must be true or false.

Many statements or propositions are constructed by combining one or more propositions, new propositions called compound propositions are formed existing propositions using logical connectives. A compound proposition is a combination of simple propositions and hence, can be broken down in primitive propositions.

6.3.1 Example of Proposition

ILLUSTRATION 1: Consider the following sentences

(i) New Delhi is the capital of India.

(ii) 7 is a prime number.

(iii) Every quadrilateral is a rectangle.

(iv) The earth is a planet.

(v) Three plus six is9.

(vi) The sun is a star.

(vii) Delhi is in America.

Each of the sentences (i), (ii), (iv) & (v) is a true declarative sentence and so each of them is a proposition.

Each of the sentences (iii), (vi), (vii) is a false declarative sentence and so each of them is a proposition.

All the above propositions are atomic propositions

ILLUSTRATION 2: Consider the following sentences:

i) Go to bed.

ii) Give me a glass of water.

iii) How are you?

iv) Where are you going?

v) May god bless you!

vi) May you livelong!

vii) $x + 2 = 5$

viii) $u + v < w$

Sentences (i) & (ii) are imperative sentences, so they are not propositions. Each of the sentences (iii) & (iv) is interrogative. So, they cannot be propositions. Similarly, (v) & (vi) are also not declarative sentences and hence not propositions. The expression (vii) and (viii) are not propositions, since the variables in these expressions have not been assigned values and hence, they are neither true or false.

Space for learners:

CHECK YOUR PROGRESS-I

1.Define proposition.
2.Which of the following sentences are propositions? What are the truth values of those that are propositions?

(a) $3 + 4 = 7$

(b) $5 + 7 = 10$

(c) There are 35 days in a month.

(d) $x + 3 = 12$

(e)Answer these questions.

3.Write down the truth value of the following propositions:

(a) All the sides of a rhombus are equal in length.

(b) $\sqrt{3}$ is a rational number.

(c) The number 30 has four prime factors.

(d) Every square matrix is non-singular.

(e) $1 + \sqrt{8}$ is an irrational number.

Space for learners:

6.4 PROPOSITIONAL VARIABLES

Now, we will abbreviate propositions by using propositional variables. Each proposition will be represented by a propositional variable. Propositional variables are usually represented as lower-case letters, such as *p*, *q*, *r*, *s*, etc. The capital letters *A*, *B*, *C*, ..., *P*, *Q*, ... with the exception of T and F are also used. Each variable can take one of two values: true or false.

Example 1: Consider the propositions

(i) Guwahati is in India.
(ii) $6 + 8 = 14$
(iii) The sun is shining.

Now we can assign propositional variables *p*, *q*, *r* for the propositions (i), (ii) and (iii).

Space for learners:

The propositions (i), (ii) and (iii) can be represented by

p: Guwahati is in India

$q: 6 + 8 = 14$

And r: The sun is shining

6.5 TRUTH TABLES

A table which gives the truth values of a compound proposition in terms of its component parts is called a 'Truth Table'. A truth table consists of rows and columns. The initial columns are filled with the possible truth values of the component parts and the last column is filled with the truth values of the compound proposition on the basis of the truth values of the component parts written in the initial columns. If the compound proposition is consisting of n component parts, then its truth table will contain 2^n rows.

A truth table displays the relationship between the truth values of propositions.

Note: Truth tables are very useful in the determination of propositions constructed from simple propositions.

6.6 LOGICAL CONNECTIVES

Till now, we have considered simple or primary propositions which are declarative sentences, each of which cannot be expressed as a combination of more than one sentence. We often combine simple (primary) propositions to form compound propositions by using certain connecting words known as logical connectives or logical operators. Primary statements are combined by means of five logical connectives.

Now we will discuss in details about these five logical connectives which will allow us to build up compound proposition sand their truth values expressed in a tabular form, called Truth Table.

Five Basic Logical Connectives

	Logical Connectives	Name of the Connectives	Symbols of the connectives
1	Not	Negation (or Denial)	$\sim$
2	And	Conjunction	$\wedge$
3	Or	Disjunction	$\vee$
4	If … then	Conditional	$\rightarrow$
5	If and only if	Biconditional	$\leftrightarrow$

Space for learners:

6.6.1 Negation

The denial of a proposition P is called its negation and is written as $\sim P$ and read as 'not P'. Negation of any proposition P is formed by writing "It is not the case that'' or "It is false that'' before p or inserting in p the word "not''.

Let us consider the proposition

P: All integers are rational numbers.

The negation of this statement is:

$\sim P$: It is not the case that all integers are rational numbers.

or

$\sim P$: It is false that all integers are rational numbers.

or

$\sim P$: It is not true that all integers are rational numbers.

Let us consider another the proposition,

P : 7 >9

The negation of this statement is $\sim P$:$\sim$ (7>9) or $\sim p$:(7<9)

Truth Table of Negation: If the truth value of "P''is T, then the truth value of $\sim P$ is F. Also, if the truth value of "P''is F, then the truth value of $\sim P$ is T.

The truth table of for the negation of a proposition

P	$\sim P$
T	F
F	T

Example 1: Write the negation of the following propositions:

(i) $\sqrt{7}$is arational

(ii) Every natural number is greater than zero.

(iii) All primes are odd.

(iv) All mathematicians are men.

Solution:

(i) Let $p$denote the given proposition i.e.,

P: $\sqrt{7}$ is arational.

The negation of this proposition is given by

$\sim P$: It is not the case that $\sqrt{7}$ is arational.

Or

$\sim P$: $\sqrt{7}$ is not arational.

Or

$\sim P$: It is false that $\sqrt{7}$ is arational.

(ii) The negation of the given proposition is:

It is false that every natural number is greater than 0.

OR,

There exists a natural number which is not greater than0.

(iii) The negation of the given proposition is

There exists a prime which is not odd.

OR
Some primes are not odd.
OR

At least one prime is not odd.

(iv) The negation of the given proposition is:

Some mathematicians are not men.
OR

There exists a mathematician who is not man.

OR

At least one mathematician is not man.

OR

Space for learners:

It is false that all mathematicians are me

Space for learners:

CHECK YOUR PROGRESS-II

4. Why Logical Connectives are used?
5. Write the negation of the following propositions-

i) Bangalore is the capital of Karnataka.

ii) The Earth is round.

iii) The Sun is cold.

iv) Some even integers are prime.

v) Both the diagonals of a rectangle have the same length.

vi) $4+7=10$

vii) Today is Monday

viii) If it snows, Samir does not drive the car.

6.6.2 Conjunction

The conjunction of two propositions P and Q is the proposition "P *and* Q" which is denoted by$P \wedge Q$.P,Q are called the components of $P \wedge Q$.

Illustrative Examples:

(i) The conjunction of the propositions:

P:It is raining

$Q: 2+2=4$ is

$P \wedge Q$:It is raining and $2+2=4$.

(ii) Consider the proposition

P : The Earth is round and the Sun is cold.

Its components are:

Q: The Earth is round.

R : The Sun is cold.

Truth table: The statement $P \wedge Q$ has the truth value Twhenever both P and Q have the truth value T; Otherwise, it has the truth value F.

The truth table for conjunction of two propositions

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

6.6.3 Disjunction

The disjunction of the two propositions P and$Q$ is the statement "$P or\ Q$", denoted by $P \vee Q$. P,$Q$are called the components of $P \vee Q$.

Examples:

(i) Consider the compound proposition

P: Two lines intersect at a point or they are parallel.
The component propositions of are:
Q : Two lines intersect at a point.
R : Two lines are parallel.

(ii) Consider another proposition

P: 45 is a multiple of 4 or 6.
Its component propositions are:
Q: 45 is a multiple of 4.
R: 45 is a multiple of 6.

Truth table: The statement $P \vee Q$ hasthetruthvalueFonlywhen both$P$ and Q havethetruthvalueF,$P \vee Q$ istrueifeither$P$ istrue or P is true (or both P and Q are true).

Truth table for disjunction of two propositions

P	**Q**	**P∨Q**
T	T	T
T	F	F
F	T	F
F	F	F

Example 2: Write the component propositions of the following compound propositions and check whether the compound proposition is true or false.

Space for learners:

(i) 50 is a multiple of both 2and5.

(ii) Mumbai is the capital of Gujrat or Maharashtra.

(iii) A rectangle is a quadrilateral or a 5-sidedpolygon.

Solution:

i) The component statements of the given statement are

P: 50 is multiple of2

Q : 50 is multiple of 5

We observe that both $P$and $Q$are true statements. Therefore, the compound statement $P \wedge Q$ is true.

ii) The components proposition of the given proposition are

P: Mumbai is the capital of Gujrat.

Q: Mumbai is the capital of Maharashtra.

We find that P is false and Q is true. Therefore, the compound statement,$P \vee Q$is true.

iii) The component propositions are

P: A rectangle is a quadrilateral.

Q: A rectangle is a 5-sided polygon.

We observe that P is true and Q is false. Therefore, the compound proposition $P \vee Q$ is true.

Space for learners:

CHECK YOUR PROGRESS-III

6. Write the following propositions in symbolic form:

i) Pavan is rich and Raghav is not happy.

ii) Pavan is not rich and Raghav is happy.

iii) Naveen is poor but happy.

iv) Naveen is rich or unhappy

v) Naveen and Amal are both smart.

vi) It is not true that Naveen and Amal are both smart

vii) Naveen is poor or he is both rich and unhappy

vii) Naveen is neither rich nor happy.

7**.** Write the component statements of the following compound statements and find true values of the compound statements.

i) Delhi is in India and 2 + 2 =4.

ii) Delhi is in England and 2 + 2 =4.

iii) Delhi is in India and 2 + 2 = 5.

iv) Delhi is in England and 2 + 2 =5.

v) Square of an integer is positive or negative.

vi) The sky is blue and the grass is green.

vii) The earth is round or the sun is cold.

viii) All rational numbers are real and all real numbers are complex.

ix) 25 is a multiple of 5 and8.

x) 125 is a multiple of 7or8.

Space for learners:

6.6.4 Conditional Statements

If P and Q are any two statements, then the statement “if P, then Q”, is called a conditional statement. It is denoted by P→Q.

Example: Let,

P: Amulya works hard.

Q:Amulya will pass the examination.

Space for learners:

Then,

$P \rightarrow Q$: If Amulya works hard, then he will pass the examination.

The statement P is called the ***antecedent*** and Q is called the ***consequent*** in $P \rightarrow Q$. The sign "→" is called the sign of implication.

The conditional statement $P \rightarrow Q$ can also be read as:

i) P only if Q
ii) Q if P
iii) Q provided that P
iv) P is sufficient for Q
v) Q is necessary conditions for P
vi) P implies Q
(vii) Q is implied by P.

Truth table: If the antecedent P is true and the consequent Q is false, then the conditional statement $P \rightarrow Q$ is false, otherwise it is true as given in the following table.

The truth table for the conditional $P \rightarrow Q$

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Example 3: Write each of the following statements in the form "If–then"

i) You get job implies that your credentials are good.

ii) A quadrilateral is a parallelogram if its diagonals bisect each other.

iii) To get A+ in the class, it is necessary that you do all the exercises of the book.

Solution:

(i) The given statement can be written as "If you get a job, then your credentials are good."

(ii) The given statement can be written as-

"If the diagonal of a quadrilateral bisects each other, then it is a parallelogram".

(iii) The given statement can be written as

"If you are to get A+ in the class, then you are to do all the exercises of the book".

Example 4: Write the following conditional statements in symbolic form and hence, find truth values.

i) If $2 + 2 = 4$, then Guwahati is in Assam

ii) If $2 + 2 = 4$, then Guwahati is in Bihar

iii) if $2 + 2 = 5$, then Guwahati is in Assam

iv) If$2+2=5$, then Guwahati is in Bihar

Solution: Let,

P: $2 + 2 =4$

Q: Guwahati is in Assam

R: $2 + 2 =5$

S: Guwahati is in Maharashtra, Then

i) The given statement is $P\rightarrow Q$

As P and Q have truth values T each, so $P\rightarrow Q$ has truth value T, i.e., the given conditional statement is true.

ii) The given statement is $P\rightarrow S$

P	S	$P\rightarrow S$
T	F	F

So, the given statement is false.

iii) The given statement is $R\rightarrow Q$

R	Q	$R\rightarrow Q$
F	T	T

So, the given statement is true.

iv) The given statement is $R\rightarrow S$

R	S	$R\rightarrow S$
F	F	T

Space for learners:

So, the given statement is true.

Space for learners:

CHECK YOUR PROGRESS-IV

8. Write down the truth value of each of the following implication.

i) If 3 + 2 = 7, then Paris is the capital of India.

ii) If 3 + 4 = 7, then 3 >7

iii) If 4 > 5, then 5 <6.

iv) If 7 > 3, then 6 <14

v) If 7 > 3, then 14 > 9.

6.6.5 Biconditional Statements

If P and Q are any two statements, then the statement 'P if and only if Q' is called a biconditional statement which is denoted by P↔Q. 'P if and only if Q' is also abbreviated as "P if Q".

The biconditional 'P if and only if Q' is regarded as having the same meaning as 'if P, then Q and if Q, then P'. So, the biconditional P↔Q is the conjunction of the conditionals P→Q and Q→P i.e., (P→Q) ∧ (Q→P) is same asP↔Q.

The statement P↔Q can also be read as

a) Q if and only if P

b) P implies Q and Q implies P

c) P is necessary and sufficient condition for Q

d) Q is necessary and sufficient condition for P

The truth table for the biconditional P↔Q

P	Q	P↔Q
T	T	T
T	F	F
F	T	F
F	F	T

Thus, the biconditional P→Q is true only when both P, Q have identical truth values, otherwise it is false.

For examples:

1. A triangle is equilateral if and only if it is equiangular.
2. 8> 4 if and only if 8 – 4 is positive.
3. 2+2=4ifandonlyifitisraining.
4. Two lines are parallel if and only if they have the same slope.

Example 5: Write the truth value of each of the following biconditional statements.

i)4 > 2 if and only if 0 < 4 – 2.

ii) 3 < 2 if and only if 2 <1.

iii) 3 + 5 > 7 if and only if 4 + 6 <10.

iv) 2 + 5 = 7 if and only if Guwahati is in Assam.

Solution:

i) L e t P: 4 >2

Q: 0 < 4 – 2

Then, the given statement is P→Q.

Clearly, P is true and Q is true and therefore, P→Q is true.

Hence, the given statement is true, and its truth value is T.

(ii) Let P:3 <2

Q: 2 <1

Then, the given statement is P→Q.

Clearly, P is false and Q is false and therefore, P→Q is true. Hence, the given statement is true, and its truth value is T.

(iii) Let, P: 3 + 5 >7

Q: 4 + 6 < 10

Then, the given statement is P→Q.

Clearly, P is true and Q is false and therefore, P→Q is false. Hence, the given statement is false and therefore, its truth value is F.

Space for learners:

(iv) Let, P: 2+5=7

Q: Guwahati is in Assam

Then, the given statement is $P \rightarrow Q$. As P is false, Q is true, the given statement is false.

Space for learners:

CHECK YOUR PROGRESS-V

9.Write down the truth value of each of the following:

i) 3 + 5 = 8 if and only if 4 + 3 =7.

ii) 4isevenifandonlyif1isprime.

iii) 6isoddifandonlyif2isodd.

iv) 2 + 3 = 5 if and only if 3 >5.

v) 4 + 3 = 8 if and only if 5 + 4 =10.

vi) 2 < 3 if and only if 3 <4.

6.7 SUMMING UP

- A primary proposition is a declarative sentence which cannot be further broken down or analyzed into simpler sentences.
- New propositions can be formed from primary propositions through the use of sentential connectives. The resulting statements are called compound propositions.
- The sentential connectives are also called logical connectives. These connectives are: NOT (negation), AND (conjunction), OR (disjunction), IF– THEN (conditional), IF AND ONLY IF (Bi-conditional).
- Truth tables have been introduced in the definitions of the connectives.
- The statement P is called the antecedent and Q is called the consequent in $P \rightarrow Q$.

6.8 ANSWERS TO CHECK YOUR PROGRESS

Ans. to Q. No.1: A proposition is a declarative sentence which is either True or False but not both.

Ans. to Q. No.2:

(a) Proposition, T
(b) Proposition, F
(c) Proposition, F
(d) Not proposition
(e) Not proposition

Ans. to Q. No.3: (a) T (b) F (c) F (d) F (e) T

Ans. to Q. No.4: Logical connectives are used to form new propositions or compound propositions.

Ans. to Q. No.5:

i) Bangalore is not the capital of Karnataka.

(ii) The earth is not round.

(iii) The sun is not cold.

(iv) No even integer is prime.

(v) There is at least one rectangle whose both diagonals do not have the same length.

(vi) $4 + 7 \neq 10$

(vii) Today is not Monday.

(viii) It snows and Samir drives the car.

Ans. to Q. No.6:

i) $P \wedge \sim Q$, where P: Pavan is rich
Q: Raghav is happy

ii) $\sim P \wedge Q$

iii) $\sim R \wedge H$, where R: Naveen is rich
H: Naveen is happy

iv) $R \vee \sim H$

v) $P \wedge Q$, where P: Naveen is smart
Q: Amal is smart

vi) $\sim (P \wedge Q)$

Space for learners:

vii) $\sim R \vee (R \vee \sim H)$, where R: Naveen is rich

R: Naveen is happy

viii) $\sim R \wedge \sim H$

Ans. to Q. No.7:

i) P: Delhi is in India

Q: 2 + 2 = 4

The compound statement is true.

(ii) P: Delhi in England

Q : 2 + 2 =4

The compound statement is false.

(iii) P: Delhi is in India

Q: 2 + 2 =5

The compound statement is false.

(iv) P: Delhi is in England

Q: 2 + 2 =5

The compound statement is false.

(v) P: Square of an integer is positive

Q: Square of an integer is negative

The compound statement is true.

(vi) P: The sky is blue

Q: The grass is green

The compound statement is true.

(vii) P: The earth is round

Q: The sun is cold

The compound statement is true.

(viii) P: All rational numbers are real

Q: All real numbers are complex.

Space for learners:

The compound statement is true.

(ix) P: 25 is a multiple of 5

Q: 25 is a multiple of8

The compound statement is false.

(x) P: 125 is a multiple of 7

Q: 125 is a multiple of8

The compound statement is false.

Ans. to Q. No.8: i) True, ii) False, iii) True, iv) False, v) True

Ans. to Q. No.9: i) True, ii) False, iii) True, iv) False, v) True,
vi) True.

6.9 POSSIBLE QUESTIONS

1. Find out which of the following sentences are propositions and which are not. Justify your answer.
   i) The real number x is less than2.
   ii) All real numbers are complex numbers.
   iii) Listen to me, Ravi!
2. Find the component propositions of the following and check whether they are true or not:
   i) The sky is blue and the grass is green.
   ii) The earth is round or the sun is cold.
   iii) All rational numbers are real and all real numbers are complex
   iv) 25 is a multiple of 5 and 8.
3. Write the component propositions of each of the following statements. Also, check whether the statements are true or not.
   i) Sets A and B are equal if and only if ($A \subseteq B$ and $B \subseteq A$).
   ii) $|a| < 2$ if and only if ($a > -2$ and $a < 2$)
   iii) $\triangle ABC$ is isosceles if and only if $\angle B = \angle C$.
   iv) $7 < 5$ if and only if 7 is not a prime number.
   v) ABC is a triangle if and only if $AB + BC > AC$.

Space for learners:

4. If P is true and Q is false, then find truth values of

i) $P \wedge (\sim Q)$, ii) $\sim P \vee Q$, iii) $\sim P \rightarrow Q$,
iv) $P \rightarrow (\sim Q)$, v) $\sim (P \rightarrow Q)$, iv) $P \wedge Q$

5. What is proposition? Explain with illustration.
6. What do you mean by propositional variables?
7. Discuss truth table with example.
8. What are logical connectives? Explain the logical connectives with their corresponding truth tables.
9. Discuss how conditional statements are implemented using propositions.

Space for learners:

6.10 REFERENCES AND SUGGESTED READINGS

- Rao, G. S. S. Bhishma. *Discrete Structures and Graph Theory*. SciTech Publications (India) PVT Ltd,2003
- Sharma, J.K. *Discrete Mathematics*. Macmillan Publishers India Ltd,2011
- Balaji, G. *Discrete Mathematics*. Balaji Publishers,2015
- Singaravelu, A. & Jeyaraman, M.P. *Discrete Mathematics*. Meenakshi Agency,2016
- Satyanarayana, B. & Prasad, K.S. *Discrete Mathematics and Graph Theory*. PHI Learning Private Limited,2009
- Rao, G.S. *Discrete Mathematical Structure*. New Age international (P) Limited,2009
- Singh, Y.N. *Mathematical Foundation of Computer Science*, New Age international Publishers, 2005
- Lipschutz, S & Lipson, M.L. Schaum's outline of *Theory and Problems of Discrete Mathematics*, McGraw-Hill,2007
- Chandrasekaran, N &Umaparvathi, M. *Discrete Mathematics*, PHI Learning Private Limited,2010
- Tremblay, J.P. & Manohar, *Discrete Mathematical Structures with Applications to Computer Science,* Tata McGraw Hill Education Private Limited,1997.

UNIT 7: PROPOSITIONAL CALCULUS-II

Space for learners:

Unit Structure:

7.1 INTRODUCTION

The notion of a proposition has already been introduced in the previous unit. In this unit, we define statement formula. Also, we define tautology and contradiction of statement formulas and discuss equivalence of two statement formulas. In this unit, we will also discuss tautological implication of two statement formulas and will define the concept of two-state devices.

7.2 UNIT OBJECTIVES

After going through this unit, you will be able to

- define statement (or proposition) formulas
- define tautology and contradiction
- know about logical equivalence of two different statement formulas
- know about some important equivalence formulas

7.3 STATEMENTFORMULA

Space for learners:

Statements which do not contain any connective are called simple or primary or atomic statements. On the other hand, the statements which contain one or more primary statements and at least one connective are called composite or compound statements. For example, let P and Q be any two simple statements. some of the compound statements formed by P and Q are–

$$\sim P,\ P \vee Q,\ (P \vee Q) \wedge (\sim P),\ P \vee (\sim P),\ (P \vee \sim Q) \wedge P.$$

statement variables P and Q. Therefore, P and Q are called components of the statement formulas.

Definition: A statement formula is an expression which is a string consisting of propositional variables, parenthesis and connectives. Statement formulas are constructed from simple propositions using logical connectives. An example of Statement formula is $P \wedge (Q \vee R) \rightarrow S$.

A statement formula alone has no truth value. It has truth value only when the statement variables in the formula are replaced by definite statements and it depends on the truth values of the statements used in replacing the variables.

The truth table of a statement formula (Proposition): Truth table has already been introduced in the previous unit. In general, if there are 'n' distinct components in a statement formula. We need to consider 2^n possible combinations of truth values in order to obtain the truth table.

For example, if any statement formula has two component statements namely P and Q, then 2^2 possible combinations of truth values must be considered.

Illustrative Examples:

Example 1. Construct the truth table for

(a) $\sim(P \wedge Q)$

(b) $(\sim P) \vee (\sim Q)$

Solution:

(a) Truth table:

P	Q	$P \wedge Q$	$\sim(P \wedge Q)$
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

(b) Truth table:

P	Q	$\sim P$	$\sim Q$	$(\sim P) \vee (\sim Q)$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

Example 2. Construct the truth table for $\sim P \wedge Q$

Solution:

P	Q	$\sim P$	$\sim P \wedge Q$
T	T	F	F
T	F	F	F
F	T	T	T
F	F	T	F

Example 3: Construct the truth table for P → (Q →R).

Solution: P, Q and R are the three statement variables that occur in this formula P → (Q → R). There are $2^3 = 8$ different sets of truth value assignments for the variables P, Q and R.
The following table is the truth table for P → (Q → R):

Space for learners:

P	Q	R	$Q \rightarrow R$	$P \rightarrow (Q \rightarrow R)$
T	T	T	T	T
T	T	F	F	F
T	F	T	T	T
T	F	F	T	T
F	T	T	T	T
F	T	F	T	T
F	F	T	T	T
F	F	F	T	T

Space for learners:

Example 4: Construct the truth table for $P \wedge (P \vee Q)$

Solution:

P	Q	$P \vee Q$	$P \wedge (P \vee Q)$
T	T	T	T
T	F	T	T
F	T	T	F
F	F	F	F

Example 5: Construct the truth table for $(P \vee Q) \vee {\sim}P$

Solution:

P	Q	$P \vee Q$	${\sim}P$	$(P \vee Q) \vee {\sim}P$
T	T	T	F	T
T	F	T	F	T
F	T	T	T	T
F	F	F	T	T

CHECK YOUR PROGRESS-I

1. Construct the truth tables for the following formulas
   a) $\sim({\sim}P \wedge {\sim}Q)$
   b) $({\sim}P \vee Q) \wedge ({\sim}Q \vee P)$
   c) $(P \wedge Q) \rightarrow (P \vee Q)$
   d) $(Q \wedge (P \rightarrow Q)) \rightarrow P$

7.4 TAUTOLOGY

We have already defined truth table of a statement formula. In general, the final column of a given formula contains both T and F. There are some formulas whose truth values are always T oral ways F regardless of the truth value assignments to the variables. This situation occurs because of the special construction of these formulas.

Definition: A statement formula which is true regardless of the truth values of the statements which replace the variables in it is called a universally valid formula or a tautology or a logical truth.

A straight forward method to determine whether a given formula is a tautology is to construct its truth table. In the table, if the column below the statement formula contains T only, then it is a tautology. The conjunction of two tautologies is also a tautology. Let us denote by A and B two statement formulas which are tautologies. If we assign any truth values of the variables of A and B, then the truth values of both A and B will be T. Thus, the truth value of $A \wedge B$ will be T, so that $A \wedge B$ will be atautology.

Example 6: Verify whether P v (~P) is at tautology.

Solution:

P	$\boldsymbol{\sim P}$	$\boldsymbol{P \vee \sim P}$
T	F	T
F	T	T

As the entries in the last column are T, the given formula is a tautology.

Example 7: Show that the proposition $(P \vee Q) \leftrightarrow (Q \vee P)$is atautology.

Solution:

P	**Q**	$\boldsymbol{P \vee Q}$	$\boldsymbol{Q \vee P}$	$\boldsymbol{(P \vee Q) \leftrightarrow (Q \vee P)}$
T	T	T	T	T
T	F	T	T	T
F	T	T	T	T
F	F	F	F	T

Space for learners:

The last column entries are T. Therefore, given formula is a tautology.

Example 8: Verify whether $(P \to Q) \land (Q \to P)$is atautology.

Solution:

P	**Q**	$\boldsymbol{P \to Q}$	$\boldsymbol{Q \to P}$	$\boldsymbol{(P \to Q) \land (Q \to P)}$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F

All the entries in the resulting column are not T, hence the given proposition is not a tautology.

Example 9: Show that the proposition $(P \land \sim Q) \lor \sim(P \land \sim Q)$ is a tautology.

Solution:

P	**Q**	$\boldsymbol{\sim Q}$	$\boldsymbol{P \land \sim Q}$	$\boldsymbol{\sim(P \land \sim Q)}$	$\boldsymbol{(P \land \sim Q) \lor \sim(P \land \sim Q)}$
T	T	F	F	T	T
T	F	T	T	F	T
F	T	F	F	T	T
F	F	T	F	T	T

As the entries in the last column are T, the given proposition is a tautology.

Example 10: Verify that the proposition $P \lor \sim(P \land Q)$ is a tautology.

Solution:

P	**Q**	$\boldsymbol{P \land Q}$	$\boldsymbol{\sim(P \land Q)}$	$\boldsymbol{P \lor \sim(P \land Q)}$
T	T	T	F	T
T	F	F	T	T
F	T	F	T	T
F	F	F	T	T

As the entries in the last column are T, the given proposition is a tautology.

Space for learners:

CHECK YOUR PROGRESS-II

2. Prove that the following are tautologies (using truth tables):

a) $Q \vee (P \wedge \sim Q) \vee (\sim P \wedge \sim Q)$

b) $(P \rightarrow Q) \leftrightarrow (\sim P \vee Q)$

c) $\sim (P \vee Q) \vee (\sim P \wedge Q) \vee P$

3. Show that $((\sim P) \vee (\sim Q)) \vee P$is a tautology.

Space for learners:

7.5 CONTRADICTION

Definition: A statement formula which is false regardless of in the truth values of the statements which replace the variables in it is called a contradiction., if each entry in the final column of the truth table of a statement formula is F only then it is called as contradiction.

Clearly, the negation of a contradiction is a tautology. We may call a statement formula which is a contradiction as identically false.

Example 11: Verify that $P \wedge (\sim P)$ is acontradiction.

Solution:

P	**~P**	**P ∧ (~P)**
T	F	F
F	T	F

Since the last column has F only, the statement formula is a contradiction.

Example 12: Verify the statement (P ∧ Q) ∧~ (P vQ).

Solution:

P	**Q**	**P ∧ Q**	**P vQ**	**~ (P vQ)**	**(P ∧ Q) ∧ ~ (P vQ)**
T	T	T	T	F	F
T	F	F	T	F	F
F	T	F	T	F	F
F	F	F	F	T	F

Since the truth value of (P ∧ Q) ∧ ~ (P vQ) is F, for all values of P and Q, the proposition is a contradiction.

Example 13: Prove that, if A (p, q, ⋯) is a tautology, then ~A (p, q,⋯) is a contradiction and conversely.

Solution: Since a tautology is always true, the negation of a tautology is always false i.e., is a contradiction and vice-versa.

7.6 LOGICALEQUIVALENCE

Two statement formulas A (P, Q, ...) and B (P, Q, ...) are said to be logically equivalent or simply equivalent if they have identical truth tables. In other words, corresponding to identical truth values of P, Q, ... the truth values of A & B must be same. If A and B are equivalent, we shall write A≡B or A ⇔B.

Example 14: Show that P is equivalent to the following formulae.

(i)$\sim\sim P$ (ii) $P \wedge P$ (iii) $P \vee P$ (iv) $P \vee (P \wedge Q)$

(v) $P \wedge (P \vee Q)$

Solution:

P	**Q**	$\sim P$	$\sim\sim P$	$P \wedge P$	$P \vee P$	$P \wedge Q$	$P \vee (P \wedge Q)$	$P \vee Q$	$P \wedge (P \vee Q)$
T	T	F	T	T	T	T	T	T	T

Space for learners:

T	F	F	T	T	T	F	T	T	T
F	T	T	F	F	F	F	F	T	F
F	F	T	F	F	F	F	F	F	F

Here the 4^{th} ,5^{th} ,6^{th} ,7^{th} ,8^{th} ,10^{th} columns give the truth values of the formulas. The columns 1,4,5,6,8,10 have the identical truth values. Hence P is equivalent to all given formulas.

Example 15: Prove that $P \vee Q \Leftrightarrow \sim(\sim P \wedge \sim Q)$

Solution:

P	**Q**	**P∨Q**	**~P**	**~Q**	**~P∧~Q**	**~ (~P∧~Q)**
T	T	T	F	F	F	T
T	F	T	F	T	F	T
F	T	T	T	F	F	T
F	F	F	T	T	T	F

The truth table shows that P∨Qand ~ (~P∧~Q) have identical truth value column. So, $P \vee Q \Leftrightarrow \sim(\sim P \wedge \sim Q)$.

Example 16: Prove that $P \rightarrow Q \Leftrightarrow (\sim P \vee Q)$

Solution:

P	**Q**	**P → Q**	**~P**	**~P ∨ Q**
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Here, columns of P→Q and ~P ∨ Q are identical.

Hence, $P \rightarrow Q \Leftrightarrow (\sim P \vee Q)$.

Space for learners:

Space for learners:

CHECK YOUR PROGRESS-III

4.Explain the equivalence of propositions.

5.Show the following equivalences using truth table method:

a) $\sim(P \rightarrow Q) \Leftrightarrow P \wedge \sim Q$

b) $P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$

c) $P \rightarrow Q \Leftrightarrow \sim Q \rightarrow \sim P$

7.6.1 Equivalent Formulas

Using respective truth tables, we can prove the following equivalence:

Idempotent Laws	(i) $P \vee P \Leftrightarrow P$ (ii) $P \wedge P \Leftrightarrow P$
Associative Laws	(i) $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$ (ii) $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$
Commutative Laws	(i) $P \vee Q \Leftrightarrow Q \vee P$ (ii) $P \wedge Q \Leftrightarrow Q \wedge P$
De Morgan's Laws	(i) $\sim(P \wedge Q) \Leftrightarrow \sim P \vee \sim Q$ (ii) $\sim(P \vee Q) \Leftrightarrow \sim P \wedge \sim Q$
Distributive Laws	(i) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$ (ii) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$
Complement Laws	(i) $P \wedge \sim P \Leftrightarrow F$ (ii) $P \vee \sim P \Leftrightarrow T$
Dominance Laws	(i) $P \vee T \Leftrightarrow T$ (ii) $P \wedge F \Leftrightarrow F$
Identity Laws	(i) $P \wedge T \Leftrightarrow P$ (ii) $P \vee F \Leftrightarrow P$
Absorption Laws	(i) $P \vee (P \wedge Q) \Leftrightarrow P$ (ii) $P \wedge (P \vee Q) \Leftrightarrow P$
Double negation Law	$\sim(\sim P) = P$
Contra positive Law	$P \rightarrow Q \Leftrightarrow \sim Q \rightarrow \sim P$

Conditional as disjunction	$P \to Q \Leftrightarrow \sim P \vee Q$
Biconditional as conditional	$P \leftrightarrow Q \Leftrightarrow (P \to Q) \wedge (Q \to P)$
Exportation Laws	$P \to (Q \to R) \Leftrightarrow (P \wedge Q) \to R$

Space for learners:

Check yourself the above formulas as an exercise by truth table technique. Here, T and F respectively stands true statement and false statement.

Replacement Process: Consider the formula A: P → (Q→R). The formula Q→R is a part of the formula A. If we replace Q→R by an equivalent formula ~Q∨R in A, we get another formula B:P→(~Q∨R). We can easily verify that the formulas A and B are equivalent to each other. This process of obtaining B from A is known as there placement process. Using the laws stated in **7.6.1**, we can also establish equivalence of statement formulas without using truth tables.

Illustrative Examples:

Example 17: Prove that, (P→Q)∧(R→Q)⇔(P∧R)→Q

Solution:

(P → Q) ∧ (R →Q)

⇔(~P ∨ Q) ∧ (~R ∨ Q)
⇔(~P∧~R)∨ Q [Distributive Law]
⇔~ (P ∨ Q)∨ Q [DeMorgan's Law]
⇔(P∧R)→Q

Example18: Prove that, (~P∧(~Q∧R))∨(Q∧R)∨(P∧R)⇔R

Solution:

(~P∧(~Q∧R))∨(Q∧R)∨(P∧R)

⇔((~P ∧ ~Q)∧ R) ∨ ((Q ∨ P)∧ R) (Associative Law & distributive Law)

⇔(~ (P∨Q)∧R)∨((Q∨P)∧R) [DeMorgan's Law]

⇔(~ (P∨Q)∨(P∨Q))∧R (Distributive Law)

⇔T ∧ R Since ~S ∨ S ⇔T

⇔R as T ∧ R ⇔R

Example 19: Show that $P \to (Q \to R) \Leftrightarrow P \to (\sim Q \vee R) \Leftrightarrow (\sim P \wedge Q) \vee R$

Solution:

$P \to (Q \to R)$

$\Leftrightarrow\ P \to (\sim Q \vee R)$ [$\because P \to Q \Leftrightarrow \sim P \vee Q$]

$\Leftrightarrow \sim P \vee (\sim Q \vee R)$ [$\because P \to Q \Leftrightarrow \sim P \vee Q$]

$\Leftrightarrow (\sim P \vee \sim Q) \vee R$ [by Associative Law]

$\Leftrightarrow \sim(P \wedge Q) \vee R$ [By De Morgan's Law]

Hence $P \to (Q \to R) \Leftrightarrow P \to (\sim Q \vee R) \Leftrightarrow (\sim P \wedge Q) \vee R$

CHECK YOUR PROGRESS-IV

6. Prove that:

a) $(P \to Q) \wedge (R \to Q) \Leftrightarrow (P \vee R) \to Q$

b) $(P \vee Q) \wedge \sim(\sim P \wedge Q) \Leftrightarrow P$

c) $(P \to Q) \to Q \Leftrightarrow (P \vee Q)$

7.7 TAUTOLOGICAL OR LOGICAL IMPLICATIONS

Definition: A statement A is said to tautologically or logically imply a statement B if and only if A→B is a tautology. In this case, we write A→B, read as "A tautologically implies B" or "A logically implies B". We shall denote this idea by A⟹B which is read as "A implies B".

Note: Learner should be very cautious with the following four notations:

(1) → means the connective conditional

(2) ↔ means the connective Biconditional

(3) ⟺ means equivalent

(4) ⟹ means tautological implications.

Space for learners:

Space for learners:

Let us Know

i) $\Longrightarrow$ is not connective, A$\Longrightarrow$B is not a statement formula.

ii) A$\Longrightarrow$B states that A$\rightarrow$B is a tautology or A logically implies B.

iii) A$\Longrightarrow$B guarantees that B has the truth value T whenever A has the truth value T.

iv) By constructing the truth table, we can determine A$\Longrightarrow$B.

v) A$\Leftrightarrow$B if and only if A$\Longrightarrow$B and B$\Longrightarrow$A i.e., if each of two formulas A and B tautologically or logically implies the other, then A and B are equivalent.

Illustrative Examples:

Example 20: Show that $(P \wedge Q) \Longrightarrow (P \rightarrow Q)$

Solution: To prove the given proposition, it is enough to prove that $(P \wedge Q) \rightarrow (P \rightarrow Q)$is a tautology

P	**Q**	$\boldsymbol{P \wedge Q}$	$\boldsymbol{P \rightarrow Q}$	$\boldsymbol{(P \wedge Q) \rightarrow (P \rightarrow Q)}$
T	T	T	T	T
T	F	F	F	T
F	T	F	T	T
F	F	F	T	T

Since the last column of the truth table of$(P \wedge Q) \rightarrow (P \rightarrow Q)$ contains only T's, so$(P \wedge Q) \rightarrow (P \rightarrow Q)$is a tautology.

Hence $(P \wedge Q) \Longrightarrow (P \rightarrow Q)$

Example 21: Prove that $(P \rightarrow (Q \rightarrow R)) \Longrightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$ by constructing the truth table.

Solution:

To prove the given proposition, it is enough to prove that $(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$ is a tautology.

P	Q	R	$Q \to R$	$P \to Q$	$P \to R$	$(P \to (Q \to R))$	$(P \to Q) \to (P \to R)$	$(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
T	T	T	T	T	T	T	T	T
T	T	F	F	T	F	F	F	T
T	F	T	T	F	T	T	T	T
T	F	F	T	F	F	T	T	T
F	T	T	T	T	T	T	T	T
F	T	F	F	T	T	T	T	T
F	F	T	T	T	T	T	T	T
F	F	F	T	T	T	T	T	T

Since the last column of the truth table of $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$ contains only T's, so $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$ is a tautology.

Hence, $(P \to (Q \to R)) \Rightarrow ((P \to Q) \to (P \to R))$

Some Important Logical Implications:

1. $P \wedge Q \Rightarrow P$
2. $P \wedge Q \Rightarrow Q$
3. $P \Rightarrow P \vee Q$
4. $\sim P \Rightarrow P \to Q$
5. $Q \Rightarrow P \to Q$
6. $\sim (P \to Q) \Rightarrow P$
7. $\sim (P \to Q) \Rightarrow \sim Q$
8. $P \wedge (P \to Q) \Rightarrow Q$
9. $(P \to Q) \wedge (Q \to R) \Rightarrow P \to R$
10. $(P \vee Q) \wedge (P \to R) \wedge (Q \to R) \Rightarrow R$

Check yourself the above logical implications by using the truth table.

Example 22: Show that $P \wedge (P \to Q) \Rightarrow Q$ without constructing the truth table.

Solution: We have to prove that $[P \wedge (P \to Q)] \to Q$ is a tautology.

$[P \wedge (P \to Q)] \to Q$

$\Leftrightarrow [P \wedge (\sim P \vee Q)] \to Q$ $\quad [\because P \to Q \Leftrightarrow \sim P \vee Q]$

$\Leftrightarrow \sim [P \wedge (\sim P \vee Q)] \vee Q$ $\quad [\because P \to Q \Leftrightarrow \sim P \vee Q]$

Space for learners:

$\Leftrightarrow [\sim P \vee \sim(\sim P \vee Q)] \vee Q$ [DeMorgan's Law]

$\Leftrightarrow [\sim P \vee (P \wedge \sim Q)] \vee Q$ [DeMorgan's Law]

$\Leftrightarrow [(\sim P \vee P) \wedge (\sim P \vee \sim Q)] \vee Q$ [Distributive Law]

$\Leftrightarrow [T \wedge (\sim P \vee \sim Q)] \vee Q$ [Complement Law]

$\Leftrightarrow [\sim P \vee \sim Q] \vee Q$ [Identity Law]

$\Leftrightarrow [\sim P \vee (\sim Q \vee Q)]$ [Associative Law]

$\Leftrightarrow \sim P \vee T$ [Complement Law]

$\Leftrightarrow T$ [Identity Law]

Hence, $P \wedge (P \rightarrow Q) \Rightarrow Q$

CHECK YOUR PROGRESS-V

7.Show the following logical implications using the truth table:

d) $Q \Rightarrow P \rightarrow Q$

e) $\sim(P \rightarrow Q) \Rightarrow \sim Q$

8.Show the following logical implications without constructing the truth tables:

a) $P \wedge Q \Rightarrow P \vee Q$

b) $P \wedge Q \Rightarrow P \rightarrow Q$

7.8TWO-STATE DEVICES

Let us consider the example of an electric switch which is used for turning "On" and "Off "an electric light. It has wo states "On" and "Off ". So, it is a two-state device. Let us consider another example of a magnetic core which is used in computer. In magnetic core, there lies a doughnut-shaped metal disc with a wire coil wrapped around it. It may be magnetized in one direction, if current is passed through the coil in one way and may be magnetized in the opposite direction, it the current is reversed. So, the magnetic core is a two-state device.

Space for learners:

7.9 SUMMING UP

Space for learners:

- A statement formula is an expression which is a string consisting of (capital letters with or without subscripts), parentheses and connective symbols (∨, ∧, →, ↔, ∼), which produces a statement when the variables are replaced by statements.
- A statement formula which is true regardless of the truth values of the statements which replace the variables in it is called a universally valid formula or a tautology or a logical truth.
- A statement formula which is false regardless of the truth values of the statements which replaces the variables in it a contradiction.
- The statement formulas A and B are equivalent provided A ↔B is a tautology; and conversely, if A↔B is a tautology, then A and B are equivalent. We shall represent the equivalence of A and B by writing "A ⇔B" which is read as "A is equivalent to B."
- A statement A is said is to tautologically imply a statement B if and only if A → B is a tautology. We shall denote this idea by A ⟹ B which is read as "A logically implies B".

7.10 ANSWERS TO CHECK YOUR PROGRESS

Ans. to Q. 1:

(a) The variable that occur in the formula are P and Q, so we have to consider 4 possible combinations of truth values of two statements P and Q.

P	Q	$\sim P$	$\sim Q$	$\sim P \wedge \sim Q$	$\sim(\sim P \wedge \sim Q)$
T	T	F	F	F	T
T	F	F	T	F	T
F	T	T	F	F	T
F	F	T	T	T	F

(b) The variable are P and Q, clearly there are 2^2rows in the truth table of this formula.

Space for learners:

P	Q	~P	~Q	~P ∨ Q	~Q ∨ P	(~P ∨ Q) ∧(~Q ∨ P)
T	T	F	F	T	T	T
T	F	F	T	F	T	F
F	T	T	F	T	F	F
F	F	T	T	T	T	T

(c)

P	Q	$P \wedge Q$	$P \vee Q$	$(P \wedge Q) \rightarrow (P \vee Q)$
T	T	T	T	T
T	F	F	T	T
F	T	F	T	T
F	F	F	F	T

(d)

P	Q	$P \rightarrow Q$	$Q \wedge (P \rightarrow Q)$	$\big(Q \wedge (P \rightarrow Q)\big) \rightarrow P$
T	T	T	T	T
T	F	F	F	T
F	T	T	T	F
F	F	T	F	T

Answer to Q. 2:

(a)

P	Q	$\sim P$	$\sim Q$	$P \wedge \sim Q$	$Q \vee (P \wedge \sim Q)$	$\sim P \wedge \sim Q$	$Q \vee (P \wedge \sim Q) \vee (\sim P \wedge \sim Q)$
T	T	F	F	F	T	F	T
T	F	F	T	T	T	F	T
F	T	T	F	F	T	F	T
F	F	T	T	F	F	T	T

All the entries in the last column are T, the given formula is a tautology.

(b)

P	Q	~P	~P ∨ Q	P → Q	(P → Q) ↔(~P ∨ Q)
T	T	F	T	T	T
T	F	F	T	F	T
F	T	T	T	T	T
F	F	T	F	F	T

All the entries in the last column are T, the given formula is a tautology. Similarly, for (c) construct truth tables.

Answer to Q. 3:

Truth table for $\big((\sim P) \vee (\sim Q)\big) \vee P$

$\boldsymbol{P}$	$\boldsymbol{Q}$	$\boldsymbol{\sim P}$	$\boldsymbol{\sim Q}$	$(\boldsymbol{\sim P}) \vee (\boldsymbol{\sim Q})$	$\big((\boldsymbol{\sim P}) \vee (\boldsymbol{\sim Q})\big) \vee \boldsymbol{P}$
T	T	F	F	F	T
T	F	F	T	T	T
F	T	T	F	T	T
F	F	T	T	T	T

The last column contains only T.

$\therefore \big((\sim P) \vee (\sim Q)\big) \vee P$ is a tautology.

Ans. To Q. 4: Two propositions are logically equivalent or simply equivalent if they have exactly the same truth values under all circumstances.

Ans. To Q. 5:

(a)

P	Q	~Q	P → Q	~ (P → Q)	P ∧ ~Q
T	T	F	T	F	F
T	F	T	F	T	T
F	T	F	T	F	F
F	F	T	T	F	F

As ~ (P → Q) and P ∧ ~Q have identical truth columns, so ~ (P → Q)⇔ P ∧ ~Q.

Space for learners:

(b)

P	**Q**	**P → Q**	**Q → P**	**P ↔ Q**	**(P → Q)∧ (Q → P)**
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

As $P \leftrightarrow Q$ and $(P \rightarrow Q) \wedge (Q \rightarrow P)$ have identical truth columns, so, $P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$.

(c)

P	**Q**	**~P**	**~Q**	**P → Q**	**~Q → ~P**
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

As $P \rightarrow Q$ and $\sim Q \rightarrow \sim P$ have identical truth columns, so $P \rightarrow Q \Leftrightarrow \sim Q \rightarrow \sim P$.

Ans. to Q. 6:

(a) We know that $P \rightarrow Q \Leftrightarrow \sim P \vee Q$

Similarly, $R \rightarrow Q \Leftrightarrow \sim R \vee Q$

Now, $(P \rightarrow Q) \wedge (R \rightarrow Q) \Leftrightarrow (\sim P \vee Q) \wedge (\sim R \vee Q)$
$\Leftrightarrow (\sim P \wedge \sim R) \vee Q$ (By distributive law)
$\Leftrightarrow (\sim(P \vee R)) \vee Q$ (By DeMorgan's law)
$\Leftrightarrow (P \vee R) \rightarrow Q$.

(b) $(P \vee Q) \wedge \sim(\sim P \wedge Q)$

$\Leftrightarrow (P \vee Q) \wedge (\sim\sim P \vee \sim Q)$ [De Morgan's Law]

$\Leftrightarrow (P \vee Q) \wedge (P \vee \sim Q)$ [Law of Double Negation]

$\Leftrightarrow P \vee (Q \wedge \sim Q)$ [Distributive Law]

$\Leftrightarrow P \vee F$ [Inverse Law]

$\Leftrightarrow P$ [Identity Law]

Space for learners:

(c) $(P \to Q) \to Q$

$\Leftrightarrow (\sim P \vee Q) \to Q$ [Conditional as disjunction]

$\Leftrightarrow \sim(\sim P \vee Q) \vee Q$ [Conditional as disjunction]

$\Leftrightarrow (\sim\sim P \wedge \sim Q) \vee Q$ [De Morgan's Law]

$\Leftrightarrow (P \wedge \sim Q) \vee Q$ [Law of Double Negation]

$\Leftrightarrow (P \vee Q) \wedge (\sim Q \vee Q)$ [Distributive Law]

$\Leftrightarrow (P \vee Q) \wedge T$ [$\sim Q \vee Q = T$]

$\Leftrightarrow P \vee Q$ [$\because P \wedge T = P$]

Hence, $(P \to Q) \to Q \Leftrightarrow P \vee Q$

Ans. to Q. 7:

(a)

P	Q	P → Q	Q → (P → Q)
T	T	T	T
T	F	F	T
F	T	T	T
F	F	T	T

Since, $Q \to (P \to Q)$ is a tautology, Therefore $Q \Rightarrow P \to Q$.

(b)

P	Q	~Q	P→Q	~ (P → Q)	~ (P → Q) →~Q
T	T	F	T	F	T
T	F	T	F	T	T
F	T	F	T	F	T
F	F	T	T	F	T

Since $\sim(P \to Q) \to \sim Q$ is a tautology, therefore $\sim(P \to Q) \Rightarrow \sim Q$.

Ans. to Q. 8:

(a) We have to prove that $P \wedge Q \to P \vee Q$ is a tautology.

$P \wedge Q \to P \vee Q$

$\Leftrightarrow \sim(P \wedge Q) \vee (P \vee Q)$ [Conditional as disjunction]

$\Leftrightarrow (\sim P \vee \sim Q) \vee (P \vee Q)$ [De Morgan's Law]

$\Leftrightarrow (P \vee \sim P) \vee (Q \vee \sim Q)$ [Associative and Commutative law]

$\Leftrightarrow T \vee T$ [$P \vee \sim P = T, Q \vee \sim Q = T$]

$\Leftrightarrow T$ [Idempotent Law]

Space for learners:

Hence, $P \wedge Q \Longrightarrow P \vee Q$

(b) We have to prove that $P \wedge Q \to (P \to Q)$is a tautology.

$P \wedge Q \to (P \to Q)$

$\Leftrightarrow$ $(P \wedge Q) \to (\sim P \vee Q)$ [Conditional as disjunction]

$\Leftrightarrow$ $\sim(P \wedge Q) \vee (\sim P \vee Q)$ [Conditional as disjunction]

$\Leftrightarrow$ $(\sim P \vee \sim Q) \vee (\sim P \vee Q)$ [De Morgan's Law]

$\Leftrightarrow$ $\sim P \vee (\sim Q \vee Q)$ [Associative Law]

$\Leftrightarrow$ $\sim P \vee T$ [$\sim$Q$\vee$ Q $=$ T]

$\Leftrightarrow$ T

Hence, $P \wedge Q \to P \vee Q$ is a tautology.

$\therefore$ $P \wedge Q \Longrightarrow P \vee Q$

7.11 POSSIBLE QUESTIONS

1. Construct the truth table for each of the following:

(a) (P ∧ Q) → (P ∨Q)

(b) (P ∧ Q) →~P

(c) (P → Q) ∧ (~P ∨ Q)

2. With the help of truth tables, prove the following:

(a) (P → Q) ⟺(~P ∨ Q)

(b) (P → Q) ⟺(~Q → ~P)

(c) (P∧Q)⟺(P→Q)∧(Q→P)

3. Use the truth table to determine whether the proposition $\big((\sim P) \vee Q\big) \vee \big(P \wedge (\sim Q)\big)$ is a tautology.

4. Show the implications without constructing the truth tables.

(a) ~ (P → Q) ⟹ P

(b) P∧ (P → Q) ⟹ Q

(c) ~Q∧ (P → Q)⟹ ~P

(d) (P∨ Q) ∧ $(\sim P)$ ⟹ Q

(e) (P→Q) → Q ⟹ P ∨ Q

(f) (P∧Q)⟹ P→Q

5. Discuss the different types of statements with examples.

Space for learners:

6. What do you mean by tautology? Explain with example

7. What is contradiction? Discuss.

8. Give a detailed discussion on logical equivalence.

9. What do you mean by tautological implications? Explain.

Space for learners:

7.12 REFERENCES AND SUGGESTED READINGS

- Rao, G.S. S. Bhishma. *Discrete Structures and Graph Theory*. SciTech Publications (India) PVT Ltd,2003
- Sharma, J.K. *Discrete Mathematics*. Macmillan Publishers India Ltd,2011
- Balaji, G. *Discrete Mathematics*. Balaji Publishers,2015
- Singaravelu, A.& Jeyaraman, M.P. *Discrete Mathematics*. Meenakshi Agency,2016
- Satyanarayana, B.& Prasad, K.S. *Discrete Mathematics and Graph Theory*. PHI Learning Private Limited,2009
- Rao,G.S. *Discrete Mathematical Structure*. New Age international (P) Limited,2009
- Singh, Y.N. *Mathematical Foundation of Computer Science*, New Age international Publishers, 2005
- Lipschutz, S & Lipson, M. L. Schaum's outline of *Theory and Problems of Discrete Mathematics*, McGraw-Hill,2007
- Chandrasekaran, N & Umaparvathi, M. *Discrete Mathematics*, PHI Learning Private Limited,201
- Tremblay, J.P. & Manohar, *Discrete Mathematical Structures with Applications to Computer Science,* Tata McGraw Hill Education Private Limited,1997

UNIT 8: PREDICATE CALCULUS

Space for learners:

Unit Structure:

8.1 INTRODUCTION

In this unit, we shall discuss about simple statements and their validity through predicates and quantifiers. Also, we apply predicate formulas to determine the truth or falsity of the statements. The soundness, completeness and compactness of the statements are also discussed in this unit.

8.2 UNIT OBJECTIVES

After going through this unit, you will be able to

- understand the logic of a computer program

- develop write programs in various computer languages.
- get ideas behind mathematical logic and inference theory
- understand mathematical logic associated with various reasoning and mathematical proofs
- understand predicates, quantifiers, free and bound variables
- know the inference theory of predicate calculus.

Space for learners:

8.3 PREDICATES

Let us consider a mathematical relation $x>10$. The Statement "x is greater than 10" has two parts. The first part, the variable x, is the subject of the statement. The second part, "is greater than 10" which refers to a property that the subject can have, is called the predicate. We can denote the statement "x is greater than 10" by the notation $P(x)$, where P denotes the predicate "is greater than 10" and x is the variable. $P(x)$ is called propositional function of x. Once a value has been assigned to the variable x, the statement $P(x)$ becomes a proposition and has a truth value.

8.4 QUANTIFIERS

Many mathematical statements assert that a property is true for all values of a variable or for some values of the variable, in a particular domain, called the universe of discourse. Mostly it is denoted by D.

The universal quantification of $P(x)$ is the statement:

$P(x)$ is true for all values of x in the universe of discourse" and is denoted by the notation,

$$\boldsymbol{(x)P(x) \text{ or } \forall x P(x).}$$

The proposition $(x)P(x$)or $\forall xP(x$ is read as "for all x,$P(x)$" or "for every x, $P(x)$". The symbol $\forall$ is called the universal quantifier.

The existential quantification of $P(x$)is the proposition. There exists at least one x (or an x) such that $P(x)$ is true" and is denoted by the notation $\boldsymbol{\exists x P(x)}$.

The symbol ∃ is called the existential quantifier.

Example 1: Express the following statement using quantifiers:

"Every Computer Science student needs a course in Mathematics"

Solution.

Let D={Students in Computer Science} (D is universe of discourse or domain).

Let $P(x)$:x needs a course in Mathematics.

We can rewrite the above expression as "For all x, x needs a course in Mathematics".

Then $\forall x P(x)$.

Example 2: Express the following statement using quantifiers:

"Every Computer Science student needs a course in Mathematics".

Solution.

Let, D={Students}

Let, $P(x)$:x is Computer Science student.

$Q(x)$:x needs a course in Mathematics.

We can rewrite the above expression as:

"For all x, if x is a Computer Science student, then x needs a course in Mathematics".

Then, $\forall x[P(x)\rightarrow Q(x)]$.

Example 3: Express the following statement using quantifiers:

"There is a student in this class, who owns a personal computer".

Solution.

Let, D={Students int his class}.

Let, $P(x)$:x owns a personal computer.

We can rewrite the above expression as:

"There exists an x, such that, x owns a personal computer".

Then, $\exists x P(x)$.

Space for learners:

Example 4: Express the following statement using quantifiers:

"Everyone who knows how to write programs in JAVA can get a high paying job".

Solution.

Let, D={Students in this class}.

Let, $P(x)$:x knows how to write programs in JAVA.

$Q(x)$:x gets a high paying job.

We can rewrite the above expression as:

"For every x, if x knows how to write programs in JAVA then he gets a high paying job".

Then $\forall x[P(x) \rightarrow Q(x)]$.

Example 5: Express the following statement using quantifiers:

"Someone who passed the first examination has not read the book".

Solution.

Let, D={Students in this class}.

Let, $P(x)$: x has passed the first examination.

$Q(x)$:x has not read the book.

We can rewrite the above expression as "There exists an x, such that x has passed the first examination and x has not read the book".

Then $\exists x[P(x) \wedge Q(x)]$.

8.4.1 Negation of a Quantified Expression

Example 6: Find the negation of following expression:

"Every student in the class has studied computer programming".

Solution.

Let, D={Students in a Class}.

Space for learners:

Let, $P(x)$:x has studied computer programming. Then the given expression is $\forall x P(x)$.

To find the negation of $\forall x P(x)$:

Negation of the above expression is "It is not the case that, every student in the class has studied computer programming". Hence it is represented as $\neg[\forall x P(x)]$.

It also means that, "there is a student in the class who has not studied computer programming", i.e., there is a student x in the class, such that, x has not studied computer programming.

Hence it is represented as $\exists x[\neg P(x)]$.

$\therefore \neg[\forall x P(x)] \equiv \exists x[\neg P(x)]$.

Example 7: Find the negation of following expression:
"There is a student in the class who has studied computer programming".
Solution:

Let, $P(x)$: x has studied computer programming.

Let, D={Students in a Class} (D is universe of discourse or domain).

Then the given expression is $\exists x P(x)$.

To find the negation of $\exists x P(x)$:

Negation of the above expression is "It is not the case that, there is a student in the class who has studied computer programming". Hence it is represented as $\neg[\exists x P(x)]$.

It also means that, "No student is found in the class, who have studied computer programming", i.e., "Every student in the class has not studied computer programming", i.e., "For every x in the class, x has not studied computer programming".

Hence it is represented as $\forall x[\neg P(x)]$.

$\therefore \neg[\exists x P(x)] \equiv \forall x[\neg P(x)]$.

Space for learners:

8.5 PREDICATE FORMULAS

We denote by $P(x_1, x_2, ..., x_n)$, an n-place predicate formula in which the letter P is an n-place predicate and x_1, x_2,…,x_n are individual variables. In general, $P(x_1, x_2, ..., x_n)$ is called an **atomic formula** of predicate calculus. The following are some examples of atomic formulas.

$A(x)$, $B(x, y)$ and $C(x, d, z)$.

A **well-formed formula** (*wf.*) of predicate calculus is defined by

(i) Every atomic formula is a well-formed formula.

(ii) If A is a well-formed formula, so is $\neg A$.

(iii) If A and B are well-formed formulas, so are $(A \vee B)$, $(A \wedge B)$, $(A \to B)$ and $(A$ € $B)$.

(iv) If A is a well-formed formula and x is any variable, so are $(x)A$ and $(\exists x)A$.

(v) Only the formulas obtained by applying rules (i)-(iv) are well-formed formulas.

CHECK YOUR PROGRESS-I

1. A property that the subject can have, is called the ________________
2. The symbol _______ is called the existential quantifier.
3. The symbol _______ is called the universal quantifier.
4. The negation of a statement is denoted by the symbol

Space for learners:

8.6 FREE AND BOUND VARIABLES

Space for learners:

Consider the following statement:

All students are intelligent. This can be written in symbolic form as

$$(x)(S(x) \to I(x)),$$

where $S(x): x$ is a student and $I(x): x$ is intelligent.

In the above statement, if we restrict the class as the class of students, then the symbolic representation will be $(x)I(x)$. Such a restricted class is also called "Universe of Discourse".

- In any symbolic formula, the part containing $(x)A(x)$ or $\exists x A(x)$, such part is called the "x-bound" part of the formula.
- Any variable appearing in an "x- bound" part of the formula is called as a bound variable.
- Otherwise, it is called as a free variable.
- Any formula immediately following (x) or $(\exists x)$ is called the scope of the quantifier.

Example 8:

Consider the symbolic form of a statement: $(y)A(y) \vee B(y)$.

In this notation, all y in $A(y)$ is bound whereas the y in $B(y)$ is free.

The scope of (y) is $A(y)$.

8.7 INFERENCE THEORY OF PREDICATE CALCULUS

Rules of Inference:

1. **Rule P**: A premise can be introduced at any point of derivation.
2. **Rule T**: A formula can be introduced provided it is tautologically implied by previously introduced formulas in the derivation.
3. **Rule CP**: If S can be derived from R and a set of premises, then $R \to S$ can be derived from the set of premises alone.

Rule US [Universal Specification]:

Space for learners:

It is the rule of inference, which states that one can conclude that $A(k)$ is true, if $\forall y \ \ A(y)$ is true, where $'k'$ is an arbitrary member of the universe of discourse. This rule is also called the Universal Instantiation.

In other words, Universal Specification is the rule of inference which says we can conclude $A(k)$ is true for a particular element k of the universe of discourse if $\forall y \ A(y)$ is true. This k can be chose arbitrarily.

For example, if $y^2 > 0, \ \forall y \neq 0,$ then $3^2 > 0,$ for the particular value $3.$ It is true for any $k \neq 0, \ k^2 > 0.$

Rule ES [Existential Specification]:

It is the rule which allows us to conclude that $A(k)$ is true ,if $\exists y \ \ A(y)$ is true, where $'k'$ is not an arbitrary member of the universe, but one for which $A(k)$ is true. Usually we will not know, what $'k'$is, but know that it exists. Since it exists, we may call it $'k'.$ This rule is also called the Exist entail Instantiation.

In other words, Existential Specification is the rule of inference which says that there is an element k in the universe of discourse for which $A(k)$ is true if $\exists y \ A(y)$ is true. Here $'k'$ is not arbitrary, but it is specific. In practice, we may not know what $'k'$ is, but it exists. Since it exists, we give a name $'k'$ and proceed with our argument.

Rule UG [Universal Generalization]:

It is the rule which states that $\forall y \ \ A(y)$ is true, if $A(k)$ is true, where $'k'$is an arbitrary member (not a specific member) of the universe of discourse.

In other words, Universal Generalization is the rule of inference which says that $\forall y \ A(y)$ is true if $A(k)$ is true for an arbitrary element $'k'$ of the universe of discourse. This rule is used when we need to prove $\forall y \ A(y)$ is true.

Rule EG [Existential Generalization]

It is the rule that is used to conclude that, $\exists y \ \ A(y)$ when $A(k)$ is true, where $'k'$is a particular member of the universe of discourse.

In other words, Existential Generalization is the rule of inference which says that for particular element $'k'$ of the universe of discourse if $A(k)$ is true, then $\exists y \ A(y)$ is true.

We summarize the above rules in the following table.

Rule	**Inference**
US	$\forall y A(y)$ $\therefore A(k)$ for an arbitrary k
ES	$\exists y \ A(y)$ $\therefore A(k)$ for a particular k
UG	$A(k)$ for an arbitrary k $\therefore \forall y \ A(y)$
EG	$A(k)$ for some k $\therefore \exists y \ A(y)$

Remark:

We have seen rules of inference for proposition and rules of inference for quantified propositions. Sometimes, we have to use a combination of the above rules. Two such combinations of rules of inference quite often used are the Universal Modus Ponens and Universal Modus Tollens.

- **Universal Modus Ponens (MP)** says that $\forall y$, if $A(y)$ is true then $B(y)$ is true and if $A(k)$ is true for a particular element $'k'$ in the universe of discourse then $B(k)$ must also be true.

  Thus,

  $\forall y \ (A(y) \to B(y))$

  $A(k)$

  $B(k)$,

  where $'k'$ is particular element in the domain.

- **Universal Modus Tollens (MT)** says that $\forall y$, if $A(y)$ then $B(y)$ and if for a particular element $'k'$ in the universe of discourse $\neg B(k)$ is true then $\neg A(k)$ is true.

  Thus,

Space for learners:

$\forall y\ (A(y) \to B(y))$

$\neg B(k)$

$\neg A(k)$

for a particular $'k'$.

- **Universal Transitivity (UT)** says that if $\forall y(A(y) \to B(y))$ and $\forall y(B(y) \to C(y))$ are true, then $\forall y(A(y) \to C(y))$ is true, where the domains of all the quantifiers are the same.

Example 8:

Let us verify the argument by inference theory.

All men are mortal.

Socrates is a man.

Therefore, Socrates is mortal.

Solution.

Let, $D = \{\text{Human being}\}$

Let, $P(x)$: x is a man; $Q(x)$: x is mortal and s :Socrates.

Above problem becomes $\forall x[P(x) \to Q(x)]$, $P(s) \Rightarrow Q(s)$

S. No	Statement	Reason
1	$\forall x[P(x) \to Q(x)]$	Rule P (Given Premise)
2	$P(s) \to Q(s)$	Rule US, 1
3	$P(s)$	Rule P (Given Premise)
4	$Q(s)$	MP, 2, 3

Solved Problems

1. Prove the implication:

$\forall x(P(x) \to Q(x)), \forall x(R(x) \to \neg Q(x)) \Rightarrow \forall x(R(x) \to \neg P(x))$.

Solution:

Given premises are $\forall x(P(x) \to Q(x)), \forall x(R(x) \to \neg Q(x))$.

Conclusion is $\forall x(R(x) \to \neg P(x))$.

Space for learners:

S. No	Statement	Reason
1	$\forall x(P(x)\rightarrow Q(x))$	Rule P
2	$P(a)\rightarrow Q(a)$	RuleUS,1,forall a
3	$\forall x(R(x)\rightarrow \neg Q(x))$	Rule P
4	$R(a)\rightarrow \neg Q(a)$	RuleUS,3,forall a
5	$\neg Q(a)\rightarrow \neg P(a)$	RuleT,2,contrapositive,forall$a$
6	$R(a)\rightarrow \neg P(a)$	RuleT,4,5, for all a
7	$\forall x(R(x)\rightarrow \neg P(x))$	RuleUG,6

2. Prove that $\forall x(P(x)\rightarrow(Q(y)\wedge R(x)))$, $\exists xP(x)\Rightarrow Q(y)\wedge\exists x(P(x)\wedge R(x))$.

Solution:

Premises are $\forall x(P(x)\rightarrow(Q(y)\wedge R(x)))$,$\exists xP(x)$.

Conclusion is $Q(y)\wedge\exists x(P(x)\wedge R(x))$.

S.No	Statement	Reason
1	$\forall x(P(x)\rightarrow(Q(y)\wedge R(x)))$	Rule P
2	$P(a)\rightarrow(Q(y)\wedge R(a))$	RuleUS,1,for all a Rule P
3	$\exists xP(x)$	RuleES,3,for some a
4	$P(a)$	MP,2,4,for some a
5	$Q(y)\wedge R(a)$	RuleT,5
6	$Q(y)$	RuleT,5, for some a
7	$R(a)$	
8	$P(a)\wedge R(a)$	Rule T, 4,7, for some aRuleEG,8
9	$\exists x(P(x)\wedge R(x))$	RuleT,6,9
10	$Q(y)\wedge\exists x(P(x)\wedge R(x))$	

Space for learners:

3. Show by indirect method of proof, that

$\forall x(P(x) \lor Q(x)) \Rightarrow (\forall x P(x)) \lor (\exists x Q(x))$.

Solution:

By indirect method, let us assume that $\neg[(\forall x P(x)) \lor (\exists x Q(x))]$ as an additional premise and arrive at a contradiction.

S.No	Statement	Reason
1	$\neg[(\forall x P(x)) \lor (\exists x Q(x))]$	Rule P (additional premise)
2	$\neg(\forall x P(x)) \land \neg(\exists x Q(x))$	RuleT,DeMorgan'slaw,1
3	$\neg(\forall x P(x))$	RuleT,2
4	$\neg(\exists x Q(x))$	RuleT,2
5	$\exists x \neg P(x)$	RuleT,3
6	$\forall x \neg Q(x)$	RuleT,4
7	$\neg P(a)$	Rule ES, 5, for some a
8	$\neg Q(a)$	Rule US, 6, for all a
9	$\neg P(a) \land \neg Q(a)$	RuleT,7,8,for some a
10	$\neg(P(a) \lor Q(a))$	RuleT,DeMorgan'slaw,9, for some a
11	$\forall x(P(x) \lor Q(x))$	Rule P
12	$P(a) \lor Q(a)$	Rule US, 11, for all a
13	$\neg(P(a) \lor Q(a)) \land (P(a) \lor$	RuleT,10,12,for some a
14	$Q(a))$	RuleT,13
	F	

4. Prove the implication

$\forall x(P(x) \to Q(x)), \forall x(R(x) \to \neg Q(x)) \Rightarrow \forall x(R(x) \to \neg P(x))$.

Solution:

Premises are $\forall x(P(x) \to Q(x))$ and $\forall x(R(x) \to \neg Q(x))$.

Conclusion is $\forall x(R(x) \to \neg P(x))$.

Space for learners:

S.No	Statement	Reason
1	$\forall x(P(x)\rightarrow Q(x))$	Rule P
2	$P(a)\rightarrow Q(a)$	RuleUS,1,for all a
3	$\forall x(R(x)\rightarrow\neg Q(x))$	Rule P
4	$R(a)\rightarrow\neg Q(a)$	RuleUS,3,forall a
5	$Q(a)\rightarrow\neg R(a)$	Rule T, Contrapositive,4, For all a
6	$P(a)\rightarrow\neg R(a)$	Rule T, 2, 5, for all a
7	$R(a)\rightarrow\neg P(a)$	RuleT,Contrapositive,6, For all a
8	$\forall x(R(x)\rightarrow\neg P(x))$	RuleUG,7

Space for learners:

5. Show that the premises "One student in this class knows how to write programs in JAVA" and "Everyone who knows how to write programs in JAVA can get a high-paying job" imply the conclusion "Someone in this class can get a high-paying job".

Solution:

Let, D={Student}.

Let, $C(x)$:x is in this class.

$J(x)$:x knows JAVA programming.

$H(x)$:x can get a high-paying job.

Then premises are $\exists x(C(x)\wedge J(x))$ and $\forall x(J(x)\rightarrow H(x))$.

Conclusion is $\exists x(C(x)\wedge H(x))$.

S.No	Statement	Reason
1	$\exists x(C(x)\wedge J(x))$	Rule P
2	$C(a)\wedge J(a)$	RuleES,1,for some a
3	$C(a)$	Rule T, 2, for some a
4	$J(a)$	Rule T, 2, for some a
5	$\forall x(J(x)\rightarrow H(x))$	Rule P
6		RuleUS,5,for all a

7	$J(a) \rightarrow H(a)$	Rule T, MP,4,6,for some a
8	$H(a)$	Rule T, 3, 7, for some a
9	$C(a) \wedge H(a)$	RuleEG,8
	$\exists x(C(x) \wedge H(x))$	

Space for learners:

6. Show that the premises "A student in this class has not read the book" and "Everyone in this class passed the first examination" imply the conclusion "Someone who passed the first examination has not read the book".

Solution:

Let, $D=\{\text{Student}\}$.

Let, $C(x)$:x is in this class.

$R(x)$:x has not read the book.

$F(x)$:x has passed the first examination.

Then the premises are $\exists x(C(x) \wedge R(x))$, $\forall x(C(x) \rightarrow F(x))$.

Conclusion is $\exists x(F(x) \wedge R(x))$.

S.No	Statement	Reason
1	$\exists x(C(x) \wedge R(x))$	Rule P
2	$C(a) \wedge R(a)$	RuleES,1, for some a
3	$C(a)$	Rule T, 2, for some a
4	$R(a)$	Rule T, 2, for some a
5	$\forall x(C(x) \rightarrow F(x))$	Rule P
6	$C(a) \rightarrow F(a)$	RuleUS,5,for all a
7	$F(a)$	RuleT,MP,3,6,for some a
8	$F(a) \wedge R(a)$	Rule T, 4, 7, for some a
9	$\exists x(F(x) \wedge R(x))$	Rule EG,8

8.8 VALIDITY

In the practical life, the validity of a statement made by a person is important. Suppose a person makes a validity of a statement which may be true depending on the nature of the statement. For example, if the statement is "Daily it is raining or it is raining on some days".

A predicate formula is said to have validity if every assignment in every structure satisfies it.

Examples:

1. $\exists y\, P \rightarrow \exists \forall y \neg P$
2. $\forall y\, P \rightarrow \neg \exists y \neg P$
3. $\exists y (P \vee Q) \leftrightarrow \exists y\, P \vee \exists y\, Q$
4. $\forall y\, (P \wedge Q) \leftrightarrow \forall y\, P \wedge \forall y\, Q$
5. $\forall y\; y = y$

8.9. SOUNDNESS, COMPLETENESS AND COMPACTNESS

There are distinct concepts of "truth" ($\models$) and "provability" ($\vdash$). We'd like them to be the same, in the sense that we should only be able to prove things that are true, and if they are true, we should be able to prove them. These two properties are known as **soundness** and **completeness**.

A proof system is **sound** if everything that is provable is true. In other words, if $A_1,\ldots,A_n \vdash S$ then $A_1,\ldots,A_n \models S$.

A proof system is **complete** if everything that is true has a proof. In other words, if $A_1,\ldots,A_n \models S$ then $A_1,\ldots,A_n \vdash S$.

A set W of well-formed formulas is called satisfiable if and only if there is a truth assignment that satisfies every member of W.

A set of well-formed formulas is satisfiable if and only if every finite subset is satisfiable (**Compactness Theorem**).

Space for learners:

CHECK YOUR PROGRESS-II

5. In the statement $(x)(S(x) \to I(x))$, _______ is free and ______ is bound variables.
6. A proof system is _______if everything that is provable is true.
7. A proof system is _________if everything that is true has a proof.
8. A set of well-formed formulas is ____________if and only if every finite subset is satisfiable (**Compactness Theorem**).

Space for learners:

8.10 SUMMING UP

- Propositions have truth values.
- A property is true for all values of a variable or for some values of the variable, in a particular domain. It is called the universe of discourse.
- Conjunction, disjunction or negation operations can be applied on propositions.
- Every atomic formula is a well-formed formula.
- Any variable appearing in an "x - bound" part of the formula is called as a bound variable. Otherwise, it is called as a free variable.
- Any formula immediately following (x) or $(\exists x)$ is called the scope of the quantifier.
- A predicate formula is said to have validity if every assignment in every structure satisfies it.
- A proof system is **sound** if everything that is provable is true. A proof system is **complete** if everything that is true has a proof.
- A set W of well-formed formulas is called satisfiable if and only if there is a truth assignment that satisfies every member of W.

8.11 ANSWERS TO CHECK YOUR PROGRESS

Space for learners:

1. Predicate
2. ∃
3. ∀
4. ¬
5. *I(x), S(x)*
6. Sound
7. Complete
8. Satisfiable

8.12 POSSIBLE QUESTIONS

1. Express the following statements using predicates and both quantifiers.

   (i) All men are mortal.

   (ii) Every apple is red.

   (iii) All birds can fly.

   (iv) There is an integer which is odd and prime.

   (v) Every student of this class visited either Mumbai or New Delhi".

2. For the following statements, write the symbolic form using predicates and quantifiers, and then their negation forms.

   (i) Everybody who is healthy can do all types of works.

   (ii) Some people are not admired by everyone.

   (iii) Everyone should help his neighbours or his neighbours will not help him.

3. Show that the premises "Everyone in the Computer Science branch has studied Discrete Mathematics" and "John is in Computer Science branch" imply the conclusion "John has studied Discrete Mathematics".

Space for learners:

4. Verify the validity of the following statement.

   Every living thing is a plant or an animal. John's gold fish is alive and it is not a plant. All animals have hearts. Therefore John's gold fish has a heart.

5. Find the free and bound variables in the following:

   (i) $\forall y\ (A(y) \wedge B(y)) \rightarrow \forall y\ (A(y)) \wedge C(y)$.

   (ii) $(\forall y\ A(y)\ \text{€}\quad B(y) \wedge \exists y\ C(y)) \wedge D(y)$.

8.13 REFERENCES AND SUGGESTED READINGS

- Bernad Kolman, Robert C. Busby and Sharon Cutler Ross, *Discrete Mathematical Structures*, Pearson, USA. 2014.
- Kenneth Rosen, *Discrete Mathematics and Its Applications*, McGraw-Hill Higher Education, New York, 2019.
- Senthil Kumar B. V. and Hemen Dutta, *Discrete Mathematical Structures: A Succinct Foundation*, CRC Press, Boca Raton FL, 2020.
- Seymour Lipschutz and Marc Lipson, *Schaums Outline of Discrete Mathematics*, MCGraw-Hill, New York, 2007.
- G. Shankar Rao, *Discrete Mathematics Structures*, New Age International Pvt. Ltd., India, 2007.
- Sriraman Sridharan and R. Balakrishnan, *Discrete Mathematics: Graph Algorithms*, Algebraic Structures, Coding Theory and Cryptography, CRC Press, Boca Raton, FL, 2020.
- Susanna S. Epp, *Discrete Mathematics with Applications*, Cengage Learning, Boston USA, 2019.
- J. P. Tremblay and R. Manohar, *Discrete Mathematical Structures with Applications to Computer Science*, Tata McGraw-Hill, New Delhi, India, 2008.
- Iqbal H. Jebril, Hemen Dutta and Ilwoo Cho, *Concise Introduction to Logic and Set Theory*, CRC Press, Boca Raton FL, 2021.