

FOUNDATIONS OF MATHEMATICS

B.Sc. Mathematics

Core Course I

I Semester

(2011 Admission onwards)



UNIVERSITY OF CALICUT

SCHOOL OF DISTANCE EDUCATION

Calicut University P.O. Malappuram, Kerala, India 673 635

349

UNIVERSITY OF CALICUT

SCHOOL OF DISTANCE EDUCATION

B.Sc Mathematics

I Semester

Core Course I

FOUNDATIONS OF MATHEMATICS

MODULE I & II

*Prepared by: Sri. V.N. Mohammed
Department of Mathematics
TMG College
Tirur, Malappuram*

MODULE III & IV

*Prepared by: Sri. Shinoj K.M.
Department of Mathematics
St. Joseph's College, Devagiri*

*Scrutinised By: Sri. C. P. Mohammed,
Poolakkandy House,
Nanmanda P.O. Calicut*

Layout: Computer Section, SDE

©
Reserved

CONTENTS		PAGE
MODULE - 1	SET OPERATIONS	5
MODULE - 2	FUNCTIONS	30
MODULE - 3	BASIC LOGIC-1	55
MODULE - 4	BASIC LOGIC 2	70

MODULE-1

SET OPERATIONS

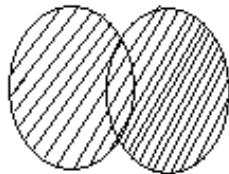
Definition:-

Let A and B be two sets, the union of A and B, denoted by $A \cup B$ is the set that contains those elements that are either in A or in B or in Both

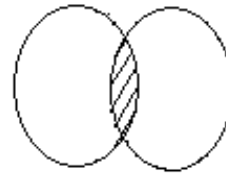
We can write $A \cup B = \{x / x \in A \vee x \in B\}$

The intersection of two sets A and B, denoted by $A \cap B$ is the set that contains those elements that are in both A and B

i.e., $A \cap B = \{x | x \in A \wedge x \in B\}$



$A \cup B$



$A \cap B$

Example:-

1) Let $A = \{a, e, i, o, u\}$, $B = \{a, b, c, d, e\}$

Then $A \cup B = \{a, b, c, d, e, i, o, u\}$, $A \cap B = \{a, e\}$

2) Let $A = \{x | x \text{ is an even positive integer}\}$

$B = \{x | x \text{ is an odd positive integer}\}$ then

$A \cup B = \{x | x \text{ is a positive integer}\}$ and $A \cap B = \emptyset$

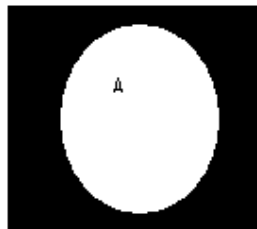
Note:-

Two sets A and B are said to be disjoint if $A \cap B = \emptyset$

Definition:-

Let U be the universal set. then the **complement** of a set A, denoted by \bar{A} is the set of all elements of U which are not in A.

ie., $\bar{A} = \{x \in U / x \notin A\}$.



\bar{A} (Shaded)

Example:-

Let $U = \{ 1,2,3,4,5,6,7,8 \}$ and $A = \{1,3,5\}$ then $\bar{A} = \{2,4,6,7,8 \}$

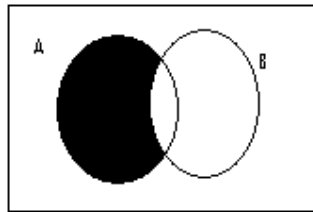
Definition:-

Let A and B are two sets the difference of A and B, denoted by $A - B$, is the set consisting of those element in A which are not in B.

ie., $A - B = \{ x \mid x \in A \text{ and } x \notin B \}$.

The **symmetric difference** of two sets A and B, denoted by $A \oplus B$ is the set of those elements which belong to A or B but not to both A and B.

ie., $A \oplus B = \{ x \mid x \in A - B \text{ or } x \in B - A \}$.



$A - B$



$A \oplus B$

Example:-

Let $A = \{a, e, i, o, u\}$, $B = \{a, b, c, d, e\}$

then $A - B = \{i, o, u\}$, $B - A = \{b, c, d\}$

Symmetric difference

Let A and B be two sets then symmetric difference of A and B denoted by $A \oplus B$ is the set consisting of those elements which belong to A or B but not to both A and B.

ie $A \oplus B = \{x \mid x \in A - B \text{ or } x \in B - A \}$



$A \oplus B$

Example:-

Let $A = \{1,2,3,5,9\}$ $B = \{2,7,11\}$ then

$A - B = \{1,3,5,9\}$ and $B - A = \{7,11\}$

Remark:-

If $A \subset B$ then $A - B = \emptyset$ and $A \oplus B = B - A$

if $A \cap B = \emptyset$ then $A - B = A$, $B - A = B$ and $A \oplus B = A \cup B$

Set identities

Identity	Name
$A \cup \emptyset = A$ $A \cap U = A$	Identity laws
$A \cup U = A$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{\overline{A}} = A$	Complementation laws
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cap C) = (A \cup B) \cap C$ $A \cap (B \cup C) = (A \cap B) \cup C$	Associative laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive laws
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption law Absorption law
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Compliment laws

These identities can be proved by 3 methods

Example:-

1. Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Solution.

Method 1.

Let $x \in \overline{A \cup B}$ then $x \notin A \cup B$ (definition of compliment)
 $\Rightarrow \neg [x \in A \cup B]$ (definition of negation)
 $\Rightarrow \neg [x \in A \vee x \in B]$ (definition of union)
 $\Rightarrow \neg [x \in A] \wedge \neg [x \in B]$ (De Morgan's law of logic)
 $\Rightarrow [x \notin A] \wedge [x \notin B]$ (definition of negation)
 $\Rightarrow x \in \overline{A} \wedge x \in \overline{B}$ (definition of compliment)
 $\Rightarrow x \in \overline{A} \cap \overline{B}$ (definition of intersection)

$$\therefore \overline{A \cup B} \subseteq \overline{A} \cap \overline{B} \dots\dots\dots(1)$$

Let $x \in \overline{A} \cap \overline{B}$ then $x \in \overline{A} \wedge x \in \overline{B}$ (definition of intersection)
 $\Rightarrow [x \notin A] \wedge [x \notin B]$ (definition of compliment)
 $\Rightarrow \neg[x \in A] \wedge \neg[x \in B]$ (definition of negation)
 $\Rightarrow \neg[x \in A \vee x \in B]$ (De Morgan's law of logic)
 $\Rightarrow \neg[x \in A \cup B]$ (definition of union)
 $\Rightarrow x \notin A \cup B$ (definition of negation)
 $\Rightarrow x \in \overline{A \cup B}$ (definition of compliment)

$$\therefore \overline{A} \cap \overline{B} \subseteq \overline{A \cup B} \dots\dots\dots(2)$$

From (1)and (2) $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Method 2.

$\overline{A \cup B} = \{x | x \notin A \cup B\}$ (definition of compliment)
 $= \{x | \neg[x \in A \cup B]\}$ (definition of negation)
 $= \{x | \neg[x \in A \vee x \in B]\}$ (definition of union)
 $= \{x | \neg[x \in A] \wedge \neg[x \in B]\}$ (De Morgan's law of logic)
 $= \{x | [x \notin A] \wedge [x \notin B]\}$ (definition of negation)
 $= \{x | x \in \overline{A} \wedge x \in \overline{B}\}$ (definition of compliment)
 $= \{x | x \in \overline{A} \cap \overline{B}\}$ (definition of intersection)
 $= \overline{A} \cap \overline{B}$

Method 3.

Let us draw the membership table for the above identity as follows:

A	B	$A \cup B$	$\overline{A \cup B}$	\overline{A}	\overline{B}	$\overline{A} \cap \overline{B}$
1	1	1	0	0	0	0
1	0	1	0	0	1	0
0	1	1	0	1	0	0
0	0	0	1	1	1	1

In the above membership table, since the column headed by $\overline{A \cup B}$ is identical to the column headed by $\overline{A} \cap \overline{B}$, $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

2. Prove that $A \cup (B \cup C) = (A \cup B) \cup C$

Solution.

Method 1.

Let $x \in A \cup (B \cup C)$ then $x \in A \vee x \in B \cup C$ (definition of union)
 $\Rightarrow x \in A \vee [x \in B \vee x \in C]$ (definition of union)
 $\Rightarrow [x \in A \vee x \in B] \vee x \in C$ (associative law of logic)
 $\Rightarrow x \in A \cup B \vee x \in C$ (definition of union)
 $\Rightarrow x \in (A \cup B) \cup C$ (definition of union)

$\therefore A \cup (B \cup C) \subseteq (A \cup B) \cup C \dots\dots\dots(1)$

Let $x \in (A \cup B) \cup C$ then $x \in A \cup B \vee x \in C$ (definition of union)
 $\Rightarrow [x \in A \vee x \in B] \vee x \in C$ (definition of union)
 $\Rightarrow x \in A \vee [x \in B \vee x \in C]$ (associative law of logic)
 $\Rightarrow x \in A \vee x \in B \cup C$ (definition of union)
 $\Rightarrow x \in A \cup (B \cup C)$ (definition of union)

$\therefore (A \cup B) \cup C \subseteq A \cup (B \cup C) \dots\dots\dots(2)$

From (1) and (2),

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

Method 2.

$A \cup (B \cup C) = \{x \mid x \in A \vee x \in B \cup C\}$ by definition of union
 $= \{x \mid x \in A \vee [x \in B \vee x \in C]\}$ by definition of union
 $= \{x \mid [x \in A \vee x \in B] \vee x \in C\}$ by associative law of logic
 $= \{x \mid x \in A \cup B \vee x \in C\}$ by definition of union
 $= \{x \mid x \in (A \cup B) \cup C\}$ by definition of union
 $= (A \cup B) \cup C$

Method 3.

Let us draw the membership table for the above identity as follows:

A	B	C	$A \cup B$	$B \cup C$	$A \cup (B \cup C)$	$(A \cup B) \cup C$
1	1	1	1	1	1	1
1	1	0	1	1	1	1
1	0	1	1	1	1	1
1	0	0	1	0	1	1
0	1	1	1	1	1	1
0	1	0	1	1	1	1
0	0	1	0	1	1	1
0	0	0	0	0	0	0

In the above membership table, since the column headed by $A \cup (B \cup C)$ is identical to the column headed by $(A \cup B) \cup C$, we have $A \cup (B \cup C) = (A \cup B) \cup C$.

3. For any two sets A and B, prove that $A - B = A \cap \bar{B}$.

Using the result and set identities, prove that $(A - B) - C = A - (B \cup C)$

Solution:-

$$\begin{aligned}
 A - B &= \{x \mid x \in A \wedge x \notin B\} && \text{(definition of difference)} \\
 &= \{x \mid x \in A \wedge x \in \bar{B}\} && \text{(definition of compliment)} \\
 &= \{x \mid x \in A \cap \bar{B}\} && \text{(definition of intersection)} \\
 &= A \cap \bar{B}.
 \end{aligned}$$

$$\begin{aligned}
 (A - B) - C &= (A - B) \cap \bar{C} && \text{(using } A - B = A \cap \bar{B} \text{)} \\
 &= (A \cap \bar{B}) \cap \bar{C} && \text{(using } A - B = A \cap \bar{B} \text{)} \\
 &= A \cap (\bar{B} \cap \bar{C}) && \text{(associative law of intersection)} \\
 &= A \cap \overline{(B \cup C)} && \text{(De-Morgan's law)} \\
 &= A - (B \cup C). && \text{(using } A - B = A \cap \bar{B} \text{)}
 \end{aligned}$$

4. For any three sets A, B and C, prove that $\overline{A \cup (B \cap C)} = (\bar{C} \cup \bar{B}) \cap \bar{A}$.

Solution:-

$$\begin{aligned}
 \overline{A \cup (B \cap C)} &= \bar{A} \cap \overline{(B \cap C)} && \text{(using De Morgan's law)} \\
 &= \bar{A} \cap (\bar{B} \cup \bar{C}) && \text{(using De Morgan's law)} \\
 &= (\bar{B} \cup \bar{C}) \cap \bar{A} && \text{(commutative law of intersection)} \\
 &= (\bar{C} \cup \bar{B}) \cap \bar{A} && \text{(commutative law for union)}
 \end{aligned}$$

5. For any three sets A, B and C, prove that

$$(A - B) - C = (A - C) - (B - C).$$

Solution:-

$$\begin{aligned}
 (A - B) - C &= (A - B) \cap \bar{C} && \text{(using } A - B = A \cap \bar{B} \text{)} \\
 &= (A \cap \bar{B}) \cap \bar{C} && \text{(using } A - B = A \cap \bar{B} \text{)} \\
 &= A \cap (\bar{B} \cap \bar{C}) && \text{(associative law)} \\
 &= A \cap [(\bar{B} \cap \bar{C}) \cup \emptyset] && \text{(identity law)} \\
 &= A \cap [(\bar{B} \cap \bar{C}) \cup (C \cap \bar{C})] && \text{(compliment law)} \\
 &= A \cap [(\bar{C} \cap \bar{B}) \cup (\bar{C} \cap C)] && \text{(commutative law)}
 \end{aligned}$$

$$\begin{aligned}
 &= A \cap [\bar{C} \cap (\bar{B} \cup C)] && \text{(distributive law)} \\
 &= (A \cap \bar{C}) \cap (\bar{B} \cup C) && \text{(associative law)} \\
 &= (A \cap \bar{C}) \cap (\bar{B} \cup \bar{\bar{C}}) && \text{(complementation law)} \\
 &= (A \cap \bar{C}) \cap (\overline{B \cap C}) && \text{(De Morgan's law)} \\
 &= (A - C) \cap \overline{B - C} && \text{(using } A - B = A \cap \bar{B} \text{)} \\
 &= (A - C) - (B - C). && \text{(using } A - B = A \cap \bar{B} \text{)}.
 \end{aligned}$$

GENERALISED UNION AND INTERSECTION

Definition(Intersection):-

If $A_1, A_2 \dots A_n$ are n sets then their intersection is denoted and defined as,

$$\bigcap_{i=1}^n A_i = \{x|x \in A_i \text{ for all } i=1,2,\dots,n\}$$

Similarly, if $A_1, A_2 \dots A_n, \dots$ are infinite collection of sets then their intersection denoted and defined by

$$\bigcap_{i=1}^{\infty} A_i = \{x|x \in A_j \text{ for all } j=1,2,\dots\}$$

Definition(Union):-

If $A_1, A_2 \dots A_n$ are n sets then their union is denoted and defined as,

$$\bigcup_{i=1}^n A_i = \{x|x \in A_i \text{ for some } i=1,2,\dots,n\}$$

Similarly, if $A_1, A_2 \dots A_n, \dots$ are infinite collection of sets then their union is denoted and defined by

$$\bigcup_{i=1}^{\infty} A_i = \{x|x \in A_j \text{ for all } j=1,2,\dots\}$$

Example:-

- Let $A_i = \{1,2,3,\dots,i\}$ for $i=1,2,3,\dots$

Then
$$\begin{aligned}
 \bigcup_{i=1}^{\infty} A_i &= \{1\} \cup \{1,2\} \cup \{1,2,3\} \cup \dots \\
 &= \{1,2,3,\dots\}
 \end{aligned}$$

and
$$\begin{aligned}
 \bigcap_{i=1}^{\infty} A_i &= \{1\} \cap \{1,2\} \cap \{1,2,3\} \cap \dots \\
 &= \{1\}
 \end{aligned}$$

2. Let $A_i = \{i, i + 1, i + 2, \dots\}$

$$\bigcup_{i=1}^n A_i = \bigcup_{i=1}^n \{i, i + 1, i + 2, \dots\}$$

$$= \{1, 2, 3, \dots\} \cup \{2, 3, 4, \dots\} \cup \dots \cup \{n, n + 1, n + 2, \dots\}$$

$$= \{1, 2, 3, \dots\},$$

and $\bigcap_{i=1}^{\infty} A_i = \bigcap_{i=1}^n \{i, i + 1, i + 2, \dots\}$

$$= \{1, 2, 3, \dots\} \cap \{2, 3, 4, \dots\} \cap \dots \cap \{n, n + 1, n + 2, \dots\}$$

$$= \{n, n + 1, n + 2, \dots\}$$

Computer representation of sets

Assume that the universal set U is finite set. First specify an arbitrary ordering of the elements of U , for instance represent a subset A of U with bit string of length n , where the i^{th} bit in this string is 1 if $a_i \in A$ and is zero if $a_i \notin A$.

To find the bit string for the compliment of a set from the bit string for that set, we simply change each 1 to a 0 and each 0 to a 1.

The bit in the i^{th} position of the bit string for the union of two sets is 1 if either or both of the bits in the i^{th} position of the two strings, representing the sets, are 1 and is 0 when both bits are 0. Hence the bit string for the union is the bitwise OR of the bit strings for the two sets.

The bit in the i^{th} position of the bit string for the intersection of two sets is 1 if both of the bits in the i^{th} position of the two string, representing the sets, are 1 and is 0 when either or both of the bits are zero. Hence the bit string for the intersection is the bitwise AND of the bit strings for the two sets.

Similarly the bit string for the symmetric difference of two sets is the bitwise XOR of the bit strings for the two sets.

Q. suppose the universal set is $U = \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$ express the subsets with bit strings. Also find the set specified by the bit string 11 1100 1111.

Ans:- Let us give an ordering to the universal set U by taking $a_i = \forall i = 1, 2, \dots, 10$ then the bit string representing any subset of U is of length 10 and the bit in the i^{th} position is 1 if $a_i = i$ is an element of the subset and otherwise is 0 hence the bit string representing the set $\{2, 3, 6, 7, 9\}$ is of length 10 and has 1 in the 2nd, 3rd, 6th, 7th and 9th positions and 0 elsewhere the bit string representing the given subset is 01 1001 1010.

In the given bit string bits in the 5th and 6th position is 0 and 1 elsewhere. Hence the subsets specified by this string contain every element of the universal set except $a_5 = 5$ and $a_6 = 6$. hence required subset is $\{1, 2, 3, 4, 7, 8, 9, 10\}$

Q. suppose the universal set is $U = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$, $A = \{4, 6, 10, 12, 18\}$ and

$B = \{4, 8, 12, 16, 20\}$ find the bit strings representing \bar{A} , $A \cup B$ and $A \cap B$

Ans:- Let us give an ordering to U by taking $a_i = 2i$ for all $i = 1, 2, \dots, 10$. then the bit string representing any subset of U is of length 10 and the bit in the i^{th} position is 1 if $a_i = 2i$ is an element of the subset and otherwise is 0.

Hence the bit string representing the sets A is 10 1011 0010

Hence the bit string representing the sets B is 01 0101 0101

Hence the bit string representing \bar{A} is 10 0100 1101.

Bit string representing $A \cup B$ and $A \cap B$ are respectively given by

$01\ 1011\ 0010 \vee 01\ 0101\ 0101 = 01\ 1111\ 0111$ and

$01\ 1011\ 0010 \wedge 01\ 0101\ 0101 = 01\ 0001\ 0000$.

Relations:

Definition:-

An ordered pair consists of 2 elements x and y where x is designated as the first element and y as the second element.

i.e., $(x, y) = (a, b)$ if and only if $x = a$ and $y = b$

Definition:-

Let A and B be two sets, then the Cartesian product or product set of A and B is denoted and defined by,

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

Cartesian product of n sets A_1, A_2, \dots, A_n is denoted and defined by,

$$A_1 \times A_2 \times \dots \times A_n = \{ (a_1, a_2, \dots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n \}$$

Note:-

We write $A \times A \times A \times \dots \times A$ (n factors) as A^n .

Example:-

1. Let $A = \{2, 4\}$ and $B = \{1, 3, 5\}$

Then $A \times B = \{(2, 1), (2, 3), (2, 5), (4, 1), (4, 3), (4, 5)\}$

and $B \times A = \{(1, 2), (1, 4), (3, 2), (3, 4), (5, 2), (5, 4)\}$

Clearly $A \times B \neq B \times A$.

2. Let $A = \{0, 1\}$, $B = \{2, 3\}$ and $C = \{4, 5\}$. then,

$$A \times B \times C = \{(0, 2, 4), (0, 2, 5), (0, 3, 4), (0, 3, 5), (1, 2, 4), (1, 2, 5), (1, 3, 4), (1, 3, 5)\}.$$

Note:-

$A \times B$ need not be equal to $B \times A$.

But If $n(T)$ denote number of elements in any set T.

Then $n(A \times B) = n(B \times A)$.

Q. Prove that $(A \times B) \cap (A \times C) = A \times (B \cap C)$.

$$\begin{aligned} \text{We have, } (A \times B) \cap (A \times C) &= \{(x, y) / (x, y) \in A \times B \text{ and } (x, y) \in A \times C\} \\ &= \{(x, y) / x \in A, y \in B \text{ and } x \in A, y \in C\} \\ &= \{(x, y) / (x \in A \text{ and } y \in B \cap C)\} \\ &= A \times (B \cap C) \end{aligned}$$

Definition:-

Let A and B be two sets, A binary relation or simply a relation from A to B is a subset of $A \times B$.

If a is related to b by the Relation R then we write aRb or $(a,b) \in R$

Domain of a relation R from A to B is the set $\{a | (a,b) \in R\}$

The set $\{b | (a,b) \in R\}$ is called the range of R

If R is a relation from A to A we say that R is a relation on A

Example:-

1. Let $A = \{2,3,4\}$ and $B = \{3,4,5,6\}$

Let R be the relation aRb if a is a factor of b

Then $R = \{(2,4), (2,6), (3,3), (3,6), (4,4)\}$

Here Domain of R is $\{2,3,4\}$ and Range of R is $\{3,4,6\}$

2. Let $A = B = \mathbb{N}$, the set of all natural numbers

Let $R = \{(x,y) / y=2x\}$

Then $R \subseteq \mathbb{N} \times \mathbb{N}$ so R is a relational.

Domain of R is \mathbb{N} and Range of R is positive even numbers

Note:-

For any set A the relation $A \times A$ and Φ are called universal relation and empty relation respectively.

Definition:-

Let R be a relation from a set A to a set B. Then the inverse of R denoted by R^{-1} is,

$$R^{-1} = \{(b, a) | (a, b) \in R\}$$

Example:-

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

And Let $R = \{(2,4), (2,6), (3,3), (3,6), (4,4)\}$ Then

$R^{-1} = \{(4,2), (6,2), (3,3), (6,3), (4,4)\}$

Note:-

If R is a relation then R^{-1} is also a relation and $(R^{-1})^{-1} = R$.

Graph of a Relation

Let S be a relation on \mathbb{R} , set of real numbers then $S \subset \mathbb{R}^2$. the pictorial representation of S is called graph of S

Example: 1

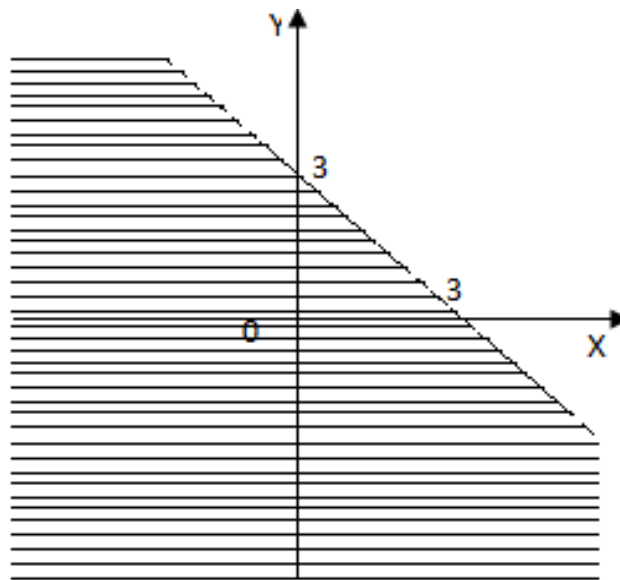
Consider $S = \{(x,y) | y < 3-x\}$

Draw the line $y = 3 - x$. it divide the plane in to 2 regions. One region contains the graph of S .

$(0, 0) \in S$. ($\because 0 < 3 - 0$)

\therefore Graph of S is region containing $(0, 0)$.

Note that Points on the line are not in the graph.



GRAPH OF $S = \{(x, y) : y < 3 - x\}$

Example: 2

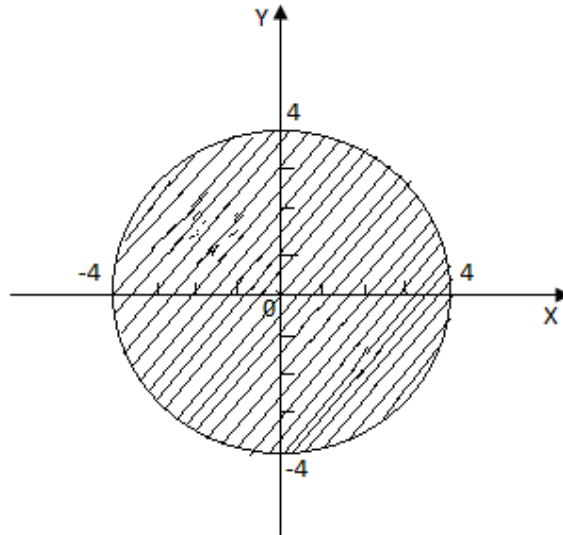
Consider $S = \{(x,y) | x^2 + y^2 \leq 16\}$

Plot the circle $x^2 + y^2 = 16$, which is a circle with centre origin & radius 4.

The circle divide the plane in to 2 regions.

$\because 0^2 + 0^2 < 16$, $(0,0) \in S$.

\therefore the interior of the circle together with circle is the graph of S

GRAPH OF $S = \{(x, y) : x^2 + y^2 \leq 16\}$

Representation of Relation on Finite sets

Suppose A and B are finite sets and R be a relation on A to B then R being a subset of the finite set $A \times B$, is a finite set. The following are the two ways of picturing the relation R from A to B .

1.Relation matrix:-

Let $A = \{a_1, a_2, a_3, \dots, a_m\}$ and $B = \{b_1, b_2, b_3, \dots, b_n\}$ and R be a relation from A to B . The relation matrix on R can be obtained by first constructing a table whose columns are preceded by a column consisting of successive elements of A and whose rows are headed by a row consisting of successive elements of B . For any $1 \leq i \leq m$ and $1 \leq j \leq n$, if $a_i R b_j$, then we enter 1 in the i th row and j th column. The matrix representing the relation R can be written down from the table. It is an $m \times n$ matrix with all its entries 0 or 1

Example:-

Let $A = \{1, 2, 3, 4\}$ and $B = \{x, y, z\}$. Let R be the following relation from A to B .

$$R = \{(1, y), (1, z), (2, x), (3, y), (4, x), (4, z)\}.$$

The relation matrix M_R of R is given below:

	x	y	z
1	0	1	1
2	1	0	0
3	0	1	0
4	1	0	1

$$\therefore M_R = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

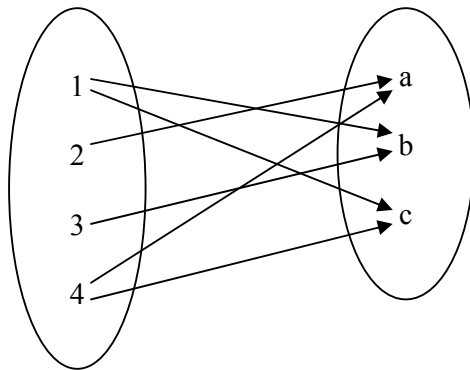
2. Arrow Diagram;-

Write down the elements of a A and the elements of B in two disjoint disks and then draw an arrow from $a \in A$ to $b \in B$ whenever a is related to b. this picture is called the arrow diagram of the relation.

Example:-

Let $A = \{1,2,3,4\}$, $B = \{a,b,c\}$.

and Let $R = \{(1, b),(1, c),(2, a),(3, b),(4, a),(4, c)\}$



ARROW DIAGRAM REPRESENTING R

Composition of Relations :-

Let A, B, C be sets and R the a relation from A to B and Let S be a relation from B toC.

Then the composition of R and S Denoted by $R \circ S$ is ,

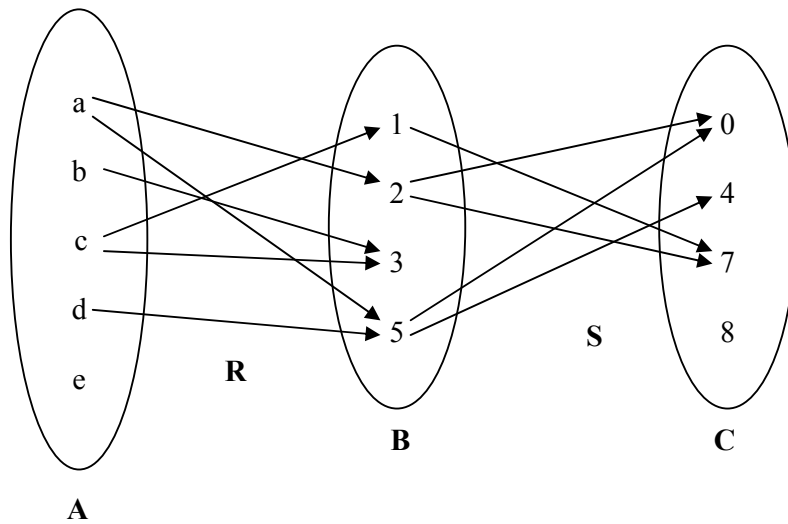
$$R \circ S = \{(a,c) \mid \exists b \in B \text{ for which } (a, b) \in R \text{ and } (b, c) \in S\}.$$

Example:-

Let $A = \{a,b,c,d,e\}$, $B = \{1,2,3,5\}$ & $C = \{0,4,7,8\}$

Let $R = \{(a,2),(a,5),(b,3),(c,1),(c,3),(d,5)\}$ And $S = \{(1,7),(2,0),(2,7),(5,0),(5,4)\}$

Then $R \circ S = \{(a,0),(a,4),(a,7),(c,7),(d,0),(d,4)\}$.



ARROW DIAGRAM REPRESENTING $R \circ S$

$R \circ S$ Using Matrices :-

Let M_R, M_S and $M_{R \circ S}$ denote respectively the matrices of the relation R, S and $R \circ S$ given above. Then

$$M_R = \begin{matrix} & \begin{matrix} 1 & 2 & 3 & 5 \end{matrix} \\ \begin{matrix} a \\ b \\ c \\ d \\ e \end{matrix} & \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix}$$

$$M_S = \begin{matrix} & \begin{matrix} 0 & 4 & 7 & 8 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \end{matrix} & \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \end{matrix}$$

$$\text{Then } M_{R \circ S} = \begin{matrix} & \begin{matrix} 0 & 4 & 7 & 8 \end{matrix} \\ \begin{matrix} a \\ b \\ c \\ d \\ e \end{matrix} & \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix}$$

Multiplying M_R and M_S we obtain

$$M_R M_S = \begin{matrix} & \begin{matrix} 0 & 4 & 7 & 8 \end{matrix} \\ \begin{matrix} a \\ b \\ c \\ d \\ e \end{matrix} & \begin{bmatrix} 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix}$$

Comparing $M_R M_S$ and $M_{R \circ S}$ we can see that both $M_R M_S$ and $M_{R \circ S}$ have the same zero entries. The nonzero entries of $M_R M_S$ tell us which elements are related by $R \circ S$.

Theorem. Let A, B, C, D be sets. Suppose R is a relation from A to B , S is a relation from B to C and T is a relation from C to D . Then

$$(R \circ S) \circ T = R \circ (S \circ T). \quad [\text{Associative law}]$$

Proof.

Given R is a relation from A to B , S is a relation from B to C and T is a relation from C to D .

Then $R \circ S$ is a relation from A to C and hence $(R \circ S) \circ T$ is a relation from A to D .

Also $S \circ T$ is a relation from B to D and hence $R \circ (S \circ T)$ is a relation from A to D .

Thus both $(R \circ S) \circ T$ and $R \circ (S \circ T)$ are relations from A to D .

From the definition of the composition of the relation, we have $(a, d) \in (R \circ S) \circ T$

$$\Rightarrow \exists c \in C, \text{ such that } (a, c) \in R \circ S \text{ and } (c, d) \in T$$

$$\Rightarrow \exists c \in C \text{ and } b \in B, \text{ such that } (a, b) \in R, (b, c) \in S \text{ and } (c, d) \in T$$

$$\Rightarrow \exists b \in B, \text{ such that } (a, b) \in R \text{ and } (b, d) \in S \circ T$$

$$[\text{Since } bSc, cTd \Rightarrow b(S \circ T)d]$$

$$\Rightarrow (a, d) \in R \circ (S \circ T).$$

$$\therefore (R \circ S) \circ T \subseteq R \circ (S \circ T). \dots\dots(1)$$

Similarly, we can prove that

$$(a, d) \in R \circ (S \circ T) \Rightarrow (a, d) \in (R \circ S) \circ T.$$

$$\therefore R \circ (S \circ T) \subseteq (R \circ S) \circ T. \dots\dots(2)$$

From(1) and (2), we get $(R \circ S) \circ T = R \circ (S \circ T)$

Types of Relations:-

1. Reflexive Relation

A relation R on a set A is Reflective if every elements of A is related to itself.

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

Ex: i). Consider \mathbb{N} , set of all natural numbers.

The relation \leq defined on \mathbb{N} is a reflexive relation, but The relation $<$ defined on \mathbb{N} is not reflexive

2. Symmetric Relation

A relation R in a set A is symmetric if whenever a related to b , then b related to a ie., R is symmetric if $(a, b) \in R \Rightarrow (b, a) \in R$

Ex:-Let the relation R on, set \mathbb{R} of all real numbers defined by aRb if $a+b > 0$

if aRb then $a + b > 0$

$$\Rightarrow b + a > 0$$

$$\therefore bRa$$

$\therefore R$ is a symmetric relation

Antisymmetric Relation

A relation R on a set A is anti symmetric if whenever aRb and bRa then $a=b$.

Ex:- consider \mathbb{Z} , set of all integers .

Let R be the relation \leq defined on \mathbb{Z} .

If $a \leq b$ and $b \leq a$ then $a = b$.

$\therefore R$ is anti symmetric.

Note:

The property of being symmetric and antisymmetric are not negations of each other .

Consider $R = \{(1,1), (2,2), (3,3)\}$ it is both symmetric and antisymmetric.

$R = \{(1,3), (3,1), (2,3)\}$ is neither symmetric nor antisymmetric.

4. Transitive relation

A relation R on a set A is transitive if whenever a is related to b and b is related to c then a related to c .

i.e., aRb and $bRc \implies aRc$

Ex: Consider \leq on \mathbb{Z}

If $a \leq b$ and $b \leq c$ then $a \leq c$

$\therefore \leq$ is a transitive relation

Example:-

Consider $A = \{1, 2, 3, 4\}$ and relations on A

$R_1 = \{(1,1), (1,2), (2,3), (1,3), (4,4)\}$

$R_2 = \{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4)\}$

$R_3 = \{(1,3), (2,1)\}$

$R_4 = \emptyset$, the empty relation

$R_5 = A \times A$, the universal relation

Here R_1 is not reflexive (since $(2, 2) \notin R_1$)

Here R_1 is not symmetric (since $(1, 2) \in R_1$ but $(2, 1) \notin R_1$)

R_1 is antisymmetric and transitive.

R_2 is reflexive, symmetric and transitive but not antisymmetric

(Since $(1, 2) \in R_2$ and $(2, 1) \in R_2$ but $1 \neq 2$)

R_3 is not reflexive, not symmetric and not transitive but R_3 is antisymmetric,

because we cannot find $a, b \in A$ such that $(a, b) \in R_3$ and $(b, a) \in R_3$

R_4 is symmetric, antisymmetric, and transitive but not reflexive

R_5 is reflexive, symmetric and transitive but not antisymmetric

because $(1, 2) \in R_5$ and $(2, 1) \in R_5$ but $1 \neq 2$

Q. prove that a relation R is transitive iff $R^n \subseteq R \forall n \geq 1$

Proof:-

Let R be a relation on a set A .

suppose R is transitive

(To prove that $R^n \subseteq R \forall n \geq 1$)

We use method of induction

Since $R \subseteq R$, it is true for $n = 1$

Suppose the result is true for $n = m$

That is $R^m \subseteq R$

Let $(a, c) \in R^{m+1}$

$\because R^{m+1} = R^m \circ R$, by definition of composition of relation, $\exists b \in A$ such that

$(a, b) \in R^m$ and $(b, c) \in R$

$\Rightarrow \exists b \in A$ $(a, b) \in R$ and $(b, c) \in R$

($\because (a, b) \in R^m \subseteq R$)

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

($\because R$ is transitive)

$\Rightarrow R^{m+1} \subseteq R$

\therefore the result is true for $n = m+1$

\therefore by mathematical induction $R^n \subseteq R \forall n \geq 1$

Conversely suppose $R^n \subseteq R \forall n \geq 1$

(T.P.T R is transitive)

Let $a, b, c \in A$ and $(a, b), (b, c) \in R$

Then $(a, c) \in R \circ R = R^2 \subseteq R$ (by assumption)

$\therefore (a, c) \in R$

$\therefore R$ is transitive

Hence the proof.

Definition:-

Let S be a non empty set. A partition of S is a collection $p = \{A_i\}$ of non empty subsets of S such that

i) each $a \in S$ belongs to one of the A_i

ii) the sets $\{A_i\}$ are mutually disjoint, i.e., if $A_i \neq A_j$, then $A_i \cap A_j = \emptyset$.

The subsets in a partition are called cells.

Given a partition $P = \{A_i\}$ of a set S , any element $b \in A_i$ is called a representative of the cell A_i and a subset B of S , consisting of exactly one element from each of the cells of P is called **system of representatives**.

Example.

Let $S = \{1,2,3,\dots,8,9\}$.

Consider the following collection of subsets of S :

$$P_1 = \{\{1,3,5\}, \{2,6\}, \{4,8,9\}\}$$

$$P_2 = \{\{1,3,5\}, \{2,4,6,8\}, \{5,7,9\}\}$$

$$P_3 = \{\{1,3,5\}, \{2,4,6,8\}, \{7,9\}\}.$$

Among these collection of subsets ,only P_3 is a partition of S .

P_1 is not a partition of S ($\because 7 \in S$ does not belong to any of the subsets in P_1).

P_2 is not a partition of S ($\because \{1,3,5\}$ and $\{5,7,9\}$ are not disjoint).

$\{1,3,5\}$, $\{2,4,6,8\}$ and $\{7,9\}$ are the cells of the partition P_3 .

$B = \{1,2,7\}$ is a system of representatives of the partition P_3 .

Definition:-

Consider a nonempty set S . A relation R on S is an **equivalence relation** if R is reflexive, symmetric and transitive.

- i.e.,
- (i) For every $a \in S$, aRa . (reflexivity)
 - (ii) For every $a, b \in S$,if aRb ,then bRa . (symmetry)
 - (iii) For every $a, b, c \in S$,if aRb and bRc ,then aRc . (transitivity)

Examples

1. Let S be any nonempty set. Consider the relation '=' of equality on S . Obviously, this relation satisfies the following properties:

- (i) $\because a = a$ for every $a \in S$, = is reflexive
- (ii) if $a=b$, then $b = a$. $\therefore =$ is symmetric
- (iii) if $a = b$ and $b = c$, then $a = c$. $\therefore =$ is transitive

Hence '=' is an equivalence relation on S .

2. Consider the set \mathbb{Z} , of all integers .Let us define a relation R on \mathbb{Z} as aRb if and only if $a - b$ is an even integer.

- (i) For any $a \in \mathbb{Z}$, $a - a = 0$, an even number.

Hence aRa ,for all $a \in \mathbb{Z}$

$\therefore R$ is reflexive.

- (ii) For any $a, b \in \mathbb{Z}$, we have

$$aRb \Rightarrow a - b \text{ is an even integer}$$

$$\Rightarrow -(b - a) \text{ is an even integer}$$

$$\Rightarrow b - a \text{ is an even integer}$$

$$\Rightarrow bRa.$$

$\therefore R$ is symmetric.

(iii) For any $a, b, c \in \mathbb{Z}$, we have

aRb and $bRc \Rightarrow a - b$ is an even integer and $b - c$ is an even integer

$\Rightarrow (a - b) + (b - c)$ is an even integer

$\Rightarrow aRc$.

$\therefore R$ is transitive.

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

3. Consider the set \mathbb{Z} , of all integers.

Let m be a fixed positive integer. Two integers $a, b \in \mathbb{Z}$, are said to be 'congruent modulo m ', written as ' $a \equiv b \pmod{m}$ ', if m divides $a - b$.

Then, 'congruent modulo m ' is an equivalence relation on \mathbb{Z}

For,

(i) reflexive:

For any $a \in \mathbb{Z}$, $a - a = 0$ is divisible by m

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

$\therefore \equiv$ is reflexive.

(ii) symmetric

Let $a, b \in \mathbb{Z}$,

And $a \equiv b \pmod{m}$ then $a - b$ is divisible by m

$\Rightarrow a - b = mk$, for some $k \in \mathbb{Z}$

$\Rightarrow b - a = m(-k)$, $-k \in \mathbb{Z}$

$\Rightarrow b \equiv a \pmod{m}$.

$\therefore \equiv$ is symmetric.

(iii) transitive

let $a, b, c \in \mathbb{Z}$

and $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a - b$ and $b - c$ are divisible by m

$\Rightarrow a - b = mk_1$ and $b - c = mk_2$, for some $k_1, k_2 \in \mathbb{Z}$

$\Rightarrow a - b + b - c = m(k_1 + k_2)$

$\Rightarrow a - c = m(k_1 + k_2)$, $k_1 + k_2 \in \mathbb{Z}$

$\Rightarrow a \equiv c \pmod{m}$.

$\therefore \equiv$ is transitive.

Thus the relation 'congruent modulo m ' \equiv is an equivalence relation on \mathbb{Z} .

Equivalence Relation and Partitions

Definition:-

Let R be an equivalence relation on a set S . For each $a \in S$, let $[a]$ denote the set of all elements of S which are related to a under R .

$$\text{i.e., } [a] = \{x \in S : (a, x) \in R\}.$$

This subsets of S is known as the **equivalence class** of a in S under R .

The collection of all such equivalence classes in S under R is known as the **quotient set** of S by R and is denoted by S/R .

$$\text{i.e., } S/R = \{[a] : a \in S\}.$$

Example:-

1. Let R_5 be the relation on the set \mathbb{Z} of integers, defined by $a \equiv b \pmod{5}$ if $a - b$ is divisible by 5.

Then R_5 is an equivalence relation on \mathbb{Z}

For,

R_5 is reflexive

Let $a \in \mathbb{Z}$

Then $a - a = 0$ is divisible by 5.

$$\therefore a \equiv a \pmod{5}$$

$\therefore R_5$ is reflexive.

R_5 is symmetric:

Let $a \equiv b \pmod{5}$

Then $a - b$ is divisible by 5.

$$\Rightarrow a - b = 5k, \quad k \in \mathbb{Z}$$

$$\Rightarrow b - a = -5k = 5(-k), \quad -k \in \mathbb{Z}$$

$\Rightarrow b - a$ is divisible by 5.

$$\Rightarrow b \equiv a \pmod{5}$$

$\therefore R_5$ is symmetric.

R_5 is transitive

Let $a \equiv b \pmod{5}$ and $b \equiv c \pmod{5}$

Then $a - b = 5k_1$ and $b - c = 5k_2$, for some $k_1, k_2 \in \mathbb{Z}$

$$\Rightarrow a - b + b - c = 5(k_1 + k_2)$$

$$\Rightarrow a - c = 5P, \quad P = k_1 + k_2 \in \mathbb{Z}$$

$$\Rightarrow a \equiv c \pmod{5}$$

$\therefore R_5$ is transitive.

$\therefore R_5$ is an equivalence relation

The equivalence classes are:

$$[0] = \{\dots, -10, -5, 0, 5, 10, \dots\}$$

$$[1] = \{\dots, -9, -4, 1, 6, 11, \dots\}$$

$$[2] = \{\dots, -8, -3, 2, 7, 12, \dots\}$$

$$[3] = \{\dots, -7, -2, 3, 8, 13, \dots\}$$

$$[4] = \{\dots, -6, -1, 4, 9, 14, \dots\}$$

$$\therefore \mathbb{Z} / R_5 = \{[0], [1], [2], [3], [4]\}.$$

We know that any integer a can be uniquely expressed as $a = 5q+r$, where $q \in \mathbb{Z}$ is the quotient and $0 \leq r < 5$ is the remainder obtained when a is divided by 5.

Then clearly, $a \in [r]$.

$$\therefore \mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4].$$

Also these equivalence classes are disjoint .Hence they form a partition of \mathbb{Z} . This quotient set \mathbb{Z} / R_5 is usually denoted by \mathbb{Z} / R_5 or simply Z_5 .

Theorem 1.

Let R be an equivalence relation on a set S . Then the quotient set S / R is a partition of S . Specifically:

- (i) For each a in S , we have $a \in [a]$.
- (ii) $[a] = [b]$, if and only if $(a, b) \in R$.
- (iii) If $[a] \neq [b]$, then $[a]$ and $[b]$ are disjoint.

Proof.

Since R is an equivalence relation on S , it is reflexive, symmetric and transitive.

(i) Since R is reflexive, for each $a \in S$, $(a, a) \in R$.

Hence, from the definition of equivalence classes of a , it follows that $a \in [a]$, $\forall a \in S$.

(ii) let $a, b \in S$ and let $(a, b) \in R$.

(Then we have to prove that $[a] = [b]$).

Let $x \in [b]$.

Then, by definition of equivalence class of b , $(b, x) \in R$.

By hypothesis, $(a, b) \in R$.

Since R is transitive and $(a, b), (b, x) \in R$ implies $(a, x) \in R$.

$$\therefore x \in [a].$$

$$\therefore [b] \subseteq [a] \text{-----(1)}$$

Let $x \in [a]$.

Then, by definition of equivalence class of $a, (a, x) \in R$.

By hypothesis, $(a, b) \in R$ and hence by symmetry of $R, (b, a) \in R$.

Since R is transitive $(b, a), (a, x) \in R$ implies $(b, x) \in R$.

$$\therefore x \in [b]$$

$$\therefore [a] \subseteq [b] \text{-----(2).}$$

$$\therefore \text{ from (1) and (2) } [a] = [b].$$

Conversely suppose $[a] = [b]$.

$$\text{Then } [a] = [b] \Rightarrow b \in [b] = [a] \Rightarrow (a, b) \in R$$

Hence (ii)

(iii) Let $a, b \in S$ and $[a] \neq [b]$.

(we have to prove that $[a]$ and $[b]$ are disjoint.)

If possible, let $[a]$ and $[b]$ are not disjoint i.e., $[a] \cap [b] \neq \emptyset$

Let $x \in [a] \cap [b]$.

Then $x \in [a]$ and $x \in [b]$

$$\Rightarrow (a, x) \in R \text{ and } (b, x) \in R$$

$$\Rightarrow (a, x) \in R \text{ and } (x, b) \in R \quad \text{[by symmetry of R]}$$

$$\Rightarrow (a, b) \in R \quad \text{[by transitivity of R]}$$

$$\Rightarrow [a] = [b]. \quad \text{[by (ii)]}$$

This is a contradiction. Hence our assumption that $[a]$ and $[b]$ are not disjoint, is wrong.

$$\therefore [a] \text{ and } [b] \text{ are disjoint.}$$

Hence (iii))

From (i), (ii) and (iii) it follows that each $a \in S$ belongs to some element of S / R and elements of S / R are mutually disjoint.

Hence S / R is a partition of S .

Theorem 2.

Suppose $P = \{A_i\}$ is a partition of a set S . Then there is an equivalence relation ' \sim ' on S such that the quotient set S / \sim of equivalence classes is the same as the partition $P = \{A_i\}$.

Proof:

Given $P = \{A_i\}$ is a partition of the set S . For any $a, b \in S$, define $a \sim b$ if a and b belongs to the same cell A_k in P .

Then ' \sim ' is a relation on S and it satisfies the following properties:

(i) Reflexive

Let $a \in S$. Since P is a partition of S , \exists some A_k in P such that $a \in A_k$.

Hence $a \sim a$.

\therefore ' \sim ' is reflexive.

(ii) Symmetric

From the definition of the relation \sim , we get

$a \sim b \implies a, b \in A_k$, for some $A_k \in P \implies b \sim a$.

Hence the relation \sim is symmetric.

(iii) Transitive

Let $a, b, c \in S$ and let $a \sim b$ and $b \sim c$.

Then from the definition of the relation \sim , it follows that $a, b \in A_i$ and $b, c \in A_j$, for some $A_i, A_j \in P$.

Then $b \in A_i \cap A_j$ and hence $A_i \cap A_j \neq \emptyset$

Since P is a partition, $A_i \cap A_j \neq \emptyset$ implies $A_i = A_j$.

Then $a, c \in A_i$ and so $a \sim c$.

Thus $a \sim b$ and $b \sim c$ implies $a \sim c$.

Hence the relation \sim is transitive.

\therefore it is an equivalence relation on S .

Furthermore, for any $a \in S$, since P is a partition of S , $a \in A_k$ for some $A_k \in P$ and so

$[a] = \{x : a \sim x\} = \{x : x \text{ is in the same cell } A_k \text{ as } a\} = A_k$.

Thus the equivalence classes under \sim are the same as the cells in the partition.

$\therefore S / \sim = P$.

Definition:-

Let S be a nonempty set. A relation R on S is called a partial ordering of S or a partial order on S

If R is reflexive, antisymmetric and transitive

A set together with a partial ordering R is called a partially ordered set or poset.

Example:-

1. Let P denote a collection of sets. Set inclusion ' \subseteq ' is a relation defined on P

Reflexive

Since $A \subseteq A$ of any set in P , set inclusion is a reflexive relation on P .

Antisymmetric

For any two sets A and B , $A \subseteq B$ and $B \subseteq A$ implies.

$A = B$.

Hence \subseteq is antisymmetric

Transitive

Let $A, B, C \in P$, $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$

$\therefore \subseteq$ is transitive

$\therefore \subseteq$ is a partial ordering on P

2. Let P be the set of all positive integers consider the relation ' $|$ ' of divisibility on P defined by for any $a, b \in P$ $a|b$ if \exists a $k \in P$ such that $b = ka$.

$\because a = 1 \times a$ for every $a \in P$, $a|a$ for every $a \in P$

$\therefore '|$ ' is reflexive.

Let $a, b \in P$, $a|b$ and $b|a$

Then $b = k_1a$ and $a = k_2b$ for some $k_1, k_2 \in P$

$$\Rightarrow b = k_1a = k_1k_2b$$

$$\Rightarrow k_1k_2 = 1, k_1, k_2 \in P$$

$$\Rightarrow k_1 = 1 \text{ and } k_2 = 1$$

$$\Rightarrow a = b$$

$\therefore '|$ ' is antisymmetric

Let $a, b, c \in P$, $a|b$ and $b|c$:

Then $b = k_1a$ and $c = k_2b$ for some $k_1, k_2 \in P$.

$$\Rightarrow c = k_2b = k_2k_1a.$$

$$\Rightarrow a|c (\because k_1, k_2 \in P \Rightarrow k_1k_2 \in P).$$

$\therefore '|$ ' is transitive.

$\therefore '|$ ' is a partial ordering on \mathbb{N} .

Note:-' $|$ ' is not a partial ordering on \mathbb{Z} , set of all integers.

Since $-3|3$ and $3|-3$ but $3 \neq -3$, ' $|$ ' is not antisymmetric on \mathbb{Z} .

Q. Consider \mathbb{Z} , set of all integers. Define $a \sim b$ if $b = a^r$, for some positive integer r , Show that ' \sim ' is a partial ordering of \mathbb{Z} .

Solution:-

(i) Reflexive:

Since $a = a^1$, we have $a \sim a$, for all a in \mathbb{Z} .

Hence \sim is reflexive.

(ii) Antisymmetric:

Suppose $a \sim b$ and $b \sim a$.

$$a \sim b \implies b = a^r, \text{ for some integer } r$$

$$b \sim a \implies a = b^r, \text{ for some integer } s$$

$$\text{Then } a = (a^r)^s = a^{rs}.$$

Now we have to consider four possibilities:

Case 1. $rs = 1$. Then $r = 1$ and $s = 1$ and so $a = b$.

Case 2. $a = 1$. Then $b = 1^r = 1 = a$.

Case 3. $b = 1$. Then $a = 1^s = 1 = b$.

Case 4. $a = -1$. Then $b = 1$ or $b = -1$. By case 3, $b \neq 1$. Hence $b = -1 = a$.

Thus in all cases $a = b$.

Hence the relation \sim is antisymmetric.

(iii) Transitive:

Suppose $a \sim b$ and $b \sim c$.

$$a \sim b \text{ and } b \sim c \implies b = a^r \text{ and } c = b^s, \text{ for some integers } r \text{ and } s$$

$$\implies c = (a^r)^s = a^{rs}, \text{ for some integers } r \text{ and } s$$

$$\implies a \sim c.$$

Hence the relation \sim is transitive.

$\therefore \sim$ is a partial ordering of \mathbb{Z} .

Definition:-

For any set S , a subset of the product set S^n is called an **n-ary relation** on S . In particular, a subset of S^3 is called a **ternary relation**.

Example:-

The equation $x^2 + y^2 + z^2 = 1$ determines a ternary relation T on the set \mathbb{R} of real numbers.

ie., a triple (x, y, z) is coordinates of a point in \mathbb{R}^3 on the sphere S with radius 1 and center at the origin $0 = (0, 0, 0)$.

MODULE 2

FUNCTIONS

Definitions:-

Let X and Y be any two nonempty sets. A **function** or **mapping** from X to Y is a rule that assigns to each element in X a unique element in Y .

If f denotes these assignments we write

$$f: X \rightarrow Y$$

which reads ' f is a function from X into Y ' or ' f maps X into Y ' .

The set X is called the domain of the function f and Y is called target set or co-domain of f

Further if $x \in X$, then the element y in Y , which is assigned to x is called the image of x under f or the value of f at x and is denoted by $f(x)$, which reads ' f of x '. Here x is called **pre-image** of f

The set consisting precisely of those elements in Y which appear as the image of at least one element in X is called range or image of f .

$$\text{ie., } \text{Im}(f) = \{y \in Y : y = f(x) \text{ for some } x \in X\}$$

We usually denote the domain of f by $\text{Dom}(f)$ and range of f by $\text{Im}(f)$ or $f(X)$.

Note:- $\text{Im}(f) \subseteq Y$.

Let $f: X \rightarrow Y$ and $A \subseteq X$. then,

$$f[A] = \{f(a) / a \in A\} \text{ is called image of } A.$$

if $B \subseteq Y$, then $f^{-1}[B] = \{a \in X : f(a) \in B\}$ is called pre-image of B .

Note:-

If f is a function then we assume, unless other wise stated, that the domain of the function is \mathbb{R} or largest subset of \mathbb{R} for which the formula is well defined and range is \mathbb{R} . Such function are called real valued function.

Examples:-

1. The arrow diagram given below defines a function f from $X = \{x_1, x_2, x_3, x_4\}$

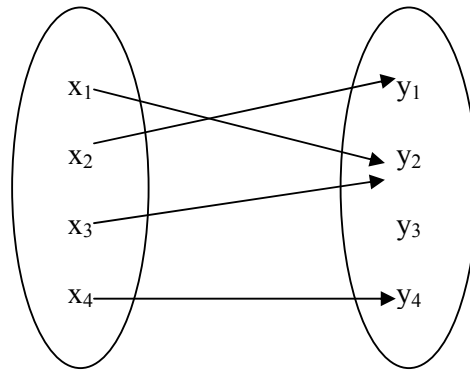
$$\text{and } Y = \{y_1, y_2, y_3, y_4\}.$$

Here X is the domain and Y is the target set.

$$f(x_1) = y_2, \quad f(x_2) = y_1, \quad f(x_3) = y_2, \quad \text{and } f(x_4) = y_4$$

Here $\text{Im}(f) = \{y_1, y_2, y_4\}$,

which is a proper subset of the target set



ARROW DIAGRAM OF f

2. Consider any set A . then the function $I_A : A \rightarrow A$ defined by

$$I_A(a) = a, \forall a \in A \text{ is called the identity function.}$$

3. A function $f : \mathbb{R} \rightarrow \mathbb{R}$ of the form $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, a_i \in \mathbb{R} \quad \forall i = 0, 1, 2, 3, \dots, n$ is called Polynomial function

Definition:-

Let X and Y be two sets and $f : X \rightarrow Y$ be a function, then the set $\{(x, y) \mid x \in X \text{ and } Y = f(x)\}$ is called graph of f .

Note:-

We can also define a function $f : X \rightarrow Y$ is a relation from X to Y , such that each $x \in X$ belongs to a unique ordered pair (x, y) in f .

Q. 1. Find the domain and range of the following real valued functions:

(i) $\sqrt{(2x - 3)(5 - 3x)}$. (ii) $\frac{1}{(2x - 3)(x + 1)}$ (iii) $\left| \frac{x - 1}{x - 1} \right|$

Solution:- (i) Let $y = f(x) = \sqrt{(2x - 3)(5 - 3x)}$.

$f(x)$ is defined for all real values of x for which $(2x - 3)(5 - 3x) \geq 0$.

$$\Rightarrow x \in [3/2, 5/3].$$

Hence, domain of $f = \text{Dom}(f) = [3/2, 5/3]$.

Now, $y = \sqrt{(2x - 3)(5 - 3x)}$ i.e., $y = \sqrt{-6x^2 + 19x - 15}$.

Squaring, $y^2 = -6x^2 + 19x - 15$ i.e., $6x^2 - 19x + y^2 + 15 = 0$.

Since $x \in \mathbb{R}$, the discriminant of the above quadratic in $x \geq 0$

$$\begin{aligned} \therefore (-19)^2 - 24(y^2 + 15) &\geq 0 \Rightarrow 361 - 24y^2 - 360 \geq 0 \\ &\Rightarrow 1 - 24y^2 \geq 0 \Rightarrow y^2 \leq 1/24 \\ &\Rightarrow -1/2\sqrt{6} \leq y \leq 1/2\sqrt{6}. \end{aligned}$$

Taking $y = \sqrt{(2x - 3)(5 - 3x)}$ to be positive, we get

$$\text{Range of } f = \text{Im}(f) = [0, 1/2\sqrt{6}].$$

$$(ii) \text{ Let } y = f(x) = \frac{1}{(2x - 3)(x + 1)}$$

The above function is not defined for values of x for which $(2x - 3)(x + 1) = 0$

$$\text{But } (2x - 3)(x + 1) = 0 \Rightarrow x = 3/2 \text{ or } x = -1.$$

Hence domain of $f = \text{Dom}(f) = \mathbb{R} - \{-1, 3/2\}$.

$$y = \frac{1}{(2x - 3)(x + 1)} \Rightarrow y(2x^2 - x - 3) = 1 \Rightarrow 2yx^2 - yx - 3y - 1 = 0.$$

Since $x \in \mathbb{R}$, the discriminant of the above quadratic in $x \geq 0$

$$\begin{aligned} \therefore (-y)^2 - 4.2y.(-3y - 1) &\geq 0 \Rightarrow 25y^2 + 8y \geq 0 \Rightarrow y(25y + 8) \geq 0 \\ &\Rightarrow y \geq 0 \text{ or } y \leq -8/25 \\ &\Rightarrow y \in [0, \infty) \text{ or } y \in (\infty, -8/25] \end{aligned}$$

But $f(x) \neq 0$, for all $x \in \text{Dom}(f)$.

Hence range of $f = \text{Im}(f) = (-\infty, -8/25] \cup (0, \infty)$.

$$(iii) \text{ Let } y = f(x) = \frac{|x - 1|}{x - 1}$$

Here f is not defined at $x=1$.

$$\therefore \text{Dom}(f) = \mathbb{R} - \{1\}.$$

By the definition of absolute value of a real number, we have

$$|x - 1| = \begin{cases} x - 1, & \text{if } x \geq 1 \\ 1 - x, & \text{if } x < 1 \end{cases}$$

Hence if $x \geq 1$, $f(x) = |x - 1| / x - 1 = x - 1 / x - 1 = 1$,

and if $x < 1$, $f(x) = |x - 1| / x - 1 = 1 - x / x - 1 = -1$.

Hence range of $f = \text{Im}(f) = \{-1, 1\}$.

Examples:-

1. Let $f : \mathbb{R} \rightarrow \mathbb{R} : f(x) = x^2$ and $g : \mathbb{R} \rightarrow \mathbb{R} : g(x) = 2x + 3$.

Then $g \circ f : \mathbb{R} \rightarrow \mathbb{R}$ and $g \circ f(x) = g[f(x)] = g[x^2] = 2x^2 + 3$

and $f \circ g : \mathbb{R} \rightarrow \mathbb{R}$ and $f \circ g(x) = f[g(x)] = f[2x + 3] = (2x + 3)^2$.

Obviously, $g \circ f \neq f \circ g$.

2. Let $f : \mathbb{R} \rightarrow \mathbb{R} : f(x) = x^3$ and $g : \mathbb{R} \rightarrow \mathbb{R} : g(x) = \sin x$.

Then $g \circ f : \mathbb{R} \rightarrow \mathbb{R}$ and $g \circ f(x) = g[f(x)] = g[x^3] = \sin x^3$

and $f \circ g : \mathbb{R} \rightarrow \mathbb{R}$ and $f \circ g(x) = f[g(x)] = f[\sin x] = \sin^3 x$.

Obviously, $g \circ f \neq f \circ g$.

Theorem.(Associativity of composition of function).

Let $f : A \rightarrow B$, $g : B \rightarrow C$ and $h : C \rightarrow D$. Then

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

Proof.

Given $f : A \rightarrow B$, $g : B \rightarrow C$ and $h : C \rightarrow D$. Then by definition of composition of functions, we have

$$g \circ f : A \rightarrow C \text{ and hence } h \circ (g \circ f) : A \rightarrow D$$

$$g \circ f : B \rightarrow D \text{ and hence } (h \circ g) \circ f : A \rightarrow D$$

$$\therefore h \circ (g \circ f) \text{ and } (h \circ g) \circ f \text{ have the same domain and target set.}$$

Let $a \in A$

$$\text{Then } [h \circ (g \circ f)](a) = h[(g \circ f)(a)] = h[g(f(a))]$$

$$\text{And } [(h \circ g) \circ f](a) = (h \circ g)[f(a)] = h[g(f(a))]$$

$$\text{Thus } [h \circ (g \circ f)](a) = [(h \circ g) \circ f](a) \quad \forall a \in A$$

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

BIJECTIVE FUNCTIONS**Definition:-**

Let $f : X \rightarrow Y$ be a function, then f is one-to-one or injective function

if for any $x_1, x_2 \in X$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

f is said to be onto or surjective if $\forall y \in Y$, $\exists x \in X$ such that $f(x) = y$

A function which is both one-to-one and onto is called a bijective function

Example:- Let $g : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $g(x) = x^2$

There for $g(3) = g(-3) = 9$, g is not one-to-one

Let $-5 \in \mathbb{R}$, there does not exist an $x \in \mathbb{R}$. Such that $f(x) = x^2 = -5$

$\therefore f$ not onto

Note:-We can make the above function bijective by restricting the domain and range to $(0, \infty)$.

Theorem:- Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ be two function prove that

i) if f and g are one-to-one then $g \circ f$ is one-to-one

ii) if f and g are one-to then $g \circ f$ is one-to

Proof:-

i) Let $x, y \in X$

Suppose $(g \circ f)x = (g \circ f)y$

Then $g(f(x)) = g(f(y))$

$\Rightarrow f(x) = f(y)$ ($\because g$ is one-to-one)

$\Rightarrow x = y$ ($\because f$ is one-to-one)

$\Rightarrow g \circ f$ is one-to-one

ii) Let $z \in Z$

$\because g$ is onto, $\exists y \in Y$ such that $g(y) = z$

$\because f$ is onto, $\exists x \in X$ such that $f(x) = y$

Then $(g \circ f)(x) = g(f(x)) = g(y) = z$

$\therefore (g \circ f)$ is onto

Note:-

Let $f : \mathbb{R} \rightarrow \mathbb{R}$ then geometrically f one-one iff every horizontal line in \mathbb{R}^2 intersect the graph of f in almost one point

f is onto iff each horizontal line in \mathbb{R}^2 intersect the graph of f at least once.

If it intersect the graph of f in exactly one point, then f is a bijection

Definition:-

Let $f : X \rightarrow Y$ then f is **invertible**, if there exist a function $f^{-1} : Y \rightarrow X$, called inverse of f , such that $f^{-1} \circ f = I_X$ and $f \circ f^{-1} = I_Y$

Where I_X is the identity function on X and I_Y is the identity function on Y .

Theorem:-

A function $f : X \rightarrow Y$ is invertible if and only if f both one-to-one and onto,

i.e., if and only if f is bijective

Proof:-

Consider the function $f : X \rightarrow Y$.

Suppose f is invertible.

Then by definition, \exists a function $f^{-1} : Y \rightarrow X$, such that

$$f^{-1} \circ f = I_X \text{ and } f \circ f^{-1} = I_Y,$$

where I_X is the identity function on X and I_Y is the identity function on Y

For any $x_1, x_2 \in X$, $f(x_1), f(x_2) \in Y$ and

$$f(x_1) = f(x_2) \implies f^{-1}(f(x_1)) = f^{-1}(f(x_2)) \quad [\because f^{-1} \text{ is a function}]$$

$$\implies (f^{-1} \circ f)(x_1) = (f^{-1} \circ f)(x_2)$$

[by the definition of composition of function]

$$\implies I_X(x_1) = I_X(x_2)$$

$$\implies x_1 = x_2$$

$\therefore f$ is one-to-one. .

Let $y \in Y$

Then $f^{-1}(y) \in X$.

Let $x = f^{-1}(y)$. Then $x \in X$ and $f(x) = f(f^{-1}(y))$

$$(f \circ f^{-1})(y)$$

[by the definition of composition of functions]

$$= I_Y(y) = y.$$

Hence f is onto.

$\therefore f$ is one-to-one and onto.

Conversely assume that f is one-one and onto.

(To Prove That f is invertible)

Let $y \in Y$

Then since f is one-to-one and onto, there exist a unique element of x in X , such that

$$f(x) = y.$$

Define $g : Y \rightarrow X$, by $g(y) = x$.

Since f is one-to-one and onto, g is a well defined map from Y to X .

Also for any $x \in X$, $(g \circ f)(x) = g[f(x)] = x$.

Hence $g \circ f = I_X$.

Similarly, for any $y \in Y$, if $y = f(x)$, $x \in X$, then by definition of g , $g(y) = x$ and so

$$(f \circ g)(y) = f[g(y)] = f(x) = y.$$

Hence $f \circ g = I_Y$.

Thus there exist a function $g : Y \rightarrow X$, such that $g \circ f = I_X$ and $f \circ g = I_Y$.

Hence f is invertible and $f^{-1} = g$

Hence the proof.

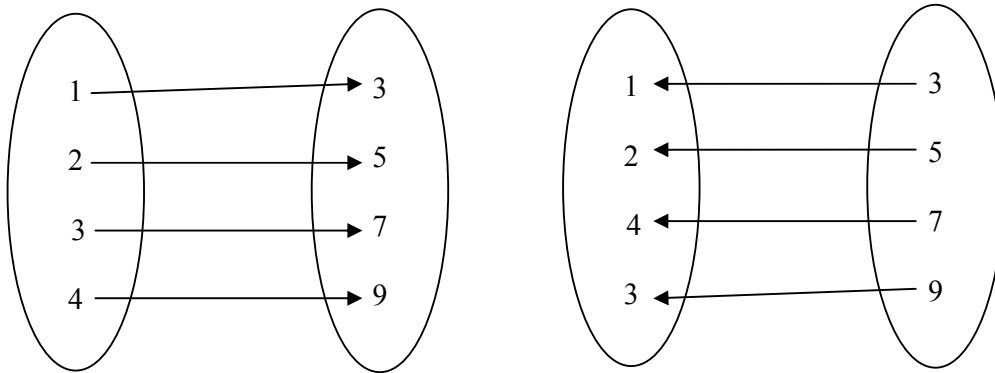
Example:-

1. The function $f : A \rightarrow B$, where $A = \{1,2,3,4\}$ and $B = \{3,5,7,9\}$, defined by

$$f(x) = 2x + 1 \text{ is one-to-one and onto.}$$

Since f is bijective, its inverse $f^{-1} : B \rightarrow A$ exist and is defined by

$$f^{-1}(y) = \frac{|y - 1|}{2}, \forall y \in B. \quad [\because y = f(x) = 2x + 1 \Rightarrow x = \frac{y-1}{2}]$$



2. Consider the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined $f(x) = 2x + 3$

Then f is one-one and onto. $\therefore f$ is invertible

$f^{-1} : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f^{-1}(x) = (x - 3)/2$ is the inverse of f

MATHEMATICAL FUNCTIONS

Definition:-

Let $x \in \mathbb{R}$ then the absolute value of x , written **ABS(x)** or $|x|$, is defined as

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$$

Example:- $|4| = 4, |-4| = 4, |4.5| = 4.5$

Floor and Ceiling Function

The floor x is denoted by $\lfloor x \rfloor$ is the greatest integer less than or equal to x .

Example:- $\lfloor 4 \rfloor = 4$, $\lfloor 4.52 \rfloor = 4$, $\lfloor -4.52 \rfloor = -5$,

The ceiling of x , denoted by $\lceil x \rceil$ least integer greater than or equal to x .

Example:- $\lceil 8 \rceil = 8 = \lceil -8 \rceil$, $\lceil 6.58 \rceil = 7$, $\lceil -6.58 \rceil = -6$

Definition (Integer function):-

The integer function written as $\text{INT}(x)$ associates x to an integer obtained by deleting the fractional part of the number.

Example:- $\text{INT}(5) = 5$ $\text{INT}(4.52) = 4$ $\text{INT}(-4.52) = -4$

Note:-

All the functions defined above are functions: $\mathbb{R} \rightarrow \mathbb{Z}$

Definition:

Let $k \in \mathbb{Z}$, set of all integers and $m \in \mathbb{N}$, set of all natural numbers. then $k(\text{mod } m)$ read as 'k modulo m' is the integer remainder when k is divided by m .

ie., $K(\text{mod } m) = r \in \mathbb{Z}$. such that $k = mq + r$, $q \in \mathbb{Z}$.

Examples:-

a) $28(\text{mod } 6) = 4$,

b) $25(\text{mod } 5) = 0$

c) $-28(\text{mod } 6) = 2$ (since $-28 = 6(-5) + 2$)

d) $-3(\text{mod } 8) = 5$ (since $-3 = (-1)8 + 5$)

Definition (Modular Arithmetic Functions):-

For any positive integer M , called modulus, 'congruence modulo M ' is a relation on the set of all integers denoted by $a \equiv b \pmod{M}$, read as 'a is congruent to b modulo M, and defined by

$a \equiv b \pmod{M}$ if and only if M divides $b - a$

Arithmetic modulo M refers to the arithmetic operations of addition, multiplication and subtraction where the arithmetic value is replaced by its equivalent value in the set

$$\{0, 1, 2, \dots, M-1\} \text{ or } \{1, 2, \dots, M\}$$

For example, in arithmetic modulo 15

$$9 + 13 = 22 \equiv 22 - 15 = 7$$

$$4 - 9 = -5 \equiv -5 + 15 = 10$$

$$5 \times 18 = 90 \equiv 0 \equiv 15$$

Definition(Logarithmic functions):-

The function defined by $f(x)=a^x$, $x \in \mathbf{R}$ is called an exponential function.

A function $: (0,\infty) \rightarrow \mathbf{R}$ defined by $y = \log x$ iff $b^y = x$.

Is called logarithmic function with base point a.

Note:-

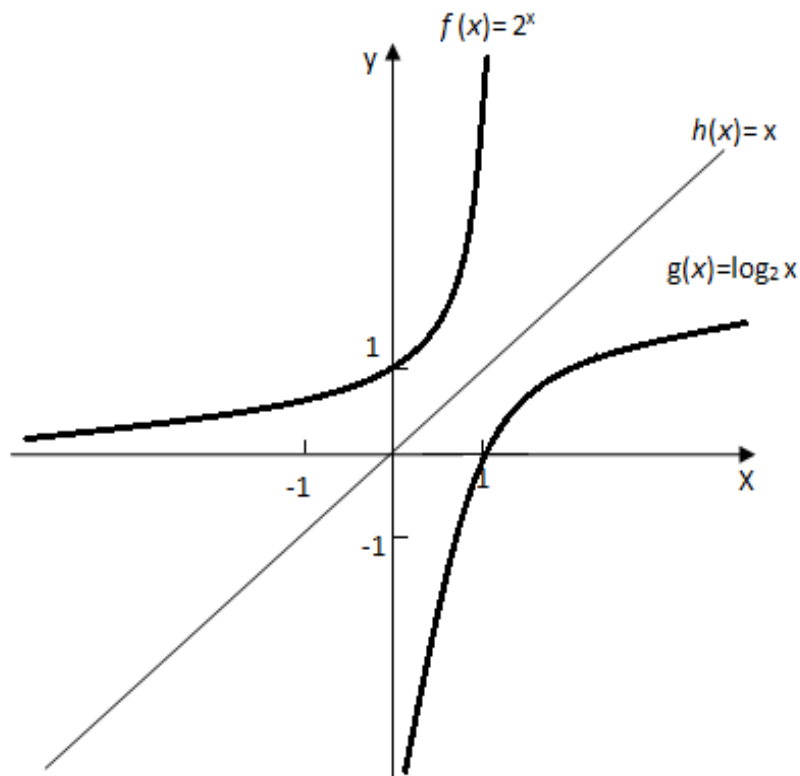
Exponential function and logarithmic functions are inverse to each other.

Example:-

Consider the Exponential function $f(x)=2^x$ and logarithmic function ,

$g(x)=\log_2 x$

since $f(x)$ and $g(x)$ are inverse functions they are symmetric with respect to the line $y = x$.



GRAPH OF 2^x AND \log

Recursively defined functions:-

A function is said to be recursively defined if the function refers to itself.

There are two steps to define a function with domain \mathbf{N} .

Basis step:-

The steps specifies the values of the function at initial values known as base values.

Recursive step:-

The steps give a rule for finding its value at an integer from its values at smaller integers.

Example:-

1 . Recursive definition of factorial function

a)if $n=0$,then $n!=1$.

b)if $n>0$,then $n!=n.(n-1)!$

Ex: 2 Fibonacci sequence:-

Fibonacci sequence is as follows 0,1,1,2,3,5,8,13,.....

Recursive Definition:

(a) if $n = 0$ or $n=1$ then $F_n=n$

(b) if $n > 1$ then $F_n=F_{n-2}+F_{n-1}$

Q. Let n denotes a positive integer. Suppose a function L is defined recursively as follows:

$$L(n) = \begin{cases} 0, & \text{if } n = 1 \\ L\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + 1, & \text{if } n > 1 \end{cases}$$

Find $L(25)$ and describe what this function does.

Solution:- $L(25)$ can be found recursively as follows:

$$\begin{aligned} L(25) &= L\left(\left\lfloor \frac{25}{2} \right\rfloor\right) + 1 = L(12) + 1 \quad \{\because \lfloor 25/2 \rfloor = 12\} \\ &= [L(\lfloor 6 \rfloor) + 1] + 2 = L(5) + 2 \quad \{\because \lfloor 6 \rfloor = 6\} \\ &= [L(\lfloor 3 \rfloor) + 1] + 2 = L(3) + 3 \quad \{\because \lfloor 3 \rfloor = 3\} \\ &= [L(\lfloor 3/2 \rfloor) + 1] + 3 = L(1) + 4 \quad \{\because \lfloor 3/2 \rfloor = \lfloor 1.5 \rfloor = 1\} \\ &= 0 + 4 = 4. \end{aligned}$$

Here each time n is divided by 2, the value of L is increased by 1.

Hence L is the greatest integer such that $2^L \leq n$. Hence $L(n) = \lfloor \log_2 n \rfloor$.

Definition (Restriction Function):-

Let $f: X \rightarrow Y$ and $A \subseteq X$ then f induces a function f' on A defined by

$$f'(a) = f(a), \forall a \in A.$$

This function $f|_A$ is denoted by $f|_A$ is called restriction of f to A

Example:-

Let $f : \mathbf{R} \rightarrow \mathbf{R}$ be defined by $f(x) = x^2$. Let $D = [0, \infty)$.

Then $f|_D$ is the restriction of f to the nonnegative real numbers.

Hence $f|_D$ is defined by $f|_D(x) = x^2$, for all $x \in D = [0, \infty)$.

Note that f is not one-to-one, but its restriction function $f|_D$ is one-to-one.

Definition (Extension function):-

Let f be a function from X into Y i.e., $f : X \rightarrow Y$ and Z be a superset of X . Let

$F : Z \rightarrow Y$ be a function on Z such that

$$F(x) = f(x), \text{ for all } x \in X.$$

This function F is called the **extension** of f to Z

Note:-

if F is an extension of f to Z , then f is the restriction of F to X
i.e., $f = F|_X$.

Example:-

Consider the function $f : [0, \infty) \rightarrow \mathbf{R} : f(x) = x$. Then the absolute value function

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$$

is an extension of f to \mathbf{R} , the set of all real numbers

Consider $F : \mathbf{R} \rightarrow \mathbf{R}$ defined by $F(x) = (x + |x|)/2$. Then \mathbf{R} is super set of $[0, \infty)$,

Let $x \in (0, \infty)$

$$\text{Then } F(x) = (x + |x|) / 2 = (x + x) / 2 = x = f(x)$$

\therefore F is an another extension of f

The identity function $I_{\mathbf{R}}$ from \mathbf{R} to \mathbf{R} is also an extension of f .

Note:-

From the above example it is clear that the extension of a function is not unique

Inclusion Map

Let A be a subset of X , Let i be the function from A to X , defined by

$i(a) = a$, for every $a \in A$. Then i is called the inclusion map

Example:-

$f : \mathbf{Z} \rightarrow \mathbf{R}$ defined by $f(n) = n$ is the inclusion map from \mathbf{Z} , the set of all integers to \mathbf{R} , the set of all real numbers.

Characteristic Function

Consider the universal set U . For any subset A of U , let χ_A be the function from U to $\{0,1\}$, defined by

$$\chi_A(x) = \begin{cases} 1, & \text{if } x \in A \\ 0, & \text{if } x \notin A \end{cases}$$

Then χ_A is called the **characteristic function** of A

Example:-

1. The characteristic function of \mathbf{Q} , the set of all rational numbers is

$\chi_{\mathbf{Q}} : \mathbb{R} \rightarrow \{0, 1\}$ defined by

$$\chi_{\mathbf{Q}}(x) = \begin{cases} 1, & \text{if } x \text{ is rational number} \\ 0, & \text{if } x \text{ is irrational number} \end{cases}$$

2. Let $U = \{a, b, c, d, e\}$ and the function f

$$\{(a, 1), (b, 0), (c, 1), (d, 1), (e, 1)\}.$$

If $A = \{a, c, d\}$, then $f : U \rightarrow \{0, 1\}$ such that

$$f(x) = \begin{cases} 1, & \text{if } x \in A \\ 0, & \text{if } x \notin A \end{cases}$$

Hence f is characteristic function of A .

Definition(Canonical Map):-

Let ' \equiv ' be an equivalence relation on a set S . Then we know that \equiv induces a partition of S into equivalence classes, called quotient set of S by \equiv , which is denoted and defined by

$$S/\equiv = \{[a] : a \in S\}.$$

The function $f : S \rightarrow S/\equiv$, defined by $f(a) = [a]$ is called canonical or natural map.

Example:-

Consider the relation \equiv of congruence modulo 6 on the set \mathbb{Z} , of integers. Then we know that for any two integers a and b

$$a \equiv b \pmod{6} \text{ if } a - b \text{ is divisible by } 6.$$

Then \equiv is an equivalence relation on \mathbb{Z} . There are two distinct equivalence classes

$$[0] = \{\dots, -12, -6, 0, 6, 12, \dots\}$$

$$[1] = \{\dots, -11, -5, 1, 7, 13, \dots\}$$

$$[2] = \{\dots, -10, -4, 2, 8, 14, \dots\}$$

$$[3] = \{\dots, -9, -3, 3, 9, 15, \dots\}$$

$$[4] = \{\dots, -8, -2, 4, 10, 16, \dots\}$$

$$[5] = \{\dots, -7, -1, 5, 11, 17, \dots\}$$

Hence $S \equiv = \{[0], [1], [2],[3],[4], [5]\}$.

Let $f: S \rightarrow S/\equiv$ be the canonical map.

Then $f(8) = [8] = [2]$

$f(19) = [19] = [1]$

$f(-28) = [-28] = [2]$.

Q. Let A and B be subsets of universal set U .

Then prove that $\chi_{A \cup B} = \chi_A + \chi_B - \chi_{A \cap B}$

Solution:-

Let $x \in U$.

Let $x \in A \cup B$.

Then $\chi_{A \cup B} = 1$.

Also $x \in A \cup B \Rightarrow x \in A$ or $x \in B$.

Then there are 3 cases.

Case 1: $x \in A$ and $x \notin B$

Then $x \notin A \cap B$ and hence

$\chi_A(x) = 1, \chi_B(x) = 0$ and $\chi_{A \cap B}(x) = 0$.

$\therefore \chi_A(x) + \chi_B(x) - \chi_{A \cup B}(x) = 1 + 0 - 0 = 1 = \chi_{A \cup B}$

Case 2: $x \notin A$ and $x \in B$,

Then $x \notin A \cap B$ and hence

$\chi_A(x) = 0, \chi_B(x) = 1, \chi_{A \cap B}(x) = 0$

$\therefore \chi_A(x) + \chi_B(x) - \chi_{A \cup B}(x) = 0 + 1 - 0 = 1 = \chi_{A \cup B}$.

Case 3: $x \in A$ and $x \in B$,

Then $x \in A \cap B$ and hence

$\chi_A(x) = 1, \chi_B(x) = 1$ and $\chi_{A \cup B}(x) = 1$.

$\therefore \chi_A(x) + \chi_B(x) - \chi_{A \cup B}(x) = 1 + 1 - 1 = 1 = \chi_{A \cup B}$.

\therefore when $x \in A \cup B$, $\chi_{A \cup B} = \chi_A + \chi_B - \chi_{A \cap B}$

Now let $x \notin A \cup B$.

Then $\chi_{A \cup B}(x) = 0$

Aiso $x \notin A \cup B \Rightarrow x \notin A$ and $x \notin B \Rightarrow x \notin A, x \notin B$ and $x \notin A \cap B$.

Hence $\chi_A(x) = 0, \chi_B(x) = 0$ and $\chi_{A \cup B}(x) = 0$.

$\therefore \chi_A(x) + \chi_B(x) - \chi_{A \cup B}(x) = 0 + 0 - 0 = 0 = \chi_{A \cup B}(x)$

Thus when $x \notin A \cup B$, $\chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_{A \cup B}(x)$.

$$\therefore \chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_{A \cup B}(x), \quad \forall x \in U$$

$$\therefore \chi_{A \cup B} = \chi_A + \chi_B - \chi_{A \cup B}.$$

FUNDAMENTAL FACTORIZATION OF A FUNCTION

Consider any function $f: X \rightarrow Y$. Define a relation ' \sim ' on X as follows:

$$x_1 \sim x_2 \text{ if } f(x_1) = f(x_2), \quad \forall x_1, x_2 \in X.$$

Then the relation ' \sim ' has the following properties:

(i) For any $x \in X$, $f(x) = f(x)$ and hence $x \sim x$.

\therefore the relation is reflexive.

(ii) For any $x_1, x_2 \in X$,

$$x_1 \sim x_2 \Rightarrow f(x_1) = f(x_2) \Rightarrow f(x_2) = f(x_1) \Rightarrow x_2 \sim x_1.$$

\therefore the relation is symmetric.

(iii) For any $x_1, x_2, x_3 \in X$

$$\begin{aligned} x_1 \sim x_2 \text{ and } x_2 \sim x_3 &\Rightarrow f(x_1) = f(x_2) \Rightarrow f(x_2) = f(x_3) \\ &\Rightarrow f(x_1) = f(x_3) \end{aligned}$$

Hence the relation \sim is transitive.

\therefore it is an equivalence relation on X .

$$\text{Let } X/f = X / \sim = \{[x] : x \in X\}.$$

Lemma. The function $f^* : X/f \rightarrow f(X)$, defined by

$$f^*([x]) = f(x)$$

is well defined and bijective.

Proof.

Let $[x_1], [x_2] \in X/f$,

$$[x_1] = [x_2] \Rightarrow x_1 \sim x_2 \Rightarrow f(x_1) = f(x_2) \Rightarrow f^*([x_1]) = f^*([x_2]).$$

Hence f^* is a well-defined function from X/f to $f(X)$.

Let $[x_1], [x_2] \in X/f$,

$$f^*([x_1]) = f^*([x_2]) \Rightarrow f(x_1) = f(x_2) \Rightarrow x_1 \sim x_2 \Rightarrow [x_1] = [x_2].$$

Hence f^* is one-to-one.

let $y \in f(X)$.

then $\exists x \in X$ such that $y = f(x)$.

Since $x \in X$, $[x] \in X/f$ and $f^*([x]) = f(x) = y$.

Hence f^* is onto.

Thus f^* is bijective.

Theorem:-

Let $f : X \rightarrow Y$, $f^* : X/f \rightarrow f(X)$ be defined by $f^*([x]) = f(x)$, \mathbf{n} be the canonical mapping from X into X/f and \mathbf{i} be the inclusion map from $f(X)$ into Y Then $f = \mathbf{i} \circ f^* \circ \mathbf{n}$.

Proof.

Given $f : X \rightarrow Y$ and $f^* : X/f \rightarrow f(X)$ be defined by $f^*([x]) = f(x)$. Then by the previous lemma f^* is well-defined and bijective.

The canonical map $\mathbf{n} : X \rightarrow X/f$ is defined by

$$\mathbf{n}(x) = [x], \text{ for all } x \in X$$

The inclusion map $\mathbf{i} : f(X) \rightarrow Y$ is defined by

$$\mathbf{i}(y) = y, \text{ for all } y \in f(X).$$

Then the definition of composition of function, we have

$$\mathbf{i} \circ f^* : X/f \rightarrow Y \quad \text{and} \quad \mathbf{i} \circ f^* \circ \mathbf{n} : X \rightarrow Y.$$

Also for all $x \in X$,

$$\begin{aligned} (\mathbf{i} \circ f^* \circ \mathbf{n})(x) &= (\mathbf{i} \circ f^*)(\mathbf{n}(x)) = (\mathbf{i} \circ f^*)([x]) \\ &= \mathbf{i}(f^*([x])) = \mathbf{i}(f(x)) = f(x). \end{aligned}$$

Hence $f = \mathbf{i} \circ f^* \circ \mathbf{n}$.

Q. Let $A = \{1,2,3,4,5\}$ and let $f = A \rightarrow A$ be defined by

$$f = \{(1,4),(2,1),(3,4),(4,2),(5,4)\}.$$

(a) Find A/f and $f(A)$.

(b) verify the factorization $f = \mathbf{i} \circ f^* \circ \mathbf{n}$.

Solution.

(a) Since $f(1) = f(3) = f(5) = 4$, $f(2) = 1$ and $f(4) = 2$, $[1] = [3] = [5] = \{1,3,5\}$, $[2] = \{2\}$ and $[4] = \{4\}$.

$$\therefore A/f = \{[1],[2],[4]\}$$

$$\text{and } f(A) = \{1,2,4\}.$$

(b) The function $f^* : A/f \rightarrow f(A)$ is defined by $f^*([a]) = f(a)$, for all $a \in A$,

Hence

$$f^*([1]) = f(1) = 4, \quad f^*([2]) = f(2) = 1 \quad \text{and} \quad f^*([4]) = f(4) = 2.$$

The canonical map $\mathbf{n} : A \rightarrow A/f$ is defined by

$$\mathbf{n}(a) = [a], \text{ for all } a \in A.$$

$$\therefore \mathbf{n}(1) = [1], \quad \mathbf{n}(2) = [2], \quad \mathbf{n}(3) = [3] = [1], \quad \mathbf{n}(4) = [4] \quad \text{and} \quad \mathbf{n}(5) = [5] = [1].$$

The inclusion map $\mathbf{i} : f(A) \rightarrow A$ is defined by $\mathbf{i}(b) = b$, for all $b \in f(A)$.

$$\therefore \mathbf{i}(1) = 1, \quad \mathbf{i}(2) = 2 \quad \text{and} \quad \mathbf{i}(4) = 4.$$

$$\begin{aligned} \text{Hence } (i \circ f^* \circ n)(1) &= (i \circ f^*)(n(1)) = (i \circ f^*)([1]) \\ &= i(f^*([1])) = i(4) = 4 = f(1). \\ (i \circ f^* \circ n)(2) &= (i \circ f^*)(n(2)) = (i \circ f^*)([2]) \\ &= i(f^*([2])) = i(1) = 1 = f(2). \\ (i \circ f^* \circ n)(3) &= (i \circ f^*)(n(3)) = (i \circ f^*)([3]). \\ &= i(f^*([1])) = i(4) = 4 = f(3). \quad \{ \because [3] = [1] \} \\ (i \circ f^* \circ n)(4) &= (i \circ f^*)(n(4)) = (i \circ f^*)([4]). \\ &= i(f^*([4])) = i(f(2)) = f(2). \\ (i \circ f^* \circ n)(5) &= (i \circ f^*)(n(5)) = (i \circ f^*)([5]). \\ &= i(f^*([1])) = i(4) = 4 = f(5). \quad \{ \because [5] = [1] \} \\ i \circ f^* \circ n &= f. \end{aligned}$$

ASSOCIATED SET FUNCTIONS

Definition:-

Let $f : X \rightarrow Y$. and A sub X then image of A is denoted and defined by

$$f(A) = \{ f(a) : a \in A \}$$

If B sub Y , then **pre-image** or **inverse image** of B , is denoted and defined by

$$f^{-1}[B] = \{ x \in X : f(x) \in B \}$$

Note:-

A function which map sets in to sets is called a set function

Example:-

Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x^4$. Then

$$\begin{aligned} f[\{-2, -1, 0, 1, 2\}] &= \{0, 1, 16\}; f[(-1, 0)] = (0, 1) \\ f^{-1}[\{1, 81\}] &= \{-3, -1, 1, 3\}; f^{-1}[(0, 1)] = (-1, 0) \cup (0, 1). \end{aligned}$$

Theorem:-

Let $f : X \rightarrow Y$ and let $A \subseteq X$ and $B \subseteq Y$. Then

- (i) $A \subseteq f^{-1} \circ f[A]$.
- (ii) $f \circ f^{-1}[B] \subseteq B$.

Proof:-

(i) let $x \in X$,

$$x \in A \Rightarrow f(x) \in f[A] \Rightarrow x \in f^{-1}[f[A]] = f^{-1} \circ f[A].$$

$$\therefore A \subseteq f^{-1} \circ f[A].$$

(ii) let $y \in f \circ f^{-1}[B] \Rightarrow y \in f[f^{-1}[B]]$

$$\Rightarrow y = f(x), \text{ for some } x \in f^{-1}[B]$$

$$\begin{aligned} &\Rightarrow y = f(x), \text{ for some } x, \text{ such that } f(x) \in B \\ &\Rightarrow y = f(x) \in B \\ \therefore & f \circ f^{-1}[B] \subseteq B. \end{aligned}$$

Remark- The inclusion in the above theorem can be proper

Consider $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x^2$.

Let $A = (1,2)$. Then

$$f^{-1} \circ f[A] = f^{-1}[f(1,2)] = f^{-1}[(1,4)] = (1,2) \cup (-2, -1).$$

$$\therefore (1, 2) = A \subseteq f^{-1} \circ f[A]$$

Now let $B = (-\infty, 0] = \{x : x \leq 0\}$. then

$$f^{-1} \circ f[B] = f^{-1}[f(-\infty, 0]] = f^{-1}[\{0\}] = \{0\}$$

$$\therefore f \circ f^{-1}[B] \subseteq (-\infty, 0] = B$$

Q. Let $f : X \rightarrow Y$ and let $A \subseteq X$ and $B \subseteq X$.

Then prove that.

- a) $f[A \cup B] = f[A] \cup f[B]$.
- b) $f[A \cap B] \subseteq f[A] \cap f[B]$.
- c) give an example to show that the inclusion can be proper.

Proof:-

Let $y \in f[A \cup B] \Rightarrow y = f(x)$ for some $x \in A \cup B$.

$$\Rightarrow y = f(x) \text{ for some } x \in A \text{ or } x \in B.$$

$$\Rightarrow y = f(x) \in f[A] \text{ or } f(x) \in f[B].$$

$$\therefore f[A \cup B] \subseteq f[A] \cup f[B]. \dots\dots\dots(1)$$

Let $y \in f[A] \cap f[B] \Rightarrow y \in f[A] \text{ or } y \in f[B]$.

$$\Rightarrow y = f(x_1), \text{ for some } x \in A \text{ or } y = f(x_2) \text{ for some } x_2 \in A.$$

$$\Rightarrow y = f(x), \text{ for some } x \in A \text{ or } x \in B.$$

$$\Rightarrow y = f(x), \text{ for some } x \in A \cup B.$$

$$\Rightarrow y = f[A \cup B].$$

$$f[A] \cup f[B] \subseteq f[A \cup B] \dots\dots\dots(2)$$

From (1) and (2), we get

$$f[A \cup B] = f[A] \cup f[B].$$

b).

Let $y \in f[A \cap B] \Rightarrow y = f(x)$ for some $x \in A \cap B$.

$$\Rightarrow y = f(x) \text{ for some } x \in A \text{ or } x \in B.$$

$$\Rightarrow y = f(x) \in f[A] \text{ and } y = f(x) \in f[B].$$

$$\Rightarrow y \in f[A] \cap f[B].$$

$$\therefore f[A \cap B] \subseteq f[A] \cap f[B].$$

c) Consider the function $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x^2$.

Let $A = [-2, 0]$ and $B = [0, 2]$. Then

$$f[A \cap B] = f[-2, 0] \cap f[0, 2] = f[\{0\}] = \{0\}$$

and $f[A] \cap f[B] = f[-2, 0] \cap f[0, 2] = [0, 4] \cap [0, 4] = [0, 4].$

$$\therefore f[A \cap B] \subsetneq f[A] \cap f[B]$$

ALGORITHMS AND FUNCTIONS

An algorithm M is a step-by-step list of well defined instruction for solving a particular problem, say, to find the output $f(X)$ for a given function f with input X.

Example:-

1. Polynomial Evaluation. Consider the polynomial

$$f(x) = 2x^3 - 7x^2 + 4x - 15$$

we can find $f(y)$ in two methods

Direct Method: Here we substitute $x = 5$ directly in the polynomial to obtain

$$\begin{aligned} f(5) &= 2(125) - 7(25) + 4(5) - 15 \\ &= 250 - 175 + 20 - 15 \\ &= 80 \end{aligned}$$

Here there are $3 + 2 + 1 = 6$ multiplications and three additions. In general, Evaluating a polynomial of degree n would require approximately $n + (n - 1) + \dots + 2 + 1 = n(n - 1)/2$ multiplications and n additions

Horner's Method or Synthetic division:

Here we write the polynomial by successively factoring out x as follows:

$$\begin{aligned} f(x) &= (2x^2 - 7x + 4)x - 15 = [(2x - 7)x + 4]x - 15 \\ \text{Then } f(5) &= [(3)5 + 4]5 - 15 = (19)5 - 15 = 80. \end{aligned}$$

Observe that here there are only 3 multiplications and 3 additions.

The above calculations are equivalent to the following synthetic division:

$$\begin{array}{r|rrrr} 5 & 2 & -7 & +4 & -15 \\ & & 10 & +15 & +95 \\ \hline & 2 & +3 & +19 & +80 \end{array}$$

2. finding GCD(Greatest Common Divisor):

Let a and b be two positive integers .we can find $\text{gcd}(a,b)$ by 2 methods.

(a) Direct methods:

Finding all divisors of a and b and pick the largest.

Let a=15, b=20

The divisors of 15 = 1,3,5,15

The divisors of 20 = 1, 2,4,5,10,20.

$$\therefore \text{Gcd}(15,20) = 5.$$

(b) Euclidian algorithm:

Devide a by b.then we get remainder r_1 and $q_1 \in \mathbb{Z}$. such that $a=bq_1 + r_1$.

then divide b by r_1 to get second remained r_2 and $q_2 \in \mathbb{Z}$ such that

$$b = r_1q_2 + r_2$$

$$r_1 = r_2q_3 + r_3$$

$$r_2 = r_3q_4 + r_4$$

.

.

.

Proceeding like that we get $r_m = 0$

Then $\text{gcd}(a, b) = r_{m-1}$

Example:-

Let a = 164, b = 30

$$164 = 30 \times 5 + 14$$

$$30 = 14 \times 2 + 2$$

$$14 = 2 \times 7 + 0$$

$$\therefore \text{gcd}(164, 30) = 2$$

Complexity of algorithm:

There are two norms to measure the efficiency of an algorithm, space complexity and time complexity.

The space complexity refers to how much storage space the algorithm needs.

The time complexity refers to the time it taken to run an algorithm. it is a function of size n of the input data.

Definition(Big O Notation):-

Let f and g be the two functions: \mathbb{Z} to \mathbb{R} , we say that f(x) is big-oh of g(x) or f(x) is of order g(x) written as $f(x) = O(g(x))$

If there exists a real number k and positive constant C such that for all $x > k$,

$$|f(x)| \leq C|g(x)|$$

Where C and K are called witness to the relationship $f(x) = O(g(x))$

Q. Show that if $P(x)$ is a polynomial of degree n , $p(x) = O(x^n)$

Solution:-

Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $a_i \in \mathbb{R}$ for $i = 0, 1, 2, 3, \dots, n$

Let $x > 1$

$$\begin{aligned} |P(x)| &= |a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0| \\ &\leq |a_n| x^n + |a_{n-1}| x^{n-1} + \dots + |a_1| x + |a_0| \\ &= \left[|a_n| + \frac{|a_{n-1}|}{x} + \dots + \frac{|a_1|}{x^{n-1}} + \frac{|a_0|}{x^n} \right] x^n \\ &\leq [|a_n| + |a_{n-1}| + \dots + |a_1| + |a_0|] x^n \\ &\quad \left(\because x > 1 \Rightarrow \frac{1}{x} < 1 \right) \end{aligned}$$

Let $C = |a_n| + |a_{n-1}| + \dots + |a_1| + |a_0|$ and $k = 1$, then we get

$$\begin{aligned} |P(x)| &\leq C x^n, \text{ for all } x > k \\ \therefore p(x) &= O(x^n) \end{aligned}$$

FURTHER THEORY OF SETS

Definition:-

Let \mathcal{A} be a collection of sets. The union of \mathcal{A} denoted and defined by,

$$\bigcup_{A \in \mathcal{A}} A = \{ x \mid x \in A \text{ for some } A \in \mathcal{A} \}$$

Let \mathcal{A} be a non-empty collection of sets, then the intersection of \mathcal{A} denoted and defined by

$$\bigcap_{A \in \mathcal{A}} A = \{ x \mid x \in A \text{ for every } A \in \mathcal{A} \}$$

Note:-

If \mathcal{A} is a finite set then the above definition coincide with our previous definition of union and intersection

Example:- Let $\mathcal{A} = \{ A_i \mid i = 1, 2, 3, \dots \}$ where,

$$A_i = \{ 1, 2, 3, \dots, i \}$$

Then $\bigcup_{A_i \in \mathcal{A}} A_i =$ set of all natural numbers

$$\text{and } \bigcap_{A_i \in \mathcal{A}} A_i = \{ 1 \}.$$

Definition:-

Let I be a nonempty set and \mathcal{L} be a collection of sets

Then a function $f : I \rightarrow \mathcal{L}$ is called an **indexing function**

For any $i \in I$, denote the image $f(i)$ by A_i

Then set $\{ A_i, i \in I \}$ is called **indexed collection** of sets.

Note:- $\cup \{A_i, i \in I\} = \{x \mid x \in A_i \text{ for some } i \in I\}$

Example:-

- Let \mathbb{Z} be the set of all integers. For each $n \in \mathbb{Z}$, let $A_n = (-\infty, n]$.

Let $x \in \mathbb{R}$

then there exist n_1 and n_2 such that $n_1 < x < n_2$

$$\therefore x \in A_{n_2} \text{ and } x \notin A_{n_1}$$

$$\therefore x \in \cup_n A_n \text{ and } x \notin \cap_n A_n$$

Since x is arbitrary, $\cup_n A_n = \mathbb{R}$ and $\cap_n A_n = \emptyset$

- Let $I = \{1,2,3,4,5,6\}$ and $J = \{2,4\}$ and let $A_i = \{1,2,\dots,3i\}$

For $i = 1,2,\dots,6$ then,

$$\cup_i A_i = \{1,2,\dots,18\}$$

$$\cap_i A_i = \{1,2,3\}$$

$$\cup_{i \in J} A_i = \{1,2,\dots,12\}$$

$$\cap_{i \in J} A_i = \{1,2,3,4,5,6\}$$

Theorem.

Let B and $\{A_i\}$ with $i \in I$ be subsets of a universal set U . Then

- $B \cap (\cup_i A_i) = \cup_i \{B \cap A_i\}$ and $B \cup (\cap_i A_i) = \cap_i \{B \cup A_i\}$.
- $[\cup_i A_i]^c = \cap_i A_i^c$ and $[\cap_i A_i]^c = \cup_i A_i^c$.
- If J is any subset of I , then $\cup_{i \in J} A_i \subseteq \cup_{i \in I} A_i \subseteq U$ and $\cap_{i \in J} A_i \supseteq \cap_{i \in I} A_i$

Proof:-

$$\begin{aligned} \text{a) } B \cap (\cup_i A_i) &= \{x: x \in B \text{ and } x \in \cup_i A_i\} \\ &= \{x: x \in B \text{ and } \exists i_0 \text{ such that } x \in A_{i_0}\} \\ &= \{x: \exists i_0 \text{ such that } x \in B \cap A_{i_0}\} \\ &= \cup_i \{B \cap A_i\} \end{aligned}$$

$$\begin{aligned} B \cup (\cap_i A_i) &= \{x: x \in B \text{ or } x \in \cap_i A_i\} \\ &= \{x: x \in B \text{ or } x \in A_i, \forall i\} \\ &= \{x: \forall i, x \in B \text{ or } x \in A_i\} \\ &= \{x: x \in B \cup A_i, \forall i\} \\ &= \cap_i \{B \cup A_i\}. \end{aligned}$$

$$\begin{aligned} \text{b) } [\cup_i A_i]^c &= \{x: x \notin \cup_i A_i\} \\ &= \{x: \forall i, x \notin A_i\} \\ &= \{x: \forall i, x \in A_i^c\} \\ &= \cap_i A_i^c. \end{aligned}$$

$$\begin{aligned}
 [\bigcap_i A_i]^c &= \{x : x \notin \bigcap_i A_i\} \\
 &= \{x : \exists i_0 \text{ such that } x \notin A_{i_0}\} \\
 &= \{x : \exists i_0 \text{ such that } x \in A_{i_0}^c\} \\
 &= \bigcup_i A_i^c.
 \end{aligned}$$

c) If J is any subset of I , then

$$\bigcup_{i \in J} A_i \subseteq \bigcup_{i \in I} A_i \quad \text{and} \quad \bigcap_{i \in J} A_i \supseteq \bigcap_{i \in I} A_i$$

Proof:-

$$\begin{aligned}
 x \in \bigcup_{i \in J} A_i &\Rightarrow \exists i_0 \in J \text{ such that } x \in A_{i_0} \\
 &\Rightarrow \exists i_0 \in I \text{ such that } x \in A_{i_0} \quad (\because J \subseteq I) \\
 &\Rightarrow x \in \bigcup_{i \in I} A_i \\
 &\quad \bigcup_{i \in J} A_i \subseteq \bigcup_{i \in I} A_i \\
 x \in \bigcap_{i \in J} A_i &\Rightarrow \forall i \in J, x \in A_i \\
 &\Rightarrow \forall i \in I, x \in A_i \\
 &\Rightarrow x \in \bigcap_{i \in I} A_i. \\
 \therefore \bigcap_{i \in J} A_i &\supseteq \bigcap_{i \in I} A_i.
 \end{aligned}$$

Definition (Equipotent Sets):-

Two sets A and B are said to be **equipotent** or said to have the same cardinality, written $A \approx B$ if \exists a function $f : A \rightarrow B$ which is bijective.

Theorem:-

The relation \approx of being equipotent is an equivalence relation in any collection of sets

Proof:-

(i) **Reflexive**

Let A be a set, then the identity function
 $I_A : A \rightarrow A$, defined by,
 $I_A(a) = a$, for all $a \in A$.
 is one-one and onto
 $\therefore A \approx A$.

(ii) **Symmetric**

Let A and B be two sets, and $A \approx B$
 Then $\exists f : A \rightarrow B$ which is a bijection
 $\therefore \exists f^{-1} : B \rightarrow A$ which is also a bijection
 $\therefore B \approx A$.

(iii) **Transitive**

Let A, B, C be three sets and suppose $A \approx B$ and $B \approx C$
 Then $\exists f, g : A \rightarrow C$ both are bijective
 $\therefore g \circ f : A \rightarrow C$ is also bijective
 $\therefore A \approx C$
 Hence \approx is an equivalence relation.

Example:-

Let $A = \{a, b, c\}$ and $B = \{x, y, z\}$.

Define $f : A \rightarrow B$ by

$$f(a) = y, f(b) = z, f(c) = x$$

then f is clearly a bijection

$$\therefore A \approx B$$

Ex:2. Let $A = [0, 1]$, the closed unit interval and $B = [a, b]$, where a and b are any two real numbers with $a < b$.

Consider the function $f : [0, 1] \rightarrow [a, b]$, defined by

$$f(x) = (b - a)x + a, \forall x \in [0, 1].$$

Let $x_1, x_2 \in [0, 1]$

Suppose $f(x_1) = f(x_2)$

$$\text{Then } (b - a)x_1 + a = (b - a)x_2 + a$$

$$\Rightarrow x_1 = x_2$$

$\therefore f$ is one-to-one.

Let $y \in [a, b]$, then $a \leq y \leq b$

$$\Rightarrow 0 \leq y - a \leq b - a$$

$$\Rightarrow 0 \leq \frac{y - a}{b - a} \leq 1.$$

Hence $\exists x = \frac{y - a}{b - a} \in [0, 1]$ such that $f\left(\frac{y - a}{b - a}\right) = y$.

$\therefore f$ is onto.

$\therefore f$ is bijective.

$\therefore [0, 1] \approx [a, b]$

Remark:

Any two closed intervals have the same cardinality.

Question: Prove that $[0, 1] \approx (0, 1)$

Solution:

Let $[0, 1] = \{0, 1, 1/2, 1/3, \dots\} \cup A$ and $(0, 1) = \{1/2, 1/3, 1/4, \dots\} \cup A$

where $A = [0, 1] - \{0, 1, 1/2, 1/3, \dots\} = (0, 1) - \{1/2, 1/3, 1/4, \dots\}$

consider the function $f : [0, 1] \rightarrow (0, 1)$, defined by

$$f(x) = \begin{cases} 1/2 & \text{if } x = 0 \\ 1/n + 2 & \text{if } x = 1/n, n \in \mathbb{N} \\ x & \text{if } x \in A \end{cases}$$

is one-to-one and onto.

Hence $[0, 1] \approx (0, 1)$

Denumerable and Countable Sets

Definition:-

A set D is said to be *denumerable* or *accountably infinite* if $D \approx \mathbb{N}$, the set of all natural numbers.

A set is said to be *countable* if it is finite or denumerable. a set which is not countable is called non denumerable set.

Note:-

A set is Denumerable if and only if its elements can be arranged as a sequence of distinct items. So $[0,1]$ is non denumerable.

Example:

$$1. \quad \text{Let } A = \left\{ \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \dots \right\}.$$

Consider the mapping $f : \mathbb{N} \rightarrow A$, defined by

$$f(n) = \frac{n}{n+1}, \text{ for all } n \in \mathbb{N}$$

Then f is one to one and onto.

$$\therefore A \approx \mathbb{N}.$$

Hence A is denumerable.

$$2. \quad \text{The function } f : \mathbb{N} \rightarrow \mathbb{Z} \text{ defined by } f(n) = \frac{n}{2}, \quad \text{if } n \text{ is even}$$

$$= -\left(\frac{n-1}{2}\right) \text{ if } n \text{ is odd}$$

is one to one and onto.

$$\therefore \mathbb{N} \approx \mathbb{Z}$$

Definition (Cardinal Numbers)

The cardinal number of a set A is denoted by $|A|$. Two sets A and B have same cardinality if $A \approx B$.

i.e., $|A| = |B|$ if and only if $A \approx B$.

$|\mathbb{N}| = \aleph_0$, read as aleph-nought **and** $|[0,1]| = C$, called the power continuum

Remark:-

- (i) If A is a denumerable set then $|A| = \aleph_0$.
- (ii) If A is non-denumerable set then $|A| = C$.

MODULE -3

BASIC LOGIC-1

1) Basic Concepts

Proposition : A declarative sentence which is either true or false is known as a proposition

If a proposition is true we say that it has a truth value T. If a proposition is false it has the truth value F.

Negation : If p is a proposition then the negation of p , $\neg p$ is the proposition “it is not the case p ”. The truth table of the negation of a proposition is as follows

P	$\neg P$
T	F
F	T

Conjunction: Let p and q be two propositions. The conjunction of p and q is the proposition “ p and q ” and is denoted by $p \wedge q$

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Eg : Let p : Kerala is a state in India q : Trivandrum is the capital of kerala

Then $p \wedge q$: Kerala is a state in India and Trivandrum is the capital of Kerala

Disjunction : Let p and q be two propositions then the proposition “ p or q ”, denoted by $p \vee q$ is the disjunction of p and q

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Remark: The “exclusive or” of p and q is denoted by $p \oplus q$.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Implication (Conditional statement) : The implication, $p \rightarrow q$ is the proposition “ if p then q”. Here p is called the hypothesis or premise and q is called the conclusion or consequence.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Note that $p \rightarrow q$ is false, only when p is true and q is false.

Bi-implication : the bi-implication (biconditional) of p and q, denoted by $p \leftrightarrow q$ is the proposition “ p if and only if q”.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Note that $p \leftrightarrow q$ is true, only when both p and q have the same truth value.

Converse, Inverse and Contrapositive :

The converse of $p \rightarrow q$ is $q \rightarrow p$

The inverse of $p \rightarrow q$ is $\neg p \rightarrow \neg q$

The contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$

Equivalent Propositions : Two propositions are equivalent if the columns giving their truth values in the truth table are identical.

Example 1: Show that $p \rightarrow q$ and its contrapositive are equivalent

Answer: The 3rd and 6th columns in the following table are identical. So $p \rightarrow q$ and $\neg q \rightarrow \neg p$ are equivalent.

p	q	$p \rightarrow q$	$\neg q$	$\neg p$	$\neg q \rightarrow \neg p$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Example 2 :Show that $q \rightarrow p$ and $\neg p \rightarrow q$ are equivalent

Answer:

p	q	$q \rightarrow p$	$\neg p$	$\neg q$	$\neg p \rightarrow \neg q$
T	T	T	F	F	T
T	F	T	F	T	T
F	T	F	T	F	F
F	F	T	T	T	T

Exercise: Construct the truth table for each of the following propositions

- 1) $p \rightarrow \neg q$ 2) $\neg p \rightarrow q$ 3) $(p \rightarrow q) \vee (\neg p \rightarrow q)$ 4) $(p \rightarrow q) \wedge (\neg p \rightarrow q)$
 5) $(p \leftrightarrow q) \vee (\neg p \leftrightarrow q)$

Problem: 1) What are the contrapositive, the converse and the inverse of the conditional statement “The home team wins whenever it is raining”.

Answer: The given statement can be rewritten as “If it is raining the home team wins”

The contrapositive of this proposition is “If the home team does not win then it is not raining.

The converse is “If the home team wins then it is raining”

The inverse is “If it is not raining then the home team does not win”

Problem 2): Let p be the statement “ you can take the flight” and q be the statement “you buy a ticket”. Write the bi-implication $p \leftrightarrow q$

Answer : $p \leftrightarrow q$: “ you can take the flight if and only if you buy a ticket”

Problem 3 : Determine whether each of the following conditional statements are true or false.

- (i) If $1+1=2$ then $2+2=5$
- (ii) If $1+1=3$ then $2+2=4$
- (iii) If $1+1=3$ then $2+2=5$
- (iv) If the monkeys can fly then $1+1=3$

Answers : (i) False (ii) True (iii) True (iv) True

Problem 4) Find the bitwise OR , bitwise AND and bitwise XOR (exclusive or) of the following bitstrings

(i) 01 1011 0110 and 11 0001 1101

(ii) 101 1110 and 010 0001

Answers (i) 01 1011 0110
11 0001 1101

Bitwise OR 11 1011 1111

Bitwise AND 01 0001 0100

Bitwise XOR 10 1010 1011

(ii) 101 1110
010 0001

Bitwise OR 111 1111

Bitwise AND 000 0000

Bitwise XOR 111 1111

Exercise: 1) Construct the truth table for the following compound propositions

a) $p \wedge \neg p$ b) $p \vee \neg p$ c) $(p \vee \neg q) \rightarrow p$

2) Translate the following statements into logical expressions

a) It is below freezing and snowing

b) You can access the internet from the campus only if you are
Mathematics student or you are not a freshman

c) You can take the flight if and only if you buy a ticket

3 Construct the truth table for the following compound propositions

a) $(p \rightarrow q) \vee (q \rightarrow p)$ b) $(p \vee \neg q) \rightarrow (p \wedge q)$

c) $(p \vee q) \rightarrow (p \oplus q)$ d) $(p \leftrightarrow q) \oplus (\neg p \leftrightarrow \neg q)$

e) $(p \leftrightarrow q) \oplus (\neg p \leftrightarrow q)$

4) Translate the following statement in to a logical expression

“You cannot ride the roller coaster if you are under 4 feet tall
unless you are older than 16 years old”

Tautology: A compound proposition which always true is called a tautology

Eg: $p \vee \neg p$

Contradiction : If a compound proposition is always false then it is known as a contradiction

Eg: $p \wedge \neg p$

Contingency: A compound proposition which is neither a tautology nor a Contradiction is called a contingency

Eg: $p \vee q$

Remark: Two compound propositions are said to be logically equivalent when their truth values are same. When p and q are logically equivalent we write $p \equiv q$

1) Prove that $\neg(\neg p) \equiv p$ (Double negation law)

Ans:

p	$\neg p$	$\neg(\neg p)$
T	F	T
F	T	F

2) Show that $p \wedge T \equiv p$ (Identity law)

Sol:

p	T	$p \wedge T$
T	T	T
F	T	F

3) Show that $p \vee F \equiv p$ (Identity law)

Sol:

p	F	$p \vee F$
T	F	T
F	F	F

Show that $p \vee T \equiv T$ and $p \wedge F \equiv F$ (Domination laws)

Sol:

p	T	$p \vee T$	F	$p \wedge F$
T	T	T	F	F
F	T	T	F	F

- 5) Prove that The Demorgan's laws
- (i) $\neg(p \vee q) \equiv \neg p \wedge \neg q$
 - (ii) $\neg(p \wedge q) \equiv \neg p \vee \neg q$

Ans:

P	q	$\neg p$	$\neg q$	$\neg p \wedge \neg q$	$p \vee q$	$\neg(p \vee q)$
T	T	F	F	F	T	F
T	F	F	T	F	T	F
F	T	T	F	F	T	F
F	F	T	T	T	F	T

Similarly we can prove $\neg(p \wedge q) \equiv \neg p \vee \neg q$

Exercise

- 1) Prove the commutative laws: $p \vee q \equiv q \vee p$ and $p \wedge q \equiv q \wedge p$
- 2) Prove the associative laws : $p \vee (q \vee r) \equiv (p \vee q) \vee r$ and $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
- 3) Prove the distributive laws: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ and $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
- 4) Prove the absorption laws : $p \vee (p \wedge q) \equiv p$ and $p \wedge (p \vee q) \equiv p$
- 5) Prove the negation laws : $p \vee \neg p \equiv T$ and $p \wedge \neg p \equiv F$
- 6) Show that $p \rightarrow q \equiv \neg p \vee q$

- 7) Show that $\neg(p \oplus q) \equiv p \leftrightarrow q$
 8) Show that $p \vee q \equiv \neg p \rightarrow q$
 9) Show that $\neg(p \rightarrow q) \equiv p \wedge \neg q$
 10) Show that $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$
 11) Show that $(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$
 12) Show that $((p \rightarrow r) \vee (q \rightarrow r)) \equiv (p \wedge q) \rightarrow r$
 13) Show that $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
 14) Show that $p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

Worked out problems

- 1) Show that $\neg(p \rightarrow q)$ and $p \wedge \neg q$ are logically equivalent

$$\begin{aligned} \text{Ans: } \neg(p \rightarrow q) &\equiv \neg(\neg p \vee q) && \text{Since } p \rightarrow q \equiv \neg p \vee q \\ &\equiv \neg(\neg p) \wedge \neg q && \text{using De-Morgan's law} \\ &\equiv p \wedge \neg q && \text{since } \neg(\neg p) \equiv p \end{aligned}$$

- 2) Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent

$$\begin{aligned} \text{Ans: } \neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) && \text{using De-Morgan's law} \\ &\equiv \neg p \wedge (\neg(\neg p) \vee \neg q) && \text{using De-Morgan's law} \\ &\equiv \neg p \wedge (p \vee \neg q) && \text{using double negation law} \\ &\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{using distributive law} \\ &\equiv F \vee (\neg p \wedge \neg q) && \text{using negation law} \\ &\equiv (\neg p \wedge \neg q) \vee F && \text{using commutative law} \\ &\equiv (\neg p \wedge \neg q) && \text{using identity law} \end{aligned}$$

- 3) Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology

$$\begin{aligned} \text{Ans: } (p \wedge q) \rightarrow (p \vee q) &\equiv [\neg(p \wedge q)] \vee (p \vee q) && \text{Since } r \rightarrow q \equiv \neg r \vee q \\ &\equiv (\neg p \vee \neg q) \vee (p \vee q) && \text{using De-Morgan's law} \\ &\equiv (\neg p \vee p) \vee (\neg q \vee q) && \text{using associative law} \\ &\equiv T \vee T && \text{using negation law} \\ &\equiv T \end{aligned}$$

- 4) Use De-Morgan's law to express the negation of "John is rich and intelligent"

Ans: Let p be "John is rich" and q be "John is intelligent". Then the given proposition is $p \wedge q$. By De-Morgan's law $\neg(p \wedge q) \equiv \neg p \vee \neg q$

\therefore The negation of the given statement is "John is not rich or John is not intelligent"

5) Use De-Morgan's law to express the negation of " Hari will go to the concert or Steve will go to the concert."

Ans: Let p be the proposition " Hari will go to the concert" and q be " Steve will go to the concert". The given statement is $p \vee q$.

By De-Morgan's law $\neg(p \vee q) \equiv \neg p \wedge \neg q$

\therefore The negation of the given proposition is " Hari will not go to the concert and Steve will not go to the concert"

6) Show that $(P \rightarrow q) \rightarrow r$ and $p \rightarrow (q \rightarrow r)$ are not logically equivalent

Ans: Consider the case when p, q, r are false. Then $p \rightarrow q$ is true so $(p \rightarrow q) \rightarrow r$ is false.

But $(q \rightarrow r)$ is true and $p \rightarrow (q \rightarrow r)$ is true. Therefore they have different truth values atleast in one case. So they are not logically equivalent'

7) Show that $(p \wedge q) \rightarrow r$ and $(p \rightarrow r) \wedge (q \rightarrow r)$ are not logically equivalent

Ans: Consider the case when p, q, r are F, T, F respectively.

Then $(p \wedge q)$ is false and $(p \wedge q) \rightarrow r$ is true

But $p \rightarrow r$ is true and $q \rightarrow r$ is false

So $(p \rightarrow r) \wedge (q \rightarrow r)$ is false.

So they are not logically equivalent

8) Show that $(p \rightarrow q) \rightarrow (r \rightarrow s)$ and $(p \rightarrow r) \rightarrow (q \rightarrow s)$ are not logically equivalent

Ans: Let p, q, r, s have truth values F, T, F, F respectively

So $(p \rightarrow q) \rightarrow (r \rightarrow s)$ has the truth value true

But $(p \rightarrow r) \rightarrow (q \rightarrow s)$ has the truth value false

So they are not equivalent

Exercises 1) Use De-Morgan's law to express the negation of

a) "Michael has a cell phone and he has a computer"

b) Charles will bicycle or run tomorrow"

2) Use De-Morgan's law to express the negation of

a) Maria walks or takes the bus to the class

b) Ibrahim is smart and hard working.

c) James is young and strong

3) Show That $\neg(p \rightarrow q) \rightarrow \neg q$ is a tautology

4) Show that $[(\neg p) \wedge (p \vee q) \rightarrow q]$ is a tautology

5) Show that $[(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)]$ is a tautology

PREDICATES AND QUANTIFIERS
Predicates:

Let us consider the statement “ x is greater than 3”. This statement has two parts. The first part the variable x , is the subject of the statement. The second part, the predicate, “is greater than 3” refers to a property that the subject of the statement can have.

We can denote the statement “ x is greater than 3” by $P(x)$ where P denotes the Predicate “is greater than 3” and x is the variable. The statement $P(x)$ is also said to be the value of the propositional function P at x . Once a value has been assigned to the variable x , the statement $P(x)$ becomes a proposition and has a truth value.

Examples: 1) Let $P(x)$ denotes the statement “ $x > 3$ ”. What are the truth values of $P(4)$ and $P(2)$? $P(4)$ is the proposition “ $4 > 3$ ”, which has the truth value T. $P(2)$ is the Proposition “ $2 > 3$ ”, which has the truth value F.

2) Let $A(x)$ denote the statement “computer x is under attack by an intruder” suppose that of the computers of the campus only CS2 and MATH1 are currently under attack by intruders what are the truth values of $A(\text{CS1})$, $A(\text{CS2})$ and $A(\text{MATH1})$?

Ans: $A(\text{CS1})$ is the proposition “computer CS1 is under attack by an intruder” so it is a false proposition. Similarly we get that $A(\text{CS2})$ is a true proposition and $A(\text{MATH1})$ is a true proposition

Remark: We can also have statements that involves more than one variable. For instance, consider a statement “ $x = y + 3$ ”. We can denote this statement by $Q(x,y)$ where x and y are variables and Q is the predicate. If values are assigned to the variables x and y , the statement $Q(x,y)$ becomes a proposition and has a truth value.

Examples :

1) Let $Q(x,y)$ denotes the statement “ $x = y + 3$ ” what are the truth values of the propositions $Q(1,2)$ and $Q(3,0)$?

Ans: $Q(1,2)$ is the proposition “ $1 = 2 + 3$ ”. which is a false proposition’

$Q(3,0)$ is the proposition “ $3 = 0 + 3$ ”, which is a true proposition

2) Let $R(x, y, z)$ denote the statement “ $x + y = z$ ” What are the truth values of the propositions $R(1, 2, 3)$ and $R(0, 0, 1)$.

Ans: $R(1, 2, 3)$ is the proposition “ $1 + 2 = 3$ ” so it is a true proposition

$R(0, 0, 1)$ is the proposition “ $0 + 0 = 1$ ” which is a false proposition

Remark : In general a statement involving n variables x_1, x_2, \dots, x_n can be denoted by $P(x_1, x_2, \dots, x_n)$. A statement of the form $P(x_1, x_2, \dots, x_n)$ is the value of the proposition at the n -tuple (x_1, x_2, \dots, x_n) and P is called the n -place predicate or n -ray predicate.

The Univesal Quantifier :

The universal quantification of $P(x)$ is the statement “ $P(x)$ for all values of x in the domain”. The notation $\forall x P(x)$ denotes the universal quantification of $P(x)$. Here \forall is called the universal quantifier we read $\forall x P(x)$ as “for all x , $P(x)$ or for every x , $P(x)$ ”. An element for which $P(x)$ is false is called a counter example of $\forall x P(x)$.

Remark: The domain of propositional function is also called as universe of discourse or domain of discourse.

Remark:

Statement	When true?	When false?
$\forall x P(x)$	P(x) is true for all values of x in the domain	There is an x for which P(x) is false

1) Let Q(x) be the statement “ $x < 2$ ” > What is the truth value of the quantifier $\forall x Q(x)$ if the domain consists of all real numbers ?

Ans: We note that that Q(3) is the proposition “ $3 < 2$ ”, which is false. ie $x = 3$ is a counter example of $\forall x Q(x)$. Hence $\forall x Q(x)$ is false.

Remark : When all the elements in the domain can be listed say x_1, x_2, \dots, x_n then the universal quantifier $\forall x P(x)$ is the same as $P(x_1) \wedge P(x_2) \wedge \dots \wedge P(x_n)$

1) What is the truth value of $\forall x P(x)$ where P(x) is the statement “ $x^2 < 10$ ” and the domain consists of the positive integers not exceeding 4.

Ans: The domain consists all integers 1,2,3 and 4 the statement $\forall x P(x)$ is the same as $P(1) \wedge P(2) \wedge P(3) \wedge P(4)$. Since P(4) is “ $4^2 < 10$ ”, which is false, we get that $\forall x P(x)$ is a false proposition.

2) What is the truth value of the statement $\forall x (x^2 \geq x)$ if the domain consists of all real numbers? What is the truth value of this statement if the domain consists of all integers?

Ans: We have $x^2 \geq x$ iff
 $x^2 - x \geq 0$ iff
 $x(x-1) \geq 0$ iff

either $x \geq 0$ and $(x-1) \geq 0$ or $x \leq 0$ and $(x-1) \leq 0$
 either $x \geq 0$ and $x \geq 1$ or $x \leq 0$ and $x \leq 1$
 either $x \geq 1$ or $x \leq 0$

case (i) Let the domain be the set or all real numbers. In this case $\forall x P(x)$ is false

$x = \frac{1}{2}$ is a counter example.

Case (ii) Let the domain be the set or all integers. In this case $\forall x P(x)$ is true.

Existential Quantifier :

The existential quantifier of P(x) is the proposition “There exists an element x in the domain such that P(x). We use the notation $\exists x P(x)$ for the existential quantification of P(x). Here \exists is called the existential quantifier.

Statement	When true?	When false?
$\exists x P(x)$	There is an x for which P(x) is true	P(x) is false for all Values of x in the domain

1) Let Q(x) be the statement “ x is less than 2”. What is the truth value of the Quantification” $\exists x Q(x)$ Where the domain consists of all real numbers

Ans: When $x = 1$, the propositional function Q(x) is “ $1 < 2$ ” which is a true proposition
 $\therefore \exists x P(x)$ is true.

2) Let Q(x) be the statement “ $x = x+1$ ” What is the truth value of $\exists x Q(x)$ where the domain consists of all real numbers.

Ans : For all values of x in the domain Q(x) is false . There fore $\exists x P(x)$ is a false proposition.

Remark : When all the elements in the domain can be listed say x_1, x_2, \dots, x_n then the existential quantifier $\exists x P(x)$ is the same as the disjunction

$P(x_1) \vee P(x_2) \vee \dots \vee P(x_n)$ because the disjunction is true if and only if atleast one of $P(x_1), P(x_2), \dots, P(x_n)$ is true

1) What is the truth value of the statement $\exists x P(x)$ where P(x) is “ $x^2 > 10$ ” and the universe of discourse consists of positive integers not exceeding 4 .

Ans: P(4) is “ $4^2 > 10$ ” which is true. $\therefore \exists x P(x)$ is a true proposition

2) Let P(x) be the statement “ $x = x^2$ ”. If the domain consists of the integers. What are the truth values of the following propositions

- (i) P(0) (ii) P(1) (iii) P(2) (iv) P(-1) (v) $\forall x P(x)$ (vi) $\exists x P(x)$

Ans: (i) P(0) is “ $0 = 0^2$ ” which is true. Therefore the truth value of P(0) is T

(ii) P(1) is “ $1 = 1^2$ ” which is true . Therefore truth value of P(1) is T

(iii) The truth value of P(2) is F because P(2) is “ $2 = 2^2$ ” which is a false proposition.

(iv) P(-1) is a false proposition

(v) $\forall x P(x)$ is a false proposition since $x = 2$ is a counter example.

(vi) $\exists x P(x)$ is a true proposition

3) Determine the truth value of each of the following propositions if the domain consists all the real numbers

(i) $\exists x (x^2 = 2)$ (ii) $\exists x (x^2 = -1)$ (iii) $\forall x (x^2 + 2 \geq 1)$ (iv) $\forall x (x^2 \neq x)$

- Ans: (i) $\exists x (x^2 = 2)$ is a true proposition
 (ii) $\exists x (x^2 = -1)$ is a false proposition
 (iii) $\forall x (x^2 + 2 \geq 1)$ is a true proposition
 (iv) $\forall x (x^2 \neq x)$ is a false proposition

Exercise: 1) Let $Q(x)$ be “ $x+1 > 2x$ ” If the domain is the set of all integers what are the truth values of the propositions $Q(0)$, $Q(-1)$, $Q(2)$, $\exists x Q(x)$ and $\forall x Q(x)$

2) Determine the truth value of each of the following statements, if the domain is the set of all integers

$$\forall n(n+1 > n) , \exists n(2n = 3n) ; \exists n(n = -n); \forall n(n^2 \geq n)$$

3) Determine the truth value of each of the following propositions if the domain consists all the real numbers.

$$\exists x (x^3 = -1); \exists x (x^4 < x^2) ; \forall x((-x)^2 = x^2) \text{ and } \forall x(2x > x)$$

4) Determine the truth value of each of the following propositions, if the domain is the set of all integers

$$\forall n(n^2 \geq 0) , \exists n(n^2 = 2) \text{ and } \exists n(n^2 < 0)$$

Quantifiers with restricted domain :

1) What does the statement $\forall x < 0 (x^2 > 0)$ means when the domain is the set of real numbers

Ans: $\forall x < 0 (x^2 > 0)$ states that “ for every real number x with $x < 0$, we have $x^2 > 0$ ” ie it states that the square of a negative real number is positive. This statement is same as $\forall x (x > 0 \rightarrow x^2 > 0)$

2) What does the statement $\forall y \neq 0 (y^3 \neq 0)$ mean where the domain is the set of all real numbers

Ans: The statement $\forall y \neq 0 (y^3 \neq 0)$ states that “ for every real number y , if $y \neq 0$, $y^3 \neq 0$. It states that the cube of every nonzero real number is nonzero. This statement is the same as $\forall y (y \neq 0 \rightarrow y^3 \neq 0)$

3) What does the statement $\exists z > 0 (z^2 = 2)$ mean if the domain is the set of all real numbers.

Answer: The statement $\exists z > 0 (z^2 = 2)$ states that “ there exists a real number z with $z > 0$ such that $z^2 = 2$ ” . ie it states “ there is positive square root of 2”

This statement is same “ $\exists z (z > 0 \wedge z^2 = 2)$ ”

Remark: The restriction of a universal quantification is the same as the universal quantification of a conditional statement. On the other hand, the restriction of an existential quantification is the same as the existential quantification of a conjunction.

Precedence Of Quantifiers

The quantifiers \forall and \exists have higher precedence than all logical operators from the propositional calculus. For example $\forall xP(x) \vee Q(x)$ is the disjunction of $\forall xP(x)$ and $Q(x)$. In other words it means $(\forall xP(x)) \vee Q(x)$ rather than $\forall x(P(x) \vee Q(x))$

Binding Variables:

When a quantifier is used on the variable x we say that the occurrence of the variable is bound. An occurrence of a variable which is not bound nor set equal to a particular value is said to be a free variable.

The part of the logical expression to which the quantifier is applied is called the scope of the quantifier.

Example: Consider $\exists x(x+y=1)$. Here the variable x is bound by the existential quantifier \exists . But the variable y is free because it is not bound by a quantifier and no value is assigned to y .

Logical Equivalences involving Quantifiers

Statements involving predicates and quantifiers are logically equivalent if and only if they have the same truth value, no matter which predicates are substituted in to these statements and which domain is used for the variables in these propositional functions we use the notation $S \equiv T$ to indicate two statements S and T involving predicates and and quantifiers are logically equivalent. I show that $\forall x(P(x) \wedge Q(x))$ and $\forall xP(x) \wedge \forall xQ(x)$ are logically equivalent.

Answer : Let us call the statement $\forall x(P(x) \wedge Q(x))$ as S and $\forall xP(x) \wedge \forall xQ(x)$ as T . We can show that S and T are logically equivalent by doing two cases . First we show that if S is true then T is true. Second we show that if T is true then S is true.

Case (i) : Assume that S is true. ie $\forall x(P(x) \wedge Q(x))$ is true

ie, if a is in the domain $P(a) \wedge Q(a)$ is true

ie, if a is in the domain $P(a)$ is true and $Q(a)$ is true

ie , $\forall xP(x)$ is true and $\forall xQ(x)$ is true

ie, $\forall xP(x) \wedge \forall xQ(x)$ is true

ie T is true

Case (ii) Assume that S is true

ie , $\forall xP(x) \wedge \forall xQ(x)$ is true

ie $\forall xP(x)$ is true and $\forall xQ(x)$ is true

ie, if a is in the domain $P(a)$ is true and $Q(a)$ is true

ie, if a is in the domain $P(a) \wedge Q(a)$ is true

ie $\forall x(P(x) \wedge Q(x))$ is true

ie S is true

So we can say that $S \equiv T$

ie, $\forall x(P(x) \wedge Q(x))$ and $\forall xP(x) \wedge \forall xQ(x)$ are logically equivalent.

Exercise

- 1) Verify whether $\forall x(P(x) \vee Q(x))$ and $\forall xP(x) \vee \forall xQ(x)$ are logically Equivalent or not
- 2) Show that $\exists x(P(x) \vee Q(x))$ and $\exists xP(x) \vee \exists xQ(x)$ are logically equivalent
- 3) Show that $\exists x(P(x) \wedge Q(x))$ and $\exists xP(x) \wedge \exists xQ(x)$ are logically equivalent

Negating quantified expression

- 1) Show that $\neg \forall x P(x) \equiv \exists x \neg P(x)$

Proof: $\neg \forall x P(x)$ is true iff

$\forall x P(x)$ is false iff

There is a value of x in the domain for Which $P(x)$ is false iff

There is a value of x in the domain for Which $\neg P(x)$ is true iff

$\exists x \neg P(x)$ is true

Hence $\neg \forall x P(x) \equiv \exists x \neg P(x)$

- 2) Show that $\neg \exists x P(x) \equiv \forall x \neg P(x)$

Proof: $\neg \exists x P(x)$ is true iff

$\exists x P(x)$ is false iff

$P(x)$ is false for all values of x in the domain iff

$\neg P(x)$ is true for all values of x in the domain iff

$\forall x \neg P(x)$ is true.

Hence $\neg \exists x P(x) \equiv \forall x \neg P(x)$

Remark: The above rules of negation for quantifiers are called De-Morgan's laws of quantifiers.

- 1) What is the negation of the statement "there is an honest politician"

Answer: Let $P(x)$ be the propositional function "The politician x is honest"

The given statement is $\exists x P(x)$. By De-Morgan's law we have

$$\neg \exists x P(x) \equiv \forall x \neg P(x).$$

$\neg P(x)$ is "The politician x is dishonest"

Therefore the required negation is "All politicians are dishonest"

- 2) What is the negation of the statement "All Americans eat burgers"

Answer: Let $P(x)$ be the propositional function "x eat burgers" where the domain is the set of all Americans.

\therefore the given statement is $\forall x P(x)$

We know that $\neg \forall x P(x) \equiv \exists x \neg P(x)$

$\neg P(x)$ is x does not eat burgers

Therefore the required negation is there is an American who does not eat burgers

3) What are the negation of the statements $\forall x(x^2 > x)$ and $\exists x(x^2 = 2)$

$$\begin{aligned}\text{Ans: } \neg \forall x(x^2 > x) &\equiv \exists x \neg(x^2 > x) \\ &\equiv \exists x(x^2 \leq x) \\ \neg \exists x(x^2 = 2) &\equiv \forall x \neg(x^2 = 2) \\ &\equiv \forall x(x^2 \neq 2)\end{aligned}$$

4) Show that $\neg \forall x(P(x) \rightarrow Q(x))$ and $\exists x(P(x) \wedge \neg Q(x))$ are logically equivalent

$$\begin{aligned}\text{Proof: } \neg \forall x(P(x) \rightarrow Q(x)) &\equiv \exists x \neg(P(x) \rightarrow Q(x)) \\ &\equiv \exists x(P(x) \wedge \neg Q(x))\end{aligned}$$

5) Express the statement “Every student in this class has studied calculus” using Predicates and quantifiers

Ans: Let us take the domain as the set of all students in this class. Let $C(x)$ be “x has studied calculus”. \therefore The given statement is $\forall x C(x)$

6) Let $P(x)$ be the statement “x spends more than 5 hours every week day in class” where the domain consists of all students. Express the following quantifiers in simple English.

$$(i) \exists x P(x) \quad (ii) \forall x P(x) \quad (iii) \exists x \neg P(x) \quad (iv) \forall x \neg P(x)$$

Answers : (i) $\exists x P(x)$; There is a student in this class who spends more than 5 hours every week day in class

(ii) $\forall x P(x)$; All students in this class spend more than 5 hours in class

(iii) $\exists x \neg P(x)$: There is a student in this class who does not spend more than 5 hours every week day in the class

(iv) $\forall x \neg P(x)$: No student in this class spend more than 5 hours every week day in the class.

MODULE 4

BASIC LOGIC 2

RULES OF INFERENCE

Definition :

An argument in propositional logic is a sequence of propositions. All but the final proposition in the argument are called premises and the final proposition is called the conclusion. An argument is valid if the truth of all its premises imply that the conclusion is True. An argument form in a propositional logic is a sequence of compound propositions involving propositional variables. An argument form is valid if no matter which particular propositions are substituted for the propositional variables, the conclusion is true if all the premises are true.

Remark: The argument form Premises P_1, P_2, \dots, P_n and conclusion q is valid

$$(P_1 \wedge P_2 \wedge \dots \wedge P_n) \rightarrow q \text{ is a tautology.}$$

Law of detachment or modulus ponens

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

Proof:

p	Q	$p \rightarrow q$	$(p \rightarrow q) \wedge p$	$((p \rightarrow q) \wedge p) \rightarrow q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Remark: A valid argument can lead to an incorrect conclusion if one or more premises become false. The following is one such example'

If $2+3 = 9$ then $5 = 10$

$$\begin{array}{l} 2+3=9 \\ \hline \therefore 5=10 \end{array}$$

Here the argument is valid by modus ponens. But the conclusion is wrong.

Modus tollens

$$\begin{array}{l} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$$

Addition

$$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$$

Hypothetical syllogism

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$$

Simplification

$$\begin{array}{l} p \wedge q \\ \hline \therefore q \end{array}$$

Disjunctive syllogism

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

Resolution

$$\begin{array}{l} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$$

Conjunction

$$\begin{array}{l} p \\ q \\ \hline \therefore p \wedge q \end{array}$$

Examples 1) Consider the following argument ‘If it snows today, then we will go skiing. It is snowing today therefore we will go for skiing’. Is the above argument valid? Why?

Ans: Let P be the proposition “ it snows today” . Let q be “we will go skiing”
Then the given argument has the form

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

This is a valid argument form by modus ponens

Therefore the given argument is valid

2) Determine whether the argument given here is valid and determine whether its conclusion is true. “If $\sqrt{2} > 3/2$ then $(\sqrt{2})^2 > (\frac{3}{2})^2$, we know that $\sqrt{2} > 3/2$. Consequently

$$(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}”$$

Let P be the proposition “ $\sqrt{2} > 3/2$ ” and q be $(\sqrt{2})^2 > (\frac{3}{2})^2$ then given argument has the form

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

This is a valid argument form by modus ponens so the given argument is valid. However the conclusion is false. (Note that the second premise is false)

- 3) State which rule of inference is the basis of the following argument?
 “It is below freezing now. Therefore it is either below freezing or snowing now”

Ans: Let p be the proposition “it is below freezing now” and q “ it is snowing now”

Then the argument has the form $\frac{p}{\therefore p \vee q}$

This is an argument which uses the addition rule.

- 4) Show that the hypothesis “It is not sunny this afternoon and it is colder than yesterday”. : “we will go swimming only if it is sunny”. “If we don’t go swimming then we will take a boat trip and “If we take a boat trip then we will be home by sun set”. Leads to the conclusion “we will be home by sunset”

- Ans: p: It is sunny this afternoon
 q: It is colder than yesterday
 r: We will go swimming .
 s: We will take a boat trip
 t: We will be home at sun set

Then the hypothesis become $\neg p \wedge q, r \rightarrow p, \neg r \rightarrow s, s \rightarrow t$ and the conclusion is t we need to give a valid argument with this hypothesis and conclusion We construct an argument to show that our hypothesis leads to the desired conclusion as follows

	Step	Reason
1	$\neg p \wedge q$	Hypothesis
2	$\neg p$	Simplification using 1
3	$r \rightarrow p$	Hypothesis
4	$\neg r$	Modulus tollens using 2 and 3
5	$\neg r \rightarrow s$	Hypothesis
6	s	Modulus ponens using 4 and 5
7	$s \rightarrow t$	Hypothesis
8	t	Modulus ponens using 6 and 7

5) Show that the hypothesis “if you send me an e-mail message the I will finish writing the programme”. “ If you don’t send me an e-mail message then I will go to sleep early ‘ and “If I sleep yearly then I wake up feeling refresh” . Leads to the conclusion. “If don’t finish writing the programme then I wake up feeling refresh”

Answer: Suppose

- p : You send me an e-mail message
- q: I will finish writing the programme
- r: I will go to sleep yearly
- s : I wake up feeling refresh

Then the hypothesis become $p \rightarrow q, \neg p \rightarrow r, r \rightarrow s$ and the conclusion is $\neg q \rightarrow s$. We construct an argument which leads to the conclusion as follows

	Step	Reason
1	$p \rightarrow q$	Hypothesis
2	$\neg q \rightarrow \neg p$	Contrapositive of 1
3	$\neg p \rightarrow r$	Hypothesis
4	$\neg q \rightarrow r$	Hypothetical syllogism using 2 and 3
5	$r \rightarrow s$	Hypothesis
6	$\neg q \rightarrow s$	Hypothetical syllogism using 4 and 5

Show that the hypothesis $(p \wedge q) \vee r$ and $r \rightarrow s$ imply the conclusion $q \vee s$

	Step	Reason
1	$(p \wedge q) \vee r$	Hypothesis
2	$(p \vee r) \wedge (q \vee r)$	Distributive law
3	$q \vee r$	Simplification using 2
4	$r \rightarrow s$	Hypothesis
5	$\neg r \vee s$	$r \rightarrow s \equiv \neg r \vee s$
6	$q \vee s$	Resolution using 3 and 5

Fallacies : Several fallacies arise in incorrect arguments . These fallacies resemble rules of inference , but are base on contingencies rather than tautologies.

Fallacy of affirming the conclusion:

Consider the following argument

$$\begin{array}{l} p \rightarrow q \\ q \\ \hline \therefore p \end{array}$$

This is not a valid argument because $((p \rightarrow q) \wedge q) \rightarrow p$ is not a tautology.

However there are many incorrect arguments which treat this as a tautology. This type of incorrect reasoning is called the fallacy of the affirming conclusion.

Example: Is the following arguments valid?

If you do every problem in this book then you will learn discrete mathematics”

“You learned discrete mathematics” Therefore you did every problem in this book”

Ans: Let p: You did every problem in this book Let q: you learned discrete mathematics
Then the given argument has the form

$$\begin{array}{l} p \rightarrow q \\ q \\ \hline \therefore p \end{array}$$

This is the fallacy of affirming the conclusion. Therefore the given argument is not valid.

Fallacy of denying the hypothesis :

Consider the following argument

$$\begin{array}{l} p \rightarrow q \\ \neg p \\ \hline \therefore \neg q \end{array}$$

This is not a valid argument because $((p \rightarrow q) \wedge \neg p) \rightarrow \neg q$ is not a tautology. Many incorrect argument use this as a rule of inference this type of incorrect reasoning is called fallacy of denying the hypothesis.

Example: Is the following argument valid?

“If you do every problem in this book then you will learn discrete mathematics”

“ You did not do every problem in this book” therefore you did not learn discrete mathematics

Ans: Let p: you do every problem in this book

q: you learn discrete mathematics

The given argument has the form

$$\begin{array}{l} p \rightarrow q \\ \neg p \\ \hline \therefore \neg q \end{array}$$

This is the fallacy of denying the hypothesis. \therefore The given argument is not valid.

Rules of inference for quantified statements :

Rule of inference	Name
$\frac{\forall x P(x)}{\therefore p(c)}$	Universal instantiation
$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$	Universal generalisation
$\frac{\exists x P(x)}{P(c) \text{ for some element } c}$	Existential instantiation
$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$	Existential generalisation

1 Show that the premises “ Everyone in mathematics class has taken a course in computer science “ and “Marla is a student in this class” imply the conclusion “ Maria has taken a course in computer science”

Ans: Let $D(x)$ denotes “ x is a student in mathematics class” and $C(x)$ denote x has taken a course in computer science” . Then the premises are $\forall x(D(x) \rightarrow C(x))$ and $D(\text{Marla})$ ’ The conclusion is $C(\text{Marla})$

The following steps can be used to establish the conclusion from the premises

	Step	Reason
1	$\forall x(D(x) \rightarrow C(x))$	Premises
2	$D(\text{Marla}) \rightarrow C(\text{marla})$	Universal instantiation
3	$D(\text{Marla})$	Premises
4	$C(\text{Marla})$	Modulus ponens using 2 and 3

Introduction to proofs

Some terminology : A theorem is a statement that can be shown to be true. Less important theorems are sometimes called propositions. Theorems are sometimes referred to as facts or results. We demonstrate that a theorem is true with a proof. A proof is a valid argument that establishes the truth of a theorem. A less important theorem that is helpful in the proof of other results is called a lemma. A corollary is a theorem that can be established directly from a theorem that has been proved. A conjecture is a statement that is being proposed to be a true statement on the basis of some practical evidence or the intuition of an expert.

Methods of Proving theorems

To prove the theorem of the form $\forall x(P(x) \rightarrow Q(x))$ our goal is to show that $P(c) \rightarrow Q(c)$ is true where c is an arbitrary element in the domain and then apply Universal generalization.

Direct Proof:

A direct proof of a conditional statement $p \rightarrow q$ is constructed as follows

The first step is the assumption that p is true. Subsequent steps are constructed using rules of inference, with the final step showing that q must be true.

A direct proof shows that a conditional statement $p \rightarrow q$ is true. If p is true then q is true. So the combination of p true and q false never occurs. In a direct proof we assume that p is true and use axioms, definitions, and previously proven theorems together with rules of inference to show that q must also be true.

1) Give a direct proof to the theorem ‘ if n is an odd integer the n^2 is an odd integer’

Ans: we note that the theorem states that $\forall n(P(n) \rightarrow Q(n))$ where $P(n)$ is ‘ n is an odd integer’ and $Q(n)$ is ‘ n^2 is an odd integer’ . We prove $P(n) \rightarrow Q(n)$ is true and apply universal generalization.

We assume that the hypothesis is true ie $P(n)$ is true

ie n is an odd integer

ie, $n = 2k + 1$ where k is an integer

By squaring both sides we get

$$n^2 = (2k + 1)^2$$

$$\text{ie, } n^2 = 4k^2 + 4k + 1$$

$$\text{ie, } n^2 = 2(2k^2 + 2k) + 1$$

$$\text{ie, } n^2 = 2k' + 1 \text{ where } k' = 2k^2 + 2k, \text{ which is an integer}$$

$\therefore n^2$ is an odd integer

ie, $Q(n)$ is true

Hence $P(n) \rightarrow Q(n)$ is true.\

Therefore by universal generalization $\forall n(P(n) \rightarrow Q(n))$ is true

2) Give a direct proof of the fact that ‘ if m and n are both perfect squares then mn is a perfect square’

Ans: We note that the theorem says that $\forall m, n (P(m, n) \rightarrow Q(m, n))$ where $P(m, n)$ both m and n are perfect squares and $Q(m, n)$ is 'mn is a perfect square'. We prove $P(m, n) \rightarrow Q(m, n)$ is true and apply universal generalization. We assume the hypothesis is true.

ie, $P(m, n)$ is true

ie m and n are perfect squares.

ie $m = x^2$ where x is an integer $n = y^2$ where y is an integer

by multiplying we get $mn = x^2 y^2$

ie $mn = (xy)^2$

ie mn is a perfect square

ie $Q(m, n)$ is true

Hence $P(m, n) \rightarrow Q(m, n)$ is true

\therefore by universal generalization $\forall m, n (P(m, n) \rightarrow Q(m, n))$ is true.

Indirect proof : The proofs that don't start with the hypothesis and end with the conclusion are called indirect proofs.

Proof by contraposition : This is an extremely useful type of indirect proof. Proofs by contraposition make use of the fact that the conditional statement $p \rightarrow q$ is equivalent to its contrapositive $\neg q \rightarrow \neg p$. This means that $p \rightarrow q$ can be proved by showing that its contrapositive $\neg q \rightarrow \neg p$ is true.

In a proof by contraposition of $p \rightarrow q$ we take $\neg q$ as a hypothesis and using axioms. Definitions previously proven theorems together with rules of inferences we prove $\neg p$ is true

1) Prove that for an integer n "if $3n + 2$ is odd then n is odd".

Ans: We try a proof by contraposition.

The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "if $3n + 2$ is odd then n is odd" is false.

ie, assume that n is not odd.

ie, n is even

ie $n = 2k$ where k is an integer

Multiply both sides by 3 we get $3n = 6k$

Adding 2 on both sides we get $3n + 2 = 6k + 2$

ie, $3n + 2 = 2(3k + 1)$

$\therefore 3n + 2$ is an even integer

ie $3n + 2$ is not odd

This is the negation of the hypothesis of the theorem

\therefore The given conditional statement is true.

2) Prove that for positive integers a and b "If $n = ab$ then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ "

We try to prove by contraposition.

Assume that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ is false

ie $a > \sqrt{n}$ and $b > \sqrt{n}$

$\therefore ab > \sqrt{n}\sqrt{n}$

ie $ab > n$

ie $ab \neq n \quad \therefore ab = n$ is false,

So we get the hypothesis of the conditional statement is false

\therefore by the method of contraposition the given theorem holds.

Vacuous proof:

We can quickly prove a conditional statement or $p \rightarrow q$ to be true when we know that p is false. Consequently If we can show that p is false, then we have a proof called a vacuous proof of a conditional statement $p \rightarrow q$. Vacuous proofs are often used to establish special case of theorems.

Example: Show that $p(0)$ is true when $P(n)$ is "If $n > 1$, $n^2 > n$ " and the domain is the set of all integers.

Ans: We note that $P(0)$ is "If $0 > 1$, $0^2 > 0$ " $P(0)$ is true by vacuous proof because the hypothesis $0 > 1$ is false.

Trivial proof: A proof of $p \rightarrow q$ which uses the fact that q is true is called a trivial proof.

Example: Let $P(n)$ be "for positive integers a and b if $a \geq b$ then $a^n \geq b^n$ " and the domain consists of all the integers show that $P(0)$ is true

Ans: We note that $P(0)$ is "if $a \geq b$ then $a^0 \geq b^0$ "

ie "if $a \geq b$ then $1 \geq 1$ the conclusion of this statement $1 \geq 1$ is always true

$\therefore P(0)$ is true using trivial proof.

Proof by Contradiction

Suppose that we want to prove that a statement p is true. Furthermore suppose that we can find a contradiction F such that $\neg p \rightarrow F$ is true. Then we can conclude that $\neg p$ is false, which means P is true.

The statement $r \wedge \neg r$ is a contradiction, whenever r is a proposition. we can prove that P is true, if we can show that $\neg p \rightarrow (r \wedge \neg r)$ is true.

Proofs of this type are called proofs by contradiction.

1) Show that atleast four of any 22 days must fall on the same day of the week.

Ans: Let p be the Proposition "atleast four of any 22 days must fall on the same day of the week". Suppose that $\neg P$ is true.

ie atleast 3 days of any 22 days fall on the same day of the week.

Since there are 7 days of the week, this implies that atleast 21 days could have been chosen,. This contradicts the hypothesis that we have 22 days under consideration. ie if r is the statement "22 days are chosen" then we have shown that $\neg p \rightarrow (r \vee \neg r)$ is true. Consequently P is true.

1) Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

Ans: Let P be the proposition “ $\sqrt{2}$ is irrational”

To start a proof by contradiction, we assume that $\neg p$ is true

ie,; $\sqrt{2}$ is rational

ie,; $\sqrt{2} = \frac{a}{b}$ where a and b are integers $b \neq 0$ a,b have no common factors.

then $\sqrt{2}b = a$ ie $a^2 = 2b^2$ (1)

$\Rightarrow a^2$ is even

$\Rightarrow a$ is even

ie $a = 2k$ where k is an integer

$$a^2 = 4k^2$$

Substituting in (1) we get $4k^2 = 2b^2$

ie $b^2 = 2k^2$

$\Rightarrow b^2$ is even

$\Rightarrow b$ is even

So we get both a and b are even

Let r be the statement “ a nd b have no common factor”

Thus we have shown that $\neg p \rightarrow (r \vee \neg r)$ is true

Consequently, p must be true.

Proofs of equivalence ;

To prove a theorem which is a bi-conditional statement ie a statement of the form $p \leftrightarrow q$ we show that both $p \rightarrow q$ and $q \rightarrow p$ are true.

1) Prove the theorem “for a positive integer n, n is odd if and only if n^2 is odd”

Ans: Let P be the proposition “n is odd” and q be the proposition “ n^2 is odd”

We want to prove that $p \leftrightarrow q$.

First we prove that $p \rightarrow q$ is true

we attempt a direct proof.

Let n be odd

ie $n = 2k+1$ where k is an integer $\therefore n^2 = (2k+1)^2$

ie $n^2 = 4k^2 + 4k + 1$

ie $n^2 = 2(2k^2 + 2k) + 1$

ie n^2 is odd.

Next we prove $q \rightarrow p$ is true, we attempt a proof by contraposition. Assume that $\neg p$ is true ie; n is even

ie $n = 2k$ where k is an integer

$\therefore n^2 = 4k^2$ ie $n^2 = 2(2k^2)$

$\Rightarrow n^2$ is even. Thus we get that $\neg q$ is true. By method of contraposition $q \rightarrow p$ is true. hence by proof of equivalence $p \leftrightarrow q$ is true.

2) Show that the following statements about the integer n are equivalent.

$p_1 : n$ is even $p_2 : n-1$ is odd $p_3 : n^2$ is even.

Ans: First we assume that $p_1 \rightarrow p_2$

Assume that n is even

ie; $n = 2k$ where k is integer

$$n-1 = 2k-1$$

$\Rightarrow n-1$ is odd

Thus we have proved that $p_1 \rightarrow p_2$

next we prove that $p_2 \rightarrow p_3$

Assume that $n-1$ is odd

Then $n-1 = 2k+1$ where k is an integer

$$\text{ie } n = 2k+2 \quad \therefore n^2 = 4k^2 + 8k + 4$$

$$\text{ie } n^2 = 2(2k^2 + 4k + 2)$$

ie n^2 is even. Thus we have proved $p_2 \rightarrow p_3$ is true.

Finally we prove $p_3 \rightarrow p_1$ is true.

We prove this by method of contraposition.

Assume that n is odd ie $n = 2k+1$ where k is an integer

$$n^2 = 4k^2 + 4k + 1 \quad \text{ie } n^2 = 2(2k^2 + 2k) + 1$$

$\Rightarrow n^2$ is odd

$\therefore p_3 \rightarrow p_1$

Exhaustive proof:

Some theorems can be proved by examining a relatively small number of examples. Such proofs are called exhaustive proofs.

Example : Prove that $(n+1)^2 \geq 3^n$, if n is a positive integer less than or equal to 2

Ans: we use an exhaustive proof

$$\text{Let } n=1. \text{ Then } (n+1)^2 \geq 3^n \text{ becomes } (1+1)^2 \geq 3^1$$

ie $4 \geq 3$ which is true

$$\text{Let } n=2 \text{ Then } (n+1)^2 \geq 3^n \text{ becomes } (2+1)^2 \geq 3^2$$

ie $9 \geq 9$ Which is true

Proof by cases :

A proof by cases must cover all possible cases that arise in a theorem

Example: Prove that 'If n is an integer then $n^2 \geq n$.

We prove that $n^2 \geq n$ by considering three cases namely $n=0$, n is a positive integer and n is a negative integer.

case (i): Let $n=0$

Then the inequality $n^2 \geq n$ becomes $0 \geq 0$ which is true

case (ii) Let n be a positive integer then $n > 1$

Multiplying both sides by the positive integer n

$$n.n \geq n.1 \quad \text{ie } n^2 \geq n$$

case (iii) Let n be a negative integer

Then $n \leq -1$

But we have $n^2 \geq 0$

Clearly $n^2 \geq -1 \geq n$

$n^2 \geq n$ is true.

Existence Proofs:

A proof of a proposition $\exists x P(x)$ is called an existence proof. Sometimes an existence proof of $\exists x P(x)$ can be given by finding an element 'a' such that $P(a)$ is true. Such proofs are called non constructive existence proofs.

1) Show that there is a positive integer that can be written as the sum of the cubes of positive integers in two different ways.

Answer: Consider the positive integer 1729.

We observe that $1729 = 12^3 + 1^3$ as well as $1729 = 10^3 + 9^3$

\therefore 1729 is such a positive integer.

2) Show that there exists irrational numbers x and y such that x^y is rational

Ans: Take $x = \sqrt{2}$ and $y = \sqrt{2}$ Then $x^y = (\sqrt{2})^{\sqrt{2}}$. If $(\sqrt{2})^{\sqrt{2}}$ is rational then the theorem is true. If $(\sqrt{2})^{\sqrt{2}}$ is irrational take $x = (\sqrt{2})^{\sqrt{2}}$ and $y = \sqrt{2}$ then $x^y = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$ Which is rational

Hence The theorem is true.

Remark: The first problem is an example of a constructive existence proof and the second one is a non-constructive existence proof.

