SYLLABUS

UNIT -I:
Mathematical Logic:
Propositional Calculus: Statements and Notations, Connectives, Well Formed Formulas, Truth Tables, Tautologies, Equivalence of Formulas, Duality Law, Tautological Implications, Normal Forms, Theory of Inference for Statement Calculus, Consistency of Premises, Indirect Method of Proof. Predicate Calculus:Predicative Logic, Statement Functions, Variables and Quantifiers, Free and Bound Variables, Inference Theory for Predicate Calculus.

UNIT -II:
Set Theory:
Introduction, Operations on Binary Sets, Principle of Inclusion and Exclusion, *Relations:* Properties of Binary Relations, Relation Matrix and Digraph, Operations on Relations, Partition and Covering, Transitive Closure, Equivalence, Compatibility and Partial Ordering Relations, Hasse Diagrams, *Functions:* Bijective Functions, Composition of Functions, Inverse Functions, Permutation Functions, Recursive Functions, Lattice and its Properties.

UNIT- III:
Algebraic Structures and Number Theory:
Algebraic Structures: Algebraic Systems, Examples, General Properties, Semi Groups and Monoids, Homomorphism of Semi Groups and Monoids, Group, Subgroup, Abelian Group, Homomorphism, Isomorphism, *Number Theory:* Properties of Integers, Division Theorem, The Greatest Common Divisor, Euclidean Algorithm, Least Common Multiple, Testing for Prime Numbers, The Fundamental Theorem of Arithmetic, Modular Arithmetic (Fermat's Theorem and Euler's Theorem)

UNIT -IV:
Combinatorics:
Basic of Counting, Permutations, Permutations with Repetitions, Circular Permutations, Restricted Permutations, Combinations, Restricted Combinations, Generating Functions of Permutations and Combinations, Binomial and Multinomial Coefficients, Binomial and Multinomial Theorems, The Principles of Inclusion–Exclusion, Pigeonhole Principle and its Application.

UNIT -V:
Recurrence Relations:
Generating Functions, Function of Sequences, Partial Fractions, Calculating Coefficient of Generating Functions, Recurrence Relations, Formulation as Recurrence Relations, Solving Recurrence Relations by Substitution and Generating Functions, Method of Characteristic Roots, Solving Inhomogeneous Recurrence Relations

UNIT -VI:
Graph Theory:
Basic Concepts of Graphs, Sub graphs, Matrix Representation of Graphs: Adjacency Matrices, Incidence Matrices, Isomorphic Graphs, Paths and Circuits, Eulerian and

Hamiltonian Graphs, Multigraphs, Planar Graphs, Euler's Formula, Graph Colouring and Covering, Chromatic Number, Spanning Trees, Algorithms for Spanning Trees (Problems Only and Theorems withou*t* Proofs).

TEXT BOOKS:

1.Discrete Mathematical Structures with Applications to Computer Science,J. P.Tremblay and P. Manohar,Tata McGraw Hill.
2. Elements of Discrete Mathematics-A Computer Oriented Approach, C. L. Liu and D. P. Mohapatra, 3rdEdition, Tata McGraw Hill.
3. Discrete Mathematics and its Applications with Combinatorics and Graph Theory, K. H. Rosen, 7th Edition, Tata McGraw Hill.

REFERENCE BOOKS:

1. Discrete Mathematics for Computer Scientists and Mathematicians, J. L. Mott, A. Kandel, T.P. Baker, 2nd Edition, Prentice Hall of India.
2. Discrete Mathematical Structures, BernandKolman, Robert C. Busby, Sharon Cutler Ross, PHI.
3. Discrete Mathematics, S. K. Chakraborthy and B.K. Sarkar, Oxford, 2011.

Unit – I

Mathematical Logic

INTRODUCTION

Proposition: A **proposition** or **statement** is a declarative sentence which is either true or false but not both. The truth or falsity of a proposition is called its **truth-value.**

These two values 'true' and 'false' are denoted by the symbols *T* and *F* respectively. Sometimes these are also denoted by the symbols 1 and 0 respectively.

Example 1: Consider the following sentences:

1. Delhi is the capital of India.
2. Kolkata is a country.
3. 5 is a prime number.
4. 2 + 3 = 4.

These are propositions (or statements) because they are either true of false.

Next consider the following sentences:

5. How beautiful are you?
6. Wish you a happy new year
7. $x + y = z$
8. Take one book.

These are not propositions as they are not declarative in nature, that is, they do not declare a definite truth value *T* or *F*.

Propositional Calculus is also known as **statement calculus.** It is the branch of mathematics that is used to describe a logical system or structure. A logical system consists of (1) a universe of propositions, (2) truth tables (as axioms) for the logical operators and (3) definitions that explain equivalence and implication of propositions.

Connectives

The words or phrases or symbols which are used to make a proposition by two or more propositions are called **logical connectives** or **simply connectives.** There are five basic connectives called negation, conjunction, disjunction, conditional and biconditional.

Negation

The **negation** of a statement is generally formed by writing the word 'not' at a proper place in the statement (proposition) or by prefixing the statement with the phrase 'It is not the case that'. If *p* denotes a statement then the negation of *p* is written as *p* and read as 'not *p*'. If the truth value of *p* is *T* then the truth value of *p* is *F*. Also if the truth value of *p* is *F* then the truth value of *p* is *T*.

Table 1. Truth table for negation

p	¬p
T	F
F	T

Example 2: Consider the statement *p*: Kolkata is a city. Then ¬p: Kolkata is not a city.

Although the two statements 'Kolkata is not a city' and 'It is not the case that Kolkata is a city' are not identical, we have translated both of them by *p*. The reason is that both these statements have the same meaning.

Conjunction

The **conjunction** of two statements (or propositions) *p* and *q* is the statement $p \wedge q$ which is read as '*p* and *q*'. The statement $p \wedge q$ has the truth value *T* whenever both *p* and *q* have the truth value *T*. Otherwise it has truth value *F*.

Table 2. Truth table for conjunction

p	q	$p \wedge q$
T	*T*	*T*
T	*F*	*F*
F	*T*	*F*
F	*F*	*F*

Example 3: Consider the following statements *p* : It is raining today.

q : There are 10 chairs in the room.

Then $p \wedge q$: It is raining today and there are 10 chairs in the room.

Note: Usually, in our everyday language the conjunction 'and' is used between two statements which have some kind of relation. Thus a statement 'It is raining today and 1 + 1 = 2' sounds odd, but in logic it is a perfectly acceptable statement formed from the statements 'It is raining today' and '1 + 1 = 2'.

Example 4: Translate the following statement:

'Jack and Jill went up the hill' into symbolic form using conjunction.

Solution: Let p : Jack went up the hill, q : Jill went up the hill.

Then the given statement can be written in symbolic form as $p \wedge q$.

Disjunction

The **disjunction** of two statements p and q is the statement $p \vee q$ which is read as 'p or q'. The statement $p \vee q$ has the truth value F only when both p and q have the truth value F. Otherwise it has truth value T.

Table 3: Truth table for disjunction

p	q	$p \vee q$
T	*T*	*T*
T	*F*	*T*
F	*T*	*T*
F	*F*	*F*

Example 5: Consider the following statements *p* : I shall go to the game.

q : I shall watch the game on television.

Then $p \vee q$: I shall go to the game or watch the game on television.

Conditional proposition

If p and q are any two statements (or propositions) then the statement $p \rightarrow q$ which is read as, 'If p, then q' is called a **conditional statement** (or **proposition**) or **implication** and the connective is the **conditional connective.**

The conditional is defined by the following table:

Table 4. Truth table for conditional

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

In this conditional statement, p is called the **hypothesis** or **premise** or **antecedent** and q is called the **consequence** or **conclusion.**

To understand better, this connective can be looked as a conditional promise. If the promise is violated (broken), the conditional (implication) is false. Otherwise it is true. For this reason, the only circumstances under which the conditional $p \rightarrow q$ is false is when p is true and q is false.

Example 6: *Translate the following statement:*

'The crop will be destroyed if there is a flood' into symbolic form using conditional connective.

Solution: Let c : the crop will be destroyed; f : there is a flood.
Let us rewrite the given statement as
'If there is a flood, then the crop will be destroyed'. So, the symbolic form of the given statement is $f \rightarrow c$.

Example 7: Let p and q denote the statements:
p : You drive over 70 km per hour.
q : You get a speeding ticket.

Write the following statements into symbolic forms.

(i) You will get a speeding ticket if you drive over 70 km per hour.

(ii) Driving over 70 km per hour is sufficient for getting a speeding ticket.

(iii) If you do not drive over 70 km per hour then you will not get a speeding ticket.
(iv) Whenever you get a speeding ticket, you drive over 70 km per hour.
Solution: (i) $p \rightarrow q$ (ii) $p \rightarrow q$ (iii) $p \rightarrow q$ (iv) $q \rightarrow p$.

Notes: 1. In ordinary language, it is customary to assume some kind of relationship between the antecedent and the consequent in using the conditional. But in logic, the antecedent and the consequent in a conditional statement are not required to refer to the same subject matter. For example, the statement 'If I get sufficient money then I shall purchase a high-speed computer' sounds reasonable. On the other hand, a statement such as 'If I purchase a computer then this pen is red' does not make sense in our conventional language. But according to the definition of conditional, this proposition is perfectly acceptable and has a truth-value which depends on the truth-values of the component statements.

2. Some of the alternative terminologies used to express $p \rightarrow q$ (if *p*, then *q*) are the following: (*i*) *p* implies *q*

(*ii*) *p* only if *q* ('If *p*, then *q*' formulation emphasizes the antecedent, whereas '*p* only if *q*' formulation emphasizes the consequent. The difference is only stylistic.)

(*iii*) *q* if *p*, or *q* when *p*.

(*iv*) *q* follows from *p*, or *q* whenever *p*.

(*v*) *p* is sufficient for *q*, or a sufficient condition for *q* is *p*. (*vi*) *q* is necessary for *p*, or a necessary condition for *p* is *q*. (*vii*) *q* is consequence of *p*.

Converse, Inverse and Contrapositive

If $P \rightarrow Q$ is a conditional statement, then

(1). $Q \rightarrow P$ is called its *converse*

(2). $\neg P \rightarrow \neg Q$ is called its *inverse*

(3). $\neg Q \rightarrow \neg P$ is called its *contrapositive*.

Truth table for $Q \rightarrow P$ (converse of $P \rightarrow Q$)

P	Q	$Q \rightarrow P$
T	T	T
T	F	T
F	T	F
F	F	T

Truth table for $\neg P \rightarrow \neg Q$ (inverse of $P \rightarrow Q$)

P	Q	$\neg P$	$\neg Q$	$\neg P \rightarrow \neg Q$
T	T	F	F	T
T	F	F	T	T
F	T	T	F	F
F	F	T	T	T

Truth table for $\neg Q \rightarrow \neg P$ (contrapositive of $P \rightarrow Q$)

P	Q	$\neg Q$	$\neg P$	$\neg Q \rightarrow \neg P$
T	T	F	F	T
T	F	T	F	F
F	T	F	T	T
F	F	T	T	T

Example: Consider the statement

P : It rains.

Q: The crop will grow.

The implication $P \rightarrow Q$ states that

R: If it rains then the crop will grow.

The converse of the implication $P \rightarrow Q$, namely $Q \rightarrow P$ sates that S: If the crop will grow then there has been rain.

The inverse of the implication $P \rightarrow Q$, namely $\neg P \rightarrow \neg Q$ sates that

U: If it does not rain then the crop will not grow.

The contraposition of the implication $P \rightarrow Q$, namely $\neg Q \rightarrow \neg P$ states that T : If the crop do not grow then there has been no rain.

Example 9: *Construct the truth table for* $(p \rightarrow q) \wedge (q \rightarrow p)$

p	q	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \wedge (q \rightarrow p)$
T	*T*	*T*	*T*	*T*
T	*F*	*F*	*T*	*F*
F	*T*	*T*	*F*	*F*
F	*F*	*T*	*T*	*T*

Biconditional proposition

If p and q are any two statements (propositions), then the statement $p \leftrightarrow q$ which is read as 'p if and only if q' and abbreviated as 'p iff q' is called a **biconditional statement** and the connective is the **biconditional connective.**

The truth table of $p \leftrightarrow q$ is given by the following table:

Table 6. Truth table for biconditional

p	q	$p \leftrightarrow q$
T	*T*	*T*
T	*F*	*F*
F	*T*	*F*
F	*F*	*T*

It may be noted that p q is true only when both p and q are true or when both p and q are false. Observe that p q is true when both the conditionals $p \rightarrow q$ and $q \rightarrow p$ are true, *i.e.*, the truth-values of $(p \rightarrow q) \wedge (q \rightarrow p)$, given in Ex. 9, are identical to the truth-values of p q defined here.

Note: The notation $p \leftrightarrow q$ is also used instead of $p \leftrightarrow q$.

TAUTOLOGY AND CONTRADICTION

Tautology: A statement formula which is true regardless of the truth values of the statements which replace the variables in it is called a **universally valid formula** or a **logical truth** or a **tautology.**

Contradiction: A statement formula which is false regardless of the truth values of the statements which replace the variables in it is said to be a **contradiction.**

Contingency: A statement formula which is neither a tautology nor a contradiction is known as a **contingency.**

Substitution Instance

A formula A is called a substitution instance of another formula B if A can be obtained form B by substituting formulas for some variables of B, with the condition that the same formula is substituted for the same variable each time it occurs.

Example: Let $B : P \rightarrow (J \wedge P)$.

Substitute $R \leftrightarrow S$ for P in B, we get

$$(i): (R \leftrightarrow S) \rightarrow (J \wedge (R \leftrightarrow S))$$

Then A is a substitution instance of B.

Note that $(R \leftrightarrow S) \rightarrow (J \wedge P)$ is not a substitution instance of B because the variables

P in $J \wedge P$ was not replaced by $R \leftrightarrow S$.

Equivalence of Formulas

Two formulas A and B are said to equivalent to each other if and only if $A \leftrightarrow B$ is a tautology.

If $A \leftrightarrow B$ is a tautology, we write $A \Leftrightarrow B$ which is read as A is equivalent to B.

Note : 1. $\Leftrightarrow$ is only symbol, but not connective.
2. $A \leftrightarrow B$ is a tautology if and only if truth tables of A and B are the same.
3. Equivalence relation is symmetric and transitive.

Method I. Truth Table Method: One method to determine whether any two statement formulas are equivalent is to construct their truth tables.

Example: Prove $P \vee Q \Leftrightarrow \neg(\neg P \wedge \neg Q)$.

Solution:

P	Q	$P \vee Q$	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$	$\neg(\neg P \wedge \neg Q)$	$(P \vee Q) \Leftrightarrow \neg(\neg P \wedge \neg Q)$
T	T	T	F	F	F	T	T
T	F	T	F	T	F	T	T
F	T	T	T	F	F	T	T
F	F	F	T	T	T	F	T

As $P \vee Q \quad \neg(\neg P \wedge \neg Q)$ is a tautology, then $P \vee Q \Leftrightarrow \neg(\neg P \wedge \neg Q)$.

Example: Prove $(P \rightarrow Q) \Leftrightarrow (\neg P \vee Q)$.

Solution:

P	Q	$P \rightarrow Q$	$\neg P$	$\neg P \vee Q$	$(P \rightarrow Q) \quad (\neg P \vee Q)$
T	T	T	F	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

As $(P \rightarrow Q) \quad (\neg P \vee Q)$ is a tautology then $(P \rightarrow Q) \Leftrightarrow (\neg P \vee Q)$.

Equivalence Formulas:

1. Idempotent laws:

   (a) $P \vee P \Leftrightarrow P$ (b) $P \wedge P \Leftrightarrow P$

2. Associative laws:

   (a) $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ (b) $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$

3. Commutative laws:

   (a) $P \vee Q \Leftrightarrow Q \vee P$ (b) $P \wedge Q \Leftrightarrow Q \wedge P$

4. Distributive laws:

   $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

5. Identity laws:

   (a) (i) $P \vee F \Leftrightarrow P$ (ii) $P \vee T \Leftrightarrow T$

   (b) (i) $P \wedge T \Leftrightarrow P$ (ii) $P \wedge F \Leftrightarrow F$

6. Component laws:

   (a) (i) $P \vee \neg P \Leftrightarrow T$ (ii) $P \wedge \neg P \Leftrightarrow F$.

   (b) (i) $\neg\neg P \Leftrightarrow P$ (ii) $\neg T \Leftrightarrow F$, $\neg F \Leftrightarrow T$

7. Absorption laws:

   (a) $P \vee (P \wedge Q) \Leftrightarrow P$ (b) $P \wedge (P \vee Q) \Leftrightarrow P$

8. Demorgan's laws:

   (a) $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$ (b) $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$

Method II. Replacement Process: Consider a formula $A : P \to (Q \to R)$. The formula $Q \to R$ is a part of the formula A. If we replace $Q \to R$ by an equivalent formula $\neg Q \vee R$ in A, we get another formula $B : P \to (\neg Q \vee R)$. One can easily verify that the formulas A and B are equivalent to each other. This process of obtaining B from A as the replacement process.

Example: Prove that $P \to (Q \to R) \Leftrightarrow P \to (\neg Q \vee R) \Leftrightarrow (P \wedge Q) \to R$.(May. 2010)

Solution: $P \to (Q \to R) \Leftrightarrow P \to (\neg Q \vee R)$ $[\because Q \to R \Leftrightarrow \neg Q \vee R]$

$\Leftrightarrow \neg P \vee (\neg Q \vee R)$ $[\because P \to Q \Leftrightarrow \neg P \vee Q]$

$\Leftrightarrow (\neg P \vee \neg Q) \vee R$ [by Associative laws]

$\Leftrightarrow \neg(P \wedge Q) \vee R$ [by De Morgan's laws]

$\Leftrightarrow (P \wedge Q) \to R[\because P \to Q \Leftrightarrow \neg P \vee Q]$.

Example: Prove that $(P \to Q) \wedge (R \to Q) \Leftrightarrow (P \vee R) \to Q$.

Solution: $(P \to Q) \wedge (R \to Q) \Leftrightarrow (\neg P \vee Q) \wedge (\neg R \vee Q)$

$\Leftrightarrow (\neg P \wedge \neg R) \vee Q \Leftrightarrow$

$\neg(P \vee R) \vee Q \Leftrightarrow P \vee$

$R \to Q$

Example: Prove that $P \to (Q \to P) \Leftrightarrow \neg P \to (P \to Q)$.

Solution: $P \to (Q \to P) \Leftrightarrow \neg P \vee (Q \to P)$

$\Leftrightarrow \neg P \vee (\neg Q \vee P)$

$\Leftrightarrow (\neg P \vee P) \vee \neg Q$

$\Leftrightarrow T \vee \neg Q$

$\Leftrightarrow T$

and

$\neg P \to (P \to Q) \Leftrightarrow \neg(\neg P) \vee (P \to Q)$

$\Leftrightarrow P \vee (\neg P \vee Q) \Leftrightarrow$

$(P \vee \neg P) \vee Q \Leftrightarrow T$

$\vee Q$

$\Leftrightarrow T$

So, $P \to (Q \to P) \Leftrightarrow \neg P \to (P \to Q)$.

***Example: Prove that $(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R) \Leftrightarrow R$. (Nov. 2009)

Solution:

$(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R)$

$\Leftrightarrow ((\neg P \wedge \neg Q) \wedge R) \vee ((Q \vee P) \wedge R)$ [Associative and Distributive laws]

$\Leftrightarrow (\neg(P \vee Q) \wedge R) \vee ((Q \vee P) \wedge R)$ [De Morgan's laws]

$\Leftrightarrow (\neg(P \vee Q) \vee (P \vee Q)) \wedge R$ [Distributive laws]

$\Leftrightarrow T \wedge R$ [$\because \neg P \vee P \Leftrightarrow T$]

$\Leftrightarrow R$

**Example: Show $((P \vee Q) \wedge \neg(\neg P \wedge (\neg Q \vee \neg R))) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)$ is tautology.

Solution: By De Morgan's laws, we have

$$\neg P \wedge \neg Q \Leftrightarrow \neg(P \vee Q)$$

$$\neg P \vee \neg R \Leftrightarrow \neg(P \wedge R)$$

Therefore

$(\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R) \Leftrightarrow \neg(P \vee Q) \vee \neg(P \wedge R)$

$\Leftrightarrow \neg((P \vee Q) \wedge (P \vee R))$

Also

$\neg(\neg P \wedge (\neg Q \vee \neg R)) \Leftrightarrow \neg(\neg P \wedge \neg(Q \wedge R))$

$\Leftrightarrow P \vee (Q \wedge R)$

$\Leftrightarrow (P \vee Q) \wedge (P \vee R)$

Hence $((P \vee Q) \wedge \neg(\neg P \wedge (\neg Q \vee \neg R))) \Leftrightarrow (P \vee Q) \wedge (P \vee Q) \wedge (P \vee R)$

$\Leftrightarrow (P \vee Q) \wedge (P \vee R)$

Thus $((P \vee Q) \wedge \neg(\neg P \wedge (\neg Q \vee \neg R))) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)$

$\Leftrightarrow [(P \vee Q) \wedge (P \vee R)] \vee \neg[(P \vee Q) \wedge (P \vee R)]$

$\Leftrightarrow T$

Hence the given formula is a tautology.

Example: Show that $(P \wedge Q) \rightarrow (P \vee Q)$ is a tautology. (Nov. 2009)

Solution: $(P \wedge Q) \rightarrow (P \vee Q) \Leftrightarrow \neg(P \wedge Q) \vee (P \vee Q)$ [$\because P \rightarrow Q \Leftrightarrow \neg P \vee Q$]

$\Leftrightarrow (\neg P \vee \neg Q) \vee (P \vee Q)$ [by De Morgan's laws]

$\Leftrightarrow (\neg P \vee P) \vee (\neg Q \vee Q)$ [by Associative laws and commutative laws]

$\Leftrightarrow (T \vee T)$[by negation laws]

$\Leftrightarrow T$

Hence, the result.

Example: Write the negation of the following statements.

(a). Jan will take a job in industry or go to graduate school.
(b). James will bicycle or run tomorrow.
(c). If the processor is fast then the printer is slow.

Solution: (a). Let P : Jan will take a job in industry.
Q: Jan will go to graduate school.

The given statement can be written in the symbolic as $P \vee Q$.

The negation of $P \vee Q$ is given by $\neg(P \vee Q)$.

$$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q.$$

$\neg P \wedge \neg Q$: Jan will not take a job in industry and he will not go to graduate school.

(b). Let P : James will bicycle.
Q: James will run tomorrow.

The given statement can be written in the symbolic as $P \vee Q$.

The negation of $P \vee Q$ is given by $\neg(P \vee Q)$.

$$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q.$$

$\neg P \wedge \neg Q$: James will not bicycle and he will not run tomorrow.

(c). Let P : The processor is fast.
Q: The printer is slow.

The given statement can be written in the symbolic as $P \rightarrow Q$.

The negation of $P \rightarrow Q$ is given by $\neg(P \rightarrow Q)$.

$$\neg(P \rightarrow Q) \Leftrightarrow \neg(\neg P \vee Q) \Leftrightarrow P \wedge \neg Q.$$

$P \wedge \neg Q$: The processor is fast and the printer is fast.

Example: Use Demorgans laws to write the negation of each statement.

(a). I want a car and worth a cycle.
(b). My cat stays outside or it makes a mess.
(c). I've fallen and I can't get up.
(d). You study or you don't get a good grade.

Solution: (a). I don't want a car or not worth a cycle.
(b). My cat not stays outside and it does not make a mess.

(c). I have not fallen or I can get up.
(d). You can not study and you get a good grade.

Exercises: 1. Write the negation of the following statements.

(a). If it is raining, then the game is canceled.
(b). If he studies then he will pass the examination.

Are $(p \to q) \to r$ and $p \to (q \to r)$ logically equivalent? Justify your answer by using the rules of logic to simply both expressions and also by using truth tables. Solution: $(p \to q) \to r$ and $p \to (q \to r)$ are not logically equivalent because

Method I: Consider

$$(p \to q) \to r \Leftrightarrow (\neg p \vee q) \to r$$
$$\Leftrightarrow \neg(\neg p \vee q) \vee r \Leftrightarrow$$
$$(p \wedge \neg q) \vee r$$
$$\Leftrightarrow (p \wedge r) \vee (\neg q \wedge r)$$

and

$$p \to (q \to r) \Leftrightarrow p \to (\neg q \vee r)$$
$$\Leftrightarrow \neg p \vee (\neg q \vee r) \Leftrightarrow$$
$$\neg p \vee \neg q \vee r.$$

Method II: (Truth Table Method)

p	q	r	$p \to q$	$(p \to q) \to r$		$q \to r$	$p \to (q \to r)$
T	T	T	T		T	T	T
T	T	F	T		F	F	F
T	F	T	F		T	T	T
T	F	F	F		T	T	T
F	T	T	T		T	T	T
F	T	F	T		F	F	T
F	F	T	T		T	T	T
F	F	F	T		F	T	T

Here the truth values (columns) of $(p \to q) \to r$ and $p \to (q \to r)$ are not identical.

Consider the statement: ”If you study hard, then you will excel”. Write its converse, contra positive and logical negation in logic.

Duality Law

Two formulas A and A^* are said to be *duals* of each other if either one can be obtained from the other by replacing $\wedge$ by $\vee$ and $\vee$ by $\wedge$. The connectives $\vee$ and $\wedge$ are called *duals* of each other. If the formula A contains the special variable T or F , then A^*, its dual is obtained by replacing T by F and F by T in addition to the above mentioned interchanges.

Example: Write the dual of the following formulas:

(i). $(P \vee Q) \wedge R$ (ii). $(P \wedge Q) \vee T$ (iii). $(P \wedge Q) \vee (P \vee \neg(Q \wedge \neg S))$

Solution: The duals of the formulas may be written as

(i). $(P \wedge Q) \vee R$ (ii). $(P \vee Q) \wedge F$ (iii). $(P \vee Q) \wedge (P \wedge \neg(Q \vee \neg S))$

Result 1: The negation of the formula is equivalent to its dual in which every variable is replaced by its negation.

We can prove

$$\neg A(P_1, P_2, ..., P_n) \Leftrightarrow A^*(\neg P_1, \neg P_2, ..., \neg P_n)$$

Example: Prove that (a). $\neg(P \wedge Q) \rightarrow (\neg P \vee (\neg P \vee Q)) \Leftrightarrow (\neg P \vee Q)$

(b). $(P \vee Q) \wedge (\neg P \wedge (\neg P \wedge Q)) \Leftrightarrow (\neg P \wedge Q)$

Solution: (a). $\neg(P \wedge Q) \rightarrow (\neg P \vee (\neg P \vee Q)) \Leftrightarrow (P \wedge Q) \vee (\neg P \vee (\neg P \vee Q))$ $[\because P \rightarrow Q \Leftrightarrow \neg P \vee Q]$

$$\Leftrightarrow (P \wedge Q) \vee (\neg P \vee Q)$$

$$\Leftrightarrow (P \wedge Q) \vee \neg P \vee Q$$

$$\Leftrightarrow ((P \wedge Q) \vee \neg P)) \vee Q$$

$$\Leftrightarrow ((P \vee \neg P) \wedge (Q \vee \neg P)) \vee Q$$

$$\Leftrightarrow (T \wedge (Q \vee \neg P)) \vee Q$$

$$\Leftrightarrow (Q \vee \neg P) \vee Q$$

$$\Leftrightarrow Q \vee \neg P$$

$$\Leftrightarrow \neg P \vee Q$$

(b). From (a)

$$(P \wedge Q) \vee (\neg P \vee (\neg P \vee Q)) \Leftrightarrow \neg P \vee Q$$

Writing the dual

$$(P \vee Q) \wedge (\neg P \wedge (\neg P \wedge Q)) \Leftrightarrow (\neg P \wedge Q)$$

Tautological Implications

A statement formula A is said to *tautologically imply* a statement B if and only if $A \rightarrow B$ is a tautology.

In this case we write $A \Rightarrow B$, which is read as 'A implies B'.

Note: $\Rightarrow$ is not a connective, $A \Rightarrow B$ is not a statement formula.

$A \Rightarrow B$ states that $A \rightarrow B$ is tautology.

Clearly $A \Rightarrow B$ guarantees that B has a truth value T whenever A has the truth value T.

One can determine whether $A \Rightarrow B$ by constructing the truth tables of A and B in the same manner as was done in the determination of $A \Leftrightarrow B$. Example: Prove that $(P \rightarrow Q) \Rightarrow (\neg Q \rightarrow \neg P)$.

Solution:

P	Q	$\neg P$	$\neg Q$	$P \rightarrow Q$	$\neg Q \rightarrow \neg P$	$(P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P)$
T	T	F	F	T	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

Since all the entries in the last column are true, $(P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P)$ is a tautology.

Hence $(P \rightarrow Q) \Rightarrow (\neg Q \rightarrow \neg P)$.

In order to show any of the given implications, it is sufficient to show that an assignment of the truth value T to the antecedent of the corresponding condi-

tional leads to the truth value T for the consequent. This procedure guarantees that the conditional becomes tautology, thereby proving the implication.

Example: Prove that $\neg Q \wedge (P \rightarrow Q) \Rightarrow \neg P$.

Solution: Assume that the antecedent $\neg Q \wedge (P \rightarrow Q)$ has the truth value T, then both $\neg Q$ and $P \rightarrow Q$ have the truth value T, which means that Q has the truth value F, $P \rightarrow Q$ has the truth value T. Hence P must have the truth value F.

Therefore the consequent $\neg P$ must have the truth value T.

$$\neg Q \wedge (P \rightarrow Q) \Rightarrow \neg P.$$

Another method to show $A \Rightarrow B$ is to assume that the consequent B has the truth value F and then show that this assumption leads to A having the truth value F. Then $A \rightarrow B$ must have the truth value T.

Example: Show that $\neg(P \rightarrow Q) \Rightarrow P$.

Solution: Assume that P has the truth value F. When P has F, $P \rightarrow Q$ has T, then $\neg(P \rightarrow Q)$ has F. Hence $\neg(P \rightarrow Q) \rightarrow P$ has T.

$$\neg(P \rightarrow Q) \Rightarrow P$$

Other Connectives

We introduce the connectives NAND, NOR which have useful applications in the design of computers.

NAND: The word NAND is a combination of 'NOT' and 'AND' where 'NOT' stands for negation and 'AND' for the conjunction. It is denoted by the symbol ↑.

If P and Q are two formulas then

$$P \uparrow Q \Leftrightarrow \neg(P \wedge Q)$$

The connective ↑ has the following equivalence:

$$P \uparrow P \Leftrightarrow \neg(P \wedge P) \Leftrightarrow \neg P \vee \neg P \Leftrightarrow \neg P.$$

$(P \uparrow Q) \uparrow (P \uparrow Q) \Leftrightarrow \neg(P \uparrow Q) \Leftrightarrow \neg(\neg(P \wedge Q)) \Leftrightarrow P \wedge Q.$

$(P \uparrow P) \uparrow (Q \uparrow Q) \Leftrightarrow \neg P \uparrow \neg Q \Leftrightarrow \neg(\neg P \wedge \neg Q) \Leftrightarrow P \vee Q.$

NAND is Commutative: Let P and Q be any two statement formulas.

$$(P \uparrow Q) \Leftrightarrow \neg(P \wedge Q)$$

$$\Leftrightarrow \neg(Q \wedge P) \Leftrightarrow$$

$$(Q \uparrow P)$$

$\therefore$ NAND is commutative.

NAND is not Associative: Let P, Q and R be any three statement formulas.

Consider $\uparrow (Q \uparrow R) \Leftrightarrow \neg(P \wedge (Q \uparrow R)) \Leftrightarrow \neg(P \wedge (\neg(Q \wedge R)))$

$$\Leftrightarrow \neg P \vee (Q \wedge R))$$

$$(P \uparrow Q) \uparrow R \Leftrightarrow \neg(P \wedge Q) \uparrow R$$

$$\Leftrightarrow \neg(\neg(P \wedge Q) \wedge R) \Leftrightarrow$$

$$(P \wedge Q) \vee \neg R$$

Therefore the connective $\uparrow$ is not associative.

NOR: The word NOR is a combination of ’NOT’ and ’OR’ where ’NOT’ stands for negation and ‘OR’ for the disjunction. It is denoted by the symbol $\downarrow$.

If P and Q are two formulas then

$$P \downarrow Q \Leftrightarrow \neg(P \vee Q)$$

The connective $\downarrow$ has the following equivalence:

$P \downarrow P \Leftrightarrow \neg(P \vee P) \Leftrightarrow \neg P \wedge \neg P \Leftrightarrow \neg P.$

$(P \downarrow Q) \downarrow (P \downarrow Q) \Leftrightarrow \neg(P \downarrow Q) \Leftrightarrow \neg(\neg(P \vee Q)) \Leftrightarrow P \vee Q.$

$(P \downarrow P) \downarrow (Q \downarrow Q) \Leftrightarrow \neg P \downarrow \neg Q \Leftrightarrow \neg(\neg P \vee \neg Q) \Leftrightarrow P \wedge Q.$

NOR is Commutative: Let P and Q be any two statement formulas.

$$(P \downarrow Q) \Leftrightarrow \neg(P \vee Q)$$

$$\Leftrightarrow \neg(Q \vee P) \Leftrightarrow$$

$$(Q \downarrow P)$$

$\therefore$ NOR is commutative.

NOR is not Associative: Let P, Q and R be any three statement formulas. Consider

$$P \downarrow (Q \downarrow R) \Leftrightarrow \neg(P \vee (Q \downarrow R))$$

$$\Leftrightarrow \neg(P \vee (\neg(Q \vee R)))$$

$$\Leftrightarrow \neg P \wedge (Q \vee R)$$

$$(P \downarrow Q) \downarrow R \Leftrightarrow \neg(P \vee Q) \downarrow R$$

$$\Leftrightarrow \neg(\neg(P \vee Q) \vee R) \Leftrightarrow$$

$$(P \vee Q) \wedge \neg R$$

Therefore the connective $\downarrow$ is not associative.

Evidently, $P \uparrow Q$ and $P \downarrow Q$ are duals of each other.

Since

$$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$$

$$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q.$$

Example: Express $P \downarrow Q$ interms of $\uparrow$ only.
Solution:

$$\begin{aligned} \downarrow Q &\Leftrightarrow \neg(P \vee Q) \\ &\Leftrightarrow (P \vee Q) \uparrow (P \vee Q) \\ &\Leftrightarrow [(P \uparrow P) \uparrow (Q \uparrow Q)] \uparrow [(P \uparrow P) \uparrow (Q \uparrow Q)] \end{aligned}$$

Example: Express $P \uparrow Q$ interms of $\downarrow$ only. (May-2012)
Solution:

$$\begin{aligned} \uparrow Q &\Leftrightarrow \neg(P \wedge Q) \\ &\Leftrightarrow (P \wedge Q) \downarrow (P \wedge Q) \\ &\Leftrightarrow [(P \downarrow P) \downarrow (Q \downarrow Q)] \downarrow [(P \downarrow P) \downarrow (Q \downarrow Q)] \end{aligned}$$

Truth Tables

Example: Show that $(A \oplus B) \vee (A \downarrow B) \Leftrightarrow (A \uparrow B)$. (May-2012)
Solution: We prove this by constructing truth table.

A	B	$A \oplus B$	$A \downarrow B$	$(A \oplus B) \vee (A \downarrow B)$	$A \uparrow B$
T	T	F	F	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	T	T	T

As columns $(A \oplus B) \vee (A \downarrow B)$ and $(A \uparrow B)$ are identical.

$$\therefore (A \oplus B) \vee (A \downarrow B) \Leftrightarrow (A \uparrow B).$$

Normal Forms

If a given statement formula $A(p_1, p_2, ...p_n)$ involves n atomic variables, we have 2^n possible combinations of truth values of statements replacing the variables.

The formula A is a tautology if A has the truth value T for all possible assignments of the truth values to the variables $p_1, p_2, ...p_n$ and A is called a contradiction if A has the truth value F for all possible assignments of the truth values of the n variables. A is said to be *satis able* if A has the truth value T for atleast one combination of truth values assigned to $p_1, p_2, ...p_n$.

The problem of determining whether a given statement formula is a Tautology, or a Contradiction is called a decision problem.

The construction of truth table involves a finite number of steps, but the construc-tion may not be practical. We therefore reduce the given statement formula to normal form and find whether a given statement formula is a Tautology or Contradiction or atleast satisfiable.

It will be convenient to use the word ”product” in place of ”conjunction” and ”sum” in place of ”disjunction” in our current discussion.

A product of the variables and their negations in a formula is called an *elementary product*. Similarly, a sum of the variables and their negations in a formula is called an *elementary sum*.

Let P and Q be any atomic variables. Then P , $\neg P \wedge Q$, $\neg Q \wedge P \;\; \neg P$, $P \;\; \neg P$, and $Q \wedge \neg P$ are some examples of elementary products. On the other hand, P , $\neg P \vee Q$, $\neg Q \vee P \vee \neg P$, $P \vee \neg P$, and $Q \vee \neg P$ are some examples of elementary sums.

Any part of an elementary sum or product which is itself an elementary sum or product is called a *factor* of the original elementary sum or product. Thus $\neg Q, \wedge \neg P$, and $\neg Q \wedge P$ are some of the factors of $\neg Q \wedge P \wedge \neg P$.

Disjunctive Normal Form (DNF)

A formula which is equivalent to a given formula and which consists of a sum of elementary products is called a *disjunctive normal form* of the given formula.

Example: Obtain disjunctive normal forms of

(a) $P \wedge (P \rightarrow Q)$; (b) $\neg(P \vee Q) \leftrightarrow (P \wedge Q)$.

Solution: (a) We have

$$P \wedge (P \rightarrow Q) \Leftrightarrow P \wedge (\neg P \vee Q)$$
$$\Leftrightarrow (P \wedge \neg P) \vee (P \wedge Q)$$

(b) $\neg(P \vee Q) \leftrightarrow (P \wedge Q)$

$\Leftrightarrow (\neg(P \vee Q) \wedge (P \wedge Q)) \vee ((P \vee Q) \wedge \neg(P \wedge Q))$ [using

$R \leftrightarrow S \Leftrightarrow (R \wedge S) \vee (\neg R \wedge \neg S)$

$\Leftrightarrow ((\neg P \wedge \neg Q) \wedge (P \wedge Q)) \vee ((P \vee Q) \wedge (\neg P \vee \neg Q))$

$\Leftrightarrow (\neg P \wedge \neg Q \wedge P \wedge Q) \vee ((P \vee Q) \wedge \neg P) \vee ((P \vee Q) \wedge \neg Q)$

$\Leftrightarrow (\neg P \wedge \neg Q \wedge P \wedge Q) \vee (P \wedge \neg P) \vee (Q \wedge \neg P) \vee (P \wedge \neg Q) \vee (Q \wedge \neg Q)$

which is the required disjunctive normal form.

Note: The DNF of a given formula is not unique.

Conjunctive Normal Form (CNF)

A formula which is equivalent to a given formula and which consists of a product of elementary sums is called a *conjunctive normal form* of the given formula.

The method for obtaining conjunctive normal form of a given formula is similar to the one given for disjunctive normal form. Again, the conjunctive normal form is not unique.

Example: Obtain conjunctive normal forms of

(a) $P \wedge (P \to Q)$; (b) $\neg(P \vee Q) \leftrightarrow (P \wedge Q)$.

Solution: (a). $P \wedge (P \to Q) \Leftrightarrow P \wedge (\neg P \vee Q)$

(b). $\neg(P \vee Q) \leftrightarrow (P \wedge Q)$

$\Leftrightarrow (\neg(P \vee Q) \to (P \wedge Q)) \wedge ((P \wedge Q) \to \neg(P \vee Q))$

$\Leftrightarrow ((P \vee Q) \vee (P \wedge Q)) \wedge (\neg(P \wedge Q) \vee \neg(P \vee Q))$

$\Leftrightarrow [(P \vee Q \vee P) \wedge (P \vee Q \vee Q)] \wedge [(\neg P \vee \neg Q) \vee (\neg P \wedge \neg Q)]$

$\Leftrightarrow (P \vee Q \vee P) \wedge (P \vee Q \vee Q) \wedge (\neg P \vee \neg Q \vee \neg P) \wedge (\neg P \vee \neg Q \vee \neg Q)$

Note: A given formula is tautology if every elementary sum in CNF is tautology.

Example: Show that the formula $Q \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$ is a tautology.

Solution: First we obtain a CNF of the given formula.

$$Q \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q) \Leftrightarrow Q \vee ((P \vee \neg P) \wedge \neg Q)$$

$$\Leftrightarrow (Q \vee (P \vee \neg P)) \wedge (Q \vee \neg Q)$$

$$\Leftrightarrow (Q \vee P \vee \neg P) \wedge (Q \vee \neg Q)$$

Since each of the elementary sum is a tautology, hence the given formula is tautology.

Principal Disjunctive Normal Form

In this section, we will discuss the concept of principal disjunctive normal form (PDNF).

Minterm: For a given number of variables, the minterm consists of conjunctions in which each statement variable or its negation, but not both, appears only once.

Let P and Q be the two statement variables. Then there are 2^2 minterms given by $P \wedge Q$, $P \wedge \neg Q$, $\neg P \wedge Q$, and $\neg P \wedge \neg Q$.

Minterms for three variables P, Q and R are $P \wedge Q \wedge R$, $P \wedge Q \wedge \neg R$, $P \wedge \neg Q \wedge R$, $P \wedge \neg Q \wedge \neg R$, $\neg P \wedge Q \wedge R$, $\neg P \wedge Q \wedge \neg R$, $\neg P \wedge \neg Q \wedge R$ and $\neg P \wedge \neg Q \wedge \neg R$. From the truth tables of these minterms of P and Q, it is clear that

P	Q	$P \wedge Q$	$P \wedge \neg Q$	$\neg P \wedge Q$	$\neg P \wedge \neg Q$
T	T	T	F	F	F
T	F	F	T	F	F
F	T	F	F	T	F
F	F	F	F	F	T

(i). no two minterms are equivalent

(ii). Each minterm has the truth value T for exactly one combination of the truth values of the variables P and Q.

Definition: For a given formula, an equivalent formula consisting of disjunctions of minterms only is called the Principal disjunctive normal form of the formula.

The principle disjunctive normal formula is also called the sum-of-products canonical form.

Methods to obtain PDNF of a given formula

(a). By Truth table:

(i). Construct a truth table of the given formula.

(ii). For every truth value T in the truth table of the given formula, select the minterm which also has the value T for the same combination of the truth values of P and Q.

(iii). The disjunction of these minterms will then be equivalent to the given formula.

Example: Obtain the PDNF of $P \to Q$.
Solution: From the truth table of $P \to Q$

P	Q	$P \to Q$	Minterm
T	T	T	$P \wedge Q$
T	F	F	$P \wedge \neg Q$
F	T	T	$\neg P \wedge Q$
F	F	T	$\neg P \wedge \neg Q$

The PDNF of $P \to Q$ is $(P \wedge Q) \vee (\neg P \wedge Q) \vee (\neg P \wedge \neg Q)$.

$$\therefore P \to Q \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge Q) \vee (\neg P \wedge \neg Q).$$

Example: Obtain the PDNF for $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$.
Solution:

P	Q	R	Minterm	$P \wedge Q$	$\neg P \wedge R$	$Q \wedge R$	$(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$
T	T	T	$P \wedge Q \wedge R$	T	F	T	T
T	T	F	$P \wedge Q \wedge \neg R$	T	F	F	T
T	F	T	$P \wedge \neg Q \wedge R$	F	F	F	F
T	F	F	$P \wedge \neg Q \wedge \neg R$	F	F	F	F
F	T	T	$\neg P \wedge Q \wedge R$	F	T	T	T
F	T	F	$\neg P \wedge Q \wedge \neg R$	F	F	F	F
F	F	T	$\neg P \wedge \neg Q \wedge R$	F	T	F	T
F	F	F	$\neg P \wedge \neg Q \wedge \neg R$	F	F	F	F

The PDNF of $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$ is

$$(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R).$$

(b). Without constructing the truth table:

In order to obtain the principal disjunctive normal form of a given formula is constructed as follows:

(1). First replace →, by their equivalent formula containing only $\wedge$, $\vee$ and ¬.
(2). Next, negations are applied to the variables by De Morgan's laws followed by the application of distributive laws.
(3). Any elementarily product which is a contradiction is dropped. Minterms are ob-tained in the disjunctions by introducing the missing factors. Identical minterms appearing in the disjunctions are deleted.

Example: Obtain the principal disjunctive normal form of

$(a)\ \neg P \vee Q$; $(b)\ (P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$.

Solution:

(a) $\neg P \vee Q \Leftrightarrow (\neg P \wedge T) \vee (Q \wedge T) \quad [\because A \wedge T \Leftrightarrow A]$

$\Leftrightarrow (\neg P \wedge (Q \vee \neg Q)) \vee (Q \wedge (P \vee \neg P)) \; [\because P \vee \neg P \Leftrightarrow T]$

$\Leftrightarrow (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (Q \wedge P) \vee (Q \wedge \neg P)$

$[\because P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

$\Leftrightarrow (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (P \wedge Q) \quad [\because P \vee P \Leftrightarrow P]$

$(b)\ (P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$

$\Leftrightarrow (P \wedge Q \wedge T) \vee (\neg P \wedge R \wedge T) \vee (Q \wedge R \wedge T)$

$\Leftrightarrow (P \wedge Q \wedge (R \vee \neg R)) \vee (\neg P \wedge R \wedge (Q \vee \neg Q)) \vee (Q \wedge R \wedge (P \vee \neg P))$

$\Leftrightarrow (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge R \wedge Q)(\neg P \wedge R \wedge \neg Q)$

$\vee (Q \wedge R \wedge P) \vee (Q \wedge R \wedge \neg P)$

$\Leftrightarrow (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$

$P \vee (P \wedge Q) \Leftrightarrow P$

$P \vee (\neg P \wedge Q) \Leftrightarrow P \vee Q$

Solution: We write the principal disjunctive normal form of each formula and com-pare these normal forms.

$(a)\ P \vee (P \wedge Q) \Leftrightarrow (P \wedge T) \vee (P \wedge Q) \quad [\because P \wedge Q \Leftrightarrow P]$

$\Leftrightarrow (P \wedge (Q \vee \neg Q)) \vee (P \wedge Q) \quad [\because P \vee \neg P \Leftrightarrow T]$

$\Leftrightarrow ((P \wedge Q) \vee (P \wedge \neg Q)) \vee (P \wedge Q)$ [by distributive laws]

$\Leftrightarrow (P \wedge Q) \vee (P \wedge \neg Q) \; [\because P \vee P \Leftrightarrow P]$

which is the required PDNF.

Now, $\Leftrightarrow P \wedge T$

$\Leftrightarrow P \wedge (Q \vee \neg Q)$

$\Leftrightarrow (P \wedge Q) \vee (P \wedge \neg Q)$

which is the required PDNF.

Hence, $P \vee (P \wedge Q) \Leftrightarrow P$.

$(b)\ P \vee (\neg P \wedge Q) \Leftrightarrow (P \wedge T) \vee (\neg P \wedge Q)$

$\Leftrightarrow (P \wedge (Q \vee \neg Q)) \vee (\neg P \wedge Q)$

$\Leftrightarrow (P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q)$

which is the required PDNF.

Now,

$$P \vee Q \Leftrightarrow (P \wedge T) \vee (Q \wedge T)$$

$$\Leftrightarrow (P \wedge (Q \vee \neg Q)) \vee (Q \wedge (P \vee \neg P))$$

$$\Leftrightarrow (P \wedge Q) \vee (P \wedge \neg Q) \vee (Q \wedge P) \vee (Q \wedge \neg P)$$

$$\Leftrightarrow (P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q)$$

which is the required PDNF.

Hence, $P \vee (\neg P \wedge Q) \Leftrightarrow P \vee Q.$

Example: Obtain the principal disjunctive normal form of

$$P \rightarrow ((P \rightarrow Q) \wedge \neg(\neg Q \vee \neg P)).$$ (Nov. 2011)

Solution: Using $P \rightarrow Q \Leftrightarrow \neg P \vee Q$ and De Morgan's law, we obtain

$\rightarrow ((P \rightarrow Q) \wedge \neg(\neg Q \vee \neg P)) \Leftrightarrow \neg P$
$\vee ((\neg P \vee Q) \wedge (Q \wedge P))$

$\Leftrightarrow \neg P \vee ((\neg P \wedge Q \wedge P) \vee (Q \wedge Q \wedge P)) \Leftrightarrow$
$\neg P \vee F \vee (P \wedge Q)$

$\Leftrightarrow \neg P \vee (P \wedge Q)$

$\Leftrightarrow (\neg P \wedge T) \vee (P \wedge Q)$

$\Leftrightarrow (\neg P \wedge (Q \vee \neg Q)) \vee (P \wedge Q)$

$\Leftrightarrow (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (P \wedge Q)$

Hence $(P \wedge Q) \vee (\neg P \wedge Q) \vee (\neg P \wedge \neg Q)$ is the required PDNF.

Principal Conjunctive Normal Form

The dual of a minterm is called a Maxterm. For a given number of variables, the *maxterm* consists of disjunctions in which each variable or its negation, but not both, appears only once. Each of the maxterm has the truth value F for exactly one com-bination of the truth values of the variables. Now we define the principal conjunctive normal form.

For a given formula, an equivalent formula consisting of conjunctions of the max-terms only is known as its *principle conjunctive normal form*. This normal form is also called the *product-of-sums canonical form*.The method for obtaining the PCNF for a given formula is similar to the one described previously for PDNF.

Example: Obtain the principal conjunctive normal form of the formula (¬P→R)∧(Q↔P)
Solution:

$$(\neg P \to R) \wedge (Q \leftrightarrow P)$$

$$\Leftrightarrow [\neg(\neg P) \vee R] \wedge [(Q \to P) \wedge (P \to Q)]$$

$$\Leftrightarrow (P \vee R) \wedge [(\neg Q \vee P) \wedge (\neg P \vee Q)]$$

$$\Leftrightarrow (P \vee R \vee F) \wedge [(\neg Q \vee P \vee F) \wedge (\neg P \vee Q \vee F)]$$

$$\Leftrightarrow [(P \vee R) \vee (Q \wedge \neg Q)] \wedge [\neg Q \vee P) \vee (R \wedge \neg R)] \wedge [(\neg P \vee Q) \vee (R \wedge \neg R)]$$

$$\Leftrightarrow (P \vee R \vee Q) \wedge (P \vee R \vee \neg Q) \wedge (P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee \neg R)$$
$$\wedge (\neg P \vee Q \vee R) \wedge (\neg P \vee Q \vee \neg R)$$

$$\Leftrightarrow (P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (\neg P \vee Q \vee \neg R)$$

which is required principal conjunctive normal form.

Note: If the principal disjunctive (conjunctive) normal form of a given formula A containing n variables is known, then the principal disjunctive (conjunctive) normal form of $\neg A$ will consist of the disjunction (conjunction) of the remaining minterms (maxterms) which do not appear in the principal disjunctive (conjunctive) normal form of A. From $A \Leftrightarrow \neg\neg A$ one can obtain the principal conjunctive (disjunctive) normal form of A by repeated applications of De Morgan's laws to the principal disjunctive (conjunctive) normal form of $\neg A$.

Example: Find the PDNF form PCNF of $S : P \vee (\neg P \to (Q \vee (\neg Q \to R)))$.
Solution:

$$\Leftrightarrow P \vee (\neg P \to (Q \vee (\neg Q \to R)))$$

$$\Leftrightarrow P \vee (\neg(\neg P) \vee (Q \vee (\neg(\neg Q) \vee R))$$

$$\Leftrightarrow P \vee (P \vee Q \vee (Q \vee R)))$$

$$\Leftrightarrow P \vee (P \vee Q \vee R)$$

$$\Leftrightarrow P \vee Q \vee R$$

which is the PCNF.

Now PCNF of $\neg S$ is the conjunction of remaining maxterms, so

$$\text{PCNF of } \neg S : (P \vee Q \vee \neg R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee \neg R) \wedge (\neg P \vee Q \vee R)$$
$$\wedge (\neg P \vee Q \vee \neg R) \wedge (\neg P \vee \neg Q \vee R) \wedge (\neg P \vee \neg Q \vee \neg R)$$

Hence the PDNF of S is

$$\neg(\text{PCNF of } \neg S) : (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R)$$
$$\vee (P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (P \wedge Q \wedge R)$$

Theory of Inference for Statement Calculus

Definition: The main aim of logic is to provide rules of inference to infer a conclusion from certain premises. The theory associated with rules of inference is known as inference theory .

Definition: If a conclusion is derived from a set of premises by using the accepted rules of reasoning, then such a process of derivation is called a deduction or a formal proof and the argument is called a *valid argument* or conclusion is called a *valid conclusion*.

Note: Premises means set of assumptions, axioms, hypothesis.

Definition: Let A and B be two statement formulas. We say that "*B logically follows from A*" or "*B* is a *valid conclusion (consequence)* of the premise *A*" iff $A \rightarrow B$ is a tautology, that is $A \Rightarrow B$. *We say that from a set of premises* $\{H_1, H_2, \cdots, H_m\}$, *a conclusion C follows logically iff*

$$H_1 \wedge H_2 \wedge \ldots \wedge H_m \Rightarrow C$$

(1)

Note: To determine whether the conclusion logically follows from the given premises, we use the following methods:

- Truth table method
- Without constructing truth table method.

Validity Using Truth Tables

Given a set of premises and a conclusion, it is possible to determine whether the conclusion logically follows from the given premises by constructing truth tables as follows.

Let $P_1, P_2, \cdots, P_n$ be all the atomic variables appearing in the premises $H_1, H_2, \cdots, H_m$ and in the conclusion C. If all possible combinations of truth values are assigned to $P_1, P_2, \cdots, P_n$ and if the truth values of $H_1, H_2, ..., H_m$ and C are entered in a table. We look for the rows in which all $H_1, H_2, \cdots, H_m$ have the value T. If, for every such row, C also has the value T, then (1) holds. That is, the conclusion follows logically.

Alternatively, we look for the rows on which C has the value F. If, in every such row, at least one of the values of $H_1, H_2, \cdots, H_m$ is F, then (1) also holds. We call such a method a 'truth table technique' for the determination of the validity of a conclusion.

Example: Determine whether the conclusion C follows logically from the premises

H_1 and H_2.

(a) $H_1 : P \to Q$ $\quad$ $H_2 : P$ $\quad$ $C : Q$

(b) $H_1 : P \to Q$ $\quad$ $H_2 : \neg P$ $\quad$ $C : Q$

(c) $H_1 : P \to Q$ $\quad$ $H_2 : \neg(P \wedge Q)$ $\quad$ $C : \neg P$

(d) $H_1 : \neg P$ $\quad$ $H_2 : P \quad Q$ $\quad$ $C : \neg(P \wedge Q)$

(e) $H_1 : P \to Q$ $\quad$ $H_2 : Q$ $\quad$ $C : P$

Solution: We first construct the appropriate truth table, as shown in table.

P	Q	$P \to Q$	$\neg P$	$\neg(P \wedge Q)$	$P \quad Q$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	T	F
F	F	T	T	T	T

(a) We observe that the first row is the only row in which both the premises have the value T. The conclusion also has the value T in that row. Hence it is valid.

In (b) the third and fourth rows, the conclusion Q is true only in the third row, but not in the fourth, and hence the conclusion is not valid.
Similarly, we can show that the conclusions are valid in (c) and (d) but not in (e).

Rules of Inference

The following are two important rules of inferences.

Rule P: A premise may be introduced at any point in the derivation.

Rule T: A formula S may be introduced in a derivation if S is tautologically implied by one or more of the preceding formulas in the derivation.

Implication Formulas

$I_1 : P \wedge Q \Rightarrow P$ (simplification)

$I_2 : P \wedge Q \Rightarrow Q$

$I_3 : P \Rightarrow P \vee Q$

$I_4 : Q \Rightarrow P \vee Q$

$I_5 : \neg P \Rightarrow P \rightarrow Q$

$I_6 : Q \Rightarrow P \rightarrow Q$

$I_7 : \neg(P \rightarrow Q) \Rightarrow P$

$I_8 : \neg(P \rightarrow Q) \Rightarrow \neg Q$

$I_9 : P, Q \Rightarrow P \wedge Q$

$I_{10} : \neg P, P \vee Q \Rightarrow Q$ (disjunctive syllogism)

$I_{11} : P, P \rightarrow Q \Rightarrow Q$ (modus ponens)

$I_{12} : \neg Q, P \rightarrow Q \Rightarrow \neg P$ (modus tollens)

$I_{13} : P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$ (hypothetical syllogism)

$I_{14} : P \vee Q, P \rightarrow R, Q \rightarrow R \Rightarrow R$ (dilemma)

Example: Demonstrate that R is a valid inference from the premises $P \rightarrow Q$, $Q \rightarrow R$, and P.
Solution:

$\{1\}$	(1)	$P \rightarrow Q$	Rule P
$\{2\}$	(2)	P	Rule P,
$\{1, 2\}$	(3)	Q	Rule T, (1), (2), and I_{13}
$\{4\}$	(4)	$Q \rightarrow R$	Rule P
$\{1, 2, 4\}$	(5)	R	Rule T, (3), (4), and I_{13}

Hence the result.

Example: Show that $R \vee S$ follows logically from the premises $C \vee D$, $(C \vee D) \rightarrow \neg H$, $\neg H \rightarrow (A \wedge \neg B)$, and $(A \wedge \neg B) \rightarrow (R \vee S)$.

Solution:

{1}	(1)	$(C \vee D) \rightarrow \neg H$	Rule P
{2}	(2)	$\neg H \rightarrow (A \wedge \neg B)$	Rule P
{1, 2}	(3)	$(C \vee D) \rightarrow (A \wedge \neg B)$	Rule T, (1), (2), and I_{13}
{4}	(4)	$(A \wedge \neg B) \rightarrow (R \vee S)$	Rule P
{1, 2, 4}	(5)	$(C \vee D) \rightarrow (R \vee S)$	Rule T, (3), (4), and I_{13}
{6}	(6)	$C \vee D$	Rule P
{1, 2, 4, 6}	(7)	$R \vee S$	Rule T, (5), (6), and I_{11}

Hence the result.

Example: Show that $S \vee R$ is tautologically implied by $(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow S)$.

Solution:

{1}	(1)	$P \vee Q$	Rule P
{1}	(2)	$\neg P \rightarrow Q$	Rule T, (1) $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
{3}	(3)	$Q \rightarrow S$	Rule P
{1, 3}	(4)	$\neg P \rightarrow S$	Rule T, (2), (3), and I_{13}
{1, 3}	(5)	$\neg S \rightarrow P$	Rule T, (4), $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
{6}	(6)	$P \rightarrow R$	Rule P
{1, 3, 6}	(7)	$\neg S \rightarrow R$	Rule T, (5), (6), and I_{13}
{1, 3, 6}	(8)	$S \vee R$	Rule T, (7) and $P \rightarrow Q \Leftrightarrow \neg P \vee Q$

Hence the result.

Example: Show that $R \wedge (P \vee Q)$ is a valid conclusion from the premises $P \vee Q$,

$Q \rightarrow R$, $P \rightarrow M$, and $\neg M$.

Solution:

{1}	(1)	$P \rightarrow M$	Rule P
{2}	(2)	$\neg M$	Rule P
{1, 2}	(3)	$\neg P$	Rule T, (1), (2), and I_{12}
{4}	(4)	$P \vee Q$	Rule P
{1, 2, 4}	(5)	Q	Rule T, (3), (4), and I_{10}
{6}	(6)	$Q \rightarrow R$	Rule P

$\{1, 2, 4, 6\}$	(7)	R	Rule T, (5), (6), and I_{11}
$\{1, 2, 4, 6\}$	(8)	$R \wedge (P \vee Q)$	Rule T, (4), (7) and I_9

Hence the result.

Example: Show $I_{12} : \neg Q, P \rightarrow Q \Rightarrow \neg P$.

Solution:

$\{1\}$	(1)	$P \rightarrow Q$	Rule P
$\{1\}$	(2)	$\neg Q \rightarrow \neg P$	Rule T, (1), and $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
$\{3\}$	(3)	$\neg Q$	Rule P
$\{1, 3\}$	(4)	$\neg P$	Rule T, (2), (3), and I_{11}

Hence the result.

Example: Test the validity of the following argument:

”If you work hard, you will pass the exam. You did not pass. Therefore, you did not work hard”.

Example: Test the validity of the following statements:

”If Sachin hits a century, then he gets a free car. Sachin does not get a free car.

Therefore, Sachin has not hit a century”.

Rules of Conditional Proof or Deduction Theorem

We shall now introduce a third inference rule, known as CP or rule of conditional proof.
Rule CP: If we can derive S from R and a set of premises, then we can derive $R \rightarrow S$ from the set of premises alone.
Rule CP is not new for our purpose her because it follows from the equivalence

$$(P \wedge R) \rightarrow S \Leftrightarrow P \rightarrow (R \rightarrow S)$$

Let P denote the conjunction of the set of premises and let R be any formula. The above equivalence states that if R is included as an additional premise and S is derived from $P \wedge R$, then $R \rightarrow S$ can be derived from the premises P alone.

Rule CP is also called the *deduction theorem* and is generally used if the conclu-sion of the form $R \rightarrow S$. In such cases, R is taken as an additional premise and S is derived from the given premises and R.

Example: Show that $R \rightarrow S$ can be derived from the premises $P \rightarrow (Q \rightarrow S)$, $\neg R \vee P$, and Q. (Nov. 2011)

Solution: Instead of deriving $R \rightarrow S$, we shall include R as an additional premise and show S first.

$\{1\}$	(1) $\neg R \vee P$	Rule P
$\{2\}$	(2) R	Rule P (assumed premise)
$\{1, 2\}$	(3) P	Rule T, (1), (2), and I_{10}
$\{4\}$	(4) $P \rightarrow (Q \rightarrow S)$	Rule P
$\{1, 2, 4\}$	(5) $Q \rightarrow S$	Rule T, (3), (4), and I_{11}
$\{6\}$	(6) Q	Rule P
$\{1, 2, 4, 6\}$	(7) S	Rule T, (5), (6), and I_{11}
$\{1, 2, 4, 6\}$	(8) $R \rightarrow S$	Rule CP

Example: Show that $P \rightarrow S$ can be derived from the premises $\neg P \vee Q$, $\neg Q \vee R$, and $R \rightarrow S$.

Solution: We include P as an additional premise and derive S.

$\{1\}$	(1) $\neg P \vee Q$	Rule P
$\{2\}$	(2) P	Rule P (assumed premise)
$\{1, 2\}$	(3) Q	Rule T, (1), (2), and I_{10}
$\{4\}$	(4) $\neg Q \vee R$	Rule P
$\{1, 2, 4\}$	(5) R	Rule T, (3), (4), and I_{10}
$\{6\}$	(6) $R \rightarrow S$	Rule P
$\{1, 2, 4, 6\}$	(7) S	Rule T, (5), (6), and I_{11}
$\{1, 2, 4, 6\}$	(8) $P \rightarrow S$	Rule CP

Example: 'If there was a ball game, then traveling was difficult. If they arrived on time, then traveling was not difficult. They arrived on time. Therefore, there was no ball game'. Show that these statements constitute a valid argument. Solution: Let us indicate the statements as follows:

P : There was a ball game.
Q: Traveling was difficult.
R: They arrived on time.

Hence, the given premises are $P \to Q$, $R \to \neg Q$, and R. The conclusion is $\neg P$.

{1}	(1) $R \to \neg Q$	Rule P
{2}	(2) R	Rule P
{1, 2}	(3) $\neg Q$	Rule T, (1), (2), and I_{11}
{4}	(4) $P \to Q$	Rule P
{4}	(5) $\neg Q \to \neg P$	Rule T, (4), and $P \to Q \Leftrightarrow \neg Q \to \neg P$
{1, 2, 4}	(6) $\neg P$	Rule T, (3), (5), and I_{11}

Example: By using the method of derivation, show that following statements con-stitute a valid argument: ”If A works hard, then either B or C will enjoy. If B enjoys, then A will not work hard. If D enjoys, then C will not. Therefore, if A works hard, D will not enjoy.

Solution: Let us indicate statements as follows:

Given premises are $P \to (Q \vee R)$, $Q \to \neg P$, and $S \to \neg R$. The conclusion is $P \to \neg S$. We include P as an additional premise and derive $\neg S$.

{1}	(1) P	Rule P (additional premise)
{2}	(2) $P \to (Q \vee R)$	Rule P
{1, 2}	(3) $Q \vee R$	Rule T, (1), (2), and I_{11}
{1, 2}	(4) $\neg Q \to R$	Rule T, (3) and $P \to Q \Leftrightarrow P \vee Q$
{1, 2}	(5) $\neg R \to Q$	Rule T, (4), and $P \to Q \Leftrightarrow \neg Q \to \neg P$
{6}	(6) $Q \to \neg P$	Rule P
{1, 2, 6}	(7) $\neg R \to \neg P$	Rule T, (5), (6), and I_{13}
{1, 2, 6}	(8) $P \to R$	Rule T, (7) and $P \to Q \Leftrightarrow \neg Q \to \neg P$
{9}	(9) $S \to \neg R$	Rule P
{9}	(10) $R \to \neg S$	Rule T, (9) and $P \to Q \Leftrightarrow \neg Q \to \neg P$
{1, 2, 6, 9}	(11) $P \to \neg S$	Rule T, (8), (10) and I_{13}
{1, 2, 6, 9}	(12) $\neg S$	Rule T, (1), (11) and I_{11}

Example: Determine the validity of the following arguments using propositional logic:

”Smoking is healthy. If smoking is healthy, then cigarettes are prescribed by physi-cians. Therefore, cigarettes are prescribed by physicians”. (May-2012)

Solution: Let us indicate the statements as follows:

P : Smoking is healthy.

Q: Cigarettes are prescribed by physicians.

Hence, the given premises are P , $P \to Q$. The conclusion is Q.

{1}	(1) $P \to Q$	Rule P
{2}	(2) P	Rule P

$\{1, 2\}$	(3) Q	Rule T, (1), (2), and I_{11}

Hence, the given statements constitute a valid argument.

Consistency of Premises

A set of formulas $H_1, H_2, \cdots, H_m$ is said to be *consistent* if their conjunction has the truth value T for some assignment of the truth values to the atomic variables appearing in $H_1, H_2, \cdots, H_m$.

If, for every assignment of the truth values to the atomic variables, at least one of the formulas $H_1, H_2, \cdots, H_m$ is false, so that their conjunction is identically false, then the formulas $H_1, H_2, \cdots, H_m$ are called *inconsistent*.

Alternatively, a set of formulas $H_1, H_2, \cdots, H_m$ is inconsistent if their conjunction implies a contradiction, that is,

$$H_1 \wedge H_2 \wedge \cdots \wedge H_m \Rightarrow R \wedge \neg R$$

where R is any formula.

Example: Show that the following premises are inconsistent:

(1). If Jack misses many classes through illness, then he fails high school.
(2). If Jack fails high school, then he is uneducated.
(3). If Jack reads a lot of books, then he is not uneducated.
(4). Jack misses many classes through illness and reads a lot of books.

Solution: Let us indicate the statements as follows:

E: Jack misses many classes through illness.
S: Jack fails high school.
A: Jack reads a lot of books.
H: Jack is uneducated.

The premises are $E \rightarrow S$, $S \rightarrow H$, $A \rightarrow \neg H$, and $E \wedge A$.

$\{1\}$	(1)	$E \rightarrow S$	Rule P
$\{2\}$	(2)	$S \rightarrow H$	Rule P
$\{1, 2\}$	(3)	$E \rightarrow H$	Rule T, (1), (2), and I_{13}
$\{4\}$	(4)	$A \rightarrow \neg H$	Rule P
$\{4\}$	(5)	$H \rightarrow \neg A$	Rule T, (4), and $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
$\{1, 2, 4\}$	(6)	$E \rightarrow \neg A$	Rule T, (3), (5), and I_{13}
$\{1, 2, 4\}$	(7)	$\neg E \vee \neg A$	Rule T, (6) and $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
$\{1, 2, 4\}$	(8)	$\neg(E \wedge A)$	Rule T, (7), and $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
$\{9\}$	(9)	$E \wedge A$	Rule P
$\{1, 2, 4, 9\}$	(10)	$\neg(E \wedge A) \wedge (E \wedge A)$	Rule T, (8), (9) and I_9

Thus, the given set of premises leads to a contradiction and hence it is inconsistent.

Example: Show that the following set of premises is inconsistent: "If the contract is valid, then John is liable for penalty. If John is liable for penalty, he will go bankrupt. If the bank will loan him money, he will not go bankrupt. As a matter of fact, the contract is valid, and the bank will loan him money."

Solution: Let us indicate the statements as follows:

V : The contract is valid.

L: John is liable for penalty.

M: Bank will loan him money.

B: John will go bankrupt.

$\{1\}$	(1)	$V \to L$	Rule P
$\{2\}$	(2)	$L \to B$	Rule P
$\{1, 2\}$	(3)	$V \to B$	Rule T, (1), (2), and I_{13}
$\{4\}$	(4)	$M \to \neg B$	Rule P
$\{4\}$	(5)	$M \to \neg M$	Rule T, (4), and $P \to Q \Leftrightarrow \neg Q \to \neg P$
$\{1, 2, 4\}$	(6)	$V \to \neg M$	Rule T, (3), (5), and I_{13}
$\{1, 2, 4\}$	(7)	$\neg V \vee \neg M$	Rule T, (6) and $P \to Q \Leftrightarrow \neg P \vee Q$
$\{1, 2, 4\}$	(8)	$\neg(V \wedge M)$	Rule T, (7), and $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
$\{9\}$	(9)	$V \wedge M$	Rule P
$\{1, 2, 4, 9\}$	(10)	$\neg(V \wedge M) \wedge (V \wedge M)$	Rule T, (8), (9) and I_9

Thus, the given set of premises leads to a contradiction and hence it is inconsistent.

Indirect Method of Proof

The method of using the rule of conditional proof and the notion of an inconsistent set of premises is called the *indirect method of proof* or *proof by contradiction*.

In order to show that a conclusion C follows logically from the premises $H_1, H_2, \cdots,$ H_m, we assume that C is false and consider $\neg C$ as an additional premise. If the new set of premises is inconsistent, so that they imply a contradiction. Therefore, the assump-tion that $\neg C$ is true does not hold.

Hence, C is true whenever $H_1, H_2, \cdots, H_m$ are true. Thus, C follows logically from the premises $H_1, H_2, \cdots, H_m$.

Example: Show that $\neg(P \wedge Q)$ follows from $\neg P \wedge \neg Q$.

Solution: We introduce $\neg\neg(P \wedge Q)$ as additional premise and show that this additional premise leads to a contradiction.

{1}	(1) $\neg\neg(P \wedge Q)$	Rule P (assumed)
{1}	(2) $P \wedge Q$	Rule T, (1), and $\neg\neg P \Leftrightarrow P$
{1}	(3) P	Rule T, (2), and I_1
{4}	(4) $\neg P \wedge \neg Q$	Rule P
{4}	(5) $\neg P$	Rule T, (4), and I_1
{1, 4}	(6) $P \wedge \neg P$	Rule T, (3), (5), and I_9

Hence, our assumption is wrong.

Thus, $\neg(P \wedge Q)$ follows from $\neg P \wedge \neg Q$.

Example: Using the indirect method of proof, show that

$$P \rightarrow Q,\ Q \rightarrow R,\ \neg(P \wedge R),\ P \vee R \Rightarrow R.$$

Solution: We include $\neg R$ as an additional premise. Then we show that this leads to a contradiction.

{1}	(1) $P \rightarrow Q$	Rule P
{2}	(2) $Q \rightarrow R$	Rule P
{1, 2}	(3) $P \rightarrow R$	Rule T, (1), (2), and I_{13}
{4}	(4) $\neg R$	Rule P (assumed)
{1, 2, 4}	(5) $\neg P$	Rule T, (4), and I_{12}
{6}	(6) $P \vee R$	Rule P
{1, 2, 4, 6}	(7) R	Rule T, (5), (6) and I_{10}
{1, 2, 4, 6}	(8) $R \wedge \neg R$	Rule T, (4), (7), and I_9

Hence, our assumption is wrong.

Example: Show that the following set of premises are inconsistent, using proof by contradiction

$$P \rightarrow (Q \vee R),\ Q \rightarrow \neg P,\ S \rightarrow \neg R,\ P \Rightarrow P \rightarrow \neg S.$$

Solution: We include $\neg(P \rightarrow \neg S)$ as an additional premise. Then we show that this leads to a contradiction.

$$\therefore \neg(P \rightarrow \neg S) \Leftrightarrow \neg(\neg P \vee \neg S) \Leftrightarrow P \wedge S.$$

{1}	(1) $P \rightarrow (Q \vee R)$	Rule P
{2}	(2) P	Rule P
{1, 2}	(3) $Q \vee R$	Rule T, (1), (2), and Modus Ponens
{4}	(4) $P \wedge S$	Rule P (assumed)
{1, 2, 4}	(5) S	Rule T, (4), and $P \wedge Q \Rightarrow P$

$\{6\}$	(6) $S \rightarrow \neg R$	Rule P
$\{1, 2, 4, 6\}$	(7) $\neg R$	Rule T, (5), (6) and Modus Ponens
$\{1, 2, 4, 6\}$	(8) Q	Rule T, (3), (7), and $P \wedge Q, \neg Q \Rightarrow P$
$\{9\}$	(9) $Q \rightarrow \neg P$	Rule P
$\{1, 2, 4, 6\}$	(10) $\neg P$	Rule T, (8), (9), and $P \wedge Q, \neg Q \Rightarrow P$
$\{1, 2, 4, 6\}$	(11) $P \wedge \neg P$	Rule T, (2), (10), and $P, Q \Rightarrow P \wedge Q$
$\{1, 2, 4, 6\}$	(12) F	Rule T, (11), and $P \wedge \neg P \Leftrightarrow F$

Hence, it is proved that the given premises are inconsistent.

The Predicate Calculus

Predicate

A part of a declarative sentence describing the properties of an object is called a predicate. The logic based upon the analysis of predicate in any statement is called predicate logic.

Consider two statements:

John is a bachelor

Smith is a bachelor.

In each statement "is a bachelor" is a predicate. Both John and Smith have the same property of being a bachelor. In the statement logic, we require two different symbols to express them and these symbols do not reveal the common property of these statements. In predicate calculus these statements can be replaced by a single statement "x is a bachelor". A predicate is symbolized by a capital letters which is followed by the list of variables. The list of variables is enclosed in parenthesis. If P stands for the predicate "is a bachelor", then $P(x)$ stands for "x is a bachelor",where x is a predicate variable.

`The domain for $P(x)$: x is a bachelor, can be taken as the set of all human names. Note that $P(x)$ is not a statement, but just an expression. Once a value is assigned to x, $P(x)$ becomes a statement and has the truth value. If x is Ram, then $P(x)$ is a statement and its truth value is true.

Quantifiers

Quantifiers: Quantifiers are words that are refer to quantities such as 'some' or 'all'.

Universal Quantifier: The phrase 'forall' (denoted by $\forall$) is called the universal quantifier.

For example, consider the sentence "All human beings are mortal".

Let $P(x)$ denote 'x is a mortal'.

Then, the above sentence can be written as

$$(\forall x \in S)P(x) \text{ or } \forall x P(x)$$

where S denote the set of all human beings.

$\forall x$ represents each of the following phrases, since they have essentially the same for all x

For every x

For each x.

Existential Quantifier: The phrase 'there exists' (denoted by $\exists$) is called the exis-tential quantifier.

For example, consider the sentence

"There exists x such that $x^2 = 5$.

This sentence can be written as

$$(\exists x \in R)P(x) \text{ or } (\exists x)P(x),$$

where $P(x) : x^2 = 5$.

$\exists x$ represents each of the following phrases

There exists an x
There is an x
For some x
There is at least one x.

Example: Write the following statements in symbolic form:

(i). Something is good
(ii). Everything is good
(iii). Nothing is good
(iv). Something is not good.

Solution: Statement (i) means "There is atleast one x such that, x is good".

Statement (ii) means "Forall x, x is good".

Statement (iii) means, "Forall x, x is not good".

Statement (iv) means, "There is atleast one x such that, x is not good.

Thus, if $G(x) : x$ is good, then

statement (i) can be denoted by $(\exists x)G(x)$

statement (ii) can be denoted by $(\forall x)G(x)$

statement (iii) can be denoted by $(\forall x)\neg G(x)$

statement (iv) can be denoted by $(\exists x)\neg G(x)$.

Example: Let $K(x) : x$ is a man

$L(x) : x$ is mortal
$M(x) : x$ is an integer
$N(x) : x$ either positive or negative

Express the following using quantifiers:

- All men are mortal
- Any integer is either positive or negative.

Solution: (a) The given statement can be written as

for all x, if x is a man, then x is mortal and this can be expressed as

$$(x)(K(x) \rightarrow L(x)).$$

(b) The given statement can be written as

for all x, if x is an integer, then x is either positive or negative and this can be expressed as $(x)(M(x) \rightarrow N(x))$.

Free and Bound Variables

Given a formula containing a part of the form $(x)P\ (x)$ or $(\exists x)P\ (x)$, such a part is called an x-bound part of the formula. Any occurrence of x in an x-bound part of the formula is called a bound occurrence of x, while any occurrence of x or of any variable that is not a bound occurrence is called a free occurrence. The smallest formula immediately following $(\forall x)$ or $(\exists x)$ is called the scope of the quantifier.

Consider the following formulas:

- $(x)P\ (x, y)$
- $(x)(P\ (x) \rightarrow Q(x))$
- $(x)(P\ (x) \rightarrow (\exists y)R(x, y))$
- $(x)(P\ (x) \rightarrow R(x)) \vee (x)(R(x) \rightarrow Q(x))$
- $(\exists x)(P\ (x) \wedge Q(x))$
- $(\exists x)P\ (x) \wedge Q(x)$.

In (1), $P\ (x, y)$ is the scope of the quantifier, and occurrence of x is bound occurrence, while the occurrence of y is free occurrence.

In (2), the scope of the universal quantifier is $P\ (x) \rightarrow Q(x)$, and all concrescences of x are bound.

In (3), the scope of (x) is $P\ (x) \rightarrow (\exists y)R(x, y)$, while the scope of $(\exists y)$ is $R(x, y)$. All occurrences of both x and y are bound occurrences.

In (4), the scope of the first quantifier is $P\ (x) \rightarrow R(x)$ and the scope of the second is $R(x) \rightarrow Q(x)$. All occurrences of x are bound occurrences.

In (5), the scope $(\exists x)$ is $P\ (x) \wedge Q(x)$.

In (6), the scope of $(\exists x)$ is $P\ (x)$ and the last of occurrence of x in $Q(x)$ is free.

Negations of Quantified Statements

(i). $\neg(x)P\ (x) \Leftrightarrow (\exists x)\neg P\ (x)$

(ii). $\neg(\exists x)P\ (x) \Leftrightarrow (x)(\neg P\ (x))$.

Example: Let $P\ (x)$ denote the statement "x is a professional athlete" and let $Q(x)$ denote the statement "x plays soccer". The domain is the set of all people.

(a). Write each of the following proposition in English.

- $(x)(P\ (x) \rightarrow Q(x)$
- $(\exists x)(P\ (x) \wedge Q(x))$
- $(x)(P\ (x) \vee Q(x))$

(b). Write the negation of each of the above propositions, both in symbols and in words.

Solution:

(a). (i). For all x, if x is an professional athlete then x plays soccer.

"All professional athletes plays soccer" or "Every professional athlete plays soccer".

(ii). There exists an x such that x is a professional athlete and x plays soccer.

”Some professional athletes paly soccer”.

(iii). For all x, x is a professional athlete or x plays soccer.

”Every person is either professional athlete or plays soccer”.

(b). (i). In symbol: We know that

$$\neg(x)(P(x) \to Q(x)) \Leftrightarrow (\exists x)\neg(P(x) \to Q(x)) \Leftrightarrow (\exists x)\neg(\neg(P(x)) \vee Q(x))$$

$$\Leftrightarrow (\exists x)(P(x) \wedge \neg Q(x))$$

There exists an x such that, x is a professional athlete and x does not paly soccer. In words: ”Some professional athlete do not play soccer”.

(ii). $\neg(\exists x)(P(x) \wedge Q(x)) \Leftrightarrow (x)(\neg P(x) \vee \neg Q(x))$

In words: ”Every people is neither a professional athlete nor plays soccer” or All people either not a professional athlete or do not play soccer”.

(iii). $\neg(x)(P(x) \vee Q(x)) \Leftrightarrow (\exists x)(\neg P(x) \wedge \neg Q(x))$.

In words: ”Some people are not professional athlete or do not paly soccer”.

Inference Theory of the Predicate Calculus

To understand the inference theory of predicate calculus, it is important to be famil-iar with the following rules:

Rule US: Universal specification or instaniation

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

From $(x)A(x)$, one can conclude $A(y)$.

Rule ES: Existential specification

$$(\exists x)A(x) \Rightarrow A(y)$$

From $(\exists x)A(x)$, one can conclude $A(y)$.

Rule EG: Existential generalization

$$A(x) \Rightarrow (\exists y)A(y)$$

From $A(x)$, one can conclude $(\exists y)A(y)$.

Rule UG: Universal generalization

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

From $A(x)$, one can conclude $(y)A(y)$.

Equivalence formulas:

$E_{31} : (\exists x)[A(x) \vee B(x)] \Leftrightarrow (\exists x)A(x) \vee (\exists x)B(x)$

$E_{32} : (x)[A(x) \wedge B(x)] \Leftrightarrow (x)A(x) \wedge (x)B(x)$

$E_{33} : \neg(\exists x)A(x) \Leftrightarrow (x)\neg A(x)$

$E_{34} : \neg(x)A(x) \Leftrightarrow (\exists x)\neg A(x)$

$E_{35} : (x)(A \vee B(x)) \Leftrightarrow A \vee (x)B(x)$

$E_{36} : (\exists x)(A \wedge B(x)) \Leftrightarrow A \wedge (\exists x)B(x)$

$E_{37} : (x)A(x) \to B \Leftrightarrow (x)(A(x) \to B)$

$E_{38} : (\exists x)A(x) \to B \Leftrightarrow (x)(A(x) \to B)$

$E_{39} : A \to (x)B(x) \Leftrightarrow (x)(A \to B(x))$

$E_{40} : A \rightarrow (\exists x)B(x) \Leftrightarrow (\exists x)(A \rightarrow B(x))$

$E_{41} : (\exists x)(A(x) \rightarrow B(x)) \Leftrightarrow (x)A(x) \rightarrow (\exists x)B(x)$

$E_{42} : (\exists x)A(x) \rightarrow (x)B(X) \Leftrightarrow (x)(A(x) \rightarrow B(X))$.

Example: Verify the validity of the following arguments:

"All men are mortal. Socrates is a man. Therefore, Socrates is mortal".

or

Show that $(x)[H(x) \rightarrow M(x)] \wedge H(s) \Rightarrow M(s)$.

Solution: Let us represent the statements as follows:

$H(x)$: x is a man
$M(x)$: x is a mortal
s : Socrates

Thus, we have to show that $(x)[H(x) \rightarrow M(x)] \wedge H(s) \Rightarrow M(s)$.

{1}	(1)	$(x)[H(x) \rightarrow M(x)]$	Rule P
{1}	(2)	$H(s) \rightarrow M(s)$	Rule US, (1)
{3}	(3)	$H(s)$	Rule P
{1, 3}	(4)	$M(s)$	Rule T, (2), (3), and I_{11}

Example: Establish the validity of the following argument:"All integers are ratio-nal numbers. Some integers are powers of 2. Therefore, some rational numbers are powers of 2".

Solution: Let $P(x)$: x is an integer

$R(x)$: x is rational number

$S(x)$: x is a power of 2

Hence, the given statements becomes

$$(x)(P(x) \rightarrow R(x)), (\exists x)(P(x) \wedge S(x)) \Rightarrow (\exists x)(R(x) \wedge S(x))$$

Solution:

{1}	(1)	$(\exists x)(P(x) \wedge S(x))$	Rule P
{1}	(2)	$P(y) \wedge S(y)$	Rule ES, (1)
{1}	(3)	$P(y)$	Rule T, (2) and $P \wedge Q \Rightarrow P$
{1}	(4)	$S(y)$	Rule T, (2) and $P \wedge Q \Rightarrow Q$
{5}	(5)	$(x)(P(x) \rightarrow R(x))$	Rule P
{5}	(6)	$P(y) \rightarrow R(y)$	Rule US, (5)
{1, 5}	(7)	$R(y)$	Rule T, (3), (6) and $P, P \rightarrow Q \Rightarrow Q$
{1, 5}	(8)	$R(y) \wedge S(y)$	Rule T, (4), (7) and $P, Q \Rightarrow P \wedge Q$
{1, 5}	(9)	$(\exists x)(R(x) \wedge S(x))$	Rule EG, (8)

Hence, the given statement is valid.

Example: Show that $(x)(P(x) \rightarrow Q(x)) \wedge (x)(Q(x) \rightarrow R(x)) \Rightarrow (x)(P(x) \rightarrow R(x))$.
Solution:

$\{1\}$	(1)	$(x)(P(x) \rightarrow Q(x))$	Rule P
$\{1\}$	(2)	$P(y) \rightarrow Q(y)$	Rule US, (1)
$\{3\}$	(3)	$(x)(Q(x) \rightarrow R(x))$	Rule P
$\{3\}$	(4)	$Q(y) \rightarrow R(y)$	Rule US, (3)
$\{1, 3\}$	(5)	$P(y) \rightarrow R(y)$	Rule T, (2), (4), and I_{13}
$\{1, 3\}$	(6)	$(x)(P(x) \rightarrow R(x))$	Rule UG, (5)

Example: Show that $(\exists x)M(x)$ follows logically from the premises

$(x)(H(x) \rightarrow M(x))$ and $(\exists x)H(x)$.

Solution:

$\{1\}$	(1)	$(\exists x)H(x)$	Rule P
$\{1\}$	(2)	$H(y)$	Rule ES, (1)
$\{3\}$	(3)	$(x)(H(x) \rightarrow M(x))$	Rule P
$\{3\}$	(4)	$H(y) \rightarrow M(y)$	Rule US, (3)
$\{1, 3\}$	(5)	$M(y)$	Rule T, (2), (4), and I_{11}
$\{1, 3\}$	(6)	$(\exists x)M(x)$	Rule EG, (5)

Hence, the result.

Example: Show that $(\exists x)[P(x) \wedge Q(x)] \Rightarrow (\exists x)P(x) \wedge (\exists x)Q(x)$.
Solution:

$\{1\}$	(1)	$(\exists x)(P(x) \wedge Q(x))$	Rule P
$\{1\}$	(2)	$P(y) \wedge Q(y)$	Rule ES, (1)
$\{1\}$	(3)	$P(y)$	Rule T, (2), and I_1
$\{1\}$	(4)	$(\exists x)P(x)$	Rule EG, (3)
$\{1\}$	(5)	$Q(y)$	Rule T, (2), and I_2
$\{1\}$	(6)	$(\exists x)Q(x)$	Rule EG, (5)
$\{1\}$	(7)	$(\exists x)P(x) \wedge (\exists x)Q(x)$	Rule T, (4), (5) and I_9

Hence, the result.

Note: Is the converse true?

$\{1\}$	(1)	$(\exists x)P(x) \wedge (\exists x)Q(x)$	Rule P
$\{1\}$	(2)	$(\exists x)P(x)$	Rule T, (1) and I_1
$\{1\}$	(3)	$(\exists x)Q(x)$	Rule T, (1), and I_1
$\{1\}$	(4)	$P(y)$	Rule ES, (2)
$\{1\}$	(5)	$Q(s)$	Rule ES, (3)

Here in step (4), y is fixed, and it is not possible to use that variable again in step (5). Hence, the *converse is not true.*

Example: Show that from $(\exists x)[F(x) \wedge S(x)] \to (y)[M(y) \to W(y)]$ and $(\exists y)[M(y) \wedge \neg W(y)]$ the conclusion $(x)[F(x) \to \neg S(x)]$ follows.

{1}	(1)	$(\exists y)[M(y) \wedge \neg W(y)]$	Rule P
{1}	(2)	$[M(z) \wedge \neg W(z)]$	Rule ES, (1)
{1}	(3)	$\neg[M(z) \to W(z)]$	Rule T, (2), and $\neg(P \to Q) \Leftrightarrow P \wedge \neg Q$
{1}	(4)	$(\exists y)\neg[M(y) \to W(y)]$	Rule EG, (3)
{1}	(5)	$\neg(y)[M(y) \to W(y)]$	Rule T, (4), and $\neg(x)A(x) \Leftrightarrow (\exists x)\neg A(x)$
{1}	(6)	$(\exists x)[F(x) \wedge S(x)] \to (y)[M(y) \to W(y)]$	Rule P
{1, 6}	(7)	$\neg(\exists x)[F(x) \wedge S(x)]$	Rule T, (5), (6) and I_{12}
{1, 6}	(8)	$(x)\neg[F(x) \wedge S(x)]$	Rule T, (7), and $\neg(x)A(x) \Leftrightarrow (\exists x)\neg A(x)$
{1, 6}	(9)	$\neg[F(z) \wedge S(z)]$	Rule US, (8)
{1, 6}	(10)	$\neg F(z) \vee \neg S(z)$	Rule T, (9), and De Morgan's laws
{1, 6}	(11)	$F(z) \to \neg S(z)$	Rule T, (10), and $P \to Q \Leftrightarrow \neg P \vee Q$
{1, 6}	(12)	$(x)(F(x) \to \neg S(x))$	Rule UG, (11)

Hence, the result.

Example: Show that $(x)(P(x) \vee Q(x)) \Rightarrow (x)P(x) \vee (\exists x)Q(x)$. (May. 2012)

Solution: We shall use the indirect method of proof by assuming $\neg((x)P(x) \vee (\exists x)Q(x))$ as an additional premise.

{1}	(1)	$\neg((x)P(x) \vee (\exists x)Q(x))$	Rule P (assumed)
{1}	(2)	$\neg(x)P(x) \wedge \neg(\exists x)Q(x)$	Rule T, (1) $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$
{1}	(3)	$\neg(x)P(x)$	Rule T, (2), and I_1
{1}	(4)	$(\exists x)\neg P(x)$	Rule T, (3), and $\neg(x)A(x) \Leftrightarrow (\exists x)\neg A(x)$
{1}	(5)	$\neg(\exists x)Q(x)$	Rule T, (2), and I_2
{1}	(6)	$(x)\neg Q(x)$	Rule T, (5), and $\neg(\exists x)A(x) \Leftrightarrow (x)\neg A(x)$
{1}	(7)	$\neg P(y)$	Rule ES, (5), (6) and I_{12}
{1}	(8)	$\neg Q(y)$	Rule US, (6)
{1}	(9)	$\neg P(y) \wedge \neg Q(y)$	Rule T, (7), (8)and I_9
{1}	(10)	$\neg(P(y) \vee Q(y))$	Rule T, (9), and $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$
{11}	(11)	$(x)(P(x) \vee Q(x))$	Rule P
{11}	(12)	$(P(y) \vee Q(y))$	Rule US
{1, 11}	(13)	$\neg(P(y) \vee Q(y)) \wedge (P(y) \vee Q(y))$	Rule T, (10), (11), and I_9
{1, 11}	(14)	F	Rule T, and (13)

which is a contradiction.Hence, the statement is valid.

Example: Using predicate logic, prove the validity of the following argument: ”Every husband argues with his wife. x is a husband. Therefore, x argues with his wife”.

Solution: Let $P(x)$: x is a husband.

$Q(x)$: x argues with his wife.

Thus, we have to show that $(x)[P(x) \rightarrow Q(x)] \wedge P(x) \Rightarrow Q(y)$.

{1}	(1)	$(x)(P(x) \rightarrow Q(x))$	Rule P
{1}	(2)	$P(y) \rightarrow Q(y)$	Rule US, (1)
{1}	(3)	$P(y)$	Rule P
{1}	(4)	$Q(y)$	Rule T, (2), (3), and I_{11}

Example: Prove using rules of inference

Duke is a Labrador retriever.
All Labrador retriever like to swim.
Therefore Duke likes to swim.

Solution: We denote

$L(x)$: x is a Labrador retriever.

$S(x)$: x likes to swim.

d: Duke.

We need to show that $L(d) \wedge (x)(L(x) \rightarrow S(x)) \Rightarrow S(d)$.

{1}	(1)	$(x)(L(x) \rightarrow S(x))$	Rule P
{1}	(2)	$L(d) \rightarrow S(d)$	Rule US, (1)
{2}	(3)	$L(d)$	Rule P
{1, 2}	(4)	$S(d)$	Rule T, (2), (3), and I_{11}.

JNTUK Previous questions

1. Test the Validity of the Following argument: “All dogs are barking. Some animals are dogs. Therefore, some animals are barking”.
2. Test the Validity of the Following argument:
“Some cats are animals. Some dogs are animals. Therefore, some cats are dogs”.
3. Symbolizes and prove the validity of the following arguments :
(i) Himalaya is large. Therefore every thing is large.
(ii) Not every thing is edible. Therefore nothing is edible.
4. a) Find the PCNF of (~p↔r) ^(q↔p) ?
b) Explain in brief about duality Law?

c) Construct the Truth table for ~(~p^~q)?
d) Find the disjunctive Normal form of ~(p → (q^r)) ?

5. Define Well Formed Formula? Explain about Tautology with example?
6. Explain in detail about the Logical Connectives with Examples?

7. Obtain the principal conjunctive normal form of the formula $(\neg P \rightarrow R) \land (Q \leftrightarrow P)$
8. Prove that $(\exists x)P(x) \land Q(x) \rightarrow (\exists x)P(x) \land (\exists x)Q(x)$. Does the converse hold?
9. Show that from i) $(\exists x)(F(x) \land S(x)) \rightarrow (y)(M(y) \rightarrow W(y))$

   ii) $(\exists y)\ (M(y) \land \neg W(y))$ the conclusion $(x)(F(x) \rightarrow \neg S(x))$ follows.

10. Obtain the principal disjunctive and conjunctive normal forms of $(P \rightarrow (Q \land R)) \land (\neg P \rightarrow (\neg Q \land \neg R))$. Is this formula a tautology?
11. Prove that the following argument is valid: No Mathematicians are fools. No one who is not a fool is an administrator. Sitha is a mathematician. Therefore Sitha is not an administrator.
12. Test the Validity of the Following argument: If you work hard, you will pass the exam. You did not pass. Therefore you did not work hard.
13. Without constructing the Truth Table prove that $(p \rightarrow q) \rightarrow q = p v q$?
14. Using normal forms, show that the formula $Q \lor (P \land \neg Q) \lor (\neg P \land \neg Q)$ is a tautology.
15. Show that $(x)\ (P(x) \lor Q(x)) \rightarrow (x)P(x) \lor (\exists x)Q(x)$
16. Show that $\neg (P \land Q) \rightarrow (\neg P \lor (\neg P \lor Q)) \Leftrightarrow (\neg P \lor Q)$

    $(P \lor Q) \land (\neg P \land (\neg P \land Q)) \Leftrightarrow (\neg P \land Q)$
17. Prove that $(\exists x)\ (P(x) \land Q(x)) \rightarrow (\exists x)P(x) \land (\exists x)Q(x)$
18. Example: Prove or disprove the validity of the following arguments using the rules of inference. (i) All men are fallible (ii) All kings are men (iii) Therefore, all kings are fallible.
19. Test the Validity of the Following argument:

    "Lions are dangerous animals, there are lions, and therefore there are dangerous animals."

MULTIPLE CHOICE QUESTIONS

1: Which of the following propositions is tautology?

A.$(p \lor q) \rightarrow q$ B. $p \lor (q \rightarrow p)$ C.$p \lor (p \rightarrow q)$ D.Both (b) & (c)

Option: C

2: Which of the proposition is p^ (~ p v q) is

A.A tautology B.A contradiction C.Logically equivalent to p ^ q D.All of above

Option: C

3: Which of the following is/are tautology?

A.a v b → b ^ c B.a ^ b → b v c C.a v b → (b → c) D.None of these

Option: B

4: Logical expression (A^ B) → (C' ^ A) → (A ≡ 1) is

A.ContradictionB.Valid C.Well-formed formula D.None of these

Option: D

5: Identify the valid conclusion from the premises Pv Q, Q → R, P → M, ˥M

A.P ^ (R v R) B.P ^ (P ^ R) C.R ^ (P v Q) D.Q ^ (P v R)

Option: D

6: Let a, b, c, d be propositions. Assume that the equivalence a ↔ (b v ˥b) and b ↔ c hold. Then truth value of the formula (a ^ b) → ((a ^ c) v d) is always

A.True B.False C.Same as the truth value of a D.Same as the truth value of b

Option: A

7: Which of the following is a declarative statement?

A. It's right B. He says C.Two may not be an even integer D.I love you

Option: B

8: P → (Q → R) is equivalent to

A. (P ^ Q) → R B.(P v Q) → R C.(P v Q) → ˥R D.None of these

Option: A

9: Which of the following are tautologies?

A.((P v Q) ^ Q) ↔ Q B.((P v Q) ^ ˥P) → Q C.((P v Q) ^ P) → P D.Both (a) & (b)

Option: D

10: If F1, F2 and F3 are propositional formulae such that F1 ^ F2 → F3 and F1 ^ F2→F3 are both tautologies, then which of the following is TRUE?

A.Both F1 and F2 are tautologies B.The conjuction F1 ^ F2 is not satisfiable

C.Neither is tautologies D.None of these

Option: B

11. Consider two well-formed formulas in propositional logic

    F1 : P →˥P F2 : (P →˥P) v (˥P →) Which of the following statement is correct?

    A.F1 is satisfiable, F2 is unsatisfiable B.F1 is unsatisfiable, F2 is satisfiable

    C.F1 is unsatisfiable, F2 is valid D.F1 & F2 are both satisfiable

    Option: C

12: What can we correctly say about proposition P1 : (p v ˥q) ^ (q →r) v (r v p)

    A.P1 is tautology B.P1 is satisfiable

    C.If p is true and q is false and r is false, the P1 is true

    D.If p as true and q is true and r is false, then P1 is true

    Option: C

13: (P v Q) ^ (P → R)^ (Q →S) is equivalent to

    A.S ^ R B.S → R C.S v R D.All of above

    Option: C

14: The functionally complete set is

    A.{ ˥, ^, v } B.{↓, ^ }C.{↑} D.None of these

    Option: C

15: (P v Q) ^ (P→R) ^ (Q → R) is equivalent to

    A.P B.Q C.R D.True = T

    Option: C

16: ˥(P → Q) is equivalent to

    A.P ^ ˥Q B.P ^ QC.˥P v Q D.None of these

    Option: A

17: In propositional logic , which of the following is equivalent to p → q?

    A.~p → q B.~p v q C.~p v~ q D.p →q

    Option: B

18: Which of the following is FALSE? Read ^ as And, v as OR, ~as NOT, →as one way implication and ↔ as two way implication?

    A.((x → y)^ x) →y B.((~x →y)^ (~x ^ ~y))→y C.(x → (x v y)) D.((x v y) ↔(~x v ~y))

    Option: D

19: Which of the following well-formed formula(s) are valid?

    A.((P → Q)^(Q → R))→ (P → R) B.(P → Q) →(˥P → ˥Q)

    C.(P v (˥P v ˥Q)) →P D.((P → R) v (Q → R)) → (P v Q}→R)

    Option: A

20: Let p and q be propositions. Using only the truth table decide whether p ↔ q does not imply p → ˥q is

    A.True B.False C.None D.Both A and B

    Option: A

UNIT-2
Set Theory

Set:A set is collection of well defined objects.

In the above definition the words set and collection for all practical purposes are Synonymous. We have really used the word set to define itself.
Each of the objects in the set is called a member of an element of the set. The objects themselves can be almost anything. Books, cities, numbers, animals, flowers, etc. Elements of a set are usually denoted by lower-case letters. While sets are denoted by capital letters of English larguage.

The symbol $\in$ indicates the membership in a set.
If "*a* is an element of the set *A*", then we write $a \in A$.
The symbol $\in$ is read "is a member of " or "is an element of ".
The symbol $\notin$ is used to indicate that an object is not in the given set.
The symbol $\notin$ is read "is not a member of " or "is not an element of ".
If *x* is not an element of the set *A* then we write $x \notin A$.

Subset*:*

A set *A* is a subset of the set *B* if and only if every element of *A* is also an element of *B*. We also say that *A* is contained in *B*, and use the notation $A \subseteq B$.

Proper Subset*:*

A set *A* is called proper subset of the set *B*. If (*i*) *A* is subset of *B* and (*ii*) *B* is not a subset *A* i.e., *A* is said to be a proper subset of *B* if every element of *A* belongs to the set *B*, but there is atleast one element of *B*, which is not in *A*. If *A* is a proper subset of *B*, then we denote it by $A \subset B$.

Super set: If *A* is subset of *B*, then *B* is called a superset of *A*.

Null set: The set with no elements is called an empty set or null set. A Null set is designated by the symbol ϕ. The null set is a subset of every set, i.e., If *A* is any set then $\phi \subset A$.

Universal set:
In many discussions all the sets are considered to be subsets of one particular set. This set is called the universal set for that discussion. The Universal set is often designated by the script letter μ. Universal set in not unique and it may change from one discussion to another.

Power set:
The set of all subsets of a set *A* is called the power set of *A*.
The power set of *A* is denoted by *P* (*A*). If *A* has *n* elements in it, then *P* (*A*) has 2^n elements:

Disjoint sets:
Two sets are said to be disjoint if they have no element in common.

Union of two sets:
The union of two sets *A* and *B* is the set whose elements are all of the elements in *A* or in *B* or in both. The union of sets *A* and *B* denoted by $A \cup B$ is read as "*A* union *B*".

Intersection of two sets:
The intersection of two sets *A* and *B* is the set whose elements are all of the elements common to both *A* and *B*. The intersection of the sets of "*A*" and "*B*" is denoted by $A \bigcap B$ and is read as "*A* intersection *B*"

Difference of sets:
If *A* and *B* are subsets of the universal set *U*, then the relative complement of *B* in *A*is the set of all elements in *A* which are not in *A*. It is denoted by $A - B$ thus: $A - B = \{x \mid x \in A \text{ and } x \notin B\}$

Complement of a set:
If U is a universal set containing the set A, then $U - A$ is called the complement of A. It is denoted by A^1 . Thus $A^1 = \{x: x \notin A\}$

Inclusion-Exclusion Principle:

The inclusion–exclusion principle is a counting technique which generalizes the familiar method of obtaining the number of elements in the unionof two finite sets; symbolically expressed as

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

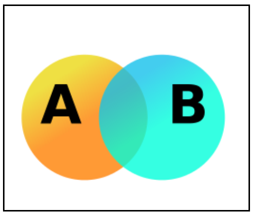


Fig.Venn diagram showing the union of sets A and B

where A and B are two finite sets and $|S|$ indicates the cardinality of a set S (which may be considered as the number of elements of the set, if the set is finite). The formula expresses the fact that the sum of the sizes of the two sets may be too large since some elements may be counted twice. The double-counted elements are those in the intersection of the two sets and the count is corrected by subtracting the size of the intersection.

The principle is more clearly seen in the case of three sets, which for the sets A, B and C is given by

$$|A \cup B \cup BC| = |A| + |B| + |C| - |A \cap B| - |C \cap B| - |A \cap C| + |A \cap B \cap C|.$$

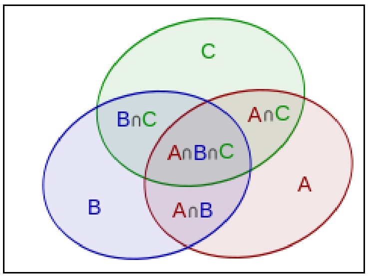


Fig.Inclusion–exclusion illustrated by a Venn diagram for three sets

This formula can be verified by counting how many times each region in the Venn diagram figure is included in the right-hand side of the formula. In this case, when removing the contributions of over-counted elements, the number of elements in the mutual intersection of the three sets has been subtracted too often, so must be added back in to get the correct total.

In general, Let A1, · · · , Ap be finite subsets of a set U. Then,

$$|A_1 \cup A_2 \cup \ldots \cup A_p| = \sum_{1 \le i \le p} |A_i| - \sum_{1 \le i_1 < i_2 \le p} |A_{i_1} \cap A_{i_2}| +$$

$$\sum_{1 \le i_1 < i_2 < i_3 \le p} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \ldots + (-1)^{p-1} |A_1 \cap A_2 \cap \cdots \cap A_p|,$$

Example: How many natural numbers $n \le 1000$ are not divisible by any of 2, 3?

Ans: Let $A_2 = \{n \in N \mid n \le 1000, 2|n\}$ and $A_3 = \{n \in N \mid n \le 1000, 3|n\}$.
Then, $|A_2 \cup A_3| = |A_2| + |A_3| - |A_2 \cap A_3| = 500 + 333 - 166 = 667$.
So, the required answer is $1000 - 667 = 333$.

Example: How many integers between 1 and 10000 are divisible by none of 2, 3, 5, 7?

Ans: For $i \in \{2, 3, 5, 7\}$, let $A_i = \{n \in N \mid n \le 10000, i|n\}$.
Therefore, the required answer is $10000 - |A_2 \cup A_3 \cup A_5 \cup A_7| = 2285$.

Relations

Definition: Any set of ordered pairs defines a *binary relation*.

We shall call a binary relation simply a relation. Binary relations represent relationships between elements of two sets. If R is a relation, a particular ordered pair, say $(x, y) \in R$ can be written as xRy and can be read as "x is in relation R to y".

Example: Give an example of a relation.
Solution: The relation "greater than" for real numbers is denoted by $'>'$. If x and y are any two real numbers such that $x > y$, then we say that $(x, y) \in >$. Thus the relation > is $\{ \} >= (x, y) : x$ and y are real numbers and $x > y$
Example: Define a relation between two sets $A = \{5, 6, 7\}$ and $B = \{x, y\}$.

Solution: If $A = \{5, 6, 7\}$ and $B = \{x, y\}$, then the subset $R = \{(5, x), (5, y), (6, x), (6, y)\}$ is a relation from A to B.

Definition: Let S be any relation. The *domain* of the relation S is defined as the set of all first elements of the ordered pairs that belong to S and is denoted by $D(S)$.

$$D(S) = \{ x : (x, y) \in S, \text{ for some } y \}$$

The *range* of the relation S is defined as the set of all second elements of the ordered pairs that belong to S and is denoted by $R(S)$.

$$R(S) = \{ y : (x, y) \in S, \text{ for some } x\}$$

Example: $A = \{2, 3, 4\}$ and $B = \{3, 4, 5, 6, 7\}$. Define a relation from A to B by $(a, b) \in R$ if a divides b.
Solution: We obtain $R = \{(2, 4), (2, 6), (3, 3), (3, 6), (4, 4)\}$.

Domain of $R = \{2, 3, 4\}$ and range of $R = \{3, 4, 6\}$.

Properties of Binary Relations in a Set

A relation R on a set X is said to be

- Reflexive relation if xRx or $(x, x) \in R, \ \forall x \in X$
- Symmetric relation if xRy then $yRx, \ \forall x, y \in X$
- Transitive relation if xRy and yRz then $xRz, \ \forall x, y, z \in X$
- Irreflexive relation if $x \not R x$ or $(x, x) \notin R, \ \forall x \in X$
- Antisymmetric relation if for every x and y in X, whenever xRy and yRx, then $x = y$.

Examples: (i). If $R_1 = \{(1, 1), (1, 2), (2, 2), (2, 3), (3, 3)\}$ be a relation on $A = \{1, 2, 3\}$, then R_1 is a reflexive relation, since for every $x \in A, (x, x) \in R_1$.

(ii). If $R_2 = \{(1, 1), (1, 2), (2, 3), (3, 3)\}$ be a relation on $A = \{1, 2, 3\}$, then R_2 is not a reflexive relation, since for every $2 \in A, (2, 2) \notin R_2$.

(iii). If $R_3 = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 1), (3, 1)\}$ be a relation on $A = \{1, 2, 3\}$, then R_3 is a symmetric relation.

(iv). If $R_4 = \{(1, 2), (2, 2), (2, 3)\}$ on $A = \{1, 2, 3\}$ is an antisymmetric.

Example: Given $S = \{1, 2, ..., 10\}$ and a relation R on S, where $R = \{(x, y) | x + y = 10\}$.
What are the properties of the relation R?

Solution: Given that

$S = \{1, 2, ..., 10\}$

- $= \{(x, y) | x + y = 10\}$
- $= \{(1, 9), (9, 1), (2, 8), (8, 2), (3, 7), (7, 3), (4, 6), (6, 4), (5, 5)\}$.

(i). For any $x \in S$ and $(x, x) \notin R$. Here, $1 \in S$ but $(1, 1) \notin R$.

$\Rightarrow$ the relation R is not reflexive. It is also not irreflexive, since $(5, 5) \in R$.

(ii). $(1, 9) \in R \Rightarrow (9, 1) \in R$

$(2, 8) \in R \Rightarrow (8, 2) \in R$.....

$\Rightarrow$ the relation is symmetric, but it is not antisymmetric. (iii). $(1, 9) \in R$ and $(9, 1) \in R$

$\Rightarrow (1, 1) \notin R$

$\Rightarrow$ The relation R is not transitive. Hence, R is symmetric.

Relation Matrix and the Graph of a Relation

Relation Matrix: A relation R from a finite set X to a finite set Y can be repre-sented by a matrix is called the *relation matrix* of R.

Let $X = \{x_1, x_2, ..., x_m\}$ and $Y = \{y_1, y_2, ..., y_n\}$ be finite sets containing m and n elements, respectively, and R be the relation from A to B. Then R can be represented by an $m \times n$ matrix $M_R = [r_{ij}]$, which is defined as follows:

$$r_{ij} = \begin{cases} 1, & \text{if } (x_i, y_j) \in R \\ 0, & \text{if } (x_i, y_j) \notin R \end{cases}$$

Example. Let $A = \{1, 2, 3, 4\}$ and $B = \{b_1, b_2, b_3\}$. Consider the relation $R = \{(1, b_2), (1, b_3), (3, b_2), (4, b_1), (4, b_3)\}$. Determine the matrix of the relation.

Solution: $A = \{1, 2, 3, 4\}$, $B = \{b_1, b_2, b_3\}$.

Relation $R = \{(1, b_2), (1, b_3), (3, b_2), (4, b_1), (4, b_3)\}$.

Matrix of the relation R is written as

That is $M_R = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$

Example: Let $A = \{1, 2, 3, 4\}$. Find the relation R on A determined by the matrix

$$M_R = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

Solution: The relation $R = \{(1, 1), (1, 3), (2, 3), (3, 1), (4, 1), (4, 2), (4, 4)\}$.

Properties of a relation in a set:

(i). If a relation is reflexive, then all the diagonal entries must be 1.

(ii). If a relation is symmetric, then the relation matrix is symmetric, i.e., $r_{ij} = r_{ji}$ for every i and j.

(iii). If a relation is antisymmetric, then its matrix is such that if $r_{ij} = 1$ then $r_{ji} = 0$ for $i \neq j$.

Graph of a Relation: A relation can also be represented pictorially by drawing its *graph*. Let R be a relation in a set $X = \{x_1, x_2, ..., x_m\}$. The elements of X are represented by points or circles called *nodes*. These nodes are called *vertices*. If $(x_i, x_j) \in R$, then we connect the nodes x_i and x_j by means of an arc and put an arrow on the arc in the direction from x_i to x_j . This is called an *edge*. If all the nodes corresponding to the ordered pairs in R are connected by arcs with proper arrows, then we get a graph of the relation R.

Note: (i). If x_iRx_j and $x_j\ Rx_i$, then we draw two arcs between x_i and x_j with arrows pointing in both directions.

(ii). If x_iRx_i, then we get an arc which starts from node x_i and returns to node x_i. This arc is called a *loop*.

Properties of relations:

(i). If a relation is reflexive, then there must be a loop at each node. On the other hand, if the relation is irreflexive, then there is no loop at any node.

(ii). If a relation is symmetric and if one node is connected to another, then there must be a return arc from the second node to the first.

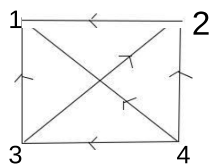
(iii). For antisymmetric relations, no such direct return path should exist.

(iv). If a relation is transitive, the situation is not so simple.

Example: Let $X = \{1, 2, 3, 4\}$ and $R=\{(x, y)|\ x > y\}$. Draw the graph of R and also give its matrix.

Solution: $R = \{(4, 1), (4, 3), (4, 2), (3, 1), (3, 2), (2, 1)\}$.

The graph of R and the matrix of R are



Graph of R

$$M_R = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

Partition and Covering of a Set

Let S be a given set and $A = \{A_1, A_2, \cdots, A_m\}$ where each A_i, $i = 1, 2, \cdots, m$ is a subset of S and

$$\bigcup_{i=1}^{m} A_i = S .$$

Then the set A is called a *covering* of S, and the sets $A_1, A_2, \cdots, A_m$ are said to *cover* S. If, in addition, the elements of A, which are subsets of S, are mutually disjoint, then A is called a *partition* of S, and the sets $A_1, A_2, \cdots, A_m$ are called the *blocks* of the partition.

Example: Let $S = \{a, b, c\}$ and consider the following collections of subsets of S. $A = \{\{a, b\}, \{b, c\}\}$, $B = \{\{a\}, \{a, c\}\}$, $C = \{\{a\}, \{b, c\}\}$, $D = \{\{a, b, c\}\}$, $E = \{\{a\}, \{b\}, \{c\}\}$, and $F = \{\{a\}, \{a, b\}, \{a, c\}\}$. Which of the above sets are covering?

Solution: The sets *A, C, D, E, F* are covering of *S*. But, the set *B* is not covering of *S*, since their union is not *S*.

Example: Let $S = \{a, b, c\}$ and consider the following collections of subsets of S. $A = \{\{a, b\}, \{b, c\}\}$, $B = \{\{a\}, \{b, c\}\}$, $C = \{\{a, b, c\}\}$, $D = \{\{a\}, \{b\}, \{c\}\}$, and $E= \{\{a\}, \{a, c\}\}$.
Which of the above sets are covering?

Solution: The sets *B*, *C* and *D* are partitions of *S* and also they are covering. Hence, every partition is a covering.

The set *A* is a covering, but it is not a partition of a set, since the sets $\{a, b\}$ and $\{b, c\}$ are not disjoint. Hence, every covering need not be a partition.

The set *E* is not partition, since the union of the subsets is not *S*. The partition *C* has one block and the partition *D* has three blocks.

Example: List of all ordered partitions $S = \{a, b, c, d\}$ of type (1, 2, 2).

Solution:

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

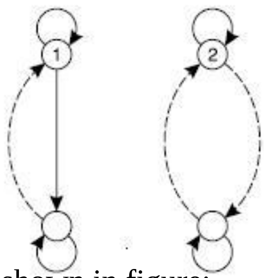
Equivalence Relations

A relation *R* in a set *X* is called an *equivalence relation* if it is reflexive, symmetric and transitive. The following are some examples of equivalence relations:

1.Equality of numbers on a set of real numbers.
2. Equality of subsets of a universal set.

Example: Let $X = \{1, 2, 3, 4\}$ and $R == \{(1, 1), (1, 4), (4, 1), (4, 4), (2, 2), (2, 3), (3, 2), (3, 3)\}$.
Prove that *R* is an equivalence relation.

$$M_R = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 01 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$



The corresponding graph of R is shown in figure:
Clearly, the relation R is reflexive, symmetric and transitive. Hence, R is an equivalence relation.
Example: Let $X = \{1, 2, 3, ..., 7\}$ and $R =(x, y)| \ x - y$ is divisible by 3. Show that R is an equivalence relation.

Solution: (i). For any $x \in X$, $x - x = 0$ is divisible by 3.

$\therefore xRx$

$\Rightarrow R$ is reflexive.

(ii). For any $x, y \in X$, if xRy, then $x - y$ is divisible by 3.

$\Rightarrow -(x - y)$ is divisible by 3.

$\Rightarrow y - x$ is divisible by 3.

$\Rightarrow yRx$

Thus, the relation R is symmetric.

(iii). For any $x, y, z \in X$, let xRy and yRz.

$\Rightarrow (x - y) + (y - z)$ is divisible by 3

$\Rightarrow x - z$ is divisible by 3

$\Rightarrow xRz$

Hence, the relation R is transitive.

Thus, the relation R is an equivalence relation.

Congruence Relation: Let I denote the set of all positive integers, and let m be apositive integer.

For $x \in I$ and $y \in I$, define R as $R = \{(x, y)| \ x - y$ is divisible by m }

The statement "$x - y$ is divisible by m" is equivalent to the statement that both x and y have the same remainder when each is divided by m.
In this case, denote R by $\equiv$ and to write xRy as $x \equiv y$ (mod m), which is read as "x equals to y modulo m". The relation $\equiv$ is called a *congruence relation*.
Example: $83 \equiv 13$(mod 5), since 83-13=70 is divisible by 5.
Example: Prove that the relation "congruence modulo m" over the set of positive integers is an equivalence relation.

Solution: Let N be the set of all positive integers and m be a positive integer. We define the relation "congruence modulo m" on N as follows:

Let $x, y \in N$. $x \equiv y$ (mod m) if and only if $x - y$ is divisible by m.

Let $x, y, z \in N$. Then

(i). $x - x = 0.m$

$\Rightarrow x \equiv x \pmod{m}$ for all $x \in N$

(ii). Let $x \equiv y \pmod{m}$. Then, $x - y$ is divisible by m.

$\Rightarrow -(x - y) = y - x$ is divisible by m.

i.e., $y \equiv x \pmod{m}$

$\therefore$ The relation $\equiv$ is symmetric.

$\Rightarrow x - y$ and $y - z$ are divisible by m. Now $(x - y) + (y - z)$ is divisible by m. i.e., $x - z$ is divisible by m.

$\Rightarrow x \equiv z \pmod{m}$

$\therefore$ The relation $\equiv$ is transitive.

Since the relation $\equiv$ is reflexive, symmetric and transitive, the relation *congruence modulo m* is an equivalence relation.

Example: Let R denote a relation on the set of ordered pairs of positive integers such that $(x,y)R(u, v)$ iff $xv = yu$. Show that R is an equivalence relation.

Solution: Let R denote a relation on the set of ordered pairs of positive integers.

Let x, y, u and v be positive integers. Given $(x, y)R(u, v)$ if and only if $xv = yu$.

(i). Since $xy = yx$ is true for all positive integers

$\Rightarrow (x, y)R(x, y)$, for all ordered pairs (x, y) of positive integers.

$\therefore$ The relation R is reflexive. (ii). Let $(x, y)R(u, v)$

$\Rightarrow xv = yu \Rightarrow yu$

$= xv \Rightarrow uy = vx$

$\Rightarrow (u, v)R(x, y)$

$\therefore$ The relation R is symmetric.

(iii). Let x, y, u, v, m and n be positive integers

Let $(x, y)R(u, v)$ and $(u, v)R(m, n)$

$\Rightarrow xv = yu$ and $un = vm$

$\Rightarrow xvun = yuvm$

$\Rightarrow xn = ym$, by canceling uv

$\Rightarrow (x, y)R(m, n)$

$\therefore$ The relation R is transitive.

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

Compatibility Relations

Definition: A relation R in X is said to be a *compatibility relation* if it is reflexive and symmetric. Clearly, all equivalence relations are compatibility relations. A compatibility relation is sometimes denoted by $\approx$.

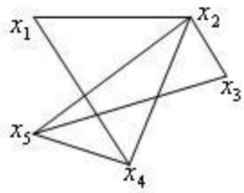
Example: Let $X = \{$ball, bed, dog, let, egg$\}$, and let the relation R be given by

$R = \{(x, y) | x, y \in X \wedge xRy$ if x and y contain some common letter$\}$.

Then R is a compatibility relation, and x, y are called compatible if xRy.

Note: ball$\approx$bed, bed$\approx$egg. But ball$\not\approx$egg. Thus $\approx$ is not transitive.

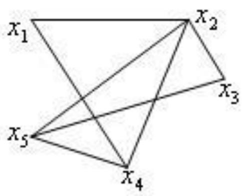
Denoting "ball" by x_1, "bed" by x_2, "dog" by x_3, "let" by x_4, and "egg" by x_5, the graph of $\approx$ is given as follows:



Maximal Compatibility Block:

Let X be a set and $\approx$ a compatibility relation on X. A subset $A \subseteq X$ is called a *maximal compatibility block* if any element of A is compatible to every other element of A and no element of $X - A$ is compatible to all the elements of A.

Example: The subsets $\{x_1, x_2, x_4\}$, $\{x_2, x_3, x_5\}$, $\{x_2, x_4, x_5\}$, $\{x_1, x_4, x_5\}$ are maximal compatibility blocks.

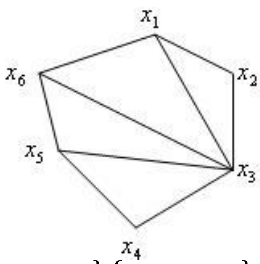


Example: Let the compatibility relation on a set $\{x_1, x_2, ..., x_6\}$ be given by the matrix:

x_2	1				
x_3	1	1			
x_4	0	0	1		
x_5	0	0	1	1	
x_6	1	0	1	0	1
	x_1	x_2	x_3	x_4	x_5

Draw the graph and find the maximal compatibility blocks of the relation.

Solution:



The maximal compatibility blocks are $\{x_1, x_2, x_3\}$,$\{x_1, x_3, x_6\}$,$\{x_3, x_5, x_6\}$,$\{x_3, x_4, x_5\}$.

Composition of Binary Relations

Let R be a relation from X to Y and S be a relation from Y to Z. Then a relation written as $R \circ S$ is called a *composite relation* of R and S where $R \circ S = \{(x, z) | x \in X, z \in Z,$ and there exists $y \in Y$ with $(x, y) \in R$ and $(y, z) \in S \}$.

Theorem: If R is relation from A to B, S is a relation from B to C and T is a relation from C to D then $T \circ (S \circ R) = (T \circ S) \circ R$

Example: Let $R = \{(1, 2), (3, 4), (2, 2)\}$ and $S = \{(4, 2), (2, 5), (3, 1), (1, 3)\}$. Find $R \circ S$, $S \circ R$, $R \circ (S \circ R)$, $(R \circ S) \circ R$, $R \circ R$, $S \circ S$, and $(R \circ R) \circ R$.

Solution: Given $R = \{(1, 2), (3, 4), (2, 2)\}$ and $S = \{(4, 2), (2, 5), (3, 1), (1, 3)\}$.

$R \circ S = \{(1, 5), (3, 2), (2, 5)\}$

$S \circ R = \{(4, 2), (3, 2), (1, 4)\} \neq R \circ S$

$(R \circ S) \circ R = \{(3, 2)\}$

$R \circ (S \circ R) = \{(3, 2)\} = (R \circ S) \circ R$

$R \circ R = \{(1, 2), (2, 2)\}$

$R \circ R \circ S = \{(4, 5), (3, 3), (1, 1)\}$

Example: Let $A = \{a, b, c\}$, and R and S be relations on A whose matrices are as given below:

$$M_R = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \text{ and } M_S = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Find the composite relations $R \circ S$, $S \circ R$, $R \circ R$, $S \circ S$ and their matrices.

Solution:

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

S= $\{(a, a), (b, b), (b, c), (c, a), (c, c)\}$. From these, we find that

$R \circ S = \{(a, a), (a, c), b, a), (b, b), (b, c), (c, b), (c, c)\}$

$S \circ R = \{(a, a), (a, c), (b, b), (b, a), (b, c), (c, a), (c, b), (c, c)\}$

$R \circ R = R^2 = \{(a, a), (a, c), (a, b), (b, a), (b, c), (b, b), (c, a), (c, b), (c, c)\}$ $S \circ S = S^2 = \{(a, a), (b, b), (b, c), (b, a), (c, a), (c, c)\}$.

The matrices of the above composite relations are as given below:

$$M_{RO\,S} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}; M_{SO\,R} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}; M_{RO\,R} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix};$$

$$M_{SO\,S} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Transitive Closure

Let X be any finite set and R be a relation in X. The relation $R^+ = R \cup R^2 \cup R^3 \cup \cdots \cup R^n$ in X is called the *transitive closure* of R in X.

Example: Let the relation $R = \{(1, 2), (2, 3), (3, 3)\}$ on the set $\{1, 2, 3\}$. What is the transitive closure of R?

Solution: Given that $R = \{(1, 2), (2, 3), (3, 3)\}$.

The transitive closure of R is $R^+ = R \cup R^2 \cup R^3 \cup \cdots =$

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

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

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

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

$R^+ = R \cup R^2 \cup R^3 \cup R^4 \cup \ldots$

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

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

Therefore $R^+ = \{(1, 2), (1, 3), (2, 3), (3, 3)\}$.

Example: Let $X = \{1, 2, 3, 4\}$ and $R = \{(1, 2), (2, 3), (3, 4)\}$ be a relation on X. Find R^+.

Solution: Given $R = \{(1, 2), (2, 3), (3, 4)\}$

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

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

$R^4 = \{(1, 4)\}$

$R^+ = \{(1, 2), (2, 3), (3, 4), (1, 3), (2, 4), (1, 4)\}$.

Partial Ordering

A binary relation R in a set P is called a *partial order relation* or a *partial ordering* in P iff R is reflexive, antisymmetric, and transitive. i.e.,

- aRa for all $a \in P$
- aRb and $bRa \Rightarrow a = b$
- aRb and $bRc \Rightarrow aRc$

A set P together with a partial ordering R is called a *partial ordered set* or *poset*. The relation R is often denoted by the symbol $\leq$ which is different from the usual less than equal to symbol. Thus, if $\leq$ is a partial order in P , then the ordered pair $(P, \leq)$ is called a poset.

Example: Show that the relation "greater than or equal to" is a partial ordering on the set of integers.

Solution: Let Z be the set of all integers and the relation $R = '\geq'$

(i). Since $a \geq a$ for every integer a, the relation $'\geq'$ is reflexive.

(ii). Let a and b be any two integers.

Let aRb and $bRa \Rightarrow a \geq b$ and $b \geq a$

$\Rightarrow a = b$

$\therefore$ The relation $'\geq'$ is antisymmetric. (iii).

Let a, b and c be any three integers.

Let aRb and $bRc \Rightarrow a \geq b$ and $b \geq c$

$\Rightarrow a \geq c$

$\therefore$ The relation $'\geq'$ is transitive.

Since the relation $'\geq'$ is reflexive, antisymmetric and transitive, $'\geq'$ is partial ordering on the set of integers. Therefore, $(Z, \geq)$ is a poset.

Example: Show that the inclusion $\subseteq$ is a partial ordering on the set power set of a set S.

Solution: Since (i). $A \subseteq A$ for all $A \subseteq S$, $\subseteq$ is reflexive.

(ii). $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$, $\subseteq$ is antisymmetric.

(iii). $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$, $\subseteq$ is transitive.

Thus, the relation $\subseteq$ is a partial ordering on the power set of S.

Example: Show that the divisibility relation $'/'$ is a partial ordering on the set of positive integers.

Solution: Let Z^+ be the set of positive integers.

Since (i). a/a for all $a \in Z^+$, $/$ is reflexive.

(ii). a/b and $b/a \Rightarrow a = b$, $/$ is antisymmetric.

(iii). a/b and $b/c \Rightarrow a/c$, $/$ is transitive.

It follows that $/$ is a partial ordering on Z^+ and $(Z^+, /)$ is a poset.

Note: On the set of all integers, the above relation is not a partial order as a and $-a$ both divide each other, but $a = -a$. i.e., the relation is not antisymmetric. Definition: Let $(P, \leq)$ be a partially ordered set. If for every $x, y \in P$ we have either $x \leq y \vee y \leq x$, then $\leq$ is called a *simple ordering* or *linear ordering* on P , and $(P, \leq)$ is called a *totally ordered* or *simply ordered set* or a *chain*.

Note: It is not necessary to have $x \leq y$ or $y \leq x$ for every x and y in a poset P . In fact, x may not be related to y, in which case we say that x and y are incomparable. Examples:

(i). The poset $(Z, \leq)$ is a totally ordered.

Since $a \leq b$ or $b \leq a$ whenever a and b are integers.

(ii). The divisibility relation $/$ is a partial ordering on the set of positive integers.

Therefore $(Z^+, /)$ is a poset and it is not a totally ordered, since it contain elements that are incomparable, such as 5 and 7, 3 and 5.

Definition: In a poset $(P, \leq)$, an element $y \in P$ is said to *cover* an element $x \in P$ if $x < y$ and if there does not exist any element $z \in P$ such that $x \leq z$ and $z \leq y$; that is, y covers $x \Leftrightarrow (x < y \wedge (x \leq z \leq y \Rightarrow x = z \vee z = y))$.

Hasse Diagrams

A partial order $\leq$ on a set P can be represented by means of a diagram known as Hasse diagram of $(P, \leq)$. In such a diagram,

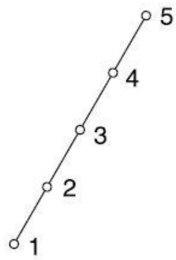
(i). Each element is represented by a small circle or dot.

(ii). The circle for $x \in P$ is drawn below the circle for $y \in P$ if $x < y$, and a line is drawn between x and y if y covers x.

(iii). If $x < y$ but y does not cover x, then x and y are not connected directly by a single line.

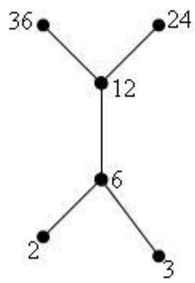
Note: For totally ordered set (P, $\leq$), the Hasse diagram consists of circles one below the other. The poset is called a chain.

Example: Let $P = \{1, 2, 3, 4, 5\}$ and $\leq$ be the relation "less than or equal to" then the Hasse diagram is:



It is a totally ordered set.

Example: Let $X = \{2, 3, 6, 12, 24, 36\}$, and the relation $\leq$ be such that $x \leq y$ if x divides y. Draw the Hasse diagram of (X, $\leq$). Solution: The Hasse diagram is is shown below:



It is not a total order set.

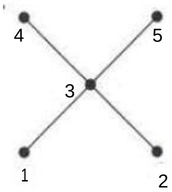
Example: Draw the Hasse diagram for the relation R on $A = \{1, 2, 3, 4, 5\}$ whose relation matrix given below:

$$M_R = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

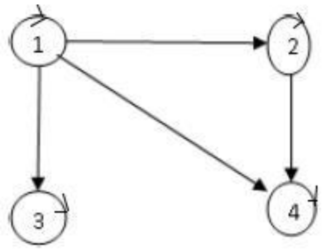
Solution:

R= $\{(1, 1), (1, 3), (1, 4), (1, 5), (2, 2), (2, 3), (2, 4), (2, 5), (3, 3), (3, 4), (3, 5), (4, 4), (5.5)\}$.

Hasse diagram for M_R is



Example: A partial order R on the set $A = \{1, 2, 3, 4\}$ is represented by the following digraph. Draw the Hasse diagram for R.

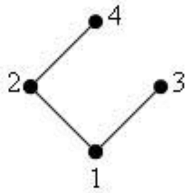


Solution: By examining the given digraph , we find that

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

We check that R is reflexive, transitive and antisymmetric. Therefore, R is partial order relation on A.

The hasse diagram of R is shown below:



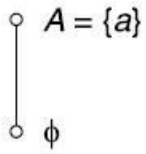
Example: Let A be a finite set and $\rho(A)$ be its power set. Let $\subseteq$ be the inclusion relation on the elements of $\rho(A)$. Draw the Hasse diagram of $\rho(A), \subseteq)$ for

- $A = \{a\}$
- $A = \{a, b\}$.

Solution: (i). Let $A = \{a\}$

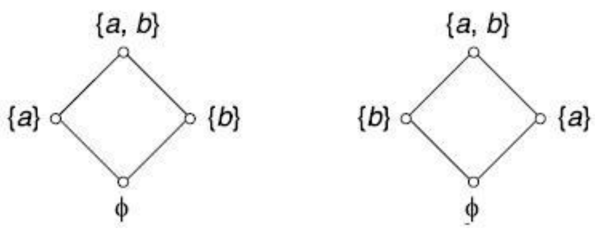
$\rho(A) = \{\phi, a\}$

Hasse diagram of $(\rho(A), \subseteq)$ is shown in Fig:



(ii). Let $A = \{a, b\}$. $\rho(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$.

The Hasse diagram for $(\rho(A), \subseteq)$ is shown in fig:

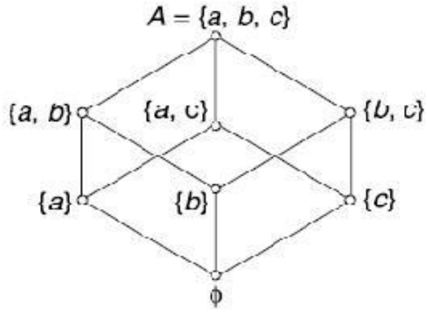


Example: Draw the Hasse diagram for the partial ordering $\subseteq$ on the power set $P(S)$ where $S = \{a, b, c\}$.

Solution: $S = \{a, b, c\}$.

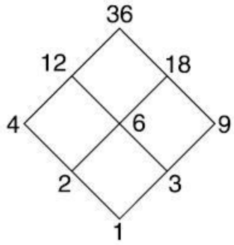
$P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Hasse diagram for the partial ordered set is shown in fig:



Example: Draw the Hasse diagram representing the positive divisions of 36 (i.e., D_{36}).

Solution: We have $D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ if and only a divides b. The Hasse diagram for R is shown in Fig.



Minimal and Maximal elements(members): Let $(P, \leq)$ denote a partially or-dered set. An element $y \in P$ is called a *minimal member* of P relative to $\leq$ if for no $x \in P$, is $x < y$.

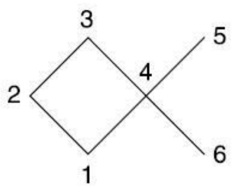
Similarly an element $y \in P$ is called a maximal member of P relative to the partial ordering $\leq$ if for no $x \in P$, is $y < x$.

Note:

(i). The minimal and maximal members of a partially ordered set need not unique.

(ii). Maximal and minimal elements are easily calculated from the Hasse diagram. They are the *'top'* and *'bottom'* elements in the diagram.

Example:



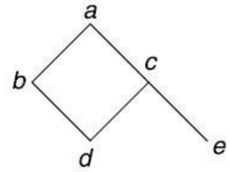
In the Hasse diagram, there are two maximal elements and two minimal elements.

The elements 3, 5 are maximal and the elements 1 and 6 are minimal.

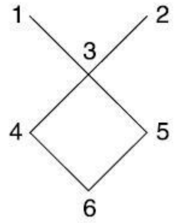
Example: Let $A = \{a, b, c, d, e\}$ and let the partial order on A in the natural way.

The element a is maximal.

The elements d and e are minimal.



Upper and Lower Bounds: Let $(P, \leq)$ be a partially ordered set and let $A \subseteq P$. Any element $x \in P$ is called an *upper bound* for A if for all $a \in A$, $a \leq x$. Similarly, any element $x \in P$ is called a *lower bound* for A if for all $a \in A$, $x \leq a$. Example: $A = \{1, 2, 3, ..., 6\}$ be ordered as pictured in figure.

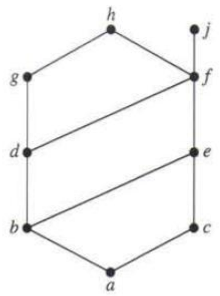


If $B = \{4, 5\}$ then the upper bounds of B are 1, 2, 3. The lower bound of B is 6.

Least Upper Bound and Greatest Lower Bound:

Let $(P, \leq)$ be a partial ordered set and let $A \subseteq P$. An element $x \in P$ is a *least upper bound* or *supremum* for A if x is an upper bound for A and $x \leq y$ where y is any upper bound for A. Similarly, the *the greatest lower bound* or *in mum* for A is an element $x \in P$ such that x is a lower bound and $y \leq x$ for all lower bounds y.

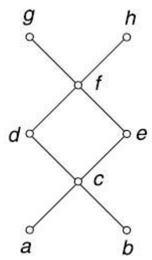
Example: Find the great lower bound and the least upper bound of $\{b, d, g\}$, if they exist in the poset shown in fig:



Solution: The upper bounds of $\{b, d, g\}$ are g and h. Since $g < h$, g is the least upper bound. The lower bounds of $\{b, d, g\}$ are a and b. Since $a < b$, b is the greatest lower bound.

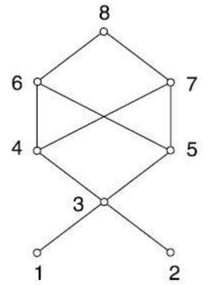
Example: Let $A = \{a, b, c, d, e, f, g, h\}$ denote a partially ordered set whose Hasse diagram is shown in Fig:

If $B = \{c, d, e\}$ then f, g, h are upper bounds of B. The element f is least upper bound.



Example: Consider the poset $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ whose Hasse diagram is shown in Fig and let $B = \{3, 4, 5\}$

The elements 1, 2, 3 are lower bounds of B. 3 is greatest lower bound.



Functions

A function is a special case of relation.

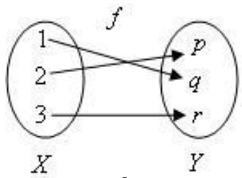
Definition: Let X and Y be any two sets. A relation f from X to Y is called a function if for every $x \in X$, there is a unique element $y \in Y$ such that $(x, y) \in f$. Note: The definition of function requires that a relation must satisfies two additional conditions in order to qualify as a function. These conditions are as follows:

(i) For every $x \in X$ must be related to some $y \in Y$, i.e., the domain of f must be X and nor merely a subset of X.

(ii). Uniqueness, i.e., $(x, y) \in f$ and $(x, z) \in f \Rightarrow y = z$.

The notation $f : X \rightarrow Y$, means f is a function from X to Y.

Example: Let $X = \{1, 2, 3\}$, $Y = \{p, q, r\}$ and $f = \{(1, p), (2, q), (3, r)\}$ then $f(1) = p$, $f(2) = q$, $f(3) = r$. Clearly f is a function from X to Y.



Domain and Range of a Function: If $f : X \rightarrow Y$ is a function, then X is called the Domain of f and the set Y is called the codomain of f. The range of f is defined as the set of all images under f.

It is denoted by $f(X) = \{y|$ for some x in X, $f(x) = y\}$ and is called the image of X in Y. The Range f is also denoted by R_f.

Example: If the function f is defined by $f(x)=x^2 + 1$ on the set $\{-2, -1, 0, 1, 2\}$, find the range of f.

Solution: $f(-2) = (-2)^2 + 1 = 5$

$f(-1) = (-1)^2 + 1 = 2$

$f(0) = 0 + 1 = 1$

$f(1) = 1 + 1 = 2$

$f(2) = 4 + 1 = 5$

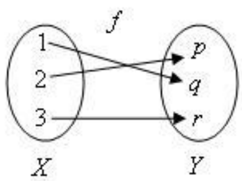
Therefore, the range of $f = \{1, 2, 5\}$.

Types of Functions

One-to-one(Injection): A mapping $f : X \rightarrow Y$ is called *one-to-one* if distinct elements of X are mapped into distinct elements of Y, i.e., f is one-to-one if

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

or equivalently $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ for $x_1, x_2 \in X$.



Example: $f : R \to R$ defined by $f(x) = 3x, \ \forall x \in R$ is one-one, since

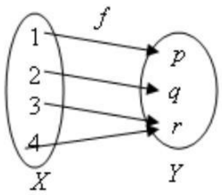
$$f(x_1) = f(x_2) \Rightarrow 3x_1 = 3x_2 \Rightarrow x_1 = x_2, \ \forall x_1, x_2 \in R.$$

Example: Determine whether $f : Z \to Z$ given by $f(x) = x^2$, $x \in Z$ is a one-to-One function.

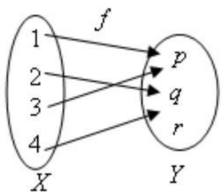
Solution: The function $f : Z \to Z$ given by $f(x) = x^2$, $x \in Z$ is not a one-to-one function. This is because both 3 and -3 have 9 as their image, which is against the definition of a one-to-one function.

Onto(Surjection): A mapping $f : X \to Y$ is called *onto* if the range set $R_f = Y$.

If $f : X \to Y$ is onto, then each element of Y is f-image of atleast one element of X.
i.e., $\{f(x) : x \in X\} = Y$.
If f is not onto, then it is said to be *into*.



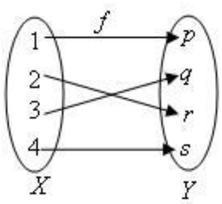
Surjective



Not Surjective

Example: $f : R \to R$, given by $f(x) = 2x, \ \forall x \in R$ is onto.

Bijection or One-to-One, Onto: A mapping $f : X \to Y$ is called *one-to-one, onto* or *bijective* if it is both one-to-one and onto. Such a mapping is also called a one-to-one correspondence between X and Y .



Example: Show that a mapping $f : R \to R$ defined by $f(x) = 2x + 1$ for $x \in R$ is a bijective map from R to R.

Solution: Let $f : R \to R$ defined by $f(x) = 2x + 1$ for $x \in R$. We need to prove that f is a bijective map, i.e., it is enough to prove that f is one-one and onto.

- Proof of f being one-to-one
  Let x and y be any two elements in R such that $f(x) = f(y)$
  $\Rightarrow 2x + 1 = 2y + 1$
  $\Rightarrow x = y$
  Thus, $f(x) = f(y) \Rightarrow x = y$
  This implies that f is one-to-one.

- Proof of f being onto
  Let y be any element in the codomain R

  $\Rightarrow f(x) = y$

  $\Rightarrow 2x + 1 = y$

  $\Rightarrow x = (y-1)/2$

Clearly, $x = (y-1)/2 \in R$

Thus, every element in the codomain has pre-image in the domain.
This implies that f is onto
Hence, f is a bijective map.

Identity function: Let X be any set and f be a function such that $f : X \rightarrow X$ is defined by $f(x) = x$ for all $x \in X$. Then, f is called the identity function or identity transformation on X. It can be denoted by I or I_X.

Note: The identity function is both one-to-one and onto.

Let $I_X(x) = I_X(y)$

$\Rightarrow x = y$

$\Rightarrow I_X$ is one-to-one

I_X is onto since $x = I_X(x)$ for all x.

Composition of Functions

Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ be two functions. Then the composition of f and g denoted by $g \circ f$, is the function from X to Z defined as

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

Note. In the above definition it is assumed that the range of the function f is a subset of Y (the Domain of g), i.e., $R_f \subseteq D_g$. $g \circ f$ is called the left composition g with f.

Example: Let $X = \{1, 2, 3\}$, $Y = \{p, q\}$ and $Z = \{a, b\}$. Also let $f : X \rightarrow Y$ be f $= \{(1, p), (2, q), (3, q)\}$ and $g : Y \rightarrow Z$ be given by $g = \{(p, b), (q, b)\}$. Find $g \circ f$. Solution: $g \circ f = \{(1, b), (2, b), (3, b)$.

Example: Let $X = \{1, 2, 3\}$ and f, g, h and s be the functions from X to X given by

$$f = \{(1, 2), (2, 3), (3, 1)\} \qquad g = \{(1, 2), (2, 1), (3, 3)\}$$
$$h = \{(1, 1), (2, 2), (3, 1)\} \qquad s = \{(1, 1), (2, 2), (3, 3)\}$$

Find $f \circ f$; $g \circ f$; $f \circ h \circ g$; $s \circ g$; $g \circ s$; $s \circ s$; and $f \circ s$.

Solution:

$$f \circ g = \{(1, 3), (2, 2), (3, 1)\}$$
$$g \circ f = \{(1, 1), (2, 3), (3, 2)\} \neq f \circ g$$
$$f \circ h \circ g = f \circ (h \circ g) = f \circ \{(1, 2), (2, 1), (3, 1)\}$$
$$= \{(1, 3), (2, 2), (3, 2)\}$$
$$s \circ g = \{(1, 2), (2, 1), (3, 3)\} = g$$
$$g \circ s = \{(1, 2), (2, 1), (3, 3)\}$$

$$\therefore s \circ g = g \circ s = g$$

$$s \circ s = \{(1, 1), (2, 2), (3, 3)\} = s$$
$$f \circ s = \{(1, 2), (2, 3), (3, 1)\}$$

Thus, s ∘ s = s, f ∘ g ≠ g ∘ f, s ∘ g = g ∘ s = g and h ∘ s = s ∘ h = h.

Example: Let $f(x) = x + 2$, $g(x) = x - 2$ and $h(x) = 3x$ for $x \in R$, where R is the set of real numbers. Find $g \circ f$; $f \circ g$; $f \circ f$; $g \circ g$; $f \circ h$; $h \circ g$; $h \circ f$; and $f \circ h \circ g$.

Solution: $f : R \to R$ is defined by $f(x) = x + 2$

f: $R \to R$ is defined by $g(x) = x - 2$

$h : R \to R$ is defined by $h(x) = 3x$

- $g \circ f : R \to R$

  Let $x \in R$. Thus, we can write

  $(g \circ f)(x) = g(f(x)) = g(x + 2) = x + 2 - 2 = x$

  $\therefore (g \circ f)(x) = \{(x, x)| x \in R\}$
- $(f \circ g)(x) = f(g(x)) = f(x - 2) = (x - 2) + 2 = x$

  $\therefore f \circ g = \{(x, x)| x \in R\}$
- $(f \circ f)(x) = f(f(x)) = f(x + 2) = x + 2 + 2 = x + 4$

  $\therefore f \circ f = \{(x, x + 4)| x \in R\}$
- $(g \circ g)(x) = g(g(x)) = g(x - 2) = x - 2 - 2 = x - 4$

  $\Rightarrow g \circ g = \{(x, x - 4)| x \in R\}$
- $(f \circ h)(x) = f(h(x)) = f(3x) = 3x + 2$

  $\therefore f \circ h = \{(x, 3x + 2)| x \in R\}$
- $(h \circ g)(x) = h(g(x)) = h(x - 2) = 3(x - 2) = 3x - 6$

  $\therefore h \circ g = \{(x, 3x - 6)| x \in R\}$
- $(h \circ f)(x) = h(f(x)) = h(x + 2) = 3(x + 2) = 3x + 6$ $h \circ f =$

  $\{(x, 3x + 6)| x \in R\}$
- $(f \circ h \circ g)(x) = [f \circ (h \circ g)](x)$

  $f(h \circ g(x)) = f(3x - 6) = 3x - 6 + 2 = 3x - 4$

  $\therefore f \circ h \circ g = \{(x, 3x - 4)| x \in R\}$.

Example: What is composition of functions? Let f and g be functions from R to R, where R is a set of real numbers defined by $f(x) = x^2 + 3x + 1$ and $g(x) = 2x - 3$. Find the composition of functions: i) $f \circ f$ ii) $f \circ g$ iii) $g \circ f$.

Inverse Functions

A function $f : X \to Y$ is aid to be *invertible* of its inverse function f^{-1} is also function from the range of f into X.

Theorem: A function $f : X \to Y$ is invertible $\Leftrightarrow f$ is one-to-one and onto.

Example: Let $X = \{a, b, c, d\}$ and $Y = \{(1, 2, 3, 4\}$ and let $f : X \to Y$ be given by $f = \{(a, 1), (b, 2), (c, 2), (d, 3)\}$. Is f^{-1} a function?

Solution: $f^{-1} = \{(1, a), (2, b), (2, c), (3, d)\}$. Here, 2 has two distinct images b and c.

Therefore, f^{-1} is not a function.

Example: Let R be the set of real numbers and $f : R \to R$ be given by $f = \{(x, x^2)| x \in R\}$. Is f^{-1} a function?

Solution: The inverse of the given function is defined as $f^{-1} = \{(x^2, x)| x \in R\}$.

Therefore, it is not a function.

Theorem: If $f : X \to Y$ and $g : Y \to X$ be such that $g \circ f = I_X$ and $f \circ g = I_Y$, then f and g are both invertible. Furthermore, $f^{-1} = g$ and $g^{-1} = f$.

Example: Let $X = \{1, 2, 3, 4\}$ and f and g be functions from X to X given by $f = \{(1, 4), (2, 1), (3, 2), (4, 3)\}$ and $g = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$. Prove that f and g are inverses of each other.

Solution: We check that

$(g \circ f)(1) = g(f(1)) = g(4) = 1 = I_X(1)$, $\quad (f \circ g)(1) = f(g(1)) = f(2) = 1 = I_X(1)$.

$(g \circ f)(2) = g(f(2)) = g(1) = 2 = I_X(2)$, $\quad (f \circ g)(2) = f(g(2)) = f(3) = 2 = I_X(2)$.

$(g \circ f)(3) = g(f(3)) = g(2) = 3 = I_X(3)$, $\quad (f \circ g)(3) = f(g(3)) = f(4) = 3 = I_X(3)$.

$(g \circ f)(4) = g(f(4)) = g(3) = 4 = I_X(4)$, $\quad (f \circ g)(4) = f(g(4)) = f(1) = 4 = I_X(4)$.

Thus, for all $x \in X$, $(g \circ f)(x) = I_X(x)$ and $(f \circ g)(x) = I_X(x)$. Therefore g is inverse of f and f is inverse of g.

Example: Show that the functions $f(x) = x^3$ and $g(x) = x^{1/3}$ for $x \in R$ are inverses of one another.

Solution: $f : R \to R$ is defined by $f(x) = x^3$; f: $R \to R$ is defined by $g(x) = x^{1/3}$

$$(f \circ g)(x) = f(g(x)) = f(x^{1/3}) = x^{3(1/3)} = x = I_X(x)$$

i.e., $(f \circ g)(x) = I_X(x)$

and $(g \circ f)(x) = g(f(x)) = g(x^3) = x^{3(1/3)} = x = I_X(x)$

i.e., $(g \circ f)(x) = I_X(x)$

Thus, $f = g^{-1}$ or $g = f^{-1}$

i.e., f and g are inverses of one other.

***Example: $f : R \to R$ is defined by $f(x) = ax + b$, for $a, b \in R$ and $a \neq 0$. Show that f is invertible and find the inverse of f.

(i) First we shall show that f is one-to-one

Let $x_1, x_2 \in R$ such that $f(x_1) = f(x_2)$

$\Rightarrow ax_1 + b = ax_2 + b$

$\Rightarrow ax_1 = ax_2$

$\Rightarrow x_1 = x_2$

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

- To show that f is onto.

  Let $y \in R$(codomain) such that $y = f(x)$ for some $x \in R$.

  $\Rightarrow y = ax + b$

  $\Rightarrow ax = y - b$

  $\Rightarrow x = (y-b)/a$

Given $y \in R$(codomain), there exists an element $x = (y-b)/a \in R$ such that $f(x) = y$.

$\therefore f$ is onto

$\Rightarrow f$ is invertible and $f^{-1}(x)= (x-b)/a$

Example: Let $f : R \rightarrow R$ be given by $f(x) = x^3 - 2$. Find f^{-1}.

(i) First we shall show that f is one-to-one

Let $x_1, x_2 \in R$ such that $f(x_1) = f(x_2)$

$\Rightarrow x^3_1 - 2 = x^3_2 -$

$2 \Rightarrow x^3_1 = x^3_2$

$\Rightarrow x_1 = x_2$

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

- To show that f is onto.

  $\Rightarrow y = x^3 - 2$

  $\Rightarrow x^3 = y+2$

  $\Rightarrow x= \sqrt[3]{y+2}$

Given $y \in R$(codomain), there exists an element $x = \sqrt[3]{y+2} \in R$ such that $f(x) = y$.

$\therefore f$ is onto

$\Rightarrow f$ is invertible and $f^{-1}(x) = \sqrt[3]{x+2}$

Floor and Ceiling functions:

Let x be a real number, then the least integer that is not less than x is called the CEILING of x.

The CEILING of x is denoted by $\lceil x \rceil$.

Examples: $\lceil 2.15 \rceil = 3, \lceil \sqrt{5} \rceil = 3, \lceil -7.4 \rceil = -7, \lceil -2 \rceil = -2$

Let x be any real number, then the greatest integer that does not exceed x is called the Floor of x.

The FLOOR of x is denoted by $\lfloor x \rfloor$.

Examples: $\lfloor 5.14 \rfloor = 5, \lfloor \sqrt{5} \rfloor = 2, \lfloor -7.6 \rfloor = -8, \lfloor 6 \rfloor = 6, \lfloor -3 \rfloor = -3$

Example: Let f and g abe functions from the positive real numbers to positive real numbers defined by $f(x) = \lfloor 2x \rfloor$, $g(x) = x^2$. Calculate $f \circ g$ and $g \circ f$.

Solution: $f \circ g(x) = f(g(x)) = f(x^2) = \lfloor 2x^2 \rfloor$

$g \circ f(x) = g(f(x)) = g(\lfloor 2x \rfloor) = (\lfloor 2x \rfloor)^2$

Recursive Function

Total function: Any function $f : N^n \rightarrow N$ is called *total* if it is defined for every n-tuple in N^n.

Example: $f(x, y) = x + y$, which is defined for all $x, y \in N$ and hence it is a total function.

Partial function: If $f : D \rightarrow N$ where $D \subseteq N^n$, then f is called a *partial function*.

Example: $g(x, y) = x - y$, which is defined for only $x, y \in N$ which satisfy $x \geq y$.

Hence $g(x, y)$ is partial.

Initial functions:

The initial functions over the set of natural numbers is given by

- ***Zero function*** Z: $Z(x) = 0$, for all x.
- ***Successor function*** S: $S(x) = x + 1$, for all x.
- ***Projection function*** U_i^n: $U_i^n(x_1, x_2, ..., x_n) = x_i$ for all n tuples $(x_1, x_2, ..., x_n)$, $1 \leq i \leq n$.

Projection function is also called *generalized identity function*.

For example, $U_1^1(x) = x$ for every $x \in N$ is the identity function.

$U_1^2(x, y) = x$, $U_1^3(2, 6, 9) = 2$, $U_2^3(2, 6, 9) = 6$, $U_3^3(2, 6, 9) = 9$.

Composition of functions of more than one variable:

The operation of composition will be used to generate the other function.

Let $f_1(x, y)$, $f_2(x, y)$ and $g(x, y)$ be any three functions. Then the composition of g with f_1 and f_2 is defined as a function $h(x, y)$ given by

$$h(x, y) = g(f_1(x, y), f_2(x, y)).$$

In general, let $f_1, f_2, ..., f_n$ each be partial function of m variables and g be a partial function of n variables. Then the composition of g with $f_1, f_2, ..., f_n$ produces a partial function h given by

$$h(x_1, x_2, ..., x_m) = g(f_1(x_1, x_2, ..., x_m), ..., f_n(x_1, x_2, ...x_m)).$$

Note: The function h is total iff $f_1, f_2, ..., f_n$ and g are total.

Example: Let $f_1(x, y) = x + y$, $f_2(x, y) = xy + y^2$ and $g(x, y) = xy$. Then

$$\begin{aligned} h(x, y) &= g(f_1(x, y), f_2(x, y)) \\ &= g(x + y, xy + y^2) \\ &= (x + y)(xy + y^2) \end{aligned}$$

Recursion: The following operation which defines a function $f(x_1, x_2, ..., x_n, y)$ of $n + 1$ variables by using other functions $g(x_1, x_2, .., x_n)$ and $h(x_1, x_2, ..., x_n, y, z)$ of n and $n + 2$ variables, respectively, is called *recursion*.

$$f(x_1, x_2, ..., x_n, 0) = g(x_1, x_2, ..., x_n)$$

$$f(x_1, x_2, ..., x_n, y + 1) = h(x_1, x_2, ..., x_n, y, f(x_1, x_2, ..., x_n, y))$$

where y is the inductive variable.

Primitive Recursive: A function f is said to be *Primitive recursive* iff it can be obtained from the initial functions by a finite number of operations of composition and recursion.

*****Example:** Show that the function $f(x, y) = x + y$ is primitive recursive. Hence compute the value of $f(2, 4)$.

Solution: Given that $f(x, y) = x + y$.

Here, $f(x, y)$ is a function of two variables. If we want f to be defined by recursion, we need a function g of single variable and a function h of three variables. Now,

$$f(x, y + 1) = x + (y + 1) = (x + y) + 1 = f(x, y) + 1.$$

Also, $f(x, 0) = x$.
We define $f(x, 0)$ as

$$f(x, 0) = x = U_1^1(x) = S(f(x, y)) = S(U_3^3(x, y, f(x, y)))$$

If we take $g(x) = U_1^1(x)$ and $h(x, y, z) = S(U_3^3(x, y, z))$, we get $f(x, 0) = g(x)$ and $f(x, y + 1) = h(x, y, z)$.
Thus, f is obtained from the initial functions U_1^1, U_3^3, and S by applying composition once and recursion once.
Hence f is primitive recursive.
Here,

$$f(2, 0) = 2$$
$$f(2, 4) = S(f(2, 3)) = S(S(f(2, 2))) = S(S(S(f(2, 1)))) = S(S(S(S(f(2, 0))))) = S(S(S(S(2))))) = S(S(S(3))) = S(S(4)) = S(5) = 6$$

Example: Show that $f(x, y) = x * y$ is primitive recursion.

Solution: Given that $f(x, y) = x * y$.
Here, $f(x, y)$ is a function of two variables. If we want f to be defined by recursion, we need a function g of single variable and a function h of three variables. Now, $f(x, 0) = 0$ and

$$f(x, y + 1) = x * (y + 1) = x * y$$

- $f(x, y) + x$

We can write

$$f(x, 0) = 0 = Z(x) \text{ and}$$
$$f(x, y + 1) = f_1(U_3^3(x, y, f(x, y)), U_1^3(x, y, f(x, y)))$$

where $f_1(x, y) = x + y$, which is primitive recursive. By taking $g(x) = Z(x) = 0$ and h defined by $h(x, y, z) = f_1(U_3^3(x, y, z), U_1^3(x, y, z)) = f(x, y + 1)$, we see that f defined by recursion. Since g and h are primitive recursive, f is primitive recursive. Example: Show that $f(x, y) = x^y$ is primitive recursive function. Solution: Note that $x^0 = 1$ for $x \neq 0$ and we put $x^0 = 0$ for $x = 0$.
Also, $x^{y+1} = x^y * x$

Here $f(x, y) = x^y$ is defined as

$$f(x, 0) = 1 = S(0) = S(Z(x))$$

$f(x, y + 1) = x * f(x, y)$

- $U_1^3(x, y, f(x, y)) * U_3^3(x, y, f(x, y))$

$h(x, y, f(x, y) = f_1(U_1^3(x, y, f(x, y)), U_3^3(x, y, f(x, y)))$ where $f_1(x, y) = x * y$, which is primitive recursive.

$\therefore f(x, y)$ is a primitive recursive function.

Example: Consider the following recursive function definition: If $x < y$ then $f(x, y) = 0$, if $y \leq x$ then $f(x, y) = f(x - y, y) + 1$. Find the value of $f(4, 7)$, $f(19, 6)$.

Solution: Given $f(x, y) = \begin{cases} 0; x < y \\ f(x-y, y)+1 \; ; y \leq x \end{cases}$

$$f(4, 7) = 0 \qquad [\because 4 < 7]$$

$$\begin{aligned} f(19, 6) &= f(19 - 6, 6) + 1 \\ &= f(13, 6) + 1 \\ f(13, 6) &= f(13 - 6, 6) + 1 \\ &= f(7, 6) + 1 \\ f(7, 6) &= f(7 - 6, 6) + 1 \\ &= f(1, 6) + 1 \\ &= 0 + 1 \\ &= 1 \\ f(13, 6) &= f(7, 6) + 1 \\ &= 1 + 1 \\ &= 2 \\ f(19, 6) &= 2 + 1 \\ &= 3 \end{aligned}$$

Example: Consider the following recursive function definition: If $x < y$ then $f(x, y) = 0$, if $y \leq x$ then $f(x, y) = f(x - y, y) + 1$. Find the value of $f(86, 17)$

Permutation Functions

Definition: A *permutation* is a one-one mapping of a non-empty set onto itself.

Let $S = \{a_1, a_2, ..., a_n\}$ be a finite set and p is a permutation on S, we list the elements of S and the corresponding functional values of $p(a_1), p(a_2), ..., p(a_n)$ in the following form:

$$\begin{pmatrix} a_1 & a_2 & . & . & . & a_n \\ p(a_1) & p(a_2) & . & . & . & p(a_n) \end{pmatrix}$$

If $p : S \to S$ is a bijection, then the number of elements in the given set is called the *degree* of its permutation.

Note: For a set with three elements, we have 3! permutations.

Example: Let $S = \{1, 2, 3\}$. The permutations of S are as follows:

$P_1=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$; $P_2=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$; $P_3=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$; $P_4=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$; $P_5=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$; $P_6=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Example: Let $S = \{1, 2, 3, 4\}$ and $p : S \to S$ be given by $f(1) = 2$, $f(2) = 1$, $f(3) = 4$, $f(4) = 3$. Write this in permutation notation.

Solution: The function can be written in permutation notation as given below:

$$f=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$$

Identity Permutation: If each element of a permutation be replaced by itself, then such a permutation is called the *identity permutation.*

Example: Let $S = \{a_1, a_2, , a_n\}$.then $I=\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ a_1 & a_2 & \dots & a_n\end{pmatrix}$ is the identity permutation on S.

Equality of Permutations: Two permutations f and g of degree n are said to be equal if and only if $f(a) = g(a)$ for all $a \in S$.

Example: Let $S = \{1, 2, 3, 4\}$

$$f=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 2 & 4\end{pmatrix};g=\begin{pmatrix}4 & 1 & 3 & 2\\ 4 & 3 & 2 & 1\end{pmatrix}$$

We have $f(1) = g(1) = 3$

$f(2) = g(2) = 1$

$f(3) = g(3) = 2$

$f(4) = g(4) = 4$

i.e., $f(a) = g(a)$ for all $a \in S$.

Product of Permutations: (or Composition of Permutations)

Let S={a,b,…h}and let $\begin{pmatrix}a & b & \dots & h\\ f(a) & f(b) & \dots & f(h)\end{pmatrix}$,g=$\begin{pmatrix}a & b & \dots & h\\ g(a) & g(b) & \dots & g(h)\end{pmatrix}$

We define the composite of f and g as follows:

$$f \circ g =\begin{pmatrix}a & b & \dots & h\\ f(a) & f(b) & \dots & f(h)\end{pmatrix} o \begin{pmatrix}a & b & \dots & h\\ g(a) & g(b) & \dots & g(h)\end{pmatrix}$$

$$=\begin{pmatrix}a & b & \dots & h\\ f(g(a)) & f(g(b)) & \dots & f(g(h))\end{pmatrix}$$

Clearly, $f \circ g$ is a permutation.

Example: Let $S = \{1, 2, 3, 4\}$ and let $f=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$ and $g=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}$ Find $f \circ g$ and $g \circ f$ in the permutation from.

Solution: $f \circ g = \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 4 & 1\end{pmatrix}; g \circ f=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}$

Note: The product of two permutations of degree n need not be commutative.

Inverse of a Permutation:

If f is a permutation on $S = \{a_1, a_2, , a_n\}$ such that $f =\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ b_1 & b_2 & \dots. & b_n\end{pmatrix}$

then there exists a permutation called the inverse f, denoted f^{-1} such that $f \circ f^{-1} = f^{-1} \circ f = I$ (the identity permutation on S)

where $f^{-1} = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$

Example: If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$, then find f^{-1}, and show that $f \circ f^{-1} = f^{-1} \circ f = I$

Solution: $f^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$

$$f \circ f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \text{o} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Similarly, $f^{-1} \circ f = I. \Rightarrow f \circ f^{-1} = f^{-1} \circ f = I.$

Cyclic Permutation: Let $S = \{a_1, a_2, ..., a_n\}$ be a finite set of n symbols. A permutation f defined on S is said to be *cyclic permutation* if f is defined such that

$$f(a_1) = a_2, f(a_2) = a_3, ..., f(a_{n-1}) = a_n \text{ and } f(a_n) = a_1.$$

Example: Let $S = \{1, 2, 3, 4\}$.

Then $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$=(1 4)(2 3) is a cyclic permutation.

Disjoint Cyclic Permutations: Let $S = \{a_1, a_2, ..., a_n\}$. If f and g are two cycles on S such that they have no common elements, then f and g are said to be disjoint cycles.

Example: Let $S = \{1, 2, 3, 4, 5, 6\}$.

If $f = (1\ 4\ 5)$ and $g = (2\ 3\ 6)$ then f and g are disjoint cyclic permutations on S.

Note: The product of two disjoint cycles is commutative.

Example: Consider the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 \end{pmatrix}$

The above permutation f can be written as $f = (1\ 2\ 3\ 4\ 5)(6\ 7)$. Which is a product of two disjoint cycles.

Transposition: A cyclic of length 2 is called a *transposition*.

Note: Every cyclic permutation is the product of transpositions.

Example: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$=(1 2 4)(3 5) = (1 4)(1 2)(3 5).

Inverse of a Cyclic Permutation: To find the inverse of any cyclic permutation, we write its elements in the reverse order.

For example, $(1\ 2\ 3\ 4)^{-1} = (4\ 3\ 2\ 1)$.

Even and Odd Permutations: A permutation *f* is said to be an *even permutation* if *f* can be expressed as the product of even number of transpositions.

A permutation *f* is said to be an *odd permutation* if *f* is expressed as the product of odd number of transpositions.

Note:

(i) An identity permutation is considered as an even permutation.

(ii) A transposition is always odd.

(iii). The product of an even and an odd permutation is odd. Similarly the product of an odd permutation and even permutations is odd.

Example: Determine whether the following permutations are even or odd permutations.

(i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$

(ii) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 7 & 8 & 6 & 1 & 4 & 3 \end{pmatrix}$

(iii) $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$

Solution: (i). For $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} = (1\ 2\ 4) = (1\ 4)(1\ 2)$

$\Rightarrow f$ is an even permutation

(ii). For $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 7 & 8 & 6 & 1 & 4 & 3 \end{pmatrix}$

= (1 2 5 6)(3 7 4 8) = (1 6)(1 5)(1 2)(3 8)(3 4)(3 7)

$\Rightarrow$ g is an even permutation.

(iii) h= $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$ = (1 4 2 3) = (1 3)(1 2)(1 4)

Product of three transpositions

$\Rightarrow h$ is an odd permutation.

Lattices

In this section, we introduce lattices which have important applications in the theory and design of computers.

Definition: A lattice is a partially ordered set $(L, \leq)$ in which every pair of elements $a, b \in L$ has a greatest lower bound and a least upper bound.

Example: Let Z^+ denote the set of all positive integers and let R denote the relation 'division' in Z^+, such that for any two elements $a, b \in Z^+$, aRb, if a divides b. Then (Z^+, R) is a lattice in which the join of a and b is the least common multiple of a and b, i.e.

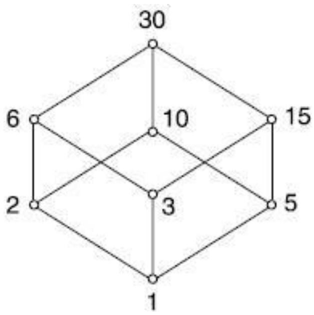
$$a \vee b = a \oplus b = \text{LCM of } a \text{ and } b,$$

and the meet of a and b, i.e. $a * b$ is the greatest common divisor (GCD) of a and b i.e.,

$$a \wedge b = a * b = \text{GCD of } a \text{ and } b.$$

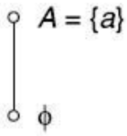
We can also write $a+b = a \vee b = a \oplus b$=LCM of a and b and $a.b = a \wedge b = a * b$=GCD of a and b.

Example: Let n be a positive integer and S_n be the set of all divisors of n If $n = 30$, $S_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$. Let R denote the relation division as defined in Example 1. Then (S_{30}, R) is a Lattice see Fig:

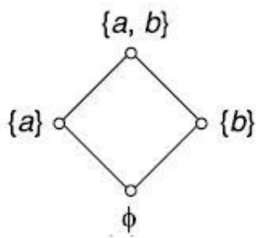


Example: Let A be any set and $P(A)$ be its power set. The poset $P(A), \subseteq)$ is a lattice in which the meet and join are the same as the operations $\cap$ and $\cup$ on sets respectively.

$S = \{a\}$, $P(A) = \{\phi, \{a\}\}$



$S = \{a, b\}$, $P(A) = \{\phi, \{a\}, \{a\}, S\}$.



Some Properties of Lattice

Let $(L, \leq)$ be a lattice and $*$ and $\oplus$ denote the two binary operation meet and join on $(L, \leq)$. Then for any $a, b, c \in L$, we have

(L1): $a * a = a$, $(L1)'$: $a \oplus a = a$ (Idempotent laws)

$(L2)$: $b * a = b * a$, $(L2)'$: $a \oplus b = b + a$ (Commutative laws)

$(L3)$: $(a * b) * c = a * (b * c)$, $(L3)'$: $(a \oplus b) \oplus c = a \oplus (b + c)$ (Associative laws)

$(L4)$: $a * (a + b) = a$, $(L4)'$: $a \oplus (a * b) = a$ (Absorption laws).

The above properties $(L1)$ to $(L4)$ can be proved easily by using definitions of meet and join. We can apply the principle of duality and obtain $(L1)'$ to $(L4)'$.

Theorem: Let $(L, \leq)$ be a lattice in which $*$ and $\oplus$ denote the operations of meet and join respectively. For any $a, \in L$, $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$.

Proof: We shall first prove that $a \leq b \Leftrightarrow a * b = b$.

In order to do this, let us assume that $a \leq b$. Also, we know that $a \leq a$.

Therefore $a \leq a * b$. From the definition of $a * b$, we have $a * b \leq a$.

Hence $a \leq b \Rightarrow a * b = a$.

Next, assume that $a * b = a$; but it is only possible if $a \leq b$, that is, $a * b = a \Rightarrow a \leq b$.
Combining these two results, we get the required equivalence.

It is possible to show that $a \leq b \Leftrightarrow a \oplus b = b$ in a similar manner.

Alternatively, from $a * b = a$, we have

$$b \oplus (a * b) = b \oplus a = a \oplus b$$

$$\text{but } b \oplus (a * b) = b$$

Hence $a \oplus b = b$ follows from $a * b = a$.

By repeating similar steps, we can show that $a * b = a$ follows from $a \oplus b = b$.

Therefore $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$.

Theorem: Let $(L, \leq)$ be a lattice. Then $b \leq c \Rightarrow \begin{cases} a * b \leq a * c \\ \mathrm{a} \oplus \mathrm{b} \leq \mathrm{a} \oplus \mathrm{c} \end{cases}$

Proof: By above theorem $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$.

To show that $a * b \leq a * c$, we shall show that $(a * b) * (a * c) = a * b$

$$\begin{aligned}(a * b) * (a * c) &= a * (b * a) * c \\ &= a * (a * b) * c \\ &= (a * a) * (b * c) \\ &= a * (b * c) \\ &= a * b\end{aligned}$$

$\therefore$ If $\mathrm{b} \leq \mathrm{c}$ then $\mathrm{a} * \mathrm{b} \leq \mathrm{a} * \mathrm{c}$. Next, let $b \leq c \Rightarrow b \oplus c = c$.

To show that $a \oplus b \leq a \oplus c$. It sufficient to show that $(a \oplus b) \oplus (a \oplus c) = a \oplus c$.

Consider, $(a \oplus b) \oplus (a \oplus c) = a \oplus (b \oplus a) \oplus c$

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

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

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

$= a \oplus b$

$\therefore$ If $b \leq c$ then $a \oplus b \leq a \oplus c$.

Note: The above properties of a Lattice are called properties of Isotonicity.

Lattice as an algebraic system:

We now define lattice as an algebraic system, so that we can apply many concepts associated with algebraic systems to lattices.

Definition: A lattice is an algebraic system $(L, *, \oplus)$ with two binary operation '$*$'and '$\oplus$' on L which are both commutative and associative and satisfy absorption laws.

Bounded Lattice:

A bounded lattice is an algebraic structure $(L,\wedge,\vee,0,1)$ sucha that $(L,\wedge,\vee)$ is a lattice, and the constants $0,1\in L$ satisfy the following:

1. for all $x\in L$, $x\wedge 1=x$ and $x\vee 1=1$
2. for all $x\in L$, $x\wedge 0=0$ and $x\vee 0=x$.

The element 1 is called the upper bound, or top of L and the element 0 is called the lower bound or bottom of L.

Distributive lattice:

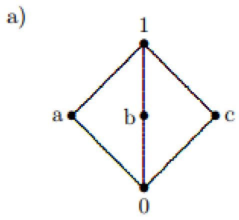
A lattice $(L,\vee,\wedge)$ is **distributive** if the following additional identity holds for all x, y, and z in L:

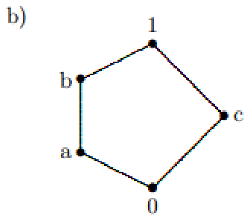
$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

Viewing lattices as partially ordered sets, this says that the meet peration preserves nonempty finite joins. It is a basic fact of lattice theory that the above condition is equivalent to its dual

$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ for all x, y, and z in L.

Example: Show that the following simple but significant lattices are not distributive.



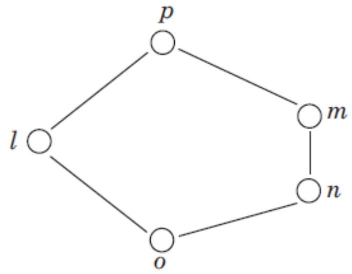


Solution a) To see that the diamond lattice is not distributive, use the middle elements of the lattice: $a \wedge (b \vee c) = a \wedge 1 = a$, but $(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$, and $a \neq 0$.

Similarly, the other distributive law fails for these three elements.

b) The pentagon lattice is also not distributive

Example: Show that lattice is not a distributive lattice.



Sol. A lattice is distributive if all of its elements follow distributive property so let we verify the distributive property between the elements *n*, *l* and *m*.

GLB(*n*, LUB(*l*, *m*)) = GLB(*n*, *p*) [∴ LUB(*l*, *m*) = *p*]

= *n* (LHS)

also LUB(GLB(*n*, *l*), GLB(*n*, *m*)) = LUB(*o*, *n*); [∴ GLB(*n*, *l*) = *o* and GLB(*n*, *m*) = *n*]

= *n* (RHS)

so LHS = RHS.

But GLB(*m*, LUB(*l*, *n*)) = GLB(*m*, *p*) [∴ LUB(*l*, *n*) = *p*]

= *m* (LHS)

also LUB(GLB(*m*, *l*), GLB(*m*, *n*)) = LUB(*o*, *n*); [∴ GLB(*m*, *l*) = *o* and GLB(*m*, *n*) = *n*]

= *n* (RHS)

Thus, LHS ≠ RHS hence distributive property doesn't hold by the lattice so lattice is not distributive.

Example: Consider the poset (X, ≤) where X = {1, 2, 3, 5, 30} and the partial ordered relation ≤ is defined as i.e. if x and y ∈X then x ≤ y means 'x divides y'. Then show that poset (I+, ≤) is a lattice.

Sol. Since GLB(*x*, *y*) = *x* ∧ *y* = *lcm*(*x*, *y*)

and LUB(*x*, *y*) = *x* ∨ *y* = *gcd*(*x*, *y*)

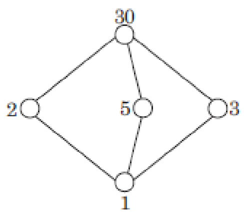
Now we can construct the operation table I and table II for GLB and LUB respectively and the Hasse diagram is shown in Fig.

Table I

LUB	1	2	3	5	30
1	1	2	3	5	30
2	2	2	30	30	30
3	3	30	3	30	30
5	5	30	30	5	30
30	30	30	30	30	30

Table II

GLB	1	2	3	5	30
1	1	1	1	1	1
2	1	2	1	1	2
3	1	1	3	1	3
5	1	1	1	5	5
30	1	2	3	5	30



Test for distributive lattice, i.e.,

GLB(*x*, LUB(*y*, *z*)) = LUB(GLB(*x*, *y*), GLB(*x*, *z*))

Assume *x* = 2, *y* = 3 and *z* = 5, then

*RHS:*GLB(2, LUB(3, 5)) = GLB(2, 30) = 2

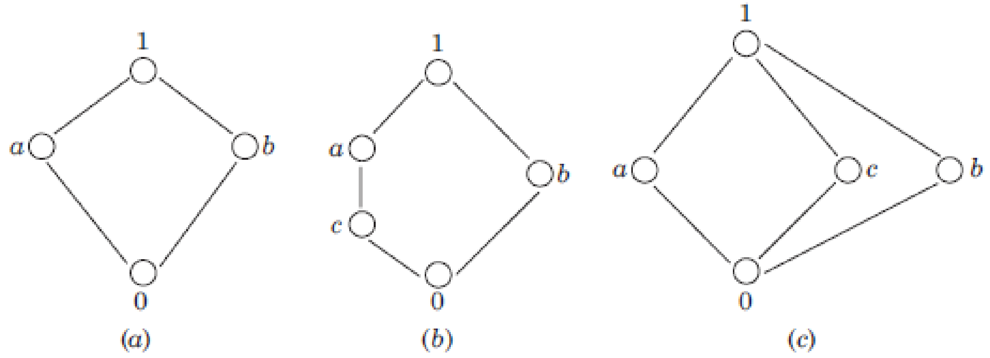
LHS: LUB(GLB(2, 3), GLB(2, 5)) = LUB(1, 1) = 1

Since*RHS* ≠ *LHS*, hence lattice is not a distributive lattice.

Complemented lattice:

A complemented lattice is a bounded lattice (with least element 0 and greatest element 1), in which every element a has a complement, i.e. an element b satisfying a ∨ b = 1 and a ∧ b = 0. Complements need not be unique.

Example: Lattices shown in Fig (a), (b) and (c) are complemented lattices.



Sol.

For the lattice (*a*) GLB(*a*, *b*) = 0 and LUB(*x*, *y*) = 1. So, the complement *a* is *b* and vise versa. Hence, a complement lattice.

For the lattice (*b*) GLB(*a*, *b*) = 0 and GLB(*c*, *b*) = 0 and LUB(*a*, *b*) = 1 and LUB(*c*, *b*) = 1; so both *a* and *c* are complement of *b*.
Hence, a complement lattice.

In the lattice (*c*) GLB(*a*, *c*) = 0 and LUB(*a*, *c*) = 1; GLB(*a*, *b*) = 0 and LUB(*a*, *b*) = 1. So, complement of *a* are *b* and *c*.
Similarly complement of *c* are *a* and *b* also *a* and *c* are complement of *b*.
Hence lattice is a complement lattice.

Previous Questions

1. a) Let R be the Relation R= {(x,y)/ x divides y)} . Draw the Hasse diagram?
   b) Explain in brief about lattice?
   c) Define Relation? List out the Operations on Relations
2. Define Relation? List out the Properties of Binary operations?
3. Let the Relation R be R={(1,2) ,(2,3),(3,3)} on the set A= {1,2,3}. What is the Transitive Closure of R?
4. Explain in brief about Inversive and Recursive functions with examples?
5. Prove that (S, ≤) is a Lattice, where S= {1,2,5,10} and ≤ is for divisibility. Prove that it is also a Distributive Lattice?
6. Prove that (S,≤) is a Lattice, where S= {1,2,3,6} and ≤ is for divisibility. Prove that it is also a Distributive Lattice?
7. Let A be a given finite set and P(A) its power set. Let ⊆ be the inclusion relation on the elements of P(A). Draw Hasse diagrams of (P(A), ⊆) for A={a}; A={a,b}; A={a,b,c} and A={a,b.c.d}.
8. Let Fx be the set of all one-to-one onto mappings from X onto X, where X={1,2,3}. Find all the elements of Fx and find the inverse of each element.
9. Show that the function f(x) = x+y is primitive recursive.
10. Let X={2,3,6,12,24,36) and a relation ≤' be such that x≤ _if x divides y. Draw the Hasse diagram of (x,≤).
11. If A={1,2,3,4} and P={{1,2},{3},{4}} is a partition of A, find the equivalence relation

determined by P.

12. Let X={1,2,3} and f, g, h and s be functions from X to X given by f={<1,2>, <2,3>, <3,1>} g={<1,2>, <2,1>, <3,3>} h={<1,1>, <2,2>, <3,1>} and s={<1,1>, <2,2>, <3,3>}. Find fog, fohog, gos, fos.
13. Let X={1,2,3,4} and R={<1,1>, <1,4>, <4,1>, <4,4>, <2,2>, <2,3>, <3,2>, <3,3>}. Write the matrix of R and sketch its graph.

14.Let X = {a,b,c,d,e} and let C = {{a,b},{c},{d,e}}. Show that the partition C defines an equivalence relation on X.

15.Show that the function f(x)= $\begin{cases} x/2; & when\ x\, is\, even \\ (x-1)/2; & when\, x\, is\, odd \end{cases}$ is primitive recursive.

16. If A={1,2,3,4} and R,S are relations on A defined by R={(1,2),(1,3),(2,4),(4,4)} S={(1,1),(1,2),(1,3),(1,4),(2,3),(2,4)} find R o S, S o R, R^2, S^2, write down there matrices.
17. Determine the number of positive integers n where 1≤n≤2000 and n is not divisible by2,3 or 5 but is divisible by 7.
18. Determine the number of positive integers n where 1≤n≤100 and n is not divisible by2,3 or 5.
19. Which elements of the poset /({2,4,5,10,12,20,25},/) are maximal and which are minimal?
20. Let X={(1,2,3} and f,g,h and s be functions from X to X given by f={(1,2),(2,3),(3,1)}, g={(1,2),(2,1),(3,3)}, h={(1,1),(2,2),(3,1) and s={(1,1),(2,2),(3,3)}.

Multiple choice questions

1. A _______ is an ordered collection of objects.
   a) Relation b) Function c) Set d) Proposition
   Answer: c
2. The set O of odd positive integers less than 10 can be expressed by ___________ .
   a) {1, 2, 3} b) {1, 3, 5, 7, 9} c) {1, 2, 5, 9} d) {1, 5, 7, 9, 11}
   Answer: b
3. Power set of empty set has exactly _____ subset.
   a) One b) Two c) Zero d) Three
   Answer: a
4. What is the Cartesian product of A = {1, 2} and B = {a, b}?
   a) {(1, a), (1, b), (2, a), (b, b)} b) {(1, 1), (2, 2), (a, a), (b, b)}
   c) {(1, a), (2, a), (1, b), (2, b)} d) {(1, 1), (a, a), (2, a), (1, b)}
   Answer: c
5. The Cartesian Product B x A is equal to the Cartesian product A x B. Is it True or False?
   a) True b) False
   Answer: b
6. What is the cardinality of the set of odd positive integers less than 10?
   a) 10 b) 5 c) 3 d) 20
   Answer: b
7. Which of the following two sets are equal?
   a) A = {1, 2} and B = {1} b) A = {1, 2} and B = {1, 2, 3}
   c) A = {1, 2, 3} and B = {2, 1, 3} d) A = {1, 2, 4} and B = {1, 2, 3}
   Answer: c
8. The set of positive integers is _________.
   a) Infinite b) Finite c) Subset d) Empty
   Answer: a

9. What is the Cardinality of the Power set of the set {0, 1, 2}.

a) 8 b) 6 c) 7 d) 9

Answer: a

10. The members of the set S = {x | x is the square of an integer and x < 100} is-----

a) {0, 2, 4, 5, 9, 58, 49, 56, 99, 12} b) {0, 1, 4, 9, 16, 25, 36, 49, 64, 81}

c) {1, 4, 9, 16, 25, 36, 64, 81, 85, 99} d) {0, 1, 4, 9, 16, 25, 36, 49, 64, 121}

Answer: b

11. Let R be the relation on the set of people consisting of (a,b) where aa is the parent of b. Let S be the relation on the set of people consisting of (a,b) where a and b are siblings. What are S∘R and R∘S?

A) (a,b) where a is a parent of b and b has a sibling; (a,b) where a is the aunt or uncle of b.

B) (a,b) where a is the parent of b and a has a sibling; (a,b) where a is the aunt or uncle of b.

C) (a,b) where a is the sibling of b's parents; (a,b) where aa is b's niece or nephew.

D) (a,b) where a is the parent of b; (a,b) where a is the aunt or uncle of b.

12. On the set of all integers, let (x,y)∈R(x,y)∈R *iff* xy≥1xy≥1. Is relation R reflexive, symmetric, antisymmetric, transitive?

A) Yes, No, No, Yes B) No, Yes, No, Yes

C) No, No, No, Yes D) No, Yes, Yes, Yes E) No, No, Yes, No

13. Let R be a non-empty relation on a collection of sets defined by ARB if and only if A∩ B = ØThen (pick the TRUE statement)

A.R is relexive and transitive B.R is symmetric and not transitive

C.R is an equivalence relation D.R is not relexive and not symmetric

Option: B

14. Consider the divides relation, m | n, on the set A = {2, 3, 4, 5, 6, 7, 8, 9, 10}. The cardinality of the covering relation for this partial order relation (i.e., the number of edges in the Hasse diagram) is

(a) 4 (b) 6 (c) 5 (d) 8 (e) 7

Ans:e

15. Consider the divides relation, m | n, on the set A = {2, 3, 4, 5, 6, 7, 8, 9, 10}. Which of the following permutations of A is not a topological sort of this partial order relation?

(a) 7,2,3,6,9,5,4,10,8 (b) 2,3,7,6,9,5,4,10,8

(c) 2,6,3,9,5,7,4,10,8 (d) 3,7,2,9,5,4,10,8,6

(e) 3,2,6,9,5,7,4,10,8

Ans:c

16. Let A = {2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} and consider the divides relation on A. Let C denote the length of the maximal chain, M the number of maximal elements, and m the number of minimal elements. Which is true?

(a) C = 3, M = 8, m = 6 *(b) C = 4, M = 8, m = 6*

(c) C = 3, M = 6, m = 6 *(d) C = 4, M = 6, m = 4*

(e) C = 3, M = 6, m = 4

Ans:a

17. What is the smallest N > 0 such that any set of N nonnegative integers must have two distinct integers whose sum or difference is divisible by 1000?

(a) 502 (b) 520 (c) 5002 (d) 5020 (e) 52002

Ans:a

18. Let R and S be binary relations on a set A. Suppose that R is reflexive, symmetric, and transitive and that S is symmetric, and transitive but is not reflexive. Which statement is always true for any such R and S?

(a) R ∪ S is symmetric but not reflexive and not transitive.

(b) R ∪ S is symmetric but not reflexive.

(c) R ∪ S is transitive and symmetric but not reflexive

(d) R ∪ S is reflexive and symmetric. (e) R ∪ S is symmetric but not transitive.
Ans:d

19. Let R be a relation on a set A. Is the transitive closure of R always equal to the transitive closure of R^2? Prove or disprove.
    Solution: Suppose A = {1, 2, 3} and R = {(1, 2),(2, 3)}. Then R2 = {(1, 3)}.
    Transitive closure of R is R∗ = {(1, 2),(2, 3),(1, 3)}.
    Transitive closure of R^2 is {(1, 3)}.
    They are not always equal.
20. Suppose R1 and R2 are transitive relations on a set A. Is the relation R1 ∪ R2 necessariy a transitive relation? Justify your answer.
    Solution: No. {(1, 2)} and {(2, 3)} are each transitive relations, but their union {(1, 2),(2, 3)} is not transitive.
21. Let D_{30} = {1, 2, 3, 4, 5, 6, 10, 15, 30} and relation I be partial ordering on D_{30}. The all lower bounds of 10 and 15 respectively are
    A.1,3 B.1,5 C.1,3,5 D.None of these Option: B
22. Hasse diagrams are drawn for
    A.partially ordered sets B.lattices C.boolean Algebra D.none of these
    Option: D
23. A self-complemented, distributive lattice is called
    A.Boolean algebra B.Modular lattice C.Complete lattice D.Self dual lattice
    Option: A
24. Let D30 = {1, 2, 3, 5, 6, 10, 15, 30} and relation I be a partial ordering on D30. The lub of 10 and 15 respectively is
    A.30 B.15 C.10 D.6 Option: A

25: Let X = {2, 3, 6, 12, 24}, and ≤ be the partial order defined by X ≤ Y if X divides Y. Number of edges in the Hasse diagram of (X, ≤) is
    A.3 B.4 C.5 D.None of these
    Option: B

26. Principle of duality is defined as
    A.≤ is replaced by ≥ B.LUB becomes GLB
    C.all properties are unaltered when ≤ is replaced by ≥
    D.all properties are unaltered when ≤ is replaced by ≥ other than 0 and 1 element.
    Option: D
27. Different partially ordered sets may be represented by the same Hasse diagram if they are
    A.same B.lattices with same order C.isomorphic D.order-isomorphic
    Option: D
28. The absorption law is defined as
    A.a * (a * b) = b B.a * (a ⊕ b) = b C.a * (a * b) = a ⊕ bD.a * (a ⊕ b) = a
    Option: D
29. A partial order is deined on the set S = {x, a_1, a_2, a_3,...... a_n, y} as x ≤ a i for all i and a_i ≤ y for all i, where n ≥ 1. Number of total orders on the set S which contain partial order ≤ is
    A.1 B.n C.n + 2 D.n ! Option: D
30. Let L be a set with a relation R which is transitive, antisymmetric and reflexive and for any two elements a, b ∈ L. Let least upper bound lub (a, b) and the greatest lower bound glb (a, b) exist. Which of the following is/are TRUE ?
    A.L is a Poset B.L is a boolean algebra C.L is a lattice D.none of these
    Option: C

UNIT-3
Algebraic Structures

Algebraic Systems with One Binary Operation
Binary Operation

Let S be a non-empty set. If $f : S \times S \to S$ is a mapping, then f is called a binary operation or binary composition in S.

The symbols $+$, $\cdot$, $*$, $\oplus$ etc are used to denote binary operations on a set.

- For $a, b \in S \Rightarrow a + b \in S \Rightarrow +$ is a binary operation in S.
- For $a, b \in S \Rightarrow a \cdot b \in S \Rightarrow \cdot$ is a binary operation in S.
- For $a, b \in S \Rightarrow a \circ b \in S \Rightarrow \circ$ is a binary operation in S.
- For $a, b \in S \Rightarrow a * b \in S \Rightarrow *$ is a binary operation in S.

- This is said to be the closure property of the binary operation and the set S is said to be closed with respect to the binary operation.

Properties of Binary Operations

Commutative: $*$ is a binary operation in a set S. If for $a, b \in S$, $a * b = b * a$, then $*$ is said to be commutative in S. This is called commutative law.

Associative: $*$ is a binary operation in a set S. If for $a, b, c \in S$, $(a*b)*c = a*(b*c)$, then $*$ is said to be associative in S. This is called associative law.

Distributive: $\circ$, $*$ are binary operations in S. If for $a, b, c \in S$, (i) $a \circ (b * c) = (a \circ b) * (a \circ c)$, (ii) $(b * c) \circ a = (b \circ a) * (c \circ a)$, then $\circ$ is said to be distributive w.r.t the operation $*$.

Example: N is the set of natural numbers.

(i) $+, \cdot$ are binary operations in N, since for $a, b \in N$, $a + b \in N$ and $a \cdot b \in N$. In other words N is said to be closed w.r.t the operations $+$ and $\cdot$.

(ii) $+, \cdot$ are commutative in N, since for $a, b \in N$, $a + b = b + a$ and $a \cdot b = b \cdot a$.

(iii) $+, \cdot$ are associative in N, since for $a, b, c \in N$,
$a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iv) is distributive w.r.t the operation $+$ in N, since for $a, b, c \in N$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

(v) The operations subtraction $(-)$ and division $(\div)$ are not binary operations in N, since for $3, 5 \in N$ does not imply $3 - 5 \in N$ and $\frac{3}{5} \in N$.

Example: A is the set of even integers.

(i) $+, \cdot$ are binary operations in A, since for $a, b \in A$, $a + b \in A$ and $a \cdot b \in A$.

(i) $+, \cdot$ are commutative in A, since for $a, b \in A$, $a + b = b + a$ and $a \cdot b = b \cdot a$.

(ii) $+, \cdot$ are associative in A, since for $a, b, c \in A$,
$a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iv) $\cdot$ is distributive w.r.t the operation $+$ in A, since for $a, b, c \in A$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

Example: Let S be a non-empty set and $\circ$ be an operation on S defined by $a \circ b = a$ for $a, b \in S$. Determine whether $\circ$ is commutative and associative in S.

Solution: Since $a \circ b = a$ for $a, b \in S$ and $b \circ a = b$ for $a, b \in S$.

$$\Rightarrow a \circ b \neq b \circ a.$$

$\therefore \circ$ is not commutative in S.

Since $(a \circ b) \circ c = a \circ c = a$

$a \circ (b \circ c) = a \circ b = a$ for $a, b, c \in S$.

$\therefore \circ$ is associative in S.

Example: $\circ$ is operation defined on Z such that $a \circ b = a + b - ab$ for $a, b \in Z$. Is the operation $\circ$ a binary operation in Z? If so, is it associative and commutative in Z?

Solution: If $a, b \in Z$, we have $a + b \in Z$, $ab \in Z$ and $a + b - ab \in Z$.

$$\Rightarrow a \circ b = a + b - ab \in Z.$$

$\therefore \circ$ is a binary operation in Z.

$$\Rightarrow a \circ b = b \circ a.$$

$\therefore \circ$ is commutative in Z.

Now

$$(a \circ b) \circ c = (a \circ b) + c - (a \circ b)c$$
$$= a + b - ab + c - (a + b - ab)c$$
$$= a + b - ab + c - ac - bc + abc$$

and

$$a \circ (b \circ c) = a + (b \circ c) - a(b \circ c)$$
$$= a + b + c - bc - a(b + c - bc)$$
$$= a + b + c - bc - ab - ac + abc$$
$$= a + b - ab + c - ac - bc + abc$$

$\Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$. $\therefore$

$\circ$ is associative in Z.

Example: Fill in blanks in the following composition table so that $\circ$ is associative in $S = \{a,b,c,d\}$.

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d				

Solution: $d \circ a = (c \circ b) \circ a$ [$\because c \circ b = d$]

$= c \circ (b \circ a)$ [$\because \circ$ is associative]

$= c \circ b$

$= d$

$d \circ b = (c \circ b) \circ b = c \circ (b \circ b) = c \circ a = c.$

$d \circ c = (c \circ b) \circ c = c \circ (b \circ c) = c \circ c = c.$

$d \circ d = (c \circ b) \circ (c \circ b)$
$= c \circ (b \circ c) \circ b$
$= c \circ c \circ b$
$= c \circ (c \circ b)$
$= c \circ d$
$= d$

Hence, the required composition table is

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d	d	c	c	d

Example: Let $P(S)$ be the power set of a non-empty set S. Let $\cap$ be an operation in $P(S)$. Prove that associative law and commutative law are true for the operation in $P(S)$.

Solution: P(S)= Set of all possible subsets of S.
Let A,B $\in$ P(S).
Since $A \subseteq S, B \subseteq S \Rightarrow A \cap B \subseteq S \Rightarrow A \cap B \in P(S)$.

$\therefore \cap$ is a binary operation in $P(S)$.

Also $A \cap B = B \cap A$

$\therefore \cap$ is commutative in $P(S)$.

Again $A \cap B$, $B \cap C$, $(A \cap B) \cap C$ and $A \cap (B \cap C)$ are subsets of S.

$\therefore (A \cap B) \cap C, A \cap (B \cap C) \in P(S)$.

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

$\therefore \cap$ is associative in $P(S)$.

Algebraic Structures

Definition: A non-empty set G equipped with one or more binary operations is called an *algebraic structure* or an *algebraic system*.
If $\circ$ is a binary operation on G, then the algebraic structure is written as $(G, \circ)$.
Example: $(N, +)$, $(Q, -)$, $(R, +)$ are algebraic structures.

Semi Group

Definition: An algebraic structure $(S, \circ)$ is called a *semi group* if the binary oper-ation $\circ$ is associative in S.
That is, $(S, \circ)$ is said to be a semi group if

(i) $a, b \in S \Rightarrow a \circ b \in S$ for all $a, b \in S$

(ii) $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in S$.

Example:

1. $(N, +)$ is a semi group. For $a, b \in N \Rightarrow a + b \in N$ and $a, b, c \in N \Rightarrow (a + b) + c = a + (b + c)$.

2. $(Q, -)$ is not a semi group. For $5, 3/2, 1 \in Q$ does not imply $(5 - 3/2) - 1 = 5 - (3/2 - 1)$.

3. $(R, +)$ is a semi group. For $a, b \in R \Rightarrow a + b \in R$ and $a, b, c \in R \Rightarrow (a + b) + c = a + (b + c)$.

Example: The operation $\circ$ is defined by $a \circ b = a$ for all $a, b \in S$. Show that $(S, \circ)$ is a semi group.

Solution: Let $a, b \in S \Rightarrow a \circ b = a \in S$.

$\therefore \circ$ is a binary operation in S. Let $a, b, c \in S$, $a \circ (b \circ c) = a \circ b = a$
$(a \circ b) \circ c = a \circ c = a$.

$\Rightarrow \circ$ is associative in S.

$\therefore (S, \circ)$ is a semi group.

Example: The operation $\circ$ is defined by $a \circ b = a + b - ab$ for all $a, b \in Z$. Show that $(Z, \circ)$ is a semi group.

Solution: Let $a, b \in Z \Rightarrow a \circ b = a + b - ab \in Z$.

$\therefore \circ$ is a binary operation in Z.

Let $a, b, c \in Z$.

$$\begin{aligned}(a \circ b) \circ c &= (a + b - ab) \circ c \\ &= a + b - ab + c - (a + b - ab)c \\ &= a + b + c - ab - bc - ac + abc\end{aligned}$$

$$\begin{aligned}a \circ (b \circ c) &= a \circ (b + c - bc) \\ &= a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - bc - ab - ac +\end{aligned}$$

$abc \Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$.

$\Rightarrow \circ$ is associative in Z. $\therefore (Z, \circ)$ is semi group.

Example: $(P(S), \cap)$ is a semi group, where $P(S)$ is the power set of a non-empty set S.
Solution: $P(S)$= Set of all possible subsets of S.

Let $A, B \in P(S)$.

Since $A \subseteq S, B \subseteq S \Rightarrow A \cap B \subseteq S \Rightarrow A \cap B \in P(S)$.

$\therefore \cap$ is a binary operation in $P(S)$. Let $A, B, C \in P(S)$.

$\therefore (A \cap B) \cap C, A \cap (B \cap C) \in P(S)$. Since $(A \cap B) \cap C$
$= A \cap (B \cap C)$

$\therefore \cap$ is associative in $P(S)$.
Hence $(P(S), \cap)$ is a semi group.

Example: $(P(S), \cup)$ is a semi group, where $P(S)$ is the power set of a non-empty set S.
Solution: $P(S)$= Set of all possible subsets of S.

Let $A, B \in P(S)$.

Since $A \subseteq S, B \subseteq S \Rightarrow A \cup B \subseteq S \Rightarrow A \cup B \in P(S)$.

$\therefore \cup$ is a binary operation in $P(S)$. Let $A, B, C \in P(S)$.

$\therefore (A \cup B) \cup C, A \cup (B \cup C) \in P(S)$. Since $(A \cup B) \cup C = A \cup (B \cup C)$

$\therefore \cup$ is associative in $P(S)$.

Hence $(P(S), \cup)$ is a semi group.

Example: Q is the set of rational numbers, $\circ$ is a binary operation defined on Q such that $a \circ b = a - b + ab$ for $a, b \in Q$. Then $(Q, \circ)$ is not a semi group.

Solution: For $a, b, c \in Q$,

$$(a \circ b) \circ c = (a \circ b) - c + (a \circ b)c$$
$$= a - b + ab - c + (a - b + ab)c$$
$$= a - b + ab - c + ac - bc + abc$$
$$a \circ (b \circ c) = a - (b \circ c) + a(b \circ c)$$
$$= a - (b - c + bc) + a(b - c_b c)$$
$$= a - b + c - bc + ab - ac + abc.$$

Therefore, $(a \circ b) \circ c \neq a \circ (b \circ c)$.

Example: Let $(A, *)$ be a semi group. Show that for a, b, c in A if $a * c = c * a$ and $b * c = c * b$, then $(a * b) * c = c * (a * b)$.

Solution: Given $(A, *)$ be a semi group, $a * c = c * a$ and $b * c = c * b$.
Consider

$$(a * b) * c = a * (b * c) \; [\because A \text{ is seme group}]$$
$$= a * (c * b) \; [\because b * c = c * b]$$
$$= (a * c) * b \; [\because A \text{ is seme group}]$$
$$= (c * a) * b \; [\because a * c = c * a]$$
$$= c * (a * b) \; [\because A \text{ is seme group}].$$

Homomorphism of Semi-Groups

Definition: Let $(S, *)$ and $(T, \circ)$ be any two semi-groups. A mapping $f : S \to T$ such that for any two elements $a, b \in S$, $f(a * b) = f(a) \circ f(b)$ is called a semi-group homomorphism.

Definition: A homomorphism of a semi-group into itself is called a semi-group en-domorphism.

Example: Let $(S_1, *_1)$, $(S_2, *_2)$ and $(S_3, *_3)$ be semigroups and $f : S_1 \to S_2$ and $g : S_2 \to S_3$ be homomorphisms. Prove that the mapping of $g \circ f : S_1 \to S_3$ is a semigroup homomorphism.

Solution: Given that $(S_1, *_1)$, $(S_2, *_2)$ and $(S_3, *_3)$ are three semigroups and $f : S_1 \to S_2$ and $g : S_2 \to S_3$ be homomorphisms.

Let a, b be two elements of S_1.

$(g \circ f)(a *_1 b) = g[f(a *_1 b)]$

$= g[f(a) *_2 f(b)]$ ($\because f$ is a homomorphism)

$= g(f(a)) *_3 g(f(b))$ ($\because g$ is a homomorphism)

$= (g \circ f)(a) *_3 (g \circ f)(b)$

$\therefore g \circ f$ is a homomorphism.

Identity Element: Let S be a non-empty set and $\circ$ be a binary operation on S. If there exists an element $e \in S$ such that $a \circ e = e \circ a = a$, for $a \in S$, then e is called an *identity element* of S.

Example:

(i) In the algebraic system $(Z, +)$, the number 0 is an identity element.

(ii) In the algebraic system $(R, \cdot)$, the number 1 is an identity element.

Note: The identity element of an algebraic system is unique.

Monoid

Definition: A semi group $(S, \circ)$ with an identity element with respect to the binary operation $\circ$ is known as a *monoid*. i.e., $(S, \circ)$ is a monoid if S is a non-empty set and $\circ$ is a binary operation in S such that $\circ$ is associative and there exists an identity element w.r.t $\circ$.

Example:

1. $(Z, +)$ is a monoid and the identity is 0.
2. $(Z, \cdot)$ is a monid and the identity is 1.

Monoid Homomorphism

Definition: Let $(M, *)$ and $(T, \circ)$ be any two monoids, e_m and e_t denote the identity elements of $(M, *)$ and $(T, \circ)$ respectively. A mapping $f : M \to T$ such that for any two elements $a, b \in M$,

$$f(a * b) = f(a) \circ f(b) \text{ and}$$

$$f(e_m) = e_t$$

is called a monoid homomorphism.

Monoid homomorphism presents the associativity and identity. It also preserves commutative. If $a \in M$ is invertible and $a^{-1} \in M$ is the inverse of a in M, then $f(a^{-1})$ is the inverse of $f(a)$, i.e., $f(a^{-1}) = [f(a)]^{-1}$.

Sub Semi group

Let $(S, *)$ be a semi group and T be a subset of S. Then $(T, *)$ is called a sub semi group of $(S, *)$ whenever T is closed under $*$. i.e., $a * b \in T$, for all $a, b \in T$.

Sub Monoid

Let $(S, *)$ be a monoid with e is the identity element and T be a non-empty subset of S. Then $(T, *)$ is the sub monoid of $(S, *)$ if $e \in T$ and $a * b \in T$, whenever $a, b \in T$. Example:

1. Under the usual addition, the semi group formed by positive integers is a sub semi group of all integers.
2. Under the usual addition, the set of all rational numbers forms a monoid. We denote it $(Q, +)$. The monoid $(Z, +)$ is a submonid of $(Q, +)$.
3. Under the usual multiplication, the set E of all even integers forms a semi group.

This semi group is sub semi group of $(Z, \cdot)$. But it is not a submonoid of $(Z, \cdot)$, because $1 \notin E$.

Example: Show that the intersection of two submonoids of a monoid is a monoid.

Solution: Let S be a monoid with e as the identity, and S_1 and S_2 be two submonoids of S. Since S_1 and S_2 are submonoids, these are monoids. Therefore $e \in S_1$ and $e \in S_2$.

Since $S_1 \cap S_2$ is a subset of S, the associative law holds in $S_1 \cap S_2$, because it holds in S. Accordingly $S_1 \cap S_2$ forms a monoid with e as the identity.

Invertible Element: Let $(S, \circ)$ be an algebraic structure with the identity element e in S w.r.t $\circ$. An element $a \in S$ is said to be *invertible* if there exists an element $x \in S$ such that $a \circ x = x \circ a = e$.

Note: The inverse of an invertible element is unique.

From the composition table, one can conclude

1. Closure Property: If all entries in the table are elements of S, then S closed under $\circ$.
2. Commutative Law: If every row of the table coincides with the corresponding column, then $\circ$ is commutative on S.
3. Identity Element: If the row headed by an element a of S coincides with the top row, then a is called the identity element.
4. Invertible Element: If the identity element e is placed in the table at the intersection of the row headed by $'a'$ and the column headed by $'b'$, then $b^{-1} = a$ and $a^{-1} = b$.

Example: $A = \{1, \omega, \omega^2\}$.

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

From the table we conclude that

1. Closure Property: Since all entries in the table are elements of A. So, closure property is satisfied.
2. Commutative Law: Since 1^{st}, 2^{nd} and 3^{rd} rows coincides with 1^{st}, 2^{nd} and 3^{rd} columns respectively. So multiplication is commutative on A.
3. Identity Element: Since row headed by 1 is same as the initial row, so 1 is the identity element.
4. Inverses: Clearly $1^{-1} = 1$, $\omega^{-1} = \omega^2$, $(\omega^2)^{-1} = \omega$.

Groups

Definition: If G is a non-empty set and $\circ$ is a binary operation defined on G such that the following three laws are satisfied then $(G, \circ)$ is a group.

Associative Law: For $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$

Identity Law: There exists $e \in G$ such that $a \circ e = a = e \circ a$ for every $a \in G$, e is called an identity element in G.

Inverse Law: For each $a \in G$, there exists an element $b \in G$ such that $a \circ b = b \circ a = e$, b is called an inverse of a.

Example: The set Z of integers is a group w.r.t. usual addition.

(i). For $a, b \in Z \Rightarrow a + b \in Z$

(ii). For $a, b, c \in Z$, $(a + b) + c = a + (b + c)$

(iii). $0 \in Z$ such that $0 + a = a + 0 = a$ for each $a \in G$

$\therefore$ 0 is the identity element in Z.

(iv). For $a \in Z$, there exists $-a \in Z$ such that $a + (-a) = (-a) + a = 0$.

$\therefore -a$ is the inverse of a. $(Z, +)$ is a group.

Example: Give an example of a monoid which is not a group.

Solution: The set N of natural numbers w.r.t usual multiplication is not a group.

(i). For $a, b \in N \Rightarrow a \cdot b$.

(ii). For $a, b, c \in N$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(iii). $1 \in N$ such that $1 \cdot a = a \cdot 1 = a$, for all $a \in N$.

$\therefore (N, \cdot)$ is a monoid.

(iv). There is no $n \in N$ such that $a \cdot n = n \cdot a = 1$ for $a \in N$.

$\therefore$ Inverse law is not true.

$\therefore$ The algebraic structure $(N, \cdot)$ is not a group.

Example: $(R, +)$ is a group, where R denote the set of real numbers.

Abelian Group (or Commutative Group): Let $(G, *)$ be a group. If $*$ is com-mutative that is $a * b = b * a$ for all $a, b \in G$ then $(G, *)$ is called an Abelian group.

Example: $(Z, +)$ is an Abelian group.

Example: Prove that $G = \{1, \omega, \omega^2\}$ is a group with respect to multiplication where $1, \omega, \omega^2$ are cube roots of unity.

Solution: We construct the composition table as follows:

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1$
ω^2	ω^2	$\omega^3 = 1$	$\omega^4 = \omega$

The algebraic system is $(G, \cdot)$ where $\omega^3 = 1$ and multiplication $\cdot$ is the binary opera-tion on G. From the composition table; it is clear that $(G, \cdot)$ is closed with respect to the oper-ation multiplication and the operation $\cdot$ is associative.

1 is the identity element in G such that $1 \cdot a = a = a \cdot 1$, $\forall a \in G$.

Each element of G is invertible

1. $1 \cdot 1 = 1 \Rightarrow 1$ is its own inverse.
2. $\omega \cdot \omega^2 = \omega^3 = 1 \Rightarrow \omega^2$ is the inverse of ω and ω is the inverse of ω^2 in G.

$\therefore (G, \cdot)$ is a group and $a \cdot b = b \cdot a$, $\forall a, b \in G$, that is commutative law holds in G with respect to multiplication.

$\therefore (G, \cdot)$ is an abelian group.

Example: Show that the set $G = \{1, -1, i, -i\}$ where $i = \sqrt{-1}$ is an abelian group with respect to multiplication as a binary operation. Solution: Let us construct the composition table:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

From the above composition, it is clear that the algebraic structure $(G, \cdot)$ is closed and satisfies the following axioms:

Associativity: For any three elements $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Since

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

$\Rightarrow 1 \cdot (-1 \cdot i) = (1 \cdot -1) \cdot i$

Similarly with any other three elements of G the properties holds.

$\therefore$ Associative law holds in $(G, \cdot)$.

Existence of identity: 1 is the identity element in $(G, \cdot)$ such that $1 \cdot a = a = a \cdot 1, \ \forall a \in G$.

Existence of inverse: $1 \cdot 1 = 1 = 1 \cdot 1 \Rightarrow 1$ is inverse of 1.

$(-1) \cdot (-1) = 1 = (-1) \cdot (-1) \Rightarrow -1$ is the inverse of (-1)

$i \cdot (-i) = 1 = -i \cdot i \Rightarrow -i$ is the inverse of i in G.

$-i \cdot i = 1 = i \cdot (-i) \Rightarrow i$ is the inverse of $-i$ in G.

Hence inverse of every element in G exists.
Thus all the axioms of a group are satisfied.

Commutativity: $a \cdot b = b \cdot a, \ \forall a, b \in G$ hold in G.

$$1 \cdot 1 = 1 = 1 \cdot 1; \quad -1 \cdot 1 = -1 = 1 \cdot -1$$
$$i \cdot 1 = i = 1 \cdot i; \ \ i \cdot -i = -i \cdot i = 1 \text{ etc.}$$

Commutative law is satisfied.
Hence $(G, \cdot)$ is an abelian group.

Example: Prove that the set Z of all integers with binary operation $*$ defined by $a * b = a + b + 1, \ \forall a, b \in Z$ is an abelian group. Solution:

Closure: Let $a, b \in Z$. Since $a + b \in Z$ and $a + b + 1 \in Z$.

$\therefore Z$ is closed under $*$.

Associativity: Let $a, b, c \in Z$.

Consider $(a * b) * c = (a + b + 1) * c$
$= a + b + 1 + c + 1$
$= a + b + c + 2$

also

$a * (b * c) = a * (b + c + 1)$

$=a + b + c + 1 + 1$

$=a + b + c + 2$

Hence $(a * b) * c = a * (b * c)$ for $a, b, c \in Z$.

Existence of Identity: Let $a \in Z$. Let $e \in Z$ such that $e * a = a * e = a$, i.e., $a + e + 1 = a$

$\Rightarrow e = -1$

$e = -1$ is the identity element in Z.

Existence of Inverse: Let $a \in Z$. Let $b \in Z$ such that $a * b = e$.

$\Rightarrow a + b + 1 = -1$

$b = -2 - a$

$\therefore$ For every $a \in Z$, there exits $-2-a \in Z$ such that $a*(-2-a) = (-2-a)*a = -1$.

$\therefore (Z, *)$ is an abelian group.

Example: Show that the set Q_+ of all positive rational numbers forms an abelian group under the composition defined by $\circ$ such that $a \circ b$ = ab/3 for $a, b \in Q_+$. Solution: Q_+ of the set of all positive rational numbers and for $a, b \in Q_+$, we have the operation $\circ$ such that $a \circ b$ = ab/3.

Associativity: $a, b, c \in Q+ \Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$.

Since $ab \in Q+$ and $ab/3 \in Q+$.

Associativity: $a, b, c \in Q+ \Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$.

Since $(a \circ b) \circ c = (ab/3) \circ c =[ab/3 .c]/3 = a/3(bc/3) = a/3 (b \circ c) = a \circ (b \circ c)$.

Existence of Identity: Let $a \in Q_+$. Let $e \in Q_+$ such that $e \circ a = a$.

i.e., ea/3 = a

$\Rightarrow ea - 3a = 0 \Rightarrow (e - 3)a = 0$

$\Rightarrow e - 3 = 0$ $\qquad (\because a \neq 0)$

$\Rightarrow e = 3$

$\therefore e = 3$ is the identity element in Q_+.

Existence of Inverse: Let $a \in Q_+$. Let $b \in Q_+$ such that $a \circ b = e$.

$\Rightarrow$ab/3 = 3

$b = 9/a$ $\qquad (\because a \neq 0)$

$\therefore$ For every $a \in Q_+$, there exists $9/a \in Q_+$ such that $a \circ 9/a = 9/a \circ a = 3$.

Commutativity: Let $a, b \in Q_+ \Rightarrow a \circ b = b \circ a$.

Since $a \circ b$ = ab/3=ba/3 = $b \circ a$.

$(Q_+, \circ)$ is an abelian group.

Exercises: 1. Prove that the set G of rational numbers other than 1 with operation $\oplus$ such that $a \oplus b = a + b - ab$ for $a, b \in G$ is abelian group.

2. Consider the algebraic system $(G, *)$, where G is the set of all non-zero real numbers and $*$ is a binary operation defined by: $a * b = \frac{ab}{4}$, $\forall a, b \in G$. Show that $(G, *)$ is an

Addition modulo m

We shall now define a composite known as "addition modulo m" where m is fixed integer.
If a and b are any two integers, and r is the least non-negative reminder obtained by dividing the ordinary sum of a and b by m, then the addition modulo m of a and b is r symbolically

$$a +_m b = r, \quad 0 \le r < m.$$

Example: $20 +_6 5 = 1$, since $20 + 5 = 25 = 4(6) + 1$, i.e., 1 is the remainder when 20+5 is divisible by 6.

Example: $-15 +_5 3 = 3$, since $-15 + 3 = -12 = 3(-5) + 3$.

Multiplication modulo p

If a and b are any two integers, and r is the least non-negative reminder obtained by dividing the ordinary product of a and b by p, then the Multiplication modulo p of a and b is r symbolically

$$a \times_p b = r, \qquad 0 \le r < p.$$

Example: Show that the set $G = \{0, 1, 2, 3, 4\}$ is an abelian group with respect to addition modulo 5.

Solution: We form the composition table as follows:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Since all the entries in the composition table are elements of G, the set G is closed with respect to addition modulo 5.

Associativity: For any three elements $a, b, c \in G$, $(a +_5 b) +_5 c$ and $a +_5 (b +_5 c)$ leave the same remainder when divided by 5.

i.e., $(a +_5 b) +_5 c = a +_5 (b +_5 c)$

$(1 +_5 3) +_5 4 = 3 = 1 +_5 (3 +_5 4)$ etc.

Existence of Identity: Clearly $0 \in G$ is the identity element, since we have

$0 +_5 9 = 4 = 9 +_5 0, \forall a \in G.$

Existence of Inverse: Each element in G is invertible with respect to addition modulo 5.

0 is its own inverse; 4 is the inverse of 1 and 1 is the inverse of 4.

2 is the inverse of 3 and 3 is the inverse of 2 with respect to addition modulo 5 in G.

Commutativity: From the composition table it is clear that $a +_5 b = b +_5 a$, $\forall a, b \in G$.

Hence $(G, +_5)$ is an abelian group.

Example: Show that the set $G = \{1, 2, 3, 4\}$ is an abelian with respect to multipli-cation modulo 5.
Solution: The composition table for multiplication modulo 5 is

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

From the above table, it is clear that G is closed with respect to the operation $\times_5$ and the binary composition $\times_5$ is associative; 1 is the identity element.
Each element in G has a inverse.
1 is its own inverse
2 is the inverse of 3
3 is the inverse of 2
4 is the inverse of 4, with respect to the binary operation $\times_5$.
Commutative law holds good in $(G, \times_5)$.
Therefore $(G, \times_5)$ is an abelian group.
Example: Consider the group, $G = \{1, 5, 7, 11, 13, 17\}$ under multiplication modulo 18.
Construct the multiplication table of G and find the values of: 5^{-1}, 7^{-1} and 17^{-1}.
Example: If G is the set of even integers, i.e., $G = \{\cdots, -4, -2, 0, 2, 4, \cdots\}$ then prove that G is an abelian group with usual addition as the operation. Solution: Let $a, b, c \in G$.

$\therefore$ We can take $a = 2x$, $b = 2y$, $c = 2z$, where $x, y, z \in Z$.

Closure: $a, b \in G \Rightarrow a + b \in G$.

Since $a + b = 2x + 2y = 2(x + y) \in G$.

Associativity: $a, b, c \in G \Rightarrow a + (b + c) = (a + b) + c$
Since

$$\begin{aligned} a + (b + c) &= 2x + (2y + 2z) \\ &= 2[x + (y + z)] \\ &= 2[(x + y) + z] \\ &= (2x + 2y) + 2z \\ &= (a + b) + c \end{aligned}$$

Existence of Identity: $a \in G$, there exists $0 \in G$ such that $a + 0 = 0 + a = a$. Since $a + 0 = 2x + 0 = 2x = a$ and $0 + a = 0 + 2x = 2x = a$

$\therefore$ 0 is the identity in G.

Existence of Inverse: $a \in G$, there exists $-a \in G$ such that $a+(-a) = (-a)+a = 0$.
Since $a + (-a) = 2x + (-2x) = 0$ and $(-a) + a = (-2x) + 2x = 0$.

$\therefore (G, +)$ is a group.

Commutativity: $a, b \in G \Rightarrow a + b = b + a$.
Since $a + b = 2x + 2y = 2(x + y) = 2(y + x) = 2y + 2x = b + a$.

$\therefore (G, +)$ is an abelian group.

Example: Show that set $G = \{x| \ x = 2^a3^b$ for $a, b \in Z\}$ is a group under multipli-cation.

Solution: Let $x, y, z \in G$. We can take $x = 2^p3^q$, $y = 2^r3^s$, $z = 2^l3^m$, where $p, q, r, s, l, m \in Z$.

We know that (i). $p + r, q + s \in Z$

(ii). $(p + r) + l = p + (r + l)$, $(q + s) + m = q + (s + m)$.

Closure: $x, y \in G \Rightarrow x \cdot y \in G$.

Since $x \cdot y = (2^p3^q)(2^r3^s) = 2^{p+r}3^{q+s} \in G$. Associativity: $x, y, z \in G \Rightarrow (x \cdot y) \cdot z = x \cdot (y \cdot z)$

Since $(x \cdot y) \cdot z = (2^p3^q2^r3^s)(2^l3^m)$

$= 2^{(p+r)+l}3^{(q+s)+m}$

$= 2^{p+(r+l)}3^{q+(s+m)}$

$= (2^p3^q)(2^r3^s2^l3^m)$

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

Existence of Identity: Let $x \in G$. We know that $e = 2^03^0 \in G$, since $0 \in Z$.

$\therefore x \cdot e = 2^p3^q2^03^0 = 2^{p+0}3^{q+0} = 2^p3^q = x$ and $e \cdot x = 2^03^02^p3^q = 2^p3^q = x$. $\therefore e \in G$ such that $x \cdot e = e \cdot x = x$

$\therefore e = 2^03^0$ is the identity element in G.

Existence of Inverse: Let $x \in G$.

Now $y = 2^{-p}3^{-q} \in G$ exists, since $-p, -q \in Z$ such that

$x \cdot y = 2^p3^q2^{-p}3^{-q} = 2^03^0 = e$ and $y \cdot x = 2^{-p}3^{-q}2^p3^q = 2^03^0 = e$.

$\therefore$ For every $x = 2^p3^q \in G$ there exists $y = 2^{-p}3^{-q} \in G$ such that $x \cdot y = y \cdot x = e$. $\therefore (G, \cdot)$ is a group.

Example: Show that the sets of all ordered pairs (a, b) of real numbers for which $a \neq 0$ w.r.t the operation $*$ defined by $(a, b) * (c, d) = (ac, bc + d)$ is a group. Is the commutative?

Solution: Let $G = \{(a, b)| \ a, b \in R$ and $a \neq 0\}$. Define a binary operation $*$ on G by $(a, b) * (c, d) = (ac, bc + d)$, for all $(a, b), (c, d) \in G$. Now we show that $(G, *)$ is a group.

Closure: $(a, b), (c, d) \in G \Rightarrow (a, b) * (c, d) = (ac, bc + d) \in G$.

Since $a \neq 0$, $c \neq 0 \Rightarrow ac \neq 0$.

Associativity: $(a, b), (c, d), (e, f) \in G \Rightarrow \{(a, b) * (c, d)\} * (e, f) = (a, b) * \{(c, d) * (e, f)\}$.

Since $\{(a, b) * (c, d)\} * (e, f) = (ac, bc + d) * (e, f)$

$= (ace, (bc + d)e + f)$

$= (ace, bce + de + f)$

Also $(a, b) * \{(c, d) * (e, f)\} = (a, b) * (ce, de + f)$

$= (a(ce), b(ce) + de + f)$

$= (ace, bce + de + f)$

Existence of Identity: Let $(a, b) \in G$. Let $(x, y) \in G$ such that $(x, y) * (a, b) = (a,b) * (x, y) = (a, b)$

$\Rightarrow (xa, ya + b) = (a, b)$

$$\Rightarrow xa = a,\ \ ya + b = b$$

$$\Rightarrow x = 1, (\because a \neq 0) \text{ and } ya = 0 \Rightarrow x = 1 \text{ and } y = 0\ (\because a \neq 0)$$

$\Rightarrow (1, 0) \in G$ such that $(a, b) * (1, 0) = (a, b)$.

$\therefore$ (1, 0) is the identity in G.

Existence of Inverse: Let $(a, b) \in G$. Let $(x, y) \in G$ such that $(x, y) * (a, b) = (1, 0)$

$$\Rightarrow (xa, ya + b) = (1, 0)$$

$\Rightarrow xa = 1, ya + b = 0 \Rightarrow x = \frac{1}{a}, y = \frac{-b}{a}$

$\therefore$ The inverse of (a, b) exits and it is (1/a,-b/a).

Commutativity: Let $(a, b), (c, d) \in G \Rightarrow (a, b) * (c, d) \neq (c, d) * (a, b)$

Since $(a, b) * (c, d) = (ac, bc + d)$ and $(c, d) * (a, b) = (ca, da + b)$.

$\therefore G$ is a group but not commutative group w.r.t $*$.

Example: If $(G, *)$ is a group then $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$.

Solution: Let $a, b \in G$ and e be the identity element in G.

Let $a \in G \Rightarrow a^{-1} \in G$ such that $a*a^{-1}=a^{-1}*a=e$ and $b\in G \Rightarrow b^{-1}\in G$ such that $b*b^{-1}=b^{-1} * b = e$.

Now $a, b \in G \Rightarrow a * b \in G$ and $(a * b)^{-1} \in G$.

Consider

$(a * b) * (b^{-1} * a^{-1}) = a * [b * (b^{-1} * a^{-1})]$ (by associativity law)

$= a * [(b * b^{-1}) * a^{-1}]$

$= a * (e * a^{-1})$ $(b * b^{-1} = e)$

$= a * a^{-1}$ (e is the identity)

$= e$

and

$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * [a^{-1} * (a * b)]$

$= b^{-1} * [(a^{-1} * a) * b]$

$= b^{-1} * [e * b]$

$= b^{-1} * b$

$= e$

$\Rightarrow (a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e$

$(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$.

Note:

1. $(b^{-1}a^{-1})^{-1} = ab$
2. $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$
3. If $(G, +)$ is a group, then $-(a + b) = (-b) + (-a)$
4. $-(a + b + c) = (-c) + (-b) + (-a)$.

Theorem: Cancelation laws hold good in G, i.e., for all $a, b, c \in G$ $a * b = a * c \Rightarrow b = c$ (left cancelation law) $b * a = c * a \Rightarrow b = c$ (right cancelation law).

Proof: G is a group. Let e be the identity element in G.

$$a \in G \Rightarrow a^{-1} \in G \text{ such that } a * a^{-1} = a^{-1} * a = e.$$

Consider

$a * b = a * c$

$\Rightarrow a^{-1} * (a * b) = a^{-1}(a * c)$

$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$ (by associative law)

$\Rightarrow e * b = e * c$ (a^{-1} is the inverse of a in G)

$\Rightarrow b = c$ (e is the identity element in G)

and

$b * a = c * a$

$\Rightarrow (b * a)a^{-1} = (c * a) * a^{-1}$

$\Rightarrow b * (a * a^{-1}) = c * (a * a^{-1})$ (by associative law)

$\Rightarrow b * e = c * e$ ($\because a * a^{-1} = e$)

$\Rightarrow b = c$ (e is the identity element in G)

Note:

1. If G is an additive group, $a + b = a + c \Rightarrow b = c$ and $b + a = c + a \Rightarrow b = c$.
2. In a semi group cancelation laws may not hold. Let S be the set of all 2×2 matrices over integers and let matrix multiplication be the binary operation defined on S. Then S is a semi group of the above operation.

If $A=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$; $B=\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$; $C=\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, then $A, B, C \in S$ and $AB = AC$, we observe that left cancellation law is not true in the semi group.

3. $(N, +)$ is a semi group. For $a, b, c \in N$

$a + b = a + c \Rightarrow b + c$ and $b + a = c + a \Rightarrow b = c$.

But $(N, +)$ is not a group.

In a semigroup even if cancellation laws holds, then semigroup is not a group.

Example: If every element of a group G is its own inverse, show that G is an abelian group.

Solution: Let $a, b \in G$. By hypothesis $a^{-1} = a$, $b^{-1} = b$.

Then $ab \in G$ and hence $(ab)^{-1} = ab$.

Now

$$(ab)^{-1} = ab$$

$$\Rightarrow b^{-1}a^{-1} = ab$$

$$\Rightarrow ba = ab$$

$\therefore G$ is an abelian group.

Note: The converse of the above not true.
For example, $(R, +)$, where R is the set of real numbers, is abelian group, but no element except 0 is its own inverse.

Example: Prove that if $a^2 = a$, then $a = e$, a being an element of a group G.

Solution: Let a be an element of a group G such that $a^2 = a$. To prove that $a = e$.

$a^2 = a \Rightarrow aa = a$

$\Rightarrow (aa)a^{-1} = aa^{-1} \Rightarrow a(aa^{-1}) = e$

$\Rightarrow ae = e$ [$\because aa^{-1} = e$] $\Rightarrow a = e$ [$\because ae = a$]

Example: In a group G having more than one element, if $x^2 = x$, for every $x \in G$.
Prove that G is abelian.

Solution: Let $a, b \in G$. Under the given hypothesis, we have $a^2 = a$, $b^2 = b$, $(ab)^2 = ab$.

$\therefore a(ab)b = (aa)(bb) = a^2b^2 = ab = (ab)^2 = (ab)(ab) = a(ba)b$

$\Rightarrow ab = ba$ (Using cancelation laws)

$\therefore G$ is abelian.

Example: Show that in a group G, for $a, b \in G$, $(ab)^2 = a^2b^2 \Leftrightarrow G$ is abelian. (May. 2012)

Solution: Let $a, b \in G$, and $(ab)^2 = a^2b^2$. To prove that G is abelian.
Then
$(ab)^2 = a^2b^2$

$\Rightarrow (ab)(ab) = (aa)(bb)$

$\Rightarrow a(ba)b = a(ab)b$ (by Associative law) $\Rightarrow ba = ab$, (by cancellation laws)

$\Rightarrow G$ is abelian.

Conversely, let G be abelian. To prove that $(ab)^2 = a^2b^2$.
Then $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2$.

***Example: If a, b are any two elements of a group $(G, \cdot)$, which commute. Show that

1. a^{-1} and b commute
2. b^{-1} and a commute
3. a^{-1} and b^{-1} commute.

Solution: $(G, \cdot)$ is a group and such that $ab = ba$.

1. $ab = ba \Rightarrow a^{-1}(ab) = a^{-1}(ba)$

$\Rightarrow (a^{-1}a)b = a^{-1}(ba)$

$\Rightarrow eb = (a^{-1}b)a$

$\Rightarrow b = (a^{-1}b)a$

$\Rightarrow ba^{-1} = [(a^{-1}b)a]a^{-1}$

$=(a^{-1}b)(aa^{-1})$

$=(a^{-1}b)e$

$=a^{-1}b$

$\Rightarrow a^{-1}$ and b commute.

1 $ab = ba \Rightarrow (ab)b^{-1} = (ba)b^{-1}$

$\Rightarrow a(bb^{-1}) =$

$(ba)b^{-1}$ $\Rightarrow$

$ae = b(ab^{-1})$

$\Rightarrow a = b(ab^{-1})$

$\Rightarrow b^{-1}a = b^{-1}[b(ab^{-1})]$

$=(b^{-1}b)(ab^{-1})]$

$=e(ab^{-1})$

$=ab^{-1}$

$\Rightarrow b^{-1}$ and a commute.

2 $ab = ba \Rightarrow (ab)^{-1} = (ba)^{-1}\ b^{-1}\ a^{-1} = a^{-1}\ \ b^{-1}$

$\Rightarrow a^{-1}$ and b^{-1} are commute.

Order of an Element

Definition: Let $(G, *)$ be a group and $a \in G$, then the least positive integer n if it exists such that $a^n = e$ is called the order of $a \in G$.

The order of an element $a \in G$ is be denoted by $O(a)$.

Example: $G = \{1, -1, i, -i\}$ is a group with respect to multiplication. 1 is the identity in G.

$1^1 = 1^2 = 1^3 = \cdots = 1 \Rightarrow O(1) = 1$.

$(-1)^2 = (-1)^4 = (-1)^6 = \cdots = 1 \Rightarrow O(-1) = 2$.

$i^4 = i^8 = i^{12} = \cdots = 1 \Rightarrow O(i) = 4$.

$(-i)^4 = (-i)^8 = \cdots = 1 \Rightarrow O(-i) = 4$.

Example: In a group G, a is an element of order 30. Find order of a^5.

Solution: Given $O(a) = 30$

$\Rightarrow a^{30} = e$, e is the identity element of G. Let $O(a^5) = n$

$\Rightarrow (a^5)^n = e$

$\Rightarrow a^{5n} = e$, where n is the least positive integer. Hence 30 is divisor of $5n$.

$\therefore n = 6$.

Hence $O(a^5) = 6$

Sub Groups

Definition: Let $(G, *)$ be a group and H be a non-empty subset of G. If $(H, *)$ is itself is a group, then $(H, *)$ is called sub-group of $(G, *)$.

Examples:

1. $(Z, +)$ is a subgroup of $(Q, +)$.

2. The additive group of even integers is a subgroup of the additive group of all integers.
3. $(N, +)$ is not a subgroup of the group $(Z, +)$, since identity does not exist in N under $+$.

Example: Let $G = \{1, -1, i, -i\}$ and $H = \{1, -1\}$.
Here G and H are groups with respect to the binary operation multiplication and H is a subset of G. Therefore $(H, \cdot)$ is a subgroup of $(G, \cdot)$.

Example: Let $H = \{0, 2, 4\} \subseteq Z_6$. Check that $(H, +_6)$ is a subgroup of $(Z_6, +_6)$.

Solution: $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\therefore (Z_6, +_6)$ is a group.

H= $\{0, 2, 4\}$.

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

The following conditions are to be satisfied in order to prove that it is a subgroup.

(i). Closure: Let $a, b \in H \Rightarrow a +_6 b \in H$.

$0, 2 \in H \Rightarrow 0 +_6 2 = 2 \in H$.

(ii). Identity Element: The row headed by 0 is exactly same as the initial row.

$\therefore$ 0 is the identity element.

(iii). Inverse: $0^{-1} = 0, 2^{-1} = 4, 4^{-1} = 2$.

Inverse exist for each element of $(H, +_6)$.

$\therefore (H, +_6)$ is a subgroup of $(Z_6, +_6)$.

Theorem: If $(G, *)$ is a group and $H \subseteq G$, then $(H, *)$ is a subgroup of $(G, *)$ if and only if

(i) $a, b \in H \Rightarrow a * b \in H$;

(ii) $a \in H \Rightarrow a^{-1} \in H$.

Proof: The condition is necessary

Let $(H, *)$ be a subgroup of $(G, *)$.

To prove that conditions (i) and (ii) are satisfied.

Since $(H, *)$ is a group, by closure property we have $a, b \in H \Rightarrow ab \in H$.

Also, by inverse property $a \in H \Rightarrow a^{-1} \in H$.

The condition is sufficient:

Let (i) and (ii) be true. To prove that $(H, *)$ is a subgroup of $(G, *)$.

We are required to prove is: $*$ is associative in H and identity $e \in H$.

That $*$ is associative in H follows from the fact that $*$ is associative in G. Since H is nonempty,

let $\quad a \in H \Rightarrow a^{-1} \in H$ (by (ii))

$\quad \therefore a \in H, a^{-1} \in H \Rightarrow aa^{-1} \in H$ (by (i))

$\Rightarrow e \in H$ ($\because aa^{-1} \in H \Rightarrow aa^{-1} \in G \Rightarrow aa^{-1} = e$, where e is the identity in G.)

$\Rightarrow$ e is the identity in H.

Hence H itself is a group.

$\therefore$ H is a subgroup of G.

Example: The set S of all ordered pairs (a, b) of real numbers for which $a \neq 0$ w.r.t the operation $\times$ defined by $(a, b) \times (c, d) = (ac, bc + d)$ is non-abelian. Let H= $\{(1, b) | b \in R\}$ is a subset of S. Show that H is a subgroup of $(S, \times)$.

Solution: Identity element in S is $(1, 0)$. Clearly $(1, 0) \in H$.

Inverse of (a, b) in S is $(1/a, -b/a)$ ($\because a \neq 0$)

Inverse of $(1, c)$ in S is $(1, -c/1)$, i.e., $(1, -c)$

Clearly $(1, c) \in H \Rightarrow (1, c)^{-1} = (1, -c) \in H$.

Let $(1, b) \in H$.

$(1, b) \times (1, c)^{-1} = (1, b) \times (1, -c)$

$= (1.1, b.1 - c) = (1, b - c) \in H$ ($\because b - c \in R$)

$\therefore (1, b), (1, c) \in H \Rightarrow (1, b) \times (1, c)^{-1} \in H \therefore H$ is a subgroup of $(S, \times)$.

Note: $\quad (1, b) \times (1, c) = (1.1, b.1 + c)$

$\qquad = (1, b + c)$

$\qquad = (1, c + b)$

$\qquad = (1, c) \times (1, b)$

$\therefore H$ is an abelian subgroup of the non-abelian group $(S, \times)$.

Theorem: If H_1 and H_2 are two subgroups of a group G, then $H_1 \cap H_2$ is also a subgroup of G.

Proof: Let H_1 and H_2 be two subgroups of a group G.

Let e be the identity element in G.

$\therefore e \in H_1$ and $e \in H_2$. $\therefore e \in H_1 \cap H_2$.

$\Rightarrow H_1 \cap H_2 \neq \phi$.

Let $a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$.

$\therefore a \in H_1, a \in H_2$ and $b \in H_1, b \in H_2$.

Since H_1 is a subgroup, $a \in H_1$ and $b \in H_1 \Rightarrow ab^{-1} \in H_1$.

Similarly $ab^{-1} \in H_2$.

$\therefore ab^{-1} \in H_1 \cap H_2$.

Thus we have, $a \in H_1 \cap H_2, b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$.

$\therefore H_1 \cap H_2$ is a subgroup of G.

Example: Let G be the group and $Z=\{x \in G \mid xy=yx$ for all $y \in G\}$. Prove that Z is a subgroup of G.

Solution: Since $e \in G$ and $ey = ye$, for all $y \in G$. It follows that $e \in Z$.
Therefore Z is non-empty.

Take any $a, b \in Z$ and any $y \in G$. Then

$$
\begin{aligned}
(ab)y &= a(by) \\
&= a(yb), \text{ since } b \in Z, by = yb \\
&= (ay)b \\
&= (ya)b \\
&= y(ab)
\end{aligned}
$$

This show that $ab \in Z$.

Let $a \in Z \Rightarrow ay = ya$ for all $y \in G$.

$\Rightarrow a^{-1}(ay)a^{-1} = a^{-1}(ya)a^{-1}$

$\Rightarrow (a^{-1}a)(ya^{-1}) = (a^{-1}y)(aa^{-1})$

$\Rightarrow e(ya^{-1}) = (a^{-1}y)e \Rightarrow a^{-1}y = ay^{-1}$

This shows that $a^{-1} \in Z$.

Thus, when $a, b \in Z$, we have $ab \in Z$ and $a^{-1} \in Z$.
Therefore Z is a subgroup of G.
This subgroup is called the *center* of G.

Homomorphism

Homomorphism into: Let $(G, *)$ and $(G', \cdot)$ be two groups and f be a mapping from G into G'. If for $a, b \in G$, $f(a*b) = f(a)\cdot f(b)$, then f is called *homomorphism G into* G'.

Homomorphism onto: Let $(G, *)$ and $(G', \cdot)$ be two groups and f be a mapping from G onto G'. If for $a, b \in G$, $f(a*b) = f(a)\cdot f(b)$, then f is called *homomorphism G onto* G'.
Also then G' is said to be a homomorphic image of G. We write this as $f(G) \cong G'$.

Isomorphism: Let $(G, *)$ and $(G', \cdot)$ be two groups and f be a one-one mapping of G onto G'.

If for $a, b \in G$, $f(a * b) = f(a) \cdot f(b)$, then f is said to be an isomorphism from G onto G'.

Endomorphism: A homomorphism of a group G into itself is called an *endomor-phism*.
Monomorphism: A homomorphism into is one-one, then it is called an *monomor-phism*.
Epimorphism: If the homomorphism is onto, then it is called *epimorphism*.
Automorphism: An isomorphism of a group G into itself is called an *automorphism*.

Example: Let G be the additive group of integers and G' be the multiplicative group. Then mapping $f : G \to G'$ given by $f(x) = 2^x$ is a group homomorphism of G into G'.

Solution: Since $x, y \in G \Rightarrow x + y \in G$ and $2^x, 2^y \in G' \Rightarrow 2^x \cdot 2^y \in G'$.

$\therefore f(x + y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y)$.

$\Rightarrow f$ is a homomorphism of G into G'.

Example: Let G be a group of positive real numbers under multiplication and G' be a group of all real numbers under addition. The mapping $f : G \to G'$ given by $f(x) = \log_{10} x$. Show that f is an isomorphism.

Solution: Given $f(x) = \log_{10} x$.

Let $a, b \in G \Rightarrow ab \in G$. Also, $f(a), f(b) \in G'$.

$\therefore f(ab) = \log_{10} ab = \log_{10} a + \log_{10} b = f(a) + f(b)$.

$\Rightarrow f$ is a homomorphism from G into G'.

Let $x_1, x_2 \in G$ and $f(x_1) = f(x_2)$

$\Rightarrow \log_{10} x_1 = \log_{10} x_2$

$\Rightarrow 10^{\log_{10} x_1} = 10^{\log_{10} x_2}$

$\Rightarrow x_1 = x_2$

$\Rightarrow f$ is one-one.

$\Rightarrow f(10^y) = \log_{10}(10^y) = y$.

$\therefore$ For ever $y \in G'$, there exists $10^y \in G$ such that $f(10^y) = y$

$\Rightarrow f$ is onto.

$\therefore f$ an isomorphism from G to G'.

Example: If R is the group of real numbers under the addition and R^+ is the group of positive real numbers under the multiplication. Let $f : R \to R^+$ be defined by $f(x) = e^x$, then show that f is an isomorphism.

Solution: Let $f : R \to R^+$ be defined by $f(x) = e^x$.

f is one-one: Let $a, b \in G$ and $f(a) = f(b)$

$\Rightarrow e^a = e^b$

$\Rightarrow \log e^a = \log e^b$

$\Rightarrow a \log e = b \log e$

$\Rightarrow a = b$

Thus f is one-one.

f is onto: If $c \in R^+$ then $\log c \in R$ and $f(\log c) = e^{\log c} = c$

Thus each element of R^+ has a pre-image in R under f and hence f is onto.

f is Homomorphism: $f(a + b) = e^{a+b} = e^a.e^b = f(a).f(b)$ Hence f is an isomorphism.

Example: Let G be a multiplicative group and $f : G \to G$ such that for $a \in G$, $f(a) = a^{-1}$. Prove that f is one-one and onto. Also, prove that f is homomorphism if and only if G is commutative.

Solution: $f : G \to G$ is a mapping such that $f(a) = a^{-1}$, for $a \in G$.

(i). To prove that f is one-one.

Let $a, b \in G$. $\therefore a^{-1}, b^{-1} \in G$ and $f(a), f(b) \in G$.

Now $f(a) = f(b)$

$\Rightarrow a^{-1} = b^{-1}$

$\Rightarrow (a^{-1})^{-1} = (b^{-1})^{-1}$

$\Rightarrow a = b$

$\therefore f$ is one-one.

(ii). To prove that f is onto.

Let $a \in G$. $\therefore a^{-1} \in G$ such that $f(a^{-1}) = (a^{-1})^{-1} = a$.

$\therefore f$ is onto.

(iii). Suppose f is a homomorphism.

For $a, \in G$, $ab \in G$. Now $f(ab) = f(a)f(b)$

$\Rightarrow (ab)^{-1} = a^{-1}b^{-1} \Rightarrow b^{-1}a^{-1} = a^{-1}b^{-1}$

$\Rightarrow (b^{-1}a^{-1})^{-1} = (a^{-1}b^{-1})^{-1}$

$\Rightarrow (a^{-1})^{-1}(b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1}$

$\Rightarrow ab = ba$

$\therefore G$ is abelian.

(iv). Suppose G is abelian $\Rightarrow ab = ba, \ \forall a, b \in G$.

For $a, b \in G$, $f(ab) = (ab)^{-1}$

$= b^{-1}a^{-1}$

$= a^{-1}b^{-1}$

$= f(a)f(b)$

$\therefore f$ is a homomorphism.

Number Theory

Properties of Integers

Let us denote the set of natural numbers (also called positive integers)by N and the set of integers by Z.
i.e., $N = \{1, 2, 3...\}$ and $Z = \{...., -2, -1, 0, 1, 2...\}$.
The following simple rules associated with addition and multiplication of these inte-gers are given below:
(a). Associative law for multiplication and addition

$(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$, for all $a, b, c \in Z$.

(b). Commutative law for multiplication and addition $a + b = b + a$ and $ab = ba$, for all $a, b \in Z$.

(c). Distritbutive law $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$, for all $a, b, c \in Z$.

(d). Additive identity 0 and multiplicative identity 1

$a + 0 = 0 + a = a$ and $a.1 = 1.a = a$, for all $a \in Z$.

(e). Additive inverse of $-a$ for any integer a

$a + (-a) = (-a) + a = 0$.

Definition: Let a and b be any two integers. Then a is said to be greater than b if $a - b$ is positive integer and it is denoted by $a > b$. $a > b$ can also be denoted by $b < a$.

Basic Properties of Integers

Divisor: A non-zero integer a is said to be *divisor* or *factor* of an integer b if there exists an integer q such that $b = aq$.
If a is divisor of b, then we will write a/b (read as a is a divisor of b). If a is divisor of b, then we say that b is divisible by a or a is a factor of b or b is multiple of a. Examples:
(a). $2/8$, since $8 = 2 \times 4$.
(b). $-4/16$, since $16 = (-4) \times (-4)$.
(c). $a/0$ for all $a \in Z$ and $a \neq 0$, because $0 = a.0$.

Theorem: Let $a, b, c \in Z$, the set of integers. Then,
(i). If a/b and $b \neq 0$, then $|a| \leq |b|$.
(ii). If a/b and b/c, then a/c.
(iii). If a/b and a/c, then $a/b + c$ and $a/b - c$.
(iv). If a/b, then for any integer m, a/bm.
(v). If a/b and a/c, then for any integers m and n, $a/bm + cn$.
(vi). If a/b and b/a then $a = \pm b$.
(vii). If a/b and $a/b + c$, then a/c.
(viii). If a/b and $m \neq 0$, then ma/mb.
Proof:

(i). We have $a/b \Rightarrow b = aq$, where $q \in Z$.

Since $b \neq 0$, therefore $q \neq 0$ and consequently $|q| \geq 1$.

Also, $|q| \geq 1 \Rightarrow |a||q| \geq |a|$

$\Rightarrow |b| \geq |a|$.

(ii). We have $a/b \Rightarrow b = aq_1$, where $q_1 \in Z$.

$b/c \Rightarrow c = bq_2$, where $q_2 \in Z$.

$\therefore c = bq_2 = (aq_1)q_2 = a(q_1q_2) = aq$, where $q = q_1q_2 \in Z. \Rightarrow a/c$.

(iii). We have $a/b \Rightarrow b = aq_1$, *where* $q_1 \in Z$.

$a/c \Rightarrow c = aq_2$, where $q_2 \in Z$.

Now $b + c = aq_1 + aq_2 = a(q_1 + q_2) = aq$, where $q = q_1 + q_2 \in Z$.

$\Rightarrow a/b + c$.

Also, $b - c = aq_1 - aq_2 = a(q_1 - q_2) = aq$, where $q = q_1 - q_2 \in Z$.

$\Rightarrow a/b - c$.

(iv). We have $a/b \Rightarrow b = aq$, where $q \in Z$.

For any integer m, $bm = (aq)m = a(qm) = aq$, where $a = qm \in Z$.

$\Rightarrow a/bm$.

(v). We have $a/b \Rightarrow b = aq_1$, where $q_1 \in Z$.

$a/c \Rightarrow c = aq_2$, where $q_2 \in Z$.

Now $bm + cn = (aq_1)m + (aq_2)n = a(q_1m + q_2n) = aq$, where $q = q_1m + q_2n \in Z$

$\Rightarrow a/mb + cn$.

(vi). We have $a/b \Rightarrow b = aq_1$, where $q_1 \in Z$.

$b/a \Rightarrow a = bq_2$, where $q_2 \in Z$.

$\therefore b = aq_1 = (bq_2)q_1 = b(q_2q_1)$

$\Rightarrow b(1 - q_2q_1) = 0$

$q_2q_1 = 1 \Rightarrow q_2 = q_1 = 1$ or $q_2 = q_1 = -1$

$\therefore a = b$ or $a = -b$ i.e., $a \pm b$. (vii). We have $a/b \Rightarrow b$

$= aq_1$, where $q_1 \in Z$.

$a/b + c \Rightarrow b + c = aq_2$, where $q_2 \in Z$

Now, $c = b - aq_2 = aq_1 - aq_2 = a(q_1 - q_2) = aq$, where $q = q_1 - q_2 \in Z$.

$\Rightarrow a/c$.

(viii). We have $a/b \Rightarrow b = aq_1$, where $q_1 \in Z$.

Since $m \neq 0$, $mb = m(aq_1) = ma(q_1)$

$\Rightarrow ma/mb$.

Greatest Common Divisor (GCD)

Common Divisor: A non-zero integer d is said to be a *common divisor* of integers a and b if d/a and d/b.

Example:

(1). $3/-15$ and $3/21 \Rightarrow 3$ is a common divisor of 15, 21.

(2). ± 1 is a common divisor of a, b, where $a, b \in Z$.

Greatest Common Divisor: A non-zero integer d is said to be a *greatest common divisor* (gcd) of a and b if

(i). d is a common divisor of a and b; and

(ii). every divisor of a and b is a divisor of d.

We write $d = (a, b)$=gcd of a, b.

Example: 2, 3 and 6 are common divisors of 18, 24.

Also 2/6 and 3/6. Therefore 6 = (18, 24).

Relatively Prime: Two integers a and b are said to be *relatively prime* if their greatest common divisor is 1, i.e., gcd(a, b)=1.

Example: Since (15, 8) = 1, 15 and 8 are relatively prime.

Note:

(i). If a, b are relatively prime then a, b have no common divisors.

(ii). $a, b \in Z$ are relatively prime iff there exists $x, y \in Z$ such that $ax + by = 1$.

Basic Properties of Greatest Common Divisors:

(1). If c/ab and gcd$(a, c) = 1$ then c/b.

Solution: We have $c/ab \Rightarrow ab = cq_1, q_1 \in Z.$

$(a, c) = 1 \Rightarrow$ there exist $x, y \in Z$ such that

$ax + cy = 1.$

$ax + cy = 1 \Rightarrow b(ax + cy) = b$

$\Rightarrow (ba)x + b(cy) = b \Rightarrow (cq_1)x + b(cy) = b \Rightarrow c[q_1x + by] = b$

$\Rightarrow cq = b$, where $q = q_1x + by \in Z \Rightarrow c/b.$

(2). If $(a, b) = 1$ and $(a, c) = 1$, then $(a, bc) = 1$.

Solution: $(a, b) = 1$, there exist $x_1, y_1 \in Z$ such that

$ax_1 + by_1 = 1$

$\Rightarrow by_1 = 1 - ax_1$——————-(1)

$(a, c) = 1$, there exist $x_2, y_2 \in Z$ such that

$ax_2 + by_2 = 1$

$\Rightarrow cy_2 = 1 - ax_2$——————-(2)

From (1) and (2), we have

$(by_1)(cy_2) = (1 - ax_1)(1 - ax_2)$

$\Rightarrow bcy_1y_2 = 1 - a(x_1 + x_2) + a^2x_1x_2 \Rightarrow a(x_1 + x_2 - ax_1x_2) + bc(y_1y_2) = 1$

$\Rightarrow ax_3 + bcy_3 = 1$, where $x_3 = x_1 + x_2 - ax_1x_2$ and $y_3 = y_1y_2$ are integers.

$\therefore$ There exists $x_3, y_3 \in Z$ such that $ax_3 + bcy_3 = 1$.

(3). If $(a, b) = d$, then $(ka, kb) = |k|d.$, k is any integer.

Solution: Since $d = (a, b) \Rightarrow$ there exist $x, y \in Z$ such that

$ax + by = d.$

$\Rightarrow k(ax) + k(by) = kd \Rightarrow (ka)x + (kb)y = kd$

$\therefore (ka, kb) = kd = k(a, b)$

(4). If $(a, b) = d$, then $(\frac{a}{d}, \frac{b}{d}) = 1$.

Solution: Since $(a, b) = d \Rightarrow$ there exist $x, y \in Z$ such that $ax + by = d$.

$$\Rightarrow (ax+by)/d = 1$$

$$\Rightarrow (a/d)x + (b/d)y = 1$$

Since d is a divisor of both a and b, a/d and b/d are both integers.
Hence (a/d,b/d) = 1.

Division Theorem (or Algorithm)

Given integers a and d are any two integers with $b > 0$, there exist a unique pair of integers q and r such that $a = dq + r$, $0 \le r < b$. The integer's q and r are called the quotient and the remainder respectively. Moreover, $r = 0$ if, and only if, $b|a$.

Proof:

Consider the set, S, of all numbers of the form a+nd, where n is an integer.

S = {a - nd : n is an integer}

S contains at least one nonnegative integer, because there is an integer, n, that ensures a-nd $\ge$ 0, namely

n = -|a| d makes a-nd = a+|a| $d^2 \ge$ a+|a| $\ge$ 0.

Now, by the well-ordering principle, there is a least nonnegative element of S, which we will call r, where r=a-nd for some n. Let q = (a-r)/d = (a-(a-nd))/d = n. To show that r < |d|, suppose to the contrary that r $\ge$ |d|. In that case, either r-|d|=a-md, where m=n+1 (if d is positive) or m=n-1 (if d is negative), and so r-|d| is an element of S that is nonnegative and smaller than r, a contradiction. Thus r < |d|.

To show uniqueness, suppose there exist q,r,q',r' with 0 $\le$ r,r' < |d|

such that a=qd + r and a =q'd + r'.

Subtracting these equations gives d(q'-q) = r'-r, so d|r'-r. Since 0 $\le$ r,r' < |d|, the difference r'-r must also be smaller than d. Since d is a divisor of this difference, it follows that the difference r'-r must be zero, i.e. r'=r, and so q'=q.

Example: If $a = 16$, $b = 5$, then $16 = 3 \times 5 + 1$; $0 \le 1 < 5$.

Euclidean Algorithm for finding the GCD

An efficient method for finding the greatest common divisor of two integers based on the quotient and remainder technique is called the Euclidean algorithm. The following lemma provides the key to this algorithm.

Lemma: If $a = bq + r$, where a, b, q and r are integers, then gcd(a, b)=gcd(b, r).

Statement: When a and b are any two integers ($a > b$), if r_1 is the remainder when a is divided by b, r_2 is the remainder when b is divided by r_1, r_3 is the remainder when r_1 is divided by r_2 and so on and if $r_{k+1} = 0$, then the last non-zero remainder r_k is the gcd(a, b).

Proof:

By the unique division principle, a divided by b gives quotient q and remainder r,

such that $a = bq+r$, with $0 \le r < |b|$.

Consider now, a sequence of divisions, beginning with a divided by b giving quotient q_1 and remainder b_1, then b divided by b_1 giving quotient q_2 and remainder b_2, etc.

$a=bq_1+b_1$,
$b=b_1q_2+b_2$,
$b_1=b_2q_3+b_3$,
...
$b_{n-2}=b_{n-1}q_n+b_n$,
$b_{n-1}=b_nq_{n+1}$

In this sequence of divisions, $0 \le b_1 < |b|$, $0 \le b_2 < |b_1|$, etc., so we have the sequence $|b| > |b_1| > |b_2| > ... \ge 0$. Since each b is strictly smaller than the one before it, eventually one of them will be 0. We will let b_n be the last non-zero element of this sequence.

From the last equation, we see $b_n \mid b_{n-1}$, and then from this fact and the equation before it, we see that $b_n \mid b_{n-2}$, and from the one before that, we see that $b_n \mid b_{n-3}$, etc. Following the chain backwards, it follows that $b_n \mid b$, and $b_n \mid a$. So we see that b_n is a common divisor of a and b.

To see that b_n is the *greatest* common divisor of a and b, consider, d, an arbitrary common divisor of a and b. From the first equation, $a-bq_1=b_1$, we see $d|b_1$, and from the second, equation, $b-b_1q_2=b_2$, we see $d|b_2$, etc. Following the chain to the bottom, we see that $d|b_n$. Since an arbitrary common divisor of a and b divides b_n, we see that b_n is the greatest common divisor of a and b.

Example: Find the gcd of 42823 and 6409.

Solution: By Euclid Algorithm for 42823 and 6409, we have

42823= 6.6409+ 4369, r1= 4369,
6409= 1.4369+2040, r2= 2040,
4369= 2.2040+289, r3 = 289,
2040= 7.289+ 17, r4 = 17,
289= 17.17+ 0,
r5 = 0

$\therefore r_4 = 17$ is the last non-zero remainder. $\therefore d = (42823, 6409) = 17$.

Example: Find the gcd of 826, 1890.

Solution: By Euclid Algorithm for 826 and 1890, we have

1890= 2.826+ 238, r_1= 238
826= 3.238+ 112, r_2= 112
238= 2.112+ 14, r_3 = 14
112= 8.14 + 0, r_4 = 0

$\therefore r_3 = 14$ is the last non-zero remainder. $\therefore d = (826, 1890) = 14$.

****Example: Find the gcd of 615 and 1080, and find the integers x and y such that gcd(615, 1080) = $615x + 1080y$.

Solution: By Euclid Algorithm for 615 and 1080, we have

$$1080 = 1.615 + 465,\ r_1 = 465 - - - - - (1)$$

$$615 = 1.465 + 150,\ r_2 = 150 - - - - - (2)$$

$$465 = 3.150 + 15,\ r_3 = 15 - - - - - - (3)$$

$$150 = 10.15 + 0,\ r_4 = 0 - - - - - - - (4)$$

$\therefore r_3 = 15$ is the last non-zero remainder.

$\therefore d = (615, 1080) = 15$. Now, we find x and y such that

$615x + 1080y = 15$.

To find x and y, we begin with last non-zero remainder as follows.

$d = 15 = 465 + (-3).150$; using (3)

$=465 + (-3)\{615 + (-1)465\}$; using (2)
$=(-3).615 + (4).465$
$=(-3).615 + 4\{1080 + (-1).615\}$; using (1)
$=(-7).615 + (4).1080$
$=615x + 1080y$

Thus gcd(615, 1080) = 15 provided $15 = 615x + 1080y$, where $x = -7$ and $y = 4$.

Example: Find the gcd of 427 and 616 and express it in the form $427x + 616y$.

Solution: By Euclid Algorithm for 427 and 616, we have

616= 1.427+189, r_1 = 189.........(1)
427= 2.189+49, r_2 = 49............(2)
189= 3.49+ 42, r_3 = 42..............(3)
49= 1.42+ 7, r_4 = 7..................(4)
42= 6.7 + 0, r_5 = 0....................(5)

$\therefore r_5 = 7$ is the last non-zero remainder.

$\therefore d = (427, 616) = 7$. Now, we find x and y such that

$427x + 616y = 7$.

To find x and y, we begin with last non-zero remainder as follows.

$d = 7 = 49 + (-1).42$; using (4)

$=49 + (-1)\{189 + (-3).49\}$; using (3)
$=4.49 - 189$
$=4.\{427 + (-2).189\} - 189$; using (2)
$=4.427 + (-8).189 - 189$
$=4.427 + (-9).189$
$=4.427 + (-9)\{616 + (-1)427\}$; using (1)
$=4.427 + (-9).616 + 9.427$
$=13.427 + (-9).616$

Thus gcd(427, 616) = 7 provided $7 = 427x + 616y$, where $x = 13$ and $y = -9$.
Example: For any positive integer n, prove that the integers $8n + 3$ and $5n + 2$ are relatively prime.
Solution: If $n = 1$, then gcd($8n + 3$, $5n + 2$)=gcd(11, 7) = 1.
If $n \geq 2$, then we have $8n + 3 > 5n + 2$, so we may write

$8n + 3 = 1.(5n + 2) + 3n + 1$, $\quad 0 < 3n + 1 < 5n + 2$

$5n + 2 = 1.(3n + 1) + 2n + 1$, $\quad 0 < 2n + 1 < 3n + 1$

$3n + 1 = 1.(2n + 1) + n$, $\quad 0 < n < 2n + 1$

$2n + 1 = 2.n + 1$, $\quad 0 < 1 < n$

$n = n.1 + 0$.

Since the last non-zero remainder is 1, gcd($8n + 3$, $5n + 2$) = 1 for all $n \geq 1$.
Therefore the given integers $8n + 3$ and $5n + 2$ are relatively prime.
Example: If $(a, b) = 1$, then $(a + b, a - b)$ is either 1 or 2.

Solution: Let $(a + b, a - b) = d \Rightarrow d|a + b, d|a - b$.

Then $a + b = k_1d$........(1)

and $a - b = k_2d$..........(2)

Solving (1) and (2), we have

$2a = (k_1 + k_2)d$ and $2b = (k_1 - k_2)d$

$\therefore d$ divides $2a$ and $2b$

$\therefore d \leq$gcd($2a$, $2b$) = 2 gcd(a, b) = 2, since gcd(a, b) = 1 $\therefore d$ = 1 or 2.

Then $2a + b = k_1d$........ (1)

and $a + 2b = k_2d$.......... (2)

$3a = (2k_1 - k_2)d$ and $3b = (2k_2 - k_1)d$

$\therefore d$ divides $3a$ and $3b$

$\therefore d \leq$gcd($3a$, $3b$) = 3 gcd(a, b) = 3, since gcd(a, b) = 1 $\therefore d$ = 1 or 2 or 3.

But d cannot be 2, since $2a + b$ and $a + 2b$ are not both even [when a is even and b is odd, $2a + b$ is odd and $a + 2b$ is even; when a is odd and b is even, $2a + b$ is even and $a + 2b$ is odd; when both a and b are odd $2a + b$ and $a + 2b$ are odd.] Hence $d = (2a + b, a + 2b)$ is 1 or 3.

Least Common Multiple (LCM)

Let a and b be two non-zero integers. A positive integer m is said to be a *least common multiple* (lcm) of a and b if

(i) m is a common multiple of a and b i.e., a/m and b/m,

and

(ii) c is a common multiple of a and b, c is also a multiple of m

i.e., if a/c and b/c, then m/c.

In other words, if a and b are positive integers, then the smallest positive integer that is divisible by both a and b is called the least common multiple of a and b and is denoted by lcm(a, b).
Note: If either or both of a and b are negative then lcm(a, b) is always positive.
Example: lcm(5, -10)=10, lcm(16, 20)=80.

Prime Numbers

Definition: An integer *n* is called prime if $n > 1$ and if the only positive divisors of *n* are 1 and *n*. If $n > 1$ and if *n* is not prime, then *n* is called composite.

Examples: The prime numbers less than 100 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97.

Theorem: Every integer $n > 1$ is either a prime number or a product of prime numbers.

Proof: We use induction on *n*. The theorem is clearly true for $n = 2$. Assume it is true for every integer $< n$. Then if *n* is not prime it has a positive divisor $d \neq 1$, $d \neq n$. Hence $n = cd$, where $c \neq n$. But both *c* and *d* are $< n$ and > 1 so each of *c*, *d* is a product of prime numbers, hence so is *n*.

Fundamental Theorem of Arithmetic

Theorem: *Every integer n* > 1 *can be expressed as a product of prime factors in only one way, a part from the order of the factor.*

Proof:

There are two things to be proved. Both parts of the proof will use he Well-ordering Principle for the set of natural numbers.
(1) We first prove that every a > 1 can be written as a product of prime factors. (This includes the possibility of there being only one factor in case a is prime.)
Suppose bwoc that there exists a integer a > 1 such that a cannot be written as a product of primes.
By the Well-ordering Principle, there is a smallest such a.
Then by assumption a is not prime so a = bc where 1 < b, c < a.
So b and c can be written as products of prime factors (since a is the smallest positive integer than cannot be.)
But since a = bc, this makes a a product of prime factors, a contradiction.
(2) Now suppose bwoc that there exists an integer a > 1 that has two different prime factorizations, say a = p1 ⋯ ps = q1 ⋯ qt , where the pi and qj are all primes. (We allow repetitions among the pi and qj . That way, we don't have to use exponents.)
Then p1| a = q1 ⋯ qt . Since p1 is prime, by the Lemma above, p1| qj for some j .
Since qj is prime and p1 > 1, this means that p1 = qj .
For convenience, we may renumber the qj so that p1 = q1 .
We can now cancel p1 from both sides of the equation above to get p2 ⋯ ps = q2 ⋯ qt . But p2 ⋯ ps < a and by assumption a is the smallest positive integer with a non–unique prime factorization.
It follows that s = t and that p2,...,ps are the same as q2,...,qt , except possibly in a different order.
But since p1 = q1 as well, this is a contradition to the assumption that these were two different factorizations.
Thus there cannot exist such an integer a with two different factorizations

Example: Find the prime factorisation of 81, 100 and 289. Solution: $81 = 3 \times 3 \times 3 \times 3 = 3^4$

$100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$

$289 = 17 \times 17 = 17^2$.

Theorem: Let $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ and $n = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$. Then

$\gcd(m, n) = p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \ldots \times p_k^{\min(a_k,b_k)}$

$= \prod p_i^{\min(a_i,b_i)}$, where min($a$, b) represents the minimum of the two numbers a and b.

$\mathrm{lcm}(m, n) = p_1^{\max(a_1,b_1)} \times p_2^{\max(a_2,b_2)} \times \ldots \times p_k^{\max(a_k,b_k)}$

$= \prod p_i^{\max(a_i,b_i)}$, where max($a$,$b$) represents the maximum of the two numbers a and b.

Theorem: If a and b are two positive integers, then gcd(a, b).lcm(a, b) = ab.

Proof: Let prime factorisation of a and b be

m= $p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ and $n = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$

Then $\gcd(a, b) = p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \ldots \times p_k^{\min(a_k,b_k)}$ and

$\mathrm{lcm}(m, n) = p_1^{\max(a_1,b_1)} \times p_2^{\max(a_2,b_2)} \times \ldots \times p_k^{\max(a_k,b_k)}$

We observe that if min(a_i, b_i) is a_i(or b_i) then max(a_i, b_i) is b_i(or a_i), i = 1, 2.., n.

Hence gcd(a, b).lcm(a, b)

$$= p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \ldots \times p_k^{\min(a_k,b_k)} \times p_1^{\max(a_1,b_1)} . p_2^{\max(a_2,b_2)} \ldots p_k^{\max(a_k,b_k)}$$

$$= p_1^{[\min(a_1,b_1)+\max(a_1,b_1)]} . p_2^{[\min(a_2,b_2)+\max(a_2,b_2)]} \ldots p_k^{[\min(a_k,b_k)+\max(a_k,b_k)]}$$

$$= p_1^{(a_1+b_1)} . p_2^{(a_2+b_2)} \ldots p_k^{(a_k+b_k)}$$

$$= (p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k})(p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k})$$

$$= ab.$$

Example: Use prime factorisation to find the greatest common divisor of 18 and 30.

Solution: Prime factorisation of 18 and 30 are

$18 = 2^1 \times 3^2 \times 5^0$ and $30 = 2^1 \times 3^1 \times 5^1$.

$\gcd(18, 30) = 2^{\min(1,1)} \times 3^{\min(2,1)} \times 5^{\min(0,1)}$

$= 2^1 \times 3^1 \times 5^0$

$= 2 \times 3 \times 1$

$= 6$.

Example: Use prime factorisation to find the least common multiple of 119 and 544.

Solution: Prime factorisation of 119 and 544 are

$119 = 2^0 \times 7^1 \times 17^1$ and $544 = 2^5 \times 7^0 \times 17^1$.

$\mathrm{lcm}(119, 544) = 2^{\max(0,5)} \times 7^{\max(1,0)} \times 17^{\max(1,1)}$

$= 2^5 \times 7^1 \times 17^1$

$= 32 \times 7 \times 17$

$= 3808$.

Example: Using prime factorisation, find the gcd and lcm of (i). (231, 1575) (ii). (337500, 21600). Verify also gcd(m, n). lcm(m, n) = mn.

Example: Prove that $\log_3 5$ is irrational number.

Solution: If possible, let $\log_3 5$ is rational number.

$\Rightarrow \log_3 5 = u/v$, where u and v are positive integers and prime to each other.

$\therefore 3^{u/v} = 5$

i.e., $3^u = 5^v = n$, say.
This means that the integer $n > 1$ is expressed as a product (or power) of prime numbers (or a prime number) in two ways.
This contradicts the fundamental theorem arithmetic.

$\therefore \log_3 5$ is irrational number.

Example: Prove that $\sqrt{5}$ is irrational number.
Solution: If possible, let $\sqrt{5}$ is rational number.
$\Rightarrow \sqrt{5} = u/v$, where u and v are positive integers and prime to each other.
$\Rightarrow u^2 = 5v^2$...................(1)
$\Rightarrow u^2$ is divisible by 5
$\Rightarrow u$ is divisible by 5 i.e., $u = 5m$.........(2)
$\therefore$ From (1), we have $5v^2 = 25m^2$ or $v^2 = 5m^2$
i.e., v^2 and hence v is divisible by 5
i.e., $v = 5n$..........(3)
From (2) and (3), we see that u and v have a common factor 5, which contradicts the assumption.
$\therefore \sqrt{5}$ is irrational number.

Testing of Prime Numbers

Theorem: If $n > 1$ is a composite integer, then there exists a prime number p such that p/n and $p \leq \sqrt{n}$.
Proof: Since $n > 1$ is a composite integer, n can be expressed as $n = ab$, where $1 < a \leq b < n$. Then $a \leq \sqrt{n}$.
If $a > \sqrt{n}$, then $b \geq a > \sqrt{n}$.
$\therefore$ $n = ab > \sqrt{n}.\sqrt{n} = n$, i.e. $n > n$, which is a contradiction.
Thus n has a positive divisor (= a) not exceeding $\sqrt{n}$.
$a > 1$, is either prime or by the Fundamental theorem of arithmetic, has a primefactor. In ither ase, n has a prime factor $\leq \sqrt{n}$.

Algorithm to test whether an integer $n > 1$ is prime:

Step 1: Verify whether n is 2. If n is 2, then n is prime. If not goto step 2.
Step 2: Verify whether 2 divides n. If 2 divides n, then n is not a prime. If 2 does not divides n, then goto step (3).
Step 3: Find all odd primes $p \leq \sqrt{n}$.If there is no such odd prime, then n is prime otherwise, goto step (4).
Step 4: Verify whether p divides n, where p is a prime obtained in step (3). If p divides n, then n is not a prime. If p does not divide n for any odd prime p obtained in step (3), then n is prime.

Example: Determine whether the integer 113 is prime or not.
Solution: Note that 2 does not divide 113. We now find all odd primes p such that $p^2 \leq 113$.
These primes are 3, 5 and 7, since $7^2 < 113 < 11^2$.
None of these primes divide 113.
Hence, 113 is a prime.

Example: Determine whether the integer 287 is prime or not.
Solution: Note that 2 does not divide 287. We now find all odd primes p such that $p^2 \leq 287$.
These primes are 3, 5, 7, 11 and 13, since $13^2 < 287 < 17^2$.
7 divides 287.
Hence, 287 is a composite integer.

Modular Arithmetic

Congruence Relation

If a and b are integers and m is positive integer, then a is said to be congruent to b modulo m, if m divides $a - b$ or $a - b$ is multiple of m. This is denoted as

$$a \equiv b (\text{mod } m)$$

m is called the modulus of the congruence, b is called the residue of $a(\text{mod } m)$. If a is not congruent to b modulo m, then it is denoted by $a \not\equiv b(\text{mod } m)$.
Example:
(i). $89 \equiv 25(\text{mod } 4)$, since 89-25=64 is divisible by 4. Consequently 25 is the residue of 89(mod 4) and 4 is the modulus of the congruent.

(ii). $153 \equiv -7(\text{mod } 8)$, since 153-(-7)=160 is divisible by 8. Thus -7 is the residue of 153(mod 8) and 8 is the modulus of the congruent.

(iii). $24 \not\equiv 3(\text{mod } 5)$, since 24-3=21 is not divisible by 5. Thus 24 and 3 are incon-gruent modulo 5
Note: If $a \equiv b(\text{mod } m) \Leftrightarrow a - b = mk$, for some integer k

$\Leftrightarrow a = b + mk$, for some integer k.

Properties of Congruence

Property 1: The relation "Congruence modulo m" is an equivalence relation. i.e., for all integers a, b and c, the relation is

(i) Reflexive: For any integer a, we have $a \equiv a(\text{mod } m)$

(ii) Symmetric: If $a \equiv b(\text{mod } m)$, then $b \equiv a(\text{mod } m)$

(iii) Transitive: If $a \equiv b(\text{mod } m)$ and $b \equiv c(\text{mod } m)$, then $a \equiv c(\text{mod } m)$.

Proof: (i). Let a be any integer. Then $a - a = 0$ is divisible by any fixed positive integer m. Thus $a \equiv a(\text{mod } m)$.

$\therefore$ The congruence relation is reflexive.

(ii). Given $a \equiv b(\text{mod } m)$

$\Rightarrow a - b$ is divisible by $m \Rightarrow -(a - b)$ is divisible by $m \Rightarrow b - a$ is divisible by m

i.e., $b \equiv a(\text{mod } m)$.

Hence the congruence relation is symmetric.

(iii). Given $a \equiv b(\text{mod } m)$ and $b \equiv c(\text{mod } m)$

$\Rightarrow a - b$ is divisible of m and $b - c$ is divisible by m. Hence $(a - b) + (b - c) = a - c$ is divisible by m

i.e., $a \equiv c(\text{mod } m)$

$\Rightarrow$ The congruence relation is transitive.

Hence, the congruence relation is an equivalence relation.

Property 2: If $a \equiv b(\text{mod } m)$ and c is any integer, then

(i). $a \pm c \equiv b \pm c(\text{mod } m)$

(ii). $ac \equiv bc(\text{mod } m)$.

Proof:

(i). Since $a \equiv b(\text{mod } m) \Rightarrow a - b$ is divisible by m.

Now $(a \pm c) - (b \pm c) = a - b$ is divisible by m.

$\therefore a \pm c \equiv b \pm c(\text{mod } m)$.

(ii). Since $a \equiv b(\text{mod } m) \Rightarrow a - b$ is divisible by m.

Now, $(a - b)c = ac - bc$ is also divisible by m.

$\therefore ac \equiv bc(\text{mod } m)$.

Note: The converse of property (2) (ii) is not true always.

Property 3: If $ac \equiv bc(\text{mod } m)$, then $a \equiv b(\text{mod } m)$ only if $\gcd(c,m) = 1$. In fact, if c is an integer which divides m, and if $ac \equiv bc(\text{mod } m)$, then $a \equiv b \text{ mod}[\frac{m}{\gcd(c,m)}]$

Proof: Since $ac \equiv bc(\text{mod } m) \Rightarrow ac - bc$ is divisible by m.

i.e., $ac - bc = pm$, where p is an integer.

$\Rightarrow a - b = p(\frac{m}{c})$

$\therefore$ a ≡ b[mod $(\frac{m}{c})$] , provided that $\frac{m}{c}$ is an integer.

Since c divides m, $\gcd(c, m) = c$.

Hence, $a \equiv b \text{ mod } [\frac{m}{\gcd(c,m)}]$

But, if $\gcd(c, m) = 1$, then $a \equiv b(\text{mod } m)$.

Property 4: If a, b, c, d are integers and m is a positive integer such that $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m)$, then

(i). $a \pm c \equiv b \pm d(\text{mod } m)$

(ii). $ac \equiv bd(\text{mod } m)$

(iii). $a^n \equiv b^n(\text{mod } m)$, where n is a positive integer.

Proof: (i). Since $a \equiv b \pmod{m} \Rightarrow a - b$ is divisible by m.

Also $c \equiv d \pmod{m} \Rightarrow c - d$ is divisible by m.

$\therefore (a - b) \pm (c - d)$ is divisible by m. i.e., $(a \pm c) - (b \pm d)$ is divisible by m. i.e., $a \pm c \equiv b \pm d \pmod{m}$.

(ii). Since $a \equiv b \pmod{m} \Rightarrow a - b$ is divisible by m.

$\therefore (a - b)c$ is also divisible by m.

$\therefore (c - d)b$ is also divisible by m.

$\therefore (a - b)c + (c - d)b = ac - bd$ is divisible by m. i.e., $ac - bd$ is divisible by m.

i.e., $ac \equiv bd \pmod{m}$...........................(1)

(iii). In (1), put $c = a$ and $d = b$. Then, we get

$a^2 \equiv b^2 \pmod{m}$................(2)

Also $a \equiv b \pmod{m}$................(3)

Using the property (ii) in equations (2) and (3), we have $a^3 \equiv b^3 \pmod{m}$

Proceeding the above process we get

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

Fermat's Theorem

If p is a prime and $(a, p) = 1$ then $a^{p-1} - 1$ is divisible by p i.e., $a^{p-1} \equiv 1 \pmod{p}$.

Proof

We offer several proofs using different techniques to prove the statement $a^p \equiv a \pmod{p}$. If $\gcd(a, p) = 1$, then we can cancel a factor of a from both sides and retrieve the first version of the theorem.

Proof by Induction

The most straightforward way to prove this theorem is by by applying the induction principle. We fix p as a prime number. The base case, $1^p \equiv 1 \pmod{p}$, is obviously true. Suppose the statement $a^p \equiv a \pmod{p}$ is true. Then, by the binomial theorem,

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1.$$

Note that p divides into any binomial coefficient of the form $\binom{p}{k}$ for $1 \le k \le p-1$. This follows by the definition of the binomial coefficient as $\binom{p}{k} = \frac{p!}{k!(p-k)!}$; since p is prime, then p divides the numerator, but not the denominator.

Taken $\bmod p$, all of the middle terms disappear, and we end up with $(a+1)^p \equiv a^p + 1 \pmod p$. Since we also know that $a^p \equiv a \pmod p$, then $(a+1)^p \equiv a+1 \pmod p$, as desired.

Example: Using Fermat's theorem, compute the values of

(i) 3^{302}(mod 5),

(ii) 3^{302}(mod 7) and

(iii) 3^{302}(mod 11).

Solution: By Fermat' s theorem, 5 is a prime number and 5 does not divide 3, we have

$$3^{5-1} \equiv 1 \pmod 5$$

$$3^4 \equiv 1 \pmod 5$$

$$(3^4)^{75} \equiv 1^{75} \pmod 5$$

$$3^{300} \equiv 1 \pmod 5$$

$$3^{302} \equiv 3^2 = 9 \pmod 5$$

$$3^{302} \equiv 4 \pmod 5 \text{.............(1)}$$

Similarly, 7 is a prime number and 7 does not divide 3, we have

$$3^6 \equiv 1 \pmod 7$$

$$(3^6)^{50} \equiv 1^{50} \pmod 7$$

$$3^{300} \equiv 1 \pmod 7$$

$$3^{302} \equiv 3^2 = 9 \pmod 7$$

$$3^{302} \equiv 2 \pmod 7 \text{.............(2)}$$

and 11 is a prime number and 11 does not divide 3, we have

$$3^{10} \equiv 1 \pmod{11}$$

$$(3^{10})^{30} \equiv 1^{30} \pmod{11}$$

$$3^{300} \equiv 1 \pmod{11}$$

$$3^{302} \equiv 3^2 = 9 \pmod{11} \text{.............(3)}$$

Example: Using Fermat's theorem, find 3^{201}(mod 11).

Example: Using Fermat's theorem, prove that $4^{13332} \equiv 16$ (mod 13331). Also, give an example to show that the Fermat theorem is true for a composite integer. Solution:

(i). Since 13331 is a prime number and 13331 does not divide 4.

By Fermat's theorem, we have

$4^{13331-1} \equiv 1$ (mod 13, 331)

$4^{13330} \equiv 1$ (mod 13, 331)

$4^{13331} \equiv 4$ (mod 13, 331)

$4^{13332} \equiv 16$ (mod 13, 331)

(ii). Since 11 is prime and 11 does not divide 2.

By Fermat's theorem, we have

$2^{11-1} \equiv 1 \pmod{11}$

i.e., $2^{10} \equiv 1 \pmod{11}$

$(2^{10})^{34} \equiv 1^{34} \pmod{11}$

$2^{340} \equiv 1 \pmod{11}$.............(1)

Also,

$2^5 \equiv 1 \pmod{31}$

$(2^5)^{68} \equiv 1^{68} \pmod{31}$

$2^{340} \equiv 1 \pmod{31}$.............(2)

From (1) and (2), we get

$2^{340} - 1$ is divisible by $11 \times 31 = 341$, since gcd(11, 31) = 1.

i.e., $2^{340} \equiv 1 \pmod{341}$.

Thus, even though 341 is not prime, Fermat theorem is satisfied.

Euler's totient Function:

Euler's totient function counts the positive integers up to a given integer n that are relatively prime to n. It is written using the Greek letter phi as $\phi(n)$, and may also be called Euler's phi function. It can be defined more formally as the number of integers k in the range $1 \le k \le n$ for which the greatest common divisor gcd(n, k) is equal to 1. The integers k of this form are sometimes referred to as totatives of n.

Computing Euler's totient function:

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right),$$

where the product is over the distinct prime numbers dividing

Example: Find $\phi(21)$, $\phi(35)$, $\phi(240)$

Solution:

$\phi(21) = \phi(3 \times 7)$

$= 21\,(1-\frac{1}{3})(1-\frac{1}{7})$

$= 12$

$\phi(35) = \phi(5 \times 7)$

$= 35\,(1-\frac{1}{5})(1-\frac{1}{7})$

$= 24$

$\phi(240) = \phi(15 \times 16)$

$=\phi(3\times 5\times 2^4)$

$=240\ (1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{2})$

$= 64$

Euler's Theorem: If a and $n > 0$ are integers such that $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 (\text{mod } n)$.
Proof:

Consider the elements $r_1, r_2, \ldots, r_{\phi(n)}$ of (Z/n) the congruence classes of integers that are relatively prime to n.

For $a \in (Z/n)$ the claim is that multiplication by a is a permutation of this set; that is, the set $\{ ar_1, ar_2, \ldots, ar_{\phi(n)} \}$ equals (Z/n). The claim is true because multiplication by a is a function from the finite set (Z/n) to itself that has an inverse, namely multiplication by 1/a (mod n)

Now, given the claim, consider the product of all the elements of (Z/n), on one hand, it is $r_1 r_2, \ldots r_{\phi(n)}$. On the other hand, it is $ar_1\ ar_2 \ldots ar_{\phi(n)}$. So these products are congruent mod n

$$r_1\ r_2 \ldots r_{\phi(n)} \equiv ar_1\ ar_2 \ldots ar_{\phi(n)}$$

$$r_1\ r_2 \ldots r_{\phi(n)} \equiv a^{\phi(n)}\ r_1\ r_2 \ldots r_{\phi(n)}$$

$$1 \equiv a^{\phi(n)}$$

where, cancellation of the r_i is allowed because they all have multiplicative inverses(mod n)

Example: Find the remainder 29^{202} when divided by 13.

Solution: We first note that (29,13)=1.

Hence we can apply Euler's Theorem to get that $29^{\phi(13)} \equiv 1 (\text{mod}13)$.
Since 13 is prime, it follows that $\phi(13)=12$, hence $29^{12} \equiv 1(\text{mod}13)$.
We can now apply the division algorithm between 202 and 12 as follows:

$$202=12(16)+10$$

Hence it follows that $29^{202}=(29^{12})^{26}\cdot 29^{10} \equiv (1)^{26}\cdot 29^{10} \equiv 29^{10}(\text{mod}13)$.
Also we note that 29 can be reduced to 3 (mod 13), and hence:

$$29^{10} \equiv 3^{10}=59049 \equiv 3(\text{mod}13)^2$$

Hence when 29^{202} is divided by 13, the remainder leftover is 3.

Example: Find the remainder of 99^{999999} when divided by 23.
Solution: Once again we note that (99,23)=1, hence it follows that $99^{\phi(23)} \equiv 1(\text{mod}23)$.
Once again, since 23 is prime, it goes that $\phi(23)=22$, and more appropriately 9922≡1(mod23).
We will now use the division algorithm between 999999 and 22 to get that:

$$999999=22(45454)+11$$

Hence it follows that
$99^{999999}=(99^{22})^{45454}\cdot 99^{11} \equiv 1^{45454}\cdot 99^{11} \equiv 7^{11}=1977326743 \equiv 22(\text{mod}23)$.
Hence the remainder of 99^{999999} when divided by 23 is 22.
Note that we can solve the final congruence a little differently as:
$99^{1}1 \equiv 7^{11}=(7^2)^5\cdot 7=(49)^5\cdot 7 \equiv 3^5\cdot 7=1701 \equiv 22(\text{mod}23)$.
There are many ways to evaluate these sort of congruences, some easier than others.

Example: What is the remainder when 13^{18} is divided by 19?
Solution: If $y^{\phi(z)}$ is divided by z, the remainder will always be 1; if y, z are co-prime
In this case the Euler number of 19 is 18
(The Euler number of a prime number is always 1 less than the number).
As 13 and 19 are co-prime to each other, the remainder will be 1.

Example: Now, let us solve the question given at the beginning of the article using the concept of Euler Number: What is the remainder of $19^{2200002}/23$?

Solution: The Euler Number of the divisor i.e. 23 is 22, where 19 and 23 are co-prime.

Hence, the remainder will be 1 for any power which is of the form of 220000.

The given power is 2200002.

Dividing that power by 22, the remaining power will be 2.

Your job remains to find the remainder of $19^2/23$.

As you know the square of 19, just divide 361 by 23 and get the remainder as 16.

Example: Find the last digit of 55^5.

Sol: We first note that finding the last digit of 55^5 can be obtained by reducing 55^5 (mod 10), that is evaluating 55^5(mod10).

We note that (10, 55) = 5, and hence this pair is not relatively prime, however, we know that 55 has a prime power decomposition of

55 = 5 x 11. (11, 10) = 1,

hence it follows that $11^{\phi(10)} \equiv 1 (mod10)$.

We note that $\phi(10)=4$. Hence $11^4 \equiv 1(mod10)$, and more appropriately:

$55^5=5^5 \cdot 11^5=5^5 \cdot 11^4 \cdot 11 \equiv 5^{12} \cdot (1)^4 \cdot 11 \equiv 34375 \equiv 5(mod10)$

Hence the last digit of 55^5 is 5.

Example: Find the last two digits of 3333^{4444}.

Sol:

We first note that finding the last two digits of 3333^{4444} can be obtained by reducing 3333^{4444} (mod 100).

Since (3333, 100) = 1, we can apply this theorem.

We first calculate that $\phi(100)=\phi(2^2)\phi(5^2)=(2)(5)(4)=40$.

Hence it follows from Euler's theorem that $3333^{40} \equiv 1(mod100)$.

Now let's apply the division algorithm on 4444 and 40 as follows:

$$4444=40(111)+4$$

Hence it follows that:

$3333^{4444} \equiv (3333^{40})^{111} \cdot 3333^4 \equiv (1)^{111} \cdot 3333^4 (mod100) \equiv 33^4=1185921 \equiv 21(mod100)$

Hence the last two digits of 3333^{4444} are 2 and 1.

Previous questions

1. a) Prove that a group consisting of three elements is an abelian group?
   b) Prove that G={-1,1,i,-i} is an abelian group under multiplication?
2. a) Let G= {-1,0,1} . Verify that G forms an abelian group under addition?
   b) Prove that the Cancellation laws holds good in a group G.?
3. Prove that the order of a^{-1} is same as the order of a.?
4. a) Explain in brief about fermats theorem?
   b) Explain in brief about Division theorem?
   c) Explain in brief about GCD with example?
5. Explain in brief about Euler's theorem with examples?
6. Explain in brief about Principle of Mathematical Induction with examples?
7. Define Prime number? Explain in brief about the procedure for testing of prime numbers?
8. Prove that the sum of two odd integers is an even integer?
9. State Division algorithm and apply it for a dividend of 170 and divisor of 11.
10. Using Fermat's theorem, find 3^{201} mod 11.
11. Use Euler's theorem to find a number between 0 and 9 such that *a* is congruent to 7^{1000} (mod 10)
12. Find the integers x such that i) 5x≡4 (mod 3) ii) 7x≡6 (mod 5) iii) 9x≡8 (mod 7)
13. Determine GCD (1970, 1066) using Euclidean algorithm.
14. If a=1820 and b=231, find GCD (a, b). Express GCD as a linear combination of a and b.
15. Find 11^7 mod 13 using modular arithmetic.

Multiple choice questions

1. If a|b and b|c, then a|c.
   a) True b) False
   Answer: a
2. GCD(a,b) is the same as GCD(|a|,|b|).
   a) True b) False
   Answer: a
3. Calculate the GCD of 1160718174 and 316258250 using Euclidean algorithm.
   a) 882 b) 770 c) 1078 d) 1225
   Answer: c
4. Calculate the GCD of 102947526 and 239821932 using Euclidean algorithm.
   a) 11 b) 12 c) 8 d) 6
   Answer: d
5. Calculate the GCD of 8376238 and 1921023 using Euclidean algorithm.
   a) 13 b) 12 c) 17 d) 7
   Answer: a
6. What is 11 mod 7 and -11 mod 7?
   a) 4 and 5 b) 4 and 4 c) 5 and 3 d) 4 and -4
   Answer: d
7. Which of the following is a valid property for concurrency?
   a) a = b (mod n) if n|(a-b) b) a = b (mod n) implies b = a (mod n)
   c) a = b (mod n) and b = c (mod n) implies a = c (mod n)
   d) All of the mentioned
   Answer: d
8. [(a mod n) + (b mod n)] mod n = (a+b) mod n
   a) True b) False
9. [(a mod n) – (b mod n)] mod n = (b – a) mod n
   a) True b) False
   Answer:b

10. 11^7 mod 13 =

a) 3 b) 7 c) 5 d) 15

Answer: d

11. The multiplicative Inverse of 1234 mod 4321 is

a) 3239 b) 3213 c) 3242 d) Does not exist

Answer: a

12. The multiplicative Inverse of 550 mod 1769 is

a) 434 b) 224 c) 550 d) Does not exist

Answer: a

13. The multiplicative Inverse of 24140 mod 40902 is

a) 2355 b) 5343 c) 3534 d) Does not exist

Answer: d

14. GCD(a,b) = GCD(b,a mod b)

a) True b) False

Answer: a

15. Define an equivalence relation R on the positive integers A = {2, 3, 4, . . . , 20} by m R n if the largest prime divisor of m is the same as the largest prime divisor of n. The number of equivalence classes of R is

(a) 8 (b) 10 (c) 9 (d) 11 (e) 7

Ans:a

16. The set of all nth roots of unity under multiplication of complex numbers form a/an

A.semi group with identity B.commutative semigroups with identity

C.group D.abelian group

Option: D

17. Which of the following statements is FALSE ?

A.The set of rational numbers is an abelian group under addition

B.The set of rational integers is an abelian group under addition

C.The set of rational numbers form an abelian group under multiplication

D.None of these

Option: D

18.In the group G = {2, 4, 6, 8) under multiplication modulo 10, the identity element is

A.6 B.8 C.4 D.2

Option: A

19. Match the following

A. Groups	I. Associativity
B. Semi groups	II. Identity
C. Monoids	III. Commutative
D. Abelian Groups	IV Left inverse

A. A B C D — IV I II III B. A B C D — III I IV II C. A B C D — II III I IV D. A B C D — I II III IV

Option: A

20. Let (Z,*) be an algebraic structure, where Z is the set of integers and the operation * is defined by n*m = maximum(n,m). Which of the following statements is TRUE for (Z,*)?

A.(Z, *) is a monoid B.(Z, *) is an abelian group C.(Z, *) is a group D.None

Option: D

21. Some group (G,0) is known to be abelian. Then which of the following is TRUE for G ?

A.$g = g^{-1}$ for every $g \in G$ B.$g = g^2$ for every $g \in G$

C.$(g \text{ o } h)^2 = g^2 \text{o } h^2$ for every $g,h \in G$ D.G is of finite order

Option: C

22. If the binary operation * is deined on a set of ordered pairs of real numbers as (a, b)*(c, d)

= (ad + bc, bd) and is associative, then (1, 2) * (3, 5) * (3, 4) equals

A.(74,40) B.(32,40) C.(23,11) D.(7,11)

Option: A

23. The linear combination of gcd(252, 198) = 18 is

a) 252*4 – 198*5 b) 252*5 – 198*4 c) 252*5 – 198*2 d) 252*4 – 198*4

Answer:a

24. The inverse of 3 modulo 7 is

a) -1 b) -2 c) -3 d) -4

Answer:b

25. The integer 561 is a Carmichael number.

a) True b) False

Answer:a

26. The linear combination of gcd(117, 213) = 3 can be written as

a) 11*213 + (-20)*117 b) 10*213 + (-20)*117

c) 11*117 + (-20)*213 d) 20*213 + (-25)*117

Answer:a

27. The inverse of 7 modulo 26 is

a) 12 b) 14 c) 15 d) 20

Answer:c

28. The inverse of 19 modulo 141 is

a) 50 b) 51 c) 54 d) 52

Answer:d

29. The value of 5^{2003} mod 7 is

a) 3 b) 4 c) 8 d) 9

Answer:a

30. The solution of the linear congruence 4x = 5(mod 9) is

a) 6(mod 9) b) 8(mod 9) c) 9(mod 9) d) 10(mod 9)

Answer:b

31. The linear combination of gcd(10 ,11) = 1 can be written as

a) (-1)*10 + 1*11 b) (-2)*10 + 2*11

c) 1*10 + (-1)*11 d) (-1)*10 + 2*11

Answer:a