Unit-I

Logic and Proofs

Propositions:

Defn:

A proposition (statement) is a declarative sentence that is either true or false, but not both.

Example:

1. Chennai is the capital of Tamil Nadu. [True]
2. 2+7 = 10 [False].

Notation:

* P, Q, R, S ... are used to denote propositions.
* T is used to denote True propositions.
* F is used to denote False propositions.

Defn:

Atomic statements: (Primary statements) (Simple).

Declarative sentences which cannot be further split into simpler sentences are called Atomic statements (also called primary statements or primitive statements).

Example:

Ramu is a boy.

Logical Connectives - Compound Propositions - Conditional & Biconditional Propositions - Truth tables. [1.1]

The area of logic that deals with propositions is called the propositional calculus or propositional logic.

Five Basic Connectives

S.No	Eng-Lang usages	Logical Connectives	Type of operator	Symbols.
1.	and	Conjunction	binary	$\wedge$
2.	or	disjunction	binary	$\vee$
3.	not	negation (or) denial	unary	$\neg$ (or) $\sim$
4.	if ... then	implication (or) Conditional	binary	$\rightarrow$
5.	if and only if	biconditional	binary	$\leftrightarrow$

Molecular statements.

Defn:

New statements can be formed from atomic statements through the use of connectives such as 'and', 'but', 'or' etc. The resulting statements are called molecular or compound or composite statements.

Example: Niranjan is a boy and Sita is a girl.

Defn:

* Compound Propositions:

Many mathematical statements are constructed by combining one or more propositions, new propositions called compound propositions, are formed from existing propositions using logical operators.

* Truth Table.

A table, giving the truth values of a compound statment in terms of its component parts, is called Truth table.

Defn: Negation [$\neg$ or $\sim$] [Not]

The negation of a statement is generally formed by introducing the word 'not' at a proper place in the statement.

If 'P' denotes a statement, then the negation of P is written as '$\neg P$' and read as 'not P'.

* If the truth values of P is T, then the truth value of $\neg P$ is F
* If the truth value of P is F, then the truth value of $\neg P$ is T

Table - 1

The truth table for the negation of a proposition

P	$\neg P$
T	F
F	T

Defn: Conjunction [$\wedge$] [AND]

The conjunction of two statements 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 P and Q have the truth value T; otherwise it has the truth value F.

Defn: Disjunction [$\vee$] [or]

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 true value F; otherwise it is true.

Defn: Conditional Statement [If, ... then] [$\rightarrow$]

If P and Q are any two statements, then the statement $P \rightarrow Q$ which is read as 'If P, then Q' is called a conditional statement.

* The statement $P \rightarrow Q$ has the truth value F when Q has the truth value F and P has the truth value T, otherwise it has the truth value T.

Note: In this implication P is called the hypothesis (or antecedent or premise) and Q is called the conclusion (or consequence).

Defn: Biconditional (equivalence) statement [$\leftrightarrow$] [if and only if]

If P and Q are any two statements, 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.

* The statement $P \leftrightarrow Q$ has the truth value T whenever both P and Q have identical true values.

Note: $P \leftrightarrow Q$ has exactly the same truth value as $(P \rightarrow Q) \wedge (Q \rightarrow P)$.

Defn: Exclusive or of P and Q [$P \oplus Q$]

Let P and Q be propositions. The exclusive or of P and Q, denoted by $P \oplus Q$, is the proposition that is true when exactly one of P and Q is true and is false otherwise.

Converse, Contrapositive, Inverse.

1. The proposition $Q \rightarrow P$ is called the converse $P \rightarrow Q$
2. The proposition $\neg Q \rightarrow \neg P$ is called the contrapositive of $P \rightarrow Q$
3. The proposition $\neg P \rightarrow \neg Q$ is called the inverse of $P \rightarrow Q$

Defn: Contrapositive [A.U. N/D 2005]

If $P \to Q$ is an implication, then the converse of $P \to Q$ is the implication $Q \to P$, and the contrapositive of $P \to Q$ is the implication $\neg P \to \neg P$.

Example: Give the converse and the contrapositive of the implication "If it is raining, then I get wet". [AU A/M 2004]

Solution:

P: It is raining

Q: I get wet.

$Q \to P$: (converse): If I get wet, then it is raining.

$\neg Q \to \neg P$: (contrapositive) If I do not get wet, then it is not raining.

		Conjunction	Disjunction	Negation	Conditional	Bi-conditional	Converse	Inverse	Contrapositive
P	Q	$P \wedge Q$	$P \vee Q$	$\neg P$	$P \to Q$	$P \leftrightarrow Q$	$Q \to P$	$\neg P \to \neg Q$	$\neg Q \to \neg P$
T	T	T	T	F	T	T	T	T	T
T	F	F	F	T	F	F	T	T	F
F	T	F	T	T	T	F	F	F	T
F	F	F	F	T	T	T	T	T	T

Well-formed formulas.

A well formed formula can be generated by the following rules:

1. A statement variable standing alone is a well formed formula.
2. If A is a well-formed formula, then $\neg A$ is a well-formed formula.
3. If A and B are well-formed formulas, then $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ and $(A \leftrightarrow B)$ are well-formed formulas.
4. A string of symbols containing the statement variables, connectives, and parenthesis is a well-formed formula, iff it can be obtained by finitely many applications of the rules 1, 2 and 3.

Precedence of Logical Operators

Precendence of Logical operators	
Operator	Precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Translate English sentences.

Example: 1 How can this English sentence be translated into a logical expression? [MCA A/M 2003]

"You can access the Internet from campus only if you are a computerscience major or you are not a freshman."

Solution:

a: You can access the Internet from campus.

b: You are a computer science major.

c: You are a freshman.

$\neg c$: You are not a freshman.

$$a \rightarrow (b \vee \neg c)$$

Note: 'only if' represents the symbol $\rightarrow$, 'or' represents '$\vee$', not represents the symbol '$\wedge$'.

Example: 2 State the truth value of "If tigers have wings, then the earth travels round the sun". [AU A/M 2003]

Solution: Let P: Tigers have wings. "F"

Q: The earth travels round the sun "T"

The given statement is $P \rightarrow Q$, has the truth value "T".

Boolean searches:

In Boolean searches, the connective AND is used to match both of two search terms, the connective OR is used to match one or both of two search terms, and the connective NOT is used to exclude a particular search term.

Logic puzzels:

Using logical reasioning puzzles can be solved are known as logic puzzles.

Example: 3.

Write the following statement in symbolic form "You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 years old."

Solution: Let a: You can ride the roller coaster.

b: You are under 4 feet tall

c: You are older than 16 yearks old.

Then the sentence can be translated $(b \wedge \neg c) \rightarrow a$

Example: 4 Let p and q be the proporitions "Swimming at the Chennai shore is allowed" and "Sharks have been spotted near the shore", respectively. Express each of these compound propositions as an English sentence.

(a) $\neg q$ (b) $\neg p \vee q$ (c) $p \wedge q$ (d) $\neg q \rightarrow p$ (e) $p \rightarrow \neg q$ (f) $\neg p \wedge (p \vee \neg q)$

Solution:

(a) Sharks have not been spotted near the shore.

(b) Swimming at the Chennai shore is not allowed, or sharks have been spotted near the shore.

(c) Swimming at the Chennai shore is allowed and sharkes have been spotted near the store.

(d) If sharks have not been spotted near the shore, then swimming at the Chennai shore is allowed.

(e) If swimming at the Chennai shore is allowed, then sharks have not been spotted near the shore.

(f) Swimming at the Chennai shore is not allowed, and either swimming at the chennai shore is allowed or sharks have not been spotted near the shore

Logic and Bit operations

Computers represent information using bits.

A bit has two possible values, namely 0 (zero) and 1 (one). We will use a 1 bit to represent true and a 0 bit to represent false. That is, 1 represents T, 0 represents F.

We will use the notation OR, AND and XOR for the operators $\vee$, $\wedge$ and $\oplus$

x	y	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Defn: A bit string is a sequence of zero or more bits. The length of this string is the number of bits in the string.

Truth Table

Example: 1 Construct the truth table for $P \vee \neg Q$ [MCA 1995, MU]

Solution:

P	Q	$\neg Q$	$P \vee \neg Q$
T	T	F	T
T	F	T	T
F	T	F	F
F	F	T	T

Example: 2 Construct the truth table for $P \wedge (P \vee Q)$ [MCA MU 94]

Soln:

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

Example: 3 Construct the truth table for $(P \vee Q) \vee \neg P$ [MCA MU 94]

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

Example: 4

Construct the truth table for the following: [MCA 95 M.U]

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

Solu:

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

Example: 5

$(\neg P \wedge (\neg Q \wedge R)) \vee ((Q \wedge R) \vee (P \wedge R))$ [AU A/M 2003]

Example: 6.

Construct the truth table for $(P \to Q) \wedge (Q \to P)$ [MCA MU1991]

Example: 7

Construct the truth table for $(Q \wedge (P \to Q)) \to P$ [MCA MU1993]

Example: 8

Construct the truth table for $(P \wedge Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$ [MCA MU1996]

Example: 9

(i) Construct the truth table for $\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$ [MCA MU1990]

(ii) $(P \to Q) \wedge (Q \to P)$ [MCA MU 1991]

Propositional Equivalences

★ **Tautology:**

A statement that is true for all possible values of its propositional variables is called a tautology or universely valid formula or a logical truth.

★ **Contradiction**

A Statement that is always false is called a contradiction or absurdity.

Note: 1. The negation of a contradiction is a Tautology (is called a contingency)

2. A propositional function that is neither a tautology nor a contradiction

3.

Tautology.	Contradiction	Fallacy
In the result column all the entries are 'T'	In the result column all the entries are 'F'	In the result column any one entry is 'F'

Example: 1

Show that $Q \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$ is tautology.

Solu: Let $S = Q \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$ [MCA MU 1996]

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

Since the truth value in the last column is T, the given formula is a tautology.

Examples: 2 Using the truth table verify that the proposition $(P \wedge Q) \wedge \neg(P \vee Q)$ [AU N/D 2003]

Solu:

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

All the entries in the last column are F therefore the given proposition is a contradiction.

Logical Equivalences and Implications - De Morgan's Laws.

Compound propositions that have the same truth values in all possible cases are called logically equivalent.

Defn: The propositions P and Q are called logically equivalent if $P \leftrightarrow$ is a tautology.

Note: The notation $P \equiv Q$ denotes that P and Q are logically equivalent. (or) we use $P \Leftrightarrow Q$ also.

Example:1 Show that P is equivalent to the following formulae.
(i) $\neg\neg P$ (ii) $P \wedge P$ (iii) $P \vee P$ (iv) $P \vee (P \wedge Q)$ (v) $P \wedge (P \vee Q)$
[MCA MU 1996]

1	2	3	4	5	6	7	8	9	10
P	Q	$\neg P$	$\neg\neg P$	$P \wedge P$	$P \vee P$	$P \wedge Q$	$P \vee (P \wedge Q)$	$P \vee Q$	$P \wedge (P \vee Q)$
T	T	F	T	T	T	T	T	T	T
T	F	F	T	T	T	F	T	T	T
F	T	T	F	F	F	F	F	T	F
F	F	T	F	F	F	F	F	F	F

Here the 4th, 5th, 6th, 8th, 10th columns give the truth values of the formulas. The columns 1, 4, 6, 8, 10 have identical truth values. Hence P is equivalent to all the given formulas.

Example:2 Show that P is equivalent to the following formulae.
(i) $(P \wedge Q) \vee (P \wedge \neg Q)$ (ii) $(P \vee Q) \wedge (P \vee \neg Q)$ [MCA MU May 1995]

Soln:

1	2	3	4	5	6	7	8	9
P	Q	$P \wedge Q$	$\neg Q$	$P \wedge \neg Q$	$(P \wedge Q) \vee (P \wedge \neg Q)$	$P \vee Q$	$P \vee \neg Q$	$(P \vee Q) \wedge (P \vee \neg Q)$
T	T	T	F	F	T	T	T	T
T	F	F	T	T	T	T	T	T
F	T	F	F	F	F	T	F	F
F	F	F	T	F	F	F	T	F

Columns 1, 6, 9 have identical truth values.
Hence $P \Leftrightarrow (P \wedge Q) \vee (P \wedge \neg Q)$
$\Leftrightarrow (P \vee Q) \wedge (P \vee \neg Q)$.

Table logic equivalences

Equivalence	Name
$P \wedge T \Leftrightarrow P$ $P \vee F \Leftrightarrow P$	Identity laws
$P \vee T \Leftrightarrow T$ $P \wedge F \Leftrightarrow F$	Domination laws
$P \vee P \Leftrightarrow P$ $P \wedge P \Leftrightarrow P$	Idempotent laws.
$\neg(\neg P) \Leftrightarrow P$	Double negation law
$P \vee Q \Leftrightarrow Q \vee P$ $P \wedge Q \Leftrightarrow Q \wedge P$	Commutative laws.
$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$	Associative laws.
$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$ $(P \vee Q) \wedge R \Leftrightarrow (P \wedge R) \vee (Q \wedge R)$ $(P \wedge Q) \vee R \Leftrightarrow (P \vee R) \wedge (Q \vee R)$	Distributive laws.
$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$ $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	De Morgan's law.
$P \vee (P \wedge Q) \Leftrightarrow P$ $P \wedge (P \vee Q) \Leftrightarrow P$	Absorption laws.
$P \vee \neg P \Leftrightarrow T$ (or) $\neg P \vee P \Leftrightarrow T$ $P \wedge \neg P \Leftrightarrow F$ (or) $\neg P \wedge P \Leftrightarrow F$	Negation laws
Contrapositive law	$P \rightarrow q \Leftrightarrow \neg P \rightarrow \neg q$

Bicondition as conditional · $P \Leftrightarrow q \Leftrightarrow (P \rightarrow q) \wedge (q \rightarrow P)$. | Complement laws: $P \wedge \neg P \Leftrightarrow F$ & $P \vee \neg P \Leftrightarrow T$
Conditional as disjunction - $P \rightarrow q \Leftrightarrow \neg P \vee q$ | Exportations laws $P \rightarrow (q \rightarrow r) \Leftrightarrow (P \wedge q) \rightarrow r$

Replacement Process

Consider the formula $A : P \rightarrow (Q \rightarrow R)$.

Here $Q \rightarrow R$ is a part of the formula A.

If we replace $Q \rightarrow R$ by an equivalent formula $\neg Q \vee R$ in A, we get another formula.

$B: P \rightarrow (\neg Q \vee R)$. We can easily verify that the formulas A and B are equivalent to each other.

This process of obtaining B from A is know as the replacement process.

Tautological Implications

A statement A is said to tautologically imply a statement B if and only if $A \rightarrow B$ is a tautology. In this case, we write $A \Rightarrow B$, read as "A implies B"

Example.

Show that $(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R) \Leftrightarrow R$ [AU N/D 2003]

Solution:

	Reasons.
(i) $\neg P \wedge (\neg Q \wedge R)$	
$\Leftrightarrow (\neg P \wedge \neg Q) \wedge R$	Associative law.
$\Leftrightarrow \neg (P \vee Q) \wedge R$	Demorgan's law
(ii) $Q \wedge R \vee (P \wedge R) \Leftrightarrow (Q \vee P) \wedge R$	Distributive law.
$\Leftrightarrow (P \vee Q) \wedge R$	Commutative law.
$(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R)$	Given.
$\Leftrightarrow (\neg (P \vee Q) \wedge R) \vee ((P \vee Q) \wedge R)$	by (i) & (ii)
$\Leftrightarrow (\neg (P \vee Q) \vee (P \vee Q)) \wedge R$	Distributive law.
$\Leftrightarrow T \wedge R$	Negation law.
$\Leftrightarrow R$	Identity law

Example: 2

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

Solu:

$(P \vee Q) \wedge \neg(\neg P \wedge Q)$	Reasons
$\Leftrightarrow (P \vee Q) \wedge (\neg\neg P \vee \neg Q)$	Demorgan's law.
$\Leftrightarrow (P \vee Q) \wedge (P \vee \neg Q)$	Double negation law.
$\Leftrightarrow P \vee (Q \wedge \neg Q)$	Distributive law of $\vee$ over $\wedge$.
$\Leftrightarrow P \vee F$	Negation law.
$\Leftrightarrow P$	Identity law.

Example: 3.

Show that $\neg(P \wedge Q) \rightarrow (\neg P \vee (\neg P \vee Q)) \Leftrightarrow (\neg P \vee Q)$ [AU A/M 2004]

Use only the $\Leftrightarrow$ laws.

	Reasons.
(i) $\neg P \vee (\neg P \vee Q) \Leftrightarrow (\neg P \vee \neg P) \vee Q$ $\Leftrightarrow \neg P \vee Q$	Associative law Idempotent law $P \vee P = P$.
$\neg(P \wedge Q) \rightarrow (\neg P \vee (\neg P \vee Q))$	Given.
$\Leftrightarrow \neg(P \wedge Q) \rightarrow (\neg P \vee Q)$	by (i)
$\Leftrightarrow (P \wedge Q) \vee (\neg P \vee Q)$	$P \rightarrow Q \Leftrightarrow \neg P \vee Q$
$\Leftrightarrow (P \vee (\neg P \vee Q)) \wedge (Q \vee (\neg P \vee Q))$	Distributive law $[(P \wedge Q) \vee R \Leftrightarrow (P \vee R) \wedge (Q \vee R)]$
$\Leftrightarrow ((P \vee \neg P) \vee Q) \wedge (Q \vee (Q \vee \neg P))$	Associative law & Commutative law.
$\Leftrightarrow (T \vee Q) \wedge ((Q \vee Q) \vee \neg P)$	Negation law & Associative law.
$\Leftrightarrow T \wedge (Q \vee \neg P)$	Domination law & Idempotent law
$\Leftrightarrow Q \vee \neg P$	Identity law.
$\Leftrightarrow \neg P \vee Q$	Commutative law.

Example: 4.

Show that $(P \vee Q) \wedge (\neg P \wedge (\neg P \wedge Q)) \Leftrightarrow (\neg P \wedge Q)$ [MCA MU May 1995]

Solu:

$(P \vee Q) \wedge (\neg P \wedge (\neg P \wedge Q))$	Reasons.
$\Leftrightarrow (P \vee Q) \wedge ((\neg P \wedge \neg P) \wedge Q)$	Associative law.
$\Leftrightarrow ((P \vee Q) \wedge (\neg P \wedge Q))$	Since $\neg P \wedge \neg P \Leftrightarrow \neg P$.
$\Leftrightarrow ((P \vee Q) \wedge \neg P) \wedge Q$	Associative law.
$\Leftrightarrow ((P \wedge \neg P) \vee (Q \wedge \neg P)) \wedge Q$	Distributive law.
$\Leftrightarrow (F \vee (Q \wedge \neg P)) \wedge Q$	Negation law $(P \wedge \neg P \Leftrightarrow F)$
$\Leftrightarrow (Q \wedge \neg P) \wedge Q$	Identity law.
$\Leftrightarrow (\neg P \wedge Q) \wedge Q$	Commutative law.
$\Leftrightarrow \neg P \wedge (Q \wedge Q)$	Associative
$\Leftrightarrow \neg P \wedge Q$	Idempotent law.

Example: 5

Show that $P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R \Leftrightarrow P \rightarrow (\neg Q \vee R)$

[MCA MU Dec. 92, May 93, Nov. 94, May 95]

Solution:

$P \rightarrow (Q \rightarrow R)$	Reasons.
$\Leftrightarrow P \rightarrow (\neg Q \vee R)$	Since $Q \rightarrow P \Leftrightarrow \neg Q \vee R$
$\Leftrightarrow \neg P \vee (\neg Q \vee R)$	Since $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
$\Leftrightarrow (\neg P \vee \neg Q) \vee R$	Associative law.
$\Leftrightarrow \neg (P \wedge Q) \vee R$	Demorgan's law.
$\Leftrightarrow (P \wedge Q) \rightarrow R$	$\therefore \neg P \vee Q \Leftrightarrow P \rightarrow Q$.

Example: 6

Show that $P \to (Q \to P) \Leftrightarrow \neg P \to (P \to Q)$

[MCA MU May 1995]

Solu:

(i) $P \to (Q \to P)$	Reasons
$\Leftrightarrow P \to [\neg Q \vee P]$	$\because Q \to P \Leftrightarrow \neg Q \vee P$
$\Leftrightarrow \neg P \vee [\neg Q \vee P]$	$\because P \to Q \Leftrightarrow \neg P \vee Q$
$\Leftrightarrow \neg P \vee (P \vee \neg Q)$	Commutative.
$\Leftrightarrow (\neg P \vee P) \vee \neg Q$	Associative.
$\Leftrightarrow T \vee \neg Q$	Negation.
$\Leftrightarrow T$	Since $T \vee \neg Q \Leftrightarrow T$

(ii) $\neg P \to (P \to Q)$	Reasons.
$\Leftrightarrow \neg P \to (\neg P \vee Q)$	$\because P \to Q \Leftrightarrow \neg P \vee Q$
$\Leftrightarrow \neg(\neg P) \vee (\neg P \vee Q)$	"
$\Leftrightarrow P \vee (\neg P \vee Q)$	Double negation.
$\Leftrightarrow (P \vee \neg P) \vee Q$	Associative
$\Leftrightarrow T \vee Q$	$P \vee \neg P \Leftrightarrow T$
$\Leftrightarrow T$	

From (i) & (ii) we get $P \to (Q \to P) \Leftrightarrow \neg P \to (P \to Q)$.

Example: 7

Show that $P \to (Q \vee R) \Leftrightarrow (P \to Q) \vee (P \to R)$

[MCA MU May 1997]

Solu:

	Reason.
(i) $P \to (Q \vee R) \Leftrightarrow \neg P \vee (Q \vee R)$	$P \to Q \Leftrightarrow \neg P \vee Q$
(ii) $(P \to Q) \vee (P \to R)$	
$\Leftrightarrow (\neg P \vee Q) \vee (\neg P \vee R)$	
$\Leftrightarrow \neg P \vee (Q \vee \neg P) \vee R$	
$\Leftrightarrow \neg P \vee \{\neg P \vee Q\} \vee R$	Commutative law.
$\Leftrightarrow \neg P \vee (Q \vee R)$	Idempotent law.
From (i) & (ii) we get $P \to (Q \vee R) \Leftrightarrow (P \to Q) \vee (P \to R)$	

Example: 8

Show that $(P \to Q) \wedge (R \to Q) \Leftrightarrow (P \vee R) \to Q$

[MCA ND 2002]

$(P \to Q) \wedge (R \to Q)$	Reasons.
$\Leftrightarrow (\neg P \vee Q) \wedge (\neg R \vee Q)$	Since $P \to Q \Leftrightarrow \neg P \vee Q$
$\Leftrightarrow (\neg P \wedge \neg R) \vee Q$	Distributive law.
$\Leftrightarrow \neg (P \vee R) \vee Q$	De Morgan's law.
$\Leftrightarrow P \vee R \to Q$	Since $\neg P \vee Q \Leftrightarrow P \to Q$.

Duality:

The dual of a compound proposition that contains only the logical operators $\vee$, $\wedge$ and $\neg$ is the proposition obtained by replacing each $\vee$ by $\wedge$, each $\wedge$ by $\vee$, each T by F and each F by T. The dual of proposition A is denoted by A^*.

Theorem: Duality principle theorem.

If A and A^* be dual formulas and if $P_1, \ldots P_n$ be the atomic variables that occur in A and A^*.

(i.e) $A = A(P_1, \ldots, P_n)$ and $A^* = A^*(P_1, P_2 \ldots P_n)$ then

$\neg A(P_1, \ldots, P_n) \Leftrightarrow A^*(\neg P_1, \ldots P_n)$ and

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

That is the negation of a formula is equivalent to its dual in which every variable is replaced by its negation.

Note: If any two formulas A and B are equivalent, then their duals A^* and B^* are also equivalent.

★. Functionally complete sets of connectives [AU AM 2005]

A set of connectives in which every formula can be expressed as another equivalent formula containing connectives from this set is called functionally complete set of connectives.

A collection of logical operators is called functionally complete if every compound proposition is logically equivalent to a compound proposition involving only these logical operators.

Example:

The set of connectives $\{\wedge, \neg\}$ and $\{\vee, \neg\}$ are functionally complete.

$\{\neg\}$, $\{\wedge\}$, $\{\vee\}$ or $\{\vee, \wedge\}$ are not functionally complete.

Note: From the five connectives $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$ we have obtained atleast two sets of functionally complete connectives.

Example: 1.

Write an equivalent formula for $P \wedge (Q \leftrightarrow R)$ which contains neither the biconditional nor the conditional.

Solu:

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

Thus the required formula is $P \wedge ((\neg Q \vee R) \wedge (\neg R \vee Q))$.

Example: 2 [AU ND 2004]

Show that $\{\vee, \wedge\}$ is not functionally complete.

Solu:

$\neg P$ cannot be expressed using the connectives $\{\vee, \wedge\}$. Since no such contribution of statement exist with $\{\vee, \wedge\}$ as input is T and the output is F.

The other connectives

Exclusive OR

Let P and Q be any two formulas. Then the formula $P \bar{\vee} Q$, in which the connective $\bar{\vee}$ is called an exclusive OR, is true whenever either P or Q, but not both, is true.

NAND ($\uparrow$)

"NAND" is a word which is a combination of the words "NOT" and "AND" when NOT stands for negation and "AND" stands for conjunction. It is denoted by the symbol "$\uparrow$".

Let P and Q be any two statement formulas, then "P NAND Q" is denoted by "$P \uparrow Q$" and is defined as $P \uparrow Q \Leftrightarrow \neg(P \wedge Q)$

NOR ($\downarrow$)

The word "NOR" is a combination of "NOT" and "OR" where NOT stands for negation and "OR" stands for disjunction. It is denoted by "$\downarrow$". Let P and Q be any statement formulas, then "P NOR Q" is denoted by "$P \downarrow Q$" and is defined as $P \downarrow Q \Leftrightarrow \neg(P \vee Q)$.

Some basic properties of NAND and NOR

1. $P \uparrow Q \Rightarrow Q \uparrow P$, $P \downarrow Q \Leftrightarrow Q \downarrow P$ (Commutative)
2. $P \uparrow (Q \uparrow R) \Leftrightarrow P \uparrow \neg(Q \wedge R)$
   $\Leftrightarrow \neg(P \wedge \neg(Q \wedge R))$
   $\Leftrightarrow \neg P \vee (Q \wedge R)$

   $P \uparrow (Q \uparrow R) \not\Leftrightarrow (P \wedge Q) \vee \neg R$ (not associative).

Similarly, $P \downarrow (Q \downarrow R)$ also not associative.

Note: The operators $\uparrow$ and $\downarrow$ are called the sheffer stroke and the pierce arrow after H.M. Sheffer and C.S. Peirce, respectively

Example: Construct the truth table for $(P \bar{\vee} Q) \rightarrow P$ [MCA 90 1-U]

Solu:

P	Q	$P \bar{\vee} Q$	$(P \bar{\vee} Q) \rightarrow P$
T	T	F	T
T	F	T	T
F	T	T	F
F	F	F	T

Normal Forms:

The standard forms are called canonical forms or normal forms.

Note: It will be convenient to use the word "product" in place of "conjunction" and "sum" in place of "disjunction".

Defn: Elementary product.

A product of the variable and their negations in a formula is called an elementary product. (product means conjunct

Example: Let P and Q be any two atomic variables. Then P, $\neg P \wedge Q$, $\neg Q \wedge P$, $P \wedge \neg P$ and $Q \wedge \neg P$ are elementary products.

Elementary Sum:

Defn: A sum of the variable and their negations in a formula is called an elementary sum. (sum means disjunction).

Example: Let P and Q be any two variables. Then P, $\neg P \vee Q$, $\neg Q \vee P$, $P \vee \neg P$ and $Q \vee \neg P$ are elementary sums.

Defn: Factor

Any part of an elementary product or elementary sum, which is itself an elementary product of sum is a factor of the product or sum.

Example: $Q \vee P$ is a factor of $\neg Q \vee Q \vee P$.

Note: 1. An elementary product is identically false if it contains atleast one pair of factors in which one is negation of the other.

Example: $P \wedge \neg P \Leftrightarrow F$.

Note: 2 An elementary sum is identically false if it contains atleast one pair of factors in which one is negation of the other.

Example: $P \vee \neg P \Leftrightarrow T$.

Disjunctive Normal Form (DNF)

Defn: A formula which is equivalent to a given formula and which consists of a sum of elementary products is called a disjunctive normal form (DNF) of the given formula.

Example: Obtain the DNF for $(P \rightarrow (Q \wedge R)) \wedge (\neg(\neg P \rightarrow \neg Q) \vee \neg R)$ [AU ND 2003]

Soln:

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

$\Leftrightarrow (\neg P \vee (Q \wedge R)) \wedge ((P \vee \neg Q) \wedge \neg R)$ Demorgan & Double negation law.

$\Leftrightarrow (\neg P \vee (Q \wedge R)) \wedge ((P \wedge \neg R) \vee (\neg Q \wedge \neg R))$ Distributive law.

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

$\Leftrightarrow ((\neg P \wedge P) \wedge \neg R) \vee (\neg P \wedge (\neg Q \wedge \neg R)) \vee ((Q \wedge R) \wedge (P \wedge \neg R))$ Extended distributive law.

$\vee ((Q \wedge R) \wedge (\neg Q \wedge \neg R))$ Associative law

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

$\Leftrightarrow F \vee (\neg P \wedge (\neg Q \wedge \neg R)) \vee ((Q \wedge R) \wedge (P \wedge \neg R)) \vee ((Q \wedge R) \wedge (\neg Q \wedge \neg R))$ Negation law.

$\Leftrightarrow (\neg P \wedge (\neg Q \wedge \neg R)) \vee ((Q \wedge R) \wedge (P \wedge \neg R)) \vee ((Q \wedge R) \wedge (\neg Q \wedge \neg R))$ Domination law.

This is the required DNF, as it is a product of elementary sums. Identity law.

~~Example:~~ ~~Obtain a conjunctive normal of form~~

Conjunctive normal form:

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

Example:2 [AU ND 2003]

Obtain a CNF for $(P \rightarrow (Q \wedge R)) \wedge (\neg P \rightarrow (\neg Q \wedge \neg R))$

Solu:

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

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

$\Leftrightarrow ((\neg P \vee Q) \wedge (\neg P \vee R)) \wedge (P \vee \neg Q) \wedge (P \vee \neg R)$ Distributive law.

This is a CNF, as it is a product of elementary sums.

Example:3

Obtain CNF, ~~as it is a product of elementary sw~~ of the formula $P \rightarrow ((P \rightarrow Q) \wedge \neg(\neg Q \vee \neg P))$ [AU ND 2003]

Solu:

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

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

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

$\Leftrightarrow \neg P \vee ((\neg P \vee Q) \wedge (Q \wedge P))$ Demorgan's law.

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

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

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

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

This is a CNF, as it is a product of elementary sums.

Min terms.

Let P & Q be two statement variables. Construct all possible formula which consist of conjunctions of P or its negation and conjuctions of Q or its negation. None of the formula should contain both a variable and its negation. Delete formula if it is the Commutative of any one of the remaining formulae. Such conjunctions of P & Q are called the minterms of P and Q.

Example:
Min terms of P&Q are P∧Q, P∧¬Q, ¬P∧Q and ¬P∧¬Q

Note: 1. P∧Q or Q∧P is included but not both.
2. P∧¬P and Q∧¬Q are not allowed.
3. No two minterms are equivalent.
4. Each minterm has the truth value T for exactly one combination of the truth values of the variables P and Q.
5. In general for given n-number of variables there will be 2^n minterms.

Principal Disjunctive Normal Form: (PDNF)

A formula which is equivalent to a given formula and which consists of sum of its min-terms is called "principal disjunctive normal form". (or) "sum of products of canonical form" of the given formula.

Construction of PDNF without truth table:

1. To replace conditionals and biconditionals by their equivalent formula involving ∧, ∨, ¬ only.
2. To use DeMorgan's laws and distributive laws.
3. to drop any elementary product which is a contradiction.
4. to obtain minterms in the disjunctions by introducing missing factors.
5. to delete indentical minterms keeping only one, that appear in the disjunction.

Max terms:

For a given number of variables, the maxterm consists of disjunctions in which each variable or its negation, but not both, appears only once

Remarks:

1. The maxterms are the duals of minterms.
2. Different maxterms have the truth value for different combination of the truth values of the variables.

Principal Conjunctive Normal Form (PCNF)

An equivalent formula consisting of conjunctions of maxterms only is known as its principal conjunctive normal form or the product-of-sums canonical form.

Remark:

Every formula which is not a tautology has an equivalent PCNF which is unique except for the rearrangement of the factors in the maxterms as well as in the conjunctions.

Example: 1

Obtain the pdnf of $P \leftrightarrow Q$. Also find pcnf.

Solu:

Let $S \Leftrightarrow P \leftrightarrow Q$

Method: 1

truth table.

P	Q	S	Minterm	Maxterm
T	T	T	$P \wedge Q$	—
T	F	F	—	$\neg P \vee Q$
F	T	F	—	$P \vee \neg Q$
F	F	T	$\neg P \wedge \neg Q$	—

$\therefore S \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$ pdnf by using minterms

$S \Leftrightarrow (\neg P \vee Q) \wedge (P \vee \neg Q)$ pcnf by using maxterms.

Method: 2

$S \Leftrightarrow P \leftrightarrow Q$

$\Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$ [$\because P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$]

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

$\Leftrightarrow (\neg P \wedge \neg Q) \vee (\neg P \wedge P) \vee (Q \wedge \neg Q) \vee (Q \wedge P)$ [$\because$ extended distributive law]

$\Leftrightarrow (\neg P \wedge \neg Q) \vee (Q \wedge P)$ [$\because (\neg P \wedge P), (Q \wedge \neg Q)$ terms droped]

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

$\therefore S \Leftrightarrow (\neg P \wedge \neg Q) \vee (P \wedge Q)$ (pdnf)

$\neg S \Leftrightarrow$ The remaing minterms.

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

$\neg(\neg S) \Leftrightarrow$ Apply duality principal to $\neg S$.

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

Example: 2

Obtain PDNF of $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$. Also find PCNF. [MCA MU AM 2003]

Solu: Let $S \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$

Let $A = (\neg P \wedge R) \vee (Q \wedge R)$

Truth table

P	Q	R	$P \wedge Q$	$\neg P \wedge R$	$Q \wedge R$	A	S	Minterm	Maxterm
T	T	T	T	F	T	T	T	$P \wedge Q \wedge R$	
T	T	F	T	F	F	F	T	$P \wedge Q \wedge \neg R$	
T	F	T	F	F	F	F	F		$\neg P \vee Q \vee \neg R$
T	F	F	F	F	F	F	F		$\neg P \vee Q \vee R$
F	T	T	F	T	T	T	T	$\neg P \wedge Q \wedge R$	
F	T	F	F	F	F	F	F		$P \vee \neg Q \vee R$
F	F	T	F	T	F	T	T	$\neg P \wedge \neg Q \wedge R$	
F	F	F	F	F	F	F	F		$P \vee Q \vee R$

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

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

Example: 3 [AUND 2004, AUAM 2004, AUAM 2003, AUAM 2005, AUND 200

Without constructing the truth table obtain the product of sums canonical form of the formula. $(\neg P \to R) \wedge (Q \leftrightarrow P)$. Hence find the sum of products canonical form.

Solu: Let $S \Leftrightarrow (\neg P \to R) \wedge (Q \leftrightarrow P)$

Method: I Truth table method.

(T) (F)→∨

P	Q	R	¬P	¬P→R	Q↔P	S	Minterm	maxterm
T	T	T	F	T	T	T	P∧Q∧R	
T	T	F	F	T	T	T	P∧Q∧¬R	
T	F	T	F	T	F	F	—	¬P∨Q∨¬R
T	F	F	F	T	F	F	—	¬P∨Q∨R
F	T	T	T	T	F	F	—	P∨¬Q∨¬R
F	T	F	T	F	F	F	—	P∨¬Q∨R
F	F	T	T	T	T	T	¬P∧¬Q∧R	—
F	F	F	T	F	T	F	—	P∨Q∨R

$S \Leftrightarrow (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R)$ pdnf.

$S \Leftrightarrow (\neg P \vee Q \vee \neg R) \wedge (P \vee \neg Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee Q \vee R)$ pcnf.

Method: 2

Let $S \Leftrightarrow (\neg P \to R) \wedge (Q \leftrightarrow P)$

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

$(\because P \to Q \Leftrightarrow \neg P \vee Q,\ Q \leftrightarrow P \Leftrightarrow (Q \to P) \wedge (P \to Q))$

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

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

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

$[\because P \vee F = P]$.

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

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

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

$\wedge [(\neg P \vee Q \vee R) \wedge (\neg P \vee Q \vee \neg R)]$. [$\because$ By distributive law].

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

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

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

$\neg S \Leftrightarrow$ the remaining max terms of P, Q and R.

Max terms of P, Q, R are

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

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

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

$\neg(\neg S) \Leftrightarrow$ Apply duality principle to $\neg S$.

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

pdnf.

———— x ———— x ————

Example:

Obtain the product of sums canonical form for $(P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge \neg R)$. [AU Nov/Dec. 2007]

Solu:

Let $S \Leftrightarrow (P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge \neg R)$.

pdnf is given.

$\neg S \Leftrightarrow$ The remaining minterms.

The minterms of P, Q, R are $P \wedge Q \wedge R$, $P \wedge Q \wedge \neg R$, $P \wedge \neg Q \wedge R$, $\neg P \wedge Q \wedge R$, $P \wedge \neg Q \wedge \neg R$, $\neg P \wedge Q \wedge \neg R$, $\neg P \wedge \neg Q \wedge R$, $\neg P \wedge \neg Q \wedge \neg R$

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

$\neg(\neg S) \Leftrightarrow$ Apply duality ~~principal~~ principle to $\neg S$ we get pcnf.

$S \Leftrightarrow (\neg P \vee \neg Q \vee R) \wedge (\neg P \vee Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee Q \vee \neg R)$. pcnf

Rules of inference.

Defn: Inference theory.

The main function of logic is to provide rules of inference, or principles of reasoning. The theory associated with such rules is known as inference theory, because it is concerned with the inferring of a conclusion from certain premises.

Defn: Valid argument or valid conclusion

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 or conclusion is called a valid argument or valid conclusion.

Note: The method of determine whether the conclusion logically follows from the given premises by constructing the relevant truth table is called "truth table technique".

Defn:
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 $A \to B$ is a tautology, that is $A \Rightarrow B$.

Just as the defn. of implication was extended to include a set of formulas rather than a single formula, we say that from a set of premises $\{H_1, H_2, \ldots, H_m\}$ a conclusion C follows logically if $H_1 \wedge H_2 \wedge \ldots \wedge H_m \Rightarrow C$.

I. Truth table technique:

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

(i) Let $P_1, P_2, \ldots P_n$ be all the atomic variables appearing in the premises $H_1, H_2, \ldots H_m$ and the conclusion C. If all possible combinations of truth values are assigned to $P_1, P_2, \ldots P_n$ and if the truth values of $H_1, H_2, \ldots H_m$ and C are entered in a table, then it is easy to see from such a table whether.

$H_1 \wedge H_2 \wedge \ldots \wedge H_m \Rightarrow C$ is true.

(ii) We look for the rows in which all $H_1, H_2, \ldots H_m$ have the value T. If, for every such row, C also has the value T, then.

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

(iii) Alternatively, we may look for the rows in which C has the value F. If, in every such row, atleast one of the values of $H_1, H_2, \ldots H_m$ is F, then $H_1 \wedge H_2 \wedge \ldots \wedge H_m \Rightarrow C$.

Example:

Determine whether the conclusion C follows logically from the premises H_1 and H_2.

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

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

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

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

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

Sol:

P	Q	P→Q	¬P	¬Q	¬(P∧Q)	P↔Q	(P→Q)∧P
T	T	T	F	F	F	T	T
T	F	F	F	T	T	F	F
F	T	T	T	F	T	F	F
F	F	T	T	T	T	T	F

(a) $((P \to Q) \wedge P) \to Q$ — Valid.

P	Q	(P→Q)∧¬P
T	T	F
T	F	F
F	T	T
F	F	T

(b) : $((P \to Q) \wedge \neg P) \to \neg$ — Not valid.

P	Q	(P→Q)∧¬(P∧Q)
T	T	F
T	F	T
F	T	T
F	F	T

(c) : $((P \to Q) \wedge \neg(P \wedge Q)) \to \neg P$ — Valid.

P	Q	¬P∧(P↔Q)
T	T	F
T	F	F
F	T	F
F	F	T

(d) : $(\neg P \wedge (P \leftrightarrow Q)) \to \neg(P \wedge Q)$ — Valid.

P	Q	(P→Q)∧Q
T	T	T
T	F	F
F	T	T
F	F	F

(e) $((P \to Q) \wedge Q) \to P$ — Not valid.

Implications

I_1	$P \wedge Q \Rightarrow P$	Simplification.
I_2	$P \wedge Q \Rightarrow Q$	
I_3	$P \Rightarrow P \vee Q$	Addition.
I_4	$Q \Rightarrow P \vee Q$	
I_5	$\neg P \Rightarrow P \to Q$	
I_6	$Q \Rightarrow P \to Q$	
I_7	$\neg(P \to Q) \Rightarrow P$	
I_8	$\neg(P \to Q) \Rightarrow \neg Q$	
I_9	$P, Q \Rightarrow P \wedge Q$	
I_{10}	$\neg P, P \vee Q \Rightarrow Q$	(disjunctive syllogism)
I_{11}	$P, P \to Q \Rightarrow Q$	(modus ponens)
I_{12}	$\neg Q, P \to Q \Rightarrow \neg P$	(modus tollens)
I_{13}	$P \to Q, Q \to R \Rightarrow P \to R$	(hypothetical syllogism)
I_{14}	$P \vee Q, P \to R, Q \to R \Rightarrow R$	dilemma.

Equivalences

E_1	$\neg\neg P \Leftrightarrow$	double negation
E_2	$P \wedge Q \Leftrightarrow Q \wedge P$	Commutative laws
E_3	$P \vee Q \Leftrightarrow Q \vee P$	
E_4	$(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$	Associative laws
E_5	$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$	
E_6	$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$	Distributive laws.
E_7	$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$	
E_8	$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$	De Morgan's laws
E_9	$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	
E_{10}	$P \vee P \Leftrightarrow P$	
E_{11}	$P \wedge P \Leftrightarrow P$	
E_{12}	$R \vee (P \wedge \neg P) \Leftrightarrow R$	
E_{13}	$R \wedge (P \vee \neg P) \Leftrightarrow R$	
E_{14}	$R \vee (P \vee \neg P) \Leftrightarrow T$	
E_{15}	$R \wedge (P \wedge \neg P) \Leftrightarrow F$	
E_{16}	$P \to Q \Leftrightarrow \neg P \vee Q$	
E_{17}	$\neg(P \to Q) \Leftrightarrow P \wedge \neg Q$	
E_{18}	$P \to Q \Leftrightarrow \neg Q \to \neg P$	
E_{19}	$P \to (Q \to R) \Leftrightarrow (P \wedge Q) \to R$	
E_{20}	$\neg(P \leftrightarrow Q) \Leftrightarrow P \leftrightarrow \neg Q$	
E_{21}	$P \leftrightarrow Q \Leftrightarrow (P \to Q) \wedge (Q \to P)$	
E_{22}	$(P \leftrightarrow Q) \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$	

11) Without using truth table:

Rules of Inference.

Rule of Inference	Tautology	Name
P $P \to Q$ $\therefore Q$	$[P \wedge (P \to Q)] \to Q$	Modus ponens
$\neg Q$ $P \to Q$ $\therefore \neg P$	$[\neg Q \wedge (P \to Q)] \to \neg P$	Modus tollens
$P \to Q$ $Q \to R$ $\therefore P \to R$	$[(P \to Q) \wedge (Q \to R)] \to (P \to R)$	Hypothetical syllogism
$P \vee Q$ $\neg P$ $\therefore Q$	$[(P \vee Q) \wedge \neg P] \to Q$	Disjunctive syllogism.
P $\therefore P \vee Q$	$P \to (P \vee Q)$	Addition.
$P \wedge Q$ $\therefore P$	$(P \wedge Q) \to P$	Simplification.
P Q $\therefore P \wedge Q$	$[(P) \wedge (Q)] \to (P \wedge Q)$	Conjunction.
$P \vee Q$ $\neg P \vee R$ $\therefore Q \vee R$	$[(P \vee Q) \wedge (\neg P \vee R)] \to Q \vee R.$	Resolution

Rules for inferences theorey

Rule: P

A premise may be introduced at any point in the ~~derivation~~ derivation.

Rule: T

A formula S may be introduced in a derivation if S is atautologically implied by any one or more of the preceding formulas in the derivation.

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 ~~premise~~ premises alone.

Note: 1. Rule CP is also called the deduction theorem.

2. Whenever the assumed premise is used in the derivation then the method of derivation is called indirect method of derivation.

Example:

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

Solu:

	Step	Derivation	~~Rule~~ Reason.
{1}	(1)	$P \rightarrow Q$	P
{2}	(2)	P	P
{1, 2}	(3)	Q	T, (1), (2) and I_{11} $[P, P \rightarrow Q \Rightarrow Q]$
{3}	(4)	$Q \rightarrow R$	P
{1, 2, 3}	(5)	R	T, (3), (4) and I_{11} $[R, Q \rightarrow R \Rightarrow R]$

Example: 2

Show that RVS follows logically from the premises $C \vee D$, $(C \vee D) \to \neg H$, $\neg H \to (A \wedge \neg B)$ and $(A \wedge \neg B) \to (R \vee S)$. [MCA MJ 2006].

Premise	Step	Derivation	Reason.
{1}	(1)	$(C \vee D) \to \neg H$	P
{2}	(2)	$\neg H \to (A \wedge \neg B)$	P
{1, 2}	(3)	$(C \vee D) \to (A \wedge \neg B)$	T, (1), (2) and I_{13}
{4}	(4)	$(A \wedge \neg B) \to (R \vee S)$	P
{1, 2, 4}	(5)	$(C \vee D) \to (R \vee S)$	T, (3), (4) and I_{13}
{6}	(6)	$(C \vee D)$	P
{1, 2, 4, 6}	(7)	$(R \vee S)$	T, (5), (6) and I_{11}

Example: 3

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

Solu:

{1}	(1)	$P \vee Q$	P
{1}	(2)	$\neg P \to Q$	T, (1), E, and E_{16} $P \to Q \Leftrightarrow \neg P \vee Q$ and $\neg\neg P \Leftrightarrow P$
{3}	(3)	$Q \to S$	P
{1, 3}	(4)	$\neg P \to S$	T, (2), (3), $(P \to Q), (Q \to R) \Rightarrow P \to R$
{5}	(5)	$\neg S \to P$	T, (4), $\neg(P \to Q) \Leftrightarrow \neg Q \to \neg P$; $\neg\neg P \Leftrightarrow P$
{6}	(6)	$P \to R$	P
{1, 3, 6}	(7)	$\neg S \to R$	T, (5), (6), $P \to Q, Q \to R \Rightarrow P \to R$
{1, 3, 6}	(8)	$S \vee R$	T, (7), $P \to R \Leftrightarrow \neg P \vee Q$ $\neg\neg P \Leftrightarrow P$

Example: 4

Show that $R \wedge (P \vee Q)$ is a valid conclusion from the premises $P \vee Q$, $Q \rightarrow R$, $P \rightarrow M$ and $\neg M$

Solu:

	Step	Derivation	Reason.
{1}	(1)	$P \rightarrow M$	P
{2}	(2)	$\neg M$	P
{1, 2}	(3)	$\neg P$	T, (1), (2) and $\neg Q, P \rightarrow Q \Rightarrow \neg P$
{4}	(4)	$P \vee Q$	P
{1, 2, 4}	(5)	Q	T, (3), (4) and $\neg P, P \vee Q \Rightarrow Q$
{6}	(6)	$Q \rightarrow R$	P
{1, 2, 4, 6}	(7)	R	T, (5), (6) and $Q, Q \rightarrow R \Rightarrow R$
{1, 2, 4, 6}	(8)	$R \wedge (P \vee Q)$	T, (4), (7) and $P, Q \Rightarrow P \wedge Q$

Example: 5

Show that $\neg Q, P \rightarrow Q \Rightarrow \neg P$

Solu:

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

Example: 6

Show that $R \rightarrow S$ can be derived from the premises $P \rightarrow (Q \rightarrow S)$, $\neg R$, $V P$ and Q. [AU NVD 2005]

Solu:

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

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

Consistency of Premises and Indirect method of proof.

Defn:

A set of formulas $H_1, H_2 \ldots H_m$ 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 $H_1, H_2 \ldots H_m$.

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

In other way, a set of formulas $H_1, H_2, \ldots H_m$ is inconsistent if their conjunction implies a contradiction, that is. $H_1 \wedge H_2 \wedge \ldots \wedge H_m \Rightarrow R \wedge \neg R$ where R is any formula. Note that $R \wedge \neg R$ is a contradiction, and it is necessary and sufficient for the implication that $H_1 \wedge H_2 \wedge \ldots \wedge H_m$ be a contradiction.

In direct method of proof:

The notion of inconsistency is used in a procedure called proof by contradiction or reduction and absurdum or indirect method of proof.

The technique of indirect method of proof runs as follows:

1. Introduce the negation of the desired conclusion as a new premise.
2. From the new premise, together with the given premises, derive a contradiction.
3. Assert the desired conclusion as a logical inference from the premises.

Example: 1

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

Soln:

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

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

Example: 2.

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, ~~enter~~ contract is valid and the bank will loan him money.

Soln

We indicate the given statements as follows:

P: The contract is valid

Q: John is liable for penalty

R: Bank will ~~lend~~ loan him money.

S: He will go bankrupt.

Then the given premises are.

$P \to Q$, $Q \to S$, $R \to \neg S$, $P \wedge R$.

{1}	(1)	$P \to Q$	P
{2}	(2)	$Q \to S$	P
{1,2}	(3)	$P \to S$	T, (1), (2) and $P \to Q, Q \to S \Rightarrow P \to S$
{4}	(4)	$P \wedge R$	P
{4}	(5)	P	T, (4) $P \wedge Q \Rightarrow P$
{4}	(6)	R	T, (4)
{1,2,4}	(7)	S	T, (3), (5), P, $P \to S \Rightarrow S$
{8}	(8)	$R \to \neg S$	P
{4,8}	(9)	$\neg S$	T, (6), (8)
{1,2,4,8}	(10)	$S \wedge \neg S$	T, (7), (9); contradiction.

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

Example:3

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.

[AU AM 2004]

Solu:

P : Jack misses many classes

Q : Jack fails high school.

R : Jack reads a lot of books.

S : Jack is uneducated.

The premises are ~~S, R~~ $P \to Q$, $Q \to S$, $R \to \neg S$ and $P \wedge R$.

{1}	(1)	$P \to Q$	P
{2}	(2)	$Q \to S$	P
{1,2}	(3)	$P \to S$	T, (1), (2) and $P \to Q, Q \to S \Rightarrow P \to S$
{4}	(4)	$R \to \neg S$	P
{4}	(5)	$S \to \neg R$	T, (4), $P \to Q \Rightarrow \neg Q \to \neg P$
{1,2,4}	(6)	$P \to \neg R$	T, (3), (5), $P \to Q, Q \to R \Rightarrow P \to R$.
{1,2,4}	(7)	$\neg P \vee \neg R$	T, (6) and $P \to Q \Rightarrow \neg P \vee Q$
{1,2,4}	(8)	$\neg (P \wedge R)$	T, (7), Demorgan's Law.
{9}	(9)	$P \wedge R$	P
{1,2,4,9}	(10)	$\Leftarrow (P \wedge R) \wedge \neg (P \wedge R)$	T, (8), (9), $P, Q \Rightarrow P \wedge Q$

Example: 4

Using indirect method of proof, derive $P \to \neg S$ from $P \to Q \vee R$, $Q \to \neg P$, $S \to \neg R$, P.

Solu: The desired result is $P \to \neg S$. Its negation is $P \wedge S$. Since $P \wedge S \leftrightarrow \neg(\neg P \vee \neg S) \leftrightarrow \neg(P \to \neg S)$ is a tautology from the law of negation for implication. We include $P \wedge S$ as an additional premise.

{1}	(1)	$P \to (Q \vee R)$	P
{2}	(2)	P	P
{1,2}	(3)	$Q \vee R$	T, (1), (2), P, $P \to Q \Rightarrow Q$
{4}	(4)	$S \to \neg R$	P
{5}	(5)	$P \wedge S$	P
{5}	(6)	S	T, (5)
{4,5}	(7)	$\neg R$	T, (4), (6) and P, $P \to Q \Rightarrow Q$
{1,2,4,5}	(8)	Q	T, (3), (7), $\neg P$, $P \vee Q \Rightarrow Q$
{9}	(9)	$Q \to \neg P$	P
{1,2,4,5,9}	(10)	$\neg P$	T, (8), (9), P, $P \to Q \Rightarrow Q$
{1,2,4,5,9}	(11)	$P \wedge \neg P$	T, (2), (10), Contradiction.

The additional premise $P \wedge S$ and the given premises together lead to a contradiction. So $\neg(P \wedge S)$ is derivable from $P \to Q \vee R$, $Q \to \neg P$, $S \to \neg R$, P.

Unit-I

The Predicate Calculus:

The predicate calculus deals with the study of predicates.

Example:

"Ram is a boy"

In the above statement, "is a boy" is the predicate and the name "Ram" is the subject.

If we denote the predicate "is a boy" by B and subject "Ram" by 'r', then the statement "Ram is a boy" can be represented as B(r).

Note:

Always we denote predicates by capital letters and the subjects by small letters.

Example:

"Sam is poor and Ram is intelligent."

The statement "Sam is poor" can be represented by P(s) and "Ram is intelligent" can be represented by I(r).

∴ The given statement canbe symbolized as $P(s) \wedge I(r)$.

Defn:

* If there is only one name of object associated with a predicate then it is known as 1-place predicate.

Ex:- Pavithra is rich.

* If there are two names of objects associated with a predicate then it is known as 2-place predicate.

Ex. Renuka is shorter than Manjula.

* If there are three names of objects associated with a predicate then it is known as 3-place predicate.

Ex: Mr. X sits between Mr. Y and Mr. Z.

Generally,

An n-place predicate is a predicate requiring n-names of objects where $n>0$. It is denoted by $P(a_1, a_2, \ldots a_n)$ where $a_1, a_2 \ldots a_n$ are the names of objects associated with predicate P.

Scanned by TapScanner

Defn:
A simple statement function of one variable is defined to be an expression consisting of a predicate symbol and an individual variable.

Ex. $M(x)$: x is mortal.

Note:
A statement function becomes a statement when the variable is replaced by the name of any object.

Defn:
Compound statement function is obtained by combining one or more simple statement functions using logical connective.

Ex: Let $M(x)$: x is a man and $H(x)$: x is a mortal be the 2-simple statement functions. Then we can form compound statement functions as

(i) $M(x) \wedge H(x)$ (ii) $M(x) \vee H(x)$ (iii) $M(x) \rightarrow H(x)$ (iv) $\neg H(x)$ (v) $M(x) \leftrightarrow \neg H(x)$

Defn:
A statement function of 2 variables is an expression consisting of a predicate symbol and 2 individual variables.

Ex: $G(x,y)$: x is taller than y.

Quantifiers:

Quantifier is one which is used to quantify the nature of variables.

There are 2 important quantifiers which are "for all" and "for some" where "some" means "atleast one".

Defn:
The quantifier "for all x" is called the universal quantifier. It is denoted by the symbol "$(\forall x$ or $(x))$". The universal quantifier is equivalent to each of the following phrases.

1. For all x
2. For every x
3. For each x
4. Everything x is such that
5. Each thing x is such that.

Ex: "Every apple is red." This statement can be restated as follows:
For all x, if (x is an apple $A(x)$) then (x is red $R(x)$)
(ie) $(\forall x)(A(x) \rightarrow R(x))$ (Symbolic form).

Scanned by TapScanner

Defn:

The quantifier for "some x" is called the existential quantifier. It is denoted by the symbol "$(\exists x)$". The existential quantifier is also equivalent to each of the following phrases.

1. For some x
2. Some x such that
3. There exists an x such that
4. There is an x such that
5. There is atleast one x such that

Example: 1

"Some men are clever"

The above statement can be restated as,

"there is an x such that x is a man and x is clever."

(i.e) $(\exists x)(M(x) \wedge C(x))$ where $M(x)$: x is a man.
$C(x)$: x is clever.

Example: 2

Given $M(x)$: x is a mammal; $W(x)$: x is warm blooded.
Translate into formula: Every mammal is warm blooded.

Soln:

The given statement, "Every mammal is warm blooded" can be restated as, "For all x, if x is a mammal then x is warm blooded".

(i.e) $(\forall x)(M(x) \rightarrow W(x))$. [Symbolic form].

Example: 3

Given $R(x)$: x is a road and $D(x)$: x lead to Denmark.
Symbolize the following statement: It is not true that all roads lead to Denmark.

Soln:

Consider, "All roads lead to Denmark". This can be rephrased as "For all x, if x is a road then x leads to Denmark".

(i.e) $(\forall x)(R(x) \rightarrow D(x))$

(i.e) $(\forall x)(\neg R(x) \vee D(x))$ [$\because P \rightarrow Q \Leftrightarrow \neg P \vee Q$].

Now, the given statement (Symbolic form) can be rephrased as,
"It is false that, for all x, if x is a road then x leads to Denmark"

Scanned by TapScanner

Its symbolic form is

$$\neg((\forall x)(\neg R(x) \vee D(x)))$$

(ie) $\neg\{(\forall x)\neg(\neg R(x) \vee D(x))$

(ie) $(\exists x)(\neg\neg R(x) \wedge \neg D(x))$

(ie) $(\exists x)(R(x) \wedge \neg D(x))$.

Example: 4

Give the symbolic form of the statement, "Every parrot is ugly".

Soln: Given, "Every parrot is ugly"

Now, $P(x)$: x is a parrot

$U(x)$: x is ugly

$\therefore (x)(P(x) \rightarrow U(x))$.

Defn:

The n-place predicate along with n in individual variables is called an n-place predicate formula.

For example, $P(x_1, x_2, \ldots x_n)$ denotes an n-place predicate formula in which the letter P is an n-place predicate and $x_1, x_2, \ldots x_n$ are individual variables.

Ex: $P(x,y)$, $R(x)$, $Q(x,y,z)$ are all predicate formulas.

Note: Predicate formula is known as atomic formula.

Defn:

* The variable is said to be bound if it is concerned with either universal $(\forall x)$ or existential $(\exists x)$ quantifier.
* The scope of the quantifier is the formulae immediately following the quantifier.
* The variable which is not concerned with any quantifier is called free variable.

Example:

1. $(\forall x)[P(x,y)]$.

In this formula, x is said to be bound and y is said to be free and the scope of the quantifier is $P(x,y)$.

Scanned by TapScanner

Defn:
Variables which are quantified stands for only those objects which are members of a particular set or class. Such a set is called the Universe of discourse or domain or simply universe.

The universe may be, the class of human beings, or numbers or some other objects. The truth value of a statement depends upon the universe.

Example: 1
Use quantifiers to express the statement "Every Computer Science student needs a course in Discrete Mathematics".

Solu:
Let the universe of discourse be the set of all Computer Science students.

Let $P(x)$: x needs a course in Discrete Mathematics.

The given statement can be reframed as,

"For all x, x needs a course in Discrete Mathematics"

(ie) $(\forall x)\, P(x)$ – Symbolic form.

Example: 2
Let $P(x)$: $x < 32$ and $Q(x)$: x is a multiple of 10. with universe of discourse as all +ve integers. Find the truth value of $(\exists x)(P(x) \to Q(x))$.

Solu:
Given $P(x)$: $x < 32$; $Q(x)$: x is a multiple of 10.

Universe of discourse: $U = \{1, 2, 3, \ldots\}$

To find: the truth value.

Now, 20 is an element in U.

$\therefore$ $P(20)$: $20 < 32$ is true.

$Q(20)$: 20 is a multiple of 10 which is true.

$\therefore$ $P(20) \to Q(20)$ is true.

(ie) There exists atleast one $x = 20$, $P(x) \to Q(x)$ is true.

Hence $(\exists x)(P(x) \to Q(x))$ is true.

Scanned by TapScanner

The theory of Inference for Predicate Calculus:

Example: 1

Prove that $(\exists x)(P(x) \wedge Q(x)) \Rightarrow (\exists x) P(x) \wedge (\exists x) Q(x)$

Sol:

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

Example: 2

Show that $(x)(P(x) \vee Q(x)) \Rightarrow (x) P(x) \vee (\exists x) Q(x)$.

Sol: We shall use the method of contrapositive.

{1}	1.	$\neg[(x) P(x) \vee (\exists x) Q(x)]$	Assumed premise – Rule P
{1}	2.	$(\exists x) \neg P(x) \wedge (x) \neg Q(x)$	Rule-T (Demorgan's law)
{1}	3.	$(\exists x) \neg P(x)$	Rule-T ($P \wedge Q \Rightarrow P$)
{1}	4.	$(x) \neg Q(x)$	Rule-T ($P \wedge Q \Rightarrow Q$)
{1}	5.	$\neg P(y)$	Rule ES
{1}	6.	$\neg Q(y)$	Rule US
{1}	7.	$\neg P(y) \wedge \neg Q(y)$	Rule T ($P, Q \Rightarrow P \wedge Q$)
{1}	8.	$\neg(P(y) \vee Q(y))$	Rule T (Demorgan's law)
{1}	9.	$(\exists x) \neg(P(x) \vee Q(x))$	Rule EG
{1}	10	$\neg[(x) P(x) \vee Q(x)]$	Rule T (Apply $\neg$).

Hence we have,

$$\neg[(x) P(x) \vee (\exists x) Q(x)] \Rightarrow \neg[(x) P(x) \vee Q(x)]$$

Therefore, by method of contrapositive, we have

$$(x)(P(x) \vee Q(x)) \Rightarrow (x) P(x) \vee (\exists x) Q(x).$$

Scanned by TapScanner

Example: 3

Use CP rule and obtain the following implication
$(x)(P(x) \to Q(x)),\ (x)(R(x) \to \neg Q(x)) \Rightarrow (x)(R(x) \to \neg P(x))$.

Soln:

1.	$(x)(P(x) \to Q(x))$	Rule P
2.	$P(y) \to Q(y)$	Rule US
3.	$(x)(R(x) \to \neg Q(x))$	Rule P
4.	$R(y) \to \neg Q(y)$	Rule US
5.	$Q(y) \to \neg R(y)$	Rule T (Taking $\neg$ in 4.)
6.	$P(y) \to \neg R(y)$	Rule T ($P \to Q, Q \to R \Rightarrow P \to R$)
7.	$R(y) \to \neg P(y)$	Rule T (Taking $\neg$ in 6.)
8.	$(x)(R(x) \to \neg P(x))$	Rule UG

Example: 4

Show that: $(x)(P(x) \to Q(x)) \Rightarrow (x)P(x) \to (x)Q(x)$.

Soln:

We prove this problem by indirect method (method of contrapositive).

{1}	1.	$\neg((x)P(x) \to (x)Q(x))$	Assumed premises
{1}	2.	$(x)P(x) \wedge \neg((x)Q(x))$	Rule T ($\neg(P \to Q) \Rightarrow P \wedge \neg Q$)
{1}	3.	$(x)P(x)$	Rule T ($P \wedge Q \Rightarrow P$)
{1}	4.	$\neg((x)Q(x))$	Rule T ($P \wedge Q \Rightarrow Q$)
{1}	5.	$(\exists x)\neg Q(x)$	Rule -T (4.)
{1}	6.	$P(y)$	Rule US (3.)
{1}	7.	$\neg Q(y)$	Rule ES (5.)
{1}	8.	$P(y) \wedge \neg Q(y)$	Rule T, ($P, Q \Rightarrow P \wedge Q$) (6. & 7.)
{1}	9.	$\neg(P(y) \to Q(y))$	Rule T, ($P \wedge \neg Q \Leftrightarrow \neg(P \to Q)$) (8.)
{1}	10.	$(\exists x)\neg(P(x) \to Q(x))$	Rule EG
{1}	11.	$\neg((x)(P(x) \to Q(x)))$	Rule T (Taking $\neg$ in 10.)

∴ By the method of contrapositive, we have
$(x)(P(x) \to Q(x)) \Rightarrow (x)P(x) \to (x)Q(x)$ //.

Scanned by TapScanner

Rules of inference for Quantified statements

Rules in Quantifiers

Rule US: (Universal Specification)

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

If a statement of the form $(\forall x)(A(x))$ is assumed to be true, then the universal quantifier can be dropped to obtain $A(y)$ is true for any arbitrary object 'y' in the universe.

Rule ES: [Existential Specification]

From $(\exists x)\,A(x)$ one can conclude $A(y)$ provided that y is not free in any given premise and also not free in any prior step of the derivation. These requirements can easily be met by choosing a new variable each time ES is used.

Rule EG: [Existential Generalization]

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

If $A(x)$ is true for some element x in the universe, then $(\exists(y))\,A(y)$ is true.

Rule UG:

From $A(x)$ one can conclude $(y)\,A(y)$ provided that x is not free in any of the given premises and provided that if x is free in a prior step which resulted from use of ES, then no variables introduced by that use of ES appear free in $A(x)$.

Scanned by TapScanner

Example: 1

Show that $(x)\, H(x) \rightarrow M(x) \wedge H(s) \Rightarrow M(s)$. Not that this problem is a symbolic translation of a well-known argument known as the "Socrates argument" which is given by:

All men are mortal.
Socrates is a man.
Therefore Socrates is amortal.

If we denote $H(x)$: x is a man, $M(x)$: x is amortal, and s: Socrates, we can put the argument in the above form.

Solu:

$\{1\}$	(1)	$(x)\, H(x) \rightarrow M(x)$	P
$\{1\}$	(2)	$H(s) \rightarrow M(s)$	US, (1)
$\{3\}$	(3)	$H(s)$	P
$\{1,3\}$	(4)	$M(s)$	T, (2), (3), modus ponens

Note that in step2 first we remove the universal quantifier.

Example: 2.

Show that $(x)(P(x) \vee Q(x)) \Rightarrow (x)\, P(x) \vee (\exists x)\, Q(x)$ [AU N/D 2003]

Solu:

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)	$\neg((x) P(x) \vee (\exists x)\, Q(x))$	P (assumed
$\{1\}$	(2)	$\neg(x)\, P(x) \wedge \neg(\exists x)\, Q(x)$	T, (1), $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$
$\{1\}$	(3)	$\neg(x)\, P(x)$	T, (2), $P \wedge Q \Rightarrow P$
$\{1\}$	(4)	$(\exists x) \neg P(x)$	T, (3),
$\{1\}$	(5)	$\neg(\exists x)\, Q(x)$	T, (2), $P \wedge Q \Rightarrow Q$

Scanned by TapScanner

{1}	(6)	$\exists x \neg Q(x)$	T, (5)
{1}	(7)	$\neg P(y)$	ES, (4)
{1}	(8)	$\neg Q(y)$	US, (6)
{1}	(9)	$\neg P(y) \wedge \neg Q(y)$	T, (7), (8), $P, Q \Rightarrow P \wedge Q$
{1}	(10)	$\neg(P(y) \vee Q(y))$	T, (9), $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$.
{11}	(11)	$\forall x (P(x) \vee Q(x))$	P
{11}	(12)	$P(y) \vee Q(y)$	US, (11)
{1, 11}	(13)	$\neg(P(y) \vee Q(y)) \wedge (P(y) \vee Q(y))$	T, (10), (12), $P, Q \Rightarrow P \wedge Q$ Contradiction.

Example:3

Using CP or otherwise obtain the following implication.

$(\forall x)(P(x) \rightarrow Q(x)), (\forall x)(R(x) \rightarrow \neg Q(x)) \Rightarrow (\forall x)(R(x) \rightarrow \neg P(x))$

[AU MJ 2006]

Solu:

{1}	(1)	$(\forall x)(P(x) \rightarrow Q(x))$	P
{2}	(2)	$(\forall x)(R(x) \rightarrow \neg Q(x))$	P
{2}	(3)	$R(y) \rightarrow \neg Q(y)$	US, (2)
{4}	(4)	$R(y)$	P (assumed)
{2,4}	(5)	$\neg Q(y)$	T, (3), (4).
{1}	(6)	$P(y) \rightarrow Q(y)$	US, (1)
{1,2,4}	(7)	$\neg P(y)$	T, (5), (6)
{1,2,4}	(8)	$R(y) \rightarrow \neg P(y)$	CP, (4) (7)
{1,2}	(9)	$(\forall x)(R(x) \rightarrow \neg P(x))$	UG, (9).

Hence the argument is valid.

Scanned by TapScanner

Validity of verbal arguments. Unit – I

Example: 1.

Determine the validity of the following argument. If two sides of a triangle are equal, then opposite angles are equal.

Two sides of a triangle are not equal.

Therefore, the opposite angles are not equal.

Soln:

Let P : Two sides of a triangle ~~is~~ are equal.

Q : The two opposite angle are equal.

The premises can be represented as

$P \rightarrow Q$ and $\neg P$ and the conclusion as $\neg Q$.

If the argument is a valid one then

$((P \rightarrow Q) \wedge \neg P) \rightarrow \neg Q$ will be tautology.

Let us now construct the truth table for

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

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

From the truth table we can infer that, $(P \rightarrow Q) \wedge \neg P) \rightarrow \neg Q$ is not a tautology. Hence the argument is not valid.

Scanned by TapScanner

Example: 2

Show that the following sets of premises are inconsistent.

$P \to Q,\ P \to R,\ Q \to \neg R,\ P$ [AU MJ 2006]

Solu:

1.	$P \to Q$	P
2.	$Q \to \neg R$	P
3.	$P \to \neg R$	from ① & ②, T
4.	P	P
5.	$\neg R$	P
6.	$P \to R$	P
7.	$\neg P$	T, from ⑤ & 6.
8.	$P \wedge \neg P$	T

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

Example: 3

Show that the following implication by using indirect method

$(R \to \neg Q),\ RVS,\ S \to \neg Q,\ P \to Q \Rightarrow \neg P$ [AU. MJ 2006]

Solu: To use the indirect method, we will include $\neg\neg P \Leftrightarrow P$ as an additional premise and prove a contradiction.

1.	P	P
2.	$P \to Q$	P
3.	Q	T, (1), 2. and modus ponens.
4.	$R \to \neg Q$	P
5.	$S \to \neg Q$	P
6.	$(RVS) \to \neg Q$	T; 4, 5 and equivalence
7.	RVS	P
8.	$\neg Q$	T, 6, 7 and modus ponens
9.	$Q \wedge \neg Q$	T, 3, 8 and conjunction
10.	F	T, 9, and negation law (contradiction.

Scanned by TapScanner

Unit-II

Combinatorics

Mathematical Induction:

☆ Principle of Mathematical Induction:

Let P(n) be a statement or proposition involving for all positive integers n. Then we complete two steps.

Basis step: If P(1) is true.

Inductive step: If P(k+1) is true on the assumption that P(k) is true.

Example: 1 Prove by induction

$1+2+3+\cdots+n = \frac{n(n+1)}{2}$, $n \geq 1$.

Solu:

Let P(n) ; $1+2+3+\cdots+n = \frac{n(n+1)}{2}$, $n \geq 1$

Step: 1 To prove P(1) is true

For $n=1$, we have $1 = \frac{1(1+1)}{2}$

(i.e) $1 = 1$ So P(1) is true.

Step: 2 Assume that P(k) is true for any positive integer k

(i.e) $1+2+3+\cdots+k = \frac{k(k+1)}{2}$

Step: 3 To prove ; P(k+1) is true.

(i.e) To prove $P(k+1) = \frac{(k+1)(k+2)}{2}$

Now, $(1+2+\cdots+k)+k+1 = \frac{k(k+1)}{2}+k+1$

$$= \frac{k(k+1)+2(k+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

$$= \frac{(k+1)((k+1)+1)}{2}$$

which is $P(k+1)$.

(i.e) $P(k+1)$ is true whether $P(k)$ is true.

By the principle of mathematical induction $P(n)$ is true for all positive integer n.

Example: 2

8m Show that $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$

Soln:

Let $P(n) : \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$.

Step: 1. To prove $P(1)$ is true

(i.e) $\frac{1}{1\cdot 2} = \frac{1}{1+1} \Rightarrow \frac{1}{2} = \frac{1}{2}$.

Hence $P(1)$ is true.

Step: 2 Assume that $P(k)$ is true.

(i.e) $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{k(k+1)} = \frac{k}{k+1}$

Step: 3 To prove $P(k+1)$ is true.

(i.e) $P(k+1) = \frac{k+1}{(k+1)+1} = \frac{k+1}{k+2}$.

Now,

$$\left[\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{k(k+1)}\right] + \frac{1}{(k+1)(k+2)} = \frac{k}{k+1} + \left[\frac{1}{(k+1)(k+2)}\right]$$

$$= \frac{k(k+2)+1}{(k+1)(k+2)}$$

$$= \frac{k^2+2k+1}{(k+1)(k+2)}$$

$$= \frac{(k+1)^2}{(k+1)(k+2)} = \frac{k+1}{k+2}$$

which $P(k+1)$

That is $P(k+1)$ is true whenever $P(k)$ is true.

By the principle of mathematical induction $P(n)$ is true.

Example: 3

Prove the formula for sum of first n cubes using the mathematical induction. $S_n = \left[\frac{n(n+1)}{2}\right]^2$.

Soln:

Let $P(n): 1^3+2^3+\cdots+n^3 = \left(\frac{n(n+1)}{2}\right)^2$.

Step:1 To prove $P(1)$ is true

$$1^3 = \left[\frac{1(1+1)}{2}\right] \Rightarrow 1 = 1.$$

Hence $P(1)$ is true.

Step:2 Assume that $P(k)$ is true.

(i.e) $1^3+2^3+\cdots+k^3 = \left(\frac{k(k+1)}{2}\right)^2$

Step:3 To prove: $P(k+1)$ is true.

(i.e) To prove $P(k+1) = \left[\frac{(k+1)(k+2)}{2}\right]^2$

Now $\left[1^3+2^3+\cdots+k^3\right]+(k+1)^3 = \left(\frac{k(k+1)}{2}\right)^2+(k+1)^3$

$$= \frac{k^2(k+1)^2}{4}+(k+1)^3 = \frac{k^2(k+1)^2+(k+1)^3\cdot 4}{4}$$

$$= \frac{(k+1)^2}{4}\left(k^2+4(k+1)\right) = \frac{(k+1)^2(k+2)^2}{4}$$

$$= \left[\frac{(k+1)(k+2)}{2}\right]^2 = P(k+1)$$

Therefore $P(k+1)$ is true whenever $P(k)$ is true.

Example: 4

2m Use mathematical induction to prove that $n^3 - n$ is divisible by 3 whether n is a positive integer.

Solu: ~~To prove~~ Let $P(n)$ & $(n^3 - n)$ is divisible by 3.

Step: 1 To prove $P(1)$ is true.

$1 - 1 = 0$ is divisible by 3.

Hence $P(1)$ is true.

Step: 2 Assume that $P(k)$ is true.

(i.e) $(k^3 - k)$ is divisible by 3.

Step: 3 To prove $P(k+1)$ is true.

(i.e) To prove $(k+1)^3 - k+1)$ is divisible by 3.

Now, $(k+1)^3 - k+1 = (k^3 + 3k^2 + 3k + 1) - k + 1$

$= (k^3 - k) + 3(k^2 + k)$

which is divisible by 3

Hence $P(k+1)$ is true

This completes the inductive step.

—x—x—

Strong Induction and Well-ordering

* Principle of strong induction:

It is sometimes convenient to replace the induction hypothesis P(k) by the stronger assumption P(1), P(2), P(3), ... P(k) are true.

The resulting principle known as the principle of strong mathematical induction.

Step: 1 Inductive base: To prove P(1) is true.

Step: 2 Strong inductive hypothesis: Assume that P(n) is true for all integers $1 \le n \le k$

Step: 3 Inductive Step: To prove that P(k+1) is true on basis of the strong inductive hypothesis.

Example: 1

Prove by mathematical induction that $6^{n+2} + 7^{2n+1}$ is divisible by 43 for each positive integer

Solu: Let $P(n) : 6^{n+2} + 7^{2n+1}$ is divisible by 43

Step: 1 To prove P(1) is true.

$6^{1+2} + 7^{2+1} = 6^3 + 7^3 = 216 + 343 = 559 = 43 \times 13$

which is divisible by 43. $\therefore$ P(1) is true.

Step: 2 Assume that P(k) is true

(i.e) $6^{k+2} + 7^{2k+1} = (43)(m)$ for some integer m.

Step: 3 To prove P(k+1) is true.

Now $6^{(k+1)+2} + 7^{2(k+1)+1} = 6^{k+3} + 7^{2k+3} = 6(6^{k+2}) + 7^{(2k+1)} \cdot 7$

$= 6(6^{k+2}) + (49)\,7^{2k+1} = 6(6^{k+2}) + (43+6)\,7^{2k+1}$

$= 6(6^{k+2} + 7^{2k+1}) + (43)7^{2k+1}$

$= 6(43)(m) + (43)\,7^{2k+1}$

$= 43\left[6m + 7^{2k+1}\right]$

which is divisible by 43.

Hence P(k+1) is true whenever P(k) is true.

By the principle of mathematical induction P(n) is true for all positive integer n.

Example: 2

Any positive integer $n \geq 2$ is either a prime or a product of primes. To prove this we use the principle of strong mathematical induction.

Solu: Let P(n) : $n \geq 2$ is either a prime or a product of primes.

Step: 1 To prove P(2) is true.

$2 = 2$ is a prime. Hence P(2) is true.

Step: 2 Assume that the statement is ~~either~~ true for $2 \leq n \leq k$

Step: 3 To prove P(k+1) is true.

For integer k+1, if k+1 is a prime, the statement is true. If k+1 is not a prime, then k+1 can be written as pq, for some $2 \leq p \leq k$ and $2 \leq q \leq k$.

According to the induction hypothesis, p is either a prime or a product of prime. Also q is either a prime or a product of prime. Consequently, pq is a product of prime.

Example: 3

Which amount of money can be found using just two dollar bills and five-dollar bills? Prove your answer using strong induction.

Solu:

We can form all amounts except $1 and $3

Let P(n): We can form n dollars using just 2 dollar and 5 dollar bills.

(i.e) P(n) is true for all $n \geq 5$ (It is clear that $1 and $3 cannot be formed and that $2 and $4 can be formed)

Step: 1 $5 = 5$ and $6 = 2+2+2$.

Step: 2 Assume the inductive hypothesis, that P(j) is true for all k with $5 \leq j \leq k$, where k is an arbitrary integer greater than or equal to 6.

Step: 3 To prove P(k+1) is true.

$k-1 \geq 5$, we know that P(k-1) is true, ~~that~~ :

that is that we can form k+1 dollars.

Add another 2-dollar bill and we have formed k+1 dollars.

— × — × —

★ The well-ordering property.

Every non-empty set of non-negative integers has a least element. The well-ordering property can often be used directly in proofs.

Example: 4.

Show that strong induction is a valid method of proof by showing that it follows from the well-ordering property.

Soln: Let P(n): Given statement.

Assume that the well-ordering property holds.

Suppose that P(1) is true and that the conditional statement $[P(1) \wedge P(2) \wedge \dots \rightarrow P(n)] \rightarrow P(n+1)$ is true for every positive integer n.

Let S be the set of positive integers n for which P(n) is false.

We will show $S = \phi$

Assume that $S \neq \phi$.

Then by the well-ordering property there is a least integer m in S.

We know that m cannot be 1 because P(1) is true

If $n = m$ is the least integer such that P(n) is false,

P(1), P(2), ..., P(m-1) are true, and $m - 1 \geq 1$.

Because $[P(1) \wedge P(2) \wedge \dots \wedge P(m-1)] \rightarrow P(m)$ is true it follows that P(m) must also be true, which is a contradiction.

Hence $S = \phi$.

— x — x —

The Basics of Counting

★ Basing Counting Principles

The two basic counting principles are

1. The product rule
2. The sum rule.

1. The product rule

If one job can be done in m ways and following this another job can be done in n ways then the total number of ways in which both the jobs can be done in the stated order is mn.

2. The Sum rule

If one job can be done in m ways and another job can be done in n ways and if there is no way common to both jobs then the total number of ways in which either of the two jobs can be done is equal to m+n.

Example: 1.

How many different bit strings of length seven are there?

Solu:

Each of the seven bits can be chosen in two ways because each bit is either 0 or 1.

∴ The product rule shows there are a total of $2^7 = 128$ different bit strings of length seven.

Example: 2

How many different 8-bit strings are there that end with 0111?

Solu:

A 8 bit strings that end with 0111 can be constructed in 4 steps.

By selecting 1st bit, 2nd bit, 3rd bit and 4th bit and each bit can be selected in 2 ways.

∴ The total number of 8 bit strings that end with 0111 is equal to $2 \cdot 2 \cdot 2 \cdot 2 = 2^4 = 16$.

Example:

How many one-to-one functions are there from a set with m elements to one with n elements?

Solu:

Case(i): When $m > n$ there are no one-to-one functions from a set with m-elements to set with n-elements.

Case(ii): When $m \leq n$

Suppose the elements in the domain are $a_1, a_2 \ldots a_m$ There are n-ways to choose the value of the function at a_1.

The value of the function at a_2 can be picked in $n-1$ ways.

In general, the value of the function at a_k can be chosen in $n-k+1$ ways.

By the product rule, there are $n(n-1)(n-2)\ldots(n-m+1)$ one to one functions from a set with m-elements to one with n elements.

---

* Inclusion - Exclusion Principle in General

Let $P_1, P_2, \ldots P_n$ are finite sets.

Then $|P_1 \cup P_2 \cup \ldots \cup P_n| = \sum_{1 \le i \le n} |P_i| - \sum_{1 \le i \le j \le n} |P_i \cap P_j| +$

$$\sum_{1 \le i \le j \le k \le n} |P_i \cap P_j \cap P_k| - \ldots + (-1)^{n-1} |P_1 \cap P_2 \cap \ldots \cap P_n|$$

Example:

Am 40 computer programmers interviewed for a job. 25 knew JAVA, 28 knew ORACLE, and 7 knew neither language. How many knew both languages?

Solu:

Now $|J| = 25$ [$\because J \to$ JAVA]

$|O| = 28$ [$\because O \to$ ORACLE].

$|J \cup O| = 40 - 7$

$= 33$

Computer programmers who knew both language are

$|J \cap O| = 25 + 28 - 33 = 20.$

The Pigeonhole Principle.

Theorem: The pigeon hole principle.

If k is a positive integer and k+1 or more objects are placed into k boxes, then there is atleast one box containing two or more of the objects.

Corollary:

A function f from a set with k+1 or more elements to a set with k elements is not one-to-one.

Theorem:

If n-pigeons are assigned to m pigeonholes, and $m < n$, then atleast one pigeonhole contains two or more pigeons.

Theorem: The generalization / extension of the pigeonhole principle

If k pigeons are assigned to n pigeonholes, then one of the pigeonholes must contain atleast $\left\lceil \frac{k-1}{n} \right\rceil + 1$ pigeons.

Theorem:

If n objects are place into k boxes, then there is atleast one box containing atleast $\lceil n/k \rceil$ objects.

Example: 1.

Give two examples based on pigeonhole principle.

Solu:

1. Among any group of 367 people, there must be atleast two with the same birth day, because there are only 366 maximum possible birth days.

2. In any group of 27 English words, there must be atleast two that starts with the same letter, since there are 26 letters in English alphabet.

Example:
A bag contains 12 pairs of socks (each pair is in different color). If a person draws the socks one by one at random, determine atmost how many draws are required to get atleast one pair of matched socks.

Sol:
Let n denote the number of the draw. For $n \leq 12$, it is possible that socks drawn are of different colors since there are 12 colors.

For $n = 13$, all socks cannot have different colors. atleast two must have the same color. Here 13 as the number of pigeons and 12 colors as 12 pigeonholes. Thus, atmost 13 draws are required to have atleast one pair of socks of the same color.

Example:
Let $n_1, n_2, \ldots n_t$ be possible integers. Show that if $n_1 + n_2 + \ldots + n_t - t + 1$ objects are placed in t boxes, then for some i, $i = 1, 2, \ldots t$, the i^{th} box contains atleast n_i objects.

Sol:
Assume that the conclusion part of the given statement is false. Here $n_1, n_2, \ldots$ are pigeons t boxes are

pigeonholes, Then every hole contains n_j or less number of pigeons, $j=1,2,\ldots n$. Then the total number of pigeons would be less than or equal to.

$$(n_1-1)+(n_2-1)+\cdots+(n_t-1) = n_1+n_2+\cdots+n_t-t$$
$$= m-1$$

This is a contradiction. Since the number of pigeons is equal to m. Hence the assumption made is wrong, and the given statement is true.

Example:

Seven members of a family have total Rs. 2886 in their pockets. Show that atleast one of them must have atleast Rs. 416 in his pocket.

Solu: Let us assume.

members $\longrightarrow$ pigeonholes

Rupees $\longrightarrow$ pigeons.

No. 2886 pigeons are to be assigned to 7 pigeonholes.

Using the extended pigeonhole principle.

(i.e) $\frac{k-1}{n}+1$ where $k=2886$, $n=7$.

$\therefore \frac{2886-1}{7}+1 = 416$

Hence there are 416 rupees in one member's pocket.

Permutations and Combinations.

* Permutation

A permutation of a set of distinct objects is an ordered arrangement of those objects.

Note: Permutation means selection and arrangement of factors.

Notation: ${}^nP_r$ (or) $P(n,r)$ (or) $P_{n,r}$ (or) P_n^r (or) $(n)_r$

* r-Permutation.

An r-permutation of n (distinct) elements $x_1, x_2, \ldots, x_n$ is an ordering of an r-element subset $\{x_1, x_2, \ldots x_n\}$. The number of r-permutations of a set of n-distinct elements is denoted by $P(n,r)$

Results:

1. ${}^nP_r = \frac{n!}{(n-r)!}$
2. $P(n,n) = n!$
3. $P(n,r) = 0$ if $r > n$
4. $P(n,0) = 1$ whenever n is a non negative integer

since there is exactly one way to order zero elements.

Combinations:

A combination is a selection of objects without regard to order. (or) A combination is an unordered collection of distinct objects.

Note:

1. The number of r-combinations of n distinct objects is denoted by ${}^nC_r$ (or) $C_{(n,r)}$ (or) $\binom{n}{r}$.

2. ${}^nC_n = {}^nC_0 = 1$

3. ${}^nC_r = {}^nC_{n-r}$ (or) $C(n, n-r) = C(n, r)$

4. $C(n,r) = \frac{P(n,r)}{r!} = \frac{n!}{r!\,(n-r)!}$

Example:

Find the value of these quantities (a) $P(6,3)$ (b) $P(8,1)$ (c) $P(8,8)$, (d) $C(5,3)$ (e) $C(8,0)$.

Solu: Formula. 1. $P(n,r) = \frac{n!}{(n-r)!}$ 2. $C(n,r) = \frac{n!}{(n-r)!\,r!}$

(a) $P(6,3) = \frac{6!}{(6-3)!} = \frac{6!}{3!} = 120$

(b) $P(8,1) = \frac{8!}{(8-1)!} = \frac{8!}{7!} = 8$

(c) $P(8,8) = \frac{8!}{(8-8)!} = \frac{8!}{0!} = 40,320$

(d) $C(5,3) = \frac{5!}{(5-3)!\,3!} = \frac{5!}{2!\,3!} = 10$

(e) $C(8,0) = \frac{8!}{(8-0)!\,0!} = \frac{8!}{8!} = 1$.

Example: 2

Determine the value of n if $^{20}C_{n+2} = {}^{20}C_{2n-1}$

Solu: Given $^{20}C_{n+2} = {}^{20}C_{2n-1}$

Formula $^nC_x = {}^nC_y \Rightarrow n = x+y$ or $x = y$.

$\therefore n+2 = 2n-1$

$\Rightarrow 3 = n$ (i.e) $n = 3$.

Example: 3

How many bit strings of length 10 contain

(a) exactly four 1's (b) atmost four 1's (c) atleast four 1's (d) an equal number of 0's and 1's.?

Solu:

(a) A bit string of length 10 can be considered to have 10 positions, should be filled with four 1's and six 0's.

$\therefore$ Number of required bit strings $= \frac{10!}{4!\,6!} = 210$.

(b) $\therefore$ Required number of bit strings.

$$= \frac{10!}{0!10!} + \frac{10!}{1!\,9!} + \frac{10!}{2!\,8!} + \frac{10!}{3!\,7!} + \frac{10!}{4!\,6!} = 386$$

(c) $\therefore$ Required number of bit strings. ($\because$ Dec. total = 10)

$$= \frac{10!}{4!\,6!} + \frac{10!}{5!\,5!} + \frac{10!}{6!\,4!} + \frac{10!}{7!\,3!} + \frac{10!}{8!\,2!} + \frac{10!}{9!\,1!} + \frac{10!}{10!\,0!}$$

$= 848$.

(d) $\therefore$ Required number of bit strings $= \frac{10!}{5!\,5!} = 252$.

Example: 4

How many possibilities are there for the win, place and show (first, second and third) positions in a horse race with 12 horses if all orders of finish are possible?

Soln:

The number of ways to pick the three winners is the number of ordered selections of three elements from 12,

(i.e) $P(12,3) = (12)(11)(10) = 1320$.

Recurrence Relations:

Defn: Recurrence Relations (Some times called difference equation).

A recurrence relation for the sequence $\{a_n\}$ is an equation that shows a_n in terms of one or more of the previous terms of the sequence $a_0, a_1, \ldots, a_{n-1}$ for all integers n with $n \geq n_0$, where n_0 is a non-negative integer.

Note: A sequence is called a solution of a recurrence relation if its terms satisfy the recurrence relation.

Example:

The Fibonacci sequence is defined by the recurrence relation $a_r = a_{r-2} + a_{r-1}$, $r \geq 2$, with the initial conditions $a_0 = 1$ and $a_1 = 1$.

Example: 1.

Let $\{A_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-2} + a_{n-1}$ for $n = 2, 3, 4, 5, \ldots$ and suppose that $a_0 = 3$ and $a_1 = 5$. What are a_2 and a_3?

Soln:

Given $a_n = a_{n-2} + a_{n-1}$

$a_2 = a_0 + a_1 = 3 + 5 = 8$

$a_3 = a_1 + a_2 = 5 + 8 = 13$

Example: 2

Find the first five terms of the sequence defined by each of these recurrence relations and initial conditions. (a) $a_n = 6 \cdot a_{n-1}$, given $a_0 = 2$

(b) $a_n = a_{n-1} + 3\, a_{n-2}$, $a_0 = 1$, $a_1 = 2$

(c) $a_n = a_{n-1} + a_{n-3}$, $a_0 = 1$, $a_1 = 2$, $a_2 = 0$.

Soln:

(a) $a_n = 6a_{n-1}$, given $a_0 = 2$.

$a_1 = 6a_0 = 6(2) = 12$

$a_2 = 6a_1 = 6(12) = 72$

$a_3 = 6a_2 = 6(72) = 432$

$a_4 = 6a_3 = 6(432) = 2592$.

(b) $a_n = a_{n-1} + 3a_{n-2}$, given $a_0 = 1$, $a_1 = 2$

$a_2 = a_1 + 3a_0 = 2 + 3(1) = 5$

$a_3 = a_2 + 3a_1 = 5 + 3(2) = 11$

$a_4 = a_3 + 3a_2 = 11 + 3(5) = 26.$

(c) $a_n = a_{n-1} + a_{n-3}$, $a_0 = 1$, $a_1 = 2$, $a_2 = 0$

$a_3 = a_2 + a_0 = 2 + 1 = 3$

$a_4 = a_3 + a_1 = 3 + 2 = 5$

Example: 3

Is the sequence $\{a_n\}$ a solution of the recurrence relation $a_n = 8 = 8a_{n-1} - 16a_{n-2}$ if

(a) $a_n = 0$, (b) $a_n = 1$, (c) $a_n = n4^n$

Soln:

(a) $a_n = 0$, Yes.

$\Rightarrow a_{n-1} = 0 \Rightarrow a_{n-2} = 0$

$\therefore a_n = 8a_{n-1} - 16a_{n-2}$ is true.

(b) $a_n = 1$, NO.

$\Rightarrow a_{n-1} = 1, \Rightarrow a_{n-2} = 1$

$8a_{n-1} - 16a_{n-2} = 8(1) - 16(1) = -8 \neq 1$

(c) $a_n = n4^n$, Yes.

$\Rightarrow a_{n-1} = (n-1)4^{n-1}$

$\Rightarrow a_{n-2} = (n-2)4^{n-2}.$

$\therefore 8a_{n-1} - 16a_{n-2} = 8(n-1)4^{n-1} - 16(n-2)4^{n-2}$

$= 4^{n-1}\left[8(n-1) - 16(n-1)\frac{1}{4}\right]$

$$= 4^{n-1}\left[8(n-1) - 4(n-2)\right]$$

$$= 4^{n-1} \cdot 4\left[2(n-1) - (n-2)\right]$$

$$= 4^{n}\left[2n - 2 - n + 2\right]$$

$$= 4^{n} \cdot n = n4^{n}$$

$$= a_n.$$

Example: 4 (Rabbits and the Fibonacci Numbers)

A young pair of rabbits (one of each sex) is placed on an island. A pair of rabbits does not breed until they are 2 months old. After they are 2 months old, each pair of rabbits produces another pair each month. Find a recurrence relation for the number of pairs of rabbits on the island after n-months, assuming that no rabbits ever die.

Soln:

Let f_n the number of pairs of rabbits after n-months

Show that f_n, $n = 1, 2, 3, \ldots$ are the terms of Fibonacci sequence.

The rabbit population can be modeled using a recurrence relation.

At the end of the first month, the number of pairs of rabbits on the island is $f_1 = 1$.

Since this pair does not breeding during the second month, $f_2 = 1$ also.

To find the number of pairs after n months, add the number on the island the previous month, f_{n-1} and the number of newborn pairs, which equals f_{n-2}.

Since each newborn pair comes from a pair atleast 2 months old.

Consequently, the sequence $\{f_n\}$ satisfies the recurrence relation

$$f_n = f_{n-1} + f_{n-2}.$$

for $n \geq 3$ together with the initial conditions $f_1 = 1$ and $f_2 = 1$.

Since this recurrence relation and the initial condition ~~$f_1 = 1$ and $f_2 = 1$. Since~~ uniquely determine this sequence, the number of pairs of rabbits on the island after n - ~~nath~~ months is given by the nth Fiboracci number.

Solving Linear Recurrence Relations

Defn: Linear Recurrence Relation with constant co-efficient.

A linear recurrence relation with constant coefficient is of the form

$$C_0 a_n + C_1 a_{n-1} + C_2 a_{n-2} + \cdots + C_k a_{n-k} = f(n)$$

where C's are constant.

A linear homogeneous recurrence relation with constant co-efficients of degree K is of the form

$a_n = C_1 a_{n-1} + C_2 a_{n-2} + \cdots + C_k a_{n-k}$, where $C_1, C_2, \ldots C_k$ are real nos. and $C_k \neq 0$

Example: 1

Find an explicit formula for the Fibonacci numbers

Soln:

The sequence of Fibonacci numbers satisfies the recurrence relations $f_n = f_{n-1} + f_{n-2}$ $\longrightarrow$ ①

and satisfies the initial conditions $f_0 = 0$ and $f_1 = 1$.

① $\Rightarrow f_n - f_{n-1} - f_{n-2} = 0$ $\longrightarrow$ ②

Let $f_n = r^n$ be a solution of the given equ.

② $\Rightarrow r^n - r^{n-1} - r^{n-2} = 0$.

(i.e) $r^n\left[1 - \frac{1}{r} - \frac{1}{r^2}\right] = 0$

$\therefore$ The characteristic equ. is $r^2 - r - 1 = 0$.

$$\Rightarrow r = \frac{1 \pm \sqrt{(-1)^2 - 4(-1)}}{2}$$

$$= \frac{1 \pm \sqrt{1+4}}{2}$$

Let $r_1 = \frac{1+\sqrt{5}}{2}$, $r_2 = \frac{1-\sqrt{5}}{2}$

Now, $f_n = \alpha_1 (r_1)^n + \alpha_2 (r_2)^n$

$$= \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1 \mp \sqrt{5}}{2}\right)^n \longrightarrow ③$$

$$f_0 = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^0 + \alpha_2 \left(\frac{1 \mp \sqrt{5}}{2}\right)^0 = 0$$

$\Rightarrow \alpha_1 + \alpha_2 = 0$ $\longrightarrow$ ④

$f_1 = 1 \Rightarrow f_1 = \alpha_1\left(\frac{1+\sqrt{5}}{2}\right) + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right) = 1$

$(1+\sqrt{5})\alpha_1 + (1-\sqrt{5})\alpha_2 = 2. \longrightarrow (5)$

$(4) \times (1+\sqrt{5}) \Rightarrow (1+\sqrt{5})\alpha_1 + (1+\sqrt{5})\alpha_2 = 0 \longrightarrow (6)$

$(5) \times 1 \Rightarrow (1+\sqrt{5})\alpha_1 + (1-\sqrt{5})\alpha_2 = 2 \longrightarrow (7)$

$(6) - (7) \Rightarrow 2\sqrt{5}\alpha_2 = -2$

$\alpha_2 = \frac{-1}{\sqrt{5}}$

$(4) \Rightarrow \alpha_1 = \frac{1}{\sqrt{5}}$

$(5) \Rightarrow f_n = \left(\frac{1}{\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$

Example: 2

What is the solution of the recurrence relation $a_n = 2a_{n-1}$ for $n \geq 1, a_0 = 3$.

Sol: Given $a_n = 2a_{n-1}$ (i.e) $a_n - 2a_{n-1} = 0 \longrightarrow (1)$

Let $a_n = r^n$ be a solution of (1).

$(1) \Rightarrow r^n - 2r^{n-1} = 0$

$\Rightarrow r^n\left[1 - \frac{2}{r}\right] = 0 \Rightarrow r^n\left[\frac{r-2}{r}\right] = 0.$

∴ The characteristic equation is $r - 2 = 0$.

$\Rightarrow r = 2.$

∴ $a_n = \alpha 2^n \longrightarrow (2)$

Given $a_0 = 3 \Rightarrow a_0 = \alpha 2^0 = 3 \Rightarrow \alpha = 3.$

∴ $(2) \Rightarrow a_n = 3(2^n)$ //.

Example: 3

Find the solution to the recurrence relation $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$ with initial conditions $a_0 = 1$, $a_1 = -2$ and $a_2 = -1$

Solu:

Given $a_n + 3a_{n-1} + 3a_{n-2} + a_{n-3} = 0 \longrightarrow (1)$

Let $a_n = r^n$ be a solu. of (1).

$r^n + 3r^{n-1} + 3r^{n-2} + r^{n-3} = 0.$

$\Rightarrow r^n \left[1 + \frac{3}{r} + \frac{3}{r^2} + \frac{1}{r^3}\right] = 0$

$\Rightarrow r^n \left[\frac{r^3 + 3r^2 + 3r + 1}{r^3}\right] = 0$

$\therefore$ The characteristic eqn. is $r^3 + 3r^2 + 3r + 1 = 0.$

(i.e) $(r+1)^3 = 0.$

(i.e) $r = -1, -1, -1.$

Hence $a_n = \alpha_1 (-1)^n + \alpha_2 n (-1)^n + \alpha_3 n^2 (-1)^n \longrightarrow (2)$

Given $a_0 = 0 \Rightarrow a_0 = \alpha_1 (-1)^0 + \alpha_2 (0)(-1)^n + \alpha_3 (0)(-1)^n = 1$

$\Rightarrow \alpha_1 = 1.$

Given $a_1 = -2 \Rightarrow a_1 = \alpha_1 (-1)^1 + \alpha_2 (1)(-1)^1 + \alpha_3 (1)^2 (-1)^1 = -2$

$\Rightarrow -\alpha_1 - \alpha_2 - \alpha_3 = -2.$

$\Rightarrow -1 - \alpha_2 - \alpha_3 = -2$

$\Rightarrow \alpha_2 + \alpha_3 = 1 \longrightarrow (3)$

Given: $a_2 = -1 \Rightarrow a_2 = \alpha_1(-1)^2 + \alpha_2(2)(-1)^2 + \alpha_3(2)^2(-1)^2$ (13)

$= -1$

$\Rightarrow \alpha_1 + 2\alpha_2 + 4\alpha_3 = -1$

$\Rightarrow 1 + 2\alpha_2 + 4\alpha_3 = -1$

$\Rightarrow 2\alpha_2 + 4\alpha_3 = -2$

$\Rightarrow \alpha_2 + 2\alpha_3 = -1 \longrightarrow (4)$

(2) − (4) $\Rightarrow -\alpha_3 = 2$

$\Rightarrow \alpha_3 = -2$

(3) $\Rightarrow \alpha_2 = 3$

$\therefore$ (2) $\Rightarrow a_n = (-1)^n + 3n(-1)^n - 2n^2(-1)^n$

Example: 4

What form does a particular solu. of a linear non-homogeneous recurrence relation $a_n = 6a_{n-1} - 9a_{n-2} + F(n)$ have when $F(n) = 3^n$, $F(n) = n3^n$, $F(n) = n^2 2^n$ and $F(n) = (n^2+1)3^n$?

Solu: The associated linear homogeneous recurrence relation is $a_n = 6a_{n-1} - 9a_{n-2}$

Its characteristic equ. is $r^2 - 6r + 9 = (r-3)^2 = 0$

(i.e) $r = 3, 3$.

$F(n)$ is of the form $p(n).s^n$.

$s=3$ is a root with multiplicity $m=2$.
but $s=2$ is not a root.

Hence Particular solution has the form,

$p_0 n^2 3^n$ if $F(n) = 3^n$

$n^2(p_1 n + p_0) 3^n$ if $F(n) = n 3^n$

$(p_2 n^2 + p_1 n + p_0) 2^n$ if $F(n) = n^2 2^n$

$n^2(p_2 n^2 + p_1 n + p_0) 3^n$ if $F(n) = (n^2+1) 3^n$.

———— x ———— x ————

Generating Functions

Defn: Generating Function.

The generating function for the sequence $a_0, a_1, \ldots a_k \ldots$ of real numbers is the infinite series.

$$G(x) = a_0 + a_1 x + \cdots + a_k x^k + \cdots = \sum_{k=0}^{\infty} a_k x^k$$

Theorem:

Let $f(x) = \sum_{k=0}^{\infty} a_k x^k$ and $g(x) = \sum_{k=0}^{\infty} b_k x^k$. Then

$$f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k \text{ and}$$

$$f(x) \cdot g(x) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) x^k$$

Defn:

Let u be a real number and k a non-negative integer. Then the extended binomial co-efficient $\binom{u}{k}$ is defined by $\binom{u}{k} = \begin{cases} u(u-1)\ldots(u-k+1)/k! & \text{if } k>0 \\ 1 & \text{if } k=0. \end{cases}$

Theorem: The extended binomial theorem.

Let x be a real number with $|x|<1$ and let u be a real number. Then $(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k$

Example: 1.

What is the generating fun. for the seq. 1, 1, 1, 1, 1?

Soln:

The generating fun. of 1, 1, 1, 1, 1 is

$$1 + x + x^2 + x^3 + x^4$$

(i.e) $1 + x + x^2 + x^3 + x^4 = \frac{x^5 - 1}{x-1}$ when $x \neq 1$

Consequently $G(x) = \frac{x^5-1}{x-1}$ is the G.F. of the seq. 1, 1, 1, 1, 1.

Example: 2

Find the generation fun. for the finite seq. 2, 2, 2, 2, 2.

Soln: The generating fun. of 2, 2, 2, 2, 2 is

$$2 + 2x + 2x^2 + 2x^4$$

(i.e) $2 + 2x + 2x^2 + 2x^3 + 2x^4 = 2[1 + x + x^2 + x^3 + x^4]$

$$= 2\left[\frac{x^5-1}{x-1}\right] \text{ when } x \neq 1$$

Consequently, $G(x) = 2\left[\frac{x^5-1}{x-1}\right]$ is the G.F. of the sequence 2, 2, 2, 2, 2.

Example: 3

Find the values of the extended binomial co-efficient $\binom{-2}{4}$ and $\binom{1/3}{0}$.

Solu: We know that

$$\binom{u}{k} = \begin{cases} u(u-1)\cdots\cdots\frac{u-k+1}{k!} & \text{if } k>0 \\ 1 & \text{if } k=0 \end{cases}$$

(i) $\binom{-2}{4} = \dfrac{(-2)(-2-1)(-2-2)(-2-3)}{4!}$

$= \dfrac{(-2)(-3)(-4)(-5)}{4!}$

$= \dfrac{120}{24} = 5$

(ii) $\binom{1/3}{0} = 1$.

Example: 4

Find the generating fun. for $(1+x)^{-n}$ where n is a positive integer.

Solu: $(1+x)^{-n} = \sum_{k=0}^{n} \binom{-n}{k} x^k$ by extended binomial theore

W.K.T, $\binom{-n}{r} = (-1)^r C(n+r-1, r)$

$\therefore (1+x)^{-n} = \sum_{k=0}^{n} (-1)^k C(n+k-1, k)\, x^k$

Example: 6

Find the generating fun. for the seq. 1, 4, 16, 64, 256.

Soln: The generating fun. of $1, 4, 4^2, 4^3, 4^4, \ldots 4^n$

$$1 + 4x + 4^2x^2 + 4^3x^3 + 4^4x^4 + \cdots\cdots$$

Let $G(x) = 1 + 4x + 4^2x^2 + 4^3x^3 + 4^4x^4 + \cdots$

$$\Rightarrow G(x) = \frac{1}{1-4x} \quad \text{(by example: 5)}.$$

Example: 5

Find the G.F. for the seq. $1, a, a^2, a^3, \ldots$ where a is a fixed constant.

Soln: The generating fun. of $1, a, a^2, \ldots$ is

$$1 + ax + a^2x^2 + \cdots$$

Let $G(x) = 1 + ax + a^2x^2 + a^3x^3 + \cdots \rightarrow (1)$

$$\therefore G(x) - 1 = ax + a^2x^2 + a^3x^3 + \cdots$$

$$= ax\left[1 + ax + a^2x^2 + \cdots\right]$$

$$\Rightarrow \frac{G(x) - 1}{ax} = 1 + ax + a^2x^2 + \cdots$$

$$= G(x) \text{ by } (1).$$

$$\Rightarrow G(x) - 1 = ax\,G(x)$$

$$\Rightarrow G(x) - ax\,G(x) = 1 \Rightarrow G(x)(1 - ax) = 1$$

$$\Rightarrow G(x) = \frac{1}{1-ax}$$ which is the required G.F.

Note:

1. $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ generates the sequence $(1, 1, 1, \ldots)$
2. $\frac{x}{1-x} = \sum_{n=0}^{\infty} x^{n+1} = \sum_{r=1}^{\infty} x^r$ generates $(0, 1, 1, \ldots)$
3. $\frac{x^2}{1-x} = \sum_{n=0}^{\infty} x^{n+2} = \sum_{r=2}^{\infty} x^r$ generates $(0, 0, 1, 1, 1, \ldots)$
4. $G(x) = \sum_{n=0}^{\infty} a_n x^n$ generates $(a_0, a_1, a_2, \ldots)$
5. $G(x) - a_0 = \sum_{n=1}^{\infty} a_n x^n$ generates $(0, a_1, a_2, \ldots)$
6. $G(x) - a_0 - a_1 x = \sum_{n=2}^{\infty} a_n x^n$ generates $(0, 0, a_2, a_3, \ldots)$

Example: 7

Find a closed form for the generating fun. of $3, -3, 3, -3, 3, -3 \ldots$

Solu: We have $\frac{3}{1+x} = 3(1+x)^{-1}$ $= 3(1 - x + x^2 - x^3 + \cdots)$

$= 3 + (-3)x + 3x^2 + (-3)x^3 + \cdots$

$= \sum_{n=0}^{\infty} (-3)^n x^n.$

Hence the required G.F is $\frac{3}{1+x}$.

Example: 8

Find a closed form for the generating fun. for the seq. $\{a_n\}$ when $a_n = 3^n$ for all $n = 0, 1, 2, \ldots$

Solu: Given $a_n = 3^n$, $n = 0, 1, 2, \ldots$

$a_0 = 3^0, a_1 = 3, a_2 = 3^2, a_3 = 3^3, \ldots$

(i.e) $1, 3, 3^2, 3^3, \ldots$

The G.F. of $1, 3, 3^2, 3^3, \ldots$ is

$G(x) = 1 + 3x + 3^2x^2 + \cdots = \frac{1}{1-3x}$ which is the G.F. of the given sequence $= (1-3x)^{-1}$

Example: 9

Find the co-efficient of x^{10} in $(1+x^5+x^{10}+x^{15}+\ldots)^3$

Solu:

W.K.T,

$$(1+x^5+x^{10}+x^{15}+\ldots)^3 = \left[(1-x^5)^{-1}\right]^3$$

$$= (1-x^5)^{-3}$$

$$= \sum C(3+r-1, r)\, x^{5r}$$

To find the co-efficient of x^{10}, put $5r = 10$

$$\Rightarrow r = 2.$$

$\therefore$ The required co-efficient is $C(3+2-1, 2) = C(4, 2)$

$$= {}^4C_2 = 6.$$

Example: 10

Find the co-efficient of x^{10} in $(x^3+x^4+x^5+\ldots)^3$

Solu:

Given: $(x^3+x^4+x^5+\ldots)^3 = x^9(1+x+x^2+\ldots)^3$

$$= x^9\left[(1-x)^{-1}\right]^3$$

$$= x^9 (1-x)^{-3}$$

$$= x^9 \sum C(3+r-1, r)\, x^r$$

$$= \sum C(3+r-1, r)\, x^{9+r}$$

To find the co-efficient of x^{10}

(i.e) $9+r = 10 \Rightarrow r = 1$.

$\therefore$ The required co-efficient is $C(3+1-1, 1) = C(3, 1)$

$$= {}^3C_1$$

$$= 3 \text{ Ans.}$$

Example: 11

Find the co-efficient of x^{18} in

$(x+x^2+x^3+x^4+x^5)(x^2+x^3+x^4+\cdots)^5$

Solu:

We know that,

$(x+x^2+x^3+x^4+x^5)(x^2+x^3+x^4+\cdots)^5$

$= x(1+x+x^2+x^3+x^4)\cdot x^{10}(1+x+x^2+\cdots)^5$

$= x^{11}(1+x+x^2+x^3+x^4)[(1-x)^{-1}]^5$

$= x^{11}\cdot\left[\frac{1-x^5}{1-x}\right](1-x)^{-5}$

$= x^{11}(1-x^5)(1-x)^{-6}$

$= (x^{11}-x^{16})(1-x)^{-6}$

$= (x^{11}-x^{16})\sum c(6+r-1,r)x^r$

$= \sum c(6+r-1,r)x^{11+r} - \sum c(6+r-1,r)x^{16+r}$

Hence the co-efficient of x^{18} is

$c(6+7-1,7) - c(6+2-1,2)$

$= c(12,7) - c(7,2)$

$= 792 - 21$

$= 771$.

Example: 12

Using generating function, prove the relation

$c(n,r) = c(n-1,r) + c(n-1,r-1)$ [Pascal's Identity].

Solu:

W.K.T, $c(n,r)$ is the co-efficient of x^r in $(1+x)^n$.

But $(1+x)^n = (1+x)^{n-1} + x(1+x)^{n-1}$ ⟶ ①

The co-efficient of x^r in $(1+x)^{n-1}$ is $C(n-1, r)$

The co-efficient of x^r in $(1+x)^{n-1}$ is $C(n-1, r-1)$

This shows that,

$$C(n, r) = C(n-1, r) + C(n-1, r-1)$$

[∵ the co-efficient of x^r in L.H.S. of ① is equal to the sum of co-efficients of x^r of the two terms in the R.H.S of ①].

Example: 13

Use generating functions to show that

$\sum_{k=0}^{n} C(n,k)^2 = C(2n, n)$ whenever n is a positive integer.

Solu:

To prove $\sum_{k=0}^{n} C(n,k)^2 = C(2n, n)$

$C(2n, n)$ is the co-efficient of x^n in $(1+x)^{2n}$ ⟶ ①

$$(1+x)^{2n} = [(1+x)^n]^2$$

$$= [C(n,0) + C(n,1)x + C(n,2)x^2 + \cdots + C(n,n)x^n]^2$$

The co-efficient of x^n in this expression is

$$C(n,0)C(n,n) + C(n,1)C(n,n-1) + \cdots + C(n,n)C(n,0)$$

$$= \sum_{k=0}^{n} C(n,k)^2 \quad [\because C(n,n-k) = C(n,k)] \longrightarrow ②$$

From ① & ②, both $c(2n,n)$ and $\sum_{k=0}^{n} c(n,k)^2$ represent the co-efficient of x^n in $(1+x)^{2n}$

$\therefore \sum_{k=0}^{n} c(n,k)^2 = c(2n,n)$.

Example: 14

Use generating funs. to find an explicit formula for the Fibonacci numbers.

Soln:

Let $G(x) = \sum_{k=0}^{\infty} f_k x^k$

$\Rightarrow G(x) - xG(x) - x^2 G(x) = f_0 + (f_1 - f_0)x + \sum_{k=2}^{\infty} (f_k - f_{k-1} - f_{k-2}) x^k$

$= 0 + x + \sum_{k=2}^{\infty} 0 \cdot x^k$

$= x$.

$\Rightarrow G(x)[1 - x - x^2] = x$.

$\Rightarrow G(x) = \frac{x}{1-x-x^2} = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\alpha x}\right) - \frac{1}{\sqrt{5}}\left(\frac{1}{1-\beta x}\right)$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$.

$\frac{1}{1-\alpha x} = \sum_{k=0}^{\infty} \alpha^k x^k$.

$\frac{1}{1-\beta x} = \sum_{k=0}^{\infty} \beta^k x^k$.

$\therefore G(x) = \frac{1}{\sqrt{5}} \sum_{k=0}^{\infty} (\alpha^k - \beta^k) x^k$

Hence $f_k = \frac{1}{\sqrt{5}} (\alpha^k - \beta^k)$.

Inclusion and Exclusion - Applications of Inclusion and Exclusion:

★ Principle of Inclusion and Exclusion.

Let X and Y be two finite subsets of a universal set U. If X and Y are disjoint, then

$$|X \cup Y| = |X| + |Y|$$

If X and Y are not disjoint, then

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

This is called the principle of inclusion and exclusion.

Theorem:

For any finite sets A, B & C, we have

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

(i.e) we include $n(A)$, $n(B)$, $n(C)$ & $n(A \cap B \cap C)$, and then we exclude $n(A \cap B)$, $n(A \cap C)$ & $n(B \cap C)$.

Theorem: $n(A_1 \cup A_2 \cup A_3 \cup \dots \cup A_m) = S_1 - S_2 + S_3 - \dots + (-1)^{m-1} S_m$

Example:

Give a formula for the number of elements in the union of four sets.

Sol: By the ~~Pmpc~~ Principle of inclusion and exclusion we get

$$|A_1 \cup A_2 \cup A_3 \cup A_4| = |A_1| + |A_2| + |A_3| + |A_4| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_3| - |A_2 \cap A_4| - |A_3 \cap A_4| + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| - |A_1 \cap A_2 \cap A_3 \cap A_4|$$

Example: 2

A total of 1232 students have taken a course in Tamil, 879 have taken a course in English and 114 have taken a course in Telugu. Further, 103 have taken courses in both Tamil and English, 23 have taken courses in both Tamil and Telugu and 14 have taken courses in both English and Telugu. If 2092 students have taken at least one of Tamil, English and Telugu, how many students have taken a course in all three languages?

Solu: Let T → Students who have taken a course in Tamil

E → Students who have taken a course in English

R → Students who have taken a course in Telugu

(i.e) $|T| = 1232$, $|E| = 879$, $|R| = 114$

$|T \cap E| = 103$, $|E \cap R| = 23$, $|E \cap R| = 14$ and

$|T \cup E \cup R| = 2092$

By the principle of inclusion and exclusion we get

$$|T \cup E \cup R| = |T| + |E| + |R| - |T \cap E| - |E \cap R| - |T \cap R| + |T \cap E \cap R|$$

$$\Rightarrow 2092 = 1232 + 879 + 114 - 103 - 23 - 14 + |T \cap E \cap R|$$

$$\Rightarrow |T \cap E \cap R| = 7.$$

∴ There are seven students who have taken courses in Tamil, English, Telugu.

Example: 3

Find the number of positive integers ~~are~~ not exceeding 100 that are not divisible by 7 or by 11.

Soln:

Let A be the set of +ve integers not exceeding 100 that are divisible by 7.

Let B be the set of +ve integers not exceeding 100 that are divisible by 11.

Then $A \cup B$ is the set of positive integers not exceeding 100 that are divisible by either 7 or 11 and $A \cap B$ is the set of positive integers not exceeding 100 that are divisible by both 7 and 11.

We know that among the positive integers not exceeding 100 there are $\left[\frac{100}{7}\right]$ integers divisible by 7 and $\left[\frac{100}{11}\right]$ integers divisible by 11.

Since 7 and 11 are relatively prime, the integers are divisible by both 7 and 11 are those divisible by (7)(11).

There are $\frac{100}{(7)(11)}$ positive integers not exceeding 100 that are divisible by both 7 and 11.

$\therefore |A \cup B| = |A| + |B| - |A \cap B| = \left[\frac{100}{7}\right] + \left[\frac{100}{11}\right] - \left[\frac{100}{(7)(11)}\right]$

$= 14 + 9 - 1 = 22$.

Example: 4

Among the first 1000 positive integers: Determin the integers which are not divisible by 5, nor by 7, nor by 9.

Solu:

Let A be the set of number of integers divisible by 5

B be the number of integers divisible by 7

C be the number of integers divisible by 9.

$\therefore |A| = \left[\frac{1000}{5}\right] = 200$; $|B| = \left[\frac{1000}{7}\right] = 142$

$|C| = \left[\frac{1000}{9}\right] = 111$; $|A \cap B| = \left[\frac{1000}{5 \times 7}\right] = 28$

$|A \cap C| = \left[\frac{1000}{5 \times 9}\right] = 22$; $|B \cap C| = \left[\frac{1000}{7 \times 9}\right] = 15$

$|A \cap B \cap C| = \left[\frac{1000}{5 \times 7 \times 9}\right] = 3$

∴ The number of integers divisible by 5, 7 and 9.

$|A \cup B \cup C| = 200 + 142 + 111 - 28 - 22 - 15 + 3$

$= 391$

The number of integers not divisible by 5, nor by 7, nor by 9. = Total number of integers − Integers divisible by 5, 7 and 9

$= 1000 - 391 = 609$ //.

Example: 5

In a survey of 300 students, 64 had taken a Mathematics course, 94 had taken a English course, 58 had taken a computer course, 28 had taken both a Mathematics and a computer course, 26 had taken both English and Mathematics course, 22 had taken both a English and a Computer course, 14 had taken all three courses. How many students were surveyed who had taken non of the three courses?

Solu: Given $|M| = 64$; $|E| = 94$; $|C| = 58$, $|M \cap C| = 28$, $|M \cap E| = 26$; $|E \cap C| = 22$; $|M \cap E \cap C| = 14$.

$$|M \cup E \cup C| = |M| + |E| + |C| - |M \cap C| - |M \cap E| - |E \cap C| + |M \cap E \cap C|$$

$$= 64 + 94 + 58 - 28 - 22 + 14 = 154$$

Students who had taken none of the courses

$$= 300 - 154 = 146.$$

Example: 9

How many solutions does $x_1 + x_2 + x_3 = 13$ have, where x_1, x_2 and x_3 are non-negative integers with $x_1 < 6$, $x_2 < 6$ and $x_3 < 6$?

Solu:

To apply the principle of inclusion-exclusion, let a solution have property P_1 if $x_1 \geq 6$, property P_2 if $x_2 \geq 6$, property P_3 if $x_3 \geq 6$.

Problem:

How many integers between 1 to 100 that are
(i) not divisible by 7, 11 or 13
(ii) divisible by 3 but not by 7.

Soln:

(i) Let A, B & C denotes respectively the number of integers between 1 to 100 that are divisible by 7, 11 and 13 respectively

Now, $|A| = \left[\frac{100}{7}\right] = 14$

$|B| = \left[\frac{100}{11}\right] = 9$

$|C| = \left[\frac{100}{13}\right] = 7$

$|A \cap B| = \left[\frac{100}{7 \times 11}\right] = 1$

$|A \cap C| = \left[\frac{100}{7 \times 13}\right] = 1$

$|B \cap C| = \left[\frac{100}{11 \times 13}\right] = 0.$

$|A \cap B \cap C| = \left[\frac{100}{7 \times 11 \times 13}\right] = 0.$

The number of integers between 1-100 that are divisible by 7, 11 or 13 is $|A \cup B \cup C|$.

By principle of inclusion and exclusion $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

$= 14 + 9 + 7 - (1 + 1 + 0) + 0$

$= 30 - 2 = 28.$

Now, The number of integer not divisible by any of 7, 11 and 13 $= \text{Total} - |A \cup B \cup C|$

$= 100 - 28$

$= 72$ //.

(ii) Let A and B denote the no. of integers between 1-100 that are divisible by 3 and 7 respectively.

$|A| = \left[\frac{100}{3}\right] = 33$

$|B| = \left[\frac{100}{7}\right] = 14$

$|A \cap B| = \left[\frac{100}{3 \times 7}\right] = 4$

The number of integers divisible by 3 but not by 7

$= |A| - |A \cap B|$

$= 33 - 4$

$= 29$ //.

Problem:

Find the number of the integers between 1 to 100 that are divisible by (i) 2, 3, 5 or 7 (ii) 2, 3, 5 but not by 7.

Soln:

(i) Let A, B, C and D denote the number of positive integers between 1-100 that are devisible by 2, 3, 5 & 7 respectively.

Now, $|A| = \left[\frac{100}{2}\right] = 50$ $|B| = \left[\frac{100}{3}\right] = 33$ $|C| = \left[\frac{100}{5}\right] = 20$

$|D| = \left[\frac{100}{7}\right] = 14$. $|A \cap B| = \left[\frac{100}{2 \times 3}\right] = 16$, $|A \cap C| = \left[\frac{100}{2 \times 5}\right] = 10$

$|A \cap D| = \left[\frac{100}{14}\right] = 7$ $|B \cap C| = \left[\frac{100}{3 \times 5}\right] = 6$, $|B \cap D| = \left[\frac{100}{3 \times 7}\right] = 4$

$|C \cap D| = \left[\frac{100}{5 \times 7}\right] = 2$, $|A \cap B \cap C| = \left[\frac{100}{2 \times 3 \times 5}\right] = 3$

$|A \cap B \cap D| = \left[\frac{100}{2 \times 3 \times 7}\right] = 2$, $|A \cap C \cap D| = \left[\frac{100}{2 \times 5 \times 7}\right] = 1$

$|B \cap C \cap D| = \left[\frac{100}{3 \times 5 \times 7}\right] = 0$, $|A \cap B \cap C \cap D| = 0$

By the Principle of inclusion and exclusion,

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

$= 50 + 33 + 20 + 14 - 16 - 10 - 7 - 6 - 4 - 2 + 3$
$+ 2 + 1 + 0 - 0$

$= 117 - 45 + 6 = 123 - 45 = 78$.

(ii) The number of integers between 1-100 that are divisible by 2, 3, 5 but not by 7.

$= |A \cap B \cap C| - |A \cap B \cap C \cap D|$

$= 3 - 0 = 3$.

Problem:
Determine the number of positive integers n, $1 \le n \le 1000$, that are divisible by 2, 3, or 5 but are divisible by 7.

Solu:
Let A, B, C & D denote respectively the number of integers between 1 - 1000 that are divisible by 2, 3, 5 and 7 respectively.

Now, $|A \cup B \cup C \cup D| = |A| + |B| + |C| + |D| - |A \cap B| - |A \cap C| - |A \cap D|$
$- |B \cap C| - |B \cap D| - |C \cap D| + |A \cap B \cap C|$
$+ |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D|$
$- |A \cap B \cap C \cap D|$

Here

∴ the number of ~~the~~ integers between 1-1000 that are not divisible by 2, 3, 5 but divisible by 7

$= |D| - |A \cap D| - |B \cap D| - |C \cap D| + |A \cap B \cap D|$
$+ |A \cap C \cap D| + |B \cap C \cap D| - |A \cap B \cap C \cap D|$

Now, $|D| = \left[\frac{1000}{7}\right] = 142$. $|A \cap D| = \left[\frac{1000}{2 \times 7}\right] = 71$

$|B \cap D| = \left[\frac{1000}{3 \times 7}\right] = 47$, $|C \cap D| = \left[\frac{1000}{5 \times 7}\right] = 28$

$|A \cap B \cap D| = \left[\frac{1000}{2 \times 3 \times 7}\right] = 23$; $|A \cap C \cap D| = \left[\frac{1000}{2 \times 5 \times 7}\right] = 14$

$|B \cap C \cap D| = \left[\frac{1000}{3 \times 5 \times 7}\right] = 10$, $|A \cap B \cap C \cap D| = \left[\frac{1000}{2 \times 3 \times 5 \times 7}\right] = 5$

∴

Validity of verbal arguments.

Example: 1.

Determine the validity of the following argument.
If two sides of a triangle are equal, then opposite angles are equal.

Two sides of a triangle are not equal.
Therefore, the opposite angles are not equal.

Soln:

Let P: Two sides of a triangle ~~is~~ are equal.
Q: The two opposite angle are equal.

The premises can be represented as
$P \to Q$ and $\neg P$ and the conclusion as $\neg Q$.

If the argument is a valid one then
$((P \to Q) \wedge \neg P) \to \neg Q$ will be tautology.

Let us now construct the truth table for
$((P \to Q) \wedge \neg P) \to \neg Q$

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

From the truth table we can infer that, $(P \to Q \wedge \neg P) \to \neg Q$ is not a tautology. Hence the argument is not valid.

Example: 2

Show that the following sets of premises are inconsistent.

$P \to Q,\ P \to R,\ Q \to \neg R,\ P$ [AU MJ 2006]

Solu:

1.	$P \to Q$	P
2.	$Q \to \neg R$	P
3.	$P \to \neg R$	from ① & ②, T
4.	P	P
5.	$\neg R$	P
6.	$P \to R$	P
7.	$\neg P$	T, from ⑤ & 6.
8.	$P \wedge \neg P$	T

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

Example: 3

Show that the following implication by using indirect method.

$(R \to \neg Q),\ RVS,\ S \to \neg Q,\ P \to Q \Rightarrow \neg P$. [AU. MJ 2006]

Solu: To use the indirect method, we will include $\neg\neg P \Leftrightarrow P$ as an additional premise and prove a contradiction.

1.	P	P
2.	$P \to Q$	P
3.	Q	T, (1), 2. and modus ponens.
4.	$R \to \neg Q$	P
5.	$S \to \neg Q$	P
6.	$(RVS) \to \neg Q$	T; 4, 5 and equivalence
7.	RVS	P
8.	$\neg Q$	T, 6, 7 and modus ponens
9.	$Q \wedge \neg Q$	T, 3, 8 and conjunction
10.	F	T, 9, and negation law (contradiction.

Rules of inference for Quantified statements

Rules in Quantifiers

Rule US: (Universal Specification)

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

If a statement of the form $(\forall x)(A(x))$ is assumed to be true, then the universal quantifier can be dropped to obtain $A(y)$ is true for any arbitrary object 'y' in the universe.

Rule ES: [Existential Specification]

From $(\exists x)\,A(x)$ one can conclude $A(y)$ provided that y is not free in any given premise and also not free in any prior step of the derivation. These requirements can easily be met by choosing a new variable each time ES is used.

Rule EG: [Existential Generalization]

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

If $A(x)$ is true for some element x in the universe, then $(\exists(y))\,A(y)$ is true.

Rule UG:

From $A(x)$ one can conclude $(y)\,A(y)$ provided that x is not free in any of the given premises and provided that if x is free in a prior step which resulted from use of ES, then no variables introduced by that use of ES appear free in $A(x)$.

Example: 1

Show that $(x)\, H(x) \to M(x) \wedge H(s) \Rightarrow M(s)$. Not that this problem is a symbolic translation of a well-known argument known as the "Socrates argument" which is given by:

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

If we denote $H(x)$: x is a man, $M(x)$: x is a mortal, and s: Socrates, we can put the argument in the above form.

Solu:

$\{1\}$	(1)	$(x)\, H(x) \to M(x)$	P
$\{1\}$	(2)	$H(s) \to M(s)$	US, (1)
$\{3\}$	(3)	$H(s)$	P
$\{1,3\}$	(4)	$M(s)$	T, (2), (3), modus ponens.

Note that in Step 2 first we remove the universal quantifier.

Example: 2.

Show that $(x)(P(x) \vee Q(x)) \Rightarrow (x)\, P(x) \vee (\exists x)\, Q(x)$ [AU N/D 2003]

Solu:

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)	$\neg((x) P(x) \vee (\exists x)\, Q(x))$	P (assumed)
$\{1\}$	(2)	$\neg(x)\, P(x) \wedge \neg(\exists x)\, Q(x)$	T, (1), $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$.
$\{1\}$	(3)	$\neg(x)\, P(x)$	T, (2), $P \wedge Q \Rightarrow P$
$\{1\}$	(4)	$(\exists x) \neg P(x)$	T, (3),
$\{1\}$	(5)	$\neg(\exists x)\, Q(x)$	T, (2), $P \wedge Q \Rightarrow Q$

{1}	(6)	$\exists x \neg Q(x)$	T, (5)
{1}	(7)	$\neg P(y)$	ES, (4)
{1}	(8)	$\neg Q(y)$	US, (6)
{1}	(9)	$\neg P(y) \wedge \neg Q(y)$	T, (7), (8), $P, Q \Rightarrow P \wedge Q$
{1}	(10)	$\neg(P(y) \vee Q(y))$	T, (9), $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$
{11}	(11)	$\forall x (P(x) \vee Q(x))$	P
{11}	(12)	$P(y) \vee Q(y)$	US, (11)
{1, 11}	(13)	$\neg(P(y) \vee Q(y)) \wedge (P(y) \vee Q(y))$	T, (10), (12), $P, Q \Rightarrow P \wedge Q$ Contradiction.

Example 3

Using CP or otherwise obtain the following implication.

$(\forall x)(P(x) \rightarrow Q(x)), (\forall x)(R(x) \rightarrow \neg Q(x)) \Rightarrow (\forall x)(R(x) \rightarrow \neg P(x))$

[AU MJ 2006]

Solu:

{1}	(1)	$(\forall x)(P(x) \rightarrow Q(x))$	P
{2}	(2)	$(\forall x)(R(x) \rightarrow \neg Q(x))$	P
{2}	(3)	$R(y) \rightarrow \neg Q(y)$	US, (2)
{4}	(4)	$R(y)$	P (assumed)
{2, 4}	(5)	$\neg Q(y)$	T, (3), (4).
{1}	(6)	$P(y) \rightarrow Q(y)$	US, (1)
{1, 2, 4}	(7)	$\neg P(y)$	T, (5), (6)
{1, 2, 4}	(8)	$R(y) \rightarrow \neg P(y)$	CP, (4) (7)
{1, 2}	(9)	$(\forall x)(R(x) \rightarrow \neg P(x))$	UG, (9).

Hence the argument is valid.

Unit-IV

Graphs

Graphs and Graph Models

Defn: (Graph)

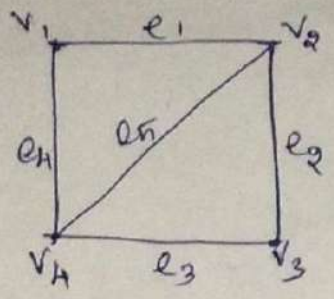
A graph $G = (V(G), E(G))$ consists of V, a non-empty set of vertices (nodes or points) and E, a set of edges (also called lines).

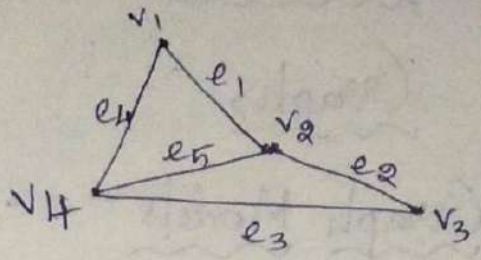
(i.e) A graph G is an ordered triple $(V(G), E(G), \phi)$ consists of non-empty set V called the set of vertices (nodes or points) of the graph G, E is said to be the set of edges of the graph G, and ϕ is a mapping from the set of edges E to a set of order or un-ordered pairs of elements of V.

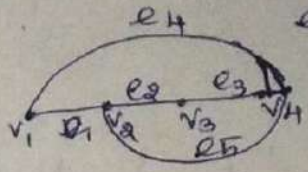
Example:

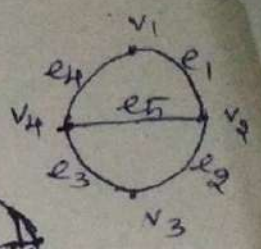
Let $G = (V(G), E(G), \phi)$ where $V(G) = \{v_1, v_2, v_3, v_4\}$ and $E(G) = \{e_1, e_2, e_3, e_4, e_5\}$ and ϕ is defined by $\phi(e_1) = \{v_1, v_2\}$, $\phi(e_2) = \{v_2, v_3\}$, $\phi(e_3) = \{v_3, v_4\}$, $\phi(e_4) = \{v_4, v_1\}$ $\phi(e_5) = \{v_4, v_2\}$.

Now, the diagramatic form of G is as follows.



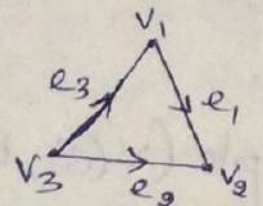




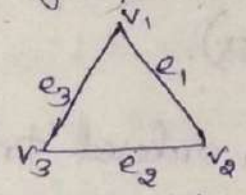


Defn:

A graph in which every edge is undirected is called an undirected graph. A graph in which every edge is directed is called a digraph or directed graph.



Directed graph.



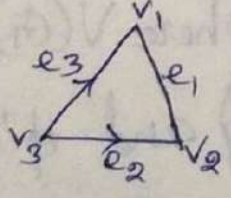
Undirected graph.

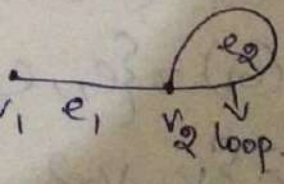
The edge e_1 is incident with the vertices v_1 and v_2 also the vertex v_1 is incident with e_1 and e_3.

The vertices v_1 & v_2 are also called the initial and terminal vertices of the edge e_1.

Defn: Mixed graph.

If some edges are directed and some are undirect in a graph, then the graph is a mixed graph.





Defn: Loop.

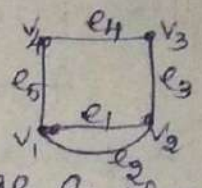
A loop is an edge whose vertices are equal.

(i.e) An edge of a graph which joins a vertex to itself is called a loop.

Defn: Parallel Edges.

If two edges have same end points then the edges are called parallel edges.

For example, e_1 & e_2 and e_4 & e_5 are called parallel edges. Since e_1 and e_2 have the same pair of vertices (v_1, v_2) as their terminal vertices.



Defn: Incident.

If the vertex v_i is an end vertex of some edge e_k then e_k is said to be incident with v_i.

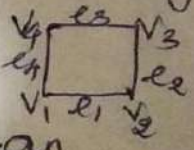
Defn: Adjacent edges and vertices.

Two edges are said to be adjacent if they are incident on a common vertex. [e_3 & e_4 are adjacent].

Two vertices v_i & v_j are said to be adjacent if v_iv_j is an edge of the graph. [v_3 & v_4 are adjacent].

Defn: Simple graph.

A graph which has neither loops nor parallel edges is called a simple graph.



Defn: Isolated vertex.

A vertex having no edge incident on it is called an isolated vertex. It is obvious that for an isolated vertex degree is zero.

One can easily note that isolated vertex is not adjacent to any vertex. [In the above graph v_5 is an isolated vertex].

Defn: Pendentant Vertex

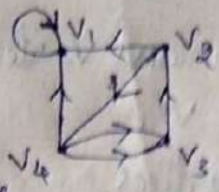
If the degree of any vertex is one, then that vertex is called pendent vertex.

Defn: Multigraph

A graph which contains some parallel edges is called a multigraph.

Defn: Pseudograph

A graph in which loops and parallel edges are allowed is called a pseudograph.



Defn: Degree of a Vertex

The number of edges incident at the vertex V_i is called the degree of the vertex with self loops counted twice and it is denoted by $d(V_i)$.

Example:

$d(V_1) = 4$; $d(V_3) = 3$ (for the above graph).
$d(V_2) = 3$; $d(V_4) = 4$

Defn:

In a directed graph, the indegree of a vertex V, denoted by $\deg^-(V)$ and defined by the number of edges with V as their terminal vertex.

The outdegree of V, denoted by $\deg^+(V)$, is the number of edges with V as their initial vertex.

Note: A loop at a vertex contributes 1 to both the indegree and the outdegree of this vertex.

Ex: In the above graph.

$\deg^-(V_1) = 3$; $\deg^+(V_1) = 1$; $\deg(V_1) = 3+1 = 4$
$\deg^-(V_2) = 1$; $\deg^+(V_2) = 2$; $\deg(V_2) = 1+2 = 3$
$\deg^-(V_3) = 2$; $\deg^+(V_3) = 1$; $\deg(V_3) = 2+1 = 3$
$\deg^-(V_4) = 1$; $\deg^+(V_4) = 3$; $\deg(V_4) = 1+3 = 4$

Theorems

Theorem: 1 (The Handshaking Theorem)

For any graph G with E edges and V vertices $v_1, v_2, \ldots v_n$, $\sum_{i=1}^{n} d(v_i) = 2E$.

Proof:

Let $G = G(V, E)$ be any graph, where $V = \{v_1, v_2, \ldots v_n\}$ $E = \{e_1, e_2, \ldots e_n\}$.

Since each edges contributes twice as a degree, the sum of the degree of all vertices in G is twice as the number of edges in G.

(i.e) $\sum_{n=1}^{n} d(v_i) = 2|E| = 2e$.

Note:

This theorem applies even if multiple edges and loops are present.

Theorem: 2

The number of odd degree vertices is always even.

Proof:

Let $G = \{V, E\}$ be any graph with 'n' number of vertices and 'e' number of edges.

Let $V_1, V_2, \ldots V_k$ be the vertices of odd degree and $V_1', V_2', \ldots V_m'$ be the vertices of even degree.

T.P k is even.

We know that $\sum_{i=1}^{n} d(V_i) = 2|E| = 2e$

$\Rightarrow \sum_{i=1}^{k} d(V_i) + \sum_{j=1}^{m} d(V_j') = 2e$

Each of $d(V_j')$ is even $\Rightarrow \sum_{j=1}^{m} d(V_j')$ and $2e$ are even numbers (being the sum of even numbers)

$\therefore \sum_{i=1}^{k} d(V_i)$ + an even number = an even number.

$\Rightarrow \sum_{i=1}^{k} d(V_i)$ = an even number.

Since, each term $d(V_i)$ is odd,

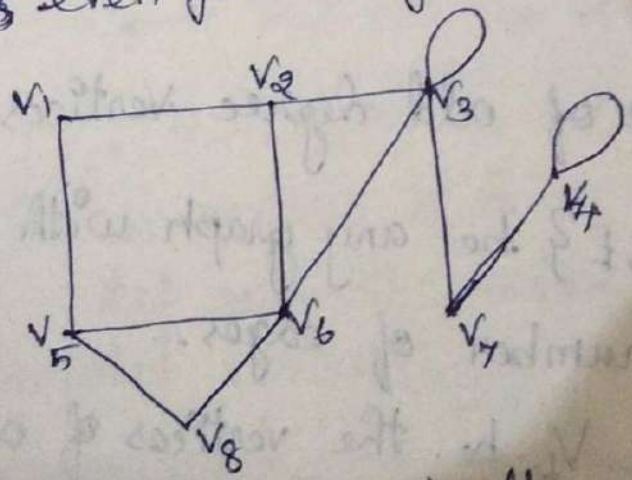
the number of terms in the LHS sum must be even.

$\Rightarrow k$ is even.

Hence the theorem.

Problem:

Verify that the sum of the degree of all the vertices is even for the graph.

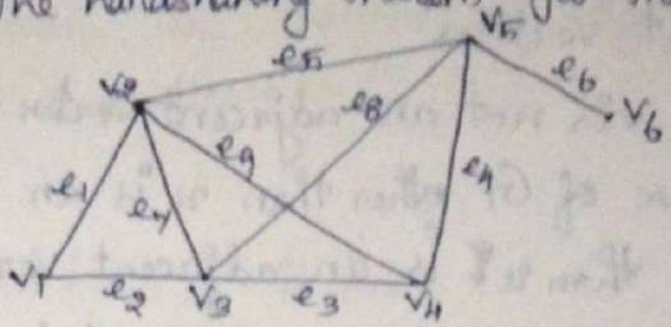


Soln: The sum of degree of all vertices = $d(v_1)+d(v_2)+\cdots$

$= 2+3+5+3+3+4+2+2$

$= 24$, which is even.

Problem:
Verify the handshaking theorem for the graph.



Solu: T.P $\sum_{i=1}^{6} d(v_i) = 2$ (no. of edges).

Now, $\sum_{i=1}^{6} d(v_i) = d(v_1) + d(v_2) + \ldots + d(v_6)$

$= 2+4+4+3+4+1$

$= 18.$

Also, 2 (no. of edges) $= 2 \times 9 = 18$

Hence $\sum_{i} d(v_i) = 2$ (no. of edges)

Theorem: 3

A simple graph with atleast two vertices has atleast two vertices of same degree.

Proof: Let G be a simple graph with $n \geq 2$ vertices. The graph G has no loop and parallel edges.

Hence the degree of each vertices is $\leq n-1$

Suppose that all the vertices of G are of different degrees.

$\therefore$ $0, 1, 2, 3, \ldots, n-1$ are the possible degrees for n-vertices of G.

Let u be the vertex with degree 0. Then u is an isolated vertex.

Let v be the vertex with degree n-1. Then v has n-1 adjacent vertices.

Because v is not an adjacent vertex of itself, therefore every vertex of G is other than u is an adjacent vertex of G other than u is an adjacent vertex u.

Hence u cannot be an isolated vertex, this contradiction proves that a simple graph contains two vertices of same.

Note:

The converse of the above theorem is not true.

Theorem: 4.

The degree of a vertex of a a simple graph G on n vertices cannot exceed n-1.

Proof:

Let v be a vertex of G because G is simple, no multiple edges or loops are allowed in G.

Thus v can be adjacent to atmost all the remaining n-1 vertices of G.

Hence v may have maximum degree n-1 in G.

Then $0 \leq \deg_G(v) \leq n-1 \quad \forall \; v \in V(G)$

Theorem: 5

The maximum number of edges in a simple graph with n-vertices is $\frac{n(n-1)}{2}$.

Proof: Using handshaking theorem,

$$\sum_{i} d(v_i) = 2e, \text{ where } e \text{ is the number of edges.}$$

W.K.T, $\sum_{i=1}^{n} d(v_i) = 2e = \text{even}$.

$$\Rightarrow d(v_1)+d(v_2)+\cdots+d(v_n) = 2e$$

Now, maximum degree of each vertex is $(n-1)$,

$$\therefore (n-1)+(n-1)+\cdots+(n-1) = 2e$$

$$\Rightarrow n(n-1) = 2e$$

$$\Rightarrow e = \frac{n(n-1)}{2}.$$

Theorem: 6

The sum of the indegree vertices of a digraph G is equal to the sum of the outdegree vertices of a digraph.

Let G be a directed graph, then $\sum_{v \in V_4} \deg^+_G(v) = \sum_{v \in V} \deg^-_G(v) = e$ (OR)

Proof:

Each edges has an initial vertex and a terminal vertex.

$\therefore$ Each edge contribute one indegree and one outdegree.

(i.e) Sum of the indegree = Sum of the outdegree of every vertex, which is always equal to the no. of edges.

Theorem: 7

Any self-complementary graph has $4n$ (or) $4n+1$ vertices.

Proof:

Let G be a given self-complementary graph with P-vertices.

$\therefore$ If $\bar{G}$ is complement of G, then $G \cong \bar{G}$.

(i.e) No. of edges in G = no. of edges in $\bar{G}$ $\rightarrow$ ①

W.K.T, No. of edges in G + No. of edges in $\bar{G}$ = $\frac{P(P-1)}{2}$

$\Rightarrow$ No. of edges in G + No. of edges in G = $\frac{P(P-1)}{2}$ (By ①)

$\Rightarrow 2 \cdot$ (No. of edges in G) = $\frac{P(P-1)}{2}$

$\Rightarrow$ No. of edges in G = $\frac{P(P-1)}{4}$.

(ie) $\frac{p(p-1)}{4}$ is an integer.

But either p or (p-1) is odd.

Thus the product of two consecutive integers which is divisible by 4.

∴ either p or (p-1) is a multiple of 4.

(ie) $p = 4n$ or $p-1 = 4n$

(ie) $p = 4n$ or $p = 4n+1$.

Hence the proof.

Example:

For the following degree sequences, 4, 4, 4, 3, 2 find if there exist a graph or not.

Solu:

Sum of the degrees of all vertices $= 4+4+4+3+2$

$= 17$, which is an odd number.

Since the sum of the degrees of all vertices always even, there is no such graph exist.

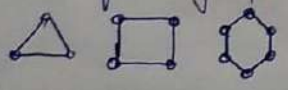
Defn:

If every vertex of a simple graph has the same degree, then the graph is called a regular graph.

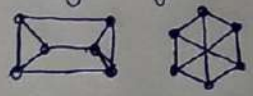
If every vertex in a regular graph has degree k, then the graph is called k-regular.

Examples:

* 2-regular graphs



3-regular graphs



Defn:

A simple graph G with 'n' vertices is said to be a complete graph if the degree of every vertex is n-1

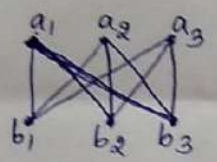
The complete graph on 'n' vertices is denoted by K_n. The graphs K_n, for n = 1, 2, 3, 4, 5 are displayed in figures as follows.

Defn:
A graph G is said to be bipartite if its vertex set $V(G)$ can be partitioned into two disjoint non-empty sets V_1 and V_2, $V_1 \cup V_2 = V(G)$, such that every edge in $E(G)$ has one end vertex in V_1 and another end vertex in V_2. (so that no edges in G, connects either two vertices in V_1 or two vertices in V_2).

Ex.


$\rightarrow K_{2,3}$ graph.

Defn:
A bipartite graph G, with the bipartition V_1 and V_2 is called complete bipartite graph, if every vertex in V_1 is adjacent to every vertex in V_2. Clearly, every vertex in V_2 is adjacent to every vertex in V_1.

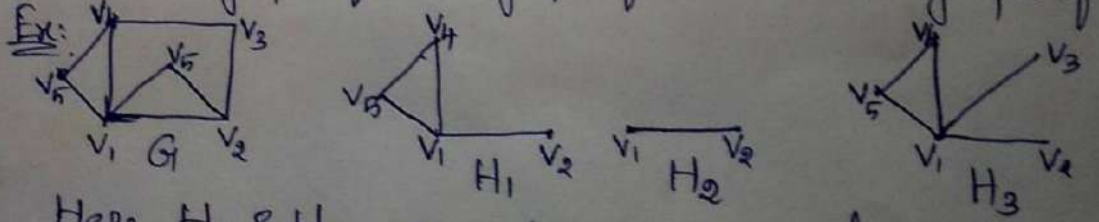
Ex:


$K_{3,3}$-graph.

Defn:
A graph $H = (V', E')$ is called a subgraph of $G = (V, E)$, if $V' \subseteq V$ and $E' \subseteq E$.

In otherwords, a graph H is said to be a subgraph of G if all the vertices and all the edges of H are in G and if the adjacency is preserved in H exactly as in G.

Note:
1. Each graph has its own subgraph.
2. A single vertex in a graph G is a subgraph of G
3. A single edge in G, together with its end vertices is also a subgraph of G.
4. A subgraph of a subgraph of G is also a subgraph of G.

Ex:


Here H_1 & H_2 are subgraphs of G and H_3 is not a subgraph of G.

Graph Representation:

There are many useful ways to represent graphs. We can represent a graph in the form of adjacency lists, which are very useful in computer programming.

Defn: (Adjacency Matrix of a Simple Graph).

Let $G = (V, E)$ be a simple graph with n-vertices $\{v_1, v_2, \ldots v_n\}$. Its adjacency matrix is denoted by $A = [a_{ij}]$ and defined by

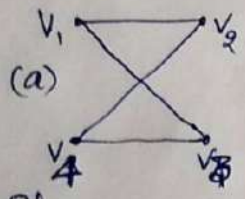
$$A = [a_{ij}] = \begin{cases} 1 & \text{if there exist an edge between } v_i \text{ and } v_j \\ 0 & \text{otherwise.} \end{cases}$$

Note:

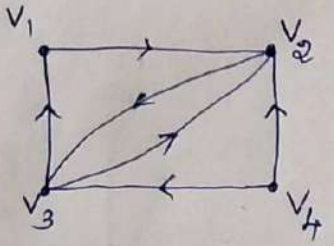
1. The adjacency matrix of a graph is based on the ordering chosen for the vertices. Hence there are as many $n!$ different adjacency matrices for a graph with n-vertices, since there are $n!$ different ordering of n.
2. The adjacency matrix of a simple graph is symmetric, that is $a_{ij} = a_{ji}$. Since simple graph has no loops, $a_{ii} = 0 \; \forall \; i = 1, 2 \ldots n$.

Example:

(a)



(b)



Sol: Adjacency matrix.

(a)

$$A = [a_{ij}] = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

(b)

$$A = [a_{ij}] = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array}.$$

Note:

1. Sum of all the entries in any row is equal to the degree of the vertex corresponding to that row.
2. All the entries along the leading diagonal are zero iff the graph has no self loop.
3. Given any square, symmetric, binary matrix A of order n, one can easily construct a graph G with n vertices (without parallel-edges) such that A is the adjacency matrix of G.

Defn: Path matrix.

If $G = (V, E)$ be a simple digraph in which $|V| = n$ and the nodes of G are assumed to be ordered. An $n \times n$ matrix P whose elements are given by

$$P_{ij} = \begin{cases} 1 & \text{if there exists a path from } v_i \text{ to } v_j \\ 0 & \text{otherwise.} \end{cases}$$

is called the path matrix (reachability matrix) of the graph G.

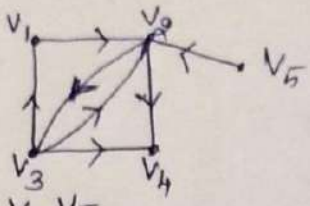
Note:

The path matrix only shows the presence or absence of atleast one path between a pair of vertices and also the presence or absence of a cycle at any node. It does not, however, show all the path that may exist.

Defn: Incidence

Example:

Find the path matrix of



Solu: Path matrix is

$$B = [b_{ij}] = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

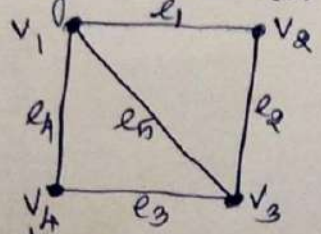
Defn: Incidence Matrix

Let $G = (V, E)$ be an undirected graph with n-vertices $\{v_1, v_2, \ldots v_n\}$ and m-edges $\{e_1, e_2, \ldots e_m\}$. Then the $(n \times m)$ matrix $B = [b_{ij}]$, where

$$b_{ij} = \begin{cases} 1 & \text{when edge } e_j \text{ incident on } v_i \\ 0 & \text{otherwise.} \end{cases}$$

Example:

Find incidence matrix of the following graph and give your observations regarding the entries of B.



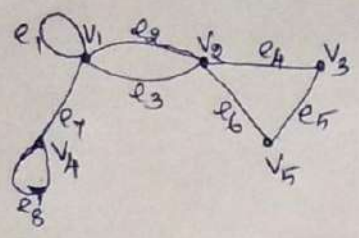
Solu: Incidence matrix.

$$B = [b_{ij}] = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

Observations:

1. Since each edge is incident on exactly two vertices, each column on B has exactly two 1's.
2. The sum of the entries in any one row gives the degree of the vertex corresponding to the row.
3. The rank of $B = 3$.

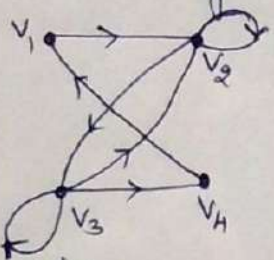
Example:
Find the incidence matrix of



Solu: Incidence matrix

$$B = [b_{ij}] = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \end{array} \begin{array}{c} \begin{array}{cccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

Example:
Find the adjacency matrix of the graphs. Hence find degree of each vertex.

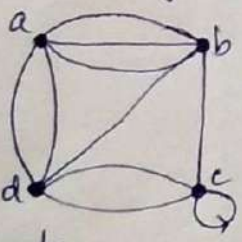


Solu:

$$A = [a_{ij}] = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \end{array} \begin{array}{c} \begin{array}{cccc} V_1 & V_2 & V_3 & V_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Now,
$\text{Deg}(V_1)$ = Sum of the entries of row 1 = 1
$\text{Deg}(V_2)$ = Sum of the entries of row 2 = 2
$\text{Deg}(V_3)$ = Sum of the entries of row 3 = 3
$\text{Deg}(V_4)$ = Sum of the entries of row 4 = 1

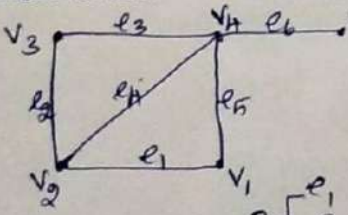
Example:
Obtain adjacency matrix to represent the pseudograph show below:



Solu: Adjacency matrix

$$A = [a_{ij}] = \begin{bmatrix} 0 & 3 & 0 & 2 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 2 & 1 & 2 & 0 \end{bmatrix}$$

Example:
Find the path matrix $P(V_2, V_4)$ for the following graph G and what is the observation on matrix $P(V_2, V_4)$.

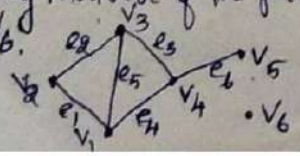


Solu: There are 3 different paths from V_2 to V_4. These paths from V_2 to V_4 are $\{e_4\}$, $\{e_1, e_5\}$, $\{e_2, e_3\}$ say P_1, P_2, P_3 respectively.

$$P(V_2, V_4) = \begin{array}{c} \\ P_1 \\ P_2 \\ P_3 \end{array} \begin{array}{c} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

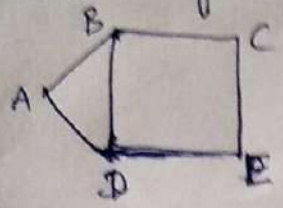
Observations:
1. A column of all 0's will correspond to an edge that does not lie on any path between v_i and v_j.
2. A column of all 1's will correspond to an edge lie in every path between v_i & v_j.

H.W Example:
Find the adjacency matrix of the following graphs. Hence find the degree of the vertices V_1, V_3 and V_6.



Example:

Find all the simple paths from A to E and all cycles with respect to vertex A of the given graph.



Soln: Simple paths from A to E are

(i) $A \to B \to C \to E$
(ii) $A \to B \to D \to E$
(iii) $A \to D \to E$
(iv) $A \to D \to B \to C \to E$

The cycles are

(i) $A \to B \to C \to E \to D \to A$
(ii) $A \to D \to E \to C \to B \to A$

Graph Isomorphism

Defn:

Two graphs G_1 and G_2 are said to be Isomorphic to each other, if there exist a one-to-one correspondence between the vertex sets which preserves adjacency of the vertices.

However, the definition of isomorphism of two graphs were easy, but the given graph having 'n' vertices itself has n! ways of one-to-one correspondence.

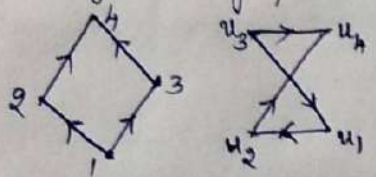
So before going for isomorphism, we can verify whether they have the same number of vertices and edges and if the degree sequence of the graphs are same. If not, then we can say the graphs are not isomorphic.

Note:

1. If G_1 and G_2 are isomorphic then G_1 and G_2 have
   (i) the same number of vertices
   (ii) the same number of edges
   (iii) An equal number of vertices with a given degree
2. However, these conditions are not sufficient for graph Isomorphism.

Example: 1.

Check the given 2 graphs G and G' are isomorphic or not.

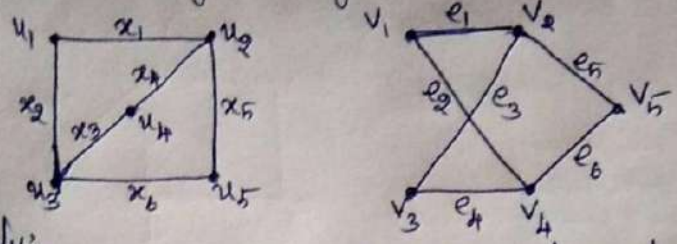


Soln: Both G and G' have same number of vertices (namely 4) and same number of edges. Now, under the mapping. $1 \to u_3$; $2 \to u_1$; $3 \to u_4$; $4 \to u_2$

The edges (1,3) (1,2) (2,4) and (3,4) are mapped into (u_3, u_4) (u_3, u_1) (u_1, u_2) and (u_4, u_2). ∴ Adjacency of vertex sets are satisfied. ∴ G & G' are isomorphic.

Example: 2.

Check the given 2 graphs G and G' are Isomorphic or not.



Soln:

The number of vertices 5 and number of edges 6 are same.

The degree sequence are same. Since in G we have the vertices u_2 & u_3 of degree 3. They must be mapped to the vertices v_2 and v_4 in G'

Define a mapping: $u_1 \to v_1$, $u_3 \to v_2$, $u_5 \to v_3$, $u_2 \to v_4$ and $u_4 \to v_5$

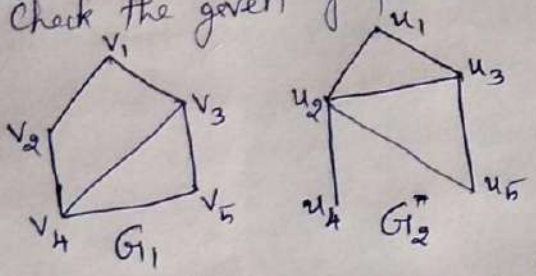
Then the edges x_1, x_2, x_6, x_5, x_3 and x_4 are mapped into e_1, e_2, e_3, e_4, e_5 and e_6

∴ there is 1-1 correspondance between the vertices and edges.

∴ G & G' are isomorphic.

Example: 3

Check the given graphs G_1 and G_2 are isomorphic or not.



Soln:

The number of vertices 5 and number of edges 6 are same.

But there is no one-to-one correspondence between edges in G_1 and G_2.

For, the graph G_1 have the degree sequence 2, 2, 2, 3, 3.

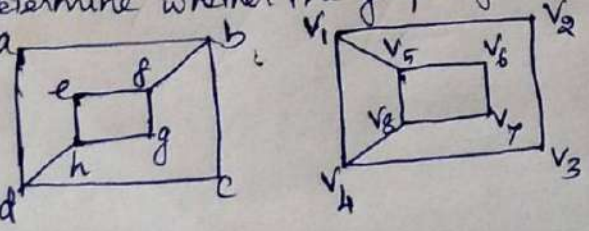
But the graph G_2 have the degree sequence 1, 2, 2, 3 4.

∴ G_1 & G_2 are not Isomorphic.

Example: 4

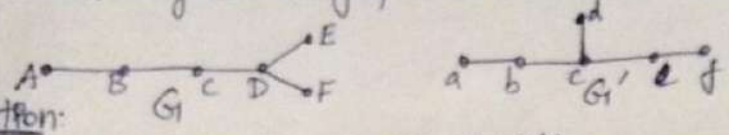
Determine whether the graphs given below are Isomorphic. or not.

H.W



Example: 5

Check the given two graphs G and G' are Isomorphic or not.



Solution:

Here both the graphs G and G' have same number of vertices and edges. But in G, the vertex D is adjacent to two pendent vertices (E & F).

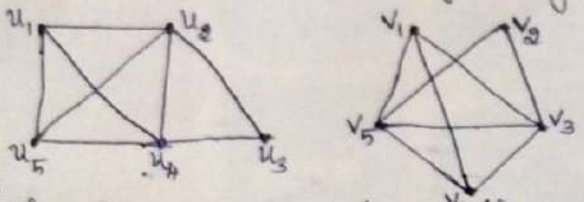
If G and G' were Isomorphic, then the image of this vertex in G' should be adjacent of two pendent vertices in H.

But in G', there is no vertex which is adjacent to two pendent vertices.

Hence G & H are not Isomorphic.

Example: 6

Determine whether the following pairs of graphs are Isomorphic.



Soln: The given 2 graphs have the same number of vertices (5) and same number of edges (8).

If we assign $u_1 \to v_1$; $u_2 \to v_5$; $u_3 \to v_2$; $u_4 \to v_3$; $u_5 \to v_4$.

Then the adjacency is preserved, which is evidently given by their adjacency matrix.

	u_1	u_2	u_3	u_4	u_5
u_1	0	1	0	1	1
u_2	1	0	1	1	1
u_3	0	1	0	1	0
u_4	1	1	1	0	1
u_5	1	1	0	1	0

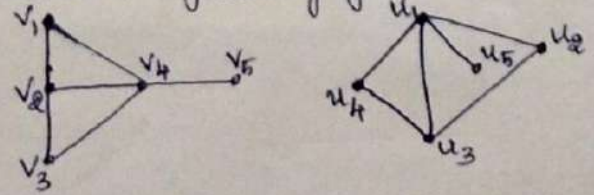
	v_1	v_5	v_2	v_3	v_4
v_1	0	1	0	1	1
v_2	1	0	1	1	1
v_3	0	1	0	1	0
v_4	1	1	1	0	1
v_5	1	1	0	1	0

∴ The given 2 graphs are Isomorphic.

Example: 7.

State whether the following graphs are isomorphic or not.

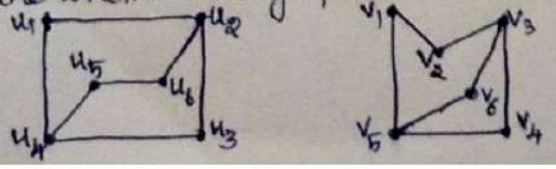
H.W.



Example: 8

Determine whether the graphs G and H are Isomorphic.

H.W.



Isomorphism & Adjacency:

Result: 1

Two graphs are isomorphic, iff their vertices can be labeled in such a way that the corresponding adjacency matrices are equal.

Result: 2

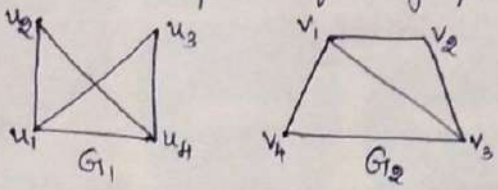
Two simple graphs G_1 and G_2 are isomorphic iff their adjacency matrices A_1 and A_2 are related by $A_1 = P^{-1} A_2 P$ where P is a permutation matrix.

Note:

A matrix whose rows are the rows of the unit matrix, but not necessarily in their natural order, is called permutation matrix.

Example: 1

Test the isomorphism of the graphs by considering their adjacency matrices



Soln:

Let A_1 and A_2 be the adjacency matrices of G_1 and G_2 respectively.

$$A_1 = \begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \\ u_4 \end{array}\begin{array}{c} \begin{array}{cccc} u_1 & u_2 & u_3 & u_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array} \qquad A_2 = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array}\begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

Now,

$$A_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \sim \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \quad C_3 \leftrightarrow C_4$$

$$\sim \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad R_3 \leftrightarrow R_4$$

$\sim A_2$.

Since A_1 & A_2 are similar, the corresponding graphs G_1 and G_2 are isomorphic.

Example: 2

Are the simple graphs with the following adjacency matrices isomorphic?

H.W. $A_1 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$, $A_2 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$

Ans: A_1 & A_2 are not similar

Example: 3

The adjacency matrices of two pairs of graph as given below. Examine the isomorphism of G and H. ~~by finding a permutation matrix.~~

H.W. $A_G = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$, $A_H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

Ans: G & H are isomorphic!

Paths, Reachability and Connectedness

Defn: (Path)
A path in a graph is a sequence $v_1, v_2, v_3, \ldots v_k$ of vertices each adjacent to the next. In other words, starting with the vertex v_1, one can travel along edges $(v_1, v_2), (v_2, v_3), \ldots$ and reach the vertex v_k.

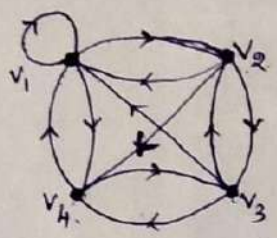
Defn: (Length of the path)
The number of edges appearing in the sequence of a path is called the length of path.

Defn: (Cycle or circuit)
A path which originates and ends in the same node is called a cycle of circuit.

Defn:
A path is said to be simple if all the edges in the path are distinct.

Defn:
A path in which all the vertices are traversed only once is called an elementary path.

Example: 1
Consider the graph:

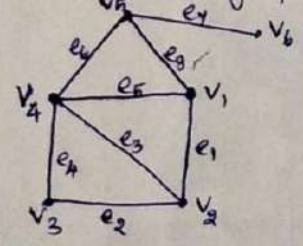


Then some of the paths originating in node v_1 and ending in node v_3 are

$P_1 = (\langle v_1, v_2\rangle, \langle v_2, v_3\rangle)$
$P_2 = (\langle v_1, v_2\rangle, \langle v_2, v_4\rangle, \langle v_4, v_3\rangle)$
$P_3 = (\langle v_1, v_2\rangle, \langle v_2, v_4\rangle, \langle v_4, v_1\rangle, \langle v_1, v_2\rangle, \langle v_2, v_3\rangle)$
$P_4 = (\langle v_1, v_2\rangle, \langle v_2, v_4\rangle, \langle v_4, v_3\rangle)$
$P_5 = (\langle v_1, v_2\rangle, \langle v_2, v_4\rangle, \langle v_4, v_1\rangle, \langle v_1, v_4\rangle, \langle v_4, v_3\rangle)$
$P_6 = (\langle$ [illegible] $, \langle v_1, v_1\rangle, \langle v_1, v_2\rangle, \langle v_2, v_3\rangle)$

Here P_1, P_2, P_4 are elementary path. P_5 is simple but not elementary.

Example: 2
Consider the graph.



From figure, $P_1 = (\langle v_4, v_1\rangle, \langle v_1, v_5\rangle, \langle v_5, v_6\rangle)$ is a path.
$P_2 = (\langle v_3, v_2\rangle, \langle v_2, v_1\rangle, \langle v_1, v_4\rangle, \langle v_4, v_3\rangle)$ is a circuit.
$P_3 = (\langle v_2, v_4\rangle, \langle v_4, v_1\rangle, \langle v_1, v_2\rangle)$ is a circuit.

Defn:
A node 'v' of a simple graph is said to be reachable from the node 'u' of the same graph, if there exist a path from u to v.

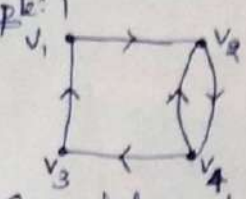
Example: In the above example v_6 is reachable from v_4 by the path P_1.

Defn: (Connected graph)

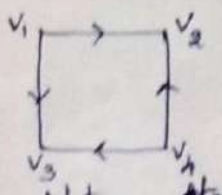
An directed graph is said to be connected if any pair of nodes are reachable from one another. That is, there is a path between any pair of nodes.

A graph which is not connected is called disconnected graph.

Example: 1



Connected graph.

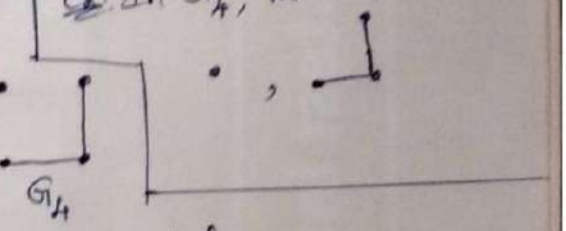


Not connected graph.

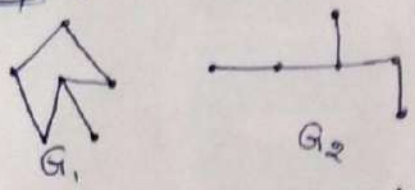
Defn:

The connected subgraphs of a graph G are called components of the graph G.

Ex: In G_4, the components are



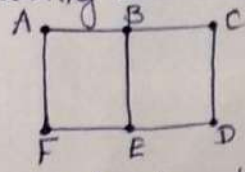
Example: 2



Here G_1 & G_2 are connected and G_3 & G_4 are not connected.

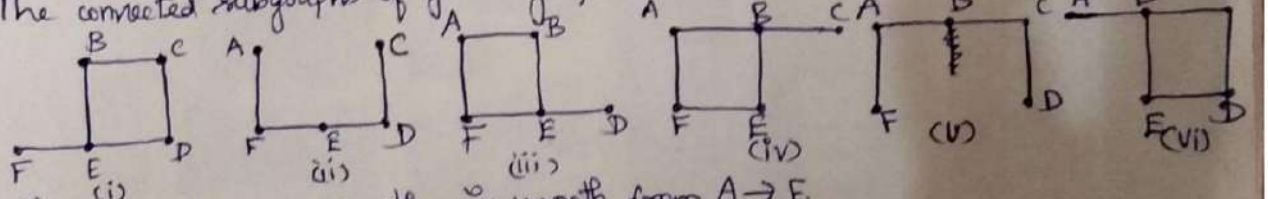
Example: 3

Find all the connected subgraph obtained from the graph given in the following figure, by deleting each vertex. List out the simple paths from A to F in each subgraph.



Soln:

The connected subgraphs of given graphs.



1. In the diagrams (i) & (vi) there is no path from A → F.
2. In the diagrams (ii) & (iv), there is a simple path, A → F
3. In the diagrams (iii) & (v), there are paths A → F and A → B → E → F.

Theorem: 1

If a graph has 'n'-vertices and a vertex 'v' is connected to a vertex 'w', then there exists a path from "v to w" of length not more than (n−1).

Soln:

Let $v, u_1, u_2, \ldots, u_{m-1}, w$ be a path in G from v to w.

By defn. of path, the vertices $v, u_1, u_2, \ldots, u_{m-1}$ and w all are distinct.

As G, contains only 'n'-vertices, it follows that $m+1 \leq n$.

(i.e.) $m \leq n-1$

Hence the proof.

Theorem: 2

A simple graph with n-vertices must be connected if it has more than $\frac{(n-1)(n-2)}{2}$ edges.

Proof:

Let G be a simple graph with n-vertices and more than $\frac{(n-1)(n-2)}{2}$ edges.

T.P G is connected.

Suppose G is not connected, then G must have at least two components

Let it be G_1 & G_2

Let V_1 be the vertex set of G_1 with $|V_1| = m$. If V_2 be the vertex set, then V_2 has $n-m$ vertices. (ie) $|V_2| = n-m \geq 1$.

Also $1 \leq m \leq n-1$ and there is no edge joining a vertex of V_1 and a vertex of V_2.

Now, $|E(G)| = |E(G_1 \cup G_2)|$

$= |E(G_1)| + |E(G_2)|$

$\leq \frac{m(m-1)}{2} + \frac{(n-m)(n-m-1)}{2}$

$= \frac{1}{2}\left[m^2 - m + n(n-m-1) - m(n-m-1)\right]$

$= \frac{1}{2}\left[m^2 - m + n((n-1)-m) - mn + m^2 + m\right]$

$= \frac{1}{2}\left[n(n-1) - nm + m^2 - nm + m^2\right]$

$= \frac{1}{2}\left[n(n-1) - 2nm + 2m^2 + 2(n-1) - 2(n-1)\right]$ [Adding & subtracting $2(n-1)$]

$= \frac{1}{2}\left[(n-1)(n-2) - 2[nm - m^2 - n + 1]\right]$

$= \frac{1}{2}\left[(n-1)(n-2) - 2[n(m-1) - m^2 + 1]\right]$

$= \frac{1}{2}\left[(n-1)(n-2) - 2[n(m-1) - (m-1)(m+1)]\right]$

$= \frac{1}{2}\left[(n-1)(n-2) - 2(m-1)(n-m-1)\right]$

$\therefore |E(G)| \leq \frac{(n-1)(n-2)}{2} - (m-1)(n-m-1)$

$\leq \frac{(n-1)(n-2)}{2}$ $(\because (m-1)(n-m-1) \geq 0$ for $1 \leq m \leq n-1)$

Which is a $\Rightarrow\Leftarrow$ to G has more than $\frac{(n-1)(n-2)}{2}$ edges.

$\therefore$ G is connected.

Theorem: 3

Let G be a simple graph with n-vertices. If $\delta(G) \geq n/2$, then G is connected where $\delta(G)$ is minimum degree of the graph G.

Proof:

Let G be a simple graph with n-vertices and $\delta(G) \geq n/2$, where $\delta(G)$ is minimum degree of the graph G.

T.P G is connected.

Let u & v be any two distinct vertices in the graph G.

Now, it is enough to prove that, there is a u-v path in G.

If there is an edge between u & v, then there is nothing to prove.

Suppose uv is not an edge of G, then $X^{\&Y}$ be the set of all vertices which are adjacent to u & v respectively.

Then $u, v \notin X \cup Y$ (∵ G is a simple graph i.e it has no loop).

$$\Rightarrow |X \cup Y| \leq n-2 \rightarrow (1)$$

Now, we have $|X| = \deg u \geq \delta(G) \geq n/2$ and

$$|Y| = \deg v \geq \delta(G) \geq n/2$$

$$\Rightarrow |X| + |Y| \geq n/2 + n/2 \geq n-1 \rightarrow (2)$$

W.K.T,

$$|X \cup Y| \geq |X| + |Y| - |X \cap Y|$$

$$n-2 \geq n-1-|X \cap Y| \quad (\text{By } (1) \& (2))$$

$$\Rightarrow -1 \geq -|X \cap Y|$$

$$\Rightarrow 1 \leq |X \cap Y| \Rightarrow X \cap Y \neq \phi$$

Let $w \in X \cap Y$.

Then uwv is a path between u & v in G

Thus every pair of distinct vertices of G, there is a path between them.

Hence G is connected.

Theorem: 4

A simple graph with n-vertices and k components can have atmost $\frac{(n-k)(n-k+1)}{2}$ edges.

Proof:

Let G be a simple graph with n-vertices and k components.

Let $n_1, n_2, \cdots n_k$ be the number of vertices in each of k-components of the graph G.

Then $n_1+n_2+\cdots+n_k = n = v(G)$.

(ie) $\sum_{i=1}^{k} n_i = n \rightarrow (1)$

Now, $\sum_{i=1}^{k} (n_i-1) = (n_1-1)+(n_2-1)+\cdots+(n_k-1)$

$= \sum_{i=1}^{k} n_i - k = n-k$ (By (1))

Squaring on both sides,

$\left[\sum_{i=1}^{k} (n_i-1)\right]^2 = (n-k)^2$

$(n_1-1)^2+(n_2-1)^2+\cdots+(n_k-1)^2 \le n^2+k^2-2nk$

$\Rightarrow n_1^2+1-2n_1+n_2^2+1-2n_2+\cdots+n_k^2+1-2n_k \le n^2+k^2-2nk$

$\Rightarrow \sum_{i=1}^{k} n_i^2 + k - 2n \le n^2+k^2-2nk$

$\Rightarrow \sum_{i=1}^{k} n_i^2 \le n^2+k^2-2nk+2n-k$

$= n^2+k(k-1)-2n(k-1)$

$= n^2+(k-1)(k-2n)$

$\therefore \sum_{i=1}^{k} n_i^2 \le n^2+(k-1)(k-2n) \rightarrow (2)$

Since G is simple graph, the maximum number of edges of G in its components is $\frac{n_i(n_i-1)}{2}$

$\therefore$ Maximum no. of edges of $G = \sum_{i=1}^{k} \frac{n_i(n_i-1)}{2}$

$= \sum_{i=1}^{k} \left(\frac{n_i^2-n_i}{2}\right)$

$= \frac{1}{2}\sum_{i=1}^{k} n_i^2 - \frac{1}{2}\sum_{i=1}^{k} n_i$

$\le \frac{1}{2}(n^2+(k-1)(k-2n)) - \frac{n}{2}$ (By (1) & (2))

$= \frac{1}{2}(n^2-2nk+k^2-k+2n-n)$

$= \frac{1}{2}((n-k)^2+n-k)$

$= \frac{1}{2}(n-k)(n-k+1)$ //.

Hence Proved. //.

Example:
If the simple graph G has 'v' vertices and 'e' edges, how many edges does G^c have?

Soln:
W.K.T, $|E(G \cup G^c)| = \frac{v(v-1)}{2}$

$\Rightarrow |E(G)| + |E(G^c)| = \frac{v(v-1)}{2}$

$\Rightarrow e + |E(G^c)| = \frac{v(v-1)}{2} \Rightarrow |E(G^c)| = \frac{v(v-1)}{2} - e$.

$\therefore G^c$ has $\frac{v(v-1)}{2} - e$ edges.

For example, If G has 4 vertices & 5 edges then the num of edges in G^c is $\frac{4(4-1)}{2} - 5 = 6 - 5 = 1$ edge.

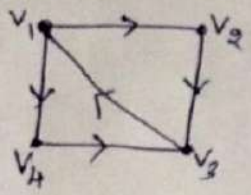
Defn:
A simple digraph is said to be Unilaterally connected, if for any pair of nodes of the graph atleast one of the nodes of the pair is reachable from the other node.

Defn:
A simple digraph is said to be strongly connected, if for any pair of nodes of the graph both the nodes of the pair are reachable from one another.

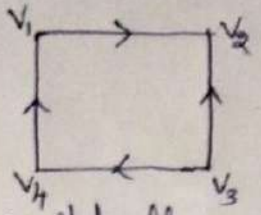
Defn:
We call a digraph is weakly connected, if it is connected as an undirected graph in which the direction of the edges is neglected.

Note:
1. A unilaterally connected digraph is weakly connected; but a weakly connected digraph is not necessarily unilaterally connected.
2. A strongly connected digraph is both unilaterally and weakly connected.
3. In a simple digraph, G = (V, E), every node of the digraph lies in exactly one strong component.

Example:



Strongly connected.

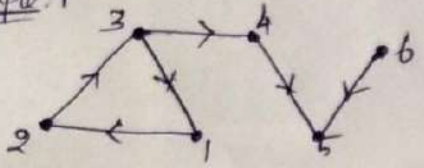


Unilaterally connected.

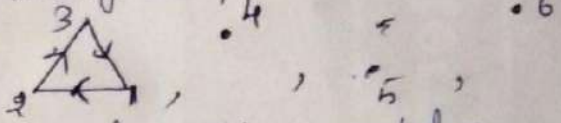
Defn:

For a simple di graph, a maximal strongly connected subgraph is called strong component.

Example: 1

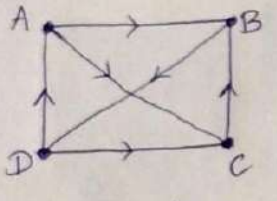


The strong components are



Example: 2

Check the given graph is strongly connected, weakly connected & unilaterally connected or not



G1

Soln:

Paths for the vertices (A,B) is

(i) $A \to B$ (ii) $B \to D \to A$

Paths for the vertices (A,D) is

(i) $A \to B \to D$ (ii) $D \to A$

Paths for the vertices (A,C) is

(i) $A \to C$ (ii) $C \to B \to D \to A$

Paths for the vertices (B,C) is

(i) $B \to D \to C$ (ii) $C \to B$

Paths for the vertices (B,D) is

(i) $B \to D$ (ii) $D \to A \to B$

Paths for the vertices (C,D) is

(i) $C \to B \to D$ (ii) $D \to C$

Since there is a path from each of the possible pairs of vertices of A,B,C,D given graph is strongly connected.

Since G1 is strongly connected, it is both weakly and unilatelly connected.

Euler Graph and Hamilton graph

Defn: Euler Path

A path of a graph G is called an Eulerian path, if it contains each edge of the graph exactly once.

Defn Eulerian circuit or Eulerian cycle.

A circuit or cycle of a graph G is called an Eulerian circuit or cycle, if it includes each edge of G exactly once.

Here starting and end vertex are same.

(or) An Eulerian circuit or cycle should satisfies the following conditions

(i) Starting and ending points are same

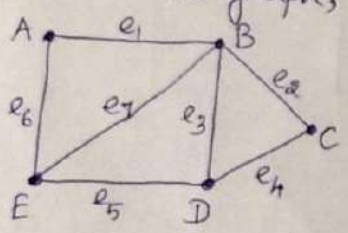
(ii) Cycle should contain all the edges of graph but exactly once.

Defn: Eulerian graph or Euler graph

Any graph containing an Eulerian circuit or cycle is called an Eulerian graph.

Example: 1

Consider the graph,



Then, the Euler path between E and D, namely

E – D – C – B – A – E – B – D

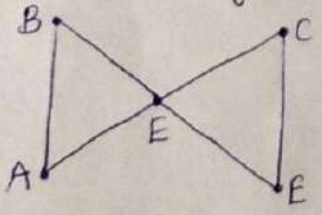
The above path consist of edges $e_5 e_4 e_2 e_1 e_6 e_7 e_3$ exactly one.

For the above graph, we can not find Eulerian circuit (cycle)

∴ The given graph is non- Eulerian.

Example: 2

Check the given graph is Euler or not



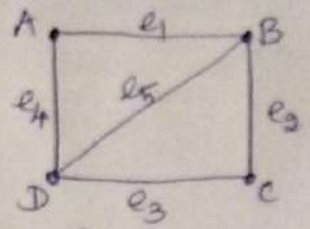
Solu: Consider the cycle A – E – C – D – E – B – A

Since, it includes each of the edges exactly once, the above cycle is an Eulerian cycle.

Since the graph contains Eulerian cycle, it is an Euler graph.

Example: 3

Find all the possible Eulerian path of the given graph. Is it Euler graph?



Sol:

Possible Euler paths are.

1. B e_5 D e_3 C e_2 B e_1 A e_4 D
2. B e_2 C e_3 D e_4 A e_1 B e_5 D
3. B e_1 A e_4 D e_3 C e_2 B e_5 D
4. D e_3 C e_2 B e_1 A e_4 D e_5 B
5. D e_5 B e_2 C e_3 D e_4 A e_1 B
6. D e_4 A e_1 B e_2 C e_3 D e_5 B

Here we cannot find Eulerian cycle.

∴ The given graph is not an Euler graph.

Theorem:

A connected graph is Euler graph (contains Eulerian circuit) iff each of its vertices is of even degree.

[Necessary and sufficient condition for Euler graph.]

Proof:

Let G be Eulerian graph.

T.P All the vertices of G are even degree.

Since G is Eulerian, G has a closed path containing all the edges.

Let V be a vertex in G.

Then every time a path ~~needs~~ a contains a vertex, it needs 2 new edges incident on V, one is for enter and other is for exit.

This is true for all vertices, because the path is closed.

∴ the degree of every vertex is even.

Conversely,

Suppose every vertices of G are of even degree.

T.P G is Eulerian.

ie) T.P G has an Euler circuit.

(ie) T.P G contains a closed path which covers all the edges.

Now, construct a closed path Σ starting at an arbitrary vertex V and going through the edges of G with no repeated edges.

Since each vertex is of even degree, it contain an edge for every vertex where we enter. The tracing can stop only at vertex V becomes an Euler Circuit.

(ie) If the closed path Σ we just traced includes all the edges of G, then G is an Euler graph.

If not, we remove all the edges in the closed path Σ from G, then we get a subgraph Σ' of G.

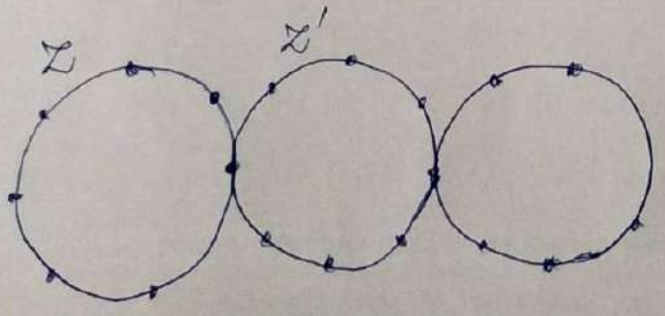
Since every vertex in G are of even degree, the degree of the vertices Σ' are also even and Σ' must touchs Σ atleast at one vertex say u, because G is connected.

Starting from u, we construct a new closed path in Σ'. As all the vertices in Σ' is of even degree, the closed path ends at u.

This closed path in Σ' combined with Σ forms a new closed path, which starts and ends at the vertex v and has more edges than Σ.

This process is repeated till we obtain a closed walk that traces all the edges of G.

Hence G is an Euler graph.



H.W

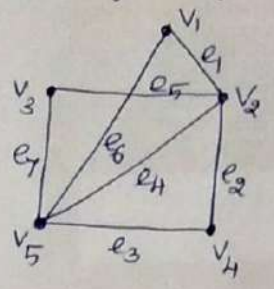
1. Check the following are Eulerian graph or not (i) complete graph K_5 (ii) Complete Bipartite graph $K_{2,3}$.
2. Check the following are Eulerian or not.

(i) 

(ii) 

Example: 1

Check the given graph is Euler graph or not.



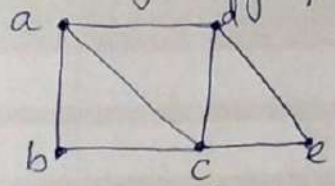
Solu:

$\deg(v_1) = 2$; $\deg(v_2) = 4$; $\deg(v_3) = 2$; $\deg(v_4) = 2$; $\deg(v_5) = 4$.

Since, all the vertices is of even degree, by the above theorem, the given graph is Euler graph.

Exaple: 2

Check the given graph is Euler or not.



Solu:

$\deg(a) = 3$; $\deg(b) = 2$; $\deg(c) = 4$; $\deg(d) = 3$, $\deg(e) = 2$.

Here degree of the vertices a & d are not even.

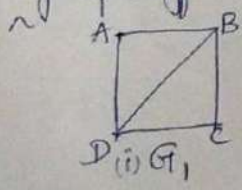
∴ By the above theorem, the given graph is not an Euler graph.

Note:

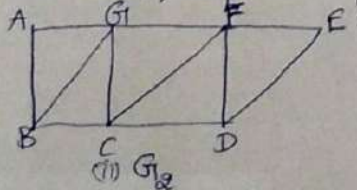
A connected graph has an Euler path but not an Euler circuit iff it has exactly two vertices of odd degree.

Example: 3

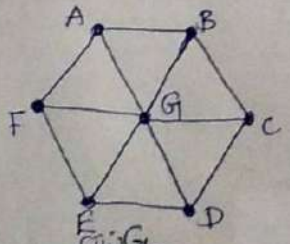
Find an Euler path and an Euler circuit, if it exists in each of the three following graphs. If it does not exist, explain why?



(i) G_1



(ii) G_2



(iii) G_3

Solu:

(i) In G_1, the vertices B & D have odd degree namely 3

∴ G_1 has exactly two vertices (B & D) of odd degree.

∴ By the above note, G_1 have an Euler path which have an end points as B & D and does not have an Eulerian circuit.

The Euler path is D – A – B – C – D – B

Since Eulerian circuit does not exist, G_1 is not an Euler graph.

(ii) G_2 has exactly two vertices of odd degree namely B & D. So it has an Eulerian path that must have B & D as end points and does not have an Euler circuit.

The Euler path is B – A – G – F – E – D – C – G – B – C – F – D

Since G_2 does not have Euler circuit, G_2 is not an Euler graph.

(iii) In G_3, there are 6 vertices of odd degree.

Hence by the above note, G_3 contains neither an Euler path nor an Euler circuit.

∴ G_3 is not an Euler graph.

Theorem: 2

If a graph G has not more than two vertices of odd degree, then there can be Euler path in G.

Proof:

Let the odd degree vertices be labelled as v and w in any arbitrary order. Add an edge to G between the vertex pair (v, w) to form a new graph G'.

Now every vertex of G' is of even degree and hence G' has an Eulerian path T.

If the edge that we added to G is now removed from T, it will split into an open path containing all edges of G which is nothing but an Euler path in G.

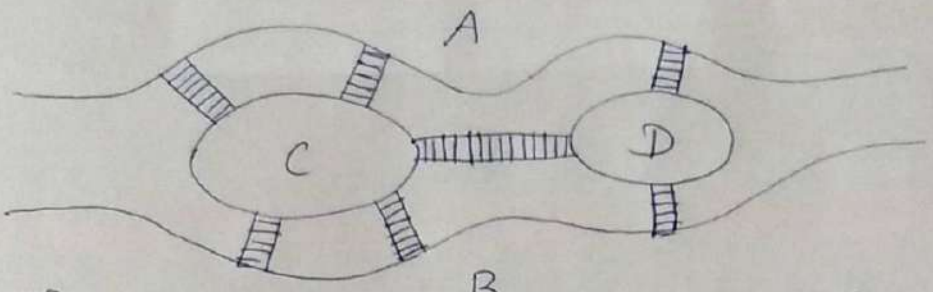
Hence the proof.

The Konigsberg Bridge Problem

Qn. Explain Konigsberg bridge problem. Represent the problem by mean of graph. Does the problem have a solution?

Solu.

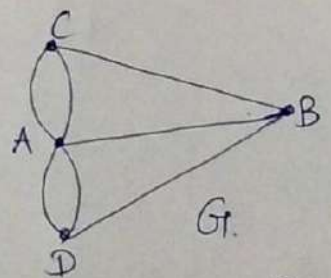
There are two islands A and B formed by a river. They are connected to each other and to the river banks C and D by means of 7 bridges, as shown below.



The problem is to start from anyone of the 4 land areas A, B, C, D & walk across each bridge exactly once and return to the starting point.

This problem is the famous Konigsberg bridge problem. [Euler proves this problem has no solution].

When the situation is represented by a graph, with vertices representing the land areas and the edges representing the bridges, the graph will be as shown below.



G.

Suppose this graph G is Eulerian, then the graph has a solution.

By the defn of Eulerian graph, G must contain an Eulerian cycle. But G has not Eulerian cycle, since the vertices C & D has degree 3, an odd number.

∴ G is not Eulerian graph.

Hence, Konigsberg bridge problem has no solution.

Hamiltonian Graph:

Defn: Hamiltonian path.

A path of a graph G is called a Hamiltonian path, if it includes each vertex of G exactly once.

Defn: Hamiltonian cycle or circuit

A circuit (cycle) of a graph G is said to be a Hamiltonian circuit (cycle), if it includes each vertex of G exactly once except the starting and ending vertices.

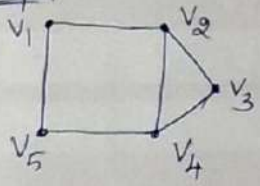
Note:

In Hamiltonian circuit the starting and ending vertex are same.

Defn: Hamiltonian Graph.

Any graph containing a Hamiltonian circuit or cycle is called a Hamiltonian graph.

Example:



Then $V_1 - V_2 - V_3 - V_4 - V_5$ is a Hamiltonian path (∵ All the vertices appears exactly once).

$V_4 - V_3 - V_2 - V_1 - V_5 - V_4$ is a Hamiltonian cycle [∵ All the vertices appears exactly once not all the edges] and starting & ending vertex are same.

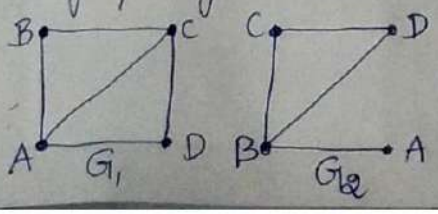
Note:

In the above example, $V_5 - V_2 - V_3 - V_4$ is a path but not a Hamiltonian path.

$V_5 - V_2 - V_3 - V_4 - V_5$ is a cycle but not a Hamiltonian cycle. (Since the vertices V_1 is not included in the cycle, it is not a Hamiltonian cycle).

Example: 1

Find Hamiltonian path and Hamiltonian cycle, if it exists in each of the graphs given below. Also identify which graph is Hamiltonian.



Soln:

For G_1, the possible Hamiltonian paths are

(i) A – B – C – D
(ii) A – D – C – B
(iii) B – C – D – A
(iv) B – A – D – C
(v) C – D – A – B
(vi) C – B – A – D
(vii) D – A – B – C
(viii) D – C – B – A

The possible Hamiltonian cycles are

(i) A – B – C – D – A
(ii) A – D – C – B – A
(iii) B – C – D – A – B
(iv) B – A – D – C – B
(v) C – D – A – B – C
(vi) C – B – A – D – C
(vii) D – A – B – C – D
(viii) D – C – B – A – D

Since all the vertices appears exactly once, but not all the edges.

Since G_1 contains Hamiltonian cycle, G_1 is a Hamiltonian graph.

For G_2, the possible Hamiltonian paths are

(i) A – B – C – D
(ii) A – B – D – C
(iii) D – C – B – A ...etc.

We cannot find a Hamiltonian cycle in G_2

∴ G_2 is not a Hamiltonian graph.

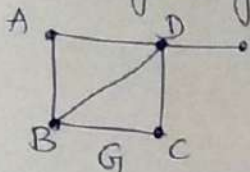
From the above example, we can list out the following properties.

Properties:

1. A Hamiltonian circuit contains a Hamiltonian path, but a graph containing a Hamiltonian path need not have a Hamiltonian cycle.
2. By deleting any one edge from Hamiltonian cycle, we can get Hamiltonian path.
3. A graph may contain more than one Hamiltonian cycle.
4. A complete graph K_n, will always have a Hamiltonian cycle, when $n \geq 3$.

Example: 2

Check the given graph is Hamiltonian or not.



Solu: In G_1, for the vertex E, degree is 1.

∴ There is no Hamiltonian cycle in G.

∴ G is not a Hamiltonian graph.

Example: 3

Show that the complete graph K_n with $n \geq 3$ has Hamiltonian cycle. Obtain a ~~the~~ edge disjoint Hamiltonian cycles in K_7. Is it Hamiltonian? and is Eulerian?

Solu:

I.P The complete graph K_n, $n \geq 3$ contains a Hamiltonian cycle.

Let u be any vertex on K_n.

Since K_n is a complete graph with n vertices, any 2 vertices are adjacent.

So we start from the vertex u and visit all the vertices in any order exactly once and come back to u.

∴ There is a Hamiltonian cycle in K_n. ⇒ K_n is a Hamiltonian with $n \geq 3$.

Now, consider the complete graph K_7.

It has two edge disjoint Hamiltonian cycles.

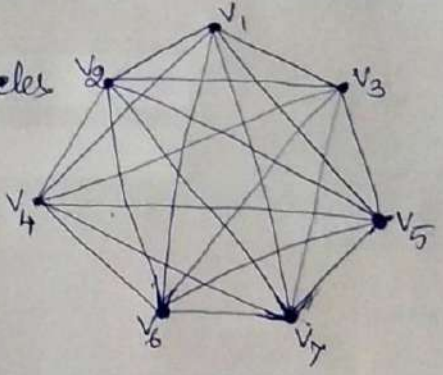
The two Hamiltonian cycles are

$V_1 - V_2 - V_3 - V_4 - V_5 - V_6 - V_7 - V_1$ and

$V_1 - V_3 - V_6 - V_2 - V_4 - V_7 - V_5 - V_1$.

∴ K_7 is Hamiltonian graph and

K_7 is Eulerian graph.



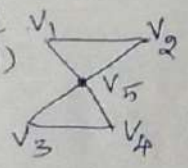
Example: 4

Give an example of a graph

(i) Eulerian but not Hamiltonian (ii) Not Eulerian but Hamiltonian (iii) Both Eulerian & Hamiltonian. (iv) Neither Eulerian nor Hamiltonian.

Solu:

(i)



Eulerian: (no repeated edges)

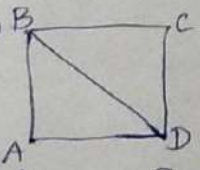
(i) all of even degrees.

(ii) cycle: $V_1 - V_2 - V_5 - V_3 - V_4 - V_5 - V_1$

Hamiltonian: (no repeated vertices)

The Hamiltonian cycle does not exist.

(ii)



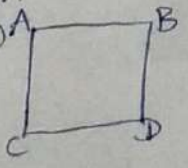
Eulerian:

Since B & D has odd degrees, it is not Eulerian.

Hamiltonian:

It is has the hamiltonian cycle A-B-C-D-A.

(iii)



Eulerian:

All of even degree & the Eulerian cycle is A-B-D-C-A.

It is an Eulerian graph.

Hamiltonian:

Hamiltonian cycle is A-B-D-C-A. It is a Hamiltonian graph.

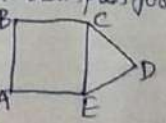
∴ Both Eulerian & Hamiltonian.

(iv)

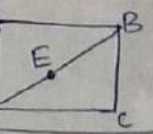
Eulerian: A & B has odd degree. ∴ It is not an Eulerian graph.

Hamiltonian: There is no Hamiltonian cycle. ∴ It is not an Hamiltonian graph.

Another examples for (i) & (iv) are (i)



(iv)



S. Meera Sudharsana
Reyathi
AP/Mathematics.

Unit-IV

Algebraic Structures (Group Theory)

Groups.

Notations:

$\mathbb{N} = \{1, 2, 3, \ldots, \infty\}$ → set of all natural numbers.

$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ → set of all integers.

$\mathbb{Z}_+ = \{0, 1, 2, \ldots\}$ → set of all positive integers.

$\mathbb{R} = (-\infty, \infty)$ → set of all real numbers.

$\mathbb{R}_+$ → set of all positive real numbers.

$\mathbb{Q} \to \mathbb{R}_q$ if $q < p$ → set of all fraction numbers.

$E = \{2, 4, \ldots, \infty\}$ → set of all even numbers.

$\mathbb{C} = \{\alpha + i\beta : \alpha, \beta \in \mathbb{R}\}$ → set of all complex numbers.

$\oplus_n$ → Addition modulo 'n'

$\otimes_n, \odot_n$ → under multiplication modulo 'n'

Defn: Group. $[G, \star]$

Let G be the group under the binary operation '$\star$' satisfies the following properties.

(i) **Closure:**
$a \star b \in G$ where $\forall a, b \in G$.

(ii) **Associative:**
$(a \star b) \star c = a \star (b \star c)$. where $a, b, c \in G$.

(iii) **Identity:**
'e' is the identy element.
$a \star e = e \star a = a$

(iv) **Inverse:**
'$\bar{a}$' is the inverse element.
$a \star \bar{a} = \bar{a} \star a = e \quad \forall a \in G$
(OR) $a \star \frac{1}{a} = \frac{1}{a} \star a = e \quad \forall a \in G$.

Results:

(i) In $(G,+)$ identity element $e=0$

(ii) In $(G,\times)$ identity element $e=1$. [or $(G,\cdot)$]

(iii) In $(G,+)$ inverse of $a = -a$

(iv) In $(G,\times)$ or $(G,\cdot)$ inverse of $a = \frac{1}{a}$.

Example:

$(\mathbb{Z},+)$ is a group.

Solu:

Let $G = \mathbb{Z} = \{0, \pm1, \pm2, \pm3, \ldots\}$

(i) **Closure:**

Let $a=1$, $b=3 \in G$

$\therefore a+b = 1+3 = 4 \in G$.

Let $a=-2$, $b=+4 \in G$

$a+b = -2+4 = 2 \in G$.

$\therefore (\mathbb{Z},+)$ satisfies closure property.

(ii) **Associative:**

Let $a=1$, $b=-2$, $c=3 \in G$.

$$a+(b+c) = 1+(-2+3) = 2 \in G.$$

$$(a+b)+c = (1-2)+3 = 2 \in G.$$

$\therefore a+(b+c) = (a+b)+c$

$\therefore (\mathbb{Z},+)$ satisfies associative.

(iii) **Identity:**

$e=0 \in \mathbb{Z}$ is the identity elemen under '+'.

Let $a \in \mathbb{Z}$.

$\Rightarrow a+e = a+0 = a$.

$\therefore (\mathbb{Z},+)$ satisfies Identity

(iv) **Inverse:**

$a' = -a \in G$ is the inverse of a.

$\Rightarrow a-a = e$; $\therefore (\mathbb{Z},+)$ satisfies Inverse.

Hence $(\mathbb{Z},+)$ is a group.

Example: [Non-group]

$(\mathbb{N}, +)$ is not a group.

Sol:

Now, $\mathbb{N} = \{1, 2, 3, \ldots\}$

Since $e = 0 \notin \mathbb{N}$,

$(\mathbb{N}, +)$ is not a group.

Defn: Abelian Group (or) Commutative Group.

A group G is said to be abelian, if it satisfies the following properties.

(i) Closure., If $a, b \in G \Rightarrow a * b \in G$

(ii) Associative, If $a, b, c \in G \Rightarrow (a * b) * c = a * (b * c)$

(iii) Identity., $\exists\, e \in G$ such that $e * a = a * e = a \;\forall\, a \in G$.

(iv) Inverse, $\exists\, a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e \;\forall\, a \in G$.

(v) Commutative. If $a, b \in G \Rightarrow a * b = b * a$.

Ex: $(\mathbb{R}, +)$ is an abelian group.

Defn: Semi Group.

A non-empty set 'S' together with a binary operation. It satisfies the following properties.

(i) closure.

(ii) Associative.

Ex: $(\mathbb{Z}, +)$ is a semi group.

Defn: Monoid.

A non-empty set M together with a binary operation '$*$' satisfies the following properties is a monoid.

(i) Closure

(ii) Associative

(iii) Identity.

Ex: $(\mathbb{Z}, +)$ is a Monoid.

Theorem: 1

If $(G, \star)$ is an abelian group, then for all $a, b \in G$, $(a \star b)^n = a^n \star b^n$

Proof:

Let $(G; \star)$ be an abelian group.

T.P $(a \star b)^n = a^n \star b^n \ \forall\ a, b \in G$.

We poove this by induction.

Case(i) Let $n = 0$.

Then $a^0 = e$, $b^0 = e$, $(a \star b)^0 = e$

$\therefore (a \star b)^0 = a^0 \star b^0$.

Let n be a positive integer.

Let $n = 1$.

Then $a^1 = a$, $b^1 = b$, $(a \star b)^1 = a \star b$

$\therefore (a \star b)^1 = a^1 \star b^1$

$\therefore$ The result is true for $n = 0$ & 1.

Case(ii). Assume the result for $n = k$.

$\therefore (a \star b)^k = a^k \star b^k \ \forall\ a, b \in G$ ——① & k is a +ve integer.

Now, $(a \star b)^{k+1} = (a \star b)^k \star (a \star b)$

$= a^k \star b^k \star (a \star b)$

$= a^k \star b^k \star (b \star a)$

$= a^k \star (b^k \star b) \star a$

$= a^k \star b^{k+1} \star a$.

$= (a^k \star a) \star b^{k+1}$

$= a^{k+1} \star b^{k+1}$

$\therefore$ The result is true for $n = k+1$ also.

∴ By principle of Induction, the theorem is true for $n = 1, 2, 3, \ldots$

Case (iii) Let n be a negative integer.

Let $n = -m$, where m is a +ve integer.

Now, $(a \star b)^n = (a \star b)^{-m}$

$= [(a \star b)^m]^{-1}$

$= [a^m \star b^m]^{-1}$ by case (ii)

$= [b^m \star a^m]^{-1} = (a^m)^{-1} \star (b^m)^{-1}$

$= a^{-m} \star b^{-m}$

$= a^n \star b^n$.

Hence $(a \star b)^n = a^n \star b^n \quad \forall\, n \in \mathbb{Z}$.

Theorem:

A group $(G, \star)$ is abelian iff $(a \star b)^2 = a^2 \star b^2$

Proof:

Assume that G is abelian.

Then $a \star b = b \star a \quad \forall\, a, b \in G$. → ①

Now, $(a \star b)^2 = (a \star b) \star (a \star b)$

$= a \star (b \star a) \star b$

$= a \star (a \star b) \star b$ (by ①).

$= a \star a \star b \star b$

$= a^2 \star b^2$

Conversely, Suppose $(a \star b)^2 = a^2 \star b^2 \quad \forall\, a, b \in G$.

T.P. $(G, \star)$ is abelian group.

Now, $(a \star b)^2 = a^2 \star b^2$

$\Rightarrow a \star b \star a \star b = a \star a \star b \star b$.

$\Rightarrow b \star a \star b = a \star b \star b$ [By left cancellation law]

$\Rightarrow b \star a = a \star b$ [By Right cancellation law]

$\therefore$ G is abelian.

— × — × — × —

Theorem: 3

Show that if every element in a group is its own inverse, then the group must be abelian. (OR)

For any group $(G, \star)$ if $a^2 = e$ with $a \neq e$, then G is abelian.

Proof:

Given $a = a^{-1}$ for all $a \in G$.

Let $a, b \in G$. Then $a = a^{-1}$ and $b = b^{-1}$

Now, $(a \star b) = (a \star b)^{-1}$

i.e) $a \star b = b^{-1} \star a^{-1}$

$= b \star a$

$\therefore$ G is abelian.

— × — × —

Theorem: 4

The identity element of a group is unique.

Proof:

Let $(G, *)$ be a group.

Let e_1 and e_2 be two identity elements in G.

Then, $e_1 * e_2 = e_1$ [$\because e_2$ is the identity.]

$e_1 * e_2 = e_2$ [$\because e_1$ is the identity]

Thus $e_1 = e_2$.

Hence the identity is unique

——— × ———.

Theorem: 5

For any element a in a group G, the inverse in unique.

Proof:

Let 'a' be any element of a group G.

If possible let a' and a'' be two inverses of a.

Then $a * a' = a' * a = e$ ——→①

$a * a'' = a'' * a = e$. ——→②

Now, $a' = a' * e = a' * (a * a'')$

$= (a' * a) * a''$

$= e * a''$

$= a''$

Hence the inverse in unique.

——— × ——— × ———.

Example:

Let G be a group and $a, b \in G$. Then

(i) $(a^{-1})^{-1} = a$.

(ii) $(a * b)^{-1} = b^{-1} * a^{-1}$

Soln:

(i) Given a^{-1} is the inverse of a.

$\therefore a * a^{-1} = a^{-1} * a = e$

$\therefore a$ is the inverse of a^{-1}

(i.e) $(a^{-1})^{-1} = a$.

(ii) $(a * b) * b^{-1} * a^{-1} = a * (b * b^{-1}) * a^{-1}$

$= a * e * a^{-1}$

$= a * a^{-1}$

$= e$

and $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$

$= b^{-1} * e * b$

$= b^{-1} * b$

$= e$

$\therefore (a * b)^{-1} = b^{-1} * a^{-1}$.

— × — . × — .

Example: Prove that the identity element is the only idempotent element of a group.

Soln: Given $(G, *)$ is a group.

Since $e * e = e$, e is idempotent.

Let a be any idempotent element of G.

Then $a * a = a$

Now, $e * a = a$ [∵ e is the identity element]

It follows that $a * a = e * a$.

By right cancellation law, we have $a = e$.

and so e is the only idempotent element.

———×———×———.

Example:

In a group G prove that an element $a \in G$ such that $a^2 = e$, $a \neq e$ iff $a = a^{-1}$

Soln:

Let us assume that $a = a^{-1}$

Then $a^2 = a * a = a * a^{-1} = e$

Conversely assume that, $a^2 = e$ with $a \neq e$.

(i.e) $a * a = e$.

(i.e) $a^{-1} * a * a = a^{-1} * e$.

(i.e) $e * a = a^{-1}$

(i.e) $a = a^{-1}$

———×———×———.

Theorem: 6

If $(G, *)$ is a finite group of order n, then for any $a \in G$, we must have $a^n = e$, where e is the identity of the group G.

Proof:

Let $O(G) = n$

Let $a \in G$.

Then order of the subgroup $\langle a \rangle$ is the order of the element a.

If $O(\langle a \rangle) = m$, then $a^m = e$ and by Lagrange's theorem, we get m/n.

Let $n = mk$

Then $a^n = a^{mk} = (a^m)^k = e^k = e$.

——— × ——— × ——— × ———

8 marks.

Problem:

Every group of order 4 is abelian.

Soln:

Let $(G, *)$ be a group of order 4 where $G = \{e, a, b, c\}$.

Since G is of even order, there exists at least one element (say) a such that $a^{-1} = a$.

Then two cases arise

(i) $b^{-1} = b$, $c^{-1} = c$

(ii) $b^{-1} = c$, $c^{-1} = b$.

Case(i) $e^{-1} = e$, $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$.

Every element as its own inverse.

$\therefore (G, *)$ is abelian.

Case (ii) $a^{-1} = a$, $b^{-1} = c$, $c^{-1} = b$

$\therefore a^2 = e$, $b * c = e$, $c * b = e$.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Since $(G, *)$ is a group, its elements will appear in a row (column) only once.

Since a, e appears in the second row and b appears in the third column, c will appear as $(2, 3)^{th}$ element.

$\therefore (2,4)^{th}$ element is b
$(3,3)^{th}$ element is a
$(3,2)^{th}$ element is c
$(4,2)^{th}$ element is b
$(4,4)^{th}$ element is a

The table is symmetric about leading diagonal and so $(G, *)$ is abelian.

Hence a group of order 4 is abelian.

Problem:

Show that $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \neq 0 \in \mathbb{R} \right\}$ is an abelian group under matrix multiplication.

Soln:

Given $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \neq 0 \in \mathbb{R} \right\}$

(i) Closure

Let $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in G$.

Then $AB = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in G$

(ii) Commutative

$AB = BA$ is true $\forall A, B \in G$, since

$AB = BA = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$ [$\because ab = ba$ is true in $\mathbb{R}$]

(iii) Associative

Matrix multiplication is associative.

(iv) Identity

$I = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in G$ is the identity in G, since

$AI = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = A \ \forall A \in G$.

(v) Inverse

$A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in G$.

Then $A^{-1} = \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} \in G$ is the inverse of A,

since $AA^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 1$ [$\because a \neq 0 \in \mathbb{R} \Rightarrow 1/a \neq 0 \in \mathbb{R}$]

Hence G is an abelian group under matrix multiplication.

Problem:

Show that the set of matrices

$G = \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \alpha \in \mathbb{R} \right\}$ forms a group under matrix multiplication.

Solu:

Let $G = \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \alpha \in \mathbb{R} \right\}$

(i) Closure.

Let $A_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$, $A_\beta = \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \in G$.

Then $A_\alpha A_\beta = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix}$

$$= \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -(\cos\alpha\sin\beta + \sin\alpha\cos\beta) \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{pmatrix}$$

$$= \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix}$$

$A_\alpha \cdot A_\beta = A_{\alpha+\beta} \in G$. $\longrightarrow$ (1)

(ii) Associative.

Matrix multiplication is associative.

(iii) Identity.

$I_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity in G.

Since $A_\alpha I_0 = I_0 A_\alpha = A_\alpha$ for $A_\alpha \in G$.

(iv) Inverse.

$A_{-\alpha}$ is the iverse of A_α for each $A_\alpha \in G$,

Since $A_\alpha A_{-\alpha} = A_{\alpha+(-\alpha)} = A_0 = I_0$, (using (1))

Hence G is a group.

Permutation Functions

Defn: A bijection from a set A to itself is called a permutation of A.

Theorem: If $A = \{a_1, a_2, \ldots a_n\}$ is a set containing n-elements then there are $n! = n(n-1)\ldots 2.1$ permutations of A.

Problem:

Let $A = \{1, 2, 3, 4, 5, 6\}$ and $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$ be a permutation of A.

(a) Write p as a product of disjoint cycles.
(b) Compute p^{-1}
(c) Compute p^2
(d) Find the period of p, that is, the smallest positive integer k such that $p^k = 1_A$.

Soln:

(a) Given $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$

Since $p(1) = 2$, $p(2) = 4$ and $p(4) = 1$, we write $p = (1, 2, 4)$ as the other elements are fixed.

(b) $p^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}$

(c) $p^2 = p \circ p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix} \circ$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}$

(d) $p^3 = p^2 \circ p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = 1_A$.

$p^4 = p$, $p^5 = p^2$ etc. ....

$\therefore$ The period of $p = 3$.

~~$(p_2 \circ p_1)^{-1} =$~~

Problem:
If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ and $g \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ are permutations, prove that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Solu: $f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ and $g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

$f^{-1} \circ g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 2 & 1 \end{pmatrix}$

$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

$(g \circ f)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

Hence $f^{-1} \circ g^{-1} = (g \circ f)^{-1}$.

Theorem: (Cayley's Theorem)

Every finite group of order 'n' is Isomorphic to permutation group of degree 'n'.

Proof:

We shall prove this theorem in 3 steps.

Step-1 : We shall first find a set G' of permutation.

Step-2 : G' is a group

Step-3 : G & G' are isomorphic.

Step-1:

Let G be a finite group of order n.

Let $a \in G$. Define $f_a : G \to G$ by $f_a(x) = ax$.

Since $f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y$, f_a is 1-1.

Since, if $y \in G$, then $f_a(a^{-1}y) = aa^{-1}y = y$.

$\Rightarrow f_a$ is onto.

Thus f_a is a bijection.

Since G has n elements, f_a is just permutation on 'n' symbols.

Now, Let $G' = \{ f_a / a \in G \}$.

Step-2: T.P G' is a group.

Let $f_a, f_b \in G'$.

$f_a \circ f_b(x) = f_a(f_b(x)) = f_a(bx) = abx = f_{ab}(x)$

Hence $f_a \circ f_b = f_{ab} \in G' \Rightarrow G'$ is closed.

$f_e \in G'$ is the identity element, where e is the identity in G.

The inverse of f_a in G' is f_a^{-1}.

$\therefore G'$ is a group.

Step-3 T.P: G & G' are isomorphic

Define $\phi : G \to G'$ by $\phi(a) = f_a$

Now, $\phi(a) = \phi(b) \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x) \Rightarrow ax = bx \Rightarrow a = b$

$\therefore \phi$ is 1-1.

Since f_a is onto, ϕ is also onto.

Also $\phi(ab) = f_{ab} = f_a \circ f_b = \phi(a) \circ \phi(b)$.

$\therefore \phi$ is a Isomorphism. (ie) $G \cong G'$. It completes the proof.

Subgroups and Homomorphisms.

Defn: Subgroup.

Let $(G, *)$ be a group and $S \subseteq G$ be such that it satisfies the following conditions:

1. $e \in S$, where e is the identity of $(G, *)$
2. For any $a \in S$, $a^{-1} \in S$
3. For $a, b \in S$, $a * b \in S$.

Then $(S, *)$ is called a subgroup of $(G, *)$

Ex: The set of all integers $\mathbb{Z}$ is a subgroup of the set of all real numbers $\mathbb{R}$ under usual addition.

(i.e) $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.

Theorem:

The necessary and sufficient condition that a non-empty subset H of a group G be a subgroup is $a \in H, b \in H \Rightarrow a * b^{-1} \in H$.

Proof:

Necessary condition:

Assume that H is a subgroup of G.

Since H itself is a group.

We have $a, b \in H \Rightarrow a * b \in H$ (Closure)

Also $b \in H \Rightarrow b^{-1} \in H$ (Inverse)

$\therefore a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a * b^{-1} \in H$.

Sufficient condition:

Let $a * b^{-1} \in H$, for all $a, b \in H$ ⟶ (1)

and H is a subset of G.

T.P H is a subgroup of G.

(i) Closure: Let $b \in H \Rightarrow b^{-1} \in H$

For, $a, b \in H \Rightarrow a, b^{-1} \in H$

$\Rightarrow a * (b^{-1})^{-1} \in H$

$\Rightarrow a * b \in H$

$\therefore H$ is closed under the operation '$*$'

(ii) Associative:

Since $H \subseteq G$, the elements of H are also the elements of G.

Since '$*$' is associative in G, it must be also associative in H.

$\therefore H$ itself is a group under the operation '$*$' in G

(iii) Identity:

Let $a \in H \Rightarrow a * a^{-1} \in H$

$\Rightarrow e \in H$

$\therefore e$ is the identity element of H.

(iv) Existense of inverse:

Let $e \in H, a \in H$

$\Rightarrow e * a^{-1} \in H$

$\Rightarrow a^{-1} \in H$. $\therefore$ Every element of H has an inverse in H.

Theorem:
The intersection of two normal subgroups of a group is a subgroup of G.

Proof:
Given H and K are subgroups of G.

Let $a, b \in H \cap K \Rightarrow a, b \in H$ and $a, b \in K$.

$\Rightarrow a * b^{-1} \in H$ and $a * b^{-1} \in H$ (as H & K are subgroups)

$\Rightarrow a * b^{-1} \in H \cap K$.

Thus $H \cap K$ is a subgroup of G.

Problem:
If H and K are subgroup of G, prove that $H \cup K$ is a subgroup of G if and only if either $H \subseteq K$ or $K \subseteq H$.

Soln:
Given H and K are two subgroups of G and $H \subseteq K$ or $K \subseteq H$.

If $H \subseteq K$, then $H \cup K = K$ which is a subgroup of G.

If $K \subseteq H$, then $H \cup K = H$ which is a subgroup of G.

Conversely suppose $K \not\subseteq H$ and $H \not\subseteq K$.

Then there exists $a \in H$ and $a \notin K$ and there exists $ab \in K$ and $b \notin H$.

Now $a, b \in H \cup K$.

Because $H \cup K$ is a subgroup, it follows that $a * b \in H \cup K$.

Hence $a * b \in H$ or $a * b \in K$.

Case (i) If $a * b \in H$

Then $a^{-1} * (a * b) \in H$

That is $b \in H$ which is a contradiction.

Case (ii) If $a * b \in K$.

Then $a * b * b^{-1} \in K$.

i.e., $a \in K$ which is a contradiction.

Thus either $H \subseteq K$ or $K \subseteq H$.

Problem:

Show that every cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +_n)$

Soln:

Let (G, o) be a cyclic group of order n.

The elements of G are $\{a, a^2, a^3, \ldots a^n = e\}$

The elements of $\mathbb{Z}_n$ are $\{[0], [1], [2], \ldots [n-1]\}$

Define $f: D \to \mathbb{Z}_n$ by

$f(e) = [0]$ and $f(a^i) = [i]$ for $i < n$ where f is one-one and onto.

Then $f(a^i a^j) = f(a^{i+j}) = [i+j]$

$= [i] +_n [j]$.

i.e. $f(a^i \cdot a^j) = f(a^i) + f(a^j)$

Hence f is an isomorphism.

(X)

Theorem: ✓

Every cyclic group is abelian.

Soln:

Let $(G, *)$ be a cyclic group generated by an element $a \in G$.

i.e. $G = \langle a \rangle$

Then for any two elements $x, y \in G$.

We have $x = a^n$, $y = a^m$, where m, n are integer.

$$\therefore x * y = a^n * a^m$$
$$= a^{n+m}$$
$$= a^{m+n}$$
$$= a^m * a^n$$
$$= y * x.$$

Thus $(G, *$ is abelian).

(X)

Theorem: [Lagrange's theorem]

The order of a subgroup of a finite group divides the order of the group.

(OR)

If G is a finite group, then $O(H) \mid O(G)$, for all sub-group H of G.

Proof:

Let $O(G) = n$ (Here n is finite)

Let $G = \{a_1 = e, a_2, a_3, \ldots, a_n\}$ and let H be a subgroup of G.

Consider the left cosets as follows.

$$e * H = \{e * h / h \in H\}$$

$$a_2 H = \{a_2 * h / h \in H\}$$

$$a_n H = \{a_n * h / h \in H\}$$

We know that any two left cosets are either identical or disjoint.

Also $O(eH) = O(H)$

$O(a_i H) = O(H)$, $\forall a_i \in G$.

Otherwise if $a * h_i = a * h_j$ for $i \neq j$, by cancellation laws, we would have $h_i = h_j$ which is a $\Rightarrow\Leftarrow$.

Let there be k-disjoint cosets of H in K.

Clearly their union equals.

(i.e) $G = (a_1H) \cup (a_2H) \cup \ldots\ldots \cup (a_kH)$

$\therefore O(G) = O(a_1H) + O(a_2H) + \ldots\ldots + O(a_kH)$

$= \underbrace{O(H) + O(H) + \ldots\ldots + O(H)}_{k\text{-times.}}$

$\therefore O(G) = k\,O(H)$

This implies $O(H)$ is a divisor of $O(G)$.

— × — × — × —

Problem:

Let $G = \{1, a, a^2, a^3\}$ $(a^4 = 1)$ be a group and $H = \{1, a^2\}$ is a subgroup of G under multiplication. Find all the cosets of H.

Soln:

Let us find the right cosets of H in G.

$H1 = \{1, a^2\} = H$

$Ha = \{a, a^3\}$.

$Ha^2 = \{a^2, a^4\} = \{a^2, 1\} = H$

and $Ha^3 = \{a^3, a^5\} = \{a^3, a\} = Ha$

$\therefore H1 = H = Ha^2 = \{1, a^2\}$ and

$Ha = Ha^3 = \{a, a^3\}$ are two distinct right cosets of H in G. Similarly, we can find the left cosets of H in G. — × —.

Problem:

Find the left cosets of $\{[0], [2]\}$ in the group $(\mathbb{Z}_4, +_4)$.

Soln:

Let $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ be a group and $H = \{[0], [2]\}$ be a subgroup of $\mathbb{Z}_4$ under $+_4$ (addition mod 4).

$\therefore$ The left cosets of H are

$[0] + H = \{[0], [2]\} = H$

$[1] + H = \{[1], [3]\}$;

$[2] + H = \{[2], [4]\} = \{[2], [0]\}$

$= \{[0], [2]\} = H$

and $[3] + H = \{[3], [5]\} = \{[3], [1]\}$

$= \{[1], [3]\} = [1] + H$

$\therefore [0] + H = [2] + H = H$ and $[1] + H = [3] + H$ are the two distinct left cosets of H in $\mathbb{Z}_4$.

— × — × —

Defn: Normal Subgroup.

A subgroup $(H, *)$ of $(G, *)$ is called a normal subgroup if for any $a \in G$, $aH = Ha$.

— × — × —

Defn:

Let $(G, \star)$ and (H, Δ) be two groups. A mapping $g: G \to H$ is called a group homomorphism from $(G, \star)$ to (H, Δ) if for any $a, b \in G$.

$$g(a \star b) = g(a) \Delta g(b).$$

Note:

1. A group homomorphism is called a monomorph-ism, epimorphism or isomorphism depending upon whether g is one-to-one; onto, or one-to-one and onto, respectively.
2. A homomorphism from a group $(G, \star)$ to $(G, \star)$ is called an endomorphism, while an isomorphism of $(G, \star)$ to $(G, \star)$ is called an automorphism.

Defn:

Let g be a group homomorphism from $(G, \star)$ to (H, Δ). The set of elements of G which are mapped into e_H, the identity of H, is called the kernel of the homomorphism g and denoted by $\ker(g)$.

Defn: Normal Subgroup

Let H be a subgroup of G under $\star$. Then H is said to be a normal subgroup of G, for every $x \in G$ and for $h \in H$, if $x \star h \star x^{-1} \in H$ (ie) $x \star H \star x^{-1} \subseteq H$.

Alternatively, a subgroup H of G is called a normal subgroup of G if $x \star h = h \star x \ \forall\, x \in G$.

Defn:

The number of distinct left (or right) cosets of H in G is called the index of H in G. It is denoted by $[G:H] = I_G(H) = \frac{O(G)}{O(H)}$.

Theorem:

Let $(G, *)$ and (H, Δ) be groups and $g: G \to H$ be a homomorphism. Then the Kernal of g is a normal subgroup.

Proof:

Let K be the Kernel of the homomorphism g

(i.e) $K = \{x \in G / g(x) = e'$, where $e' \in H$ is the identity element of $H\}$.

T.P K is a subgroup.

Let $x, y \in K$, then $g(x) = e'$ & $g(y) = e'$.

Claim: $x * y^{-1} \in K$.

By defn. of homomorphism,

$$\begin{aligned} g(x * y^{-1}) &= g(x) \Delta g(y^{-1}) \\ &= g(x) \Delta (g(y))^{-1} \\ &= e' \Delta (e')^{-1} \\ &= e' \Delta e' \\ &= e' \end{aligned}$$

Hence $x * y^{-1} \in K$ and this proves K is a subgroup of G ~~By a criterion for subgroups~~.

T.P K is normal.

Let $x \in K$, $f \in G$, then $g(x) = e'$

claim: $f * x * f^{-1} \in K$.

$$g(f \star x \star f^{-1}) = g(f) \star g(x) \star g(f^{-1})$$
$$= g(f) \cdot e' [g(f)]^{-1}$$
$$= g(f) [g(f)]^{-1}$$
$$= e'$$

$\therefore f \star x \star f^{-1} \in K$

Thus K is a normal subgroup of G.

(X) **Theorem:** (Fundamental Theorem on homomorphism of groups)

If f is a homomorphism of G onto G' with kernal K; then $G/K \cong G'$.

Proof:

Let $f: G \to G'$ be a homomorphism from the group $(G, \star)$ to the group (G', Δ).

Then $K = \ker(f) = \{x \in G / f(x) = e'\}$ is a normal subgroup of $(G, \star)$.

Also we know that the quotient set $(G/K, \otimes)$ is a group.

Define $\phi: G/K \to G'$ is mapping from the group $(G/K, \otimes)$ to the group (G', Δ) given by

$$\phi(Ka) = f(a), \text{ for any } a \in G.$$

Since, if $Ka = Kb$

$\Rightarrow a \star b^{-1} \in K$

$\Rightarrow f(a \star b^{-1}) = e'$

$\therefore f(a) \Delta f(b^{-1}) = e'$

(i.e) $f(a) \Delta [f(b)]^{-1} = e'$

$f(a) \Delta [f(b)]^{-1} \Delta f(b) = e' f(b)$

$\Rightarrow f(a) \Delta e' = f(b)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow \phi(Ka) = \phi(Kb)$

$\therefore \phi$ is well defined.

Claim: ϕ is a homomorphism

Let $Ka, Kb \in G/K$.

Now, $\phi(Ka \otimes Kb) = \phi[K(a*b)]$

$= f(a*b)$

$= f(a) \Delta f(b)$

$= \phi(Ka) \Delta \phi(Kb)$

$\therefore \phi$ is a homomorphism.

Claim: ϕ is one-to-one.

If $\phi(Ka) = \phi(Kb)$, then $f(a) = f(b)$.

$\Rightarrow f(a) \Delta f(b^{-1}) = f(b) \Delta f(b^{-1})$

$\Rightarrow f(a*b^{-1}) = f(b*b^{-1})$

$= f(e) = e'$

$\Rightarrow a*b^{-1} \in K \Rightarrow Ka = Kb.$

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

Claim: ϕ is onto.

Let y be any element of G'

Since $f: G \to G'$ is a homomorphism from G onto G', therefore there exists an element $a \in G$ such that $f(a) = y$.

$\therefore$ For every $a \in G$, $Ka \in G/K$.

We get $\phi(Ka) = f(a)$ & $f(a) = y \in G'$

$\therefore$ ϕ is onto.

$\therefore$ $\phi: G/K \to G'$ is an isomorphism.

Hence $G/K \cong G'$.

— × — × — × —

(X)

Theorem:

Prove that the intersection of two normal subgroup is a normal subgroup.

Proof: Let H and K be any two normal subgroups of a group G.

We have to prove that $H \cap K$ is normal in G.

Since H and K are subgroups of G, $e \in H$ and $e \in K$.

Hence $e \in H \cap K$.

Thus $H \cap K$ is a non-empty set.

Let $a, b \in H \cap K$.

Claim: $ab^{-1} \in H \cap K$.

Since $a, b \in H \cap K$, both a, b being to H and K.

Since H and K are subgroups of G, $ab^{-1} \in H$ and

$ab^{-1} \in K$, so that $ab^{-1} \in H \cap K$

Hence $H \cap K$ is a subgroup of G, by a criterion for subgroup.

T.P $H \cap K$ is normal.

Let $x \in H \cap K$, and let $g \in H$

Since $x \in H \cap K$ and $x \in H$ and $x \in K$

Since $x \in H$, $g \in G$

$\Rightarrow gxg^{-1} \in H$ (as H is normal.

Likewise, $x \in K$, $g \in G \Rightarrow gxg^{-1} \in K$ (as K is normal)

Hence $x \in H \cap K$ and $g \in G$

$\Rightarrow gxg^{-1} \in H \cap K$.

This $H \cap K$ is a normal subgroup of G.

(X)

Theorem:

Every subgroup of an abelian group is a normal subgroup.

Proof:

Let $(G, *)$ be an abelian group and $(N, *)$ be a subgroup.

Let g be any element in G and let $n \in N$

Now, $g * n * g^{-1} = (n * g) * g^{-1}$ [$\because G$ is abelian]

$= n * (g * g^{-1})$

$= n * e = n \in N$.

$\therefore \forall\ g \in G$ and $n \in N$, $g * n * g^{-1} \in N$

$\therefore (N, *)$ is a normal subgroup.

Theorem:

Let $f: G \to G'$ be a homomorphism, then the $\ker(f)$ is a normal subgroup of G.

Soln:

We know that $\ker(f) = \{x \in G / f(x) = e'\}$ is a subgroup of $(G, *)$.

Now, we can prove that $\ker(f)$ is a normal subgroup of G.

Let $g \in G$ and $n \in \ker(f)$.

Now, $f(g * n * g^{-1}) = f(g) \Delta f(n) \Delta f(g^{-1})$

$= f(g) \Delta e' \Delta f(g^{-1})$

$= f(g) \Delta f(g^{-1})$

$= f(g * g^{-1})$

$= f(e)$

$= e'$

$\Rightarrow g * n * g^{-1} \in \ker(f)$

$\therefore (\ker(f), *)$ is a normal subgroup of the group $(G, *)$.

Defn: Direct Product.

Let $(G, *)$ and (H, Δ) be two groups. The direct product of these two groups is the algebraic structure $(G \times H, \circ)$ in which the binary operation '$\circ$' on $G \times H$ is given by

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 * g_2, h_1 \Delta h_2)$$

for any $(g_1, h_1), (g_2, h_2) \in G \times H$.

Theorem:

The direct product of the two groups is a group.

Soln:

Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups. Their direct product is the structure $(G_1 \times G_2, *)$ in which the binary operation $*$ is defined by

$$(a_1, b_1) * (a_2, b_2) = (a_1 *_1 a_2, b_1 *_2 b_2).$$

T.P $G_1 \times G_2$ is a group.

(i) Associative of $*$

Let $a, b, c \in G_1 \times G_2$ and $a = (x_1, y_1)$, $b = (x_2, y_2)$ and $c = (x_3, y_3)$ for some $x_1, x_2, x_3 \in G_1$ and $y_1, y_2, y_3 \in G_2$

Now,

$$\begin{aligned} a * (b * c) &= (x_1, y_1) * ((x_2, y_2) * (x_3, y_3)) \\ &= (x_1, y_1) * (x_2 *_1 x_3, y_2 *_2 y_3) \quad [\text{By defn. of } *] \\ &= (x_1 *_1 (x_2 *_1 x_3), y_1 *_2 (y_2 *_2 y_3)) \\ &= ((x_1 *_1 x_2) *_1 x_3, (y_1 *_2 y_2) *_2 y_3) \quad (\text{By Associative laws}) \\ &= (x_1 *_1 x_2, y_1 *_2 y_2) * (x_3, y_3) \end{aligned}$$

(i.e) $a \star (b \star c) = x \star y((x_1, y_1) \star (x_2, y_2)) \star (x_3, y_3)$

$= (a \star b) \star c$

So associative axiom is satisfied in $G_1 \times G_2$ for $\star$.

(ii) Identity for $\star$.

If e_1 and e_2 are identities for G_1 and G_2 respectively, then $e = (e_1, e_2)$ is the identity for $G_1 \times G_2$.

Let $a = (x_1, y_1) \in G_1 \times G_2$

$a \star e = (x_1, y_1) \star (e_1, e_2)$

$= (x_1 \star_1 e_1, y_1 \star_2 e_2)$

$= (x_1, y_1) = a$

Similarly, $e \star a = a$.

So $a \star e = e \star a = a$.

Hence $e = (e_1, e_2)$ is the identity element in G.

(iii) Inverse in $G_1 \times G_2$.

The inverse of an element e in $G_1 \times G_2$ is determined componentwise.

(i.e) $a' = (x_1, y_1)' = (x_1', y_1')$

This can be verified as follows:

$= (x_1, y_1) \star (x_1', y_1')$

$= (x_1 \star_1 x_1', y_1 \star_2 y_1')$ (by defn. of $\star$)

$= (e_1, e_2) = e$

Similarly $a' \star a = (e_1, e_2) = e$.

So, $(x_1, y_1)' = (x_1', y_1')$

From (i), (ii) and (iii) it follow that $G = G_1 \times G_2$ is a group.

Problem:

How many generators are there in a cyclic group of order 10?

Soln: We have a is the generator then a^m is also generator iff and only if $(m, n) = 1$.

Now, we have, $(1, 10) = 1$, $(3, 10) = 1$, $(7, 10) = 1$, $(9, 10) = 1$

$(2, 10) = 2$, $(4, 10) = 2$, $(5, 10) = 5$, $(6, 10) = 2$, $(8, 10) = 2$ } X

∴ There are 4 generators, which are a, a^3, a^7, a^9 whenever a is a generator.

Algebraic System with two Binary Operations.

Defn: Ring

An algebraic system $(S, +, \cdot)$ is called a ring if binary operations $+$ and $\cdot$ on S satisfy the following three properties:

1. $(S, +)$ is an abelian group.
2. $(S, \cdot)$ is a semigroup
3. The operation $\cdot$ is distributive over $+$; that is for any $a, b, c \in S$,

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad \text{and} \quad (b+c) \cdot a = b \cdot a + c \cdot a.$$

Examples:

1. The set of all integers $\mathbb{Z}$, the set of all rational numbers $\mathbb{R}^+$, the set of all real numbers $\mathbb{R}$ are rings under the usual addition and usual multiplication.
2. The set of all $n \times n$ matrices M_n is a ring under the matrix addition and matrix multiplication.

Defn: Integral Domain.

A commutative ring $(S, +, \cdot)$ with identity and without divisors of zero is called an Integral Domain.

Defn: Field.

A commutative ring $(S, +, \cdot)$ which has more than one element such that every non-zero element of S has a multiplicative inverse in S is called a Field.

Defn: Sub ring

A subset $R \subseteq S$ where $(S, +, \cdot)$ is a ring is called a subring if $(R, +, \cdot)$ is a ring itself with the operations $+$ and $\cdot$ restricted to R.

Examples:

1. The ring of integers $\mathbb{Z}$ is a subring of the ring of all rational numbers $\mathbb{Q}$.
2. In $\mathbb{Z}$ the ring of all integers, the set of all even integers is a subring.

Defn: Ring Homomorphism.

Let $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be rings. A mapping $g: R \to S$ is called a ring homomorphism from $(R, +, \cdot)$ to $(S, \oplus, \odot)$ if for any $a, b \in R$.

$$g(a+b) = g(a) \oplus g(b) \text{ and}$$
$$g(a \cdot b) = g(a) \cdot g(b).$$

Examples:

1. The ring $\mathbb{Q}$ of all rational numbers, and the ring $\mathbb{R}$ of real numbers are fields.
2. The ring $(\mathbb{Z}_7, +_7, \times_7)$ is a field.
3. The ring $\mathbb{Z}$ of all integers is an Integral domain but not a field.

Defn: Cyclic Group

Let G be a group. Let $a \in G$. Then $H = \{a^n / n \in \mathbb{Z}\}$ is a subgroup of G. Then H is called the cyclic subgroup of G generated by a and is denoted by $\langle a \rangle$.

Examples:

1. In $(\mathbb{Z}, +)$, $\langle a \rangle$ where $a \in \mathbb{Z}$, the set of integers.
2. In the group $G = \{1, i, -1, -i\}$.
   $\langle i \rangle = \{i, i^2, i^3, \ldots\} = \{1, i, -1, -i\} = G$.

Defn:

Let G be a group and let $a \in G$. 'a' is called a generator of G if $\langle a \rangle = G$. A group G is cyclic if there exists an element $a \in G$ such that $\langle a \rangle = G$.

Defns:

- The Ring $(R, +, \cdot)$ is called a commutative ring, if $ab = ba$ for $a, b \in R$.
- If $(R, \cdot)$ is a monoid, then the ring $(R, +, \cdot)$ is called a ring with unity or Identity.
- If a and b are 2 non-zero elements of a ring R such that $a \cdot b = 0$, then a and b are called zero divisors.

Defn:

A commutative ring $(R, +, \cdot)$ with Identity and without zero divisors is called an Integral domain. Eg: $(\mathbb{Z}, +, \cdot)$ is an integral domain. ($\mathbb{Z}$: Integers.)

Defn:

A commutative ring with Identity $(R, +, \cdot)$ is called a field if every non-zero element has a multiplicative inverse. Thus $(R, +, \cdot)$ is a field if (i) $(R, +)$ is abelian group (ii) $(R - \{0\}, \cdot)$ is also abelian group.

Examples:

1. $(\mathbb{R}, +, \cdot)$ is a field.
2. $(\mathbb{Q}, +, \cdot)$ is a field.

However $(\mathbb{Z}, +, \cdot)$ is not a field.

Unit - V

Lattices and Boolean Algebra.

Lattices

Partial Ordering

Defn: (Partial order relation)

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.

Defn: Poset.

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

Note:

It is conventional to denote a partial ordering by the symbol $\leq$. This symbol does not necessarily mean "less than or equal to" as is used for real numbers.

Defn: Totally ordered set

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 simple ordering or linear ordering on P and $(P, \leq)$ is called a totally ordered (or simply ordered) set or a chain.

Example:
The poset $(\mathbb{Z}, \leq)$ is totally ordered, since $a \leq b$ or $b \leq a$ whenever a & b are integers.

Defn:
Let $(P, \leq)$ be a partially ordered set and let $A \subseteq P$. Any element $x \in P$ is an upper bound for A if for all $a \in A$, $a \leq x$.

Similarly, any element $x \in P$ is a lower bound for A if for all $a \in A$, $x \leq a$.

Defn:
Let $(P, \leq)$ be a poset and let $A \subseteq P$. Any 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, then greatest lower bound, or infimum for A is an element $x \in P$ such that x is a lower bound and $y \leq x$ for all lower bounds y.

Defn: Well ordered.
A partially ordered set (poset) is called well-ordered if every non-empty subset of it has a least member.

Properties of Lattices

Defn: Lattice

A Lattice in 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.

Defn: Greatest Lower Bound (GLB) and Least Upper Bound (LUB)

The GLB of a subset $\{a, b\} \subseteq L$ will be denoted by $a * b$ and the least upper bound by $a \oplus b$.

(i.e) $GLB\{a, b\} = a * b$ (meet or product of a & b)

$LUB\{a, b\} = a \oplus b$ (join or sum of a & b).

Remark:

GLB, LUB may or maynot exist for a subset.

Problem:

Is the poset $(Z^+, |)$ a lattice?

Sol:

Let a & b be two positive integers. The least upper bound and greatest ~~or~~ lower bound of these two integers are the least common multiple and the greatest common divisor of these integers, respectively.

It follows that this poset is a lattice

———— × ———— × ———— × ————

Property: 1 (Idempotent law).

Let $(L, \leq)$ be a lattice. For any $a, b \in L$ we have $a * a = a$ and $a \oplus a = a$ [idempotent law]

Proof:

Let $a, b, c \in L$, by the definition of GLB of a and b we have $a * b \leq a \longrightarrow (1)$

and if $a \leq a$ and $a \leq b$, then

$$a \leq a * b \longrightarrow (2)$$

As $a \leq a$, from (1) & (2) we have

$$a * a \leq a \text{ and } a \leq a * a.$$

By the antisymmetric property, it follows that

$$a = a * a.$$

Similarly we can prove that $a \oplus a = a$.

——— x ——— x ———.

Property: 2 [Associative]

Show that the operation of meat are join on a lattice are associative.

Solu:

T.P $(a * b) * c = a * (b * c)$

Let $a, b, c \in L$ by defn. we have

$$(a * b) * c \leq a * b. \&$$

$$(a * b) * c \leq c.$$

By the defn. of GLB of a and b, we have

$a \star b \leq a$ and $a \star b \leq b$, so by transitive property of $\leq$ we have

$$(a \star b) \star c \leq a$$

& $(a \star b) \star c \leq b$.

As $(a \star b) \star c \leq b$ and $(a \star b) \star c \leq c$

We see that $(a \star b) \star c$ is lower bound for b and c. From the defn. of $b \star c$ it follows that

$$(a \star b) \star c \leq b \star c.$$

As $(a \star b) \star c \leq a$ and $(a \star b) \star c \leq b \star c$

From the defn. of $a \star (b \star c)$, we have

$$(a \star b) \star c \leq a \star (b \star c) \longrightarrow ①$$

Now, $a \star (b \star c) \leq a$ and $a \star (b \star c) \leq (b \star c)$

As $b \star c \leq b$, by transitivity $a \star (b \star c) \leq b$

Since $a \star (b \star c) \leq a$ and $a \star (b \star c) \leq b$,

we have $a \star (b \star c) \leq (a \star b)$

As $a \star (b \star c) \leq (b \star c) \leq c$

$$a \star (b \star c) \leq (a \star b) \star c \longrightarrow ②$$

From ① & ②, by antisymmetric property, it follows that $a \star (b \star c) = (a \star b) \star c$.

Similarly we can prove that $a \oplus (b \oplus c) = (a \oplus b) \oplus c$.

Property: 3 [Commutative]

Show that the operation of meet and join on a lattice are commutative law.

(i.e) $a * b = b * a$ and $a \oplus b = b \oplus a$.

Soln:

Given $a, b \in L$ both $a * b$ and $b * a$ are GLB of a and b.

By uniqueness of GLB of $a * b$, we have

$a * b = b * a$.

Similarly $a \oplus b = b \oplus a$ holds good.

Property: 4 [Absorption law].

$a * (a \oplus b) = a$ and $a \oplus (a * b) = a$.

Soln:

Let $a, b \in L$.

Then $a \leq a$ and $a \leq a \oplus b$.

So $a \leq a * (a \oplus b)$.

On the other hand $a * (a \oplus b) \leq a$.

By antisymmetric property of $\leq$, we have

$a = a * (a \oplus b)$.

Similary, we have

$a = a \oplus (a * b) \; \forall \; a, b \in L$.

Theorem: 1.

Let $(L, \leq)$ be a lattice in which $*$ and $\oplus$ denotes the operations of meet and join respectively. For any $a, b \in L$, $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$.

(OR)

Let $(L, \leq)$ be a lattice. For any $a, b \in L$, the following are equivalent.

(i) $a \leq b$ (ii) $a * b = a$ (iii) $a \oplus b = b$.

Proof:

T.P (i) $\Leftrightarrow$ (ii)

We have $a \leq a$, assume $a \leq b$.

$\therefore a \leq a * b$.

By the defn. of GLB, we have $a * b \leq a$.

Hence by antisymmetric property, $a * b = a$

Assume that $a * b = a$, but is only possible if

$a \leq b \Rightarrow a * b = a \Rightarrow a \leq b$.

Combining these two results, we have

$a \leq b \Leftrightarrow a * b = a$.

Similary $a \leq b \Leftrightarrow a \oplus = b$. [(i) $\Leftrightarrow$ (iii)]

Alternatively T.P (ii) $\Leftrightarrow$ (iii)

Assume $a * b = a$, we have $b \oplus (a * b) = b \oplus a = a \oplus b$

~~but by~~

but by absorption law,

$b \oplus (a * b) = b$.

Hence $a \oplus b = b$.

By representing similar steps, we can show that $a * b = a$ follows from $a \oplus b = b$.

$\therefore$ (ii) $\Leftrightarrow$ (iii)

Hence the theorem

Theorem:

Let $(L, \leq)$ be a lattice. For any $a, b, c \in L$, the following inequalities, hold:

(1) Distributive Inequalities

(i) $a \oplus (b * c) \leq (a \oplus b) * (a \oplus c)$

(ii) $a * (b \oplus c) \geq (a * b) \oplus (a * c)$

(2) Modular Inequalities

(i) $a \leq c \Leftrightarrow a \oplus (b * c) \leq (a \oplus b) * c$

(ii) $a \geq c \Leftrightarrow a * (b \oplus c) \geq (a * b) \oplus c$

Proof:

As (ii) in 1, (ii) in 2 are duals of (i) in 1 and (i) in 2 respectively, it is enough to prove (i) in 1 and (i) in 2 only.

Consider (i) in 1

Let $a, b, c \in L$.

As $a \leq a \oplus b$ and $a \leq a \oplus c$

we have $a \leq [(a \oplus b) * (a \oplus c)]$

As $b * c \leq b \leq a \oplus b$ and $b * c \leq c \leq a \oplus c$,

we have $b * c \leq (a \oplus b) * (a \oplus c)$.

$\therefore (a \oplus b) * (a \oplus c)$ is an upper bound for a and $b * c$ and hence $a \oplus (b * c) \leq (a \oplus b) * (a \oplus c)$

Then (i) in 1 is proved.

The inequality (i) in 2 is special case of (i) in 1.

If $a \leq c$, then $a \oplus c = c$ and from (i) in 1 we obtain $a \oplus (b * c) \leq (a \oplus b) * (a \oplus c) = (a \oplus b) * c$

(i.e) $a \oplus (b * c) \leq (a \oplus b) * c$

Hence (i) in 2 is proved.

Thus the theorem is proved.

——— X ——— X ———.

Theorem:

In a lattice $(L, \leq)$, show that

(i) $(a * b) \oplus (c * d) \leq (a \oplus c) * (b \oplus d)$.

(ii) $(a * b) \oplus (b * c) \oplus (c * a) \leq (a \oplus b) * (b \oplus c) * (c \oplus a)$

$\forall\ a, b, c \in L$

Proof:

Let $a, b, c \in L$.

Then $a * b \leq a$ (or) $b \leq a \oplus b \longrightarrow (1)$

$a * b \leq a \leq c \oplus a \longrightarrow (2)$

$a * b \leq b \leq b \oplus c \longrightarrow (3)$

Using (1), (2) & (3), we get

$a * b \leq (a \oplus b) * (b \oplus c) * (c \oplus a)$

Similarly, $b * c \leq (a * b) * (b \oplus c) * (c \oplus a)$

$c * a \leq (a \oplus b) * (b \oplus c) * (c \oplus a)$

This prove (ii).

We have $a \leq a \oplus c$

$b \leq b \oplus d$

$\therefore a * b \leq (a \oplus c) * (b \oplus d)$.

* We know that $c \leq a \oplus c \longrightarrow (4)$

$d \leq b \oplus d \longrightarrow (5)$

$\therefore c \star d \leq (a \oplus c) \star (b \oplus d)$.

$\therefore$ By ④ & ⑤, $(a \star b) \oplus (c \star d) \leq (a \oplus c) \star (b \oplus d)$

This proves (i)

Theorem:

In a lattice $(L, \leq)$, prove that for $a, b, c \in L$

(i) $(a \star b) \oplus (a \star c) \leq a \star (b \oplus (a \star c))$

(ii) $(a \oplus b) \star (a \oplus c) \geq a \oplus (b \star (a \oplus c))$

Proof:

We know that $a \star b \leq a$, $a \star c \leq a$

$\therefore (a \star b) \oplus (a \star c) \leq a \oplus a = a \longrightarrow ①$

Also $a \star b \leq b$, $a \star c \leq a \star c$.

$\Rightarrow (a \star b) \oplus (a \star c) \leq b \oplus (a \star c) \longrightarrow ②$

From ① & ②, $(a \star b) \oplus (a \star c) \leq a \star (b \oplus (a \star c))$

This proves i)

We know that $a \leq a \oplus b$; $a \leq a \oplus c$

$\Rightarrow a = a \star a \leq (a \oplus b) \star (a \oplus c) \longrightarrow ③$

Further $b \leq a \oplus$; $a \oplus c \leq a \oplus c$

$\Rightarrow b \star (a \oplus c) \leq (a \oplus b) \star (a \oplus c) \longrightarrow ④$

By ③ & ④, $a \oplus (b \star (a \oplus c)) \leq (a \oplus b) \star (a \oplus c)$

This proves (ii)

Theorem:

In a lattice if $a \leq b \leq c$, show that

(i) $a \oplus b = b * c$ (ii) $(a * b) \oplus (b * c) = (a \oplus b) * (a \oplus c) = b$

Proof:

Let $a \leq b \leq c$

$a \leq b \Rightarrow a \oplus b = b$, $a * b = a$

$b \leq c \Rightarrow b \oplus d = c$, $b * c = b$

$a \leq c \Rightarrow d \oplus c = c$, $a * c = a$

$\therefore a \oplus b = b = b * c$

Hence (i) follows.

Now, $(a * b) \oplus (b * c) = a \oplus b = b$

$(a \oplus b) * (a \oplus c) = b * c = b$

Hence (ii) follows.

Terminology

In logic notation	In set theory notation	Computers Designers notation	Read as
$\vee$	$\cup$	$\oplus$	Joint or sum
$\wedge$	$\cap$	$*$	Meet and product
$\neg$	$\subset$	$-, '$	Complement
$\leq$	$\subseteq$	$\leq$	Partially ordered set

Defn:

A lattice is an algebraic system $(L, \star, \oplus)$ with two binary operations $\star$ and $\oplus$ on L which are both commutative, associative and satisfy the absorption laws.

Defn: Sub Lattice.

Let $(L, \star, \oplus)$ be a lattice and let $S \subseteq L$ be a subset of L. The algebra $(S, \star, \oplus)$ is a sublattice of $(L, \star, \oplus)$ iff S is closed under both operations $\star$ and $\oplus$.

Defn:

A lattice is called complete if each of its non empty subsets has a least upper bound and a greatest lower bound.

Defn:

In a bounded lattice $(L, \star, \oplus, 0, 1)$ an element $b \in L$ is called complement of an element $a \in L$ if $a \star b = 0$ and $a \oplus b = 1$

Defn:

A lattice $(L, \star, \oplus, 0, 1)$ is said to be a complemented lattice if every element of L has atleast one complement.

Defn:

A lattice $(L, *, \oplus)$ is called a distributive lattice if for any $a, b, c \in L$.

$$a * (b \oplus c) = (a * b) \oplus (a * c)$$
$$a \oplus (b * c) = (a \oplus b) * (a \oplus c)$$

(OR)

In other words, in a distributive lattice the operations $*$ and $\oplus$ distribute over each other.

Defn: Modular.

A lattice $(L, \wedge, \vee)$ is called modular if for all $x, y, z \in L$, $x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$ (modular equation).

Theorem:

(X) Every chain is a distributive lattice

Proof:

Let $(L, \leq)$ be a chain.

Let $a, b, c \in L$.

Consider the following possible cases

(i) $a \leq b$ or $a \leq c$ and

(ii) $a \geq b$ or $a \geq c$.

We shall now show that the distributive law

$a * (b \oplus c) = (a * b) \oplus (a * c)$

In case (i) $a \leq b$ or $a \leq c$ then we have

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

$\Rightarrow a \leq b \oplus c$

So $a * (b \oplus c) = a \longrightarrow (1)$

and $(a * b) \oplus (a * c) = a \oplus a = a \longrightarrow (2)$

(1) + (2) we get

$a * (b \oplus c) = (a * b) \oplus (a * c)$

In case (ii)

If $a \geq b$ and $a \geq c$ then we have

$a * b = b$, $a * c = c$ and $b \oplus c \leq a$

So that $a * (b \oplus c) = b \oplus c \longrightarrow (3)$

and $(a * b) \oplus (a * c) = b \oplus c \longrightarrow (4)$

From (3) & (4) we get

$a * (b \oplus c) = (a * b) \oplus (a * c)$

Theorem:

If $(L, *, \oplus)$ be a distributive lattice. For any $a, b, c \in L$,

$$(a * b = a * c) \wedge (a \oplus b = a \oplus c) \Rightarrow b = c$$

Proof:

$$(a * b) \oplus c = (a * c) \oplus c = c \longrightarrow (1)$$

Now, $(a * b) \oplus c = (a \oplus c) * (b \oplus c)$

$$= (a \oplus b) * (b \oplus c)$$

$$= b \oplus (a * c)$$

$$= b \oplus (a * b)$$

$$= b \longrightarrow (2)$$

From (1) & (2), $\boxed{b = c}$

Theorem:

Every distributive lattice is modular.

Proof:

Let $(L, \leq)$ be a distributive lattice

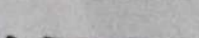
For all $a, b, c \in L$, we have

$$a \oplus (b * c) = (a \oplus b) * (a \oplus c)$$

Thus if $a \leq c$, then $a \oplus c = c$ and

$$a \oplus (b * c) = (a \oplus b) * c.$$

So if $a \leq c$, the modular equation is satisfied & L is modular.



(X)

Theorem:

Let L be a complemented, distributive lattice. For $a, b \in L$ the following are equivalent.

(i) $a \leq b$ (ii) $a \star b' = 0$ (iii) $a' \oplus b = 1$ (iv) $b' \leq a'$

where 1 denotes corresponding complement.

Proof:

Now, $a \leq b \Rightarrow a \oplus b = b$

$\Rightarrow (a \oplus b) \star b' = 0$ as $b \star b' = 0$

$\Rightarrow (a \star b') \cdot \vee (b \star b') = 0$

$\Rightarrow a \star b' = 0$ as $b \star b' = 0$.

Hence (i) $\Rightarrow$ (ii)

Now, $a \star b' = 0$

$\Rightarrow (a \star b') = 1$

$\Rightarrow a' \oplus (b') = 1$

$\Rightarrow a' \oplus b = 1$

Hence (ii) $\Rightarrow$ (iii)

Now, $a' \oplus b = 1 \Rightarrow (a' \oplus b) \star b' = b'$

$\Rightarrow (a' \star b') \oplus (b \star b') = b'$ (distributive law)

$\Rightarrow a' \star b' = b'$ as $b \star b' = 0$

$\Rightarrow b' \leq a'$

Hence (iii) $\Rightarrow$ (iv)

Now,

$b' \leq a' \Rightarrow a' * b' = b'$

$\Rightarrow a \oplus b = b$

(taking complement on both sides by Demorgan's law)

$\Rightarrow a \leq b$

Hence (iv) $\Rightarrow$ (i)

Thus (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i).

Defn:

Let $(L, *, \oplus)$ and $(S, \wedge, \vee)$ be two lattices. The algebraic system $(L \times S, \cdot, +)$ in which the binary operations + and · on $L \times S$ are such that for any (a_1, b_1) and (a_2, b_2) in $L \times S$.

$(a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_2, b_1 \wedge b_2)$

$(a_1, b_1) + (a_2, b_2) = (a_1 \oplus a_2, b_1 \vee b_2)$

is called the direct product of the lattices $(L, *, \oplus)$ and $(S, \wedge, \vee)$.

Defn

Defn:

Let $(L, *, \oplus)$ and $(S, \wedge, \vee)$ be two lattices. A mapping $g: L \to S$ is called a lattice homomorphism from the lattice $(L, *, \oplus)$ to $(S, \wedge, \vee)$ if for any $a, b \in L$.

$$g(a * b) = g(a) \wedge g(b) \text{ and } g(a \oplus b) = g(a) \vee g(b).$$

Defn: Enumeration.

A one-to-one correspondence with the elements of a set is called an enumeration.

Theorem:

(X) State and prove Isotonicity property in lattice.

Proof:

Statement: Let $(L, \leq)$ be a lattice. For $a, b, c \in L$, the following properties called isotonicity laws.

$$b \leq c \Rightarrow a * b \leq a * c \; ; \; a \oplus b \leq a \oplus c$$

(i.e) $b \leq c \Rightarrow a \wedge b \leq a \wedge c \; ; \; a \vee b \leq a \vee c$.

Proof: Let us assume that $b \leq c$.

(i) claim: $a \vee b \leq a \vee c$

Let $x = a \vee c$. Then x is lub of a & c.

$\Rightarrow x$ is an upper bound of a & c.

$\therefore a \leq x, \quad c \leq x.$

But $b \leq c, \; c \leq x, \Rightarrow b \leq x.$

Also $a \leq x.$

$\therefore x$ is an upperbound of a & b.

But $a \vee b$ is lub of a & b.

$\therefore a \vee b \leq x = a \vee c.$

(ii) claim: $a \wedge b \leq a \wedge c$

Let $y = a \wedge b \Rightarrow y$ is glb of a & b.

$\therefore y$ is a lower bound of a & b

$y \leq a, \; y \leq b$

Using $b \leq c, \; y \leq a, \; y \leq c$

$\therefore y$ is a lower bound of a & c

But $a \wedge c$ is glb of a & c

$\therefore y \leq a \wedge c \Rightarrow a \wedge b \leq a \wedge c$

——— x ——— x ———

Problem: (or) Theorem

Let $(L, \wedge, \vee)$ be a distributive lattice and $a, b, c \in L$. If $a \wedge b = a \wedge c$ and $a \vee b = a \vee c$, then $b = c$. [Cancellation laws are valid in a Distributive lattice.].

Proof:

Let $(L, \wedge, \vee)$ be any distributive lattice and $a, b, c \in L$, such that

$$a \wedge b = a \wedge c \text{ and } a \vee b = a \vee c$$

Now, $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$ [$\because L$ is distributive]

$= (a \vee b) \wedge (b \vee c)$

$= (b \vee a) \wedge (b \vee c)$

$= b \vee (a \wedge c)$

$= b \vee (a \wedge b)$

$= b$

and $(a \wedge b) \vee c = (a \wedge c) \vee c = c$

Thus $b = (a \wedge b) \vee c = c$

So that, $a \wedge b = a \wedge c$

and $a \vee b = a \vee c$

$\Rightarrow b = c$

That is, the cancellation law is valid in a distributive lattice.

Problem:
Show that the direct product of any two distributive lattices is a distributive lattice.

Solu:
Let L_1 and L_2 be two distributive lattices.
Let $x, y, z \in L_1 \times L_2$, the direct product (lattice) of L_1 & L_2.
Then $x = (a_1, a_2)$, $y = (b_1, b_2)$ and $z = (c_1, c_2)$ for some $a_1, b_1, c_1 \in L_1$ and $a_2, b_2, c_2 \in L_2$.

Now, $x \vee (y \wedge z) = (a_1, a_2) \vee (b_1, b_2) \wedge (c_1, c_2)$

$= (a_1, a_2) \vee (b_1 \wedge c_1, b_2 \wedge c_2)$

$= (a_1 \vee (b_1 \wedge c_1), a_2 \vee (b_2 \wedge c_2))$

$= ((a_1 \vee b_1) \wedge (a_1 \vee c_1), (a_2 \vee b_2) \wedge (a_2 \vee c_2))$

as L_1 & L_2 are distributive

$= ((a_1 \vee b_1), (a_2 \vee b_2)) \wedge ((a_1 \vee c_1), (a_2 \vee c_2))$

$= ((a_1, a_2) \vee (b_1, b_2)) \wedge ((a_1, a_2) \vee (c_1, c_2))$

$= (x \vee y) \wedge (x \vee z)$.

So for all $x, y, z \in L_1 \times L_2$, $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

Thus if L_1 and L_2 are distributive, then $L_1 \times L_2$ is also distributive.

(ix) Problem:

Give an example of a lattice which is a modular but not a distributive.

Solu:

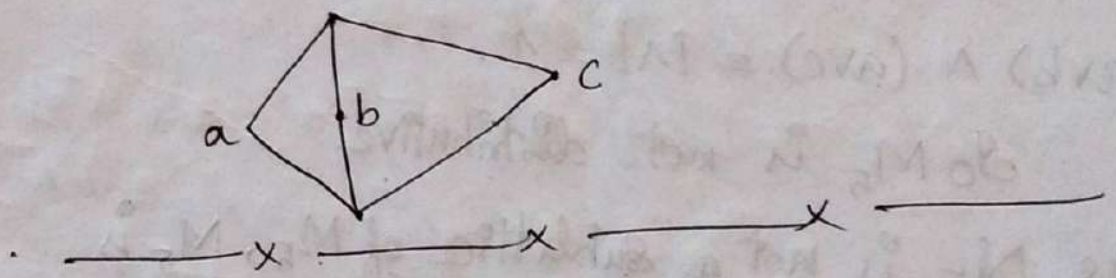
$M_5 \rightarrow$ diamond lattice.

In M_5, $a \vee (b \wedge c) = a \vee 0 = a$, zero

while $(a \vee b) \wedge (a \vee c) = 1 \wedge 1 = 1$

So M_5 is not distributive.

As N_5 is not a sublattice of M_5, M_5 is modular.



Problem

(x) Show that every distributive lattice is modular. Whether the converse is true? Justify your claim.

Solu:

Let $(L, \leq)$ be a distributive lattice.

For all $a, b, c \in L$, we have

$$a \oplus (b \star c) = (a \oplus b) \star (a \oplus c)$$

Thus If $a \leq c$, then $a \oplus c = c$ and

$$a \oplus (b \star c) = (a \oplus b) \star c.$$

So if $a \leq c$, the modular equation is satisfied and L is modular.

However, the converse is not true,

Example of lattice which is modular but not a distributive.

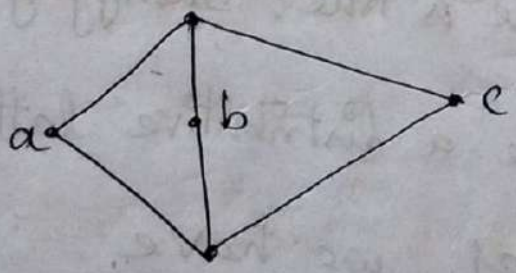
$M_5 \rightarrow$ dimond lattice.

In M_5, $a \vee (b \wedge c) = a \vee \overset{\text{zero}}{0} = a$ while

$(a \vee b) \wedge (a \vee c) = 1 \wedge 1 = 1$.

So M_5 is not distributive.

As N_5 is not a sublattice of M_5, M_5 is modular.



Boolean Algebra:

Defn: Boolean algebra.

A Boolean algebra is a complemented, distributive lattice.

Defn: Direct product.

Let $(L, \oplus, *)$ and $(S, \vee, \wedge)$ be two lattices. Then the direct product of L, and S is defined by $(L \times S, +, \star)$ where $+$ and $\star$ are defined by the following manners

$(a_1, b_1) + (a_2, b_2) = (a_1 \oplus a_2, b_1 \vee b_2)$

$(a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_2, b_1 \wedge b_2)$ $\forall\ a_1, a_2 \in L$, $\forall\ b_1, b_2 \in S$.

~~**Defn:** Lattice~~

(X) **Theorem:**

In a Boolean lattice, prove that the De-Morgan's laws.

Proof:

Let $(L, \oplus, *)$ be Boolean lattice.

(i.e) L is a complemented and distributive lattice.

The De-Morgan's laws are

(i) $\overline{a \oplus b} = \bar{a} * \bar{b}$

(ii) $\overline{a * b} = \bar{a} \oplus \bar{b}$ $\forall\ a, b \in L$.

Assume that $a, b \in L$.

$\therefore$ There exists elements $\bar{a}, \bar{b} \in L$ such that

$$a \oplus \bar{a} = 1, \quad a * \bar{a} = 0;$$
$$b \oplus \bar{b} = 1, \quad b * \bar{b} = 0.$$

(i) Claim: $\overline{a \oplus b} = \bar{a} * \bar{b}$

Now, $(a \oplus b) \oplus (\bar{a} * \bar{b}) = [(a \oplus b) \oplus \bar{a}] * [(a \oplus b) \oplus \bar{b}]$

$$= [a \oplus \bar{a} \oplus b] * [a \oplus b \oplus \bar{b}]$$
$$= [1 \oplus b] * [a \oplus 1]$$
$$= 1 * 1 = 1$$

Also, $(a \oplus b) * (\bar{a} * \bar{b}) = [(a \oplus b) * \bar{a}] * [(a \oplus b) * \bar{b}]$

$$= [(a * \bar{a}) \oplus (b * \bar{a})] * [(a * \bar{b}) \oplus (b * \bar{b})]$$
$$= [0 \oplus (b * \bar{a})] * [(a * \bar{b}) \oplus 0]$$
$$= (b * \bar{a}) * (a * \bar{b})$$
$$= b * (\bar{a} * a) * \bar{b}$$
$$= b * 0 * \bar{b}$$
$$= 0$$

Hence claim (i) is proved.

(ii) Claim: $\overline{a * b} = \bar{a} \oplus \bar{b}$

Now, $(a * b) \oplus (\bar{a} \oplus \bar{b}) = [(a * b) \oplus \bar{a}] \oplus [(a * b) \oplus \bar{b}]$

$= [(a \oplus \bar{a}) \star (b \oplus \bar{a})] \oplus [(a \oplus \bar{b}) \star (b \oplus \bar{b})]$

$= [1 \star (b \oplus \bar{a})] \oplus [(a \oplus \bar{b}) \star 1]$

$= (b \oplus \bar{a}) \oplus (a \oplus \bar{b})$

$= b \oplus (\bar{a} \oplus a) \oplus \bar{b}$

$= b \oplus 1 \oplus \bar{b}$

$= b \oplus \bar{b}$

$= 1$ //.

Also,

$(a \star b) \star (\bar{a} \oplus \bar{b}) = [(a \star b) \star \bar{a}] \star [(a \star b) \star \bar{b}]$

$= [(a \star b) \star \bar{a}] \oplus [(a \star b) \star \bar{b}]$

$= [a \star \bar{a} \star b] \oplus [a \star b \star \bar{b}]$

$= [0 \star b] \oplus [a \star 0]$

$= 0 \oplus 0$

$= 0$

There for claim (ii)° is proved.

Hence the De-Morgan's laws are proved.

——x——x——x——x——.

Problem:

Show that in any Boolean algebra,

$(a+b)(a'+c) = ac + a'b + bc$.

Solu:

Let $(B, +, \cdot, ')$ be a Boolean algebra, and $a, b, c \in B$.

$$\begin{aligned} LHS &= (a+b)(a'+c) \\ &= (a+b)a' + (a+b)c \\ &= aa' + ba' + ac + bc \\ &= 0 + a'b + ac + bc \\ &= ac + a'b + bc \\ &= RHS. \end{aligned}$$

— x — x — x —.

Problem:

In any Boolean algebra, show that $a = b$ iff $a\bar{b} + \bar{a}b = 0$

Solu:

Let $(B, +, \cdot, ', 0, 1)$ be any Boolean algebra.

Let $a, b \in B$ and $a = b$.

T.P $a\bar{b} + \bar{a}b = 0$

Now, $a\bar{b} + \bar{a}b = a\bar{a} + \bar{a}a$

$= 0 + 0$

$= 0$

Let $a\bar{b} + \bar{a}b = 0$ for all $a, b \in B$

T.P $a = b$.

Now, $a = a \cdot 1$

$= a \cdot (b + \bar{b})$

$= ab + a\bar{b}$

$= ab + \bar{a}b$

$= (a + \bar{a}) \cdot b$

$= 1 \cdot b$

$= b$.

Hence proved.

Problem:

Simplify (i) $(a \star b)' \oplus (a \oplus b)'$

(ii) $(a' \star b' \star c) \oplus (a \star b' \star c) \oplus (a \star b' \star c')$.

Soln:

(i) $(a \star b)' \oplus (a \oplus b)'$

$= (a' \oplus b') \oplus (a' \star b')$

$= [(a' \oplus b') \oplus a'] \star [(a' \oplus b') \oplus b']$

$= (a' \oplus b') \star (a' \oplus b')$

$= a' \star b'$

(ii) $(a' \star b' \star c) \oplus (a \star b' \star c) \oplus (a \star b' \star c')$

$= (a' \oplus a) \star (b' \star c)$

$= 1 \star (b' \star c)$

$= b' \star c$ //.

Theorem:

(X) In a Boolean algebra $(L, \oplus, *)$ (i.e) Complemental and distributive lattice) show that the complement $\bar{a}$ of any element $a \in L$ is unique.

Proof:

Let $a \in L$ has two complement $b \& c \in L$.

By defn, $a * b = 0$, $a \oplus b = 1$

$a * c = 0$, $a \oplus c = 1$

We have, $b = b * 1$

$= b * (a \oplus c)$

$= (b * a) \oplus (b * c)$

$= 0 \oplus (b * c)$

$= b * c \longrightarrow (1)$

$c = c * 1$

$= c * (a \oplus b)$

$= (c * a) \oplus (c * b)$

$= 0 \oplus (c * b)$

$= c * b$

$= b * c \longrightarrow (2)$

By (1) & (2), $b = c$

Hence every element of L has a unique complement.

— x — x — x —

Problem:

Let a, b, c be any elements in a Boolean algebra B. Prove that (i) $a * a = a$ (ii) $a + a = a$

Solu:

(i) Let $a = a * 1$

$= a * (a + a')$

$= (a * a) + (a * a')$

$= (a * a) + 0$

$= a * a.$

(ii) Similarly by duality,

$a + a = a.$

Problem:

Let a, b, c be any elements in a Boolean algebra B. Show that (i) $a + 1 = 1$ (ii) $a * 0 = 0$

Solu:

Let $a * 0 = (a * 0) + 0$

$= (a * 0) + (a * a')$

$= a * (0 + a')$

$= a * (a' + 0)$

$= a * a'$

$= 0.$

Similarly by duality, $a + 1 = 1.$

Problem:

Let a, b, c be any elements in a Boolean algebra B. Show that (i) $a + (a * b) = a$

(ii) $a * (a + b) = a$.

Solu:

Let $a * (a+b) = (a+0) * (a+b)$

$= a + (0 * b)$

$= a + (b * 0)$

$= a + 0$

$= a$.

Similarly by duality $a + (a * b) = a$.

Problem:

Let a, b, c any elements in a Boolean algebra B. Show that (i) $(a+b)+c = a+(b+c)$.

(ii) $(a * b) * c = a * (b * c)$

Solu:

Let $L = (a * b) * c$ and $R = a * (b * c)$

T.P $L = R$.

(i.e) T.P $a + L = a + R$

Now, $a + L = a + [(a * b) * c]$

$= [a + (a * b)] * (a + c)$

$= a * (a + 1)$

$= a$ [By Absorption law (1)]

Also, $a+R = a+(a\star(b\star c))$

$= (a+a)\star(a+(b\star c))$

$= a\star(a+(b\star c))$

$= a \longrightarrow (2)$

Thus $a+L = a+R$ [By (1) & (2)].

Next we show that,

$a'+L = a'+R$.

Now, $a'+L = a'+[(a\star b)\star c]$

$= [a'+(a\star b)]\star(a'+c)$

$= (a'+a)\star(a'+b)\star(a'+c)$

$= [1\star(a'+b)]\star(a'+c)$

$= (a'+b)\star(a'+c)$

$= a'+(b\star c) \longrightarrow (1)$

Also, $a'+R = a'+(a\star(b\star c))$

$= (a'+a)\star(a'+(b\star c))$

$= 1\star(a'+(b\star 7)c)$

$= a'+(b\star c) \longrightarrow (2)$

Thus from (1) & (2), we get $a'+L = a'+R$.

Thus we get from ① & ②,

$$a' + L = a' + R.$$

Now, $L = 0 + L = (a * a') + L$

$$= (a + L) * (a' + L)$$

$$= (a + R) * (a' + R)$$

$$= (a * a') + R$$

$$= 0 + R$$

$$= R.$$

Hence the proof.

Problem:

In any Boolean algebra, show that

$$(a+b)(b+c)(c+a') = (a'+b)(b'+c)(c'+a)$$

Proof:

$$\text{LHS} = (a+b'+0)(b+c'+0)(c+a'+0)$$

$$= (a+b'+c\cdot c')(b+c'+aa')(c+a'+bb')$$

$$= (a+b'+c)(a+b'+c')(b+c'+a)(b+c'+a')$$

$$(c+a'+b)(c+a'+b').$$

$$= \{a+b+c(a'+b+c')\} \cdot \{(b'+c+a)(b'+c+a')\}$$

$$\& \{(c'+a+b)(c'+a+b')\}$$

$= (a'+b+cc')\ (b'+c+aa')\ (c'+a+bb')$

$= (a'+b+0)\cdot(b'+c+0)\ (c'+a+0)$

$= (a'+b)(b'+c)(c'+a)$.

$=$ RHS.

Problem:

In any Boolean algebra show that

$a = 0 \Leftrightarrow ab' + a'b = b$

Soln:

If $a = 0$, clearly $ab' + a'b = 0 + 1b$

$= 0 + b = b$

Suppose $b = ab' + a'b \longrightarrow (1)$

$\therefore 0 = bb' = b'(ab' + a'b)$

$= b'(ab' + a'b)$

$= ab' + 0$

$= ab'$

Using De Morgan's from (1), we obtain

$b' = (a'+b)(a+b')$

$\therefore 0 = ab' = a(a'+b)(a+b')$

$= (aa' + ab)(a+b')$

$= (0 + ab)(a+b')$

$= ab(a+b')$,

$= aba + abb'$

$= ab + 0 = ab$.

$\therefore 0 = ab = ab'$

$\therefore 0 = ab + ab' = a(b+b')$

$= a \cdot 1 = a$

Hence $a = 0$.

Def: Hasse diagram or partially ordered set diagram

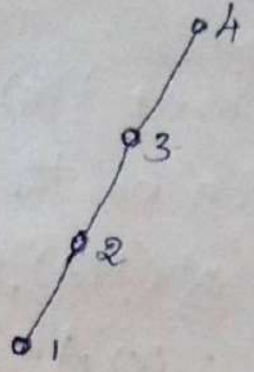
A partial ordering $\leq$ on a set P can be represented by means of a diagram known as a Hasse diagram or a partially ordered set diagram of $(P, \leq)$. In such a diagram, each element is represented by a small circle or a dot.

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.

If $x < y$ but y does not cover x, then x and y are not connected directly by a single line. However, they are connected through one or more elements of P. It is possible to obtain the set of ordered pairs in $\leq$ from such a diagram.

Example:

Let $P = \{1, 2, 3, 4\}$ and $\leq$ be the relation "less than or equal to" then the Hasse diagram is

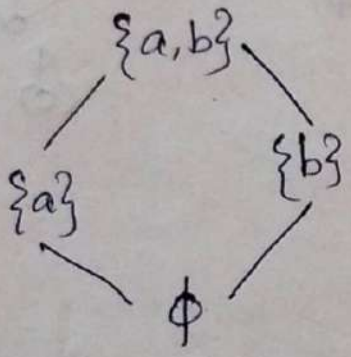


Example:

Let $A = \{a, b\}$.

$B = P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$

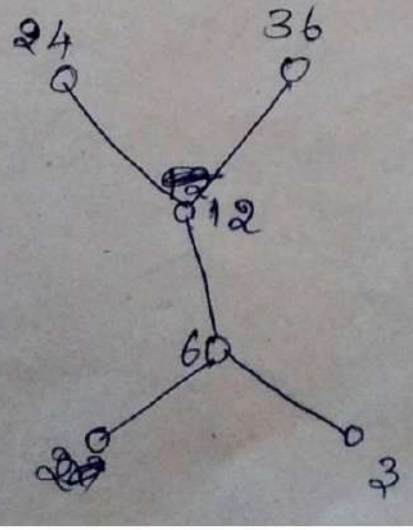
Then $\subseteq$ is a relation ~~on a whose di~~



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 $(X, \leq)$.

Solu:



Example: 5

Let A be a given finite set P(A) its power set. Let $\subseteq$ be the inclusion relation on the elements of P(A). Draw Hasse diagram of $(P(A), \subseteq)$ for

(a) $A = \{a\}$; (b) $A = \{a, b\}$; (c) $A = \{a, b, c\}$;

Soln: