UNIT-I LOGIC

Logic is concerned with all kinds of reasoning, whether they be a legal arguments or mathematical proofs or conclusions in a scientific theory based upon set of hypothesis. It is the theoretical basis for many areas of computer science such as digital logic design, construction of computer programs & its verification, artificial intelligence, automata theory etc. It is the foundation on which a comp sys is built in ... bits are switched on & off using 1's & 0's, in boolean logic, there ... T or F

There are 2 main components of logic

(i) propositional logic (ii) predicate logic.

propositional logic deals with propositions & the the analysis of propositions.

predicate logic deals with predicate which are propositions containing variables

propositional logic: The study of propositional logic consist of syntax (grammar), sematics (meaning), inference rule & derivation.

propositional logic can be considered as a language of human reasoning. This language is based on symbols which consist of

i) propositional variables denoted by p, q, r, s (which are simple statement)

ii) propositional constants denoted by T, F

iii) connectives or basic logical operators denoted by $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$.

Defn: A proposition or statement is a declarative sentence that is either T or F but not both.

Note: Sentences which are exclamatory, interrogative & imperative in nature are not proposition.

Examples:

1. $x^2+9=0$ (statement) $x+2=5$
2. $x^2+2x+1=0$ (statement)

(statement)

3. Chennai is the capital of TN (statement).
4. study Discrete mathematics (Not a statement)
5. open the door (" ")
6. can you speak tamil (" ")
7. wow! what a beautiful place (" ")

primary statements (Atomic statements)

A declarative sentence which cannot be split up into simple sentences are called primary statements.

In other words, primary statements do not contain logical connectives. (i.e, or, and, if, if & only if ...).

Eg: (i) Malini is a dancer (primary statement).

(ii) Malini is a dancer & also good singer (not a primary statement).

Compound statement: (Molecular proposition)

A proposition obtained by combining two or more propositions by means of logical connectives is called a compound statement.

Eg: Sridevi & Swathi went to their native place.

Connectives: Connective is an operation which is used to connect 2 or more than 2 statements. Simply it is called sentential connectives. It is also known as logical connectives or logical operators.

Five Basic Connectives

logical connectives	Name	symbols	Type of operator
NOT	Negation	$\neg$ (or) $\sim$	unary
AND	Conjunction	$\wedge$	Binary
OR	Disjunction	$\vee$	Binary
If...then	Conditional (or) Implication	$\rightarrow$	Binary
If & only if	Biconditional	$\rightleftarrows$ or $\leftrightarrow$	Binary

Truth table: The truth value of a proposition is either true (T) or False (F).

A truth table is a table that shows the truth value of a compound proposition & possible cases.

If the compound statement have 'n' variables then the truth value will have 2^n possibilities.

Example: 1) If the compound statement have 2 variables P & Q then the possible truth value are in the table.

Truth table:

P	T	T	F	F
Q	T	F	T	F

2) If the compound statement have 3 variables P, Q, R then the possible truth value are

P	T	T	T	T	F	F	F	F
Q	T	T	F	F	T	T	F	F
R	T	F	T	F	T	F	T	F

1) **Negation ($\neg$ or $\sim$) (not):** If P is a proposition then the negation of P is written as '$\neg$P' & is read as 'not P'. If P has truth value T then '$\neg$P' has truth value F & vice versa.

Example: 1) P: Today is saturday (T)

$\neg$P: Today is not saturday (F).

2) P: chennai is a city (T)

$\neg$P: chennai is not a city (F).

Truth table:

P	$\neg$P
T	F
F	T

Conjunction ($\wedge$) (and) : If P & q are 2 propositions then the conjunction of P & q is the compound proposition P & q and is denoted by $P \wedge q$. If both P & q have the same truth value T, then $P \wedge q$ is T otherwise $P \wedge q$ is F.

Eg: ① P : Today is monday (T)

q : This is the month of july (T)

$P \wedge q$: Today is monday & the month of july (T).

② P : $3 < 5$ (T)

q : $2+3=6$ (F)

$P \wedge q = 3 < 5$ & $2+3=6$ (F).

Truth table :

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

Disjunction ($\vee$) (or) : The disjunction of 2 statements P & Q is the statement denoted by $P \vee Q$ read as P or Q.

$P \vee Q$ has the truth value T if anyone of P or Q has truth value T & otherwise it is F.

Example : P : There are 10 birds.

Q : There are 5 birds

$P \vee Q$: There are 10 or 5 birds.

Truth table :

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

Conditional statement : ($\rightarrow$) (If...then).

If P & Q are any 2 propositions then the statement $P \rightarrow Q$ which is read as "if P then Q" is called as conditional statement, $P \rightarrow Q$ is F if P is T & Q is F. In other case $P \rightarrow Q$ is T.

Eg: P : It is hot (T)

Q : $5+3=6$ (F).

$P \rightarrow Q$: If it is hot then $5+3=6$ (F).

Truth table :

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

Biconditional : ($\leftrightarrow$ or $\rightleftarrows$) (iff)

If P & Q be any 2 statement then the

statement $P \leftrightarrow Q$ which read as "P if & only if" is called biconditional statement. The statement $P \leftrightarrow Q$ is T whenever P & Q have the same truth values & otherwise is F.

Truth value:

P :	T	T	F	F
Q :	T	F	T	F
$P \leftrightarrow Q$:	T	F	F	T

Eg: P : Selvam can write the examinations (T)

Q : Selvam pays the fees (T)

$P \leftrightarrow Q$: Selvam can write the examinations if & only if he pays the fees (T).

<u>statement formula:</u> A statement formula is an expression which is a string consisting of variables, parenthesis & connective symbols.

<u>well formed formula:</u> A well formed formula can be generated by the following rules:

i) A statement variable standing alone is a well formed formula.

ii) If A is a well formed formula, then $\neg A$ is a well formed formula.

(iii) If A & B are well formed formula, then $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ & $(A \leftrightarrow B)$ are well formed formula.

(iv) A string of symbols containing the statement variables, connectives & paranthesis is a well formed formula, iff it can be obtained by finitely many application of the above 3 steps.

Consider the following statement:

i) $\neg P \wedge Q$ is a wff.

ii) $(P \rightarrow Q) \wedge R$ is a wff.

iii) $P \rightarrow (Q \wedge R)$ is not wff. [$P \rightarrow (Q \wedge R)$ is wff or $(P \rightarrow Q) \wedge R$ is wff].

iv) $(P \rightarrow Q$ is not a wff. since one paranthesis in the right is missing while $(P \rightarrow Q)$ or $P \rightarrow Q$ are wff.

<u>Problems</u>: ① write the following statements in symbolic forms:

If either S. Pavithra takes calculus or sharnika takes sociology, then malathy will take english.

<u>Soln:</u> P : S. Pavithra takes calculus.

Q : sharnika takes sociology.

R : malathy takes English.

$(P \vee Q) \rightarrow R$.

② If P: Malathy is rich
Q: Malathy is happy.
write in symbolic form:

a) Malathy is poor but happy.
b) Malathy is rich or unhappy.
c) Malathy is neither rich nor happy.

Soln: Given P: malathy is rich —①
¬P : malathy is poor —②
Given, Q: Malathy is happy —③
¬Q: Malathy is unhappy —④

a) combining ② & ③, we get, malathy is poor & happy i.e, $\neg P \wedge Q$.
b) Combining ① + ④, malathy is rich or unhappy i.e, $P \vee \neg Q$
c) Combining ② + ④, malathy is neither rich nor happy i.e, $\neg P \vee \neg Q$.

Construct the truth table:

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

Soln

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

② $(P \wedge (P \to Q)) \to Q$.

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

③ $P \leftrightarrow (Q \vee P)$

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

④ $\neg P \vee (Q \to R)$.

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

HW ① $\neg(P \vee Q) \wedge (P \vee R)$ Ans: [FFFFFFTF]
② $(P \to Q) \leftrightarrow (\neg P \vee Q)$ Ans [TTTT]

3. $(P \wedge Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q)$ Ans: [T, T, T, F]

Tautologies & contradiction

Tautology: A logical expression is said to be a tautology if it is true under all possible assignment.

Eg:

P	¬P	P ∨ ¬P
T	F	T
F	T	T

∴ $P \vee \neg P$ is a tautology.

Contradiction: A logical expression is said to be a contradiction if it is false under all possible assignment.

Eg:

P	¬P	P ∧ ¬P
T	F	F
F	T	F

∴ $P \wedge \neg P$ is a contradiction.

Problems: ① Determine which of the following compound propositions are tautologies & which of them are contradictions, using truth tables.

$((p \to q) \wedge (q \to r)) \to (p \to r)$.

p	q	r	p→q	p→r	q→r	(p→q) ∧ (q→r)	(p→q)∧(q→r) → (p→r)
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	T	F	T
T	F	F	F	F	T	F	T
F	T	T	T	T	T	T	T
F	T	F	F	T	T	F	T
F	F	T	F	T	F	F	T
F	F	F	T	T	T	T	T

Since the truth value of the given statement is T ∀ combinations of truth values of p, q, r.

∴ It is a tautology.

② $(\underbrace{\neg(q \to r) \wedge r}_{A}) \wedge (p \to q)$ — ①

p	q	r	p→q	q→r	¬(q→r)	A	①
T	T	T	T	T	F	F	F
T	T	F	T	F	T	F	F
T	F	T	F	T	F	F	F
T	F	F	F	T	F	F	F
F	T	T	T	T	F	F	F
F	T	F	T	F	T	F	F
F	F	T	T	T	F	F	F
F	F	F	T	T	F	F	F

The given statement contains only F as the truth value. ∴ It is a contradiction.

3. $((P \vee Q) \wedge (q \to r)) \wedge (q \to r)) \to r$ Tautology.
4. $P \to (P \vee q)$ Tautology
5. $(q \to P) \wedge (\neg P \wedge q)$ Contradiction.
6. $(\neg q \wedge (P \to q)) \to \neg P$ Tautology.

Equivalence of Formulae: $\Leftrightarrow$

The two statement formulas A & B are equivalent iff $A \to B$ (or) $A \rightleftarrows B$ is a tautology. It is denoted by the symbol $A \Leftrightarrow B$ which is read as "A is equivalent to B".

Eg: $P \to Q \Leftrightarrow \neg Q \to \neg P$.

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

Tautological Implications: A statement A is said to tautologically imply to a statement B iff $A \to B$ is a tautology.
we denote it as "$A \Leftrightarrow B$" which is read as "A implies B".

Note that, $A \Leftrightarrow B$ means a 2 way implication
$A \Rightarrow B$ means a 1 way implication.

Example: ① Consider the statement $(P \wedge Q) \to P$

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

Since $(P \wedge Q) \to P$
∴ $P \wedge Q \Rightarrow P$

② prove the following equivalence

$\underset{Ⓐ}{(P \to q) \wedge (P \to r)} \longleftrightarrow \underset{Ⓑ}{P \to (q \wedge r)}$ — I

P	q	r	$P \to q$	$P \to r$	$q \wedge r$	Ⓐ	Ⓑ	Ⓘ
T	T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F	T
T	F	T	F	T	F	F	F	T
T	F	F	F	F	F	F	F	T
F	T	T	T	T	T	T	T	T
F	T	F	T	T	F	T	T	T
F	F	T	T	T	F	T	T	T
F	F	F	T	T	F	T	T	T

Since $(P \to q) \wedge (P \to r) \Leftrightarrow P \to (q \wedge r)$ is a tautology.

$(P \to q) \wedge (P \to r) \Leftrightarrow P \to (q \wedge r)$.

3. $p \to (q \to r) \Rightarrow (p \to q) \to (p \to r)$ — (I)

(A) = $p \to (q \to r)$, (B) = $(p \to q) \to (p \to r)$

p	q	r	$q \to r$	(A)	$p \to q$	$p \to r$	(B)	(I)
T	T	T	T	T	T	T	T	T
T	T	F	F	F	T	F	F	T
T	F	T	T	T	F	T	T	T
T	F	F	T	T	F	F	T	T
F	T	T	T	T	T	T	T	T
F	T	F	F	T	T	T	T	T
F	F	T	T	T	T	T	T	T
F	F	F	T	T	T	T	T	T

Since $p \to (q \to r) \to (p \to q) \to (p \to r)$ is a tautology $\therefore p \to (q \to r) \Rightarrow (p \to q) \to (p \to r)$.

4. $p \vee \neg(q \wedge r) \wedge \neg p \Rightarrow (\neg q \vee \neg r)$

5. $\neg(p \leftrightarrow q) \Leftrightarrow \neg p \leftrightarrow q$

6. $\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg q$

7. $\neg p \Rightarrow p \to q$

8. $\neg(p \to q) \Rightarrow p$

9. $p \wedge (p \to q) \to q$.

Logical Equivalences (or) Equivalence Rules

laws	Rules
1. Idempotent laws	$p \wedge p \Leftrightarrow p$, $p \vee p \Leftrightarrow p$
2. Associative laws	$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$ $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$.
3. Commutative laws	$p \wedge q \Leftrightarrow q \wedge p$ $p \vee q \Leftrightarrow q \vee p$.
4. De morgan's law	$\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$ $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$
5. Distributive law	$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
6. Complement laws	$p \wedge \neg p \Leftrightarrow F$ $p \vee \neg p \Leftrightarrow T$
7. Dominance laws	$p \vee T \Leftrightarrow T$ $p \wedge F \Leftrightarrow F$.
8. Identity laws	$p \wedge T \Leftrightarrow p$ $p \vee F \Leftrightarrow p$
9. Absorption laws	$p \vee (p \wedge q) \Leftrightarrow p$ $p \wedge (p \vee q) \Leftrightarrow p$
10. Double negation law	$\neg(\neg p) \Leftrightarrow p$
11. Contra +ve law	$p \to q \Leftrightarrow \neg q \to \neg p$

12. Conditional as disjunction $\quad P \to q \Leftrightarrow \neg p \vee q$

13. Biconditional as conditional. $\quad P \leftrightarrow q \Leftrightarrow (P \to q) \wedge (q \to P)$

① without using truth table show that $Q \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$ is a tautology.

Soln:

	Reasons
$Q \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$	
$\Rightarrow Q \vee ((P \vee \neg P) \wedge \neg Q)$	Distributive law.
$\Rightarrow Q \vee (P \vee \neg P) \wedge (Q \vee \neg Q)$	"
$\Rightarrow (Q \vee T) \wedge T$	$\because P \vee \neg P \Rightarrow T$
$\to T \wedge T$	$P \vee T = T$
$\Rightarrow T$	

$\therefore$ Given statement is tautology.

② Determine whether $(\neg Q \wedge (P \to Q)) \to \neg p$ is a tautology.

	Reason
$(\neg Q \wedge (P \to Q)) \to \neg P$	
$\Rightarrow (\neg Q \wedge (\neg P \vee Q)) \to \neg P$	Conditional as disjunction.
$\Rightarrow \neg(\neg Q \wedge (\neg P \vee Q)) \vee \neg p$	"
$\Rightarrow Q \vee (P \wedge \neg Q) \vee \neg P$	Demorgan's law
$\Rightarrow ((Q \vee P) \wedge (Q \vee \neg Q)) \vee \neg P$	distributive law.
$\Rightarrow ((Q \vee P) \wedge T) \vee \neg P$	$(P \vee \neg P = T)$
$\Rightarrow (Q \vee P) \vee \neg P$	$(\because P \wedge T \Leftrightarrow P)$
$\Rightarrow Q \vee (P \vee \neg P)$	Associate law.
$\Rightarrow Q \vee T$	$(P \vee \neg P = T)$.
$\Rightarrow T$	$(P \vee T = T)$

$\therefore$ It is tautology.

③ using truth table show that P is equivalent to (i) $(P \wedge Q) \vee (P \wedge \neg Q)$ (ii) $(P \vee Q) \wedge (P \vee \neg Q)$

Soln: To prove $P \Leftrightarrow (P \wedge Q) \vee (P \wedge \neg Q)$.

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

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

ii) To prove $P \Leftrightarrow (P \vee Q) \wedge (P \vee \neg Q)$

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

$\therefore$ the result.

Prove the following equivalences

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

① Without using truth table S.T $\neg(P \vee (\neg P \wedge Q))$ & $\neg P \wedge \neg Q$ are logically equivalent.

Soln

	Reasons
$\neg(P \vee (\neg P \wedge Q))$	
$\Leftrightarrow \neg P \wedge [\neg(\neg P) \wedge Q]$	Demorgan's law
$\Leftrightarrow \neg P \wedge [\neg(\neg P) \vee \neg Q]$	"
$\Leftrightarrow \neg P \wedge (P \vee \neg Q)$	Double negation
$\Leftrightarrow (\neg P \wedge P) \vee (\neg P \wedge \neg Q)$	Distributive law
$\Leftrightarrow F \vee (\neg P \wedge \neg Q)$	$\neg P \wedge P \Leftrightarrow F$
$\Leftrightarrow (\neg P \wedge \neg Q) \vee F$	commutative law
$\Leftrightarrow \neg P \wedge \neg Q$	Identity law.

② $(P \vee q) \wedge (\neg P \wedge (\neg P \wedge q)) \Leftrightarrow \neg P \wedge q$

Soln

	Reason
$(P \vee q) \wedge (\neg P \wedge (\neg P \wedge q))$	
$\Leftrightarrow (P \vee q) \wedge ((\neg P \wedge \neg P) \wedge q)$	Associative law
$\Leftrightarrow (P \vee q) \wedge (\neg P \wedge q)$	Idempotent law
$\Leftrightarrow (P \vee q) \wedge (q \wedge \neg P)$	Commutative law
$\Leftrightarrow ((P \vee q) \wedge q) \wedge \neg P$	Associative law.
$\Leftrightarrow q \wedge \neg P$	Absorption law
$\Leftrightarrow \neg P \wedge q$	Commutative law.

$\therefore$ It is equivalent.

③ $(P \vee Q) \wedge \neg P \Leftrightarrow \neg P \wedge Q$.

Soln

	Reasons
$(P \vee Q) \wedge \neg P$	
$\Leftrightarrow \neg P \wedge (P \vee Q)$	commutative law
$\Leftrightarrow (\neg P \wedge P) \vee (\neg P \wedge Q)$	Distributive law.
$\Leftrightarrow F \vee (\neg P \wedge Q)$	$P \wedge \neg P = F$
$\Leftrightarrow \neg P \wedge Q$	Identity law.

$\therefore$ It is equivalent.

H.W

1. $P \to (Q \to R) \Leftrightarrow (P \wedge Q) \to R$
2. $(P \to r) \wedge (Q \to r) \Leftrightarrow (P \vee q) \to r$
3. $(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R) \Leftrightarrow R$.

The Theory of Inference

Laws of Implication & Equivalence

1. Detachment law : $(p \to q) \wedge p \Rightarrow q$
2. Contrapositive law : $(p \to q) \wedge \neg q \Rightarrow \neg p$
3. Disjunctive addition: $p \Rightarrow p \vee q$, $q \Rightarrow p \vee q$.
4. Conjunctive simplification: $p \wedge q \Rightarrow p$, $p \wedge q \Rightarrow q$
5. Disjunctive simplification: $(p \vee q) \wedge \neg p \Rightarrow q$
   $(p \vee q) \wedge \neg q \Rightarrow p$.
6. Chain Rule : $(p \to q) \wedge (q \to r) \Rightarrow (p \to r)$
7. Conditional Equivalence:
   $(p \to q) \Leftrightarrow \neg q \to \neg p \Leftrightarrow \neg p \vee q$.
8. Biconditional Equivalence:
   $(p \leftrightarrow q) \Leftrightarrow (p \to q) \wedge (q \to p) \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$.

A thm consists of a set of premises & a conclusion. A thm is proved by showing that the conclusion is T whenever all the premises are assumed to be T

The Theory of Inference:

<u>Defn</u>: To check the logical validity of the conclusion, from the given set of premises, by making use of equivalences rule & implication rule. The theory associated with such things is called inference theory.

Note: premesis is a statement which is assumed to be T

Rules for Inference theory:

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

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

Rule CP: If we can derive S from R & a ~~set~~ of gnl. premises, then we can derive $R \to S$ from the set of premises alone.

In such a case R is taken as an additional premise. Rule CP is also called the deduction thm.

The analysis of the validity of the formula from the given set of premises by using derivation is called "Theory of inference".

Remark: whenever the assumed premise is used in the derivation, then the method of derivation is called indirect method of derivation.

Problems: ① Demonstrate that R is a valid inference from the premises $P \to Q$, $Q \to R$ & P.

Soln. Given premises are

1) $P \to Q$
2) $Q \to R$ Conclusion is R.
3) P.

Step	Derivation	Rule
1.	$P \to Q$	P
2.	$Q \to R$	P
3.	$P \to R$	T (1 & 2 chain rule)
4.	P	P
5.	R	T (from 3 & 4) (Detachment law)

② S.T $R \vee S$ logically follows from the premises $C \vee D$, $(C \vee D) \to \neg H$, $\neg H \to (A \wedge \neg B)$ & $(A \wedge \neg B) \to R \vee S$.

Soln: Given 1) $C \vee D$

2) $(C \vee D) \to \neg H$

3) $\neg H \to (A \wedge \neg B)$

4) $(A \wedge \neg B) \to R \vee S$.

Step	Derivation	Rule
1.	$C \vee D$	P
2.	$(C \vee D) \to \neg H$	P
3.	$\neg H$	T (from 1 & 2) Detachment law
4.	$\neg H \to (A \wedge \neg B)$	P
5.	$A \wedge \neg B$	(from 3 & 4) Detachment law
6.	$(A \wedge \neg B) \to R \vee S$	P
7.	$R \vee S$	T, from 5 & 6, Detachment law

3. S.T $R \to S$ can be derived from the premises $P \to (Q \to S)$, $\neg R \vee P$ & Q.

Soln Gnl. 1. $P \to (Q \to S)$

2. $\neg R \vee P$

3. Q

steps	Derivation	laws
1.	R	Assumed premises
2.	$\neg R \vee P$	P
3	$R \to P$	T, $P \to Q \Leftrightarrow \neg P \vee Q$
4.	P	T, (from 1 & 3) (Detachment)
5.	$P \to (Q \to S)$	P
6.	$Q \to S$	T (from 4 & 5) Detachment
7.	Q	P
8.	S	T (from 6, 7)
9.	$R \to S$	Rule CP (from 1 & 8)

Note: Rule CP is generally used if the conclusion is of the form $R \to S$

HW 1. S.T $\neg P$ follows logically from the premises $\neg(P \wedge \neg Q)$, $(\neg Q \vee R)$ & $\neg R$.

2. S.T $R \wedge (P \vee Q)$ is a valid conclusion from the premises $P \vee Q$, $Q \to R$, $P \to M$ & $\neg M$.

Consistent: The gnl. set of premises $P_1, P_2 \ldots P_m$ are said to be consistent iff $P_1 \wedge P_2 \wedge \ldots \wedge P_m = T$.

Inconsistent: The gnl. set of premises $P_1, P_2 \ldots P_m$ are said to be inconsistent iff $P_1 \wedge P_2 \ldots \wedge P_m = F$.

4. S.T the foll. premises are inconsistent.

i) If Jack misses many classes due to illness, then he fails in high school.

ii) If Jack fails in high school, then he is uneducated.

iii) If Jack reads a lot of books then he is not uneducated.

iv) Jack misses many classes due to illness & reads a lot of books.

Soln: let us consider the atomic statement

P: Jack misses many classes due to illness

Q: Jack fails in high school.

R: Jack reads a lot of books

S: Jack is uneducated.

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

step	Derivation	Rule
1.	$P \to Q$	P
2.	$Q \to S$	P
3.	$P \to S$	T (from 1 & 2) chain rule
4.	$\neg S \to \neg P$	T (from 3) $A \to B \Leftrightarrow \neg B \to \neg A$ Conditional equivalence
5.	$R \to \neg S$	P
6.	$R \to \neg P$	T (from 5 + 4)
7.	$\neg R \vee \neg P$	T (from 6) Conditional.
8.	$\neg(P \wedge R)$	T (from 7) $(\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B)$ demorgan law
9.	$P \wedge R$	P
10.	$\neg(P \wedge R) \wedge (P \wedge R)$	T (from 8 + 9) $(\neg P \wedge P \Leftrightarrow F)$ Complement law
11.	F	

2. S.T the foll statements constitute a valid argument.

If there was rain then the travelling was difficult.

If they had umbrella, then travelling was not difficult. They had umbrella ∴ there was no rain.

Soln P : There was rain.

Q : Travelling was difficult

R : They had umbrella.

∴ The gn/. premises are 1) $P \to Q$

2) $R \to \neg Q$, 3) R.

Conclusion : $\neg P$.

step	Derivation	Rule
1.	$R \to \neg Q$	P
2.	R	P
3.	$\neg Q$	T (from 1 & 2) detachment
4.	$P \to Q$	P
5.	$\neg P$.	T $(P \to Q \wedge \neg Q \Rightarrow \neg P)$ Contrapositive law

∴ It is valid conclusion.

Indirect method of proof: In this method we assume the negation of the desired conclusion as one of the gn/. premises & we arrive at a contradiction.

1. Prove by indirect method $\neg Q, P \to Q, P \vee R \Rightarrow R$.

Sol: Include $\neg R$ as a gnl. premises.

Step	Derivation	Rule
1.	$P \vee R$	P
2.	$\neg R$	Rule CP, Assumed premises
3.	P	T (from 1 & 2) $(P \vee R) \wedge \neg R \Rightarrow P$ disjunctive simplification
4.	$P \to Q$	P
5.	Q	T (from 3 & 4) (Detachment law)
6.	$\neg Q$	P
7.	$Q \wedge \neg Q$	T (from 5 & 6).

which is nothing but false. ∴ by the method of contradiction
$(P \to Q) \wedge (Q \to R) \wedge (P \vee R) \Rightarrow R$

H.W

ST $\neg(P \wedge Q)$ follows from $\neg P \wedge \neg Q$ using indirect method.

logic

Predicate Calculus: The analysis based on atomic statement is called predicate calculus
→ words which represents quantities are called

Universal Quantifier: The symbolic representation $(\forall x)$ is read as "for all x" is called universal quantifier. It is equivalent to
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.

Example: Let us consider the statement

All men are rich

To write this statement in symbolic form:

let $M(x)$: x is a man

$R(x)$: x is rich.

then $\forall x (M(x) \longrightarrow R(x))$

universally valid statement: If the statement is valid for all the values, then the st/. is called universally valid statement.

Eg: consider the statement
$P(x) = x + 0 = 0 + x = x$,
clearly $(\forall x) \in Z$, the statement $P(x)$

is valid. $\therefore$ $P(x)$ is UVS.

Existential Quantifier: The symbolic representation $(\exists x)$ read as "for some x" is called existential quantifier. It is equivalent to
1) for some x 2) for x such that 3) There exists an x such that 4) There is an such that 5) There is atleast one x such that.

Example: Some men are clever.

$m(x)$: x is a man

$c(x)$: x is clever

$\exists(x)\,(m(x) \rightarrow c(x))$

Existentially valid statement: If the statement is valid for some of the values, then the statement is called EVS.

Eg: Consider the statement $Q(x) = x^2 - 1 = 0$.
The statement $Q(x)$ is valid only for $|x| \in z$.
$\therefore$ $Q(x)$ is EVS.

Rules in Quantifiers:

Let $P(x)$ be any statement.

Rule US: universal specification.

$(\forall x)\, P(x) \Rightarrow P(y)$

Rule UG: universal Generalisation.

$P(y) \Rightarrow (\forall x)\, P(x)$.

Rule ES: Existential specification.

$\exists(x)\, P(x) \Rightarrow P(y)$.

Rule EG: Existential Generalisation.

$P(y) \Rightarrow \exists(x)\, P(x)$

Formula in Quantifier:

1. $(\exists x)\,(A(x) \vee B(x)) \Leftrightarrow (\exists x)\, A(x) \vee (\exists x)\, B(x)$
2. $(\exists x)\,(A(x) \wedge B(x)) \Leftrightarrow (\exists x)\, A(x) \wedge (\exists x)\, B(x)$
3. $(\forall x)\,(A(x) \vee B(x)) \Leftrightarrow (\forall x)\, A(x) \vee (\forall x)\, B(x)$
4. $(\forall x)\,(A(x) \wedge B(x)) \Leftrightarrow (\forall x)\, A(x) \wedge (\forall x)\, B(x)$
5. $\neg(\forall x)\, A(x) \Leftrightarrow (\exists x)\, \neg A(x)$.
6. $\neg(\exists x)\, A(x) \Leftrightarrow (\forall x)\, \neg A(x)$
7. $(\forall x)\,(A(x) \rightarrow B(x)) \Leftrightarrow (\exists x)\, A(x) \rightarrow (\forall x)\, B(x)$
8. $(\exists x)\,(A(x) \rightarrow B(x)) \Leftrightarrow (\forall x)\, A(x) \rightarrow (\exists x)\, B(x)$
9. $(\forall x)\,(A \wedge B(x)) \Leftrightarrow A \vee (\forall x)\, B(x)$
10. $(\exists x)\,(A \wedge B(x)) \Leftrightarrow A \wedge (\exists x)\, B(x)$
11. $(\forall x)\, A(x) \rightarrow B \Leftrightarrow (\exists x)\,(A(x) \rightarrow B)$
12. $(\exists x)\, A(x) \rightarrow B \Leftrightarrow (\forall x)\,(A(x) \rightarrow B)$
13. $A \rightarrow (\forall x)\, B(x) \Leftrightarrow (\forall x)\,(A \rightarrow B(x))$
14. $A \rightarrow (\exists x)\, B(x) \Leftrightarrow (\exists x)\,(A \rightarrow B(x))$

problems: 1. S.T $(\forall x)(H(x) \to M(x)) \wedge H(y) \Rightarrow M(y)$.

Soln: The premises are $(\forall x)(H(x) \to M(x))$, $H(y)$

step	Derivation	Rule
1.	$(\forall x)(H(x) \to M(x))$	P
2.	$H(y) \to M(y)$	US from ①
3.	$H(y)$	P
4.	$M(y)$	T (from ② + ③ $\because (P \to Q) \wedge P \Rightarrow Q$)

2. S.T $(\exists x)M(x)$ follows logically from the premises $(\forall x)(H(x) \to M(x)) \wedge (\exists x)H(x)$.

Soln The premises are $(\forall x)(H(x) \to M(x))$, $(\exists x)H(x)$

step	Derivation	Rule
1.	$(\forall x)(H(x) \to M(x))$	P
2.	$H(y) \to M(y)$	US from ①
3.	$(\exists x)H(x)$	P
4.	$H(y)$	ES from ③
5.	$M(y)$	T from ② + ④
6	$(\exists x)M(x)$	EG from ⑤

3. P.T $(\exists x)(P(x) \wedge Q(x)) \Rightarrow (\exists x)P(x) \wedge (\exists x)Q(x)$

Soln The premises are $(\exists x)(P(x) \wedge Q(x))$

step	Derivation	Rule
1.	$(\exists x)(P(x) \wedge Q(x))$	P
2.	$P(y) \wedge Q(y)$	ES
3.	$P(y)$	T (from ② $\because P \wedge Q \Rightarrow P$)
4.	$Q(y)$	T (from ② $\because P \wedge Q \Rightarrow Q$)
5.	$(\exists x)P(x)$	EG from ③
6.	$(\exists x)Q(x)$	EG from ④
7.	$(\exists x)P(x) \wedge (\exists x)Q(x)$	T from ⑤ + ⑥

4. S.T $(\forall x)(P(x) \to Q(x)) \wedge (\forall x)(Q(x) \to R(x)) \Rightarrow (\forall x)(P(x) \to R(x))$

Soln: The premises are
$(\forall x)(P(x) \to Q(x))$, $(\forall x)Q(x) \to R(x)$.

Step	Derivation	Rule
1.	$(\forall x)(P(x) \to Q(x))$	P
2.	$P(y) \to Q(y)$	US (from ①)
3.	$(\forall x)(Q(x) \to R(x))$	P
4.	$Q(y) \to R(y)$	US (from ③)
5.	$P(y) \to R(y)$	T (from 2 + 4)
6.	$(\forall x)(P(x) \to R(x))$	UG (from 5)

5. S.T $(\forall x)(P(x) \vee Q(x)) \Rightarrow (\forall x)P(x) \vee (\exists x)Q(x)$.

soln let us assume, $\neg[(\forall x)P(x) \vee (\exists x)Q(x)]$ as an additional premise.

Step	Derivation	Rule.
1.	$\neg[(\forall x)P(x) \vee (\exists x)Q(x)]$	CP
2.	$\neg[(\forall x)P(x) \wedge (\exists x)Q(x)]$	T (from 1)
3.	$\neg(\forall x)P(x)$	T (from 2)
4.	$\neg(\exists x)Q(x)$	T (from 2)
5.	$(\exists x)\neg P(x)$	T (from 3)
6.	$(\forall x)\neg Q(x)$	T (from 4)
7.	$\neg P(a)$	ES (from 5)
8.	$\neg Q(a)$	US (from 6)
9.	$\neg P(a) \wedge \neg Q(a)$	T (from 7 & 8)
10.	$\neg(P(a) \vee Q(a))$	T
11.	$(\forall x)(P(x) \vee Q(x))$	P
12.	$P(a) \vee Q(a)$	US (from 11)
13.	$(P(a) \vee Q(a)) \wedge \neg(P(a) \vee Q(a))$	T (from 10 & 12)

Unit - 2

Relation and Function

Relation

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

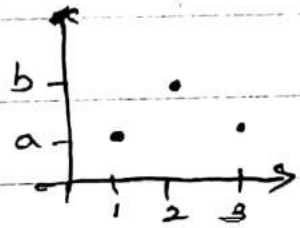
Then $A \times B = \{(1,a)(2,a)(3,a)(1,b)(2,b)(3,b)\}$

A subset of $A \times B$ is

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

R is relation from A to B.

ie, $1Ra$, $2Rb$, $3Ra$



Definition

A binary relation R from a set A to set B is defined as a subset of $A \times B$.

A relation R form A to B is represented by means of a set of ordered pairs (a,b) where $a \in A$ & $b \in B$

If $(a,b) \in R$, then a is related to b

ie, aRb

If $(a,b) \notin R$, then a is not related to b

ie, $a \not R b$.

Relation on a Set

If A is a non empty finite set then the relation A is defined as a subset of A×A.

ex:

If A = {1,2,3,4} and R = {(a,b) / a divides b} is a relation on A and R is ie.,

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

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

Note:

1) If set A has 'n' elements then the cartesian product A×A has n^2 elements. Since relation of A is a subset of A×A there are 2^{n^2} relations on a set with 'n' elts.

2) If a set A has m elements and a set B has n elements then there are 2^{mn} relations defined from A to B.

Domain and Range of a Relation:

If R is a relation from A to B, then.

Domain of $R = \{a : (a,b) \in R\}$ &

Range of $R = \{b : (a,b) \in R\}$

Inverse Relation

If R is a relation from A to B then its inverse R^{-1} is a relation from B to A and defined by

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

Ex: $R = \{(1,2)(1,3)(2,3)(2,4)(3,4)\}$ is a relation on $A = \{1,2,3,4\}$ then

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

Identity Relation

A relation R on set A defined by

$$R = \{(x,y) : (x=y)\} = I_A$$

i.e., $I_A = \{(x,x) : x \in A\}$ is called an identity relation on A.

ex:

If $A = \{1,2,3\}$ then $I_A = \{(1,1)(2,2)(3,3)\}$ is the identity relation on A.

Universal Relation:

A relation R on set A is said to be an universal relation when R coincides with $A \times A$.

ex:

If $A = \{x, y, z\}$

Then universal relation on A is

$$R = \{(x,x), (x,y) (x,z) (y,y) (y,x) (y,z) (z,z) (z,x) (z,y)\}$$

Complementary Relations

If R is relation defined on a set A, then its complementary relation $\bar{R}$ is defined by

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

ex:

If $R = \{(a,b) : a \text{ divides } b\}$ then

$\bar{R} = \{(a,b) : a \nmid b\}$

Composition of Relations:

If R is a relation from A to B and S is a relation from B to C, the composition of R and S denoted by $S \circ R$ which consists of set of order pairs (a,c) for which $a \in A$, & $c \in A$ such that $(a,b) \in R$ & $(b,c) \in S$ where $b \in B$.

i.e., $S \circ R = \{(a,c) \mid \exists\, b \in B$ with $(a,b) \in R$ and $(b,c) \in S\}$ which is a relation from A to C.

ex:

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

$S = \{(1,2)(2,3)(3,4)(4,3)\}$ are relation on $A = \{1,2,3,4\}$

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

$\because$ $(1,3) \in R$ & $(3,4) \in S \Rightarrow (1,4) \in S \circ R$

$(2,1) \in R$ & $(1,2) \in S \Rightarrow (2,2) \in S \circ R$

$(3,4) \in R$ & $(4,3) \in S \Rightarrow (3,3) \in S \circ R$

Powers of a Relation

If R is a relation defined on a set A then its powers are defined recursively by $R^1 = R$ & $R^{n+1} = R^n \circ R$.

~~ex~~ i.e., $R^2 = R \circ R$, $R^3 = R \circ^2 R$ etc.,

ex: If $R = \{(1,2)(2,3)(3,1)\}$ then

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

$(\because R^2 = R \circ R$, $1R2, 2R3 \Rightarrow 1R^2 3$ etc.,$)$

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

$(R^3 = R^2 \circ R$, $1R^2 3, 3R1 \Rightarrow 1R^3 1$

$2R^2 1, 1R2 \Rightarrow 2R^3 2$

$3R^2 2 \; 2R3 \Rightarrow 3R^3 3$

Types of Relations and their Properties:

i) Reflexive Relation:

A relation R on a set A is said to be reflexive if $(a,a) \in R$, $\forall a \in A$.

ii) Symmetric Relation.

A relation R defined on A is said to be symmetric if

$aRb \Leftrightarrow bRa$

ie., if $(a,b) \in R \Rightarrow (b,a) \in R$.

Note:

The relation R is said to be symmetric if $R = R^{-1}$

iii) Transitive Relation

A relation R is said to be transitive if $(a,b) \in R$ and $(b,c) \in R \Rightarrow (a,c) \in R$. (or)

If aRb and bRc then aRc.

ie., R is transitive if aRb and $bRc \Rightarrow aRc$.

iv) Antisymmetric Relation.

A relation R on A is said to be antisymmetric if aRb and $bRa \Rightarrow a = b$

ie., R is antisymmetric if $(a,b) \in R$ then $(b,a) \notin R$.

Note :

(i) The total number of reflexive relations defined on a set A with 'n' elements is $2^{n(n-1)}$.

Relation Matrix And the Graph of a Relation.

A relation between finite set Can be represented by means of Boolean Axger matrix (or) Zero -one matrix .

Relation Matrix:

Let R be a relation from $A = \{a_1 a_2 \cdots a_m\}$ to $B = \{b_1, b_2, b_3 \cdots b_n\}$

Then the relation R can be represented by a $m \times n$ matrix

$M_R = (m_{ij})$

where $m_{ij} = \begin{cases} 1 \text{ if } a_i R b_j \\ 0 \text{ if } a_i \not R b_j \end{cases}$

ex:

Consider the relation $R=\{(x,y)/x\le y\}$ on $A=\{1,2,3,4\}$

Soln

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

The matrix of Relation R is

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

Note:

The Relation matrix reflects some of the properties of a relation on a set.

i) If a relation is reflexive, all the diagonal elements must be 1

ii) If a relation is Symmetric, Then the relation matrix is Symmetric

iii) If a relation is antisymmetric then its relation matrix is such that if $m_{ij}=1$ then $m_{ji}=0$ for $i\ne j$

Graph of a Relation:

A relation defined on a finite set can be represented by means of a graph.

The elements of a set are represented by means of dots or small circles called nodes (or) vertex.

i) If x_i is related to x_j [$x_i R x_j$] then there is an arc joining the nodes x_i and x_j with an indication of arrow mark [$\rightarrow$]

ii) If x_i is not related to x_j [$x_i \not R x_j$], There is no arc joining the nodes x_i and x_j

iii) If x_i is related to itself [$x_i R x_i$], then there is an edge joining at node x_i and ends at x_i. Such an edge is called a loop. If [$x_i \not R x_i$] there is no loop at the node x_i.

Properties:

1) If a relation is reflexive, then there is a loop at every node.

2) If a relation is Irreflexive, then there is no loop at any node.

3) If the relation is symmedric and one node is connected to another, then there must be a return arc from second node to first.

* For antisymmetric relation, no such direct return path should exit.

Irreflexive Relation:

A relation R on a set A is irreflexive if $\forall x \in A$, $(x, x) \notin R$.

ex:

The relation "$<$" (less than) on the set of real nos., is Irreflexive.

Note: A relation R on a set 'A' is

i) Reflexive $\Leftrightarrow I_A \subseteq R$ where

$$I_A = \{(x, x) : x \in A\}$$

ii) Symmedric $\Leftrightarrow R^{-1} = R$

iii) Transitive $\Leftrightarrow R_0 R \subseteq R$.

Operations on Relations:

If R and S are relations on a set then,

$$R \cup S = \{ (x,y) / x R y \text{ or } x S y \}$$

$(x,y) \in R$ (or) $(x,y) \in S$

$$R \cap S = \{ (x,y) / (x,y) \in R \text{ and } (x,y) \in S \}$$

$$R - S = \{ (x,y) / (x,y) \in R \text{ \& } (x,y) \notin S \}$$

$$\overline{R} = \{ (x,y) / x \not R y \}$$

Matrices of the relations:

If M_R and M_S are relation matrices of R and S resp., then

$$M_{R \cup S} = M_R \vee M_S$$

$$M_{R \cap S} = M_R \wedge M_S$$

$$M_{\overline{R}} = \overline{M_R}$$

$$M_{R^{-1}} = (M_R)^T$$

$$M_{S \circ R} = (M_R)(M_S)$$

$$M_{R^n} = M_R M_R \cdots M_R$$

n Where '$\vee$' and '$\wedge$' are defined according to Boolean arithmetic

i.e., $1 \vee 1 = 1$ $\quad$ $1 \wedge 1 = 1$

$1 \vee 0 = 1$ $\quad$ $1 \wedge 0 = 0$

$0 \vee 1 = 1$ $\quad$ $0 \wedge 1 = 0$

$0 \vee 0 = 0$ $\quad$ $0 \wedge 0 = 0$

Note :

If in the digraph, the edges (x, y) and (y, z) exists then the edge (x, z) must exist for a transitive relation.

Problems :

1) Given $S = \{1, 2, \cdots 10\}$ and Relation R on S, where $R = \{(x, y) : x + y = 10\}$ What are the properties of R?

Soln

Given, $R = \{(x, y) : x + y = 10\}$

i.e., $R = \{(1,9)\ (2,8)\ (3,7)\ (4,6)\ (5,5)\ (6,4)\ (7,3)\ (8,2)\ (9,1)\}$

Properties :

i) R is neither reflexive nor irreflexive since $(5,5) \in R$ and $(x, x) \notin R$ for other elements of S.

ii) R is symmetric

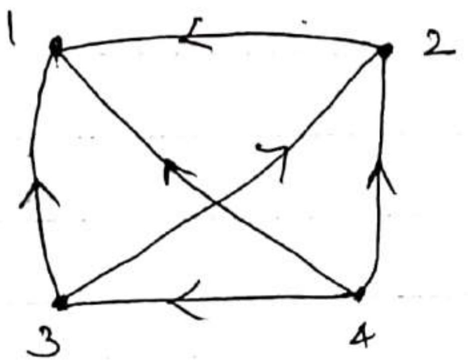
iii) R is not transitive

[i.e., $(1,9) \in R$ & $(9,1) \in R \Rightarrow (1,1) \notin R$]

3) Let $X = \{1,2,3,4\}$ and R be the relation on X defined by $R = \{(2,1)(3,1)(4,1)(3,2)(4,2)(4,3)\}$. Draw the graph of R and also give its matrix.

Soln

Graph of R:



Matrix of R:

$$M_R = \begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 3 & 1 & 1 & 0 & 0 \\ 4 & 1 & 1 & 1 & 0 \end{array}$$

4) Let $X = \{1,2,3,4\}$ & $R = \{(1,1)(1,4)(4,1)(4,4)(2,2)(2,3)(3,2)(3,3)\}$. Write

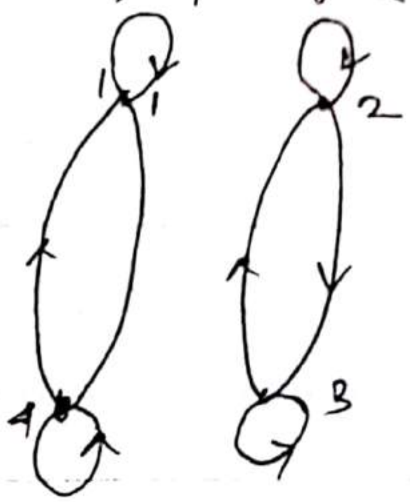
the matrix of R and draw its graph.

Soln

Matrix of R

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

Graph of R



3) Consider the set $A = \{1, 2, 3\}$. What are the properties satisfied by the following relations?

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

ii) $R_2 = \{(1,1)(2,2)(1,2)(2,1)\}$

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

iv) $R_4 = \{(1,1)(2,2)(3,3)(1,2)(2,1)(2,3)(3,2)\}$

v) $R_5 = \{(1,1)(1,2)(2,3)\}$

Soln i) R_1 is reflexive, symmetric and transitive.

ii) R_2 is symmetric, transitive but not symmetric

iii) R_3 is reflexive, transitive but not symmetric.

iv) R_4 is reflexive, symmetric but not transitive

v) R_5 satisfies none of the properties of reflexive, symmetric & transitive.

Connectivity Relation:

Let R be a relation on a set A. The connectivity relation of R is defined by

$R^{\infty} = \{(x, y) \mid$ there is a path from x to y (or) y is reachable from x by means of some path of any length$\}$

Some well known Relations and Their Properties:

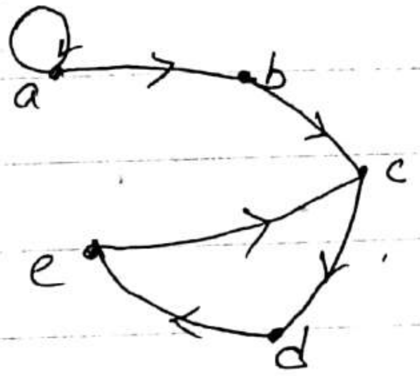
Set	Relation	Properties.
i) $\mathbb{R}$, set of real nos.,	$>$ (greater than) $<$ (less than)	Irreflexive & transitive.

ii) R, set of real nos,	= (equality)	Reflexive, Symmetric, transitive
iii) X, the collection of subsets of a set.	i) Set inclusion ($\subseteq$)	Reflexive, symmetric transitive.
	ii) Proper inclusion ($\subset$)	Irreflexive, antisymmetric, transitive.

4) Let $A = \{a, b, c, d, e\}$ and $R = \{(a,a)(a,b)(b,c)(c,e)(c,d)(d,e)\}$ be a relation on A. Compute R^2 and R^∞.

Soln

i) R^2:



$R^2 = R_o R$

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

ii) R^∞

$R^\infty = \{(x,y) / y$ is reachable from x by a path of any length$\}$

$= \{(a,a)\ (a,b)\ (a,c)\ (a,d)\ (a,e)\ (b,c)$
$(b,d)\ (b,e)\ (c,d)\ (c,e)\ (d,e)\}$ //

5) Let R and S be relations on set $A = \{1,2,3\}$ with relation matrices

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

Find the matrices of the following relations. i) $R \cup S$ ii) $R \cap S$ iii) $\overline{R}$ iv) R^{-1} v) $S \circ R$.

Soln From the matrix we get

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

i) $M_{R \cup S} = M_R \vee M_S$

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

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

ii) $M_{R \cap S} = M_R \wedge M_S.$

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

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

iii) $M_{\overline{R}} = \overline{M_R}$

$\overline{R}$ is the complement of R that consists of elements of A×A that are not in R. i.e., $\overline{R} = \{(1,2)\ (2,1)\ (3,1)\ (3,2)\ (3,3)\}$

$$\therefore M_{\overline{R}} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

iv) $M_{R^{-1}} = (M_R)^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$

v) $M_{S \circ R} = M_R \odot M_S = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \odot \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

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

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

6) If R is the relation on $A = \{1, 2, 3\}$ such that $(a,b) \in R$, if and only if $a+b =$ even, find the relation matrix M_R. Find also the relational matrices R^{-1}, $\overline{R}$ & R^2.

Soln

Given, $A = \{1,2,3\}$, $(a,b) \in R \Leftrightarrow a+b =$ even

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

$$\therefore M_R = \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \end{array}$$

i) $M_{R^{-1}} = (M_R)^T$

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

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

$$\therefore M_{\overline{R}} = \overline{M_R} = \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \end{array}$$

(which is the same as the matrix obtained from M_R by changing 0's to 1's & 1's to 0's)

iii) $M_{R^2} = M_R \cdot M_R$

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

$$= \begin{bmatrix} 1\vee0\vee1 & 0\vee0\vee0 & 1\vee0\vee1 \\ 0\vee0\vee0 & 0\vee1\vee0 & 0\vee0\vee0 \\ 1\vee0\vee1 & 0\vee0\vee0 & 1\vee0\vee1 \end{bmatrix}$$

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

H.W

7. Let $A = \{1,2,3\}$ & $B = \{1,2,3,4\}$ and R and S be the relations from A to B whose matrices are.

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

Compute i) $\bar{S}$ ii) $R \cap S$ iii) $R \cup S$ iv) R^{-1}

Soln From the matrices we get Relations

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

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

i) $\bar{S} = \{(1,1)\ (1,4)\ (2,2)\ (2,3)\ (3,3)\ (3,4)\}$

$$M_{\bar{S}} = \overline{M_S} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

ii) $M_{R \cap S} = M_R \wedge M_S$

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

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

iii) $M_{R \cup S} = M_R \cup M_S = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \vee \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$

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

iv) $M_{R^{-1}} = (M_R)^T = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$

8) Let R and S be relations on set A with

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

Find the matrices a) $R \cup S$ b) $R \cap S$ c) $R \cdot S$ d) $S \cdot R$.

Partition:

A Partition P of a non-empty set A is a collection of non-empty subsets of A such that,

i) Each element of A belongs to exactly one of the subsets in P.

ii) If $A_1, A_2, \cdots A_n$ are distinct subsets in P then $A = A_1 \cup A_2 \cup \cdots \cup A_n$.

ex:

List all the partitions of $A = \{1, 2, 3\}$

Soln

$P_1 = \{\{1\}, \{2\}, \{3\}\}$ $\quad P_5 = \{1, 2, 3\}$

$P_2 = \{\{1\}, \{2, 3\}\}$

$P_3 = \{\{2\}, \{1, 3\}\}$

$P_4 = \{\{3\}, \{1, 2\}\}$

Equivalence Relation:

A relation on a set A is called an equivalence relation if its reflexive, symmetric & transitive.

Problems in Relations: (Have to do the this problem in Relation topic)

1) Determine whether the relation R on the set of all integers is reflexive, symmetric, antisymmetric and/or transitive where aRb if and only if

i) $a \neq b$ ii) $ab \geq 0$, iii) $ab \geq 1$

iv) a is a multiple of b. v) $|a - b| \leq 1$)

Soln

i) $a \neq a$ is not true, Hence R is not reflexive.

$a \neq b \Rightarrow b \neq a$ $\therefore$ R is symmetric

$a \neq b$ & $b \neq c \not\Rightarrow a \neq c$

$\therefore$ R is not transitive.

ii) $a^2 \geq 0$ $\therefore$ R is reflexive.

$ab \geq 0 \Rightarrow ba \geq 0$ $\therefore$ R is symmetric

Consider,

$(2,0)$ & $(0,-3) \in R$ But $(2,-3) \notin R$

as $2(-3) < 0$ $\therefore$ R is not transitive.

iii) $a^2 \geq 1$

need not be true. Since a may be zero

$\therefore$ R is not reflexive.

$ab \geq 1 \Rightarrow ba \geq 1$ $\therefore$ R is symmetric

$ab \geq 1$ & $bc \geq 1 \Rightarrow \forall a, b, c > 0$ or < 0

if $a, b, c > 0$

least a = least b = least c = 1

$\therefore ac \geq 1$

if $a, b, c < 0$

greatest a = greatest b = greatest c = -1

$\therefore ac \geq 1$. $\therefore$ R is transitive.

iv) a is a multiple of a

$\therefore$ R is reflexive.

If 'a' is multiple of b, b is not a multiple of 'a' in general.

But if 'a' is a multiple of b & b is a multiple of a then $a = b$.

$\therefore$ R is antisymmetric.

'a' is a multiple of b & b is a mple of c then a is a multiple of c

$\therefore$ R is symmetric.

v) $|a - a| \neq 1$ $\therefore$ R is not reflexive

$|a-b|=1 \Rightarrow |b-a|=1$ ∴ R is symmetric

$|a-b|=1$ $[a-b=1 \text{ (or) } -1]$

$|b-c|=1$ $[b-c=1 \text{ (or) } -1]$

then $|a-c| = 2 \text{ (or) } 0$

i.e., $|a-c| \neq 1$ ∴ R is not transitive

Problems in Equivalence Relation:

1) P.T the relation "consequence modulo m" defined by $R=\{(x,y) / x-y$ is divisible by $m\}$ is a equivalence relation over the set of the integers. Show also that if $x_1 \equiv y_1$ & $x_2 \equiv y_2$ then $(x_1+x_2) \equiv (y_1+y_2)$

Soln

i) R is reflexive:

For any $x \equiv x \pmod{m}$

Since $x-x$ is divisible by m

∴ $(x,x) \in R \Rightarrow R$ is reflexive.

ii) R is symmetric:

Let $(a,b) \in R \Rightarrow a \equiv b \pmod{m}$

i.e., $a-b$ is divisible by m.

$b-a = -(a-b)$, which is also divisible by m.

$\therefore\ b \equiv a \pmod m \Rightarrow (b,a) \in R$

$\therefore$ R is symmetric

iii) R is transitive:

Let $(a,b) \in R$ & $(b,c) \in R$

$\therefore\ a \equiv b \pmod m$ & $b \equiv c \pmod m$

i.e., $a-b$ is divisible by m & $b-c$ is divisible by m.

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

$= k_1 m + k_2 m$

$= (k_1+k_2) m$

$\Rightarrow a-c$ is divisible by m $\Rightarrow a \equiv c \pmod m$

i.e., $(a,c) \in R \Rightarrow R$ is transitive

Hence R is an equivalence relation,

$x_1 \equiv y_1 \Rightarrow x_1 - y_1 = am$

$x_2 \equiv y_2 \Rightarrow x_2 - y_2 = bm$

$\therefore\ x_1 - y_1 + x_2 - y_2 = (a+b)m$

$(x_1+x_2) - (y_1+y_2)$ is divisible by m.

$\therefore\ (x_1+x_2) \equiv (y_1+y_2)$.

2) Let $X = \{1,2,3,\cdots 7\}$ and $R = \{x,y \mid x-y$ is divisible by $3\}$. S.T R is a equivalence relation & draw the graph

Soln

i) For any $a \in X$, $a-a$ is divisible by 3. $\therefore (a,a) \in R \ \forall a \in X$

$\therefore$ R is reflexive.

ii) Let $(a,b) \in R$

$a-b$ is divisible by 3

$\Rightarrow b-a$ is also divisible by 3

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

$\therefore$ R is symmetric

iii) Let $(a,b) \in R$ & $(b,c) \in R$

$a-b$ & $b-c$ are divisible by 3

ie., $a-b = 3k$ & $b-c = 3m$

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

$= 3(k+m)$ is divisible by 3

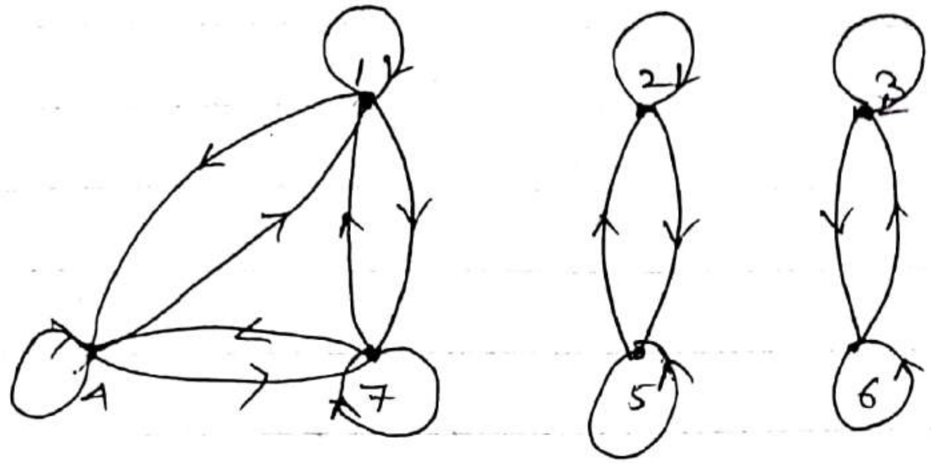
$\Rightarrow (a,c) \in R \Rightarrow$ R is transitive

$\therefore$ R is a equivalence relation.

Now

$R = \{(1,4)\ (4,1)\ (2,5)\ (5,2)\ (3,6)\ (6,3)$
$(4,7)\ (7,4)\ (1,7)\ (7,1)\ (1,1)$
$(2,2)\ (3,3)\ (4,4)\ (5,5)\ (6,6)$
$(7,7)\}$

Graphs of the relation:



Equivalence Classes:

Let R be an equivalence relation on a set A. Let $a \in A$, then the set of all those elements of A which are related to a is called an equivalence class determined by 'a' and it is denoted by $[a]$.

i.e., $[a] = \{ b \in A \mid (a,b) \in R \}$

Theorem:

Let 'R' be an equivalence relation on a set A and $[a]$, the equivalence class determined by the element a. Then

i) $a \in [a]$

ii) $a \in [b] \Leftrightarrow [a] = [b]$

iii) The equivalence classes

determined by two elements are either disjoint (or) identical.

i.e., $[a] \cap [b] = \phi$ (or) $[a] = [b]$

Proof

i) The relation R is reflexive, we have aRa, $\forall a \in A$,

$\therefore a \in [a]$, $\forall a \in A$

ii) Let $a \in [b]$, so aRb — (1)

Now inorder to S.T $[a] = [b]$, we observe that for an arbitrary element $x \in [a]$, we have

$x \in [a] \Leftrightarrow xRa$

$\Leftrightarrow xRa$ & aRb (2) (gn)

(from (1) & (2)) $\Leftrightarrow xRb$ (transitivity)

$\Leftrightarrow x \in [b]$

Converse, $\therefore [a] = [b]$

Thus $a \in [b] \Rightarrow [a] = [b]$

Again, let $[a] = [b]$

Then from (i), $a \in [a]$, and so $a \in [b]$,

Thus $[a] = [b] \Rightarrow a \in [b]$

Hence $a \in [b] \Leftrightarrow [a] = [b]$

iii) For any two classes $[a]$ and $[b]$
If $[a] \cap [b] = \phi$, then the result follows.

So, let us consider, $[a] \cap [b] \neq \phi$

Let $c \in [a] \cap [b]$

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

$\Rightarrow cRa$ & cRb

$\Rightarrow aRc$ & cRb (Symmetry)

$\Rightarrow aRb$ (transitivity)

$\Rightarrow a \in [b]$

$\Rightarrow [a] = [b]$.

Equivalently,

If $[a] \neq [b]$ then $[a] \cap [b] = \phi$.

ie., Two distinct equivalent classes are disjoint.

Quotient Set:

If R is an equivalence relation defined on X, then the set of all equivalence classes generated by elements of X is called the Quotient set of X/R

ie, $X/R = \{[x] \mid x \in X\}$

Partial Order relation:

A relation R on a set A is said to be a partial order relation if R is reflexive, antisymmetric and transitive.

Problems

1) Let $S = \{1,2,3,4,5\}$ and $A = S \times S$. The relation R on A is defined by $(a,b) R (a',b')$ iff $ab' = a'b$. S.T R is an equivalence relation and compute A/R.

Soln

i) $(a,b) R (a,b)$ since $ab = ba$

$\therefore$ R is reflexive.

ii) Let $(a,b) R (a',b')$

Then $ab' = a'b$

$\Rightarrow a'b = ab'$

$\therefore (a',b') R (a,b)$

$\therefore$ R is symmetric

iii) Let $(a,b) R (a',b')$ &

Scanned by CamScanner

$(a', b') \, R \, (a'', b'')$

$\therefore \; ab' = a'b \;\; \& \;\; a'b'' = a''b' \;\; \left\{ b'' = \frac{a''b'}{a'} \right\}$

Now, $ab'' = a. \frac{a''b'}{a'}$

$= a. \frac{a''}{a'} . \frac{a'b}{a} \quad \left(\because b' = \frac{a'b}{a} \right)$

$\therefore \; ab'' = a''b$

$\therefore \; (a, b) \, R \, (a'', b'')$

$\therefore$ R is transitive.

$\therefore$ R is an equivalence relation

To find A/R.

$S = \{1, 2, 3, 4, 5\}$

$A = S \times S$

$\therefore A/R = [\{(1,1), (2,2) (3,3) (4,4) (5,5)\},$
$\{(1,2) (2,4)\}, \{(1,3)\} \{(1,4)\} \{(1,5)\}$
$\{(2,1)\} \{(4,2)\}, \{(2,3)\} \{(2,5)\}$
$\{(3,1)\} \{(3,2)\} \{(3,4)\} \{(3,5)\},$
$\{(4,1)\} \{(4,5)\} \{(5,1)\}.]$

2) Let $A = \{1, 2, 3, 4\}$ and R be a relation A defined by the matrix.

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

Compute A/R.

Soln The relation.

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

The Equivalence class is

$[a] = \{b \in A : (a,b) \in R\}$

$[1] = \{(1,1)\} = \{1\}$
$[2] = \{(2,2)(2,3)(2,4)\} = \{2,3,4\}$
$[3] = \{(3,2)(3,3)(3,4)\} =$ "
$[4] = \{(4,2)(4,3)(4,4)\} =$ "

$\therefore A/R = \{\{1,1\}\{2,2\}\{2,3\}\{2,4\},$
$\{3,2\}\{3,3\}\{3,4\}\{4,2\},$
$\{4,3\}\{4,4\}\}.$

$= \{\{1\},\{2,3,4\}\}$

3) Prove that the intersection of two equivalence relation.

Soln Consider R_1 & R_2 are the equivalence relation.

i) Let $a \in A$.

Since R_1 is an equivalence relation on A, $(a,a) \in R_1 \;\forall\; a \in A$.

iii^ly $(a,a) \in R_2$ since R_2 is an equivalence relation.

$\therefore (a,a) \in R_1 \cap R_2 \quad \forall a \in A$.

$\Rightarrow R_1 \cap R_2$ is reflexive.

ii) Let $(a,b) \in R_1 \cap R_2$

$(a,b) \in R_1$ & $(a,b) \in R_2$

Since R_1 & R_2 are symmetric

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

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

$\therefore (b,a) \in R_1 \cap R_2$.

$\therefore R_1 \cap R_2$ is symmetric.

iii) Let $(a,b) \in R_1 \cap R_2$ & $(b,c) \in R_1 \cap R_2$

$\Rightarrow (a,b) \in R_1$ & $(b,c) \in R_1 \Rightarrow (a,c) \in R_1$ (transitive)

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

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

$\therefore R_1 \cap R_2$ is transitive.

$\therefore R_1 \cap R_2$ is an equivalence Relation.

H.W

4) Let $A = R \times R$, where R = set of real nos., . The relation S on A is defined by $(a,b) S (c,d)$ iff $a^2+b^2 =$

c^2+d^2. S.T S is an equivalence relation.

Soln

i) $(a,b) S (a,b)$ since $a^2+b^2 = a^2+b^2$

$\therefore$ S is reflexive.

ii) Let if $(a,b) S (c,d)$, then

$a^2+b^2 = c^2+d^2$.

$\therefore \quad c^2+d^2 = a^2+b^2$

$\Rightarrow \quad (c,d) S (a,b)$

$\therefore$ S is symmetric.

iii) Let $(a,b) S (c,d)$ & $(c,d) S (x,y)$

$\therefore a^2+b^2 = c^2+d^2$ & $c^2+d^2 = x^2+y^2$

$\therefore \quad a^2+b^2 = x^2+y^2 \Rightarrow (a,b) S (x,y)$

$\therefore$ S is transitive.

$\therefore$ S is an equivalence Relation

5) Let N be set of all natural nos., Prove that the relation R in N defined by $aRb \Leftrightarrow a$ divides b is a partial order relation.

Soln

i) Reflexive:

aRa, $\forall a \in N$, since every

natural number divides itself..

ii) Antisymmetric.

Let aRb & bRa

a divides b & b divides a.

This is possible only when $a=b$.

iii) Transitive.

Let aRb & bRc. Then a divides b & b divides c.

$\exists$ natural nos m & n $\ni$: $b = ma$ & $c = nb$

$\therefore$ $c = nb \Rightarrow c = n(ma) = (nm)a$

$\therefore$ a divides c and so aRc.

$\Rightarrow$ R is transitive.

$\therefore$ R is a POR.

HW

6) Let R be the set of all real nos, P.T the relation S defined by "$a \leq b$" is Partial Order relation.

Unit - III

GROUPS

Introduction:

Let A be any set. A mapping $f: A \times A \times \cdots \times A \to A$ (or) $f: A^n \to A$ is called an n-ary operation and 'n' is called the order of the operation.

For $n=1$, $f: A \to A$ is called an Unary operation

for $n=2$, $f: A \times A \to A$ is called Binary operation

Algebraic System:

A set together with a number of operations. (one or move n-ary operations) on the set is called an algebraic system (or) an Algebra.

Example:

Semigroups $(S, *)$, Monoids $(M, *)$, Groups $(G, *)$ are algebraic system with one binary operation. Rings $(R, +, \oplus)$, Integral domains $(I, +, \cdot)$, fields are algebraic system with two binary operations etc.

General Properties of Algebraic Systems:

Let $\{S, *, \oplus\}$ be an algebraic system, where $*$ and $\oplus$ are binary operations on S.

1) Closure Property

For any $a, b \in S$, $a * b \in S$

for example: If $a, b \in Z$, $a+b \in Z$ and $a * b \in Z$ where $+$ and $\times$ are the operations of addition and multiplication.

2) Associative Property:

For any $a, b, c \in S$, $(a * b) * c = a * (b * c)$

for example: If $a, b, c \in Z$

$(a+b)+c = a+(b+c)$ &

$(a * b) * c = a * (b * c)$

3) Commutative Property:

for any $a, b \in S$, $a * b = b * a$

for example: If $a, b \in Z$,

$a+b = b+a$ &

$a \times b = b \times a$

4) Identity element :

There exists a distinguished element $e \in S$, such that for any $a \in S$, $a * e = e * a = a$. The element $e \in S$ is called the identity element of S with respect to the operation $*$.

for example : 0 and 1 are the identity element of Z with respect to the operations of addition and multiplication resp., since for any $a \in Z$,

$$a + 0 = 0 + a = a$$
$$a \times 1 = 1 \times a = a.$$

5) Inverse Element.

For each $a \in S$, there exists an element $a^{-1} \in S$ such that $a * a^{-1} = a^{-1} * a = e$. The element $a^{-1} \in S$ is called the inverse of a under $*$.

for example : for each $a \in Z$, $-a$ is the inverse of a under the operation of addition. Since $a + (-a) = -a + a = 0$, where '0' is the identity element of Z under addition.

6) Distributive Property :

for any $a, b, c, \in S$

$a * (b \oplus c) = (a * b) \oplus (a * c)$

In this case, the operation $*$ is said to be distributive over the operation $\oplus$.

for example : The usual multiplication is distributive over addition.

since $a \times (b + c) = (a \times b) + (a \times c)$

7) Cancellation Property :

for any $a, b, c, \in S$ and $a \neq 0$

$a * b = a * c \Rightarrow b = c$ (left cancellation Law)

$b * c = c * a \Rightarrow b = c$ (Right cancellation Law)

ex : Cancellation property holds good for any $a, b, c, \in Z$ under addition and multiplication.

8) Idempotent Element :

An element $a \in S$ is called an idempotent element with respect to the operation. * if $a * a = a$.

ex: $0 \in Z$ is an idempotent element under addition since $0+0=0$ and $0,1 \in Z$ are idempotent element under multiplication or since $0 \times 0 = 0$ $1 \times 1 = 1$.

9) Homomorphism:

If $\{X, \cdot\}$ and $\{Y, *\}$ are two algebraic systems where '$\cdot$' and '$*$' are binary operations then a mapping $g: X \rightarrow Y$ is called a homomorphism or simply morphism from $\{X, \cdot\}$ to $\{Y, *\}$ if for any $x_1, x_2 \in X$.

$g(x_1 \cdot x_2) = g(x_1) * g(x_2)$.

Semi Groups:

Let S be a non-empty set with the binary operation '$*$'. The algebraic system $(S, *)$ is called a semigroup if the operation '$*$' satisfies the following property.

i) Closure Property: For any $a, b \in S$

$a * b \in S$

(ii) Associative Property :

For any $a, b, c \in S$,

$(a * b) * c = a * (b * c)$

Ex:

Let $(N, +)$ be an algebraic system with binary operation as $+$, where $N = \{1, 2, 3 \dots\}$ be the set of all natural nos., and $+$ is usual addition. It is clear that $(N, +)$ satisfies closure property and Associative Property.

$\therefore$ The Algebraic system $(N, +)$ is a semi-group.

Monoid.

Let M be a non-empty set with the binary operation "$*$". The algebraic system $(M, *)$ is called a Monoid if the operation $*$ satisfies the following property.

i) Closure Property : For any $a, b \in M$, $a * b \in M$

ii) Associative Property : For any $a, b, c \in M$

$(a * b) * c = a * (b * c)$

iii) Identity Element : There exists an element $e \in M \ni: e * a = a * e = a$ $\forall a \in M$.

example :

Let $(z,+)$ be an algebraic system with binary operation '+', where z is the set of all Integers

i) $x, y \in z$, $x+y \in z$

ii) $x, y, z \in z$, $(x+y)+z = x+(y+z)$

iii) $\exists$ an elt, $0 \in z$, $\ni: 0+x = x+0 = x$

Identity elt, is "0".

Groups :

A group $(G, *)$ is an algebraic system in which the binary operation "$*$" on G satisfies the following properties

i) Closure Property :

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

ii) Associative Property :

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

iii) Identity Element :

$\exists$ for every $e \in G$, $\ni$: for any $a \in G$,

$a * e = e * a = a$

iv) Inverse elt :

$\forall\ a \in G$, $\exists$ an inverse elt, of 'a' denoted by $a^{-1} \in G$ $\ni: a * a^{-1} = a^{-1} * a = e$

Ex:

Let 'z' be the set of all Integers, then the algebraic system $(z, +)$ is a group, where '+' is the usual addition multiplication

Abelian Group:

A group $(G, *)$ in which the binary operation $*$ is commutative is called an abelian group.

ie., Let $(G, *)$ be any Group, for any $a, b \in G$ if $a * b = b * a$ then $(G, *)$ is an abelian group.

ex: The group $(z, +)$ is an abelian group.

Order of a Group:

The no., of elements in a group is denoted by $O(G)$ is called the Order of the group G.

Order of an Element

Let G be a group and $a \in G$. If for some positive integer 'n', $a^n = e$ then 'n' is called the order of the element 'a' and is denoted by $O(a)$.

ex:

i) Let $G = \{1, 0, -1\}$ is not a group with respect to the operation addition

Since $1+1 = 2 \notin G$

(1st property is not satisfied)

+	1	0	-1
1	2	1	0
0	1	0	-1
-1	0	-1	-2

ii) Let $G = \{1, -1, i, -i\}$ with operation defined by multiplication

*	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

In the table we can observe that the closure property & associative property are verified.

The Identity elt is 1

$\because \; 1 \times 1 = 1, \; -1 \times 1 = -1, \; i \times 1 = i, \; -i \times 1 = -$

The inverse element of 1 is 1 ($\because 1\times 1=1$)

The inverse element of -1 is -1

The inverse elt., of i is $-i$ ($i\times -i=1$)

The inverse element of $-i$ is i

$\therefore$ G is a group.

$o(1) = 1 \quad \because (1)^1 = 1$

$o(-1) = 2 \quad (-1)^2 = 1$

$o(i) = 4 \quad (+i)^4 = 1$

$o(-i) = 4 \quad (-i)^4 = 1$

where 1 is the identity element of G

$o(G) = 4$. G is ~~the~~ an abelian group since it satisfies commutative property also.

Properties of a Group:

Property 1 (Uniqueness of Identity)

The identity element in a group is unique.

Proof:

Let e_1 and e_2 be two identity elements of G

If e_1 is the identity elt., & $e_2 \in G$, then
$e_1 * e_2 \overset{= e_2 * e_1 =}{=} e_2$ (Taking e_1 as identity) — (1)

If e_2 is the identity elt., & $e_1 \in G$, then
$e_1 * e_2 \overset{= e_2 * e_1 =}{=} e_1$ (Taking e_2 as identity) — (2)

(from (1) & (2))
$\therefore e_1 = e_2$ $\therefore$ The identity elt., is unique

Property 2

The inverse of every element is unique.

proof:

Let $(G, *)$ be a group, with identity element e. Let b and c be inverses of an element $a \in G$.

$$a * b = b * a = e \quad \text{— (1)}$$

$$a * c = c * a = e \quad \text{— (2)}$$

Let $b = b * e$

$= b * (a * c)$ (by (2))

$= (b * a) * c$

$= e * c$ (by (1))

$$\boxed{b = c}$$

$\therefore$ Inverse of every elt., in a group is unique.

Property 8 :

In any group $(G, *)$, $(a * b)^{-1} = b^{-1} * a^{-1}$ for any $a, b \in G$.

(or)

ie, The inverse of the product of two elements is equal to the product of their inverses in reverse order.

proof : Gn, $(G, *)$ be a group. We have to show that $(a*b)*(b^{-1}*a^{-1}) = (b^{-1}*a^{-1})*(a*b) = e$

To prove : $(a*b)^{-1} = b^{-1} * a^{-1}$

Let $a, b \in G$ & a^{-1}, b^{-1} be their inverses respectively.

$$\therefore \quad a * a^{-1} = e = a^{-1} * a$$

$$\& \quad b * b^{-1} = e = b^{-1} * b$$

Now $(a * b) * (b^{-1} * a^{-1}) = a * [b * (b^{-1} * a^{-1})]$

$= a * [(b * b^{-1}) * a^{-1}]$

$= a * (e * a^{-1}) \quad (b * b^{-1} = e)$

$= a * a^{-1}$

ie, $(a*b) * (b^{-1}*a^{-1}) = e$ ——— (1)

||ly we can P.T

$(b^{-1} * a^{-1}) * (a * b) = e$ —— (2)

from (1) & (2), we get

$(a * b)^{-1} = b^{-1} * a^{-1}$

ie, The inverse of $(a * b)$ is $b^{-1} * a^{-1}$

Property 4:

In a group the cancellation property are true for all $a, b, c \in G$

i) $a * b = a * c \Rightarrow b = c$

ii) $b * a = c * a \Rightarrow b = c$.

Proof:

Gn, $(G, *)$ is a group, Let e be the identity element of G.

i) Given $(a * b) = a * c$

Let a^{-1} be the inverse of 'a'

Pre multiplying by a^{-1}, we get

$a^{-1} * (a * b) = a^{-1} * (a * c)$

$(a^{-1} * a) * b = (a^{-1} * a) * c$ (By Ass. Prop)

$e * b = e * c$ (" Inverse)

$b = c$ (By Identity)

ii) Gn., $b * a = c * a$

post xplying by a^{-1}.

$\Rightarrow (b * a) * a^{-1} = (c * a) * a^{-1}$

$\Rightarrow b * (a * a^{-1}) = c * (a * a^{-1})$

$\Rightarrow b * e = c * e$

$\Rightarrow \boxed{b = c}$

Hence cancellation property are true in a group.

Subgroup:

Let G be a group with binary operation $*$. Let H be a non-empty subset of G. If H is also a group under the same operation $*$. Then H is called. a subgroup of G.

Ex:

1) Every group $(G, *)$ is a subgroup of itself.

2) Let G be a group $G = \{1, -1, i, -i\}$ with the operation xplication

The set $\{1, -1\}$ and $\{1\}$ are subgroups of G.

·	1	-1
1	1	-1

is a grou[illegible]

·	i	-i
i	-1	1
-i	1	[illegible]

is not a [illegible]

Theorem: 1

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)

$\therefore a, b \in H \Rightarrow a, b^{-1} \in H$

$\Rightarrow a * b^{-1} \in H$.

ie, $a, b \in H \Rightarrow a * b^{-1} \in H$

Sufficient Condition:

Let $a * b^{-1} \in H$ — (1) $\forall a, b \in H$

and $H \subseteq G$.

To prove: H is a subgroup of G.

For,

i) Identity: Let $a, a \in H$, $a \in H$

$\Rightarrow a * a^{-1} \in H$ (by (1))

$\Rightarrow e \in H$

Hence the identity 'e' is the elt, of H

ii) Inverse:

Let $e \in H$, $a \in H \Rightarrow e * a^{-1} \in H$

$\Rightarrow a^{-1} \in H$

i.e., Every elt. of H has an inverse which is in H.

iii) Closure:

Let $b \in H \Rightarrow b^{-1} \in H$

$\therefore$ for $a, b \in H \Rightarrow a, b^{-1} \in H$

$\Rightarrow a * (b^{-1})^{-1} \in H$

$= a * b \in H$

iv) Associative: Let $a, b, c \in H \subset G$

$\Rightarrow (a*b)*c = a*(b*c)$

Since all the four properties are true.

$\therefore$ H is a subgroup of G.

Theorem: 2

The intersection of two subgroups of a group is also a subgroup of the group. (or)

If H_1, H_2 are two subgroups of G. then $H_1 \cap H_2$ is also a subgroup of G.

Proof:

Let H_1 & H_2 be any two subgroups of G.

then $H_1 \cap H_2 \neq \phi$ because atleast the identity element is common to both H_1 & H_2.

To prove:

$H_1 \cap H_2$ is a subgroup, it's enough to show that for $a, b \in H_1 \cap H_2$

$\Rightarrow a * b^{-1} \in H_1 \cap H_2$.

Let $a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1$ &

$a, b \in H_2$

$\Rightarrow a * b^{-1} \in H_1$ & $a * b^{-1} \in H_2$

$\Rightarrow a * b^{-1} \in H_1 \cap H_2$

i.e., $a, b \in H_1 \cap H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$

$\therefore$ $H_1 \cap H_2$ is a subgroup of G.

Example:

Determine whether $H_1 = \{0, 5, 10\}$ and $H_2 = \{0, 4, 8, 12\}$ are subgroups of Z_{15} under addition

Soln

For H_1

$+_{15}$	0	5	10
0	0	5	10
5	5	10	0
10	10	0	5

For H_2

$+_{15}$	0	4	8	12
0	0	4	8	12
4	4	8	12	1
8	8	12	1	5
12	12	1	5	9

Since all the entries in the addition table for H_1 are the elts., of H_1.

$\therefore$ H_1 a subgroup of Z_{15}

IIIly all the entries in the addition table for H_2 are not the elements of H_2.

ie., H_2 is not closed under addition

$\therefore$ H_2 is not a subgroup of Z_{15}.

Cyclic Group:

A group $(G, *)$ is said to be cyclic group if there exist an element $a \in G$ $\ni$: every elt. of the group is of the form ~~a^n~~ ~~some integers~~ $\therefore$ $x = a^n$ (or) $x = na$ where 'n' is some integer. Here the element 'a' is called the generator of G and is written as $G = (a)$ is read as G is cyclic group generated by 'a'.

ex:

Let $G = \{1, -1, i, -i\}$, then $(G, *)$ is a cyclic group generated by i, since $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, $i^1 = i$

i.e., All the elements of G can be expressed as integral powers of the element i.

$\therefore$ G is a cyclic group generated by i.

Since i is the generator of G, $(i)^{-1}$ is also generator of G.

Hence G is a cyclic group & its

generators are i & $-i$,

[(1 & -1) are not generator]

Theorem: 3.

Every subgroup of a cyclic group is cyclic.

proof:

Let $G = (a)$ is a cyclic group generated by 'a' and H is its subgroup.

The elements of H are integral powers of a.

If $a^s \in H$, then the inverse $a^{-s} \in H$

$\therefore$ H contains elements which are positive as well as negative integral powers of a.

let 'm' be the least +ve integer $\ni$: $a^m \in H$, we have to prove that $H = (a^m)$, i.e., H is cyclic & its generator is a^m.

For, let a^t be any arbitrary elt, of H.

By division algorithm, $\exists$ integers q & r

$\Rightarrow$: $t = mq + r$, $0 \leq r < m$

Now, $a^t = a^{mq+r}$,

$= a^{mq} . a^r$

$\Rightarrow a^r = a^t * a^{-mq} = a^{t-mq}$ — (1)

Now, $a^m \in H \Rightarrow (a^m)^q \in H$

$= a^{mq} \in H \Rightarrow a^{-mq} \in H$

Also, $a^t, a^{-mq} \in H$

$\Rightarrow a^t * a^{-mq} \in H \Rightarrow a^{t-mq} \in H$

$\Rightarrow a^r \in H$

(by (1))

Since m is the least +ve integers

$\Rightarrow$: $a^m \in H$ and $0 \leq r < m$, $\therefore r = 0$

Hence $t = mq$

$a^t = a^{mq} = (a^m)^q \quad \forall a^t \in H$

Thus every elt., $a^t \in H$ is of the form $(a^m)^q$.

$\therefore$ H is cyclic & is generated by a^m. i.e., $H = (a^m)$

Theorem 4:

Every cyclic group is abelian

Proof:

Let $(G, *)$ be a cyclic group generated by 'a'.

Then $G = \{a^n / n \in z\}$

Let $x, y, \in G$ be any two elts,

then $x = a^m$, $y = a^n$ for some Integers m & n.

$$x * y = a^m * a^n$$
$$= a^{m+n} = a^{n+m} = a^n * a^m$$
$$= y * x$$

$\therefore x * y = y * x, \forall x, y \in G$.

$\therefore$ Every cyclic group is abelian.

Group Homomorphism:

Let $(G, *)$ & (G', Δ) be two groups. A mapping $f : G \to G'$ is said to be a group homomorphism if for any $a, b \in G$.

$f(a * b) = f(a) \Delta f(b)$

A homomorphism f is said to be group homomorphism if 'f' is 1-1 & onto.

examples:

1. Let G be the set of all integers with the operation '+'. Then $f: G \to G$ defined by $f(x) = 2x$ is a homomorphism

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

i.e., f is a homomorphism

2. Let G be the set of all integers with addition as the operation. Define; $f: G \to G'$ $\ni$ $f(x) = (x+2)$

To prove: $f(x+y) = f(x) + f(y)$

L.H.S: $f(x+y) = (x+y)+2$

R.H.S $f(x) + f(y) = x+2+y+2$
$$= x+y+4$$

$\therefore f(x+y) \neq f(x) + f(y)$

i.e., f is not homomorphism.

Scanned by CamScanner

Theorem: 5

If 'f' is a homomorphism of a group G into G', then

i) Group homomorphism preserves identities

i.e., $f(e) = e'$, e & e' are identity elt of G & G' resp.,

ii) Group homomorphism preserves inverses

i.e., $f(a^{-1}) = [f(a)]^{-1}$ $\forall$ $a \in G$.

Proof:

i) Let $a \in G$ & f is a homomorphism from G into G'.

then $f(a) \in G'$

$\therefore f(a) * e' = f(a) = f(a * e)$

$f(a) * e' = f(a) * f(e)$

$\Rightarrow \boxed{e' = f(e)}$ (by L. cancellation law)

ii) Let $a \in G$, then $a^{-1} \in G$ and

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

$\therefore e' = f(e)$

$= f(a * a^{-1})$

$= f(a) * f(a^{-1})$

i.e., $f(a) * f(a^{-1}) = e'$

i.e., $f(a^{-1})$ is the inverse of $f(a)$ in G

i.e., $[f(a)]^{-1} = f(a^{-1})$.

Theorem : 6

If $f : G \to G'$ is a group homomorphism, H is a subgroup of G, then $f(H)$ is a subgroup of G'.

proof:

Let $f(H) = \{f(x) \mid x \in G\}$

Then $f(H)$ is a non-empty subset of G'.

Let $a', b' \in f(H)$

we have $f(a) = a'$, $f(b) = b'$

for $a, b \in H$.

$$\therefore a' * (b')^{-1} = f(a) * [f(b)]^{-1}$$

$$= f(a) * f(b^{-1})$$

$$= f(a * b^{-1})$$

But $a * b^{-1} \in H \Rightarrow f(a * b^{-1}) \in f(H)$

$$\Rightarrow a' * (b')^{-1} \in f(H)$$

i.e., for $a', b' \in f(H) \Rightarrow a' * (b')^{-1} \in f(H)$

$\therefore f(H)$ is a subgroup of G'.

Kernel of a Homomorphism:

Let $f: G \to G'$ be a group homomorphim, then the set of element of G, which are mapped onto e', the identity element of G', is called the kernal of f & is denoted by $\ker(f)$

ie, $\ker(f) = \{x \in G : f(x) = e', e'$ is the identity of $G'\}$

Theorem: 7

The kernel of a homomorphism f from a group G to G' is a subgroup of G.

proof:

If $\ker(f) = \{x \in G \mid f(x) = e'\}$

Since $f(e) = e'$ is true always,

atleast $e \in \ker(f)$

ie., $\ker(f)$ is a non empty subset of G.

Let $a, b \in \ker f$

with $f(a) = e'$ & $f(b) = e'$

$\therefore f(a * b^{-1}) = f(a) * f(b^{-1})$

$= f(a) * [f(b)]^{-1}$

$= e' * e' = e'$

$\Rightarrow a * b^{-1} \in \ker f$

i.e., $a, b \in \ker f \Rightarrow a * b^{-1} \in \ker f$

$\therefore \ker f$ is a subgroup of G.

Cosets:

Let $(H, *)$ be a subgroup of $(G, *)$ and $a \in G$. Then $aH = \{a * h \mid h \in H\}$ is called left coset of H in G.

IIIly $Ha = \{h * a \mid h \in H\}$ is called right coset of H in G.

Ex:

Let $G = \{1, -1, i, -i\}$ and '$\cdot$' be usual multiplication, $H = \{1, -1\}$ is a subgroup of G. Find all the cosets of H.

Soln

$H(1) = \{1 \cdot 1, -1 \cdot 1\} = \{1, -1\} = H$

$H(-1) = \{-1 \cdot 1, -1 \cdot -1\} = \{-1, 1\} = H$

$Hi = \{i, -i\}$

$H(-i) = \{-i, i\} = Hi = H(i)$

Note:

1. H and Hi are the 2 distinct right cosets of H in G.
2. $H \cup Hi = G$ i.e., G is partitioned into 2 distinct right cosets of H in G.
3. Any two right (or left) cosets of H in G are either disjoint (or) Identical.

Thm: 8 (Lagrange's theorem).

The order of each subgroup of the a finite group is a divisor of the order of the group. i.e., $O(H) / O(G)$

Proof;

Let $(G, *)$ be a finite group & $o(G) = n$. Let $(H, *)$ be a subgroup of $(G, *)$ & $o(H) = m$.

Suppose that, $h_1, h_2 \dots h_m$ are

m members of H. For $a \in G$, the right coset Ha of H in G is defined by

$$Ha = \{h_1 * a, h_2 * a, h_3 * a \ldots h_m * a\}$$

Since there should be a 1-1 correspondence betⁿ H and Ha, the members of Ha are distinct.

Hence each right coset of H in G has m distinct members.

W.K.T any right coset of H in G are either disjoint (or) Identical. Since G is a finite, the no. of distinct right cosets of H in G will be finite say 'k'.

The union of these k distinct right cosets of H in G is equal to G.

Hence, if $Ha_1, Ha_2 \ldots Ha_k$ are 'k' distinct right cosets of H in G, then,

$$G = Ha_1 \cup Ha_2 \cup Ha_3 \cup \cdots \cup Ha_k$$

$$O(G) = O(Ha_1) \cup O(Ha_2) \cup O(Ha_3) \cup \cdots \cup O(Ha_k)$$

$$n = m + m + \cdots + m \quad (k \text{ times})$$

$$n = km \Rightarrow k = n/m$$ i.e., m is a divisor of n.

∴ o(H) is a divisor of o(G). Hence proved.

Thm 10: (Fundamental Theorem on Group Homomorphism).

Every homomorphic Image of a Group G is Isomorphic to some quotient group of G.

proof:

Let G' be the homomorphic image of a group G and $f: G \to G'$ be a homomorphism

We have already proved that

$K = \ker f = \{a \in G \mid f(a) = e'\}$ is a subgroup of $(G, *)$, where e' is the identity element of G'. Then K is a normal subgroup of G.

To prove: $G/K \cong G'$

if $a \in G$, then $Ka \in G/K$ & $f(a) \in G'$

Define $\phi: G/K \to G' \ni: \phi(Ka) = f(a)$ $\forall\, a \in G$.

i) Claim: ϕ is well defined.

Since If $Ka = Kb \Rightarrow a * b^{-1} \in K$

$\Rightarrow f(a * b^{-1}) = e'$

$\Rightarrow f(a) * f(b^{-1}) = e'$

$\Rightarrow f(a) * [f(b)]^{-1} = e'$

Scanned by CamScanner

$\Rightarrow f(a) * [f(b)]^{-1} * f(b) = e' * f(b)$

$\Rightarrow f(a) * e' = e' * f(b)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow \phi(Ka) = \phi(Kb)$

$\therefore \phi$ is well defined.

ii) To prove ϕ is a homomorphism

ii) Claim: ϕ is one-one.

If $\phi(Ka) = \phi(Kb)$ then $f(a) = f(b)$

$f(a) * f(b^{-1}) = f(b) * f(b^{-1})$

$= f(b * b^{-1})$

$f(a) * f(b^{-1}) = f(e)$

$f(a * b^{-1}) = e'$

$\Rightarrow a * b^{-1} \in K \Rightarrow Ka = Kb.$

$\therefore \phi$ is 1-1

iii) Claim: ϕ is onto.

Let y be any element of G'.

Then $y = f(a)$ for some $a \in G$.

$\therefore$ for every $a \in G$, $Ka \in G/K$

we get $\phi(Ka) = f(a)$ $\forall$ $f(a) = y \in G'$

$\therefore \phi$ is onto.

Finally Claim: ϕ is homomorphism.

Let $Ka, Kb \in G/K \Rightarrow \phi(Ka) = f(a)$

$\phi(Kb) = f(b)$

Now $\phi(Ka * Kb) = \phi(K(a * b))$

$= f(a * b) = f(a) * f(b)$

$= \phi(Ka) * \phi(Kb)$

$\therefore \phi$ is a homomorphism.

$\therefore \phi$ is an isomorphism betn G/K & G'

$\therefore G/K \cong G'$.

Rings:

An algebraic system $(R, +, \cdot)$ is called a ring if the binary operations $+$ & $\cdot$ satisfies the following properties.

i) $a+b \in R,\ \forall a, b \in R$

ii) $(a+b)+c = a+(b+c)\ \forall a, b, c \in R$

iii) there is an element $0 \in R, \ni: a+0 = 0+a = a\ \forall a \in R$

iv) $\forall a \in R, \exists -a \in R \ni: a+(-a) = -a+a = 0$

v) $a+b = b+a$

vi) $a \cdot b \in R\ \forall a, b \in R$

vii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(viii) The operation '$\cdot$' is distributive over +,

i.e., $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$

Field:

A commutative division ring is called a field.

Graphs

Definition:

A Graph $G = (V, E, \phi)$ consists of non-empty set $V = \{v_1, v_2 \cdots\}$ called the set of vertices of the graph G. $E = \{e_1, e_2, \cdots\}$ is the set of edges of the graph G, and ϕ is a mapping from the set of edges E to set of ordered or unordered pairs of elements of V.

web page can be represented by a directed

Note: vertices are the web pages available at the graph

The vertices are represented by points and each edge is represented diagramatically. by a line segment

website a directed edge from page A to page B exist ⟺ A contains a link to B.

Directed Graph:

If in a Graph $G = (V, E)$ each edge ~~e∈E~~ is associated with an ordered pair of vertices, then G is called a directed graph (or) digraph.

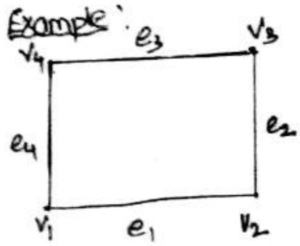
Applications: i) In C.S, G.T provides algorithm, for doing all sorts of useful things with graph- - Algorithm, Networks flow.

ii) For security purpose (or) to schematize network topologies

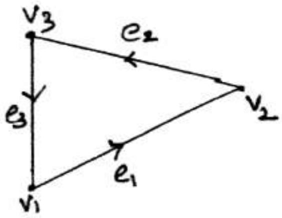
Undirected Graph:

If each edge is a associated with an unordered pair of vertices then G is called as undirected Graph.

Example:



Undirected graph

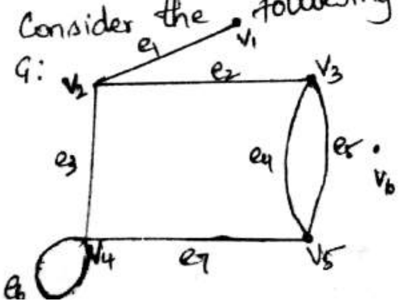


Direct graph.

Note:

In a diagram of digraph, each edge $e=(u,v)$ is represented by means of an arrow or direct curve drawn from the initial point is to the terminal point v.

Consider the following graph



where $V = \{v_1, v_2, v_3, v_4, v_5, v_6\}$

$E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$

$e_1 = \langle v_1, v_2 \rangle$ or $\langle v_2, v_1 \rangle$

$e_2 = \langle v_2, v_3 \rangle$ or $\langle v_3, v_2 \rangle$

$e_3 = \langle v_2, v_4 \rangle$

$e_4 = \langle v_3, v_5 \rangle$

$e_5 = \langle v_3, v_5 \rangle$, $e_6 = \langle v_4, v_4 \rangle$

$e_7 = \langle v_4, v_5 \rangle$

Adjacent:

The vertices v_i and v_j in the undirected graph are said to be adjacent if there is atleast one Edge between v_i and v_j. In this case, the vertices v_i and v_j are called End points of the edge 'e'. The edge 'e' is called also said to be incident with v_i & v_j.

In the graph G, v_1 and v_2, v_2 & v_3, v_3 & v_5, v_2 & v_4 are adjacent, but v_1 and v_3, v_2 and v_5 are not adjacent.

Loop:

If there is an edge from v_i to v_i then that edge is called self loop, or simply "Loop".

In the graph $G = e_6 = \langle v_4, v_4 \rangle$ is called self loop.

parallel Edges:

If two edges have the same end points then the edges are called as parallel edges.

In the graph G, $e_4 = \langle V_3, V_5 \rangle$ and $e_5 = \langle V_3, V_5 \rangle$ are called parallel Edges.

Degree of a vertex

The degree of a vertex in an undirected graph is the number of edges incident with point, with the exception that a loop at a vertex contributes twice to the degree of that vertex, the degree of a vertex V is denoted by deg(V) (or) d(V).

In a Graph G, $d(V_1) = 1$, $d(V_2) = 3$, $d(V_3) = 3$, $d(V_4) = 4$, $d(V_5) = 3$, $d(V_6) = 0$.

Isolated Vertex:

A vertex having no edge incident on it is called an isolated vertex. i.e., $d(V) = 0$, then V is called isolated vertex. In the graph G, $d(V_6) = 0$, V_6 is called isolated vertex.

Pendant vertex and Pendant Edge:

Any vertex having degree one is called pendant vertex and the corresponding edge is called Pendant Edge.

In the graph, G, $d(V_1) = 1$, the vertex V_1 is called Pendant vertex the Edge e_1 is called Pendant Edge.

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.

Adjacent Edges and vertices

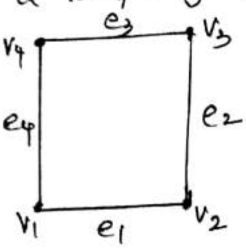
Two edges are said to be adjacent if they are incident on a common vertex. In the Graph G, e_1, e_2 and e_3 are adjacent.

Scanned by CamScanner

The vertices v_i and v_j are said to adjacent if v_i, v_j is an edge of the graph.

Simple Graph:

A graph which has neither self loops nor parallel edges is called a simple graph.

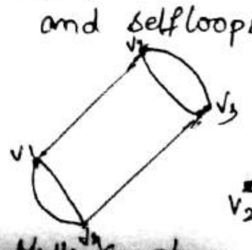


Multi Graph:

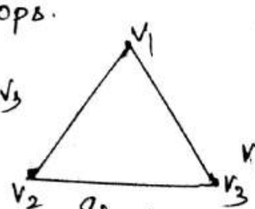
A Graph is said to be multi-graph if it has parallel Edges.

Pseudo Graphs:

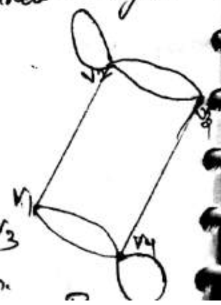
A graph is said to be Pseudo-graph if it has both parallel Edges and selfloops.



Multi Graph



Simple graph.



Trivial Graph:

A Graph with one vertex is said to be a trivial graph. $\cdot v_1$

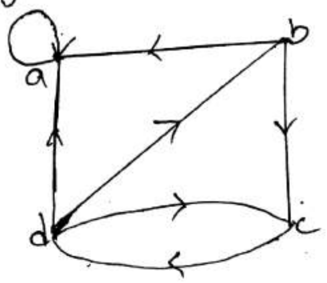
Null Graph

A Graph with isolated vertices is called Null Graph.

i.e., A graph is said to be a null graph if it has no edges between any pair of vertices. $\cdot v_1$ $v_2 \cdot$ $\cdot v_3$

Degree of vertex in a Digraph.

a) out degree b) Indegree.



$\deg^-(a) = 3$	$\deg^+(a) = 1$
$\deg^-(b) = 1$	$\deg^+(b) = 2$
$\deg^-(c) = 2$	$\deg^+(c) = 1$
$\deg^-(d) = 1$	$\deg^+(d) = 3$.
(Indegree)	(Outdegree)

Indegree:

The Number of edges with V as their terminal vertex is called indegree of V and is denoted as $deg^-(V)$

Out degree

In a directed graph, the number of edges with V as their initial vertex is called outdegree of V and is denoted as $deg^+(V)$

Source:

A vertex in a digraph with zero indegree is called a source.

Sink:

A vertex in a digraph with zero outdegree is called a sink.

Also Note that,

$$\sum deg^-(v) = \sum deg^+(v) = \text{No., of edges.}$$

Note:

A loop at a vertex contributes 1 to both the indegree and the outdegree of this vertex.

Theorem ①: Handshaking Theorem

If $G(V, E)$ is an undirected graph with 'e' edges then

$\sum deg(V_i) = 2e$.

[ie., the sum of the degrees of all the vertices of an undirected graph is twice the no., of edges of the graph and hence even.]

proof:

Since every edge is incident with exactly two vertices, every edge contributes 2 to the sum of the degree of the vertices.

$\therefore$ All of the 'e' edges contributes ($2e$) to the sum of the degree of the vertices.

$$\therefore \sum_i deg(V_i) = 2e.$$

Ex:-

$d(V_1) = 2$ $d(V_2) = 4$

$d(V_3) = 2$ $d(V_4) = 2$

No., of edges $= 5$

$\sum d(V_i) = 2+4+2+2 = 10 = 2\times e = 2\times 5 = 10$

Theorem: 2

In an undirected graph, the number of odd degree vertices are even.

proof:

Let $G = (V, E)$ be the undirected graph. Let V_1 and V_2 be the set of all vertices of even degree and set of all vertices of odd degree respectively.

Then by previous thm, we have

$$2e = \sum_{v_i \in V_1} \deg(v_i) + \sum_{v_j \in V_2} \deg(v_j) \quad (1)$$

Since each $\deg(v_i)$ is even,

$\sum_{v_i \in V} \deg v_i$ is even.

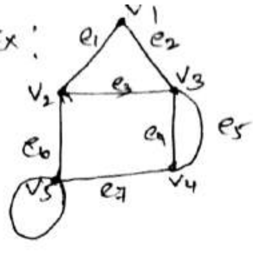
As LHS of Eqn (1) is even, we get

$\sum_{v_j \in V} \deg(v_j)$ is even.

Since each $\deg(v_j)$ is odd, the number of terms contained in $\sum_{v_j \in V_2} \deg(v_j)$ is even.

i.e., The no. of vertices of odd degree is even

Ex:



$d(v_1) = 2$
$d(v_2) = 3$
$d(v_3) = 4$
$d(v_4) = 3$
$d(v_5) = 4$

Theorem: 3

The maximum number of edges in a simple graph with 'n' vertices is $\frac{n(n-1)}{2}$

Proof:

We prove this theorem by the method of Mathematical induction 'n'.

for $n=1$, a simple graph with one vertex has no edges

$\therefore$ The result is true for $n=1$.

for $n=2$, a simple graph with 2 vertices may have atmost one edge

$\therefore \frac{2(2-1)}{2} = 1$

The result is true for $n=2$

Assume that the result is true for $n=k$, ie., a graph with

k vertices has atmost $\frac{k(k-1)}{2}$ Edges. when $n=k+1$, Let G be a graph having 'n' vertices and G' be the graph obtained from G by deleting one vertex say $v \in V(G)$

Since G' has k vertices then by the hypothesis G' has atmost $\frac{k(k-1)}{2}$ edges. Now add the vertex v to G'. [v may be adjacent to all the k vertices of G'.]

$\therefore$ The total number of edges in G are

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

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

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

$\therefore$ The result is true for $n=k+1$

Hence the maximum no. of edges in a simple graph with n vertices is $\frac{n(n-1)}{2}$.

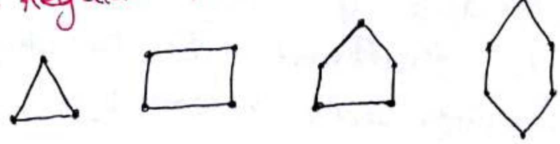
Some Special Types of Graphs:

Regular Graph:

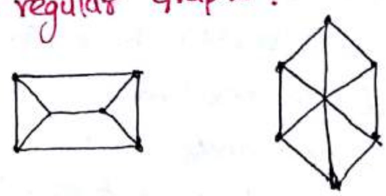
If Every vertex of a simple Graph has the same degree, then the graph is called a regular graph.

If every vertex in a regular graph has degree n then the graph is called n-regular.

2- Regular Graphs:



3- regular Graphs:



Complete Graph:

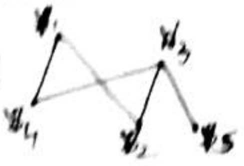
A Simple Graph, in which there is exactly one edge between each pair of distinct vertices is called a complete graph. The complete graph on 'n' vertices is denoted by K_n

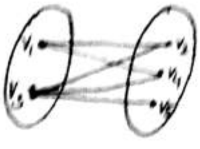
K_1 K_2 K_3 K_4 K_5

K_6

Bipartite Graph:

A simple graph G is said to be bipartite if its vertex set V can be partitioned into two disjoint non-empty sets V_1 and V_2, such that every edge of $V_1 \cup V_2 = V$, such that every edge of G has one end vertex in V_1 and another end vertex in V_2. (So that no edge in G, connects either two vertices in V_1 or two vertices in V_2).

G: 



Complete Bipartite Graph:

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.

A complete bipartite graph is denoted by $K_{m,n}$, if V_1 contains m vertices and V_2 contains n vertices, assume $m \le n$

$K_{2,3}$

$K_{3,3}$

Graph Representation:

The diagrammatic representation of a graph is very convenient for visual study, if the number of vertices and edges are vertically small. If they are large, the graph can be represented by a matrix. The matrix representation of a graph may be useful in computer programming. There are mainly two ways of representing a graph by a matrix, namely,

i) Adjacency matrix and.

ii) Incidence matrix

Adjacency Matrix of a Simple Graph:

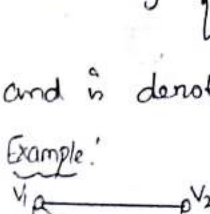
Let $G = (V, E)$ be a simple graph with 'n' vertices, Let the vertices of G be denoted as $V_1, V_2 \cdots V_n$. The adjacency matrix of G is the $n \times n$ matrix $[a_{ij}]$.

where $a_{ij} = \begin{cases} 1, & \text{if there exist an edge bet}^{n}\ v_i \,\&\, v_j \\ 0, & \text{otherwise.} \end{cases}$

and is denoted by A (or) $A(G)$.

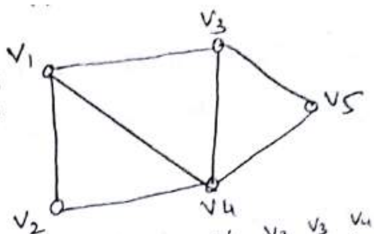
Example:

G_1:



$$A(G_1) = \begin{array}{c c} & \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{array}{c} v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} & \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

G_2:



$$A(G_2) = \begin{array}{c c} & \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{array}{c} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} & \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

The Following Basic Properties of an adjacency matrix are obvious:

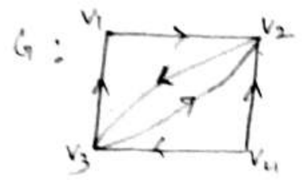
1) Since a simple graph has no loops, each diagonal entry of A, $a_{ii} = 0$, for $i = 1, 2 \cdots n$.

2) The adjacency matrix of a simple graph is symmetric $a_{ij} = a_{ji}$. Since both of these entries are 1 when v_i and v_j are adjacent and both are zero otherwise. Conversely, given any symmetric zero one (1) matrix. 'A' which contains only 0's on its diagonal there exists a simple graph G whose adjacency matrix is 'A'.

3) $\deg(v_i)$ is equal to the number of 1's in the i^{th} row or j^{th} column.

Adjacency Matrix of a Digraph.

When G is a digraph with 'n' vertices $v_1, v_2 \ldots v_n$ the matrix A (or) $A(G) = [a_{ij}]$ where $a_{ij} = \begin{cases} 1, & \text{if } (v_i, v_j) \text{ is a directed edge of } G \\ 0, & \text{otherwise} \end{cases}$ is called Adjacency Matrix of digraph.



$$A(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

$d^+(v_1) = 1$, $d^+(v_2) = 1$, $d^+(v_3) = 2$, $d^+(v_4) = 2$

$d^-(v_1) = 1$, $d^-(v_2) = 3$, $d^-(v_3) = 2$, $d^-(v_4) = 0$.

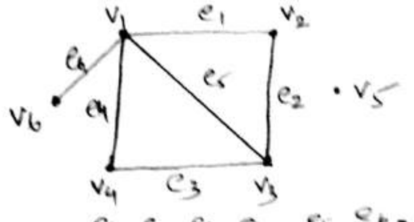
Note that, in the adjacency Matrix of a digraph the number of 1's in the i^{th} row of $A(G)$ is the Number of outdegree of the the vertex v_i (-) and the number of 1's in the j^{th} column of $A(G)$ is the number of Indegree of the vertex v_j.

For a digraph, the adjacency matrix $A(G)$ need not be symmetric.

Incidence Matrix of a Simple Graph.

When $G = (V, E)$ is an undirected Simple Graph with 'n' vertices $v_1, v_2 \ldots v_n$ and 'm' edges $e_1, e_2 \ldots e_m$ the matrix B (or) $B(G) = [b_{ij}]$ where $b_{ij} = \begin{cases} 1, & \text{when edge } e_i \text{ is Incident with } v_j \\ 0, & \text{Otherwise} \end{cases}$

is called the Incidence Matrix of G.



$$B(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{array} \begin{array}{c} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

- The following basic properties of an incidence matrix are obvious.

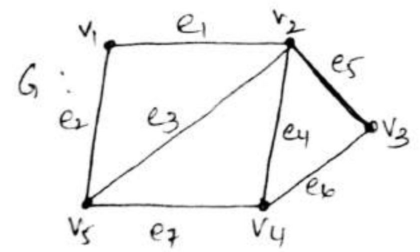
1) Each column of B contains exactly 2 unit entries.

2) A row with all 0 entries corresponds to an isolated vertex.

3) A row with a single unit entry corresponds to a pendant vertex.

4) $\deg(v_i)$ is equal to the number of 1's in the ith row.

G :

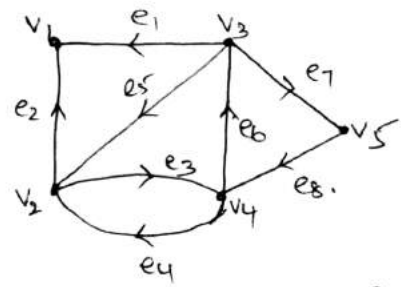


$$B(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

Incidence Matrix of a Digraph.

When $G = (V, E)$ is a digraph with 'n' vertices $v_1, v_2 \cdots v_n$ and m edges $e_1, e_2, \cdots, e_m$ the $n \times m$ matrix, B (or) $B(G) = [b_{ij}]$ where

$$b_{ij} = \begin{cases} 1, & \text{if } j^{th} \text{ edge having } i^{th} \text{ vertex as Initial Vertex} \\ -1, & \text{if } j^{th} \text{ edge having } i^{th} \text{ vertex as terminal vertex} \\ 0, & \text{otherwise.} \end{cases}$$

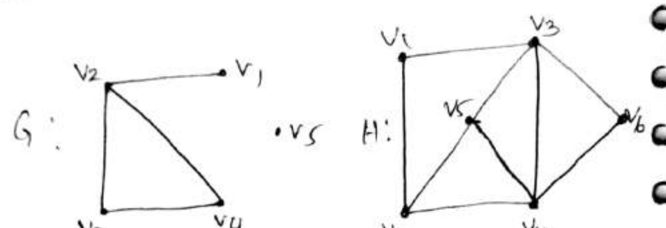


$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{cccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \end{array} \\ \begin{bmatrix} -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & -1 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & -1 & 1 & 1 \\ 0 & 0 & -1 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \end{bmatrix} \end{array}$$

Degree Sequence of a Graph:

We represent the degree of th vertices in the graph G as a no decreasing sequence called deg sequence of the graph.

Let us consider the Graphs.



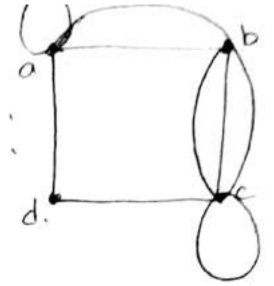
Degree sequence of G : 0, 1, 2, 2, 3

H : 2, 2, 3, 3, 4, 4.

Adjacency Matrix of a Pseudograph:

A Pseudograph (namely an undirected graph with loops and parallel edges) can also be represented by an adjacency matrix. In this case, a loop at the vertex v_i is represented by a 1 at the $(i,j)^{th}$ position and the $(i,j)^{th}$ entry equals the number of edges that are incident on v_i and v_j.

The adjacency matrix of a pseudograph is also a symmetric matrix.

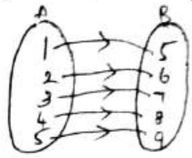


$$A(G_1) = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 1 & 2 & 0 & 1 \\ 2 & 0 & 3 & 0 \\ 0 & 3 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

[one to one : $f : A \to B$, $A = \{1, 2, 3, 4, 5\}$

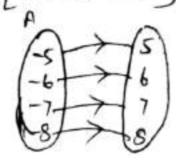
$B = \{5, 6, 7, 8, 9, 10\}$ defined by

$f(x) = x + 4$.



on-to fn : $f : A \to B$, $A = \{-5, -6, -7, -8\}$,

$B = \{5, 6, 7, 8\}$ defined by $f(x) = -x$.



Graph Isomorphism:

The simple graphs $G_1 = (V_1, E_1)$ & $G_2 = (V_2, E_2)$ are isomorphic if there is a one to one and onto fn, 'f' from V_1 to V_2 with the property that x and y are adjacent in G_1, if and only if $f(x)$ and $f(y)$ are adjacent in G_2 for all $x, y \in V_1$ such a function f is called an isomorphism.

Scanned by CamScanner

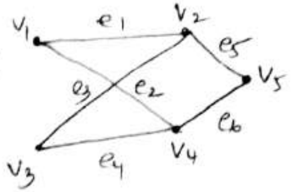
In case of isomorphism, we write $G_1 \cong G_2$. We observe that isomorphic graphs have

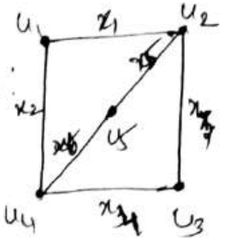
1) The same number of vertices
2) The same number of edges
3) The degree sequence of the graphs are same.

If any of those conditions is not satisfied in two graphs then we can say the graphs are not isomorphic.

Problems:

1. Show that the given graphs are isomorphic.

G_1 : 

G_2 : 

Soln:

The number of vertices in $G_1 = 5$

The number of vertices in $G_2 = 5$

The number of edges in $G_1 = 6$

The number of edges in $G_2 = 6$

Degree sequence of G_1 : 2, 2, 2, 3, 3

Degree sequence of G_2 : 2, 2, 2, 3, 3

The number of vertices and edges are same. The degree sequence are same.

Since in G_1 we've the vertices v_2 and v_4 of degree 3. They must be mapped to u_2 and u_4 in G_2.

Define a fn., $f : G_1 \to G_2$ as.

$f(v_1) = u_1$; $f(v_2) = u_2$; $f(v_3) = u_3$;

$f(v_4) = u_4$. $f(v_5) = u_5$).

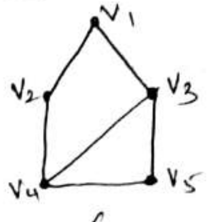
$f(e_1) = x_1$, $f(e_2) = x_2$; $f(e_3) = x_4$;

$f(e_4) = x_3$; $f(e_5) = x_6$; $f(e_6) = x_5$.

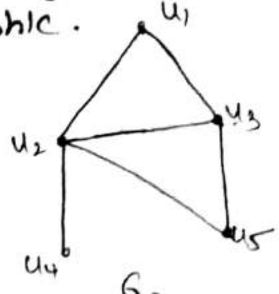
$\therefore$ f is a onto, one to one between the vertices and edges.

$\therefore$ Given Graphs G_1 and G_2 are isomorphic.

2) Show that the graphs G_1 and G_2 are not isomorphic.



G_1



G_2

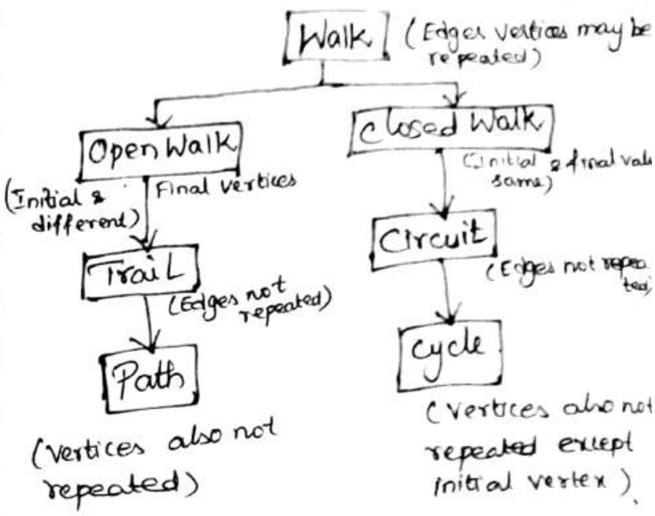
Soln:

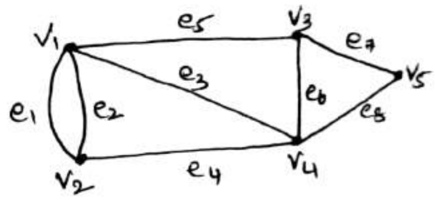
In the Graph G_1, we have the degree sequence is 2, 2, 2, 3, 3, but the degree sequence of G_2 is 1, 2, 2, 3, 4, so we are not able to find 1-1 correspondence betn the edges of G_1 & G_2.

$\therefore$ G_1 and G_2 are not isomorphic.

Connectivity:

WALK: A walk is an undirected graph $G = (V, E)$ is a finite non-empty sequence $\omega = v_0 e_1 v_1 e_2 v_2 e_3 \ldots v_{k-1} e_k v_k$ consisting of vertices and edges alternatively, such that e_i connects v_{i-1} and v_i. The vertices v_0 and v_k are called origin and terminus of the walk ω. The other vertices are called internal vertices





Open walk:

A walk is open if its initial (starting) and final (Ending) vertices are different

Closed Walk:

A walk is closed if its initial and final vertices are the same.

Trail:

A trail is an open walk in which no edges is repeated, Vertices

Scanned by CamScanner

can be repeated in a trail

Circuit:

A circuit is a closed trail or a circuit is a closed walk in which no edges is repeated vertices may be repeated.

path:

A path is trail with no repeated vertex (or) a path is an open walk in which neither any Edge nor any vertex is repeated. It is also called an Elementary path.

Cycle:

A cycle is a circuit in which no vertex is repeated except the initial vertex, or a cycle is a closed walk in which neither any edge nor any vertex except the initial vertex is repeated.

Example:

1) Open walk: $v_1 e_5 v_3 e_7 v_5 e_8 v_4 e_6 v_3 e_5 v_1 e_1 v_2$.

2) Closed walk: $v_2 e_4 v_4 e_6 v_3 e_6 v_4 e_3 v_1 e_2 v_2$

3) Trail: $v_1 e_1 v_2 e_2 v_1 e_5 v_3 e_7 v_5$

4) Circuit: $v_1 e_1 v_2 e_2 v_1 e_5 v_3 e_7 v_5 e_8 v_4 e_3 v_1$

5) Path: $v_1 e_5 v_3 e_7 v_5 e_8 v_4 e_4 v_2$

6. Cycle: $v_1 e_3 v_4 e_8 v_5 e_7 v_3 e_5 v_1$

Directed Walk:

A directed walk in a digraph G is a finite non-null sequence $w = v_0 e_1 v_1 e_2 v_2 e_3 \cdots v_{k-1} e_k v_k$ consists of vertices and directed edges alternating in which each directed edge e_i has v_{i-1} as initial vertex, v_i as terminal vertex.

Open Directed Walk:

An open directed walk is a directed walk whose initial and final vertices are distinct.

Closed Directed Walk:

A closed directed walk is a directed walk whose initial & End vertises are the same.

Directed Trail:

A directed trial is an open directed walk in which no edge is repeated.

Directed Circuit:

A directed circuit is a closed directed walk in which no directed edge is repeated. It is closed directed trail.

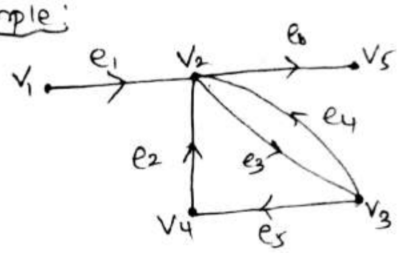
Directed Path:

A directed path is a directed trail with no repeated vertex. It is an open directed walk in which neither any directed edge nor any vertex is repeated.

Directed Cycle:

A directed cycle is a directed circuit in which no vertex is repeated except the initial vertex which is also the end vertex of the sequence. It is a closed walk in with neither any directed edge nor any vertex, except the initial vertex is repeated.

Example:



Open directed Walk:

$v_1 e_1 v_2 e_3 v_3 e_4 v_2 e_3 v_3 e_4 v_2 e_6 v_5$

Closed directed Walk:

$v_2 e_3 v_3 e_4 v_2 e_3 v_3 e_5 v_4 e_2 v_2$

Directed Trail:

$v_1 e_1 v_2 e_3 v_3 e_4 v_2 e_6 v_5$

Directed Circuit:

$v_2 e_3 v_3 e_5 v_4 e_2 v_2$

Directed Circuit: $V_2 e_3 V_3 e_5 V_4 e_2 V_2$

Directed Path: $V_1 e_1 V_2 e_6 V_5$

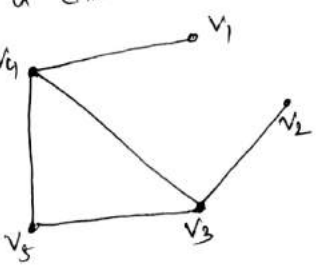
Directed Cycle: $V_2 e_3 V_3 e_4 V_2$.

Connected And DisConnected Graph:

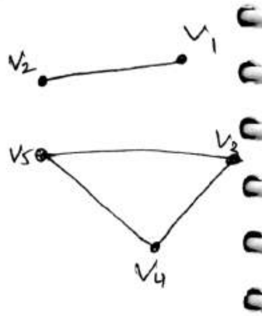
An undirected graph is said to be connected if there exists atleast one path between any pair of vertices of the graph.

A graph, which is not connected is a disconnected graph.

G:



H:



Here G is connected but not H Since there is no path between V_1 and V_5. In that case we say H is a disconnected graph.

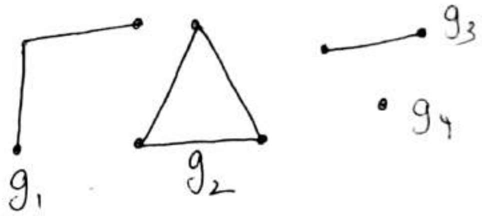
Components of a Graph:

A Disconnected graph consists of two (or) more connected graphs. Each of these connected graphs is called a component graph.

In otherwords, the connected subgraphs of a graph G are called components of the graph G.

The number of components is denoted by $\omega(G)$

G:



Here $\omega(G) = 4$.

Remark:

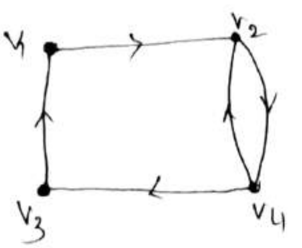
i) For a connected graph $\omega(G) =$

ii) For a null graph having 'n' vertices $\omega(G) = n$.

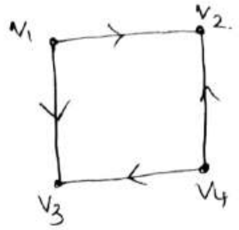
Scanned by CamScanner

Defn.

A digraph is said to be connected if there exists atleast one directed path between every pair of vertices.



Connected.



Disconnected.

Theorem; 4:

A simple graph with 'n' vertices and 'k' components can have atmost $\frac{(n-k)(n-k+1)}{2}$ edges.

proof:

Let $n_1, n_2, \ldots n_k$ be the number of vertices in each of k components of the graph G.

i.e., $\sum_{i=1}^{k} n_i = n$ —(1)

Consider

$$\sum_{i=1}^{k} (n_i - 1) = (n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1)$$

$$= \sum_{i=1}^{k} n_i - k = n - k$$

(by (1))

Squaring on both sides we get

$$(n_1-1)^2 + (n_2-1)^2 + \cdots + (n_k-1)^2 \leq (n-k)^2$$

$$\sum_{i=1}^{k} n_i^2 - 2n + k \leq (n-k)^2$$

$$\sum_{i=1}^{k} n_i^2 \leq (n-k)^2 + 2n - k \quad \text{—(2)}$$

Since G is simple, the maximum number of edges of G in its components is $\frac{n_i(n_i-1)}{2}$.

$\therefore$ Maximum number of edges of G.

$$= \sum_{i=1}^{k} \frac{n_i(n_i-1)}{2} = \sum_{i=1}^{k} \left(\frac{n_i^2 - n_i}{2}\right)$$

$$\Rightarrow \frac{1}{2}\left[\sum_{i=1}^{k} n_i^2 - \sum_{i=1}^{k} n_i\right]$$

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

(by (1) & (2))

$$\Rightarrow \leq \frac{1}{2}\left[(n-k)^2 + (n-k)\right]$$

$$\Rightarrow \leq \frac{1}{2}\left[(n-k)[n-k+1]\right]$$

$\therefore$ Maximum number of edges of $G \leq \frac{(n-k)(n-k+1)}{2}$

Theorem :

If a graph has exactly two vertices of odd degree, there must be a path joining these two vertices.

Proof:

Let G be a graph having exactly two vertices u and v of odd degree.

If G is connected, then there is a u-v path.

Let G be not connected and let G_1 be the component of G containing the vertex G.

We observe that,

i) G_1 is connected subgraph of G.

ii) $d_{G_1}(v) = d_G(v)$ for every vertex v of G,

iii) $u \in G_1$ and $d(u)$ = odd integer (degree)

iv) If $v \notin G_1$ and u is the only odd degree vertex in G_1, then it is a contradiction the theorem.

W.K.T In a graph the number of odd degree vertices are even.

v) If $v \in G_1$, then $u, v, \in G_1$ and G_1 is connected, therefore there is a u-v path in G_1 and hence in G.

From the case (iv) and (v)

We get there is a u-v path in G.

Subgraph:

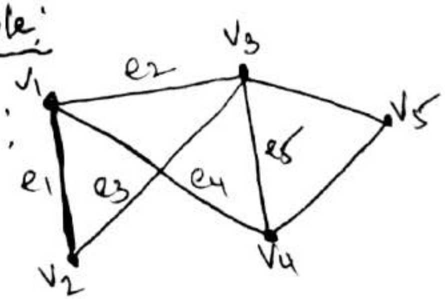
A graph $H = (V(H), E(H))$ is said to be subgraph of a graph $G = (V(G), E(G))$ if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$.

Spanning Subgraph:

A Subgraph H of G is said to be a spanning subgraph of G if $V(H) = V(G)$.

Example:

G :



Theorem: 6

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.

To prove that G is connected.

Suppose if G is not connected then G must have atleast 2 components. Let it be G_1 and G_2. Let V_1 be the vertex set of G_1 with $|V_1| = m$. If V_2 is the vertex set of G_2. Then $|V_2| = n-m$. Then

i) $1 \le m \le n-1$

ii) There is no edge joining a vertex of V_1 and a vertex of V_2

iii) $|V_2| = n-m \geq 1$

Now, $|E(G)| = |E(G_1 \cup G_2)|$

$= |E(G_1)| + |E(G_2)|$

$\le \frac{m(m-1)}{2} + \frac{(n-m)(n-m-1)}{2}$

(By Thm ③)

$\le \frac{1}{2}\left[m^2 - m + n(n-m-1) - m(n-m-1)\right]$

$\le \frac{1}{2}\left[n(n-1) - nm - m(n-m-1) + m^2 - m\right]$

$\le \frac{1}{2}\left[n(n-1) + 2n - 2 - 2n + 2 - nm - nm + m^2 + m + m^2 - m\right]$

[Adding & subtracting $2n-2$]

$\le \frac{1}{2}\left[n(n-1) - 2(n-1) + 2n - 2 - 2nm + 2m^2\right]$

$\le \frac{1}{2}\left[n(n-1) - 2(n-1) + 2n(1-m) + 2(m^2-1)\right]$

$\le \frac{1}{2}\left[(n-1)(n-2) + 2n(1-m) + 2(m-1)(m+1)\right]$

$\le \frac{1}{2}\left[(n-1)(n-2) - 2n(m-1) + 2(m-1)(m+1)\right]$

$\le \frac{1}{2}\left[(n-1)(n-2) - 2(m-1)(n-m-1)\right]$

$|E(G)| \le \frac{(n-1)(n-2)}{2}$. Since $(m-1) \cdot (n-m-1) \geq 0$ for $1 \le m \le n-1$

which is a contradiction as G has

Scanned by CamScanner

more than $\frac{(n-1)(n-2)}{2}$ Edges.

Hence G is a connected graph.

Euler Graph And Hamilton Graph:

Eulerian Path:

A path of a graph G is called a Eulerian path, if it contains each edge of the graph exactly once.

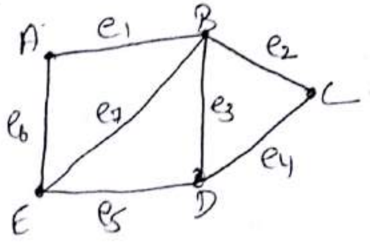
Eulerian Circuit (or) Eulerian cycle:

A circuit of a graph G is called an Eulerian circuit if it includes each edge of G exactly once.

Eulerian Graph: (or) Euler Graph:

Any graph containing an Eulerian circuit is called an Eulerian graph.

ex:

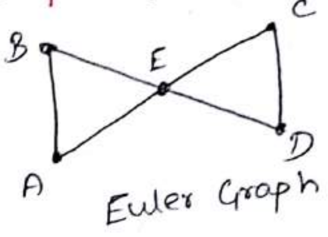


Eulerian Path. E & D

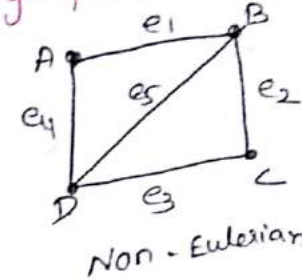
$E \xrightarrow{e_5} D \xrightarrow{e_4} C \xrightarrow{e_2} B \xrightarrow{e_1} A \xrightarrow{e_6} E \xrightarrow{e_7} B \xrightarrow{e_3} D$

For the above graph, we can not find Eulerian circuit (cycle). Therefore, given graph is non-Eulerian.

Example for Euler graph:



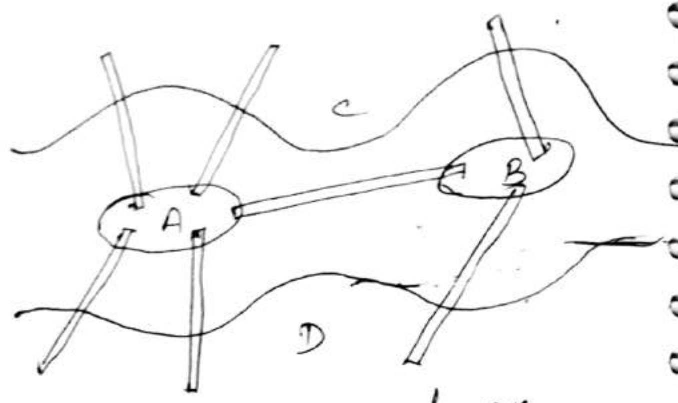
Euler Graph



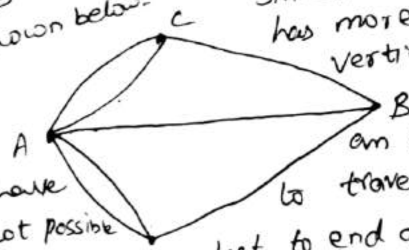
Non-Eulerian

Konigsberg Bridge Problem:

There are two islands A & B formed by a river. They are connected to each other and to river banks C and D by means of 7 bridges. The problem is to start from any one of the 4 land areas A, B, C, D walk across each bridge exactly once and returning to the starting point.



This problem is a famous Konigsberg bridge problem. When the situation is represented by a graph with vertices representing the land areas and the edges the bridges, we get a multigraph as shown below.



Since the above graph has more than two vertices of odd degree, we cannot have an Euler trail.

∴ It is not possible to travel all the bridges exactly once from start to end of any town.

[In a town of Konigsberg, Prussia was divided into 4 sections by the branches of the Preger river]

This problem is the same as that of drawing the graph without lifting the pen from the paper and without retracing any line.

In otherwords, the problem is to find whether there is an Eulerian circuit (a simple circuit containing every edge) in a graph.

But a connected graph has an Eulerian circuit if and only if each of its vertices is of even degree.

In the present case, all the vertices are of odd degree.

Hence, Konigsberg bridge problem has no solution.

Theorem : 9.

A connected graph is Euler graph (contains Eulerian circuit) if and only if each of its vertices is of even degree.

proof:

Let G be any graph having an Eulerian circuit and let c be an Eulerian circuit of G with origin & terminus vertex as u. Each time a vertex v occurs as an internal vertex of c, then two of the edges incident with v are accounted for degree.

We get, for internal vertex $v \in V(G)$

$$d(v) = 2 \times \begin{cases} \text{no., of times } v \text{ occur inside} \\ \text{the Euler circuit } c. \end{cases}$$

$$= \text{Even degree.}$$

and since an Euler circuit c contains every edge of G and c starts and ends at u.

$$\therefore d(u) = 2 + 2 \times \begin{cases} \text{no., of times } u \text{ occur} \\ \text{inside } c. \end{cases}$$

$$= \text{Even degree}$$

$\therefore$ G has all the vertices of Even degree.

Conversely,

Assume each of its vertices has an even degree.

Claim:

G has an Eulerian circuit,

Suppose not, i.e., Assume G be connected graph which is not having an Euler circuit, with all vertex of even degree and less number of edges.

i.e., Any graph having less number of edges than G then it has an Eulerian circuit. Since each vertex of u has degree atleast two, therefore G contains closed path. Let c be a closed path of Maximum possible length in G. If c itself has all the edges of G, then c itself an Eulerian circuit in G.

By assumption, c is not an Euler circuit of G and $G - E(c)$ has some component G' with $|E(G')| > 0$, c has less number of edges than G, therefore 'C' itself is an Eulerian, and C has all the vertices of even degree thus the connected graph G' also has all the vertices of even degree.

Since $|E(G')| < |E(G)|$,

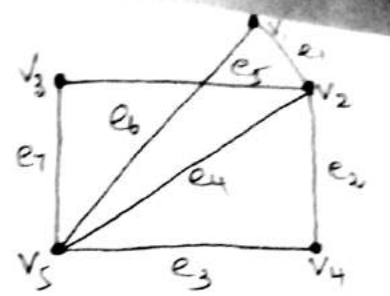
$\therefore$ G' has an Euler Circuit C'.

Because G is connected, there is a vertex v in both C and C'. Now join C and C' and transverse all the edges of C and C' with common vertex v, we get CC' is a closed path in G and $E(CC') > E(C)$, which is not possible for the choices of C.

$\therefore$ G has an Eulerian Circuit

$\therefore$ G is a Euler Graph.

1) Check the given graph is Euler graph or not.



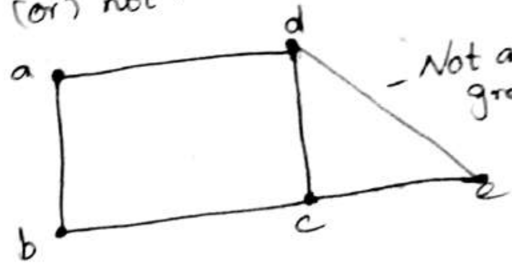
__Soln__

$d(v_1) = 2$, $d(v_2) = 4$; $d(v_3) = 2$

$d(v_4) = 2$ $d(v_5) = 4$.

Since, all the vertices is of even degree, by the above theorem the given graph is Euler graph.

2) Check whether the given graph is Euler (or) not.



– Not a Euler graph

Hamilton path.

A path of a graph G is called a Hamilton path, if it includes each vertex of G exactly one.

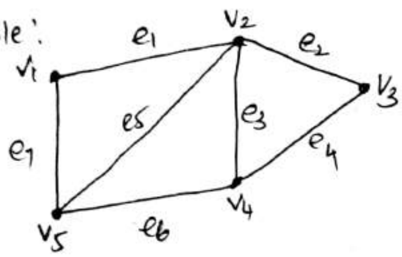
Hamilton cycle:

A cycle of a graph G is called a Hamilton cycle G, if it includes each vertex of G exactly one, except the starting and ending vertices.

Hamiltonian Graph:

Any graph containing a Hamiton cycle is called a Hamiltoniak graph.

example:



Hamilton cycle:

$v_4 - v_3 - v_2 - v_1 - v_5 - v_4$

P_1 : $v_1 e_1 v_2 e_5 v_5 e_6 v_4 e_4 v_3$ - Hamilton path.

Hamilton path : $v_1 - v_2 - v_3 - v_4 - v_5$

P_1 : $v_1 e_1$ - - Hamilton path.

P_2 : $v_5 e_5 v_2 e_2 v_3 e_4 v_4$ is a path but not Hamilton path.

C_1 : $v_4 e_4 v_3 e_2 v_2 e_1 v_1 e_7 v_5 e_6 v_4$ is a Hamilton cycle.

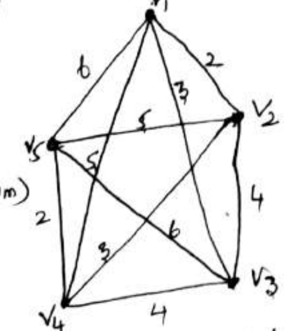
C_2 : $v_5 e_5 v_2 e_2 v_3 e_4 v_4 e_6 v_5$ is a cycle but not Hamilton cycle

Travelling Salesman Problem:

A salesman starts from his home and plans a trip to visit n-1 other places and return back to home. The natural objective is to minimize the total travelling time. If we assign each edge of K_n of a weights equal to the travelling time between the corresponding places then we seek a Hamilton cycle with minimum total weights. This problem is known as Travelling salesman problem.

Nearer Neighbour Algorithm:

Let $V_1, V_2 \ldots V_n$ be the vertices of K_n and w_{ij} denote the weight of edge $\langle V_i, V_j \rangle$ from an arbitrary starting vertex, move to a vertex with the least lost incident edge, and continue always visiting an unvisited neighbours of the current vertex until we visit all the vertices and return back to the starting vertex. Consider the weighted graph K_5. Let V_1 be the starting vertex.



i) from V_1 go to V_2 (Since $w(V_1, V_2)$ is minimum)

ii) from V_2 go to V_4

iii) from V_4 go to V_5

iv) from V_5 go to V_3 (V_2 is visited vertex, V_1 is starting vertex)

v) from V_3 go to V_1

The travelling route is $V_1 V_2 V_4 V_5 V_3 V_1$

The $2+2+2+6+3 = 16$ ... the circuit is 16

Problem:

1) Give an Example of a graph which is

i) Eulerian but not Hamiltonian

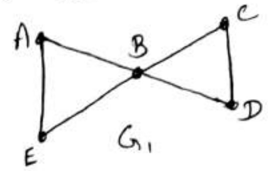
ii) Hamiltonian but not Eulerian.

iii) Both Eulerian and Hamitonian

iv) Non Eulearian and non Hamiltonian

Soln:

1) Eulerian but not Hamiltonian.



G_1 contains the Eulerian cycle.

A-B-C-D-B-E-A

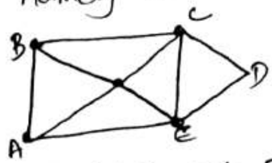
$\therefore G_1$ is Euler graph.

We cannot find Hamiltonian cycle. As the vertex B is repeated twice.

2) Hamiltonian but not Eulerian.

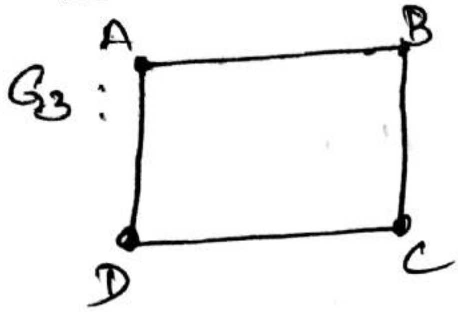
Since G_2 contains the Hamiltonian Cycle namely A-B-C-D-E-A. G_2 is Hamiltonian graph.

G_2 :



Since the degree of the vertex A is 3, deg(A) is not an even no., ... is not an Euler graph.

3) Both Eulerian and Hamiltonian.

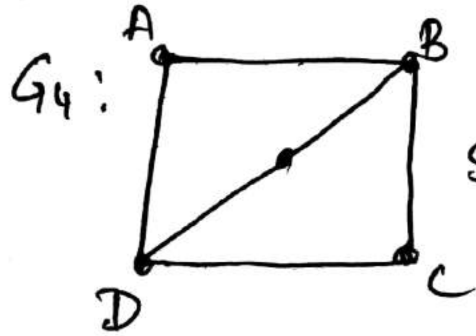


G_3 : A – B – C – D – A

Since the cycle contains all the edges G_3 is Eulerian. Since the cycle contain all the vertices exactly once, G_2 is Hamiltonian.

$\therefore$ G_3 is both Eulerian & Hamiltonian.

4) Non-Eulerian & non-Hamiltonian :



deg(B) = deg(D) = 3

Since degree of B and D are not an even number G_4 is not a Euler graph. As no cycle passes through each of the vertices exactly once, the given graph G_4 is not Hamiltonian.

$\therefore$ G_4 is neither Euler graph nor Hamiltonian graph.

Unit-5

BOOLEAN ALGEBRA

A complemented distributive Lattice is called Boolean Algebra.

i.e., A Boolean algebra is distributive Lattice with '0' element and '1' element in which every element has a complement.

i.e., A Boolean algebra is a non empty set with 2 binary operations $\wedge$ and $\vee$ and is satisfied by the following conditions.

$\forall\ a, b, c \in L$

1. L_1 : $a \wedge a = a$	$a \vee a = a$
2. L_2 : $a \wedge b = b \wedge a$	$a \vee b = b \vee a$
3. L_3 : $a \wedge (b \wedge c) = (a \wedge b) \wedge c$	$a \vee (b \vee c) = (a \vee b) \vee c$
4. L_4 : $a \wedge (a \vee b) = a$	$a \vee (a \wedge b) = a$

5. D_1 : $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

6. D_2 : $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

7. There exist elements '0' and '1' such that

$$a \wedge 0 = 0,\ a \vee 0 = a,\quad a \wedge 1 = a \text{ and } a \vee 1 = 1 \quad \forall\ a$$

8. $\forall\ a \in L$, there exist corresponding element a' in L such that $a \wedge a' = 0$ and $a \vee a' = 1$.

Note: Boolean Algebra is denoted by $(B, \wedge, \vee, 0, 1)$

Example :

$(\rho(A), \cup, \cap)$ is a Boolean Algebra, where A is any finite set.

Here, '0' element is ϕ

'1' element is given set A

Complement of $a = a' = A - a$

In a Boolean Algebra

$$(0)' = 1$$

and $$(1)' = 0$$

Note :

(1) In Lattice we have used the notations $\vee$ for sum and $\wedge$ for product. Boolean Algebra is a special case of Lattice and we use '+' for Boolean sum and '·' for Boolean Product.

(2) Therefore, here after we use the notations + and · instead of $\vee$ and $\wedge$ respectively.

Boolean Sum is defined as

$1 + 1 = 1 \quad 1 + 0 = 1 \quad 0 + 1 = 1 \quad 0 + 0 = 0$

Boolean Product is defined as

$1 \cdot 1 = 1 \quad 1 \cdot 0 = 0 \quad 0 \cdot 1 = 0 \quad 0 \cdot 0 = 0$

« Example : 1 »

Prove that $a + ab = a$

Solution :

LHS $= a + ab$

$= a(1 + b)$ (Distributive law)

$= a(1)$ $(\because 1 + a = 1)$

$\boxed{a + ab = a}$ $(a \cdot 1 = a)$

« Example : 2 »

Prove that $a + \bar{a}b = a + b$

Solution :

LHS $= a + \bar{a}b$

$= a + ab + \bar{a}b$ $(\because a = a + ab)$

$= a + b(a + \bar{a})$ (Distributive law)

$= a + b(1)$ $(\because a + \bar{a} = 1)$

$\boxed{a + \bar{a}b = a + b}$ $(\because a \cdot 1 = a)$

« Example : 3 »

Prove that $(a + b)(a + c) = a + bc$

Solution :

LHS $= (a + b)(a + c)$

$= aa + ac + ab + bc$ (Distributive law)

$= a + ac + ab + bc$ $(\because a \cdot a = a)$

$= a(1 + c) + ab + bc$ (Distributive law)

$= a + ab + bc$ $(\because 1 + a = 1)$

$(\because a + ab = a)$

$\boxed{(a + b)(a + c) = a + bc}$

« Example : 4 »

In any Boolean Algebra, show that $a = b$ ***iff*** $a\bar{b} + \bar{a}b = 0$

Solution :

Let (B, ·, +, 0, 1) be any Boolean Algebra.

Let $a, b \in B$ and $a = b$ ... (1)

Claim : $a\bar{b} + \bar{a}b = 0$

Now, $a\bar{b} + \bar{a}b = a \cdot \bar{b} + \bar{a} \cdot b$

$= a \cdot \bar{a} + \bar{a} \cdot a$ (Using (1))

$= 0 + 0$ $(\because a \cdot a' = 0)$

$= 0$

$\therefore$ $a\bar{b} + \bar{a}b = 0$

Conversely, Assume

$a\bar{b} + \bar{a}b = 0$

$\Rightarrow$ $a + a\bar{b} + \bar{a}b = a$ (Left Cancelation law)

$\Rightarrow$ $a + \bar{a}b = a$ (Absorption law)

$\Rightarrow$ $(a + \bar{a}) \cdot (a + b) = a$ (Distributive law)

$\Rightarrow$ $1 \cdot (a + b) = a$ $(a + \bar{a} = 1)$

$\Rightarrow$ $a + b = a$ $(a \cdot 1 = a)$ ... (A)

Consider, $a\bar{b} + \bar{a}b = 0$

$\Rightarrow$ $a\bar{b} + \bar{a}b + b = b$ (Right Cancelation law)

$\Rightarrow$ $a\bar{b} + b = b$ (Absorption law)

$\Rightarrow$ $(a + b) \cdot (b + \bar{b}) = b$ (Distributive law)

$\Rightarrow$ $(a + b) \cdot 1 = b$ $(b + \bar{b} = 1)$

$\Rightarrow$ $a + b = b$ $(b \cdot 1 = b)$ ... (B)

From (A) and (B)

$a = a + b = b$

$\Rightarrow$ $a = b$

« Example : 5 »

In any Boolean Algebra, show that

$$(a \cdot \bar{b}) + (b \cdot \bar{a}) = (a + b) \cdot (\bar{a} + \bar{b})$$

Solution :

Let $(B, \cdot, +, 0, 1)$ be any Boolean Algebra.

Let $a, b \in B$

Now $(a \cdot \bar{b}) + (b \cdot \bar{a}) = (a + (b \cdot \bar{a})) \cdot (\bar{b} + (b \cdot \bar{a}))$

(Distributive rule)

$= (a + b) \cdot (a + \bar{a}) \cdot (\bar{b} + b) \cdot (\bar{b} + \bar{a})$

(Distributive rule)

$= (a + b) \cdot (1) \cdot (1) \cdot (\bar{a} + \bar{b})$

$= (a + b) \cdot (\bar{a} + \bar{b})$

« Example : 6 »

Evaluate the expression for $\bar{a} = 0$, $a = 1$, $b = 1$, $c = 1$ *and* $d = 1$. $X = \bar{a} \cdot b + c\,(\overline{a \cdot d})$.

Solution :

$X = \bar{a}.b + c\,(\overline{a \cdot d})$

$= 0 \cdot 1 + 1\,(\overline{1 \cdot 1})$

$= 0 \cdot 1 + 1(\bar{1})$

$= 0 \cdot 1 + 1\,(0)$

$= 0 + 0 = 0$

« Example : 7 »

Evaluate the expression for $X = a\,[\overline{(b+c)+\bar{d}}]$ for $a = 0$, $b = 0$, $c = 1$ and $d = 1$.

Solution :

$X = a\,[\overline{(b+c)+\bar{d}}\,]$

$= 0\ \overline{(0+1)+\bar{1}}$

$= 0\,[\overline{1+0}\,]$

$= 0\,[0+1]$

$= 0\,[\,1\,]$

$= 0$

« Example : 8 »

Reduce the expression $a\,.\,\bar{a}b$.

Solution :

$a\,.\,\bar{a}b = 0 \cdot b$ $\quad [\because a\bar{a} = 0]$

$= 0$ $\quad [\because a \cdot 0 = 0]$

« Example : 9 »

Reduce the expression $a\,(a+c) = aa + ac$.

Solution :

$a\,(a+c) = aa + ac$

$= a + ac$ $\quad [\because a \cdot a = a]$

$= a\,(1+c)$ $\quad$ (Distributive law)

$= a$ $\quad [\,a + 1 = 1]$

« Example : 10 »

Reduce the expression $ab + abc + ab\bar{c} + \bar{a}bc$.

Solution :

$ab + abc + ab\bar{c} + \bar{a}bc$

$= ab\,(1+c) + ab\bar{c} + \bar{a}bc$

$= ab + ab\bar{c} + \bar{a}bc$ $\quad [\because a + 1 = 1]$

$= ab\,(1+\bar{c}) + \bar{a}bc$

$= ab + \bar{a}bc$ $\quad [\because a + 1 = 1]$

$= b\,(a + \bar{a}c)$

$= b\,(a+c)$ $\quad [\because a + \bar{a}b = a + b]$

« Example : 11 »

Reduce the expression $xy + \overline{xz} + x\bar{y}z\,(xy+z)$.

Solution :

$xy + \overline{xz} + x\bar{y}z\,(xy+z)$

$= xy + \overline{xz} + xx\bar{y}yz + x\bar{y}zz$ $\quad$ (Distributive law)

$= xy + \overline{xz} + x\bar{y}zz$ $\quad (\because a \cdot \bar{a} = 0)$

$= xy + \overline{xz} + x\bar{y}z$ $\quad (\because a \cdot a = a)$

$= xy + \bar{x} + \bar{z} + x\bar{y}z$ $\quad (\overline{ab} = \bar{a} + \bar{b})$

$= \bar{x} + x\bar{y}z + y + \bar{z}$ $\quad$ (Commutative law)

$= \bar{x} + \bar{y}z + y + \bar{z}$ $\quad (a + \bar{a}b = a + b)$

Here $b = \bar{y}z$

$= \bar{x} + y + \bar{z} + \bar{y}z$ $\quad$ (Commutative law)

$= \bar{x} + y + \bar{z} + \bar{y}$ $\quad (a + \bar{a}b = a + b)$

$= \bar{x} + \bar{z} + 1$ $\quad (a + \bar{a} = 1)$

$= 1$ $\quad (a + 1 = 1)$

« Example : 12 »

Reduce the expression $\bar{a}b\bar{c}d + \bar{a}bcd + abd$.

Solution :

$\bar{a}b\bar{c}d + \bar{a}bcd + abd$

$= \bar{a}bd(\bar{c} + c) + abd$ $\quad$ (Distributive law)

$= \bar{a}bd + abd$ $\quad (\because a + \bar{a} = 1)$

$= bd(\bar{a} + a)$ $\quad$ (Distributive law)

$= bd$ $\quad (a + \bar{a} = 1)$

« Example : 13 »

Simplify the expression $z(y + z)(x + y + z)$

Solution :

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

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

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

$= z(y + 1)(x + y + z)$

$= z(x + y + z)$

$= zx + zy + zz$

$= zx + zy + z$

$= z(x + y + 1)$

$= z$

« Example : 14 »

Simplify the expression $(x + \bar{y} + \bar{z})(x + \bar{y} + z)$.

Solution :

$(x + \bar{y} + \bar{z})(x + \bar{y} + z)$

$= xx + x\bar{y} + xz + \bar{y}x + \bar{y}\,\bar{y} + \bar{y}z + \bar{z}x + \bar{z}\,\bar{y} + \bar{z}z$

$= x + x\bar{y} + xz + \bar{y}x + \bar{y} + \bar{y}z + \bar{z}x + \bar{z}\,\bar{y} + \bar{z}z$

$= x(1 + \bar{y} + z + \bar{y} + \bar{z}) + \bar{y}(1 + z + \bar{z}) + 0$

$= x \cdot 1 + \bar{y} \cdot 1$

$= x + \bar{y}$

« Example : 15 »

Simplify the expression $(a \cdot b) + (b + c)$.

Solution :

$Y = (a \cdot b) + (b + c)$

$= b(a + 1) + c$

$= b \cdot 1 + c$

$= b + c$

« Example : 16 »

Prove that, in any Boolean Algebra

$$a\overline{b} + b\overline{c} + c\overline{a} = \overline{a}b + \overline{b}c + \overline{c}a$$

Solution :

Now $a\overline{b} + b\overline{c} + c\overline{a} = a\overline{b}\cdot 1 + b\overline{c}\cdot 1 + c\overline{a}\cdot 1$

$$= a\overline{b}\,(c+\overline{c}) + b\overline{c}\,(a+\overline{a}) + c\overline{a}\,(b+\overline{b})$$

$$= a\,\overline{b}\,c + a\,\overline{b}\,\overline{c} + b\,\overline{c}\,a + b\,\overline{c}\,\overline{a} + c\,\overline{a}\,b + c\,\overline{a}\,\overline{b}$$

$(\because\ a+\overline{a} = 1)$

$$= a\,\overline{b}\,c + \overline{a}\,\overline{b}c + b\,a\,\overline{c} + \overline{b}\,a\,c + c\,\overline{a}\,b + \overline{c}\,\overline{a}\,b$$

(Distributive rule)

$$= (a+\overline{a})\,\overline{b}\,c + (b+\overline{b})\,a\overline{c} + (c+\overline{c})\,\overline{a}b$$

$$= \overline{b}c\,(a+\overline{a}) + \overline{c}a\,(b+\overline{b}) + \overline{a}b\,(c+\overline{c})$$

$$= \overline{b}c\cdot 1 + \overline{c}a\cdot 1 + \overline{a}b\cdot 1 \qquad (\because\ a+\overline{a} = 1)$$

$$= \overline{b}c + \overline{c}a + \overline{a}b$$

$$= \overline{a}b + \overline{b}c + \overline{c}a$$

« Example : 17 »

Show that in any Boolean algebra

$$(a+b)\,(a'+c) = ac + a'b + bc$$

Solution :

Let (B, ·, +, 0, 1) be any Boolean Algebra.

$$\text{LHS} = (a+b)\cdot(a'+c)$$

$$= (a+b)\cdot a' + (a+b)\cdot c$$

(Distributive rule)

$$= a\cdot a' + b\cdot a' + a\cdot c + b\cdot c$$

(Distributive rule)

$$= 0 + a'b + a\,c + b\,c \quad (\because a\cdot a' = 0)$$

$$= a\,c + a'b + b\,c$$

$$= \text{RHS}$$

« Example : 18 »

Prove the following Boolean identities:

1. $a + (a'\cdot b) = a + b$
2. $a\cdot(a' + b) = a\cdot b$
3. $(a\cdot b) + (a\cdot b') = a$

Solution :

(1) $\text{LHS} = a + (a'\cdot b)$

$$= (a+a')\cdot(a+b) \qquad \text{(Distributive rule)}$$

$$= 1\cdot(a+b) \qquad (\because a + a' = 1)$$

$$= a + b \qquad (a\cdot 1 = a)$$

$$= \text{RHS}$$

(2) $a\cdot(a'+b) = a\cdot b$

$\text{LHS} = a\cdot(a'+b)$

$$= (a\cdot a') + (a\cdot b) \qquad \text{(Distributive rule)}$$

$$= 0 + (a\cdot b) \qquad (a\cdot a' = 0)$$

$$= a\cdot b \qquad (a + 0 = a)$$

$$= \text{RHS}$$

(3) $(a\cdot b) + (a\cdot b') = a$

$\text{LHS} = (a + (a\cdot b'))\cdot(b + (a\cdot b'))$

$\Rightarrow ((a+a)\cdot(a+b'))\cdot((b+a)\cdot(b+b'))$ (Distributive)

$\Rightarrow (a\cdot(a+b'))\cdot((b+a)\cdot 1)$ (Idempotent)

$\Rightarrow (a \cdot (a+b)) \cdot (b+a)$ (Absorption)

$\Rightarrow a \cdot (a+b)$ (Absorption)

$\Rightarrow a$

$\Rightarrow$ RHS

« Example : 19 »

Show that in a Boolean algebra the law of the double complement holds.

(or)

Prove the involution law $(a')' = a$

Solution :

It is enough to show that

$$a' + a = 1 \quad \text{and} \quad a \cdot a' = 0$$

By domination laws of Boolean Algebra, we get

$$a + a' = 1 \quad \text{and} \quad a \cdot a' = 0$$

By commutative laws, we get

$$a' + a = 1 \quad \text{and} \quad a' \cdot a = 0$$

$\therefore$ Complement of a' is a

$$(a')' = a$$

i.e., $a'' = a$

« Example : 20 »

Prove that $x \cdot (x+y) = x$

Solution :

$x \cdot (x+y) = (x+0) \cdot (x+y)$ ($\because x + 0 = x$ – Identity law)

$= x + 0 \cdot y$ (Distributive)

$= x + 0$ ($x \cdot 0 = 0$ - Dominance Rule)

$= x$

« Example : 21 »

Simplify : (1) $(a \cdot b)' + (a+b)'$

(2) $(a' \cdot b' \cdot c) + (a \cdot b' \cdot c)$

Solution :

(1) $(a \cdot b)' + (a+b)'$

$= (a' + b') + (a' \cdot b')$ (Demorgan's law)

$= ((a' + b') + a') \cdot ((a' + b') + b')$ (Distributive law)

$= (a' + b') \cdot (a' \cdot b')$ (Idempotent)

$= (a' \cdot (a' \cdot b')) + (b' \cdot (a' \cdot b'))$ (Distributive law)

$= (a' \cdot a' \cdot b') + (b' \cdot b' \cdot a')$ (Associative law)

$= (a' \cdot b') + (a' \cdot b)$ (Idempotent)

$= (a' \cdot b')$ (Idempotent)

(2) $(a' \cdot b' \cdot c) + (a \cdot b' \cdot c)$

$= (a' + a) \cdot (b' \cdot c)$ (Distributive rule)

$= 1 \cdot (b' \cdot c)$ $(a + a' = 1)$

$= b' \cdot c (a \cdot 1 = a)$

« Example : 22 »

Let a, b, c be any 3 elements of Boolean Algebra B, prove that (1) $a \cdot a = a$ (2) $a + a = a$

Solution :

Let $a = a \cdot 1$

$$= a \cdot (a + a') \qquad (a + a' = 1)$$

$$= a \cdot a + a \cdot a' \qquad \text{(Distributive rule)}$$

$$= (a \cdot a) + 0 \qquad (\because a + a' = 0)$$

$$= a \cdot a \qquad (a + 0 = a)$$

$$\therefore \quad a = a \cdot a$$

By taking dual of $a \cdot a = a$, we have $a + a = a$

« Example : 23 »

Let a, b, c $\in B$. Show that (1) $a \cdot 0 = 0$ (2) $a + 1 = 1$

Solution :

$$a \cdot 0 = (a \cdot 0) + 0 \qquad (a + 0 = a)$$

$$= (a \cdot 0) + (a \cdot a') \qquad (\because a + a' = 0)$$

$$= a \cdot (0 + a') \qquad \text{(Distributive rule)}$$

$$= a \cdot (a' + 0) \qquad \text{(Commutative rule)}$$

$$= a \cdot a' \qquad (a' + 0 = a)$$

$$= 0$$

$$\therefore \quad a \cdot 0 = 0 \qquad (a \cdot a' = 0)$$

By taking dual, of $a \cdot 0 = 0$, we have $a + 1 = 1$

« Example : 24 »

Prove the following Boolean identities:

(1) $a + (a' \cdot b) = a + b$

(2) $(a \cdot b) + (a \cdot b') = a$

(3) $a \cdot (a' + b) = a \cdot b$

Solution :

(1) $$a + (a' \cdot b) = (a + a') \cdot (a + b) \qquad \text{(Distributive rule)}$$

$$= 1 \cdot (a + b) \qquad (\because a + a' = 1)$$

$$= a + b \qquad (a \cdot 1 = a)$$

(2) $$(a \cdot b) + (a \cdot b') = a \cdot (b + b') \qquad \text{(Distributive rule)}$$

$$= a \cdot 1 \qquad (b + b' = 1)$$

$$= a$$

$$\therefore \quad (a \cdot b) + (a \cdot b') = a \qquad (b \cdot 1 = b)$$

(3) $$a \cdot (a' + b) = (a \cdot a') + (a \cdot b) \qquad \text{(Distributive rule)}$$

$$= 0 + (a \cdot b)$$

$$= a \cdot b$$

$$\therefore \quad a \cdot (a' + b) = a \cdot b$$

◂◂ Example : 25 ▸▸

Show that

$$(a_1' \cdot a_2' \cdot a_3' \cdot a_4') + (a_1' \cdot a_2' \cdot a_3' \cdot a_4) + (a_1' \cdot a_2' \cdot a_3 \cdot a_4)$$

$$+ (a_1' \cdot a_2' \cdot a_3 \cdot a_4') = a_1' \cdot a_2'$$

Solution :

$$\left(a_1' \cdot a_2' \cdot a_3' \cdot a_4'\right) + \left(a_1' \cdot a_2' \cdot a_3' \cdot a_4\right) = a_1' \cdot a_2' \cdot a_3'$$

and

$$\left(a_1' \cdot a_2' \cdot a_3 \cdot a_4\right) + \left(a_1' \cdot a_2' \cdot a_3 \cdot a_4'\right) = a_1' \cdot a_2' \cdot a_3$$

Hence the given formula is equal to

$$\left(a_1' \cdot a_2' \cdot a_3'\right) + \left(a_1' \cdot a_2' \cdot a_3\right) = a_1' \cdot a_2'$$

◂◂ Example : 26 ▸▸

Find the value of $a_1 . a_2 . \left[(a_1 . a_4) + a_2' + \left(a_3 \cdot a_1'\right)\right]$ *for* $a_1 = a,\ a_2 = 1,\ a_3 = b$ *and* $a_4 = 1$ *where a, b, 1 are elements of Boolean algebra.*

Solution :

By substituting the required elements in the expression, we get

$$a \cdot 1 \cdot [\,(a \cdot 1) + 1' + (b \cdot a')\,]$$

$$= a \cdot [\,a + 0 + (b \cdot b)\,]$$

$$= a \cdot (a + b)$$

$$= a \cdot 1$$

$$= a$$

Alternatively, the given expression can be written in an equivalent form as

$$\left(a_1 \cdot a_2 \cdot a_1 \cdot a_4\right) + \left(a_1 \cdot a_2 \cdot a_2'\right) + \left(a_1 \cdot a_2 \cdot a_3 \cdot a_1'\right)$$

$$= \left(a_1 \cdot a_2 \cdot a_4\right) + 0 + 0$$

$$= a_1 \cdot a_2 \cdot a_4$$

Now replacing variables, we get

$$a \cdot 1 \cdot 1 = a$$

◂◂ Example : 27 ▸▸

Apply Demorgan's theorem to the following expression

(i) $\overline{(x + \overline{y})\,(\overline{x} + y)}$; (ii) $\overline{(a + b + c)\,d}$

Solution :

(i) $\overline{(x + \overline{y})\,(\overline{x} + y)} = \overline{a + \overline{b}} + \overline{\overline{a} + b}$ Demorgan's theorem

$= \overline{a} \cdot \overline{\overline{b}} + \overline{\overline{a}} \cdot b$ Demorgan's theorem

$= \overline{a} \cdot b + a \cdot \overline{b}$ $(\overline{\overline{a}} = a)$

$= a \oplus b$

(ii) $\overline{(a + b + c)\,d} = \overline{a + b + c} + \overline{d}$ Demorgan's theorem

$= \overline{a} \cdot \overline{b} \cdot \overline{c} + \overline{d}$ Demorgan's theorem