## UNIT - I LOGIC AND PROOFS

## Proposition:

A statement that is either true or false put not both is called a proposition.

## Example:

1. $2+2=4$--- True
2. 4 is a even prime number ----- False

## Statement:

Declarative sentences which cannot be further split into simpler sentences are called atomic statement.

## Example:

India is a country.

## Molecular statements :

New statement can be formed from atomic statement using connectives. The resulting statements are called molecular statements.

## Example:

Jack \& Jill went upto hill.

## Conjunction:

Let $\mathrm{P} \& \mathrm{Q}$ be a propositions then the conjunction of $\mathrm{P} \& \mathrm{Q}$ is denoted by $\mathrm{P} \wedge \mathrm{Q}$. The truth table is as follows.

| P | Q | $\mathrm{P} \wedge \mathrm{Q}$ |
| :---: | :---: | :---: |
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | F |

## Disjunction:

The disjunction of two statement $\mathrm{P} \& \mathrm{Q}$ is defined by PVQ. The truth table is as follows.

| P | Q | PVQ |
| :---: | :---: | :---: |
| T | T | T |
| T | F | T |
| F | T | T |
| F | F | F |

## Conditional:

If $\mathrm{P} \& \mathrm{Q}$ are any two statements, then the statement $\mathrm{P} \rightarrow \mathrm{Q}$, "if P then $Q$ " is called conditional proposition (or) statement.

| P | Q | $\mathrm{P} \rightarrow \mathrm{Q}$ |
| :---: | :---: | :---: |
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

## Biconditional:

If $P \& Q$ are any two statements, then the statement $p \leftrightarrow Q$ is called biconditional statement.

| P | Q | $\mathrm{P} \leftrightarrow \mathrm{Q}$ |
| :---: | :---: | :---: |
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | T |

## Tautology and Contradiction:

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

A statement which is false for all possible truth values of the variables in the statement is called contradiction.
Prove that $(\mathbf{7 P} \wedge(\mathbf{7} \wedge \wedge \mathbf{R}) \mathbf{V}(\mathbf{Q} \wedge \mathbf{R}) V(\mathbf{P} \wedge \mathbf{R}) \Leftrightarrow \mathbf{R}$

## Solution:

$$
\begin{aligned}
& (7 P \wedge(7 Q \wedge R) V(Q \wedge R) V(P \wedge R) \\
& \Leftrightarrow>(7 P \wedge(7 Q \wedge R) V(Q V P) \wedge R[\text { distributive law] } \\
& \Leftrightarrow \Rightarrow(7 P \wedge 7 Q \wedge R V(Q V P) \wedge R[\text { Associative law }] \\
& \Leftrightarrow=>(7(P V Q) \wedge R) V(Q V P) \wedge R[\text { Demergan's law] } \\
& \Leftrightarrow \Rightarrow 7(P V Q) V(P V Q) \wedge R[\text { Distributive law] }
\end{aligned}
$$

$$
\begin{aligned}
& \Leftrightarrow=>\mathrm{T} \wedge \mathrm{R} \text { [Tautology law] } \\
& \Leftrightarrow \mathrm{R} \text { [Identity law] }
\end{aligned}
$$

Using the truth table verify that the proposition $(\mathbf{P} \wedge \mathbf{Q}) \wedge 7(P V Q)$ Solution:

| P | Q | $\mathrm{P} \wedge \mathrm{Q}$ | PVQ | $7(\mathrm{PVQ})$ | $(\mathrm{P} \wedge \mathrm{Q} \wedge 7(\mathrm{PVQ})$ |
| :--- | :--- | :---: | :---: | :---: | :---: |
| T | T | T | T | F | F |
| T | F | F | T | F | F |
| F | T | F | T | F | F |
| F | F | F | F | T | F |

Show that the proposition $(\mathbf{P V Q}) \Leftrightarrow(\mathrm{QVP})$ is a tautology.
Solution:

| P | Q | PVQ | QVP | $(\mathrm{PVQ}) \Leftrightarrow(\mathrm{QVP})$ |
| :---: | :---: | :---: | :---: | :---: |
| T | T | T | T | T |
| T | F | T | T | T |
| F | T | T | T | T |
| F | F | F | F | T |

Let p : There is rain and q : I buy an Umbrella
Contrapositive: $\neg \mathrm{q} \rightarrow \neg \mathrm{p}$
That is "If I don't buy an umbrella, then there is no rain"
Converse: $q \rightarrow p$
That is "If I buy an umbrella , then there is rain"
Inverse: $\neg \mathrm{p} \rightarrow \neg \mathrm{q}$
That is "If there is no rain ,then I will not buy an umbrella"
Get the contra positive of the statement "If it is raining then I get wet" Let p : it is raining and
q : I get wet
Given $\mathrm{p} \rightarrow \mathrm{q}$.
Its contra positive is given by $\neg \mathrm{q} \rightarrow \neg \mathrm{p}$
That is "If I don't get wet then it is not raining"

## Write the contra positive of the conditional statement: "If you obey traffic rules, then you will not be fined.

Let p: you obey traffic rules and q : you will be fined
Given $\mathrm{p} \rightarrow\rceil \mathrm{q}$.
Its contra positive is given by $\mathrm{q} \rightarrow\rceil \mathrm{p}$.
That is "you will be fined only if you won't obey traffic rules"

## Universal quantification

The Universal quantification of a predicate formula $P(x)$ is the proposition, denoted by $\forall x P(x)$ that is true if $P($ a $)$ is true for all subject a.

## Existential quantification

The Existential quantification of a predicate formula $P(x)$ is the proposition, denoted by $\exists x P(x)$ that is true if $P(\mathrm{a})$ is true for some subject a.
Rewrite the following using quantifiers "Every student in the class studied calculus".
Let $P(x): x$ is a student and
$Q(x): x$ studied calculus

$$
\text { Symbolic form } \forall x(P(x) \rightarrow Q(x))
$$

Write the statement in symbolic form "Some real numbers are rational".
Let $R(x): x$ is a real number and
$Q(x): x$ is rational

$$
\text { Symbolic form: } \exists x(R(x) \wedge Q(x)) .
$$

Write the statement in symbolic form "Some integers are not square of any integers".
Let $I(x)$ : x is an integer and
$\mathrm{S}(\mathrm{x})$ : x is a square of any integer
Symbolic form:

$$
\exists x(I(x) \wedge \neg S(x))
$$

Express in symbolic form, everyone who is healthy can do all kinds of work. Let $P(x): x$ is healthy and $Q(x): x$ do all work
Symbolic form is

$$
\forall x(P(x) \rightarrow Q(x))
$$

## PART - B

1 What is meant by Tautology? Without using truth table, show that $((\boldsymbol{P} \vee \boldsymbol{Q}) \wedge \neg(\neg \boldsymbol{P} \wedge(\neg \boldsymbol{Q} \vee \neg \boldsymbol{R}))) \vee(\neg \boldsymbol{P} \wedge \neg \boldsymbol{Q}) \vee(\neg \boldsymbol{P} \wedge \neg \boldsymbol{R})$ is a tautology.
Solution: A Statement formula which is true always irrespective of the truth values of the individual variables is called a tautology.
Consider $\neg(\neg P \wedge(\neg Q \vee \neg R) \Rightarrow \neg(\neg P \wedge \neg(Q \wedge R) \Rightarrow P \vee(Q \wedge R) \Rightarrow(P \vee Q) \wedge(P \vee R)$
Consider $(\neg P \wedge \neg Q) \vee(\neg P \wedge \neg R) \Rightarrow \neg(P \vee Q) \vee \neg(P \vee R) \Rightarrow \neg((P \vee Q) \wedge(P \vee R))$
Using (1) and (2)

$$
\begin{aligned}
& ((P \vee Q) \wedge(P \vee Q) \wedge(P \vee R)) \vee \neg((P \vee Q) \wedge(P \vee R)) \\
& \Rightarrow[(P \vee Q) \wedge(P \vee R)] \vee \neg[(P \vee Q) \wedge(P \vee R)] \Rightarrow T
\end{aligned}
$$

2 Prove that $(P \vee Q) \wedge(\neg \mathbf{P} \wedge(\neg \mathbf{P} \wedge Q)) \Leftrightarrow(\neg \mathbf{P} \wedge Q)$.

## Solution:

Let $S=(\boldsymbol{P} \vee \boldsymbol{Q}) \wedge(\neg \mathbf{P} \wedge(\neg \mathbf{P} \wedge \boldsymbol{Q})) \Leftrightarrow(\neg \mathbf{P} \wedge \boldsymbol{Q})$
$(P \vee Q) \wedge(\neg \mathrm{P} \wedge(\neg \mathrm{P} \wedge Q) \Rightarrow((P \vee Q) \wedge(\neg \mathrm{P} \wedge Q))$
$\Rightarrow(P \wedge \neg \mathrm{P} \wedge Q) \vee(\mathrm{Q} \wedge \mathrm{Q} \wedge \neg \mathrm{P})$
$\Rightarrow(\mathrm{F} \wedge Q) \vee(\mathrm{Q} \wedge \neg \mathrm{P})$
$\Rightarrow(\mathrm{F}) \vee(\mathrm{Q} \wedge \neg \mathrm{P})$
$\Rightarrow(\mathrm{Q} \wedge \neg \mathrm{P})$
3 Prove that $(P \rightarrow Q) \wedge(R \rightarrow Q) \Leftrightarrow(P \vee R) \rightarrow Q$.
Solution:

| $(P \rightarrow Q) \wedge(R \rightarrow Q)$ | Reasons |
| :--- | :--- |
| $\Leftrightarrow(\neg P \vee Q) \wedge(\neg R \vee Q)$ | Since $P \rightarrow Q \Leftrightarrow \neg P \vee Q$ |
| $\Leftrightarrow(\neg P \wedge \neg R) \vee Q)$ | Distribution law |
| $\Leftrightarrow \neg(P \vee R) \vee Q$ | De morgan's law |
| $\Leftrightarrow$ | since $P \rightarrow Q \Leftrightarrow \neg P \vee Q$ |

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

## Solution:

Let

$$
\begin{aligned}
& S \Leftrightarrow(\neg P \rightarrow R) \wedge(Q \leftrightarrow P) \\
& \Leftrightarrow(\neg(\neg P) \vee R) \wedge((Q \rightarrow P) \wedge(P \rightarrow Q)) \\
& \Leftrightarrow(P \vee R) \wedge(\neg Q \vee P) \wedge(\neg P \vee Q) \\
& \Leftrightarrow[(P \vee R) \vee F] \wedge[(\neg Q \vee P) \vee F] \wedge[(\neg P \vee Q) \vee F] \\
& \Leftrightarrow[(P \vee R) \vee(Q \wedge \neg Q) \wedge[(\neg Q \vee P) \vee(R \wedge \neg R)] \wedge[(\neg P \vee Q) \vee(R \wedge \neg R)] \\
& \Leftrightarrow(P \vee R \vee Q) \wedge(P \vee R \vee \neg Q) \wedge(\neg Q \vee P \vee R) \wedge(\neg Q \vee P \vee \neg R) \wedge \\
&(\neg P \vee Q \vee R) \wedge(\neg P \vee Q \vee \neg R) \\
& S \Leftrightarrow(P \vee R \vee Q) \wedge(P \vee R \vee \neg Q) \wedge(P \vee \neg Q \vee \neg R) \wedge(\neg P \vee Q \vee R) \wedge(\neg P \vee Q \vee \neg R)
\end{aligned}
$$

(PCNF)
$\neg S \Leftrightarrow$ The remaining maxterms of $\mathrm{P}, \mathrm{Q}$ and R .
$\therefore \neg S \Leftrightarrow(P \vee Q \vee \neg R) \wedge(\neg P \vee \neg Q \vee R) \wedge(\neg P \vee \neg Q \vee \neg R)$.
$\neg \neg(S) \Leftrightarrow$ Apply duality principle to $\neg S$
$S \Leftrightarrow(\neg P \wedge \neg Q \wedge R) \vee(P \wedge Q \wedge \neg R) \vee(P \wedge Q \wedge R) \quad(P D N F)$
5 Obtain PCNF and PDNF of the formula $(P \wedge Q) \vee(\neg P \wedge R) \vee(Q \wedge R)$ ] Solution:
Let $\mathrm{S}=(P \wedge Q) \vee(\neg P \wedge R) \vee(Q \wedge R)$
$=(P \wedge Q \wedge T) \vee(\neg P \wedge R \wedge T) \vee(Q \wedge R \wedge T)$
$=(P \wedge Q \wedge(R \vee \neg R)) \vee(\neg P \wedge R \wedge(Q \vee \neg Q)) \vee(Q \wedge R \wedge(P \vee \neg P))$
$=(P \wedge Q \wedge R) \vee(\neg P \wedge Q \wedge R) \vee(P \wedge Q \wedge \neg R) \vee(\neg P \wedge \neg Q \wedge R)$
Which is PDNF of S
To find PCNF
The PDNF of $\neg S$ is $(P \wedge \neg Q \wedge R) \vee(P \wedge \neg Q \wedge \neg R) \vee(\neg P \wedge Q \wedge R) \vee(\neg P \wedge \neg Q \wedge \neg R)$ $\neg(\neg S)=S=(\neg P \vee Q \vee \neg R) \wedge(\neg P \vee Q \vee R) \wedge(P \vee \neg Q \vee \neg R) \wedge(P \vee Q \vee R)$
Which is PCNF of $S$
6 Obtain PCNF and PDNF of the formula $(P \rightarrow(Q \wedge R)) \wedge(\neg P \rightarrow(\neg Q \wedge \neg R))$ ] Solution:

```
Let \(S=(\boldsymbol{P} \rightarrow(\boldsymbol{Q} \wedge \boldsymbol{R})) \wedge(\neg \boldsymbol{P} \rightarrow(\neg \boldsymbol{Q} \wedge \neg \boldsymbol{R}))\)
\(S=(\neg P \vee Q \vee \neg R) \wedge(\neg P \vee Q \vee R) \wedge(P \vee \neg Q \vee \neg R) \wedge(P \vee \neg Q \vee R)\)
\(\wedge(P \vee Q \vee \neg R) \wedge(\neg P \vee \neg Q \vee R)\)
```

Which is PCNF of S
To find PDNF

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

Which is PDNF of $S$
7 Show that $R \rightarrow S$ can be derived from the premises $P \rightarrow(Q \rightarrow S), \neg R \vee P$ \& $Q$ Solution:

| Steps | Premises | Rule | Reason |
| :--- | :--- | :--- | :--- |
| 1 | $R$ | Assumed <br> premises | Premises |
| 2 | $\neg R \vee P$ | Rule P |  |
| 3 | $R \rightarrow P$ | Rule T | $P \rightarrow Q \Leftrightarrow \neg P \vee Q$ |
| 4 | $P$ | Rule T | $\mathrm{P}, P \rightarrow R \Rightarrow R$ |
| 5 | $P \rightarrow(Q \rightarrow S)$ | Rule P |  |
| 6 | $Q \rightarrow S$ | Rule T | $\mathrm{P}, P \rightarrow R \Rightarrow R$ |
| 7 | $Q$ | Rule P |  |
| 8 | $S$ | Rule T | $\mathrm{P}, P \rightarrow R \Rightarrow R$ |
| 9 | $R \rightarrow S$ | Rule CP |  |

8 Show that the following sets of premises are inconsistent $P \rightarrow Q, P \rightarrow R$, $Q \rightarrow \neg R, P$.
Solution:

| Step | Derivation | Rule |
| :--- | :--- | :--- |
| 1. | $P \rightarrow Q$ | Rule P |
| 2. | $Q \rightarrow \neg R$ | Rule P |
| 3. | $P \rightarrow \neg R$ | from (1) \& (2) Rule T |
| 4. | $P$ | Rule P |
| 5. | $\neg R$ | Rule P |
| 6. | $P \rightarrow R$ | Rule P |
| 7. | $\neg P$ | Rule T from (5) \& (6) |
| 8. | $P \wedge \neg P$ | Rule T |

9 Show the premises $R \rightarrow \neg Q, R \vee S, S \rightarrow \neg Q, P \rightarrow Q, P$ are inconsistent.

## Solution:

| Step | Derivation | Rule |
| :--- | :--- | :--- |
| 1. | $P$ | Rule P |
| 2. | $P \rightarrow Q$ | Rule P |
| 3. | $Q$ | from 1,2 by rule T |
| 4. | $S \rightarrow \neg Q$ | Rule P |


| 5. | $Q \rightarrow \neg S$ | from 4 byequivalences |
| :--- | :--- | :--- |
| 6. | $\neg S$ | from 3 and 5 |
| 7. | $R \vee S$ | Rule P |
| 8. | $\neg R \rightarrow S$ | from 7 |
| 9. | $\neg S \rightarrow R$ | from 8 |
| 10. | $R$ | from 6 and 9 |
| 11. | $R \rightarrow \neg Q$ | Rule P |
| 12. | $\neg Q$ | from 10 and 11 |
| 13. | $Q \wedge \neg Q$ | from 3 and 12 |

10 Prove that the premises $P \rightarrow Q, Q \rightarrow R, R \rightarrow S, S \rightarrow \neg R$ and $P \wedge S$ are inconsistent.
[Nov/Dec -2017]

## Solution:

| Step <br> s | Premises | Rule | Reason |
| :--- | :--- | :--- | :--- |
| 1 | $P \rightarrow Q$ | P | Assumed Premises |
| 2 | $Q \rightarrow R$ | P | Assumed Premises |
| 3 | $P \rightarrow R$ | T | $P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$ |
| 4 | $\boldsymbol{R} \rightarrow \boldsymbol{S}$ | P | Assumed Premises |
| 5 | $P \rightarrow S$ | T | $P \rightarrow R, \boldsymbol{R} \rightarrow \boldsymbol{S} \Rightarrow \boldsymbol{P} \rightarrow \boldsymbol{S}$ |
| 6 | $S \rightarrow \neg R$ | P | Assumed Premises |
| 7 | $P \rightarrow \neg R$ | T | $P \rightarrow S, S \rightarrow \neg R \Rightarrow P \rightarrow \neg R$ |
| 8 | $\neg P \vee \neg R$ | T | $P \rightarrow Q \Rightarrow \neg P \vee Q$ |
| 9 | $\neg(P \wedge R)$ | T | Demorgan's Law |
| 10 | $(P \wedge S)$ | P | Assumed Premises |
| 11 | P | T | $(P \wedge S) \Rightarrow P$ |
| 12 | R | $\mathrm{T}(8,3)$ | $\mathrm{P}, P \rightarrow R \Rightarrow R$ |
| 13 | $(P \wedge R)$ | $\mathrm{T}(11,12)$ | $P, R \Rightarrow P \wedge R$ |
| 14 | $(P \wedge R) \wedge \neg(P \wedge R)$ | $\mathrm{T}(9,13)$ | $P, Q \Rightarrow P \wedge Q$ |

## 11 Show that the following premises are inconsistent.

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

## Solution:

E: Raja Kumar misses many classes
S: Raja Kumar fails high school
A: Raja Kumar reads lot of books
H: Raja Kumar is uneducated
Statement:
(1) $E \rightarrow S$
(2) $S \rightarrow H$
(3) $A \rightarrow \sim H$
(4) $E \wedge A$

Premises are : $E \rightarrow S, S \rightarrow H, \quad A \rightarrow \sim H, E \wedge A$

| 1) $E \rightarrow S$ | Rule P |
| :--- | :--- |
| 2) $S \rightarrow H$ | Rule P |
| 3) $\mathrm{E} \rightarrow \mathrm{H}$ | Rule T, 1,2 |
| 4) $A \rightarrow \sim H$ | Rule P |
| 5) $\mathrm{H} \rightarrow \sim \mathrm{A}$ | Rule T,4 |
| 6) $\mathrm{E} \rightarrow \sim \mathrm{A}$ | Rule T,3,5 |
| 7) $\sim E \vee \sim A$ | Rule T,6 |
| 8) $\sim(\mathrm{E} \wedge \mathrm{A})$ | Rule T,7 |
| 9) $\mathrm{E} \wedge \mathrm{A}$ | Rule P |
| 10) $(\mathrm{E} \wedge \mathrm{A}) \wedge \sim(\mathrm{E} \wedge \mathrm{A})$ | Rule T,8,9 |

Which is nothing but false
Therefore given set of premises are inconsistent.
12 Show that $(R \vee S)$ is a valid conclusion from the premises $(C \vee D)$, $(C \vee D) \rightarrow \neg H, \neg H \rightarrow(A \wedge \neg B),(A \wedge \neg B) \rightarrow(R \vee S)$.
Solution:

| Step | Derivation | Rule |
| :--- | :--- | :--- |
| $(1)$ | $(C \vee D) \rightarrow \neg H$ | P |
| $(2)$ | $\neg H \rightarrow(A \wedge \neg B)$ | P |
| $(3)$ | $(C \vee D) \rightarrow(A \wedge \neg B)$ | $\mathrm{T},(1),(2)$ and hypothetical syllogism |
| $(4)$ | $(A \wedge \neg B) \rightarrow(R \vee S)$ | P |
| $(5)$ | $(C \vee D) \rightarrow(R \vee S)$ | $\mathrm{T},(3),(4)$ and hypothetical syllogism |
| $(6)$ | $(C \vee D)$ | P |
| $(7)$ | $(R \vee S)$ | $\mathrm{T},(5),(6)$ and modus ponens |
|  |  |  |

13 Show that the hypotheses, "It is not sunny this afternoon and it is colder than yesterday," "We will go swimming only if it is sunny," "If we do not go swimming then we will take a canoe trip," and "If we take a canoe trip, then we will be home by sunset "lead to the conclusion "we will be home by sunset".[Nov/Dec-2013]

## Solution:

p - It is sunny this afternoon
q - It is colder than yesterday
r- we will go swimming
s - we will take a canoe trip \& t- we will be home by sunset
The given premises are $\neg p \wedge q, r \rightarrow p, \neg r \rightarrow s \& s \rightarrow t$

| Step | Premises | Rule | Reason |
| :--- | :--- | :--- | :--- |
| 1 | $\neg p \wedge q$ | Rule P |  |
| 2 | $\neg p$ | Rule T | $\mathrm{P} \wedge \mathrm{Q}=\mathrm{P}$ |
| 3 | $r \rightarrow p$ | Rule P |  |
| 4 | $\neg r$ | Rule T | $\neg P, Q \rightarrow P \Rightarrow \neg Q$ |
| 5 | $\neg r \rightarrow s$ | Rule P |  |
| 6 | $s$ | Rule T | $\mathrm{P}, P \rightarrow R \Rightarrow R$ |
| 7 | $s \rightarrow t$ | Rule P |  |
| 8 | $t$ | Rule T | $\mathrm{P}, P \rightarrow R \Rightarrow R$ |

Page No: 10

14 Show that "it rained' is a conclusion obtained from the statements. ' if it does not rain or if there is no traffic dislocation, then the sports day will be held and the cultural programme will go on " " if the sports day is held, the trophy will be awarded" and " the trophy was not awarded"
Solution: The given premises are $(\neg p \vee \neg q) \rightarrow(\mathrm{r} \wedge \mathrm{s}), r \rightarrow t, \neg t$
The conclusion is $p$

| Step | Premises | Rule | Reason |
| :--- | :--- | :--- | :--- |
| 1 | $(\neg p \vee \neg q) \rightarrow(r \wedge s)$ | Rule P |  |
| 2 | $(\neg p \rightarrow(r \wedge s)) \wedge(\neg q \rightarrow(r \wedge s))$ Rule T, 1 |  |  |
| 3 | $\neg p \rightarrow(r \wedge s)$ | Rule T,2 | $\mathrm{P} \wedge \mathrm{Q}=\mathrm{P}$ |
| 4 | $\neg(r \wedge s) \rightarrow p$ | Rule T,3 | $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$ |
| 5 | $r \rightarrow t$ | Rule P |  |
| 6 | $\neg t$ | Rule P | $\mathrm{P}, P \rightarrow R \Rightarrow R$ |
| 7 | $\neg r$ | Rule <br> T,5,6 | $\neg P, Q \rightarrow P \Rightarrow \neg Q$ |
| 8 | $\neg s \vee \neg r$ | Rule T,7 | $\mathrm{P}, P \rightarrow R \Rightarrow R$ |
| 9 | $\neg(r \wedge s)$ | Rule T,, 8 |  |
| 10 | p | Rule T,, <br> 3,9 | $\neg P, Q \rightarrow P \Rightarrow \neg Q$ |

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

## Solution:

| Step | Derivation | Rule |
| :--- | :--- | :--- |
| 1. | $(\exists x)(P(x) \wedge Q(x))$ | P |
| 2. | $P(y) \wedge Q(y)$ | $\mathrm{ES},(1)$ |
| 3. | $P(y)$ | $\mathrm{T},(2), P \wedge Q \Rightarrow P$ |
| 4. | $Q(y)$ | $\mathrm{T},(2), P \wedge Q \Rightarrow Q$ |
| 5. | $(\exists x) P(x)$ | EG, (3) |
| 6. | $(\exists x) Q(x)$ | EG, (4) |
| 7. | $(\exists x) P(x) \wedge(\exists x) Q(x)$ | T, (4), (5), DeMorgans law |

16 Show that the premises "A student in this class has not read the book" and "Everyone in this class passed the first examination" imply the conclusion "Someone who passed the first examination has not read the book". [Nov/Dec-2018]

## Solution:

$\mathrm{S}(\mathrm{x})$ : x is a student in the class
$\mathrm{R}(\mathrm{x})$ : x reads books
$\mathrm{F}(\mathrm{x})$ : x is passed the first examination
A student in this class has not read the book
$(\exists x)(s(x) \wedge \neg R(x))$
Every one in this class passed the first exam
$(\forall x) F(x)$
Conclusion:
Someone who passed the first examination has not read the book $(\exists x)(F(x) \wedge \neg R(x))$

| Steps | Premises | Rule | Reason |
| :--- | :--- | :--- | :--- |
| 1 | $(\exists x)(s(x) \wedge \neg R(x))$ | P | Premises |
| 2 | $(s(y) \wedge \neg R(y))$ | E S |  |
| 3 | $\neg R(y)$ | T | $\mathrm{P} \wedge \mathrm{Q}=\mathrm{Q}$ |
| 4 | $(\forall x) F(x)$ | P |  |
| 5 | $F(y)$ | US |  |
| 6 | $(F(y) \wedge \neg R(y))$ | T | $\mathrm{P}, \mathrm{Q}=\mathrm{P} \wedge \mathrm{Q}$ |
| 7 | $(\exists x)(F(x) \wedge \neg R(x))$ | EG |  |

17 Show that $\forall x(p(x) \vee q(x)) \Rightarrow \forall x p(x) \vee \exists x q(x)$ using the indirect method Solution:

| Steps | Premises | Rule | Reason |
| :--- | :--- | :--- | :--- |
| 1 | $\neg[\forall x p(x) \vee \exists x q(x)$ | Rule P | Assumed <br> Premises |
| 2 | $(\exists x) \neg p(x) \wedge(x) \neg q(x)$ | Rule T | Demorgan, s <br> Law |
| 3 | $\exists x \neg p(x)$ | Rule T | $\mathrm{P} \wedge \mathrm{Q}=\mathrm{P}$ |
| 4 | $(x) \neg q(x)$ | Rule T | $\mathrm{P} \wedge \mathrm{Q}=\mathrm{Q}$ |
| 5 | $\neg p(y)$ | Rule T | $\mathrm{E} . \mathrm{S}$ |
| 6 | $\neg q(y)$ | Rule T | U S |
| 7 | $\neg p(y) \wedge \neg q(y)$ | Rule T | $\mathrm{P}, \mathrm{Q}=\mathrm{P} \wedge \mathrm{Q}$ |


| 8 | $\neg(p(y) \vee q(y))$ | Rule T | Demorgan, <br> Law |
| :--- | :--- | :--- | :--- |
| 9 | $(x)(p(x) \vee q(x))$ | Rule P | G P |
| 10 | $(p(y) \vee q(y))$ | Rule T | U S |
| 11 | $(p(y) \vee q(y)) \wedge \neg(p(y) \vee q(y))$ | Rule T | $\mathrm{P}, \mathrm{Q}=\mathrm{P} \wedge \mathrm{Q}$ |

18 Using indirect method of Proof to show the $(\exists z) Q(z)$ is not valid conclusion from the premises $(x)(P(x) \rightarrow Q(x))$ and $(\exists y) Q(y)$.

## Solution:

we use the indirect method, by assuming that the conclusion $(\exists z) Q(z)$ is false.

| Step | Derivation | Rule |
| :--- | :--- | :--- |
| 1 | $\neg(\exists z) Q(z)$ | P (assumed) |
| 2 | $(\forall z) \neg Q(z)$ | $\mathrm{T},(1)$ |
| 3 | $(\exists y) \rightarrow P(y)$ | P |
| 4 | $P(a)$ | $\mathrm{ES},(3)$ |
| 5 | $7 Q(a)$ | $\mathrm{US},(2)$ |
| 6 | $P(a) \wedge \neg Q(a)$ | $\mathrm{T},(4),(5)$ |
| 7 | $\neg(P(a) \rightarrow Q(a))$ | $\mathrm{T},(6)$ |
| 8 | $\forall x(P(x) \rightarrow Q(x))$ | P |
| 9 | $P(a) \rightarrow Q(a)$ | $\mathrm{US},(8)$ |
| 10 | $(P(a) \rightarrow Q(a)) \wedge \neg(P(a) \rightarrow Q(a)) \mathrm{T},(7),(9)$, contradiction |  |

19 Show the premises "One student in this class knows how to write programs in JAVA" and "Everyone who knows how to write programs in JAVA can get a high paying job" imply the conclusion "someone in this class can get a high paying job".
Solution:
$C(x): x$ is in this class
$J(x): x$ knows JAVA programming
$H(x): x$ can get a high paying job
The premises are $\exists x(C(x) \wedge J(x))$ and $\forall x(J(x) \rightarrow H(x))$.
The conclusion is $\exists x(C(x) \wedge H(x))$

| Step | Derivation | Rule |
| :--- | :--- | :--- |
| 1 | $\exists x(C(x) \wedge J(x))$ | P |
| 2 | $C(a) \wedge J(a)$ | ES and (1) |
| 3 | $C(a)$ | From 2 |
| 4 | $J(a)$ | From 2 |
| 5 | $\forall x(J(x) \rightarrow H(x))$ | P |
| 6 | $J(a) \rightarrow H(a)$ | US and (5) |
| 7 | $H(a)$ | From (4) and (6) |
| 8 | $C(a) \wedge H(a)$ | From (3) and (7) |
| 9 | $\exists x(C(x) \wedge H(x))$ | EG and (8) |

20. Prove that $\sqrt{2}$ is irrational by giving a proof using contradiction. [May/June-2016]

## Solution:

Let $P: \sqrt{2}$ is irrational.
Assume $\sim \mathrm{P}$ is true, then $\sqrt{2}$ is rational, which leads to a contradiction.
By our assumption is $\sqrt{2}=\frac{a}{b}$,
where $a_{2}$ and $b$ have no common factors
$\Rightarrow 2=\frac{a^{2}}{b^{2}} \Rightarrow 2 b^{2}=a \stackrel{2}{\Rightarrow} a^{2}$ is even.
$\Rightarrow a=2 \mathrm{c}$
$2 b^{2}=4 c^{2} \Rightarrow b^{2}=2 c^{2} \Rightarrow b^{2}$ is even $\Rightarrow b$ is even as well.
$\Rightarrow a$ and $b$ have common factor 2 (since a and b are even)
But it contradicts (1)
This is a contradiction.
Hence $\sim \mathrm{P}$ is false.
Thus P: $\sqrt{2}$ is irrational is true.

# MA8351 - Discrete Mathematics <br> UNIT II - COMBINATORICS 

## Class Notes

## Principle of Mathematical Induction:

Let $P(n)$ denote a mathematical statement that involves one or more occurrences of the positive integer $n$ then we complete two steps:

1. Base step: $P(1)$ is true
2. Inductive step: In this step we prove that $P(k+1)$ is true on the assumption that $P(k)$ is true.

## Principle of Strong Induction:

Given a mathematical statement $P(n)$ that involves one or more occurrences of the positive integer $n$ and if

1. $P(1)$ is true
2. Whenever $P(1), P(2) \ldots P(\mathrm{k})$ are true, $P(k+1)$ is also true, then $P(n)$ is true for all $n \in \mathrm{Z}^{+}$.

1 Use mathematical induction to show that $n^{3}-n$ is divisible by 3 for $n \in$ $\boldsymbol{Z}^{+}$.

Solution: Let $P(n): n^{3}-n$ is divisible by 3 .
Step 1: $P(1): 1^{3}-1=0$ is divisible by 3. $P(1)$ is true.
Step 2: Assume $P(k)=k^{3}-k$ is divisible by 3 . That is $P(k)$ is true.
Claim: To prove $P(k+1)$ is true.
Consider $P(k+1)=(k+1)^{3}-(k+1)$

$$
=k^{3}+3 k^{2}+3 k+1-k-1
$$

$$
=\left(k^{3}-k\right)+3\left(k^{2}+k\right)
$$

Since $P(k)=k^{3}-k$ is divisible by 3 and $3\left(k^{2}+k\right)$ is divisible by 3 .
$\Rightarrow P(k+1)$ is divisible by 3 .
$\Rightarrow P(k+1)$ is true.
Hence by Principle of mathematical induction $n^{3}-n$ is divisible by 3 .

## 2 Use mathematical induction to show that

$$
\sum_{r=0}^{n} 3^{r}=\frac{3^{n+1}-1}{2}
$$

## Solution:

Let $P(n): 3^{0}+3^{1}+3^{2}+\cdots+3^{n}=\frac{3^{n+1}-1}{2}$
Step 1: $P(0): 3^{0}=\frac{3^{0+1}-1}{2}=\frac{2}{2}=1 \quad \therefore P(0)$ is true.
Step 2:
Assume that $P(k)$ is true.
$P(k): 3^{0}+3^{1}+3^{2}+\cdots+3^{k}=\frac{3^{k+1}-1}{2}$ is true.
Claim: To prove $P(k+1)$ is true.
Consider

$$
\begin{aligned}
P(k+1)=\left(3^{0}\right. & \left.+3^{1}+3^{2}+\cdots+3^{k}\right)+3^{k+1} \\
& =\frac{3^{k+1}-1}{2}+3^{k+1} \\
& =\frac{3^{k+1}-1+2\left(3^{k+1}\right)}{2}
\end{aligned}
$$

$$
\begin{array}{r}
=\frac{3\left(3^{k+1}\right)-1}{2} \\
=\frac{3^{k+2}-1}{2} \\
=\frac{3^{(k+1)+1}-1}{2}
\end{array}
$$

$\therefore P(k+1)$ is true. By the principle of mathematical induction $\sum_{r=0}^{n} 3^{r}=\frac{3^{n+1}-1}{2}$ is true.

3 Using mathematical induction prove that if $\boldsymbol{n}$ is a positive integer, then 133 divides $11^{n+1}+12^{2 n-1}$.

## Solution:

Let $P(n): 11^{n+1}+12^{2 n-1}$ is divisible by 133 .

## Base Step:

To prove $P(1)$ is true, $\mathrm{P}(1): 11^{2}+12^{1}=121+12=133$, which is divisible by 133.
$\therefore P(1)$ is true.

## Inductive Step:

Assume that $P(k)$ is true. That $11^{k+1}+12^{2 k-1}$ is divisible by 133.
i.e., $11^{k+1}+12^{2 k-1}=133 m$ for some integer.

To prove $P(k+1)$ is true.
i.e $\quad 11^{(k+1)+1}+12^{2(k+1)-1}=11^{k+1} \cdot 11+12^{2 k-1} .12^{2}$

$$
\begin{aligned}
& =11^{k+1} \cdot(144-133)+12^{2 k-1} \cdot(144) \\
& =11^{k+1} \cdot(144)+12^{2 k-1} \cdot(144)-11^{k+1} \cdot(133) \\
& =144 \cdot\left[11^{k+1}+12^{2 k-1}\right]-11^{k+1} \cdot(133)
\end{aligned}
$$

$$
\begin{aligned}
& =144 .(133 m)-11^{k+1} .(133) \\
& =133 .\left[144 m-11^{k+1}\right]
\end{aligned}
$$

which is divisible by 133.
Hence $P(k+1)$ is true whenever $P(k)$ is true.
By the principle of mathematical induction $P(n)$ is true for all positive integer $n$.
4 If $H_{n}$ denote harmonic numbers then prove that $H_{n} \geq 1+{ }_{2}^{n}$ using ${ }_{2}$ mathematical induction.

Let $P(n):{ }_{2^{n}} \geq 1+\underset{2}{n}$ where $H \underset{j}{ } \geq 1+{ }_{2}^{1} \pm{ }_{2}^{1} \pm \cdots$
Step 1: $P(1): H_{2}{ }^{1} \geq 1+\frac{1}{2}$ where $H_{2}=1+\frac{1}{2}$
$P(1): H_{2}=1+{ }_{2}^{2} \geq 1+{ }_{2}^{1}{ }_{2}$ is true.
Step 2: Assume $\mathrm{P}(\mathrm{k})$ is true.
$P(k): H_{2^{k}} \geq 1+\frac{1}{2}+\cdots+{ }_{2^{k}}^{1} \geq 1+{ }_{2}^{k}$ is true.
Claim: To prove $P(k+1)$ is true.
Consider

$$
\begin{gathered}
P(k+1): H_{2^{k+1}} \geq 1+\frac{1}{2}+\cdots+\frac{1}{2^{k}}+\frac{1}{2^{k+1}} \\
=1+\frac{1}{2}+\cdots+\frac{1}{2^{k}}+\left(\frac{1}{2^{k}+1}+\frac{1}{2^{k}+2}+\cdots+\frac{1}{2^{k}+2^{k}}\right) \\
\geq\left(1+\frac{k}{2}\right)+\left(\frac{1}{2^{k}+1}+\frac{1}{2^{k}+2}+\cdots+\frac{1}{2^{k}+2^{k}}\right) \\
\geq\left(1+\frac{k}{2}\right)+\left(2^{k} \frac{1}{2^{k+1}}\right)
\end{gathered}
$$

$$
\begin{gathered}
\geq\left(1+\frac{k}{2}\right)+\left(2^{k} \frac{1}{2^{k} 2}\right) \\
\geq\left(1+\frac{k}{2}\right)+\frac{1}{2} \\
\geq 1+\left(\frac{k+1}{2}\right)
\end{gathered}
$$

$\Rightarrow P(k+1)$ is true.
By the principle of mathematical induction $H_{2^{n}} \geq 1+\frac{n}{2}$
5 Use mathematical induction to prove the inequality $n<2^{n}$ for all positive integers.

Solution: Let $P(n): n<2^{n}, n=1,2,3 \ldots$
Step 1: $P(1): 1<2^{1}$, which is true.
Step 2: Assume $P(k)$ is true. i.e $k<2^{k}$.
Claim: To prove $P(k+1)$ is true.
$k+1<2^{k}+1<2^{k+1}$.
$\Rightarrow P(k+1)$ is true.
$\therefore P(n)$ is true for all positive integers.
6 Using Mathematical induction prove that $\sum_{i=0}^{n} i^{2}=\frac{n(n+1)(2 n+1)}{6}$

## Solution:

Let $P(n)=\sum_{i=0}^{n} i^{2}=\frac{n(n+1)(2 n+1)}{6}$
To Prove $P(1)$ is true
$P(1)=\frac{1(1+1)(2(1)+1)}{6}=\frac{6}{6}=1$

Let us assume that $P(k)$ is true
$P(k)=\frac{k(k+1)(2 k+1)}{6}$

Now to prove $P(k+1)$ is true.

$$
\begin{aligned}
& \text { ie } P(k+1)=\frac{(k+1)(k+2)(2 k+3)}{6} \\
& \begin{aligned}
P(k+1) & =1^{2}+2^{2}+\ldots+k^{2}+(k+1)^{2} \\
& =\frac{k(k+1)(2 k+1)}{6}+(k+1)^{2}
\end{aligned} \\
& \cdot P(k+1)=\frac{(k+1)(k+2)(2 k+3)}{6}
\end{aligned}
$$

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

7 If $\boldsymbol{n}$ is a positive integer, then show that
$\frac{1}{1.3}+\frac{1}{3.5}+\frac{1}{5.7}+\ldots+\frac{1}{(2 n-1)(2 n+1)}=\frac{n}{2 n+1} \forall n \geq 1$.

## Solution:

Let $P(n)=\frac{1}{1.3}+\frac{1}{3.5}+\frac{1}{5.7}+\ldots+\frac{1}{(2 n-1)(2 n+1)}=\frac{n}{2 n+1}$

Wehave toprove that $P(n)$ is true $\forall n \geq 1$.

BaseStep : Put $n=1$.
L.H.S
$\therefore P(1)=\frac{1}{(2(1)-1)(2(1)+1)}=\frac{1}{1.3}=\frac{1}{3}$
R.H.S
$\rightarrow \frac{1}{2(1)+1}-\frac{1}{3}$
$\Rightarrow$ LHS $=$ RHS
$\therefore \mathrm{P}(1)$ is true.
Inductive Step: Assume $\mathrm{P}(\mathrm{k})$ is true, $\mathrm{k}>1$.
$\Rightarrow \frac{1}{1.3}+\frac{1}{3.5}+\frac{1}{5.7}+\ldots+\frac{1}{(2 k-1)(2 k+1)}=\frac{k}{2 k+1}$ is true.
To prove $\mathrm{P}(\mathrm{k}+1)$ is true.
i.e $\frac{1}{1.3}+\frac{1}{3.5}+\frac{1}{5.7}+\ldots+\frac{1}{(2 k-1)(2 k+1)}+\frac{1}{(2(k+1)-1)(2(k+1)+1)}=\frac{k+1}{2 k+3}$ is true.
L.H.S $=\frac{1}{1.3}+\frac{1}{3.5}+\frac{1}{5.7}+\ldots+\frac{1}{(2 k-1)(2 k+1)}+\frac{1}{(2(k+1)-1)(2(k+1)+1)}$
$=\frac{k}{2 k+1}+\frac{1}{(2(k+1)-1)(2(k+1)+1)}$
$=\frac{k}{2 k+1}+\frac{1}{(2 k+1)(2 k+3)}$
$=\frac{k(2 k+3)+1}{(2 k+1)(2 k+3)}$

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

$\therefore P(k+1)$ is true.
Thus $P(k)$ is ture $\Rightarrow P(k+1)$ is true.
8 Prove by mathematical induction that $6^{n+2}+7^{2 n+1}$ is divisible by 43 for each positive integer $n$.

## Solution:

Let $P(1)$ : Inductive step: for $n=1$,

$$
6^{1+2}+7^{2+1}=559 \text {, which is divisible by } 43
$$

So $P(1)$ is true.

Assume $P(k)$ is true.
$6^{k+2}+7^{2 k+1}$ is divisible by 43.
i.e $6^{k+2}+7^{2 k+1}=43 m$ for some integer $m$.

To prove $P(k+1)$ is true.
That is to prove $6^{(k+1)+2}+7^{2(k+1)+1}$ is divisible by 43 .
Now

$$
\begin{aligned}
6^{k+3}+7^{2 k+3} & =6^{k+3}+7^{2 k+1} \cdot 7^{2} \\
= & 6\left(6^{k+2}+7^{2 k+1}\right)+43.7^{2 k+1} \\
& =6.43 m+43.7^{2 k+1} \\
& =43\left(6 m+7^{2 k+1}\right)
\end{aligned}
$$

This is divisible by 43.
So $P(k+1)$ is true. By Mathematical Induction, $P(n)$ is true for all integer $n$.
9 Using mathematical induction, show that for all positive integers $n$, $3^{2 n+1}+2^{n+2}$ is divisible by 7 .

## Solution:

Let $P(n): 3^{2 n+1}+2^{n+2}$ is divisible by 7 .

## Base Step:

To prove $P(1)$ is true,
$3^{2+1}+2^{1+2}=3^{3}+2^{3}=27+8=35=(5)(7)$, which is divisible by 7.
$\therefore P(1)$ is true.

## Inductive Step:

Assume that $P(k)$ is true. That is $3^{2 k+1}+2^{k+2}$ is divisible by 7 .

$$
\text { i.e., } 3^{2 k+1}+2^{k+2}=7 m \text { for some integer. }
$$

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

$$
\text { i.e., } \begin{aligned}
3^{2(k+1)+1}+2^{(k+1)+2} & =3^{2 k+3}+2^{k+3} \\
& =3^{2 k+1}\left(3^{2}\right)+2^{k+2}(2) \\
& =3^{2 k+1}(9)+2^{k+2}(2) \\
& =2\left[3^{2 k+1}+2^{k+2}\right]+(7) 3^{2 k+1} \\
& =2(7)(m)+(7) 3^{2 k+1}
\end{aligned}
$$

which is divisible by 7 .
Hence $P(k+1)$ is true whenever $P(k)$ is true.
By the principle of mathematical induction $P(n)$ is true for all positive integer $n$.

10 Prove that Prove that $2^{n}<n!, \forall n \geq 4$

## Solution:

Let $P(n)$ be the proposition (or inequality)

$$
2^{n}<n!\forall n \geq 4
$$

We have to prove $P(n)$ is true $\forall n \geq 4$
Basis Step: Here $\mathrm{n}_{0}=4$
$\therefore P(4)$ is $2^{2}<41 \Rightarrow 4<24$, which is true.
$\therefore P(4)$ is true.

Inductive Step: Assume $P(k)$ is true, $k>1$.

$$
\Rightarrow 2^{k}<k!\text { is true. }
$$

## To prove $P(k+1)$ is true.

i.e. To prove $2^{k+1}<(k+1)$ ! is true.

Now $2^{k+1}=2^{k} .2<k!2$

Since $k>1, k+1>2$.
$\therefore 2^{k+1}<k!.(k+1)$
$=>2^{k+1}<(k+1)!$
$\therefore P(k+1)$ is true.
Thus $P(k)$ is true $=P(k+1)$ is true.
Hence by first principle of induction $P(n)$ is true for $n \geq 4$.
$\Rightarrow 2^{n}<n!\forall n \geq 4$.

11 Prove by induction "every positive integer $n \geq 2$ is either a prime or can be written as a product of prime".

Solution: Let $P(n)$ denote the proposition "every integer $n \geq 2$ is either a prime or a product of primes". We have to prove $P(n)$ is true $\forall n \geq 2$.

Base Step: Put $n=2 . \therefore P(2)$ is 2 , which is a prime.
Thus $P(2)$ is true.
Inductive Step: Assume the proposition is true for all integers up to $k>2$. i.e $P(3), P(4) \ldots P(k)$ are true.

To prove $P(k+1)$ is true.
i. e to prove $(k+1)$ is either a prime or product of primes.

If $(k+1)$ is a prime, then we are through.
If $(k+1)$ is not a prime, it is a composite number and so it is a product of two positive integers $x$ and $y$, where $1<x, y<k+1$.

Since $x, y \leq k$, by induction hypothesis $x$ and $y$ are primes or product of primes.
$\therefore k+1=x . y$ is a product of two or more primes.
$\therefore P(k+1)$ is true.
Thus $P(3), P(4) \ldots P(k)$ are true $\Rightarrow P(k+1)$ is true.
Hence $P(n)$ is true for all $n \geq 2$.

## Pigeonhole Principle:

If $n$ pigeons are assigned to $m$ pigeon holes and $m<n$, then at least one pigeonhole contains two or more pigeons.

## The Extended Pigeonhole Principle:

If $n$ pigeons are assigned to $m$ pigeon holes then one of the pigeonholes must contain at least $\left\lfloor\frac{n-1}{m}\right\rfloor 1$ pigeons.

Note: [5.3] $=5,[-1.7]=-2$
12 Prove that in any group of six people there must be at least three mutual friends or three mutual enemies.

## Proof:

Let the six people be A, B, C, D, E and F. Fix A. The remaining five people can accommodate into two groups namely (1) Friends of A and (2) Enemies of A

Now by generalized Pigeonhole principle, at least one of the group must contain $\left(\frac{5-1}{2}\right)^{+1=3}$ people.

Let the friend of A contain 3 people. Let it be B, C, D.
Case (1): If any two of these three people (B, C, D) are friends, then these two
together with A form three mutual friends.
Case (2): If no two of these three people are friends, then these three people (B, $\mathrm{C}, \mathrm{D})$ are mutual enemies.

In either case, we get the required conclusion.
If the group of enemies of A contains three people, by the above similar argument, we get the required conclusion.

13 What is the maximum number of students required in a discrete mathematics class to be sure that at least six will receive the same grade of there are five possible grade $A, B, C, D$ and $F$ ?

## Solution:

Number of grads $=$ Number of Pigeonholes $=5=\mathrm{n}$
Let k be the number of students (Pigeon) in discrete mathematics class.
$\therefore \mathrm{k}+1=6 \Rightarrow \mathrm{k}=5$
$\therefore$ Total number of students $=k n+1=(5 \times 5)+1=26$ students.

## Permutations and Combinations:

The process of selecting things is called combination.
$n C_{r}=\frac{n!}{(n-r)!r!}$ (selecting $r$ things out of $n$ possible cases)
The process of arranging things is called permutation.

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

14 Find the number of distinct permutation that can be formed from all the letters of the word (i) RADAR (ii) UNUSUAL

## Solution:

(i) The word RADAR contains 5 letters of which 2 A's and 2 R's are there.
$\therefore$ The number of distinct permutations that can be formed from all letters of each word RADAR is $\frac{51}{2!\times 2!}{ }^{120}=30$
(ii) The word UNUSUAL contains 7 letters of which 3 U's are there.
$\therefore$ Required number of distinct permutations $=\frac{7!}{3!}=\frac{7 \times 6 \times 5 \times 4 \times 3}{3}=840$

15 There are six men and five women in a room. Find the number of ways four persons can be drawn from the room.
(1) They can be male or female
(2) Two must be men and two women
(3) They must all be of same sex

## Solution :

(i) Four persons can be drawn from $11(6+5)$ persons is ${ }^{11} C_{4}=330$ ways
(ii) Two men can be selected in ${ }^{6} C_{2}$ ways and two women can be selected in ${ }^{5} C \cdot{ }_{2}$ Hence no. of ways of selecting 2 men and 2 women are ${ }^{6} C_{2}+{ }^{5} C_{2}=25$ ways .
(iii) Number of ways of selecting four people and all of same sex is ${ }^{6} C_{4}+{ }^{5} C_{4}=20$ ways.

16 A Survey of 100 students with respect to their choice of the ice cream flavours Vanilla, Chocolate and strawberry shows that 50 students like Vanilla, 43 like chocolate , 28 like strawberry, 13 like Vanilla and chocolate, 11 like chocolate and strawberry, 12 like strawberry and Vanilla, and 5 like all of them. Find the number of students who like
(i) Vanilla only
(ii) Chocolate only
(iii) Strawberry only
(iv) Chocolate but not Strawberry
(v) Chocolate and Strawberry but not Vanilla
(vi) Vanilla or Chocolate, but not Strawberry.

Also find the number students who do not like any of these flavors.

## Solution:

Given $|\mathrm{S} \cap V \cap C|=5,|\mathrm{~S} \cap V|=12,|\mathrm{C} \cap V|=13,|\mathrm{C} \cap S|=11$
The Venn diagram shows the details
(i) Number of students who like Vanilla only $=30$
(ii) Number of students who like Chocolate only $=24$
(iii) Number of students who like Strawberry only $=10$
(iv) Number of students who like Chocolate but not Strawberry $=24+8=$ 32
(v) Number of students who like Chocolate and Strawberry but not

$$
\text { Vanilla }=6
$$

(vi) Number of students who like Vanilla or Chocolate but not Strawberry $=24+8+30=62$.

Number of students who do not like any of these flavors

$$
\begin{aligned}
& =100-(50+16+24) \\
& =100-90=10
\end{aligned}
$$

17 (a) In how many ways can the letters of the word MISSISSIPPI be arranged? (b) In how many of these arrangements, the P's are separated? (c) In how many arrangements, the I's are separated? (d) In how many arrangements, the P's are together?

Solution: (a) The word MISSISSIPPI contains 11 letters consisting of 4-I's, 4S's, 2-P's, M.
$\therefore$ the number of arrangements $=\frac{11!}{4!\times 4!\times 2!}=\frac{3991680}{1152}=34650$
(b) Since the P's are to be separated, first arrange the order 9 letters consisting of 4-I's, 4-S's and M. This can be done in $\frac{9!}{4!\times 4!}$ ways.

In each of these arrangements of 9 letters, there are 10 gaps in which the $2-\mathrm{P}$ 's can be arranged in $\frac{P(10,2)}{2!}$ ways. $=\frac{10 \times 9}{2!}=45$ ways .
$\therefore$ the total number of ways of arranging all the 11 letters which the P's are
separated is $=\frac{9!}{4!\times 4!} \times 45=\frac{16329600}{24 \times 24}=28,350$.
(c) Since the I's are to be separated from one another, first arrange the other 7 letters consisting of 4-I's, 2-P's and M. This can be done in $\frac{7!}{4!\times 2!}$ ways.

In each of these arrangements of 7 letters, there are 8 gaps in which the 4 -I's can be arranged in $\frac{P(8,4)}{4!}$ ways. $=\frac{8 \times 7 \times 6 \times 5}{4!}=70$ ways.
$\therefore$ the total number of ways of arranging all the 11 letters which the I's are separated is $=\frac{7!}{4!\times 2!} \times 70=7350$ ways.
(d) Since the P's are to be together, treat them as one unit. The remaining 9 letters consisting of 4-I's, 4-S's and M as 9 units. Thus we have 10 units, which can be arranged in $\frac{10!}{4!\times 4!}$ ways.

Since the P's are identical, by interchanging them we don't get any new arrangement.

Hence total number of arrangements in which the P's are together $\frac{10!}{4!\times 4!}=6300$ ways.

18 The password for a computer system consists of eight distinct alphabetic characters. Find the number of passwords possible that
(a) end in the string MATH
(b) begin with the string CREAM
(c) contain the word COMPUTER as a substring

Solution: There are 26 English alphabets. Password consists of 8 different alphabets.
(a) The password should end with MATH.

The other four places must be filled with the remaining 22 alphabets choosing 4 at a time. This can be done in $\mathrm{P}(22,4)$ ways.
$\therefore$ the total number of passwords $=\mathrm{P}(22,4)=22 \times 21 \times 20 \times 19=175560$.
(b) The password should begin with the string CREAM.

So, the 3places must be filled up with 3 letters from the remaining 21
letters in $\mathrm{P}(21,3)$ ways. $\therefore$ number of passwords $=\mathrm{P}(21,3)=21 \times 20 \times 19$ $=7980$
(c) The word COMPUTER contains 8 letters and so it is itself the password.
$\therefore$ the number of ways of forming the password is 1 .

## 19 How many bit strings of length 10 contains

(A) exactly four 1's
(B) at most four 1's
(C)at least four 1's
(D) an equal number of 0's and 1's

## Solution:

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

No. of required bit strings $=\frac{10!}{4!6!}=210$
2.The 10 positions should be filled with (i) no 1's and ten 0's (ii) one 1's and nine 0's (iii) two 1's and eight 0's (iv) three 1's and seven 0's (v) four 1's and six O's.Therefore Required no. of bit strings $=\frac{10!}{0!10!}+\frac{10!}{1!9!}+\frac{10!}{2!8!}+\frac{10!}{3!7!} \frac{10!}{4!6!}=386$ ways

3 The ten position are to be filled up with (i) four 1's and six 0's (or) (ii) five 1'and five 0's (or) six 1's and four 0's etc......ten 1's and zero 0's. Therefore no. of bit

$$
\text { strings }=\frac{10!}{4!6!}+\frac{10!}{5!5!} \frac{10!}{6!4!}+\frac{10!}{3!7!}+\frac{10!}{8!2!}+\frac{10!}{9!11!}+\frac{10!}{10!0!}=848 \text { ways }
$$

4. The ten positions are to be filled up with five 1's and five 0's. Therefore no. of

$$
\text { bit strings } \frac{10!}{5!5!}=252 \text { ways }
$$

20 From a committee consisting of 6 men and 7 women, in how many ways can we select a committee of (i) 3 men and 4 women. (ii) 4 members which has atleast one women. (iii) 4 persons that has atmost one man. (iv) 4 persons of both sexes.

## Solution:

(1) Three men can be selected from 6 men in $6 C_{3}$ ways, 4 women can be selected from 7 women in $7 C_{4}$ ways.

By product rule the committee of 3 men and 4 women can be selected in $6 C_{3} \times 7 C_{4}=700$
(ii) For the committee of atleast one women we have the following possibilities
(a) 1 women and 3 men
(b) 2 women and 2 men
(c) 3 women and 1 men
(d) 4 women and 0 men

Therefore, the selection can be done in
$7 C_{1} \times 6 C_{3}+7 C_{2} \times 6 C_{2}+7 C_{3} \times 6 C_{1}+7 C_{4} \times 6 C_{0}$ ways
$=7 \times 20+21 \times 15+35 \times 6+35 \times 1$
$=140+315+210+35=700$ ways
(iii) For the committee of almost one men we have the following possibilities
(a) 1 men and 3 women
(b) 0 men and 4 women

Therefore, the selection can be done in
$6 C_{1} \times 7 C_{3}+6 C_{0} \times 7 C_{4}$ ways
$=6 \times 35+1 \times 35$
$=245$ ways
(iv) For the committee of both sexes, we have the following possibilities
(a) 1 men and 3 women
(b) 2 men and 2 women
(b) 3 men and 1 women

Therefore, the selection can be done in

$$
\begin{aligned}
& 6 C_{1} \times 7 C_{3}+6 C_{2} \times 7 C_{2}+6 C_{3} \times 7 C_{1} \text { ways } \\
& =6 \times 35+15 \times 21+20 \times 7 \\
& =210+315+140 \text { ways } \\
& =665 \text { ways }
\end{aligned}
$$

21 How many permutations can be made out of the letters of the word "Basic"? How many of these (1) Begin with B? (2) End with C? (3) B and C occupy the end places?

## Solution:

There are 5 letters in the word "Basic" and all are distinct. Therefore, the number of permutations of these letters is $=5!=120$.
(i) Permutations which begin with B.

The first position can be filled in only one way i.e B and the remaining 4 letters can be arranged in 4! Ways. Therefore, total number of permutations starting with $B$ is $=1 \times 4!=24$.
(ii) Permutation which end with C.

The first position can be filled in only one way i.e., C and the remaining 4 letters can be arranged in 4 ! Ways. Therefore, total number of permutations ending with C is $=4!\times 1=24$.

Permutations in which B and C occupy end places B and C occupy end positions in 2 ! Ways i.e., $\mathrm{B}, \mathrm{C}$ and $\mathrm{C}, \mathrm{B}$ and the remaining 3 letters can be arranged in 3 ! Ways. Therefore, total number of permutations in which B and C occupy end places in $=2!\times 3!=12$.

## Principle of Inclusion - Exclusion

(i) $n\left(T_{1} \cup T_{2}\right)=n\left(T_{1}\right)+n\left(T_{2}\right)-n\left(T_{1} \cap T_{2}\right)$
(ii) $|A \cup B|=|A|+|B|-|A \cap B|$
(iii) $|A \cup B \cup C|=|A|+|B|+|C|-|A \cap B|-|B \cap C|-|C \cap A|+|A \cap B \cap C|$
(iv) $|A \cup B \cup C \cup D|=|A|+|B|+|C|+|D|-|A \cap B|-|B \cap C|-|C \cap D|-|D \cap A|-$ $|A \cap C|-|B \cap D|+|A \cap B \cap C|+|B \cap C \cap D|+|C \cap D \cap A|+|A \cap B \cap D|-|A \cap B \cap C \cap D|$.

22 Find the number of integers between 1 and 250 that are not divisible by any of the integers $2,3,5$ or 7 .

Solution: Let A, B, C, D be the sets of integers that lie between 1 and 250 both inclusive and that are divisible by $2,3,5$ and 7 respectively.

$$
|A \cap B \cap C|=\left\{\left.\begin{array}{c}
250 \\
\frac{L C M(2,3,5)}{L C M}\left|=\left|\frac{250}{\lfloor 2 \times 3 \times 5}\right|\right\rfloor
\end{array} \right\rvert\,=8\right.
$$

$$
|A \cap B \cap D|=\left\{\begin{array}{c}
250 \\
L C M(2,3,7)
\end{array}\left|=\left.\right|_{\lfloor 2 \times 3 \times 7}\right|\right\rfloor=5
$$

$$
\begin{aligned}
& \therefore|A|=\left\lfloor\frac{250}{2}\right\rfloor=125, \quad|B|=\left\lfloor\left.\frac{250}{3\rfloor} \right\rvert\,=83\right. \\
& \left.|C|=\left\lfloor\frac{250}{5}\right\rfloor|=50, \quad| D \right\rvert\,=\left\lfloor\left.\frac{250}{7\rfloor} \right\rvert\,=35\right. \\
& |A \cap B|=\left\{\left.\begin{array}{c}
250 \\
\operatorname{LCM(2,3)}
\end{array} \right\rvert\,=\left\{\left.\begin{array}{c}
250 \\
\lfloor 2 \times 3
\end{array} \right\rvert\,=41\right.\right. \\
& |A \cap C|=\left\{\begin{array} { c } 
{ 2 5 0 } \\
{ \operatorname { L C M } ( 2 , 5 ) }
\end{array} \left|=\left|\begin{array}{c}
250 \\
\lfloor 2 \times 5
\end{array}\right|=25\right.\right. \\
& |A \cap D|=\left\{\begin{array}{c}
250 \\
L C M(2,7)
\end{array}|=| \begin{array}{c}
250 \\
\left\lfloor\left.\frac{1}{2 \times 7} \right\rvert\,\right\rfloor
\end{array}=17\right. \\
& |B \cap C|=\left\{\begin{array}{c}
250 \\
\operatorname{LCM}(3,5)
\end{array}\left|=\begin{array}{c}
\mid 250 \\
\left|\begin{array}{l}
3 \times 5
\end{array}\right|
\end{array}\right|=16\right. \\
& |B \cap D|=\left\{\begin{array}{c}
250 \\
2 C M(3,7)
\end{array} \left\lvert\,=\begin{array}{c}
|250| \\
|3 \times 7|
\end{array}\right.\right]=11 \\
& |C \cap D|=\left\{\begin{array} { c } 
{ 2 5 0 } \\
{ \operatorname { L C M } ( 5 , 7 ) }
\end{array} \left|=\left|\begin{array}{c}
250 \mid \\
\mid 5 \times 7
\end{array}\right|=7\right.\right.
\end{aligned}
$$

$$
\begin{aligned}
& |A \cap C \cap D|=\left\{\begin{array}{c}
2 J U \\
L C M(2,5,7)
\end{array} \left\lvert\,=\left\{\left.\begin{array}{l}
2 J U \\
\lfloor 2 \times 5 \times 7
\end{array} \right\rvert\,=3\right.\right.\right. \\
& |B \cap C \cap D|=\left\{\begin{array}{c}
250 \\
L C M(3,5,7)
\end{array} \left\lvert\,=\left\{\left.\begin{array}{c}
250 \\
\lfloor 3 \times 5 \times 7
\end{array} \right\rvert\,=2\right.\right.\right. \\
& |A \cap B \cap C \cap D|=\left\{\begin{array} { c } 
{ 2 5 0 } \\
{ L C M ( 2 , 3 , 5 , 7 ) }
\end{array} \left|=\left|\begin{array}{l}
250 \\
\left|\frac{1}{2 \times 3 \times 5 \times 7}\right|
\end{array}\right|=1\right.\right. \\
& |A \cup B \cup C \cup D|=|A|+|B|+|C|+|D|-|A \cap B|-|A \cap C|-|A \cap D|-|B \cap C| \\
& -|B \cap D|+|C \cap D|+|A \cap B \cap C|+|A \cap B \cap D|+|A \cap C \cap D| \\
& +|B \cap C \cap D|-|A \cap B \cap C \cap D| \\
& =193
\end{aligned}
$$

Therefore, not divisible by any of the integers $2,3,5$ and $7=250-193=57$.
23 Find the number of integers between 1 and 100 that are not divisible by any of the integers $2,3,5$ or 7 .

Solution: Let A, B, C, D be the sets of integers that lie between 1 and 100 both inclusive and that are divisible by $2,3,5$ or 7 respectively.

$$
\begin{aligned}
& \therefore|A|=\left\lfloor\frac{100}{2}\right\rfloor=50, \quad|B|=\left\lfloor\frac{100}{3}\right\rfloor=33 \\
& |C|=\left\lfloor\frac{100}{5}\right\rfloor=20, \quad|D|=\left\lfloor\frac{100}{7}\right\rfloor=14 \\
& |A \cap B|=\left\{\left.\begin{array}{c}
100 \\
\operatorname{LCM}(2,3)
\end{array} \right\rvert\,=\left\{\left.\begin{array}{c}
100 \\
\lfloor 2 \times 3
\end{array} \right\rvert\,=16\right.\right. \\
& |A \cap C|=\left\{\begin{array}{c}
100 \\
\operatorname{LCM}(2,5)
\end{array}\left|=\begin{array}{c}
\mid 00 \\
|2 \times 5|
\end{array}\right|=10\right.
\end{aligned}
$$

$$
\begin{aligned}
& |A \cap D|=\left|\frac{100}{\left\lfloor\frac{L C M(2,7)}{}\right\rfloor}\right|=\left|\frac{100}{\lfloor 2 \times 7}\right|=7 \\
& |B \cap C|=\frac{\mid 00}{\left\lfloor\frac{\mid}{L C M(3,5)}\right\rfloor}=\frac{|100|}{\lfloor 3 \times 5\rfloor}=6 \\
& |B \cap D|=\frac{100}{\left\lfloor\frac{\mid}{L C M(3,7)}\right\rfloor}=\frac{|100|}{\lfloor 3 \times 7\rfloor}=4 \\
& |C \cap D|=\left|\frac{100}{\left\lfloor\frac{L C M(5,7)}{L}\right.}\right|=\left\lvert\, \frac{100}{\left.\left|\frac{1}{5 \times 7}\right|\right\rfloor}=2\right. \\
& |A \cap B \cap C|=\left\{\begin{array}{l}
\left.\left.\left\lvert\, \frac{100}{L C M(2,3,5)}\right.\right\rfloor=\left|\frac{100}{2 \times 3 \times 5}\right|\right\rfloor=3 \\
\lfloor
\end{array}\right. \\
& |A \cap B \cap D|=\left\{\begin{array}{l}
\frac{100}{L C M(2,3,7)}\left|=\left|\frac{100}{\left|\frac{L}{2 \times 3 \times 7}\right|}\right|=2\right. \\
\left\lfloor\frac{2}{2},\right.
\end{array}\right. \\
& \left.|A \cap C \cap D|=\left\{\frac{100}{\lfloor C M(2,5,7)}\right\rfloor=\left|\frac{100}{\lfloor 2 \times 5 \times 7}\right|\right\rfloor=1 \\
& \left.\left.|B \cap C \cap D|==\left|\frac{100}{\left\lfloor\frac{100}{L C M(3,5,7)}\right\rfloor=}\right| \frac{1}{\lfloor 3 \times 5 \times 7} \right\rvert\,\right\rfloor 0 \\
& |A \cap B \cap C \cap D|=\left\{\frac{100}{\left.\left\lfloor\frac{1}{L C M(2,3,5,7)}\right\rfloor=\left|\frac{100}{\mid 2 \times 3 \times 5 \times 7}\right|\right\rfloor=0}\right. \\
& |A \cup B \cup C \cup D|=|A|+|B|+|C|+|D|-|A \cap B|-|A \cap C|-|A \cap D|-|B \cap C| \\
& -|B \cap D|+|C \cap D|+|A \cap B \cap C|+|A \cap B \cap D|+|A \cap C \cap D| \\
& +|B \cap C \cap D|-|A \cap B \cap C \cap D| \\
& =78
\end{aligned}
$$

Therefore, not divisible by any of the integers $2,3,5$ and $7=100-78=22$.

24 Determine the number of positive integers $n, 1 \leq n \leq 1000$, that are not divisible by 2,3 or 5 but are divisible by 7 .

## Solution:

Let $\mathrm{A}, \mathrm{B}, \mathrm{C}$ and D denote respectively the number of integers between1-1000, that are not divisible by 2,35 and 7 respectively. Now

$$
\begin{aligned}
& |D|=\left[\frac{1000}{7}\right]=[142.8]=142 \\
& |\mathrm{~A} \cap \mathrm{~B} \cap \mathrm{C} \cap \mathrm{D}|=\left[\frac{1000}{2 \times 3 \times 5 \times 7}\right]=7
\end{aligned}
$$

The number between $1-1000$ that are divisible by 7 but not divisible by $2,3,5$ and 7
$=|D|-|\mathrm{A} \cap \mathrm{B} \cap \mathrm{C} \cap \mathrm{D}|=138$

25 Determine the number of positive integers $n, 1 \leq n \leq 2000$ that are not divisible by 2,3 or 5 , but are divisible by 7 .

## Solution:

Let A, B, C and D denote respectively the number of integers between 1 to 2000 that are divisible by $2,3,5$ and 7 respectively.

$$
\begin{aligned}
& \text { Now }|D|=\left\lfloor\frac{2000}{7}\right\rfloor=\lfloor 285.71\rfloor=285 \\
& |A \cap B \cap C \cap D|=\left\lfloor\frac{2000}{2 \times 3 \times 5 \times 7}\right\rfloor=\lfloor 9.5\rfloor=9
\end{aligned}
$$

The number between 1 to 2000 that are divisible by 7 but not divisible by 2,3 or 5 is
$|D|-A \cap B \cap C \cap D \mid=285-9=276$.

26 How many positive integers not exceeding 1000 are divisible by none of 3,7 and 11 ?

## Solution:

Let A, B and C denote respectively the number of integers between 1 to 1000 that are divisible by 3,7 and 11 respectively.

$$
\begin{aligned}
& \therefore|A|=\left\lfloor\frac { 1 0 0 0 } { 3 } \left|=333,|B|=\left|\frac{1000}{7}\right|=142,|C|=\left|\frac{1000}{11}\right|=90,\right.\right. \\
& |A \cap B|=\left\lfloor\frac { 1 0 0 0 } { 3 \times 7 } \left|=47,|A \cap C|=\left|\frac{1000}{\lfloor 3 \times 11}\right|=30,|B \cap C|=\left|\frac{1000}{\left\lfloor\frac{1 \times 1}{}\right\rfloor}\right|=12\right.\right. \\
& |A \cap B \cap C|=\left\lfloor\left.\frac{1000}{3 \times 7 \times 11} \right\rvert\,=4\right.
\end{aligned}
$$

By inclusion and exclusion principle,

$$
\begin{aligned}
|A \cup B \cup C|= & |A|+|B|+|C|-|A \cap B|-|B \cap C|-|C \cap A|+|A \cap B \cap C| \\
& =333+142+90-47-30-12+4 \\
& =480
\end{aligned}
$$

The number of integers not divisible by none of 3,7 and $11=1000-480=520$.
27 How many positive integers not exceeding 1000 are divisible by 7 or 11?

## Solution:

Let A and B denote the sets of positive integers not exceeding 1000 that are divisible by 7 or 11 .

Then $|A|=\left\lfloor\frac{1000}{7}\right\rfloor=142,|B|=\left\lfloor\frac{1000}{11}\right\rfloor=90,|A \cap B|=\left\lfloor\frac{1000}{7 \times 11}\right\rfloor=12$
The number of positive integers not exceeding 1000 that are divisible by either 7 or 11 is $|A \cap B|$. By principle of inclusion and exclusion

$$
|A \cup B|=|A|+|B|-|A \cap B|=142+90-12=220
$$

There are 220 positive integers not exceeding 1000 divisible by 7 or 11 .
28 A total of 1232 students have taken a course in Spanish, 879 have taken a course in French, and 114 have taken a course in Russian. Further, 103 have taken courses in both Spanish and French, 23 have taken courses in both Spanish and Russian and 14 have taken courses in both

French and Russian. If 2092 students have taken at least one of Spanish, French and Russian, how many students have taken a course in all three languages?

Solution: Let S-Spanish, F-French, R-Russian.

$$
\begin{aligned}
& |S|=1232, \quad|F|=879, \quad|R|=114, \quad|S \cap F|=103, \quad|S \cap R|=23 \\
& |F \cap R|=14,|S \cup F \cup R|=2092 . \\
& \quad|S \cup F \cup R|=|S|+|F|+|R|-|S \cap F|-|S \cap R|-|F \cap R|+|S \cap F \cap R| \\
& \quad=1232+879+114-103-23-14+2092
\end{aligned} \quad \begin{aligned}
& \therefore|S \cap F \cap R|=7
\end{aligned}
$$

29 There are 2500 students in a college of these 1700 have taken a course in C, 1000 have taken a course in Pascal and 550 have taken a course in networking. Further 750 have taken course in both C and Pascal, 400 have taken course in both $C$ and Networking and 275 have taken courses in both Pascal and networking. If 200 of these students have taken courses in C, Pascal and networking,
(i) How many of these 2500 students have taken a course in any of these courses C, Pascal and networking?
(ii) How many of these 2500 students have not taken any of these three courses C, Pascal and networking?

## Solution:

Let A, B, C denote student have taken a course in C, Pascal and networking respectively.

Given $|A|=1700,|B|=1000,|C|=550,|A \cap B|=750,|A \cap C|=400,|B \cap C|=$ 275, $|A \cap B \cap C|=200$
(i) Number of students who have taken any one of these course

$$
\begin{aligned}
& \quad|A \cup B \cup C|=|A|+|B|+|C|-|A \cap B|-|B \cap C|-|C \cap A|+|A \cap B \cap C| \\
& =(1700+1000+550)-(750+400+275)+200=2025 .
\end{aligned}
$$

(ii) Number of students who have not taken any of these 3 courses $=$ Total $|A \cup B \cup C|=2500-2025=475$.

## Solving Recurrence Relations

Recurrence relation: An equation that expresses $a_{n}$, the general term of the sequence $\left\{a_{n}\right\}$ in terms of one or more of the previous terms of the sequence namely $a_{0}, a_{1}, \ldots a_{n-1}$ for all $n$ with $n \geq n_{0}$, where $n_{0}$ is a non-negative integer is called a recurrence relation for $\left\{a_{n}\right\}$ or a difference equation.

Example: Consider the Fibonacci sequence $0,1,1,2,3,5,8,13 \ldots$ which can be represented by the recurrence relation $F_{n+2}=F_{n+1}+F_{n}$ where $n \geq 0$ and $F_{0}=0$ and $F_{1}=1$.

## Solving Linear Homogeneous Recurrence Relation with Constant Coefficients:

Step 1: Write down the characteristic equation of the given recurrence relation
Step 2: Find all the roots of the characteristic equation.
Step 3:
(i) Let the roots be real and distinct. Then $a_{n}=\alpha_{1} r_{1}^{n}+\alpha_{2} r^{n}{ }_{2}+\cdots+\alpha r_{n}^{n}{ }_{n}^{n}$ here $\alpha_{1}, \alpha_{2}, \ldots \alpha_{n}$ are arbitrary constants.
(ii) Let the roots be real and equal say $r=r_{1}=r_{2}=\cdots=r_{n}$. Then

$$
a_{n}=\left(\alpha_{1}+n \alpha_{2}+n^{2} \alpha_{3}+\cdots+n^{n-1} \alpha_{n}\right) r_{2}^{n}
$$

(iii) When the roots are complex conjugate

$$
a_{n}=r^{n}\left(\alpha_{1} \cos n \theta+\alpha_{2} \sin n \theta\right)
$$

Step 4: Apply initial conditions to find out the arbitrary constants.

## Solving Non-Linear Homogeneous Finite Order Liner Relation:

To solve the recurrence relation $f(k)=S(k)+c_{1} S(k-1)+\cdots+c_{n} S(k-n)$
Step 1: Write the associated homogeneous relation (i.e $f(k)=0$ ) and find its general solution call this the homogeneous solution.

Step 2: Particular solution depending on the R.H.S of the given recurrence relation.

Particular solutions for given R.H.S

| R.H.S | Form of Particular Solution |
| :--- | :--- |
| (i) a constant q | a constant d |
| (ii) a linear function $q_{0}+q_{1} k$ | a linear function $d_{0}+d_{1} k$ |
| (iii) an $m^{\text {th }}$ degree polynomial $q_{0}+q_{1} k$ <br> $+\ldots+q_{m} k^{m}$ | an $m^{\text {th }}$ degree polynomial $d_{0}+d_{1} k+$ <br> $\ldots+d_{m} k^{m}$ |
| (iv) an exponential function $q a^{k}$ | an exponential function $d a^{k}$ |

Note: The general solution of the recurrence relation is the sum of the homogeneous and particular solutions.

30 Solve the recurrence relation $\underset{n}{a}=6 a_{n-1}-9 a_{n-2}, n \geq 2, a_{0}=2, a_{\overline{1}} 3$.

Solution: Given $a_{n}=6 a_{n-1}-9 a_{n-2}, a_{0}=2, a_{1}=3$.

$$
\Rightarrow a_{n}-6 a_{n-1}+9 a_{n-2}=0
$$

Since $n-(n-2)=2$, it is of order 2 .
The characteristic equation is

$$
r^{2}-6 r+9=0 \Rightarrow(r-3)^{2}=0 \Rightarrow r=3,3
$$

The roots are real and equal.
$\therefore$ The general solution is $a_{n}=(A+B n) 3^{n}$.
We shall now find the values of $A, B$ using $a_{0}=2, a_{1}=3$.
Put $n=0, \quad \therefore a_{0}=A \quad \Rightarrow A=2$
Put $n=1, \quad \therefore a_{0}=(A+B) 3 \Rightarrow 3(2+\mathrm{B})=3$

$$
\Rightarrow B=-1
$$

$\therefore$ The general solution is $a_{n}=(2-n) 3^{n}, n \geq 0$.

31 Solve the recurrence relation $a_{n}=2\left(a_{n-1}-a_{n-2}\right)$ where $n \geq 2, a_{0}=1, a_{1}=2$.

Solution: Given

$$
\begin{aligned}
a_{n} & =2\left(a_{n-1}-a_{n-2}\right) \\
& =a_{n}-2 a_{n-1}+2 a_{n-2}=0
\end{aligned}
$$

The characteristic equation is given by

$$
\begin{gathered}
\lambda^{2}-2 \lambda+2=0 \\
\therefore \lambda=\frac{2 \pm \sqrt{4-4(2)}}{2}=\frac{2 \pm i 2}{2}=1 \pm i \\
\therefore \lambda=1+i, 1-i \\
\therefore \text { Solution is } a_{\mathrm{n}}=A(1+i)+B(1-i) \quad n
\end{gathered}
$$

Where $A$ and $B$ are arbitrary constants
Now, we have

$$
\begin{aligned}
z & =x+i y \\
& =r[\cos \theta+i \sin \theta] \\
\theta & =\tan ^{-1}\left(\frac{y}{x}\right)
\end{aligned}
$$

By Demoivre's theorem we have,

$$
\begin{aligned}
& \begin{aligned}
&(1+i)^{n}=\left[\left.2^{1}\right|^{\cos \frac{\pi}{4}+i \sin } \frac{\pi}{4}\right]^{n} \\
&=\left[\sqrt{2}^{-}\right]^{n}\binom{n \pi}{\cos \frac{n \pi}{4}} \\
& \text { and }(1-i)^{n}=\left[\sqrt{2}^{2}\right]^{n}\left(\frac{n \pi}{4}\right) \\
&\left.\cos \frac{n \pi}{4}-i \sin \frac{n \pi}{4}\right)
\end{aligned}
\end{aligned}
$$

Now,

$$
\begin{align*}
& =\left[\mathcal{F}^{\mathcal{L}^{n}}\left((A+B) \cos \frac{n \pi}{4}+i(A-B) \sin \frac{n \pi)}{4}\right)\right. \\
& \therefore a_{n}=\left[\sqrt{2}^{]^{n}}\left(\underset{1}{C \cos \frac{n \pi}{4}}+C \sin _{2} \frac{n \pi)}{4}\right)\right] \tag{1}
\end{align*}
$$

Is the required solution. Let $C_{1}=A+B, \quad C_{2}=i(A-B)$
Since $a_{0}=1, a_{1}=2$

$$
\begin{aligned}
& \text { (1) } \Rightarrow a_{0}=(\sqrt{2})\left[C_{1} \cos 0+C_{2} \sin 0\right]=0 \\
& \Rightarrow 1=C_{1} \\
& a=\left[\mathcal{F}^{1}\left(\begin{array}{c}
C \cos \pi \\
1 \\
\hline
\end{array} C_{2} \sin \overline{4}\right)\right. \\
& 2=\boldsymbol{V}^{2}\left(C^{1} \frac{1}{\sqrt{2}}+C_{2} \sin \frac{1}{\sqrt{2}}\right) \\
& \Rightarrow 2=C_{1}+C_{2} \\
& \Rightarrow C_{2}=1 \\
& \therefore a_{n}=\left[V^{]^{n}}\binom{\left.\cos ^{n \pi}+\sin n \pi\right)}{4}\right.
\end{aligned}
$$

32 Find the general solution of the recurrence relation $a_{n}-5 a_{n-1}+6 a_{n-2}=4, n \geq 2$.


The corresponding homogeneous recurrence relation is
$a_{n}-5 a_{n-1}+6 a_{n-2}=0$

Since $n-(n-2)=2$, it is of order 2 .
$\therefore$ the characteristic equation is $r^{2}-5 r+6=0$
$\Rightarrow(r-2)(r-3)=0 \Rightarrow r=2,3$
$a_{n}^{(h)}=A .2^{n}+B .3^{n}$

Given $f(n)=4^{n}, 4$ is not a root of thecharacteristicequation
$\therefore$ the particular solution is $a_{n}^{(p)}=C .4^{n}$

Substituting in the given equation (1), we get
$C .4^{n}-5 C .4^{n-1}+6 C .4^{n-2}=4^{n}$
$4^{n-2} C[16-20+6]=4^{n}$
Dividing by $4^{n-2}$
$\Rightarrow 2 C=16$
$C=8$
$\therefore a_{n}^{(p)}=8 \times 4^{n}$
Hence the generalsolution is $a_{n}=a^{(h)}+a^{(p)}{ }_{n}$

$$
=A .2^{n}+B .3^{n}+\left(8 \times 4^{n}\right)
$$

33 Solve the recurrence $a_{n}-3 a_{n-1}=2 n, a_{1}=3$

## Solution:

$a_{n}-3 a_{n-1}=2 n, a_{1}=3$
$\therefore$ the homogenous recurrence relation is $a_{n}-3 a_{n-1}=0$

Since $n-(n-1)=1$, the order is 1

The characteristic equation is $r-3=0 \Rightarrow r=3$

Hence $a_{n}^{(h)}=C .3^{n}$

Given $f(n)=2 n$, which is a polynomial of degree 1 .

Hence Particular $s$ olution is $a_{n}=A_{0}+A_{1} n$

$$
\begin{aligned}
& \therefore A_{0}+A_{1} n-3\left(A_{0}+A_{1}(n-1)\right)=2 n \\
& -2 n A_{1}=2 \Rightarrow A_{1}=-1 \\
& 3 A_{1}-2 A_{0}=0 \\
& \Rightarrow 2 A_{0}=3 A_{1} \\
& \Rightarrow 2 A_{0}=3(-1) \\
& \Rightarrow A_{0}=\frac{-3}{2} \\
& a^{(p)}=\frac{-3}{2}-n=\frac{-1}{2}(3+2 n) \\
& n
\end{aligned}
$$

$\therefore$ the generalsolution of the given recurrence relation is
$a_{n}=a_{n}^{(h)}+a_{n}^{(p)}$
$\Rightarrow a_{n}=C \cdot 3^{n}-\frac{1}{2}(3+2 n)---(1)$

Given: $a_{1}=3$

Putting $n=1$ in (1)
$a_{1}=C .3-\frac{1}{2}(3+2)$

$$
\Rightarrow 3=3 C-\frac{5}{2} \Rightarrow C=\frac{11}{6}
$$

$\therefore$ the generalsolution of the given recurrence relation is
$a=\frac{11}{{\underset{n}{6}}^{6}} 3^{n}-\frac{1}{2}(3+2 n)$

## 34 Solve the recurrence relation for the Fibonacci sequence.

## Solution:

The sequence of Fibonacci numbers satisfies the recurrence relation

$$
\begin{align*}
& f_{n}=f_{n-1}+f_{n-2} \ldots . .(1) \quad \text { and satisfies the initial conditions } f_{1}=1, f_{2}=1 . \\
& (1) \Rightarrow f_{n}-f_{n-1}-f_{n-2}=0 \ldots(2) \tag{2}
\end{align*}
$$

Let $f_{n}=r^{n}$ be a solution of the given equation.
The characteristic equation is $r^{2}-r-1=0$
$r=\frac{1 \pm \sqrt{+4}}{2}$
Let $r_{1}=\frac{1+\sqrt{5}}{2}, r_{2}=\frac{1-\sqrt{5}}{2}$
$\therefore$ By theorem

$$
\begin{aligned}
& f_{n}=\alpha_{1}\left(\left.\begin{array}{c}
1+\sqrt{5})^{n} \\
2
\end{array} \alpha_{2} \right\rvert\, \square\binom{1-\sqrt{5})^{n}}{2}\right. \\
& f_{1}=1 \Rightarrow f_{1}=\alpha_{1}\binom{1+\sqrt{5}}{2}-\left(\begin{array}{c}
(1-\sqrt{5}) \\
\alpha_{2} \\
2
\end{array}\right) \\
& (1+\sqrt{5}) \alpha_{1}+(1-\sqrt{5}) \alpha_{2}=2 \ldots(4)
\end{aligned}
$$

$$
\begin{align*}
& f_{2}=1 \Rightarrow f_{2}=\alpha_{1}\binom{1+\sqrt{5})^{2}}{2}_{2}|\square|=\binom{1-\sqrt{5}}{1}^{2} \\
& =\alpha_{1} \frac{(1+\sqrt{5})^{2}}{4}+\alpha_{2} \frac{(1-\sqrt{5})^{2}}{4}=1 \\
& =(1+\sqrt{5})^{2} \alpha_{1}+(1-\sqrt{5})^{2} \alpha_{2}=4  \tag{5}\\
& \underset{(1-\sqrt{5})}{(4) \times(1+\sqrt{5}) \alpha_{1}+(1-\sqrt{5})_{2} \alpha_{2}=2(1-\sqrt{5})} \\
& \text { (6) - (5) } \Rightarrow \alpha_{1}(1+\sqrt{5})[1-\sqrt{5}-1-\sqrt{5}]=2-2 \sqrt{5}-4 \\
& \alpha_{1}(1+\sqrt{5})[-2 \sqrt{1}]=-2-25 \\
& \alpha_{1}(1+\sqrt{5})[-2 \sqrt{5}]=-2(1+\sqrt{5}) \\
& \alpha_{1}=\frac{1}{\sqrt{5}} \\
& \text { 4) } \Rightarrow(1+\sqrt{5}) \frac{1}{\sqrt{5}}+(1-\sqrt{5}) \alpha_{2}=2 \\
& \frac{1}{\sqrt{5}}+1+(1-\sqrt{5}) \alpha_{2}=2 \\
& (1-\sqrt{5}) \alpha_{2}=2-\frac{1}{\sqrt{5}}-1 \\
& =1-\frac{1}{\sqrt{5}} \\
& (1-\sqrt{ }) \alpha_{2}=\frac{\sqrt{ }^{5}-1}{\sqrt{5}} \\
& \alpha_{2}=\frac{-1}{\sqrt{5}} \\
& \text { (3) } \Rightarrow f_{n}=\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n}+\frac{-1(1-\sqrt{5})^{n}}{\sqrt{5}}\left(\frac{1}{2}\right)
\end{align*}
$$

## Generating Function:

The generating function of a sequence $a_{0}, a_{1}, a_{2}, \ldots$ is the expression

$$
G(x)=a_{0}+a_{1} x+a_{2} x^{2}+\cdots=\sum_{n=0}^{\infty} a_{n} x^{n}
$$

Example: The generating function for the sequence $1,1,1,1$ is

$$
G(x)=1+x+x^{2}+\cdots=(1-x)^{-1}=\frac{1}{(1-x)}=\sum_{n=0}^{\infty} x^{n}
$$

## Solution of Recurrence Relation Using Generating Functions

Procedure:

Step 1: Rewrite the recurrence relation as an equation with 0 on R.H.S
Step 2: Multiply on both sides by $x^{n}$ and summing it from 0 to $\infty$.
Step 3: Put $G(x)=\sum_{n=0}^{\infty} a_{n} x^{n}$ and write $G(x)$ as function of $x$.
Step 4: Decompose $G(x)$ into partial fraction.
Step 5: Express $G(x)$ as a sum of familiar series.
Step 6: Express $a_{n}$ as the coefficient of $x^{n}$ in $G(x)$.

Note:
(i) $G(x)=\sum_{n=0}^{\infty} a_{n} x^{n}$ generates $\left(a_{0}, a_{1}, a_{2}, \ldots\right)$
(ii) $G(x)-a_{0}=\sum_{n=1}^{\infty} a_{n} x^{n}$ generates $\left(0, a_{1}, a_{2}, \ldots\right)$
(iii) $G(x)-a_{0}-a_{1} x=\sum_{n=2}^{\infty} a_{n} x^{n}$ generates $\left(0,0, a_{2}, a_{3}, \ldots\right)$

35 Use generating function to solve the recurrence relation $S(n+1)$ $2 S(n)=4^{n}$, with $S(0)=1$ and $n \geq 0$.

Solution: Given $\boldsymbol{S}(\boldsymbol{n}+\mathbf{1})-\mathbf{2 S}(\boldsymbol{n})=\mathbf{4}^{n}$, The recurrence relation can be written as

$$
a_{n+1}-\angle a_{n}-4_{n}=\mathrm{U}, n \geq \mathrm{U}
$$

Multiply (1) by $x^{n}$ and summing from $n=1$ to $\infty$
$\sum_{n=0}^{\infty} a_{n+1} x^{n}-2 \sum_{n=0}^{\infty} a_{n} x^{n}-\sum_{n=0}^{\infty} 4^{n} x^{n}=0$
$=\frac{1}{x} \sum_{n=0}^{\infty} a_{n+1} x^{n+1}-2 \sum_{n=0}^{\infty} a_{n} x^{n}-\sum_{n=0}^{\infty} 4{ }^{n n}=0$
$=\frac{1}{x}[G(x)-a(0)-2 G(x)]-\frac{1}{1-4 x}=0$
$=\frac{1}{x}(G(x)-1)-2 G(x)=\frac{1}{1-4 x}$
$G(x)\left(\frac{1}{x}-2\right)=\frac{1}{1-4 x}+\frac{1}{x}=\frac{x+1-4 x}{x(1-4 x)}=\frac{1-3 x}{x(1-4 x)}$
$G(x)=\frac{1-3 x}{(1-4 x)} \times \frac{1}{1-2 x}=\frac{1-3 x}{(1-2 x)((1-4 x)}$
$\frac{1-3 x}{(1-2 x)((1-4 x)}=\frac{A}{1-2 x}+\frac{B}{1-4 x}$

By solving we get $\mathrm{A}=1 / 2$ and $\mathrm{B}=1 / 2$
$\therefore G(x)=\frac{\frac{1}{2}}{1-2 x}+\frac{\frac{1}{2}}{1-4 x}$
$=\frac{1}{2}[1-2 x]^{-1}+\frac{1}{2}[1-4 x]^{-1}$
$=\frac{1}{2}\left[1+2 x+(2 x)^{2}+\ldots\right]+\frac{1}{2}\left[1+4 x+(4 x)^{2}+\ldots\right]$
$=\frac{1}{2} \sum_{n=0}^{\infty} 2^{n} x^{n}+\underset{2}{-\sum_{n=0}^{\infty} 4 x^{n}}$
$a_{n}=$ coefficient of $x \operatorname{in}_{n} G(x)$
$a_{n}=\frac{2^{n}}{2}+\frac{4^{n}}{2}=2^{n-1}+2(4)^{n-1}$

36 Using generating function solve $a_{n}-3 a_{n-1}=2, \forall n \geq 1, a_{0}=2$.

Let $G(x)=\sum_{n=0}^{\infty} a_{n} x^{n}$ be the generating function of the sequence $\{a\} \cdot{ }_{n}$

Given

$$
a_{n}-3 a_{n-1}=2
$$

Multiplying by $x^{n}, \quad a_{n} x^{n}-3 a_{n-1} x^{n}=2 x^{n}$

$$
\begin{gathered}
\Rightarrow a_{n} x^{n}-3 x a_{n-1} x^{n-1}=2 x^{n} \\
\Rightarrow \sum_{n=1}^{\infty} a_{n} x^{n}-3 x \sum_{n=1}^{\infty} a_{n-1} x^{n-1}=2 \sum_{n=1}^{\infty} x^{n} \\
\Rightarrow a_{0}+\sum_{n=1}^{\infty} a_{n} x^{n}-3 x \sum_{n=1}^{\infty} a_{n-1} x^{n-1}=a_{0}+2\left(x+x^{2}+x^{3}+\ldots\right) \\
\Rightarrow \sum_{n=0}^{\infty} a_{n} x^{n}-3 x G(x)=2+2 x\left(1+x+x^{2}+\ldots\right) \\
G(x)-3 x G(x) \quad=2+2 x(1-x)^{-1} \\
G(x)[1-3 x] \quad=2+\frac{2 x}{1-x}=\frac{2}{1-x} \\
G(x)=\frac{2}{(1-x)(1-3 x)}
\end{gathered}
$$

Split $\frac{2}{(1-x)(1-3 x)}$ by partial fraction

Let $\frac{2}{(1-x)(1-3 x)}=\frac{A}{(1-x)}+\frac{B}{(1-3 x)}$

$$
\Rightarrow 2=A(1-3 x)+B(1-x)
$$

When $x=1, \quad 2=A(1-3) \Rightarrow A=-1$

When $x=\frac{1}{3}, \quad 2=B\left(1-\begin{array}{r}1 \\ z\end{array}\right) \Rightarrow B=3$

$$
\begin{aligned}
& \begin{aligned}
& \therefore G(x)=\frac{2}{(1-x)(1-3 x)}=\frac{-1}{(1-x)}+\frac{3}{(1-3 x)} \\
&=-(1-x)^{-1}+3(1-3 x)^{-1}
\end{aligned} \\
& \begin{aligned}
\Rightarrow & a_{0}+a x_{1}+a x_{2}^{2}+\ldots+a x_{n}^{n}+\ldots=-\left(1+x+x^{2}+\ldots+x^{n}+\ldots\right) \\
& \quad+3\left(1+3 x+3^{2} x^{2}+\ldots+3^{n} x^{n}+\ldots\right)
\end{aligned} \\
& \begin{aligned}
\therefore & a_{n}=-1+3.3_{n}, n \geq 0
\end{aligned} \\
& a_{n}=-1+3^{n+1}, n \geq 0
\end{aligned}
$$

## 37 Use the method of generating function to solve

$$
a_{n+1}-8 a_{n}+16 a_{n-1}=4, n \geq 1, a_{0}=1, a_{1}=8
$$

$\infty$
Let $G(x)=\sum_{n=0} a_{n} x^{n}$ be the generating function of the sequence $\left\{a_{n}\right\}$.

Given

$$
a_{n+1}-8 a_{n}+16 a_{n-1}=4^{n}
$$

Multiplying by $x^{n}, \quad a_{n+1} x^{n}-8 a x_{n}^{n}+16 a{ }_{n-1} x^{n}=4^{n} x^{n}$

$$
\begin{align*}
& \Rightarrow \sum_{n=1}^{\infty} a_{n+1} x^{n}-8 \sum_{n=1}^{\infty} a_{n} x^{n}+16 \sum_{n=1}^{\infty} a_{n-1} x^{n}=\sum_{n=1}^{\infty} 4^{n} x^{n} \\
& \Rightarrow{\underset{x}{x} \sum_{n=1}^{1} n+1}_{\infty} a x^{n+1}-8 \sum_{n=1}^{\infty} a x^{n}+16 x \sum_{n=1}^{\infty} a n-1 x^{n-1}=\sum_{n=1}^{\infty}(4 x)^{n} \tag{1}
\end{align*}
$$

$$
\text { But } \left.\begin{array}{rl}
\sum_{n=1}^{\infty} a x^{n+1} & =a x^{2}+a x^{3}+a x^{4}+\ldots \\
& 2 \quad 3
\end{array}\right)
$$

$$
\begin{aligned}
& \begin{array}{c}
\sum_{n=1}^{\infty} a x^{n}=a x+a x^{2}+a x^{3}+\ldots \\
2
\end{array} \\
& \begin{array}{rl}
=a+a x+a x_{2}^{2}+a x^{3}+\ldots-a \\
0 & 1
\end{array} \\
& =G(x)-1 \\
& \therefore(1) \Rightarrow \frac{1}{x}[G(x)-1-8 x]-8[G(x)-1]+16 x G(x)=1+(4 x)+(4 x)^{2}+\ldots-1 \\
& G(x){ }^{\lceil 1}-8+16 x^{\rceil} \quad 1 \quad 8+8=\begin{array}{ll}
1 & -1
\end{array} \\
& \begin{array}{lll}
\bar{x} & J^{-}{ }_{x} & \overline{1-4 x}
\end{array} \\
& G(x)\left|\frac{1-8 x+16 x^{2}}{x}\right|-\frac{1}{x}=\frac{1-(1-4 x)}{1-4 x} \\
& G(x)\left|\frac{\left\lceil(1-4 x)^{2}\right.}{x}\right|=\frac{4 x}{1-4 x}+\frac{1}{x} \\
& G(x)\left|\frac{(1-4 x)^{2}}{x}\right|=\frac{4 x^{2}+1-4 x}{x(1-4 x)} \\
& G(x)=\frac{1-4 x+4 x^{2}}{(1-4 x)^{3}} \\
& \Rightarrow \sum_{n=0}^{\infty} a_{n} x^{n}=\left(1-4 x+4 x^{2}\right)(1-4 x)^{-3}
\end{aligned}
$$

$\therefore a_{n}=$ coefficient of $x^{n}$
$\Rightarrow a_{n}=\frac{1}{2}\left[(n+1)(n+2) 4^{n}-4 n(n+1) 4^{n-1}+4(n-1) n 4^{n-2}\right]$

$$
\begin{aligned}
& =\frac{1}{2}\left[4^{n}(n+1)(n+2-n)+n(n-1) 4^{n-1}\right] \\
& =\frac{1}{2}\left[4^{n}(n+1)(2)+\left(n^{2}-n\right) 4^{n-1}\right] \\
& =\frac{4^{n-1}}{2}\left[8(n+1)+\left(n^{2}-n\right)\right] \\
& a_{n}=\frac{4^{n-1}}{2}\left[n^{2}+7 n+8\right]
\end{aligned}
$$

38 Solve the recurrence relations $S(n)=S(n-1)+2(n-2)$ with $\mathbf{S}(\mathbf{0})=3, \mathbf{S}(\mathbf{1})=\mathbf{1}$, $\mathrm{n} \geq 2$ using generating function.

Solution:

$$
\begin{aligned}
& S(n)=S(n-1)+2 S(n-2), \quad S(0)=3, \quad S(1)=1, n \geq 2 \\
& S(n)-S(n-1)-2 S(n-2)=0---(1)
\end{aligned}
$$

Let $S(n)=a_{n}$
(1) $\Rightarrow a_{n}-a_{n-1}-2 a_{n-2}=0, \quad a_{0}=3, a_{1}=1$

Multiplying by $x^{n}$ and then summing from 2 to $\infty$, we get

$$
\begin{aligned}
& \sum_{n=2}^{\infty} a_{n} x^{n}-\sum_{n=2}^{\infty} a_{n-1} x^{n}-2 \sum_{n=2}^{\infty} a_{n-2} x^{n}=0 \\
& \sum_{n=2}^{\infty} a_{n} x^{n}-x \sum_{n=2}^{\infty} a_{n-1} x^{n-1}-2 x^{2} \sum_{n=2}^{\infty} a_{n-2} x^{n-2}=0---(2) \\
& {\left[a_{2} x^{2}+a_{3} x^{3}+\ldots\right]-x\left[a_{1} x^{1}+a_{2} x^{2}+\ldots\right]-2 x^{2}\left[a_{0}+a_{1} x^{1}+\ldots\right]_{j}=0} \\
& \left.\left[a_{0}+a_{1} x^{1}+a_{2} x^{2} \ldots-a_{0}-a_{1} x^{1}\right]_{]}-x\left[a_{0}+a_{1} x^{1}+a_{2} x^{2}+\ldots-a_{0}\right]_{j}-\left.2 x^{2}\right|_{[ } a_{0}+a_{1} x^{1}+\ldots\right]=0 \\
& {\left[G(x)-a_{0}-a_{1} x^{1}\right]-x\left[G(x)-a_{0}\right]-2 x^{2}[G(x)]=0} \\
& {[G(x)-3-x]-x[G(x)-3]-2 x^{2}[G(x)]=0} \\
& G(x)\left\lceil\mid 1-x-2 x^{2}\right\rceil \mid-3+2 x=0 \\
& G(x)=\frac{3-2 x}{1-x-2 x^{2}}=\frac{3-2 x}{(1+x)(1-2 x)}=\frac{A}{(1+x)}+\frac{B}{(1-2 x)}
\end{aligned}
$$

$$
\begin{aligned}
& 3-2 x=A(1-2 x)+B(1+x) \\
& \Rightarrow A= \frac{5}{3} \\
& \Rightarrow B= \frac{4}{3} \\
& \therefore G(x)=\frac{5}{3(1+x)}+\frac{4}{3(1-2 x)} \\
&=\frac{5}{3}(1+x)^{-1}+\frac{4}{3}(1-2 x)^{-1} \\
& \Rightarrow a_{n}=\frac{5}{3}(-1)^{n}+{ }^{4} \frac{(2)^{n}}{3} \\
& \Rightarrow\left.S(n)=\frac{5}{3}(-1)^{n}+\frac{4}{3}\right)^{n}
\end{aligned}
$$

39 Using generating function method solve the recurrence relation, $a_{n+2}-2 a_{n+1}+a_{n}=2$ where $\mathrm{n} \geq 0, a_{0}=2$ and $a_{1}=1$.

## Solution:

$$
\begin{aligned}
& a_{n+2}-2 a_{n+1}+a_{n}=2^{n}, a_{0}=2, a_{1}=1 \\
& G(x)=\sum_{n=0}^{\infty} a_{n} x^{n} \\
& \sum_{n=0}^{\infty} a_{n+2} x^{n+2}-2 \sum_{n=0}^{\infty} a_{n+1} x^{n+1}+\sum_{n=0}^{\infty} a_{n} x^{n}=\sum_{n=0}^{\infty} 2^{n} x^{n} \\
& \frac{1}{x^{2}}\left[G(x)-a_{0}-a_{1} x\right]-\frac{2}{x}\left[G(x)-a_{0}\right]+G(x)=1+(2 x)+(2 x)^{2}+\ldots \\
& \frac{1}{x^{2}}[G(x)-2-x]-\frac{2}{x}[G(x)-2]+G(x)=(1-2 x)^{-1} \\
& \frac{[G(x)-2-x]-2 x[G(x)-2]+x^{2} G(x)}{x^{2}}=(1-2 x)^{-1} \\
& G(x)-2-x-2 x G(x)+4 x+x G(x)=\frac{x^{2}}{(1-2 x)} \\
& \left.G(x)\left|\mathrm{C}^{2} \underset{x^{2}}{7-2 x+\frac{1}{⿺}}\right|^{2}+3 x-2=\frac{x^{2}}{(1-2} x\right) \\
& =\frac{x^{2}}{(1-2 x)}+{ }_{2}-3 x
\end{aligned}
$$

$G(x)=\frac{x^{2}+(2-3 x)(1-2 x)}{(1-2 x)(1-x)^{2}}$
$G(x)=\frac{7 x^{2}-7 x+2}{(1-2 x)(1-x)^{2}}$
$G(x)=\frac{7 x^{2}-7 x+2}{(1-2 x)(1-x)^{2}}=\frac{A}{(1-2 x)}+\frac{B}{(1-x)}+\frac{C}{(1-x)^{2}}$
$7 x^{2}-7 x+2=A(1-x)^{2}+B(1-x)(1-2 x)+C(1-2 x)$
Put $x=1 \Rightarrow C=-2$
Put $x=\frac{1}{2} \Rightarrow A=1$
Put $x=0 \Rightarrow B=3$
$G(x)=\frac{7 x^{2}-7 x+2}{(1-2 x)(1-x)^{2}}=\frac{1}{(1-2 x)}+\frac{3}{(1-x)}+\frac{-2}{(1-x)^{2}}$ $=(1-2 x)^{-1}+3(1-x)^{-1}-2(1-x)^{-2}$
$\left.=\left[1+2 x+(2 x)^{2}+\ldots\right]+3\left[1+x+x^{2}+\ldots\right]-2\left[1+2 x+3 x^{2}+\ldots+(n+1) x^{n}\right\rceil\right]$
$a_{n}=2^{n}+3-2(n+1)=2^{n}-2 n+1$
Solve $a_{n}=8 a_{n-1}+10_{n-1}$ with $a=1$ and $a=9$ using generating function.

## Solution:

$$
\begin{aligned}
& a_{n}=8 a_{n-1}+10^{n-1}, a_{0}=1, a_{1}=9 \\
& a_{n}-8 a_{n-1}=10^{n-1} \\
& G(x)=\sum_{n=0}^{\infty} a_{n} x^{n} \\
& \infty \quad \sum_{n=1}^{\infty} a_{n} x^{n}-8 \sum_{n=1}^{\infty} a_{n-1} x^{n}=\sum_{n=1}^{\infty} 10^{n-1} x^{n} \\
& {\left[a_{0}+\sum_{n=1}^{\infty} a_{n} x^{n}-\left.a_{0}\right|_{\mid-8} ^{\Gamma} \sum_{\left\lfloor\sum_{n=1}^{\infty} a_{n-1} x^{n-1}\right.}\right]^{\prime} \mid=x+10 x^{2}+10^{2} x^{3}+\ldots}
\end{aligned}
$$

$$
\begin{aligned}
& \left\lceil\left[G(x)-a_{0}\right] \longmapsto 8 x G(x)=x(1-10 x)^{-1}\right. \\
& G(x)-1-8 x G(x)=x(1-10 x)^{-1} \\
& G(x)[1-8 x]=\frac{x}{(1-10 x)}+1 \\
& =\frac{x+1-10 x}{(1-10 x)} \\
& G(x)=\frac{1-9 x}{(1-10 x)(1-8 x)}=\frac{A}{(1-8 x)}+\frac{B}{(1-10 x)} \\
& 1-9 x=A(1-10 x)+B(1-8 x) \\
& \text { Put } x=\frac{1}{8} \Rightarrow A=\frac{1}{2} \\
& \text { Put } x=\frac{1}{10} \Rightarrow B=\frac{1}{2} \\
& G(x)=\frac{1-9 x}{(1-10 x)(1-8 x)}=\frac{1 / 2}{(1-8 x)}+\frac{1 / 2}{(1-10 x)} \\
& =\frac{1}{2}(1-8 x)^{-1}+\frac{1}{2}(1-10 x)^{-1} \\
& a_{n}=\frac{1}{-\frac{8^{n}}{2}}+\frac{1}{1} 0_{2}^{n}=\frac{1}{8^{n}}\left(+10^{n}\right)
\end{aligned}
$$

# MA8351 - Discrete Mathematics <br> UNIT III - GRAPHS <br> Class Notes 

## Define Graph.

A graph $\mathrm{G}=(\mathrm{V}, \mathrm{E})$ consists of a finite non empty set V , the element of which are the vertices of $G$, and a finite set $E$ of unordered pairs of distinct elements of $V$ called the edges of $G$.


## Defn: Self Loop:

If there is an edge from $\mathrm{V}_{\mathrm{i}}$ to $\mathrm{V}_{\mathrm{j}}$ then that edge is called Self Loop

## Defn: Parallel Edges:

If two edges have same end points then the edges are called Parellel edges.


Edge e6 is called self loop.The edge e3 and e4 are called parallel edges

## Defn:Incident:

If the vertex $\mathrm{V}_{\mathrm{i}}$ is an end vertex of some edge $\mathrm{e}_{\mathrm{k}}$ then $\mathrm{e}_{\mathrm{k}}$ is said to be incident with Vi

## Define simple graph

A graph which has neither self loops nor parallel edges is called a simple graph.


## Defn : Isolated Vertex

A Graph having no edge incident on it is called an isolated vertex

$\mathrm{V}_{5}$ is isolated vertex

## Define Pseudo-graph.

A graph is called a pseudo-graph if it has both parallel edges and self loops.


## Defn :Digraph:

A Graph in which every edge is directed edge is called a Digraph

## Defn Undigraph:

A Graph in which every edge is undirected edge is called a Undirected graph

## Types of Graphs

(i) Complete graph.

A graph of $n$ vertices having each pair of distinct vertices joined by an edge is called a Complete graph and is denoted by $\mathrm{K}_{\mathrm{n}}$.

## (ii) Bipartite Graph

Let $G=(V, E)$ be a graph. $G$ is bipartite graph if its vertex set $V$ can be partitioned into two nonempty disjoint subsets $V_{1}$ and $V_{2}$, called a bipartition, such that each edge has one end in $\mathrm{V}_{1}$ and in $\mathrm{V}_{2}$. For eg $C_{6}$


## (iii) Complete bipartite graph with example

A complete bipartite graph is a bipartite graph with bipartition $V_{1}$ and $V_{2}$ in which each vertex of $V_{1}$ is joined by an edge to each vertex of $V_{2}$. For eg.


## Define Degree of a vertex

The number of edges incident at the vertex $v_{i}$ is called the degree of the vertex with self loops counted twice and it is denoted by $d\left(v_{i}\right)$

## Example:



## Degree of Vertex in Directed Graph:

In a directed graph the in-degree of a vertex V is denoted by degdeg ${ }^{-}(v)$ and defined by the number of edges with V as their terminal vertex. The outer-degree of V is denoted $\operatorname{bydeg}^{+}(v)$,is the number of edges with V as their initial vertex.

How many edges are there in a graph with ten vertices each of degree six.
Let e be the number of edges of the graph

$$
\begin{aligned}
2 \mathrm{e} & =\text { sum of all degrees } \\
& =10 \times 6 \\
& =60 \\
\mathrm{e} & =30
\end{aligned}
$$

Therefore there are 30 edges.

## Define regular graph.

A graph in which each vertex has the same degree is called a regular graph. A regular graph has k - regular if each vertex has degree k .

## Define Subgraph.

A graph $H=\left(V_{1}, E_{1}\right)$ is a subgraph of $G=(V, E)$ provided that $V_{1}, E_{1}$ and for each $e$ $\in E_{1}$, both ends of $e$ are in $V_{1}$.

## 1.Find the subgraph of the following graph by deleting an edge.



Solution:
The subgraph by deleting the edge is shown below


$G-v_{2} v_{3}$


$G-V_{2} V_{5}$

## Define adjacency matrix.

$\mathrm{G}=(\mathrm{V}, \mathrm{E})$ be a graph with n vertices . An " $\mathrm{n} x \mathrm{n}$ " matrix A is an adjacency matrix for G if and only if for $i \leq I, j \leq n, A(i, j)= \begin{cases}{[1} & \text { for }(i, j) \text { in } E \\ 0 & \text { for }(i, j) \text { isnot in } E\end{cases}$
Note :
The adjancy matrix of a simple graph is symmetric (i.e) $a_{i j}=a_{j i}$

## 2.Find the adjacency matrix of the graphs given below


(a)

$$
\left.\mathrm{A}=\left(a_{i j}\right)=\begin{array}{ccccc} 
& v_{1} & v_{2} & v_{3} & v_{4} \\
v_{2} & 0 & 1 & 1 & 0 \\
v_{3} & 1 & 0 & 0 & 1 \\
v_{4} & 0 & 1 & 1 & 0
\end{array}\right]
$$

(b)

$$
\left.\mathrm{A}=\left(a_{i j}\right)=\begin{array}{ccccc}
v_{1} & v_{2} & v_{3} & v_{4} \\
v_{1} & 0 & 1 & 0 & 0 \\
v_{2} & v_{3} & 0 & 0 & 1 \\
0 & 0 \\
1 & 1 & 0 & 0 \\
v_{4} & 0 & 1 & 1 & 0
\end{array}\right]
$$

3.Find the adjacency matrix of the given directed graph.
(i)
(ii)


## Answer:

(i) $\left|\begin{array}{llll}1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0\end{array}\right|$ (ii) $\left|\begin{array}{llllll}0 & 2 & 0 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 1 & 3 & 0\end{array}\right|$

## Defi: Incident Matrices

Let $\mathrm{G}=(\mathrm{V}, \mathrm{E})$ be an undirected graph with ' n ' vertices $\left\{\mathrm{V}_{1}, \mathrm{~V}_{2}, \ldots \mathrm{~V}_{\mathrm{n}}\right\}$
and $m$ edges $\left\{e_{1}, e_{i}, \ldots e\right\}_{\mathrm{m}}$ then $\mathrm{n} \times$ mmatrix $\mathrm{B}=[\mathrm{b}]_{\mathrm{ij}}$ where

$$
\mathrm{B}=\left\{\begin{array}{lc}
1 & \text { when edge } \mathrm{e}_{\mathrm{j}} \text { incidentwith } \mathrm{v}_{\mathrm{j}} \\
0 & \text { otherwise }
\end{array}\right.
$$

For Direct Graph

$$
B_{i j}=\left\{\begin{array}{cc}
1 & e_{j} \text { directed fromv }{ }_{i} \\
-1 & e_{j} \text { directedfromv }{ }_{i} \\
0 & \text { otherwise }
\end{array}\right.
$$

## 4.Find the incidence matrix of



The incidence matrix

$$
\begin{array}{llllllllllll}
e_{1} & e_{2} & e_{3} & e_{4} & e_{5} & e_{6} & e_{7} & e_{8}
\end{array}
$$

$B=\left[b_{i j}\right]=\begin{array}{r}V_{1} \\ V_{2} \\ V_{3} \\ V_{4} \\ V_{5}\end{array}\left[\begin{array}{llllllll}1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0\end{array}\right]$

## Define Graph Isomorphism:

Two graphs $G_{1}$ and $G_{2}$ are said to be Isomorphic to each other if there exists a ono to one ,onto correspondence between the vertex sets which preserves adjacency of the vertices and non adjacency of the vertices

Define Path:
A Path in a Graph is a Sequence $\mathrm{v}_{1}, \mathrm{v}_{2}, \ldots . . \mathrm{v}_{\mathrm{k}}$ of vertices each adjacent to the next.

## Length of the Path:

The number of edges appearing in the sequences of a path is called length of a Path.

## Defn:Cycle or Circuit:

A Path which originates and ends in the same node is called a Cycle or Circuit

## Define Connected graph.

A graph for which each pair of vertices is joined by a trail is connected.

## Define strongly connected graph.

A digraph $G$ is said to be strongly connected if for every pair of vertices, both vertices of the pair are reachable from one another.

## Define Eulerian Path and Eulerian Circuit.

A Path of a Graph G is called an Eulerian Path, if it contains each edge of the group exactly once

A circuit in a graph that includes each edge exactly once, the circuit is called an Eulerian circuit.

## State the condition for Eulerian cycle.

Ans: (i) Starting and ending pts are same.
(ii) Cycle should contain all edges of graph but exactly once

## Define Hamiltonian Path:

A path between two vertices in a Group is Hamiltonian it is passes through each vertex exactly once

## Define : Hamiltonian Cycle:

A Circuit of a graph $G$ is called Hamiltonian circuit if it includes each vertex of $g$ exactly once, except the starting and ending vertices.

## PART-B

## 5.State and prove Handshaking Theorem.

If $\mathrm{G}=(\mathrm{V}, \mathrm{E})$ is an undirected graph with $e$ edges, then $\sum_{i} \operatorname{deg}\left(v_{i}\right)=2 e$

## 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 the $e$ edges contribute ( $2 e$ ) to the sum of the degrees of the vertices.

$$
\text { Hence } \sum_{i} \operatorname{deg}\left(v_{i}\right)=2 e \text {. }
$$

## 6.In any graph show that the number of odd vertices is even.

## Proof:

Let $\mathrm{G}=(\mathrm{V}, \mathrm{E})$ be the undirected graph. Let $v_{1}$ and $v_{2}$ be the set of vertices of G of even and odd degrees respectively. Then by hand shaking theorem,
$2 e=\sum_{v_{i} \in v_{1}} \operatorname{deg}\left(v_{i}\right)+\sum_{v_{j} \in v_{2}} \operatorname{deg}\left(v_{j}\right)$. Since each $\operatorname{deg}\left(v_{i}\right)$ is even, $\sum_{v_{i} \in v_{1}} \operatorname{deg}\left(v_{i}\right)$ is even. Since LHS
is even, we get $\sum_{v_{j} \in v_{2}} \operatorname{deg}\left(v_{j}\right)$ is even. Since each $\operatorname{deg}\left(v_{j}\right)$ is odd, the number of terms

$$
\text { contain in } \sum_{v_{j} \in v_{2}} \operatorname{deg}\left(v_{j}\right)
$$

or $v_{2}$ is even, that is, the number of vertices of odd degree is even.
7.If $G$ is a simple graph with $\delta(G) \geq \frac{|V(G)|}{2}$ then show that $G$ is connected

Solution: let $u$ and $v$ be any 2 distinct vertices
To prove that: u-v path in G
If $u v$ is a edge then $u-v$ is a path in $G$
Suppose uv is not a path in G $\mathrm{X}=\{$ edges adjacent to u$\}$
$\mathrm{Y}=$ set of all edge adjacent to v
$\mathrm{u}, \mathrm{v} \notin X \cup Y$

$$
\begin{gathered}
|X \cup Y| \leq n-2 \\
|X \cup Y| \geq \frac{n}{2}+\frac{n}{2} \geq n-1 \\
\text { Also }|X \cup Y|=|X|+|Y|-X \cap Y \\
\Rightarrow|X \cup Y| \geq 1 \Rightarrow X \cap Y \neq \varphi
\end{gathered}
$$

Therefore $\ni$ a w $\in X \cap Y \Rightarrow$ uvw is a path in $G$
G is connected
8.Prove that the maximum number of edges in a simple graph with $\mathbf{n}$ vertices is $n_{c_{2}}=\frac{n(n-1)}{2}$

## Proof:

We prove this theorem, by the method of mathematical induction. For $n=1$, a graph with 1 vertex has no edges. Therefore the result is true for $\mathrm{n}=1$.
For $\mathrm{n}=2$, a graph with two vertices may have atmost one edge. Therefore $2(2-1)$ / $2=1$.

Hence for $\mathrm{n}=2$, the result is true.
Assume that the result is true for $\mathrm{n}=\mathrm{k}$, i.e, a graph with k vertices has atmost $\frac{k(k-1)}{2}$ edges.

Then for $\mathrm{n}=\mathrm{k}+1$, let G be a graph having n vertices and $\mathrm{G}^{\prime}$ be the graph obtained from G , by deleting one vertex say, ' v ' $\in \mathrm{V}(\mathrm{G})$.

Since $\mathrm{G}^{\prime}$ has k vertices then by the hypothesis, $\mathrm{G}^{\prime}$ has atmost $\frac{k(k-1)}{2}$ edges. Now add the vertex v to $\mathrm{G}^{\prime}$. ' v ' may be adjacent to all the k vertices of $\mathrm{G}^{\prime}$.
Therefore the total number of edges in G are $\frac{k(k-1)}{2}+\mathrm{k}=\frac{k(k+1)}{2}$.
Therefore the result is true for $\mathrm{n}=\mathrm{k}+1$.
Hence, the maximum number of edges in a simple graph with ' n ' vertices is $\frac{n(n-1)}{2}$.
9.Prove that a simple graph with at least two vertices has at least two vertices of same degree.

## Proof:

Let G be a simple graph with $\mathrm{n} \geq 2$ vertices.
The graph G has no loop and parallel edges. Hence the degree of each vertex is $\leq \mathrm{n}-1$.

Suppose that all the vertices of G are of different degrees.
Following degrees $0,1,2, \ldots, n-1$ are possible for $n$ vertices of $G$.
Let $u$ be the vertex with degree 0 . Then $u$ is an isolated vertex.
Let v be the vertex with degree $\mathrm{n}-1$ then v has $\mathrm{n}-1$ adjacent vertices.

Because $v$ is not an adjacent vertex of itself, therefore every vertex of $G$ other than $u$ is an adjacent vertex of G.

Hence u cannot be an isolated vertex, this contradiction proves that simple graph contains two vertices of same degree.
10.If $G$ is a self-complementary graph, then prove that $G$ has $n \equiv 0(\operatorname{or}) \mathbf{1}(\bmod 4)$ vertices

## Proof:

Suppose G is a graph on n-Vertices, then $E(G) \cup E(G)=\{$ The set of all pairs of vertices in $\mathrm{V}(\mathrm{G})$ \}

Let $|E(G)|=|E(G)|=\mathrm{m}$
So,

$$
\begin{gathered}
m+m=\frac{n(n-1)}{2} \\
2 m=\frac{n(n-1)}{2} \\
n(n-1)=4 m
\end{gathered}
$$

Ie., $n(n-1)$ is a multiple of 4 .
$=>$ either n or $\mathrm{n}-1$ is divisible by 4 .
i.e., G is a self-complementary simple graph with n vertices, then $n \equiv$ 0 or $1(\bmod 4)$.

## 11.Prove that a graph $G$ is connected if and only if for any partition of $v$ into

 subsets $V_{1}$ and $V_{2}$ there exists an edge joining a vertex of $V_{1}$ to a vertex of $V_{2}$ Proof:Let G be connected graph and $\mathrm{V}=\mathrm{V}_{1} \cup \mathrm{~V}_{2}$ be a partition of V into two subsets. Let $u \in V_{1}$ and $v \in V_{2}$.

Since the graph G is connected there exists a $u-v$ path in $G$ say $u=v_{0}, v_{1}, v_{2}, \ldots . . v_{n}=v$ Let I be the least positive integer such that $\mathrm{v}_{\mathrm{i}} \in \mathrm{V}_{2}$

Conversely ,suppose for any partition of V into subsets $\mathrm{V}_{1}$ and $\mathrm{V}_{2}$ there is an edge joining a vertex of $\mathrm{V}_{1}$ to a vertex of $\mathrm{V}_{2}$

Assume that G is disconnected .Then there exists at least two components in G.Let $V_{1}$ be the set of all vertices of a component of $G$ and $V_{2}=V(G)-V_{1}$. Then any edge joining one vertex in $\mathrm{V}_{1}$ and one vertex in $\mathrm{V}_{2}$. A contradiction to the hypothesis Hence G is connected
12.If a graph G has exactly two vertices of odd degree, then prove that there is a path joining these two vertices.

## Proof:

Case (i): Let G be connected.
Let $v_{1}$ and $v_{2}$ be the only vertices of $G$ with are of odd degree. But we know that number of odd vertices is even. So clearly there is a path connecting $\mathrm{v}_{1}$ and $\mathrm{v}_{2}$, because G is connected.

Case (ii): Let G be disconnected
Then the components of $G$ are connected. Hence $v_{1}$ and $v_{2}$ should belong to the same component of G. Hence, there is a path between $v_{1}$ and $v_{2}$.

## 13.If all the vertices of an undirected graph are each of degree $k$, show that the number of edges of the graph is a multiple of $k$.

proof : Let $2 n$ be the number of vertices of the given graph....(1)
Let $n_{e}$ be the number of edges of the given graph.
By Handshaking theorem, we have

$$
\begin{align*}
& \sum_{i=1}^{2 n} \operatorname{deg} v_{i}=2 n_{e} \\
& 2 n k=2 n_{e}  \tag{1}\\
& n_{e}=n k
\end{align*}
$$

Number of edges =multiple of $k$.
Hence the number of edges of the graph is a multiple of k

## 14. Show that a simple graph $G$ with $\boldsymbol{n}$ vertices is connected if it has more than

 $\frac{(n-1)(n-2)}{2}$ edges
## Proof:

Suppose G is not connected. Then it has a component of $k$ vertices for some $k$,
The most edges G could have is

$$
\begin{aligned}
C(k, 2)+C(n-k, 2) & =\frac{k(k-1)+(n-k)(n-k-1)}{2} \\
& =k^{2}-n k+\frac{n^{2}-n}{2}
\end{aligned}
$$

This quadratic function of f is minimized at $\mathrm{k}=\mathrm{n} / 2$ and maximized at $\mathrm{k}=1$ or $\mathrm{k}=\mathrm{n}-1$

Hence, if G is not connected, then the number of edges does not exceed the value of this function at 1 and at $\mathrm{n}-1$, namely $\frac{(n-1)(\mathrm{n}-2)}{2}$.

## 15.Prove that a simple graph with $n$ vertices and $k$ components can have at

 most $\frac{(\mathrm{n}-\mathrm{k})(\mathrm{n}-\mathrm{k}+1)}{2}$ edges.
## Proof:

Let the number of vertices of the ith component of G be $n_{i}, n_{i} \geq 1$..

$$
\sum_{i=1}^{k} n_{i}=n \Rightarrow \sum_{i=1}^{k}\left(n_{i}-1\right)=(n-k)
$$

Then $\Rightarrow\left(\sum_{i=1}^{k}\left(n_{i}-1\right)\right)^{2}=n \geq 2 n k+k_{2}$
that is $\sum\left(n_{i}-1\right)_{2} \leq n_{2}-2 n k+k_{2} \Rightarrow \sum n_{i_{2}} \leq n_{2}-2 n k+k_{2}+2 n-k$
$i=1$
$i=1$
Now the maximum number of edges in the ith component of $G=$

$$
\begin{aligned}
& \frac{n_{i}\left(n_{i}-1\right)}{2}=\frac{1}{2} \sum_{i=1}^{k} n_{i}^{2}-\frac{n}{2} \\
& \leq \frac{\left(n^{2}-2 n k+k+2 n-k\right)}{2} n^{2} \frac{(n-k)(n-k+1)}{2}
\end{aligned}
$$

## 16.Determine whether the graphs below are Isomorphic or not



## Solution:

The graphs $G$ and $G^{\prime}$ both have eight vertices and ten edges
In $G$, degree $(a)=2$.
Since each of the vertices $v_{2}, V_{3}, v_{6}$ and $v_{7}$ is of deg 2 in $G^{\prime}$
Therefore, $a$ in $G$ must correspond to either $v_{2}, v_{3}, v_{6}$ and $v_{7}$ of $G^{\prime}$
Each of the vertices $v_{2}, v_{3}, v_{6}$ and $v_{7}$ in $G^{\prime}$ are adjacent to another vertex of degree 2 in $\mathrm{G}^{\prime}$, which is not true for a in $G$

Therefore G and G' are not isomorphic
17.Define isomorphism between two graphs. Are the simple graphs with the following adjacency matrices isomorphic?

$$
\left[\left.\begin{array}{llllll}
0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 \\
\mid 1 & 0 & 1 & 0 & 1 & 0
\end{array} \right\rvert\,\right.
$$

$\left[\left.\begin{array}{llllll}0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ \lfloor 1 & 1 & 0 & 0 & 1 & 0\end{array} \right\rvert\,\right.$

## Answer:

Two graphs $\mathrm{G}_{1}=\left(\mathrm{V}_{1}, \mathrm{E}_{1}\right)$ and $\mathrm{G}_{2}=\left(\mathrm{V}_{2}, \mathrm{E}_{2}\right)$ are the same or isomorphic, if there is a bijection
$F: V_{1} \rightarrow V_{2}$ such that $(u, v) \in E_{1}$ if and only if $(F(u), F(v)) \in E_{2}$.


The given two graphs have
i) Same number of vertices - 6
ii) Same number of edges -8

Moreover, in the given diagram $u_{2}, u_{3}, u_{5}, u_{6}$ are of degree 3 each, $u_{1}, u_{4}$ are degree 2 .
Similarly $v_{2}, v_{3}, v_{5}, v_{6}$ are of degree 3 each, $v_{1}, v_{4}$ are of degree 2 .
Therefore the given two graphs are isomorphic.
18.Establish the isomorphic for the following graphs


## Solution:



| $\mathrm{G}_{1}$ | $\mathrm{G}_{2}$ |
| :---: | :---: |
| $\mathbf{V}\left(\mathbf{G}_{1}\right)=\left\{\mathbf{U}_{1}, \mathbf{U}_{\mathbf{2}}, \mathbf{U}_{\mathbf{3}}, \mathbf{U}_{4}, \mathbf{U}_{\mathbf{5}}\right\}$ | $\mathbf{V}\left(\mathbf{G}_{2}\right)=\left\{\mathbf{V}_{1}, \mathbf{V}_{2}, \mathbf{V}_{3}, \mathbf{V}_{4}, \mathbf{V}_{5}\right\}$ |
| $\operatorname{Deg}\left(\mathrm{U}_{1}\right)=2$ | $\operatorname{Deg}\left(\mathrm{V}_{1}\right)=2$ |
| $\operatorname{Deg}\left(\mathrm{U}_{2}\right)=2$ | $\operatorname{Deg}\left(\mathrm{V}_{2}\right)=2$ |
| $\operatorname{Deg}\left(\mathrm{U}_{3}\right)=2$ | $\operatorname{Deg}\left(\mathrm{V}_{3}\right)=2$ |
| $\operatorname{Deg}\left(\mathrm{U}_{4}\right)=2$ | $\operatorname{Deg}\left(\mathrm{V}_{4}\right)=2$ |
| $\operatorname{Deg}\left(\mathrm{U}_{5}\right)=2$ | $\operatorname{Deg}\left(\mathrm{V}_{5}\right)=2$ |

The Mapping is $\varphi: G_{1} \rightarrow G_{2}$

$$
\varphi\left(U_{1}\right)=V_{1}, \varphi\left(U_{2}\right)=V_{3}, \varphi\left(U_{3}\right)=V_{5}, \varphi\left(U_{4}\right)=V_{2}, \varphi\left(U_{5}\right)=V_{4}
$$

$\therefore$ The Mapping $\mathrm{G}_{1}$ and $\mathrm{G}_{2}$ are isomorphic.
19. Determine whether the following pairs of graph $G$ and $H$ are isomorphic


## Solution:

Both the graph G and H have
(1) Same number of vertices (6)
(2) Same number of edges (7)

If $f: u \rightarrow v$ is defined as
$\mathrm{u}_{1} \rightarrow \mathrm{v}_{2}$
$\mathrm{u}_{2} \rightarrow \mathrm{~V}_{3}$
$\mathrm{u}_{3} \rightarrow \mathrm{v}_{4}$
$\mathrm{u}_{4} \rightarrow \mathrm{v}_{1}$
$\mathrm{u}_{5} \rightarrow \mathrm{v}_{5}$
$\mathrm{u}_{6} \rightarrow \mathrm{v}_{6}$
Then the adjacency is preserved
$\therefore$ Given 2 graphs G and H are isomorphic.
20.Prove that a given connected graph $G$ is Euler graph if and only if all vertices of $\mathbf{G}$ are of even degree.

## Answer:

Suppose G is an Euler graph.
$\Rightarrow G$ contains an Euler line
$\Rightarrow \mathrm{G}$ contains a closed walk covering all edges.
To prove:
All vertices of G is of even degree.

In training the closed walk, every time the walk meets a vertex v , it goes through two new edges incident on V with one we 'entered ' and other 'exited'. This is true, for all vertices, because it is a closed walk. Thus the degree of every vertex is even. Conversely, suppose that all vertices of G are of even degree.

To prove:
G is an Euler graph.
(i.e) to prove : G contains an Euler line.

Construct a closed walk starting at an arbitrary vertex vand going through the edge of $G$ such that no edge is repeated. Because, each vertex is of even degree, we can exit from each end, every vertex where we enter, the tracing can stop only at the vertex $v$. Name the closed walk as $h$

Case (i) If h covers all edges of G , then h becomes an Euler line, and hence, G is an Euler graph.

Case (ii) If $h$ does not cover all edges of $G$ then remove all edges of $h$ from $g$ and obtain the remaining graph $G$ '. Because both $G$ and $G$ ' have all their vertex of even degree.
$\Rightarrow$ Every vertex in $\mathrm{G}^{\text {' }}$ is also of even degree.
Since G is connected, h will touch G ' atleast one vertex v'. Starting from v', we can again construct a new walk $h$ ' in $\mathrm{G}^{\text {' }}$. This will terminate only at v ', because, every vertex in $G$ ' is also of even degree.

Now, this walk h' combined with h forms a closed walk starts and ends at v and has more edges than $h$. This process is repeated until we obtain a closed walk covering all edges of G. Thus G is an Euler graph.
21. If $\mathbf{G}$ is a connected simple graph with $\mathbf{n}$ vertices with $\boldsymbol{n} \geq \mathbf{3}$, such that the degree of every vertex in $G$ is at least $n / 2$, then prove that $G$ has Hamilton cycle

## Answer:

We prove this theorem by contradiction. Suppose that the theorem is false and let G be a non-Hamiltonian simple graph with $n \geq 3$, G cannot be complete. Let u and $v$ be non-adjacent vertices in G. By choice of G, G+uv is Hamiltonian simple graph with $n \geq 3$ and $\delta \geq^{n} \frac{}{2}$
Moreover, since G is non-Hamiltonian, each Hamiltonian cycle of G+uv must contain the edges uv. Thus there is a Hamilton path $v_{1}, v_{2}, \cdots \cdots, v_{n}$ in G with origin $v=v_{1}$ and $v=v_{n}$.

Let,
$S=\left\{v_{i} / u v_{i+1} \in E\right\}$
$T=\left\{v_{i} / v_{i} v \in E\right\}$
Since

$$
v_{n} \notin S \cup T \text {, wehave }
$$

$|S \cup T|<n$ and $|S \cap T|=0$
Since if $S \cap T$ contained some vertex $v_{i}$, then G would have the Hamiltonian cycle $v_{1}, v_{2}, \cdots v_{i} v_{n} v_{n-1}, v_{i} \cdots v_{1}$ which is a contradiction.

Also, $d(u)+d(v) \neq \$+|T|=|S \cup T|+|S \cap T|<n$
But this contradicts the hypothesis $\boldsymbol{\delta} \geq^{n}$. Hence the theorem.
22. Show that the complete bipartite graph $K_{m, n}$ with $m, n \geq \mathbf{2}$ is Hamiltonian if and only if $\mathbf{m}=\mathbf{n}$.Also prove that the complete graph $K_{n}$ is hamiltonian for all $\mathrm{n} \geq 3$

## Proof:

Assume $\mathrm{m} \neq n$
Let H be a Hamiltonian cycle that goes through every vertex in $\mathrm{K}_{\mathrm{m}, \mathrm{n}}$

$$
\mathrm{H}=\mathrm{v}_{0} \mathrm{e}_{0} \mathrm{v}_{1} \mathrm{e}_{1}
$$

Since $\mathrm{K}_{\mathrm{m}, \mathrm{n}}$ is bipartite the cycle must alternate between the vertex on each side.
Since $\mathrm{m} \neq n$ thereexist a $\mathrm{v}_{\mathrm{a}}=\mathrm{v}_{\mathrm{b}} \mathrm{a}<\mathrm{b}$ inside cycle H
Which is a contradiction
Hence complete bipartite graph $\mathrm{K}_{\mathrm{m}, \mathrm{n}}$ has a hamiltonian cycle iff $\mathrm{m}=\mathrm{n}$
To prove that $\mathrm{k}_{\mathrm{n}}$ is Hamiltonian
Let $u$ be any vertex of $\mathrm{k}_{\mathrm{n}}$
Since $\mathrm{k}_{\mathrm{n}}$ is a complete graph, any 2 vertex can be joined
So we start from $u$ and visit vertices in any order exactly once and come back to $u$ Hence there is a Hamiltonian cycle in $\mathrm{k}_{\mathrm{n}}$
23.Let $G$ be a simple indirected graph with $n$ vertices. Let $u$ and $v$ be two non adjacent vertices in $\mathbf{G}$ such that $\operatorname{deg}(\mathbf{u})+\operatorname{deg}(\mathbf{v}) \geq \mathbf{n}$ in $\mathbf{G}$. Show that $\mathbf{G}$ is Hamiltonian if and only if $\mathbf{G}+\mathbf{u v}$ is Hamiltonian.

## Solution:

If G is Hamiltonian, then obviously $\mathrm{G}+\mathrm{uv}$ is also Hamiltonian.
Conversely, suppose that $\mathrm{G}+\mathrm{uv}$ is Hamiltonian, but G is not. Then by Dirac theorem, we have

$$
\operatorname{deg}(u)+\operatorname{deg}(v)<n
$$

which is a contradiction to our assumption.
Thus $G+u v$ is Hamiltonian implies $G$ is Hamiltonian.
24.If $\mathbf{G}$ is a connected simple graph with $\mathbf{n}$ vertices $(\mathbf{n} \geq 3)$ and if the degree of each vertex is atleast ${ }_{2}^{2}$, then show that $G$ is Hamiltonian

## Solution:

Suppose that the theorem is false, and let G be a maximal non Hamiltonian simple graph with $\mathrm{n} \geq 3$ and the degree of each vertex is atleast ${ }_{2}$. Since $\mathrm{n} \geq 3$, G cannot be complete.

Let $u$ and $v$ be non adjacent vertices in G,Since $G$ is the maximal NonHamiltonian, $\mathrm{G}+\mathrm{uv}$ is Hamiltonion ,each Hamilton cycle of G+uv must contain the edge uv.

Thus there is a Hamilton path $v_{1} v_{2} \ldots . . v_{n}$ in $G$ with origin $u=v_{i}$ and terminus $v=$ $\mathrm{V}_{\mathrm{n}}$

Let $\mathrm{S}=\{v i \in V(G) /\langle u, v i+1\rangle \in E(G)$
And $\mathrm{T}=\{v i \in V(G) /\langle v i, v\rangle \in E(G)$ where $\mathrm{i}=1$ to n
Since $\mathrm{v}_{\mathrm{n}} \notin \mathrm{S} \cup \mathrm{T}$ we have $|\mathrm{S} \cup \mathrm{T}|<n$ and $|\mathrm{S} \cup \mathrm{T}|=0$
Since if $S \cap T$ contains some vertex $v_{i}$, then $G$ would have the Hamilton cycle $v_{1}$ $\mathrm{V}_{2} \ldots . ., \mathrm{V}_{\mathrm{n}} \mathrm{V}_{\mathrm{n}-1} \mathrm{~V}_{\mathrm{i}+1} \mathrm{~V}_{1}$,
which is a contradiction to the assumption(fig)
Since $|\mathrm{S} \cup \mathrm{T}|<n$ and $|\mathrm{S} \cap \mathrm{T}|=0$
we get $\mathrm{d}(\mathrm{u})+\mathrm{d}(\mathrm{v})=|S|+|T|=|\mathrm{S} \cup \mathrm{T}|+|\mathrm{S} \cap \mathrm{T}|<n$
This also contradicts the hypothesis that the degree of the vertex is atleast $\frac{n}{2}$

25. Show that $K_{n}$ has a Hamiltonion cycle, for $\mathbf{n}>3$, what is the maximum number of edge disjoint Hamilton cycles possible in $K_{n}$. Obtain all the edge disjoint .Hamilton cycles in K7.

## Solution:

Each Hamilton cycle in $\mathrm{K}_{\mathrm{n}}$ consists of n edges. As $\mathrm{K}_{\mathrm{n}}$ has $\frac{n(n-1)}{2}$ edges, $\mathrm{K}_{\mathrm{n}}$ can have atmost $\frac{n-1}{2}$ edge-disjoint Hamilton cycles.

So it is enough to exhibit $\frac{n-1}{2}$ edge disjoint Hamilton cycles in $K_{n}$
W.K.T If $\mathrm{n} \geq 3$ is odd integer, then the complete graph $\mathrm{K}_{\mathrm{n}}$ contains $\frac{n-1}{2}$ edge disjoint Hamilton cycles


## 26.If $G$ is a connected simple graph with $n$ vertices with $n \geq 3$, such that the degree of every vertex in $\mathbf{G}$ is at least $n / 2$, then prove that $\mathbf{G}$ has Hamilton cycle

## Solution :

We prove this theorem by contradiction. Suppose that the theorem is false and let $G$ be a non-Hamiltonian simple graph with $n \geq 3$, $G$ cannot be complete. Let $u$ and v be non-adjacent vertices in G. By choice of G, G+uv is Hamiltonian simple graph with $n \geq 3$ and $\geq^{n} \frac{\overline{2}}{}$

Moreover, since G is non-Hamiltonian, each Hamiltonian cycle of G+uv must contain the edges uv. Thus there is a Hamilton path $v_{1}, v_{2}, \cdots \cdots, v_{n}$ in G with origin $v=v_{1}$ and $v=v_{n}$.

Let,
$S=\left\{v_{i} / u v_{i+1} \in E\right\}$
$T=\left\{v_{i} / v_{i} v \in E\right\}$
Since
$v_{n} \notin S \cup T$, wehave
$|S \cup T|<n$ and $\mid S \cap T \equiv 0$
Since if $S \cap T$ contained some vertex $v_{i}$, then G would have the Hamiltonian cycle $v_{1}, v_{2}, \cdots v_{i} v_{n} v_{n-1}, v_{i} \cdots v_{1}$ which is a contradiction.

Also, $d(u)+d(v) \neq S+|T|=|S \cup T|+|S \cap T|<n$
But this contradicts the hypothesis $\delta \geq \frac{\boldsymbol{n}}{2}$.

## Hence the theorem.

# UNIT IV - ALGEBRAIC STRUCTURES CLASS NOTES 

## Definition: Algebraic Structure (or) Algebraic system:

A non-empty set G together with one or more $n$-aryoperations say * (binary) is called an algebraic system or algebraic structure.

Example: Some binary operations are $+,-,{ }^{*}, /, \cup, \cap$.

## Properties of Binary operations:

(i) Closure: $\quad a * b=x \in G, \quad$ for all $a, b \in G$
(ii) Commutative: $a * b=b * a \quad$ for all $a, b \in G$
(iii) Associative: $(a * b) * c=a *(b * c) \quad$ for all $a, b \in G$
(iv) Identity: $\quad a * e=e * a=a \quad$ for all $a, e \in G, e$ is called identityelement.
(v) Inverse: $a * b=b * a=e$ (identity) $b$ is called inverse of 'a'and is denoted by $b=a^{-1}$.
(vi) Distributive property: $a \cdot(b \cdot c)=(a \cdot b) \cdot(a \cdot c) \quad$ left distributive
$(b \cdot c) \cdot a=(b \cdot a) \cdot(c \cdot a) \quad$ right distributive for all $a, b, c \in G$
(vii) Cancellation property: $a * b=a * c \Rightarrow b=c$ (left cancellation)
$b * a=c * a \Rightarrow b=c \quad$ (right cancellation) for all $a, b, c \in G$.
Example: ( $\mathrm{Z},+$ ) is an algebraic system.
Algebraic structures include groups, rings, fields, and lattices.

## Note:

Z - the set of all integers
Q - the set of all rational numbers
R - the set of all real numbers
C - the set of all complex numbers
$\mathrm{R}^{+}$- the set of all positive real numbers
$\mathrm{Q}^{+}$- the set of all positive rational numbers.

## Definition: Semi Group

Let S be non empty set, * be a binary operation on S . The algebraic system $(\mathrm{S}, *)$ is called a semi group, if the operation is associative.

In other words ( $\mathrm{S},{ }^{*}$ ) is a semi group if for any $\mathrm{x}, \mathrm{y}, \mathrm{z} \in \mathrm{S}$,

$$
x^{*}(y * z)=\left(x^{*} y\right)^{*} z .
$$

Examples : (Set of integers, +), and (Matrix ,*) are examples of semigroup.

## Definition: Monoid

A semi group ( $\mathrm{M},{ }^{*}$ ) with identity element with respect to the operation * is called a Monoid. In other words $\left(M,{ }^{*}\right)$ is a Monoid if for any $\mathrm{x}, \mathrm{y}, \mathrm{z} \in \mathrm{M}, \mathrm{x} *(\mathrm{y} * \mathrm{z})=(\mathrm{x} * \mathrm{y}) * \mathrm{z}$ and there exists an element $e \in M$ such that for any $x \in M$ then $e * x=x * e=x$.

## Examples :

$>\left(\right.$ Set of integers, $\left.{ }^{*}\right)$ is Monoid as 1 is an integer which is also identity element .
(Set of natural numbers, + ) is not Monoid as there doesn't exist any identity element. But this is Semigroup.
$>($ Set of whole numbers, + ) is Monoid with 0 as identity element.

## Definition: Group

An algebraic system (G,*) is called a group if it satisfies the following properties:
(i) $\quad *$ is associative.
(ii) Identity element exists.
(iii) Inverse element exists.

Note: 1. A group is always a monoid, semigroup, and algebraic structure.
2. ( $\mathrm{Z},+$ ) and Matrix multiplication are examples of groups.

## Definition: Abelian Group

In a group $(\mathrm{G}, *)$, if $\mathrm{a} * \mathrm{~b}=\mathrm{b} * \mathrm{a}$, for all $\mathrm{a}, \mathrm{b}$ in G then the group is called an abelian group.
Examples: $(\mathrm{Z},+$ ) is a example of Abelian Group but Matrix multiplication is not abelian group as it is not commutative.

## Problems

1. Show that the set $\mathbf{N}$ of natural numbers is a semigroup under the operation $x^{*} \mathbf{y}=\boldsymbol{\operatorname { m a x }}\{\mathbf{x}, \mathbf{y}\}$. Is it a Monoid?

Proof:
Closure: Let $\mathrm{x}, \mathrm{y} \in \mathrm{N}$ then

$$
\begin{gathered}
x * y=\max \{x, y\}=x, \text { if } x>y \\
\& \max \{x, y\}=y, \text { if } x<y
\end{gathered}
$$

In both cases, x or $\mathrm{y} \in \mathrm{N}$.
Hence $x * y \in N$
Hence closure is true.
Associative: Let $\mathrm{x}, \mathrm{y}, \mathrm{z} \in \mathrm{N}$

$$
\begin{aligned}
\operatorname{Now}(\mathrm{x} * \mathrm{y}) * \mathrm{z} & =\max \{\mathrm{x}, \mathrm{y}\} *, \mathrm{z} \\
& =\max \{\max \{\mathrm{x}, \mathrm{y}\}, \mathrm{z}\} \\
& =\max \{\mathrm{x}, \mathrm{y}, \mathrm{z}\} \ldots(1)
\end{aligned}
$$

$$
\begin{aligned}
\text { Now } x *(y * z)= & x * \max \{y, z) \\
& =\max (x, \max \{y, z\}\} \\
& =\max \{x, y, z\} \ldots(2)
\end{aligned}
$$

From (1) and (2), ( $x * y$ ) ${ }^{2}=x *(y * z)$
Hence N is associative.
Identity: $\mathrm{e}=1$ is the element in N such that

$$
\mathrm{x} * \mathrm{e}=\mathrm{e}^{*} \mathrm{x}=\mathrm{x}
$$

Hence ( $\mathrm{N},{ }^{*}, 1$ ) is Monoid.
2. Give an example of a semigroup that is not a monoid. Further prove that for any commutative monoid ( $M$, *), the set of idempotent elements of $M$ form a submonoid.

## Solution:

Example of a semigroup that is not a monoid:
(Set of natural numbers, + ) is not Monoid as there doesn't exist any identity element. But this is Semigroup.

Let ( $\mathrm{M}, *$ ) be a commutative monoid.
Let $S=\{a \in M / a * a=a\}$, the set of idempotent elements of M.
Clearly $e \in S$, as $e * e=e$

Let $a, b \in S$ with $a * a=a$ and $b * b=b$
Now, $(a * b) *(a * b)=(a *(b * b) * a=a * b * a=a * a * b=a * b$
Hence $a * b \in S$
$\therefore\left(S,{ }^{*}\right)$ is a submonoid of $\left(M,{ }^{*}\right)$.
3. Let $(\mathbf{S}, *)$ be a semigroup such that for $x, y \in S, x^{*} x=y$, where $s=\{x, y\}$.
$\operatorname{Pr}$ ove that (1) $x * y=y * x(2) y * y=y$

## Proof:

Since $(\mathrm{S}, *)$ is a semi group, closure property and associative property are true under *
Given $\mathrm{x} * \mathrm{x}=\mathrm{y}$
Now $x *(x * x)=(x * x) * x$
[Associative property]
$x * y=y * x$
$[\operatorname{From}(1)]$
We have $\mathrm{S}=\{x, y\}$.
Since closure property is true under * and $\mathrm{S}=\{\mathrm{x}, \mathrm{y}\}$,

$$
\begin{equation*}
x * y=x \text { or } x * y=y \tag{2}
\end{equation*}
$$

Assume x * $\mathrm{y}=\mathrm{x}$.
From (i), $x * y=y * x$.

$$
\begin{align*}
y * y & =y *(x * x)  \tag{1}\\
& =(y * x) * x \\
& =(x * y) * x \\
& =\mathrm{x} * \mathrm{x} \\
& =\mathrm{y}
\end{align*}
$$

(By Associative Property)
[ From (3)]
[From(2)]
[From (1)]
Assume x * $\mathrm{y}=\mathrm{y}$.

$$
\begin{array}{rlrl}
y * y & =(x * x) * y & & {[\text { From (1)] }}  \tag{4}\\
& =x *(x * y) & \quad(\text { By Associative Property })
\end{array}
$$

$$
\begin{equation*}
=x * y \tag{From4}
\end{equation*}
$$

$$
=\mathrm{y}
$$

$\therefore y^{*} y=y$
4. Show that $\left(\mathbf{Q}^{+}, *\right)$ is an abelian group where $*$ is defined as $a * b=\frac{a b}{2}$ for all $\mathbf{a}, \mathbf{b} \in \mathbf{Q}^{+}$

## Proof:

$\mathrm{Q}^{+}$is the set of all positive rational numbers.
To prove: $\left(\mathrm{Q}^{+}, *\right)$ is an abelian
i.e, to prove: (i) Closure
(ii) Associative
(iii) Identity
(iv) Inverse
(v) Commutativity
(i) Closure : Let $\mathrm{a}, \mathrm{b} \in \mathrm{Q}^{+}$

$$
\text { Now } a * b=\frac{a b}{2} \in \mathrm{Q}
$$

(ii) Associative: : Let $\mathrm{a}, \mathrm{b}, \mathrm{c} \in \mathrm{Q}^{+}$then

$$
\begin{aligned}
& (a * b) * c=\frac{a b}{2} * c=\frac{(a b)}{2} c=\frac{a b c}{4} \\
& a *(b * c)=a * \frac{b c}{2}=\frac{a\left(\frac{b c}{2}\right)}{2}=\frac{a b c}{4} \\
& \therefore(a * b) * c=a *(b * c)
\end{aligned}
$$

(iii) Identity: $a * e=a \Rightarrow \frac{a e}{2}=a \Rightarrow e=2 \in Q^{+}$

Therefore $\mathrm{e}=2$ is the identity element.
(iv) Inverse: Let ' $a$ ' ${ }^{-1}$ be the inverse element of ' $a$ '.

$$
a * a^{-1}=e \Rightarrow \frac{a a^{-1}}{2}=2 \Rightarrow a^{-1}=\frac{4}{a} \in Q^{+}
$$

(v) Commutativity: $a * b=\frac{a b}{2}=\frac{b a}{2}=b * a$

Hence $\left(\mathrm{Q}^{+},{ }^{*}\right)$ is an abelian group
 multiplication.
(Nov/Dec 2015)
Proof:

$$
\text { Let } \left.I=\left[\begin{array}{ll}
1 & 0 \\
0 & 1
\end{array}\right], A=\left[\begin{array}{cc}
-1 & 0 \\
0 & 1
\end{array} \left\lvert\,, B=\begin{array}{cc}
1 & 0 \\
0 & -1
\end{array}\right.\right\rceil \text { and } C=\begin{array}{cc}
\lceil-1 & 0 \\
0 & -1 \\
\hline
\end{array}\right]
$$

The matrix multiplication table is,

| $\times$ | $I$ | $A$ | $B$ | $C$ |
| :--- | :--- | :--- | :--- | :--- |
| $I$ | $I$ | $A$ | $B$ | $C$ |
| $A$ | $A$ | $I$ | $C$ | $B$ |
| $B$ | $B$ | $C$ | $I$ | $A$ |
| $C$ | $C$ | $B$ | $A$ | $I$ |

Claim 1: Closure property
Since all the elements inside the table are the elements of G.
Hence G is closed under multiplication.
Claim 2: Associative property
We know that matrix multiplication is always associative
Claim 3: Identity property
From the above table we observe that the matrix $I \in G$ is the Identity matrix.
Claim 4: Inverse property
From the above table we observe that all the matrices are inverse to each other.
Hence Inverse element exists.
Claim 5: Commutative property
From the table we have

$$
A \times B=C=B \times A,
$$

$$
\begin{aligned}
& A \times C=B=C \times A, \\
& B \times C=A=C \times B
\end{aligned}
$$

Therefore commutative property exists.
Hence G forms an abelian group under matrix multiplication.
6. Prove that $G=\{[1],[2],[3],[4]\}$ is an abelian group under multiplication modulo5. Proof: For finite set, weuse Cayley table.

| $\times_{5}$ | $[1]$ | $[2]$ | $[3]$ | $[4]$ |
| :--- | :--- | :--- | :--- | :--- |
| $[1]$ | $[1]$ | $[2]$ | $[3]$ | $[4]$ |
| $[2]$ | $[2]$ | $[4]$ | $[1]$ | $[3]$ |
| $[3]$ | $[3]$ | $[1]$ | $[4]$ | $[2]$ |
| $[4]$ | $[4]$ | $[3]$ | $[2]$ | $[1]$ |

(i) Closure property

$$
\forall[a],[b] \in G \Rightarrow[a] \times_{5}[b] \in G
$$

Clearly from the Cayley table, G is closed under $\times_{5}$.
(ii) Associative property: $[a] \times_{5}\left([b] \times{ }_{S}[c]\right)=\left([a] \times_{5}[b]\right) \times_{5}[c], \quad \forall[a],[b],[c] \in G$

In multiplication, associayive property is true.
Hence the binary operation $\times_{5}$ is associative.
(iii) Existence of Identity: From the table, we get the identity element $e=[1] \in G$
(iv) Existence of Inverse:

From the table, we get
Inverse of [1]= [1]
Inverse of [2]= [3]
Inverse of [3]= [2]
Inverse of [4]= [4]

Hence ( $G, \times_{5}$ ) is a group.
Also it is clear that $[a] \times_{5}[b]=[b] \times_{5}[a], \quad \forall[a],[b] \in G$
Therefore commutative law is true under $\times_{5}$
Hence the binary operation $\times_{5}$ is commutative.
Therefore ( $\mathrm{G}, \times_{5}$ ) is an abelian group.
7. Prove that every finite group of order $\mathbf{n}$ is isomorphic to a permutation group of degree $\mathbf{n}$.

## Proof:

Let $G$ be a finite group of order $n$.
Let $\mathrm{a} \in \mathrm{G}$
Define $f_{a}: G \rightarrow G$ by $f_{a}(x)=f_{a}(y)$

Since $f_{a}(x)=f_{a}(y) \Rightarrow x=y$
$\Rightarrow f_{a}$ is $1-1$.

Since, if $\mathrm{y} \in \mathrm{G}$, then $f_{a}\left(a^{\prime} y\right)=y$
$\Rightarrow f_{a} i s 1-1$.
$\Rightarrow f_{a}$ is a bijection.

Since G has n elements, $f_{a}$ is just permutation on n symbols.
Let $G^{\prime}=\left\{f_{a} / a \in G\right\}$
To Prove: $G^{\prime}$ is a group.
Let $f_{a}, f_{b} \in G^{\prime}$
$\Rightarrow f_{a} \circ f_{b}(x)=f_{a}\left(f_{b}(x)\right)=f_{a}(b x)=a b x=f_{a b}(x)$
$\Rightarrow G^{\prime}$ is closed .
Associative condition holds obviously.
$f_{a}$ in $G^{\prime}$ is the identity element.

The inverse of $f_{a}$ in $G^{\prime}$ is $f_{a}$
Hence $G^{\prime}$ is a group.
To Prove: $G$ and $G^{\prime}$ are isomorphic.
Define $\phi: G \rightarrow G^{\prime}$ by $\phi(a)=f_{a}$
$\phi(a)=\phi(b) \Rightarrow f_{a}=f_{b} \Rightarrow f_{a}(x)=f_{b}(x) \Rightarrow a x=b x \Rightarrow a=b$
Hence $\phi$ is 1-1.
Since $f_{a}$ is onto, $\phi$ is onto.
Also $\phi(a b)=f_{a b}=\phi(a) \circ \phi(b)$
$\therefore \phi: G \rightarrow G^{\prime}$ is an isomorphism.
$\Rightarrow G \cong G^{\prime}$
8. Let $\mathbf{G}$ be a group. Prove that $(\mathbf{a} * \mathbf{b})^{-1}=b^{-1} * \mathbf{a}^{-1}$ for all $\mathbf{a}, \mathbf{b}$ in $\mathbf{G}$.
(or) In a group, prove that the inverse of the product of two elements is equal to the product of their inverses in reverse order.

## Proof:

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

$$
\begin{aligned}
& a * a^{-1}=a^{-1} * a=e \\
& b * b^{-1}=b^{-1} * b=e \quad \text { (identity property). }
\end{aligned}
$$

$\operatorname{Now}(\mathrm{a} * \mathrm{~b}) *\left(\mathrm{~b}^{-1} * \mathrm{a}^{-1}\right)=\mathrm{a} *\left(\mathrm{~b} *\left(\mathrm{~b}^{-1} * \mathrm{a}^{-1}\right)\right) \quad(*$ is associative $)$

$$
\begin{align*}
& =a *\left(b * b^{-1}\right) * a^{-1} \\
& =a *\left(e * a^{-1}\right) \\
& =a * a^{-1}=e \quad \ldots .(1 \tag{1}
\end{align*}
$$

Similarly we can prove that $\left(b^{-1} * a^{-1}\right) *(a * b)=e$.
From (1) and (2) we have $(a * b)^{-1}=b^{-1} * a^{-1}$
9. Prove that $(\mathbf{G}, *)$ is an abelian group if and only if $(\mathbf{a} * \mathbf{b})^{2}=\mathbf{a}^{2} * \mathbf{b}^{2}$

## Proof:

Let G be an abelian group.
$\operatorname{Now}(a * b)^{2}=(a * b) *(a * b)$

$$
\begin{array}{ll}
=a *(b * a) * b & \text { (Associative law) } \\
=a *(a * b) * b & \\
=(a * a) *(b * b) & \text { (Associative law) } \\
=a^{2} * b^{2} . &
\end{array}
$$

Conversely, let $(a * b)^{2}=a^{2} * b^{2}$

$$
\begin{aligned}
\left(a^{*} b\right) *\left(a^{*} b\right) & =(a * a) *(b * b) \\
a^{*}(b * a) * b & =a *(a * b) * b(\text { Associative law })
\end{aligned}
$$

By applying left and right cancellation law we get $\mathrm{b} * \mathrm{a}=\mathrm{a} * \mathrm{~b}$.
Hence G is abelian.
10. Prove that in any group, identity element is the only idempotent element.

Proof:
Let a be an idempotent element of G, then $a^{*} a=a$. $\qquad$

Now $a \in G \Rightarrow a^{-1} \in \boldsymbol{G}$
pre multiply $\boldsymbol{a}^{-\mathbf{1}}$ on both sides of (1)

$$
\begin{aligned}
& \mathrm{a}^{-1 *(\mathrm{a} * \mathrm{a})=\mathrm{a}^{-1} * \mathrm{a}} \\
& \left(\mathrm{a}^{-1} * \mathrm{a}\right) * \mathrm{a}=\mathrm{a}^{-1 *} * \mathrm{a}=\mathrm{e} \\
& \mathrm{e}^{*} \mathrm{a}=\mathrm{e} \\
& \therefore \mathrm{a}=\mathrm{e}
\end{aligned}
$$

11. Prove that identity element of a group is unique

Proof: Let $\left(\mathrm{G},{ }^{*}\right)$ be a group.
Let ' $\mathrm{e}_{1}$ ' and ' $\mathrm{e}_{2}$ ' be the identity elements in G
Suppose $\mathrm{e}_{1}$ is the identity, then

$$
\mathrm{e}_{1} * \mathrm{e}_{2}=\mathrm{e}_{2} * \mathrm{e}_{1}=\mathrm{e}_{2}
$$

Suppose $e_{2}$ is the identity, then

$$
\mathrm{e}_{1} * \mathrm{e}_{2}=\mathrm{e}_{2} * \mathrm{e}_{1}=\mathrm{e}_{1}
$$

Therefore $e_{1}=e_{2}$.
Hence identity element is unique.

## Sub group:

Let G be a group under the operation *. Then ( H, , $^{*}$ ) is said to be a subgroup of ( G, , $^{*}$ ) if $\mathrm{H} \subseteq \mathrm{G}$ and $(\mathrm{H}, *)$ itself is a group under the operation *.
(i.e.) $\left(\mathrm{H},{ }^{*}\right)$ is said to be a subgroup of ( $\mathrm{G}, *$ ) if
> $\mathrm{e} \in \mathrm{H}$ where e is the identity element in G
$>$ for $\mathrm{a} \in \mathrm{H}, \mathrm{a}^{-1} \in \mathrm{H}$
$>$ For $\mathrm{a}, \mathrm{b} \in \mathrm{H} \Rightarrow \mathrm{a} * \mathrm{~b} \in \mathrm{H}$.
12. Prove that the necessary and sufficient condition for a non empty subset $\mathbf{H}$ of a group ( $\mathbf{G}$, *) to be a subgroup is $a, b \in H \Rightarrow a * b^{-1} \in H$.
(Nov/Dec 2012)

## Proof:

Necessary Condition:
Let us assume that $H$ is a subgroup of G . Since $H$ itself a group, we have if $a, b \in H$ implies $a * b \in H$

Since $b \in H$ then $b^{-1} \in H$ which implies $a^{*} b^{-1} \in H$
Sufficient Condition:
Let $a^{*} b^{-1} \in H$, for $a^{*} b \in H$
Claim 1: Identity property
If $a \in H$, which implies $a^{*} a^{-1}=e \in H$
Hence the identity element $e \in H$.
Claim 2: Inverse property
Let $a, e \in H$, then $e^{*} a^{-1}=a^{-1} \in H$
Hence $a^{-1}$ is the inverse of $a$.
Claim 3: Closure property
Let $a, b^{-1} \in H$, then

$$
a *\left(b^{-1}\right)^{-1}=a * b \in H
$$

Therefore $H$ is closed.

Claim 4: Associative property
Clearly * is associative.
Hence $H$ is a subgroup of G.
13. Prove that intersection of two subgroups of a group $G$ is again a subgroup of $G$, but their union need not be a subgroup of $G$. (Nov/Dec 2015)

Proof:
Claim 1: Intersection of two subgroups is again a subgroup.
Let $A$ and $B$ be two subgroups of a group G . we need to prove that $A \cap B$ is a subgroup.
(i.e.) It is enough to prove that $A \bigcap B \neq \phi$ and $a, b \in A \bigcap B \Rightarrow a^{*} b^{-1} \in A \bigcap B$.

Since $A$ and $B$ are subgroups of G , the identity element $e \in A$ and $B$.
$\therefore A \cap B \neq \phi$
Let $\quad a, b \in A \bigcap B \Rightarrow a, b \in A \quad$ and $a, b \in B$
$\Rightarrow a^{*} b^{-1} \in A$ and $a^{*} b^{-1} \in B$
$\Rightarrow a^{*} b^{-1} \in A \bigcap B$
Hence $A \cap B$ is a subgroup of G .
Claim 2: Union of two subgroups need not be a subgroup
Consider the following example,
Consider the group $(Z,+)$, where $Z$ is the set of all integers and the operation + represents usual addition.

$$
\text { Let } A=2 Z=\{0, \pm 2, \pm 4, \pm 6, \ldots\} \text { and } B=3 Z=\{0, \pm 3, \pm 6, \pm 9, \ldots\}
$$

Here $(2 Z,+)$ and $(3 Z,+)$ are both subgroups of $(Z,+)$
Let $H=2 Z \bigcup 3 Z=\{0, \pm 2, \pm 3, \pm 4, \pm 6, \ldots\}$
Note that $2,3 \in H$, but $2+3=5 \notin H \Rightarrow 5 \notin 2 Z \bigcup 3 Z$
(i.e.) $2 Z \bigcup 3 Z$ is not closed under addition.

Therefore $2 Z \bigcup 3 Z$ is not a group
Therefore $(\mathrm{H},+)$ is not a subgroup of $(\mathrm{Z},+$ ).
14. Show that the union of two subgroups of a group is a subgroup if and only if one is contained in the other.
(or)
Let $\mathbf{H} \& \mathbf{K}$ be two subgroups of a group $\mathbf{G}$. Then $H \cup K$ is a subgroup if and only if $H \subseteq K(o r) K \subseteq H$.

Proof:
Assume that $\mathrm{H} \& \mathrm{~K}$ are two subgroups of G and $H \subseteq K(o r) K \subseteq H$.
$\therefore H \cup K=K(o r) H \cup K=H$
$\Rightarrow H \cup K$ is a subgroup.
Conversely, suppose $H \cup K$ is a subgroup of G. we claim that $H \subseteq K(o r) K \subseteq H$.
Suppose $H \nsubseteq K$ and $K \nsubseteq H$.
$a \in H$ and $a \notin K, b \in K$ and $b \notin H$
Clearly $a, b \in H \cup K$
Since $H \cup K$ is a subgroup of $\mathrm{G}, a b \in H \cup K$
Case ( $i$ ) Let $a b \in H \sin$ ce $a \in H, a^{-1} \in H$ ( $H$ is a subgroup)

$$
\Rightarrow a^{-1}(a b)=b \in H \text { which is contradiction to }(2)
$$

Case (ii) Let $a b \in K \sin c e b \in K, b^{-1} \in K$ (H is a subgroup)

$$
\Rightarrow b^{-1}(a b)=b \in K \text { which is contradiction to }(2)
$$

$\therefore$ our assumption $H \nsubseteq K$ and $K \nsubseteq H$ is wrong. $\therefore H \subseteq K$ (or) $K \subseteq H$.
15. Find all the non-trivial subgroups of $\left(Z_{12},+{ }_{12}\right)$

Solution: $\quad Z_{12}=\{[0],[1],[2],[3],[4] \ldots[11]\}$

Let H be a subgroup of $\mathrm{Z}_{12}$.
Then by Lagrange's theorem $\mathrm{O}(\mathrm{H})$ divides $\mathrm{O}(\mathrm{G})$.
i.e., $\mathrm{O}(\mathrm{H})$ divides 12. (Here $\mathrm{O}(\mathrm{G})=12)$

Hence $O(H)=1,2,3,4,6$, or 12

$$
\begin{aligned}
& \mathrm{O}(\mathrm{H})=1 \Rightarrow H=\{[0]\} \\
& \mathrm{O}(\mathrm{H})=12 \Rightarrow H=Z_{12} .
\end{aligned}
$$

$$
\mathrm{O}(\mathrm{H})=2 \Rightarrow H=\{[0],[x]\}
$$

Since inverse of $[0]$ is $[0]$, inverse of $[x]$ is $[x]$.

$$
\begin{aligned}
& \therefore[x]+[x]=[0]=[12] \\
& \Rightarrow[2 x]=[12] \\
& \Rightarrow x=6 \\
& \therefore H=\{[0],[6]\} \\
& \quad \mathrm{O}(\mathrm{H})=3 \Rightarrow H=\{[0],[x],[2 x]\}
\end{aligned}
$$

Since inverse of $[0]$ is $[0]$, inverse of $[x]$ is $[2 x]$.

$$
\begin{aligned}
& \therefore[x]+[2 x]=[0]=[12] \\
& \quad \therefore[3 x]=12 \\
& \Rightarrow x=4
\end{aligned}
$$

Hence $\mathrm{H}=\{[0],[4],[8]\}$
Also $\mathrm{H}=\{[0],[x],[3 x]\}$
Since inverse of $[0]$ is $[0]$, inverse of $[x]$ is $[3 x]$

$$
\begin{gathered}
\therefore[x]+[3 x]=[0]=[12] \\
{[4 x]=[12]}
\end{gathered}
$$

$$
\Rightarrow x=3
$$

Hence $H=\{[0],[3],[9]\}$

$$
\mathrm{O}(\mathrm{H})=4 \Rightarrow \mathrm{H}=\{[0],[x],[2 x],[3 x]\}
$$

Inverse of [x] must be [3x]
$\therefore[x]+[3 x]=[0]=[12]$
$[4 x]=[12]$
$\Rightarrow \mathrm{x}=3$
Hence $\boldsymbol{H}=\{[0],[3],[6],[9]\}$

$$
\mathrm{O}(H)=6 \Rightarrow H=\{[0],[x],[2 x],[3 x][4 x],[5 x]\}
$$

Inverse of [x] must be [5x]

$$
\begin{gathered}
\therefore[x]+[5 x]=[0]=[12] \\
{[6 x]=[12]} \\
\Rightarrow \mathrm{x}=2
\end{gathered}
$$

Hence $H=\{[0],[2],[4],[6],[8],[10]\}$ are the non-trivial subgroups of $\left(Z_{12},+{ }_{12}\right)$

## Normal Subgroup:

Let H be a subgroup of G under *. Then H is said to be a normal subgroup of G , for every $x \in G$ and for every $h \in H$, if $x * h * x^{-1} \in H$

$$
\text { i.e, } x * H * x-{ }^{-1} \in H
$$

16. Prove that intersection of any two normal subgroups of a group ( $G, *$ ) is a normal subgroup of a group ( $\mathbf{G}, *$ ).
(Nov/Dec 2016)
Proof:
Let G be the group and $H$ and $K$ are the normal subgroups of G .
Since $H$ and $K$ are normal subgroups of
$\Rightarrow H$ and $K$ are subgroups of G
$\Rightarrow H \cap K$ is a subgroup of G .
Now we have to prove $H \cap K$ is normal
Since $e \in H$ and $e \in K \Rightarrow e \in H \bigcap K$.
Thus $\mathrm{H} \cap \mathrm{K}$ is nonempty.
Let $x \in G$ and $h \in H \bigcap K$
$x \in G$ and $h \in H, h \in K$
$x \in G, h \in H$ and $x \in G, h \in K$
So, $x * h * x^{-1} \in H$ and $x * h * x^{-1} \in K$
$\therefore x * h * x^{-1} \in H \cap K$
Thus $H \cap K$ is a Normal subgroup of G .
17. Prove that a sub group $H$ of a group is normal if and only if $x * H^{*} x^{-1}=H, \forall x \in G$

## Proof:

Letus assume that $x * h * x^{-1}=H$
To Prove that H is a normal group

$$
x * h * x^{-1}=H \Rightarrow x * \mathrm{H}^{*} x^{-1} \subseteq H, \forall x \in G
$$

$\Rightarrow \mathrm{H}$ is a normal subgroup of G .
Conversely, let us assume that H is normal subgroup of G .

$$
\begin{equation*}
x^{*} \mathrm{H}^{*} x^{-1} \subseteq H, \quad \forall x \in G \tag{1}
\end{equation*}
$$

Now $x \in G \Rightarrow x^{-1} \in G$

$$
\begin{array}{cc}
\text { i.e. } & x^{-1 *} * \mathrm{H}^{*}\left(x^{-1}\right)^{-1} \subseteq H, \quad \forall x \in G \\
\Rightarrow & x^{-1 *} \mathrm{H}^{*} x \subseteq H \\
\Rightarrow & x^{*}\left(x^{-1} * \mathrm{H}^{*} x\right)^{*} x^{-1} \subseteq x^{*} H * x^{-1} \\
\Rightarrow & e^{*} \mathrm{H}^{*} \mathrm{e} \subseteq x^{*} H * x^{-1} \Rightarrow H \subseteq x^{*} H * x^{-1} \tag{2}
\end{array}
$$

from $1 \& 2$ we get
$\therefore x * \mathrm{H}^{*} x^{-1}=H$

## Cosets:

(i) Left Cosets of H of G : Let $\left(\mathrm{H},{ }^{*}\right)$ be a subgroup of $\left(\mathrm{G},{ }^{*}\right)$. For any $\mathrm{a} \in \mathrm{G}$, the left coset of H denoted by a ${ }^{*} \mathrm{H}$ and the set is $a * H=\{a * h: h \in H\} \quad \forall a \in G$
(ii) Right Cosets of H of G : The right coset of H denoted by $\mathrm{H} * \mathrm{a}$ and the set is

$$
H * a=\left\{h^{*} a: h \in H\right\} \quad \forall a \in G
$$

18. Find the left cosets of $\{[0],[3]\}$ in the group $\left(Z_{6},+6\right)$
(April/May - 2015)
Answer:

$$
\text { Let } Z_{6}=\{0,1,2,3,4,5\}
$$

$$
H=\{0,3\}
$$

$$
0+H=\{0,3\}=H
$$

$$
1+H=\{1,4\}
$$

$$
\begin{aligned}
& 2+H=\{2,5\} \\
& 3+H=\{0,3\}=H \\
& 4+H=\{0,3\}=1+H \\
& 5+H=\{0,3\}=2+H
\end{aligned}
$$

$0+H, 1+H$ and $2+H$ are three distinct left cosets of $H$.
19. State and Prove Lagrange's theorem on finite groups (or) Prove that in a finite group, order of any subgroup divides the order of the group.
(May/June 2013)\& (May/June 2016)

## Proof:

Statement:
The order of each subgroup of a finite group is divides the order of the group.
Proof:
Let $G$ be a finite group and $O(G)=n$
Let $H$ be a subgroup of G and $O(H)=m$
Let $h_{1}, h_{2}, h_{3}, \ldots, h_{m}$ are the m distinct elements of $H$
For $x \in G$, the right coset of $H$ is defined by $H_{x}=\left\{h_{1} x, h_{2} x, h_{3} x, \ldots \ldots . . h_{m} x\right\}$.
Since there is a one to one correspondence between $H$ and $H_{x}$, the members of $H_{x}$ are distinct.
Hence, each right coset of $H$ in $G$ has $m$ distinct members.
We know that any two right cosets of $H$ in $G$ are either identical or disjoint.
The number of distinct right cosets of H in G is finite (say k )
The union of these k distinct cosets of $H$ in $G$ is equal to $G$.
(i.e.) $G=H_{x 1} \cup H_{x 2} \cup H_{x 3} \bigcup \bigcup \bigcup H_{x k}$

$$
\begin{aligned}
& O(G)=O\left(H_{x 1}\right)+O\left(H_{x 2}\right)+O\left(H_{x 3}\right)+\square+O\left(H_{x k}\right) \\
& n=m+m+m+\ldots+m(k \text { times }) \\
& \frac{O(G)}{O(H)}=k
\end{aligned}
$$

Hence $O(H)$ divides $O(G)$

## Group homomorphism:

Let $(\mathrm{G}, *)$ and $(\mathrm{H}, \Delta)$ be two groups. A mapping $\mathrm{f}: \mathrm{G} \rightarrow \mathrm{H}$ is said to be a group homomorphism if for any $\mathrm{a}, \mathrm{b} \in \mathrm{G}, \mathrm{f}\left(\mathrm{a}^{*} \mathrm{~b}\right)=\mathrm{f}(\mathrm{a}) \Delta \mathrm{f}(\mathrm{b})$.

Example:
Consider multiplicative group of positive real numbers $\left(R^{+},.\right)$for any complex number u, the function $f_{u}: R \xrightarrow{+} C$ defined by $f_{u}(a)=a$ is a group homomorphism.

## Kernel of a Homomorphism:

Let $f: \mathrm{G} \rightarrow G^{\prime}$ be a group homomorphism. The set of elements of G , which are mapped into $\mathrm{e}^{\prime}\left(\right.$ identity element of $\left.\mathrm{G}^{\prime}\right)$ is called kernel of f and is denoted by ker f . $\operatorname{ker} f=\left\{x \in G / f(x)=e^{\prime}\right\}$

## Isomorphism:

A mapping f from a group $\left(\mathrm{G},,^{*}\right)$ to a group $\left(\mathrm{G}^{\prime},{ }^{*}\right)$ is said to be an isomorphism if
(i) $\quad \mathrm{f}$ is a homomorphism. (i.e., $f\left(a^{*} b\right)=f(a) \Delta f(b)$
(ii) f is one-one (Injective)
(iii) f is on-to (Surjective)
20. Prove that the group homomorphism preserves identity and inverse element.
(Nov/Dec 2016)
Answer:

## Identity

Let $a \in G$

Let $f:(G, *) \rightarrow(H, \Delta)$ be a group homomorphism.
Clearly $f(a) \in H$
Now

$$
\begin{aligned}
f(a) \Delta e_{H} & =f(a) \\
f(a) \Delta e_{H} & =f\left(a^{*} e_{G}\right) \\
f(a) \Delta e_{H} & =f(a) \Delta f\left(e_{G}\right) \\
\Rightarrow e_{H} & =f\left(e_{G}\right)
\end{aligned}
$$

Hence $e_{H}$ is the identity element.

## Inverse

Let $a \in G$
Since $G$ is a group, $a^{-1} \in G$
Since G is a group, $a * a^{-1}=e_{G}$
By homomorphism
$e_{H}=f\left(e_{G}\right)$
$e_{H}=f\left(a^{*} a^{-1}\right)$
$e_{H}=f(a) \Delta f\left(a^{-1}\right)$
Hence $f\left(a^{-1}\right)$ is the inverse of $f(a)$.

## Natural Homomorphism:

Let H be a normal homomorphism of a group G. The map $f: G \rightarrow G / H$ such that $f(x)=H^{*} \mathrm{x}, \mathrm{x} \in \mathrm{G}$ is called a natural homomorphism of the group G.
21. State and prove fundamental theorem on homomorphism of groups. (or)

Prove that every homomorphic image of a group $G$ is isomorphic to some quotient group of $G$. (or)
Let $f: G \rightarrow G^{\prime}$ be a onto homomorphism of groups ith kernel K. Then $G \not K \cong G^{\prime}$
Proof:
Let f be a homomorphism. $\boldsymbol{f}: \boldsymbol{G} \boldsymbol{\rightarrow} \boldsymbol{G}^{\boldsymbol{\prime}}$
Let $\boldsymbol{G}^{\prime}$ be homomorphic image of a group G. Let K be kernel of this omomorphism. Clearly Kis normal subgroup of G. We claim $\boldsymbol{G} / \boldsymbol{K} \cong \boldsymbol{G}^{\prime}$.

Define $\phi: G / K \rightarrow G^{\prime}$ by $\phi(\boldsymbol{k} * a)=f(a) \forall a \in G$
(i) To prove $\phi$ is well defined.

We have $\mathrm{k} * \mathrm{a}=\mathrm{k}$ * b
$\Rightarrow \mathrm{a}^{*} \mathrm{~b}^{-1} \in \mathrm{k}$
$\Rightarrow \mathrm{f}\left(\mathrm{a} * \mathrm{~b}^{-1}\right)=\mathrm{e}^{\text {, }}$
$\Rightarrow \mathrm{f}(\mathrm{a}) * \mathrm{f}\left(\mathrm{b}^{-1}\right)=\mathrm{e}^{\prime}$
$\because \mathrm{f}$ is homomorphism, $\Rightarrow \mathrm{f}(\mathrm{a}) *(\mathrm{f}(\mathrm{b}))^{-1}=\mathrm{e}^{\prime}$
$\Rightarrow \mathrm{f}(\mathrm{a}) *(\mathrm{f}(\mathrm{b}))^{-1} \mathrm{f}(\mathrm{b})=\mathrm{e}^{,} * \mathrm{f}(\mathrm{b})$
Multipky $f(b)$ on both sides $\Rightarrow f(a)=f(b)$
$\Rightarrow \phi(\mathrm{k} * \mathrm{a})=\boldsymbol{\phi}(\mathrm{k} * \mathrm{~b})$
$\therefore \phi$ is well defined.
(ii) To prove $\boldsymbol{\phi}$ is one-one:

It is enough to prove that $\phi(\mathrm{k} * \mathrm{a})=\boldsymbol{\phi}(\mathrm{k} * \mathrm{~b}) \Rightarrow \mathrm{k} * \mathrm{a}=\mathrm{k} * \mathrm{~b}$
$\phi(\mathrm{k} * \mathrm{a})=\boldsymbol{\phi}(\mathrm{k} * \mathrm{~b})$
$\Rightarrow \mathrm{f}(\mathrm{a})=\mathrm{f}(\mathrm{b})$
$\Rightarrow \mathrm{f}(\mathrm{a}) *(\mathrm{f}(\mathrm{b}))^{-1}=\mathrm{f}(\mathrm{a}) *\left(\mathrm{f}\left(\mathrm{b}^{-1}\right)\right.$
$\Rightarrow \mathrm{f}(\mathrm{a}) *\left(\mathrm{f}\left(\mathrm{b}^{-1}\right)=\mathrm{f}\left(\mathrm{b} * \mathrm{~b}^{-1}\right)\right.$
$\Rightarrow \mathrm{f}\left(\mathrm{a} * \mathrm{~b}^{-1}\right)=\mathrm{f}(\mathrm{e})=\mathrm{e}^{\prime}$
$\Rightarrow \mathrm{f}\left(\mathrm{a}^{*} \mathrm{~b}^{-1}\right)=\mathrm{e}^{\prime} \Rightarrow \mathrm{a}^{*} \mathrm{~b}^{-1} \in \mathrm{~K}$
$\Rightarrow \mathrm{k} * \mathrm{a}=\mathrm{k} * \mathrm{~b} \therefore \phi$ is one-one.
(iii) To prove $\phi$ is onto:

Let $\boldsymbol{y} \in \boldsymbol{G}^{\prime}$, since f is one-one, there exists $\mathrm{a} \in \mathrm{G}$ such that $\mathrm{f}(\mathrm{a})=\mathrm{y}$
Hence $\boldsymbol{\phi}(\mathrm{k} * \mathrm{a})=\mathrm{f}(\mathrm{a})=\mathrm{y}$
$\therefore \mathrm{f}$ is onto.
(iv) To prove $\phi$ is homomorphism:

Now $\boldsymbol{\phi}(\mathrm{k} * \mathrm{a} * \mathrm{k} * \mathrm{~b})=\boldsymbol{\phi}(\mathrm{k} * \mathrm{a} * \mathrm{~b})=\mathrm{f}(\mathrm{a} * \mathrm{~b})=\mathrm{f}(\mathrm{a}) * \mathrm{f}(\mathrm{b})=\boldsymbol{\phi}(\mathrm{k} * \mathrm{a}) * \boldsymbol{\phi}(\mathrm{k} * \mathrm{~b})$
$\therefore \phi$ is homomorphism.
Since $\boldsymbol{\phi}$ is one-one, onto and homomorphism, $\boldsymbol{\phi}$ is an isomorphismbetween $\boldsymbol{G} / \boldsymbol{K} \& \boldsymbol{G}$,
$\therefore G / K \cong G^{\prime}$
22. Let $g: G \rightarrow H$ be a homomorphism from the group $\mathcal{C}, *$ to) the group $H\langle, \Delta$. Prove that the kernel of $g$ is a normal subgroup of $G$.
(May/June 2016)

## Proof:

Let K be the Kernel of the homomorphism g . That is $K=\left\{x \in G g(x)=e^{\prime}\right\}$ where $e^{\prime}$ the identity element of H . is

Let $\mathrm{x}, \mathrm{y} \in \mathrm{K}$. Now
$g\left(x^{*} y^{-1}\right)=g(x) \Delta g\left(y^{-1}\right)=g(x) \Delta[g(y)]^{-1}=e^{\prime} \Delta\left(e^{\prime}\right)^{-1}=e^{\prime} \Delta e^{\prime}=e^{\prime}$
$x^{*} y^{-1} \in K$
Therefore K is a subgroup of G. Let
$x \in K, f \in G$
$g\left(f^{*} x * f^{-1}\right)=g(f)^{*} g(x)^{*} g\left(f^{-1}\right)=g(f) e^{\prime}[g(f)]^{-1}=g(f)[g(f)]^{-1}=e^{\prime}$
$\therefore \quad f^{*} x * f^{-1} \in K$
Thus $K$ is a normal subgroup of $G$.
23. Let $\left(\mathbf{G},{ }^{*}\right)$ be a group and let $\mathbf{H}$ be normal subgroup of $\mathbf{G}$. If $\mathbf{G} / \mathbf{H}$ be the set $\{a H \mid a \in G\}$ then show that $(G / H, \otimes)$ is a group, where $a H \otimes b H=(a * b) H$, for all $a H, b H \in G \mid H$.Further show that there exists a natural homomorphism $\quad f: G \rightarrow G \mid H$

Proof:
Given: G/H=\{a*h/áG\}
We know that $e^{*} H=H$
$\therefore e H \in G / H$
$\Rightarrow \mathrm{G} / \mathrm{H}$ is non empty
If aH ,bH $\in G / H$, then $a H \otimes b H=(a * b) H \in G / H$
$\Rightarrow \mathrm{G} / \mathrm{H}$ is closed
Let $\mathrm{aH}, \mathrm{bH}, \mathrm{cH} \in G / H$
Now
$a H \otimes\{b H \otimes c H\}=a H \otimes(b * c) H$

$$
\begin{aligned}
& =(a * b * c) H \\
& =(a * b) H \otimes c H \\
& =(a H \otimes b H) \otimes c H
\end{aligned}
$$

$\Rightarrow \otimes$ is associative
$\operatorname{Now}(a H) \otimes(e H)=(a * e) H=a H$
Also $a H \otimes e H=a H$
$\therefore e H$ is the identity element for $\mathrm{G} / \mathrm{H}$
Now, $a H \otimes a^{-1} H=\left(a * a^{-1}\right) H=d H$
$\therefore a^{-1} H$ is the inverse element of $a * H$
Hence $(G / H, \otimes)$ is a group.
Define $f: G \rightarrow G \mid H$ by $f(a)=a H$
To Prove f is homomorphism:

$$
\begin{aligned}
f(a * b) & =\left(a * b^{*}\right) H \\
& =a H \otimes b H \\
& =f(a) \otimes f(b)
\end{aligned}
$$

Hence the proof.

## Cyclic group:

Let G be a group. Let $\mathrm{a} \in \mathrm{G}$. Then $H=\left\{a^{n} / n \in Z\right\}$ is a subgroup of G . H is called the cyclic subgroup of G generated by ' $a$ ' and is denoted by $\langle a\rangle$.

A group G is cyclic if there exixts an element $\mathrm{a} \in \mathrm{G}$ such that $\langle\mathrm{a}\rangle=\mathrm{G}$.

## 24. State and prove Cayley's theorem.

Statement: Every finite group of order n is isomorphic to permutation group of degree n .
Proof: Finding a set $\boldsymbol{G}^{\prime}$ of permutation.
Let G be a finite group of order n . Let $\mathrm{a} \in \mathrm{G}$.
Define $f_{a}: G \rightarrow G$ by $f_{a}(x)=a x$
To prove f is bijection

$$
\text { (i) } \begin{aligned}
& \because f_{a}(\mathrm{x})=f_{a}(y) \\
& \Rightarrow a x=a y \\
& \Rightarrow x=y
\end{aligned}
$$

$\therefore f_{a}$ is one-one.
(ii) $\because$ if $y \in G$, then $f_{a}\left(\mathrm{a}^{-1} \mathrm{y}\right)=a \mathrm{a}^{-1} \mathrm{y}=y$
$\therefore f_{a}$ is onto.
Since $\boldsymbol{f}_{\boldsymbol{a}}$ has n-elements, $\boldsymbol{f}_{\boldsymbol{a}}$ is just permutation of n-symbols.

$$
\text { Let } G^{\prime}=\left\{f_{a} / a \in G\right\}
$$

Step 2: Claim: $\boldsymbol{G}^{\prime}$ is a group.
Let $f_{a}, f_{b} \in G^{\prime}$
$f_{a \circ} f_{b}(x)=f_{a}\left(f_{b}(x)\right)=f_{a}(b x)=a b x=f_{a b}$
$\therefore f_{a} \circ f_{b}=f_{a b} \Rightarrow G^{\prime}$ is closed.
25. Every cyclic group is an abelian group.
(Nov/Dec 2013)

## Proof:

Let ( G, * $^{*}$ ) be cyclic group with generator $\mathrm{a} \in \mathrm{G}$.
For $\mathrm{x}, \mathrm{y} \in \mathrm{G}$
$\Rightarrow \mathrm{x}=\mathrm{a}^{\mathrm{k}}, \mathrm{y}=\mathrm{a}^{\mathrm{t}}$ for integers $\mathrm{k}, \mathrm{t}$.
$x * y=a^{k} * a^{t}=a^{k+t}=a^{t+k}=a^{t} * a^{k}=y * x$
Hence (G, *) is an abelian group.
26. Prove that every subgroup of a cyclic group is cyclic.
(May/June 2016)

## Proof:

Let ( $\mathrm{G}, *$ ) be the cyclic group generated by an element $\mathrm{a} \in \mathrm{G}$.
Let H be the subgroup of G .
Case (i): If H contains identity element alone, then trivially H is cyclic.
Case (ii): Suppose if H contains the element other than the identity element.
Since $\mathrm{H} \subseteq \mathrm{G}$, any element of H is of the form $\mathrm{a}^{\mathrm{k}}$ for some integer k .
Let " $m$ " be the smallest positive integer such that $\mathrm{a}^{\mathrm{m}} \in \mathrm{H}$.
Now by division algorithm theorem, we have $\mathrm{k}=\mathrm{qm}+\mathrm{r}$ where $0 \leq \mathrm{r}<\mathrm{m}$.

$$
\begin{aligned}
\text { Now } \mathrm{a}^{\mathrm{k}} & =\mathrm{a}^{\mathrm{qm}+\mathrm{r}} \\
& =\left(\mathrm{a}^{\mathrm{m}}\right)^{\mathrm{q}} \cdot \mathrm{a}^{\mathrm{r}}
\end{aligned}
$$

and from this we have $a^{r}=\left(a^{m}\right)^{-q} \cdot a^{r}$.
Since $a^{m}, a^{k} \in H$, we have $a^{r} \in H$.
Which is a contradiction that $\mathrm{a}^{\mathrm{m}} \in \mathrm{H}$ such that " m " is small.
Therefore $\mathrm{r}=0$ and $\mathrm{a}^{\mathrm{k}}=\left(\mathrm{a}^{\mathrm{m}}\right)^{\mathrm{q}}$.
Thus every element of H is a power of $\mathrm{a}^{\mathrm{m}}$
Hence H is cyclic.
27. Discuss Ring and Fields with suitable examples.
(Nov/Dec 2014)

## Answer:

Ring:
An algebraic system $(R,+, \times)$ is called a ring if the binary operations + and $\times$ satisfies the following.
(i) $(R,+)$ is an abelian group
(ii) $\quad(R, \times)$ is a semi group and
(iii) The operation $\times$ is distributive over + .

Example:
The set of all integers under usual addition and multiplication is a Ring.

## Field:

A commutative ring $(F,+, \times)$ which has more than one element such that every nonzero element of $F$ has a multiplicative inverse in $F$ is called a field.

Example:
(1) $(R,+, \times)$ is a field
$(Q,+, \times)$ is a field

## 28. Prove that every field is an integral domain, but the converse need not be true.

Proof:
Let $(F,+,$.$) be a field. That is \mathrm{F}$ is a commutative ring with unity. Now to prove F is an integral domain it is enough to prove it has non-zero divisor.

Let $a, b \in F$ such that a $. \mathrm{b}=0$ and let $a \neq 0$ then $a^{-1} \in F$

Now
$a^{-1} \cdot(a \cdot b)=\left(a^{-1} \cdot a\right) \cdot b$
$a^{-1} .0=1 . b$
$0=b$
Similarly if $b \neq 0, b^{-1}$ exists.
$\therefore(a \cdot b) \cdot b^{-1}=0 . b^{-1}=0$
$a \cdot\left(b \cdot b^{-1}\right)=0$
$a .1=0$
$a=0$
Therefore F has non-zero divisor. Hence F is an integral domain.
The converse of the above property need not be true because every integral domain is not a field.

For exmaple $(\mathrm{Z},+,$.$) is an integral domain but not a field, since only the element 1,-1$ have inverses but all the other elements in Z do not have multiplicative inverses.
29. Prove that the set $Z_{4}=\{0,1,2,3\}$ is a commutative ring with respect to the binary operation
$+_{4}$ and $\mathbf{x}_{4}$.
(Nov/Dec 2015)
Proof:
Composition table for additive modulo 4.

| +4 | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
| :---: | :---: | :---: | :---: | :---: |
| $[0]$ | 0 | 1 | 2 | 3 |
| $[1]$ | 1 | 2 | 3 | 0 |
| $[2]$ | 2 | 3 | 0 | 1 |
| $[3]$ | 3 | 0 | 1 | 2 |

Composition table for multiplicative modulo 4.

| $\mathrm{x}_{4}$ | $[0]$ | $[1]$ | $[2]$ | $[3]$ |
| :---: | :---: | :---: | :---: | :---: |
| $[0]$ | 0 | 0 | 0 | 0 |
| $[1]$ | 0 | 1 | 2 | 3 |
| $[2]$ | 0 | 2 | 0 | 2 |
| $[3]$ | 0 | 3 | 2 | 1 |

From tables, we get
(i) all the entries in both tables belongs to $Z_{4}$

Therefore $Z_{4}$ is closed under the both operations addition and multiplication.
(ii) From the both tables, entries in the first, second, third and fourth row is equal to entries in the first, second, third and fourth columns respectively.

Hence the operations are commutative.
(iii) Modular addition and Modular multiplications are always associative.
(iv) 0 is the additive identity and 1 is the multiplicative identity.
(v) Additive inverse of $0,1,2,3$ are respectively $0,3,2,1$. Multiplicative inverses of the non-zero elements 1,2 and 3 are 1,2 and 3 respectively.
(vi) If $a, b, c \in Z_{4}$ then

$$
\begin{aligned}
& a \times(b+c)=(a \times b)+(a \times c) \\
& (a+b) \times c=(a \times c)+(b \times c)
\end{aligned}
$$

The operation multiplication is distributive over addition
Hence $\left(Z_{4},{ }_{4}, \times_{4}\right)$ is a commutative ring with unity.

# Department of Mathematics <br> MA8351 - DISCRETE MATHEMATICS <br> CLASS NOTES 

## UNIT V - LATTICES \& BOOLEAN ALGEBRA

## Relation:

A relation R on a set A is well defined rule which tells whether the given two elements x \& y of A are related or not.
If x is related to y then we write xRy . Otherwise $x R^{\prime}$ y

## Note:

If A is a finite set with ' n ' elements then $\mathrm{A} \times \mathrm{A}$ has $\mathrm{n}^{2}$ elements. Therefore A x A has $2^{n^{2}}$ relations on a set.

## Reflexive:

Let X be a set, R be the relation defined on X . Then R is said to be reflexive if it satisfies the following condition x R $x$..(ie) $x R x=\{x /(x, x) \in R\} \forall x \in X$

## Symmetric:

Let X be a set, R be the relation defined on X . Then R is said to be symmetric if it satisfies the following condition $x \mathrm{R} \mathrm{y}=>y \mathrm{R} x$ (ie)
$\{(y, x) /(x, y) \in R \Rightarrow(y, x) \in R\} \forall x, y \in X$

## Transitive:

Let X be a set, R be the relation defined on X . Then R is said to be transitive if it satisfies the following condition $x \mathrm{R}$ y \& $y \mathrm{R} \mathrm{z} \Rightarrow>x \mathrm{R} \mathrm{z}$ (ie)
$\{(x, z) /(x, y) \in R \&(y, z) \in R \Rightarrow(x, z) \in R\} \forall x, y, z \in X$

## Anti Symmetric:

Let X be a set, R be the relation defined on X . Then R is said to be antisymmetric if it satisfies the following condition $x \mathrm{R}$ y \& $y \mathrm{R} x=>x=y$ $\forall x, y \in X$

## Equivalence Relation:

Let X be a set, R be the relation defined on X . If R satisfies Reflexive, Symmetric and Transitive then the relation R said to be an equivalence relation

## Partial Order Relation:

Let X be a set, R be the relation defined on X . Then R is said to be partial order relation if it satisfies Reflexive, Anti-Symmetric and Transitive.
Example: ' $\subseteq$ ' \& Divides (/) are partial order relation.

## Example: 1

- Subset relation ' $\subseteq$ ' is a partial order relation.

$$
A \subseteq A \rightarrow \text { Reflexive }
$$

$A \subseteq B \& B \subseteq A \Rightarrow A=B \quad \rightarrow$ Anti Symmetric
$A \subseteq B \& B \subseteq C \Rightarrow A \subseteq C \quad \rightarrow$ Transitive
It is reflexive, symmetric and transitive. $\therefore$ ' $\subseteq$ ' is a partial order relation.

## Example 2:

- Divides relation '/' is a partial order relation.


## Partially Ordered Set (or) Poset:

A set together with partial order relation defined on it is called partially ordered set. Usually a partial order relation is denoted by the symbol ' $\leq$ '

## Hasse Diagram:

Pictorial representation of a Poset is called Hasse diagram.

## 1. Draw the Hasse diagram for

(a) $P_{1}=\{1,2,3,4,12\}$ and $\leq$ is a relation such that $x \leq y$ if $x$ divides $y$
(b) Let $S=\{a, b, c\}$ and $\tilde{A}=P(S)=\{\phi,\{a\},\{b\},\{c\},\{a, b\},\{a, c\},\{b, c\},\{a, b$, c\} $\}$
Consider the partial order of set inclusion ( $\subseteq$ ).

Answer:
(a)
b)

2. Draw the Hasse diagram for $D_{24}=\{1,2,3,4,6,8,12,24\}$, $D_{30}=\{1,2,3,5,6,10,15,30\}, D_{36}=\{1,2,3,4,6,9,12,18,36\}$ considering the partial order divisibility.


## Upper Bound and Lower Bound:

Let $(P, \leq)$ be a Poset and A be any non-empty subset of $\mathbf{P}$. An element $a \in P$ is an upper bound of A, if $a \geq x \quad \forall x \in A$. An element $b \in P$ is an lower bound of A , if $b \leq x \forall x \in A$

## Least Upper Bound:

Let $(P, \leq)$ be a Poset and A be any non-empty subset of $P$. An element $a \in P$ is Least upper bound(LUB) (or) Supremum (Sup) of A if
(i) a is upper bound of A
(ii) $a \leq c$ where c is another upper bound of A .

## Greatest Lower Bound:

Let $(P, \leq)$ be a Poset and A be any non-empty subset of $\mathbf{P}$. An element $b \in P$ is greatest lower bound(GLB) (or) Infimum (Inf) of A if
(i) b is lower bound of A
(ii) $b \geq c$ where c is another lower bound of A .
3. Let $D_{30}=\{1,2,3,5,6,10,15,30\}$ and let the relation $R$ be divisor on $D_{30}$ Find
(a) all the lower bound of 10 and 15
(b)the greatest lower bound of 10 and 15
(c) all upper bound of 10 and 15
(d)the least upper bound of 10 and 15
(e) Draw the Hasse diagram (Nov/Dec - 2015)

Answer:
(a) The lower bounds of 10 and 15 are 1 and 5.
(b) The greatest lower bound of 10 and 15 is 5 .
(c) The upper bound of 10 and 15 is 30 .
(d) The least upper bound of 10 and 15 is also 30 .
(e) Hasse diagram


## Lattice:

A lattice is a partially ordered set (Poset) $(L, \leq)$ in which for every pair of elements $\mathrm{a}, \mathrm{b} \in L$ both greatest lower bound and least upper bound exists.

Note:
$\operatorname{GLB}\{a, b\}=a * b(o r) a \wedge b$
$L U B\{a, b\}=a \oplus b(o r) a \vee b$

Is $\left(\mathbf{S}_{\mathbf{2 4}}, \mathbf{D}\right)$ a lattice?
Solution:
$\mathrm{S}_{24}=\{1,2,3,4,6,8,12,24\}$
$D=\{\langle a, b\rangle / a \mid b\}$


In $\left(S_{24}, D\right)$, every pair of elements $a, b$ in $S_{24}$ has both lower bound and least upper bound.
Hence It is a Lattice.

## Distributive Lattice:

A lattice $(L, \wedge, \vee)$ is said to be distributive lattice if $\wedge$ and $\vee$ satisfy the following conditions
$a \vee(b \wedge c)=(a \vee b) \vee(a \vee c)$
$a \wedge(b \vee c)=(a \wedge b) \vee(a \wedge c)$

## 4. Check the given lattice is distributive or not



## Solution:

It is enough to prove that $\mathrm{D}_{1}$ (or) $\mathrm{D}_{2}$ satisfied.
Consider
$a \vee(b \wedge c)=a \vee 0=a$$(b \wedge \partial=G L B\{b, c\}=0$
$a \vee 0=L U B\{0, a\}=a$
Now
$(a \vee b) \wedge(a \vee c)=1 \wedge 1=1$
$(a \vee b)=\operatorname{LUB}\{a, b\}=1$
$(a \vee c)=L U B\{a, b\}=1$
$\therefore a \vee(b \wedge c) \neq(a \vee b) \wedge(a \vee c)$
$D_{1}$ is not satisfied
Therefore the given lattice is not distributive

## Modular Lattice:

A lattice $(L, \wedge, \vee)$ is said to be modular lattice if satisfies the following condition if $a \leq c$ then $a \vee(b \wedge c)=(a \vee b) \wedge c \forall a, b, c \in L$
5. State and prove Isotonicity property in lattice. Statement:
Let $(L, \wedge, \vee)$ be given Lattice. For any $\mathrm{a}, \mathrm{b}, \mathrm{c} \in L$, we have,

$$
\begin{aligned}
& b \leq c \Rightarrow \\
& \text { 1) } a \wedge b \leq a \wedge c \\
& \text { 2) } a \vee b \leq a \vee c
\end{aligned}
$$

## Proof:

Given $b \leq c$ Therefore $G L B\{b, c\}=b \wedge c=b$ and $\operatorname{LUB}\{b, c\}=b \vee c=c$
Claim 1: $a \wedge b \leq a \wedge c$
To prove the above, it's enough to prove $\operatorname{GLB}\{a \wedge b, a \wedge c\}=a \wedge b$
Claim 2: $a \vee b \leq a \vee c$
To prove the above it's enough to prove $L U B\{a \vee b, a \vee c\}=a \vee c$
6. In a lattice $(L, \leq, \geq)$, prove that $(a \wedge b) \vee(b \wedge c) \vee(c \wedge a)=(a \vee b) \wedge(b \vee c) \wedge(c \vee a)$ Solution:

$$
\begin{aligned}
(a \wedge b) \vee(b \wedge c) \vee(c \wedge a) & =(a \wedge b) \vee[(b \wedge c) \vee c] \wedge[(b \wedge c) \vee a] \\
& =(a \wedge b) \vee[c \wedge[(b \wedge c) \vee a] \\
& =[(a \wedge b) \vee c] \wedge[(a \wedge b) \vee[(b \wedge c) \vee a] \\
& =[(a \wedge b) \vee c] \wedge[(b \wedge c) \vee a] \\
& =[c \vee(a \wedge b)] \wedge[a \vee(b \wedge c\}] \\
& =[(c \vee a) \wedge(c \vee b)] \wedge[(a \vee b) \wedge(a \vee c)] \\
& =[(c \vee a) \wedge(b \vee c)] \wedge[(a \vee b) \wedge(c \vee a)] \\
& =(c \vee a) \wedge(b \vee c) \wedge(a \vee b) \\
& =(a \vee b) \wedge(b \vee c) \wedge(c \vee a)
\end{aligned}
$$

## 7. Prove that every finite lattice is bounded.

## Proof:

Let $(L, \wedge, \vee)$ be given Lattice.
Since $L$ is a lattice both GLB and LUB exist.
Let "a" be GLB of L and " $b$ " be LUB of $L$.
For any $\mathrm{x} \in L$, we have
$a \leq x \leq b$
$\operatorname{GLB}\{a, x\}=a \wedge x=a$
$\operatorname{LUB}\{a, x\}=a \vee x=x$
and
$G L B\{x, b\}=x \wedge b=x$
$L U B\{\mathrm{x}, \mathrm{b}\}=x \vee b=b$
Therefore any finite lattice is bounded.
8. In a distributive lattice prove that $a * b=a * c$ and $a \oplus b=a \oplus c$ imply $b=c$ (May/June - 2014)
Answer:
Consider,

$$
\begin{aligned}
b= & b \oplus(b * a) & & \text { (Absorption Law) } \\
& =b \oplus(a * b) & & (\text { Commutative Law) } \\
& =b \oplus(a * c) & & \text { (Given) } \\
& =(b \oplus a) *(b \oplus c) & & \text { (Distributive Law) }
\end{aligned}
$$

$$
\begin{aligned}
& =(a \oplus b) *(b \oplus c) & & \text { (Commutative Law) } \\
& =(a \oplus c) *(b \oplus c) & & \text { (Given) } \\
& =(c \oplus a) *(c \oplus b) & & \text { (Commutative Law) } \\
& =c \oplus(a * b) & & \text { (Distributive Law) } \\
& =c \oplus(a * c) & & \text { (Given) } \\
& =c \oplus(c * a) & & \text { (Commutative Law) } \\
& =c & & \text { (Absorption Law) } \\
\therefore b & =c & &
\end{aligned}
$$

9. In a lattice if $\boldsymbol{a} \leq \boldsymbol{b} \leq \boldsymbol{c}$, show that
(Nov/Dec - 2013)
(1) $a \oplus b=b * c$
$(2)\left(a^{*} b\right) \oplus(b * c)=(a \oplus b)^{*}(a \oplus c)=b$

## Answer:

(1) Given

$$
a \leq b \leq c
$$

Since

$$
\begin{array}{ll}
a \leq b \Rightarrow a \oplus b=b, & a * \mathrm{~b}=a \\
b \leq c \Rightarrow b \oplus c=c, & b * c=b \\
a \leq c \Rightarrow a \oplus c=c, & a * c=a \tag{3}
\end{array}
$$

From (1) and (2), we have $a \oplus b=b=b * c$
(2) LHS

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

## RHS

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

Therefore $(a * b) \oplus(b * c)=(a \oplus b) *(a \oplus c)=b$
10. Show that direct product of any two distributive lattices is a distributive lattice.
Proof:
Let $L_{1}$ and $L_{2}$ be two distributive lattices. Let $\mathrm{x}, \mathrm{y}, \mathrm{z} \in L_{1} \mathrm{X} L_{2}$ be the direct product of $L_{1}$ and $L_{2}$. Then $x=\left(a_{1}, a_{2}\right), y=\left(b_{1}, b_{2}\right)$ and $z=\left(c_{1}, c_{2}\right)$

Now

$$
\begin{aligned}
x \vee(y \wedge z) & =\left(a_{1}, a_{2}\right) \vee\left(\left(b_{1}, b_{2}\right) \wedge\left(c_{1}, c_{2}\right)\right) \\
= & \left(\left(a_{1}, a_{2}\right) \vee\left(b_{1}, b_{2}\right)\right) \wedge\left(\left(a_{1}, a_{2}\right) \vee\left(c_{1}, c_{2}\right)\right) \\
= & (x \vee y) \wedge(x \vee z)
\end{aligned}
$$

Thus direct product of any two distributive lattice is again a distributive lattice

## 11. State and prove the necessary and sufficient condition for a lattice to be modular.

## Statement:

A lattice $L$ is modular if and only if none of its sub lattices is isomorphic to the pentagon lattice $\mathrm{N}_{5}$

## Proof:

Since the pentagon lattice $\mathrm{N}_{5}$ is not a modular lattice. Hence any lattice having pentagon as a sub lattice cannot be modular.
Conversely, let $(L, \leq)$ be any non modular lattice and we shall prove there is a sub lattice which is isomorphic to $\mathrm{N}_{5}$.

## 12. Prove that every distributive lattice is modular. Is the converse true? Justify your claim.

Proof:
Let $(L, \leq)$ be a distributive lattice, for all $\mathrm{a}, \mathrm{b}, \mathrm{c} \in L$, we have
$a \oplus\left(b^{*} c\right)=(a \oplus b)^{*}(a \oplus c)$
Thus if $a \leq c$, then $a \oplus c=c$
$\therefore a \oplus(b * c)=(a \oplus b)^{*} c$
So if $a \leq c$, the modular equation is satisfied and L is modular.
However, the converse is not true, because diamond lattice is modular but not distributive.

## Boolean Algebra

A complemented distributive lattice is called Boolean algebra.
13. In any Boolean algebra, show that $a b^{\prime}+a^{\prime} b=0 \quad$ if and only if $\mathbf{a}=b$

Proof:
Let ( $\mathrm{B}, .,+, 0,1$ ) be any boolean algebra
Let $\mathrm{a}, \mathrm{b} \in \mathrm{B}$ \& $\mathrm{a}=\mathrm{b}$

Now $a b^{\prime}+a^{\prime} b=a \cdot b^{\prime}+a^{\prime} \cdot b=a \cdot a^{\prime}+a^{\prime} \cdot a=0+0=0$
Conversely let $a b^{\prime}+a^{\prime} b=0$
Now

$$
\begin{align*}
& a b^{\prime}+a^{\prime} b=0 \\
& \Rightarrow a+a b^{\prime}+a^{\prime} b=a \\
& \Rightarrow a+a b^{\prime}=a \\
& \Rightarrow\left(a+a^{\prime}\right) \cdot(a+b)=a \\
& \Rightarrow 1 \cdot(a+b)=a \Rightarrow a+b=a  \tag{1}\\
& a b^{\prime}+a^{\prime} b=0 \\
& \Rightarrow a b^{\prime}+a^{\prime} b+b=b \\
& \Rightarrow a b^{\prime}+b=b \\
& \Rightarrow(a+b) \cdot\left(b+b^{\prime}\right)=b \\
& \Rightarrow(a+b) \cdot 1=b \Rightarrow a+b=b . .
\end{align*}
$$

From(1) \& (2)
$a=b$

## 14. Show that a complemented distributive lattice is a Boolean algebra. (Nov/Dec - 2014)

Answer:
A Boolean algebra will generally be denoted by $\left(B, *, \oplus,{ }^{\prime}, 0,1\right)$ in which $(B, *, \oplus)$ a lattice with two binary operations is $*$ and $\oplus$ called the meet and join respectively.

The corresponding partially ordered set will be denoted by $(B, \leq)$. The bounds of the lattice are denoted by 0 and 1 , where 0 is the least element and 1 is the greatest element of $(B, \leq)$.

Since $(B, *, \oplus)$ is complemented and because of the fact that it is a distributive lattice, each element of B has a unique complement. We shall denote the unary operation of complementation by ', so that for any $a \in B$, the complement of $a \in B$ is denoted by $a^{\prime} \in B$.
15. Prove that in a Boolean algebra $(\mathbf{a} \vee \mathbf{b})^{\prime}=\mathbf{a}^{\prime} \wedge \mathbf{b}^{\prime}$ and $(\mathbf{a} \wedge \mathbf{b})^{\prime}=\mathbf{a}^{\prime} \vee \mathbf{b}^{\prime}$ (Nov/Dec - 2015) (April/May - 2015) \& (Nov/Dec - 2014) (or)

## Prove that De Morgon's laws hold good for a complemented distributive

 lattice $(L, \wedge, \vee)$Proof:
The De Morgon's Laws are
(1) $(a \vee b)^{\prime}=a^{\prime} \wedge b^{\prime}$
(2) $(a \wedge b)^{\prime}=a^{\prime} \vee b^{\prime}$, for all $a, b \in B$

Let $(L, \wedge, \vee)$ be a complemented distributive lattice.
Let $\mathrm{a}, \mathrm{b} \in \mathrm{L}$
Since $L$ is a complemented lattice, the complements of $a$ and $b$ exists.
Let the complement a be a ' and the complement of $b$ be $b$ '
Now

$$
\begin{aligned}
(a \vee b) \vee\left(a^{\prime} \wedge b^{\prime}\right) & =\left\{(a \vee b) \vee a^{\prime}\right\} \wedge\left\{(a \vee b) \vee b^{\prime}\right\} \\
& =\left\{a \vee\left(b \vee a^{\prime}\right)\right\} \wedge\left\{a \vee\left(b \vee b^{\prime}\right)\right\} \\
& =\left\{\left(a \vee a^{\prime}\right) \vee b\right\} \wedge(a \vee 1) \\
& =(1 \vee b) \wedge(a \vee 1) \\
& =1 \wedge 1 \\
= & 1 \\
(a \vee b) \wedge\left(a^{\prime} \wedge b^{\prime}\right) & =\left\{a \wedge\left(a^{\prime} \wedge b^{\prime}\right)\right\} \vee\left\{b \wedge\left(a^{\prime} \wedge b^{\prime}\right)\right\} \\
= & \left\{\left(a \wedge a^{\prime}\right) \wedge b^{\prime}\right\} \vee\left\{\left(b \wedge a^{\prime}\right) \wedge b^{\prime}\right\} \\
& =\left\{\left(a \wedge a^{\prime}\right) \wedge b^{\prime}\right\} \vee\left\{a a^{\prime} \wedge\left(b \wedge b^{\prime}\right)\right\} \\
& =\left\{0 \wedge b^{\prime}\right\} \vee\left(a^{\prime} \wedge 0\right) \\
& =0 \vee 0 \\
& =0
\end{aligned}
$$

hence $(a \vee b)^{\prime}=a^{\prime} \wedge b^{\prime}$
By the principle of duality, we have $(a \wedge b)^{\prime}=a^{\prime} \vee b^{\prime}$
16. Show that in a distributive lattice and complemented lattice
$a \leq b \Leftrightarrow a * b^{\prime}=\mathbf{0} \Leftrightarrow a^{\prime} \oplus b=\mathbf{1} \Leftrightarrow b^{\prime} \leq a^{\prime}$
(May/June - 2013)
Answer:

$$
a \leq b \Leftrightarrow a^{*} b^{\prime}=0 \Leftrightarrow a^{\prime} \oplus b=1 \Leftrightarrow b^{\prime} \leq a^{\prime}
$$

Claim 1: $a \leq b \Rightarrow a^{*} b^{\prime}=0$
Since $a \leq b \Rightarrow a \oplus b=b, a * \mathrm{~b}=a$
Now $a^{*} \mathrm{~b}^{\prime}=\left(\left(a^{*} b\right)^{*} \mathrm{~b}^{\prime}\right)=\left(a^{*}\left(b^{*} \mathrm{~b}^{\prime}\right)\right)=a^{*} 0=0$
Claim 2: $a^{*} b^{\prime}=0 \Rightarrow a^{\prime} \oplus b=1$
We have $a^{*} b^{\prime}=0$

Taking complement on both sides, we have

$$
\left(a^{*} b^{\prime}\right)^{\prime}=(0)^{\prime} \Rightarrow a^{\prime} \oplus b=1
$$

Claim 3: $a^{\prime} \oplus b=1 \Rightarrow b^{\prime} \leq a^{\prime}$

$$
\begin{aligned}
a^{\prime} \oplus b & =1 \\
& \Rightarrow\left(a^{\prime} \oplus b\right) * b^{\prime}=1 * b^{\prime} \\
& \Rightarrow\left(a^{\prime} * b^{\prime}\right) \oplus\left(b^{*} b^{\prime}\right)=b^{\prime} \\
& \Rightarrow\left(a^{\prime} * b^{\prime}\right) \oplus 0=b^{\prime} \\
& \Rightarrow a^{\prime *} b^{\prime}=b^{\prime} \\
& \Rightarrow b^{\prime} \leq a^{\prime}
\end{aligned}
$$

Claim 4: $b^{\prime} \leq a^{\prime} \Rightarrow a \leq b$
We have $b^{\prime} \leq a^{\prime}$
Taking complement we get

$$
\left(b^{\prime}\right)^{\prime} \geq\left(a^{\prime}\right)^{\prime} \Rightarrow a \leq b
$$

17. Show that in any Boolean algebra, $\left(a+b^{\prime}\right)\left(b+c^{\prime}\right)\left(c+a^{\prime}\right)=\left(a^{\prime}+b\right)\left(b^{\prime}+c\right)\left(c^{\prime}+a\right)$
(May/June - 2014) \& (Nov/Dec - 2013)
Answer:

$$
\begin{aligned}
&\left(a+b^{\prime}\right)\left(b+c^{\prime}\right)\left(c+a^{\prime}\right)=\left(a+b^{\prime}+0\right)\left(b+c^{\prime}+0\right)\left(c+a^{\prime}+0\right) \\
&=\left(a+b^{\prime}+c c^{\prime}\right)\left(b+c^{\prime}+a a^{\prime}\right)\left(c+a^{\prime}+b b^{\prime}\right) \\
&=\left(a+b^{\prime}+c\right) \cdot\left(a+b^{\prime}+c^{\prime}\right) \cdot\left(b+c^{\prime}+a\right) \cdot\left(b+c^{\prime}+a^{\prime}\right) \cdot\left(c+a^{\prime}+b\right) \cdot\left(c+a^{\prime}+b^{\prime}\right) \\
&=\left(a^{\prime}+b+c c^{\prime}\right)\left(b^{\prime}+c+a a^{\prime}\right)\left(c^{\prime}+a+b b^{\prime}\right) \\
&=\left(a^{\prime}+b+0\right)\left(b^{\prime}+c+0\right)\left(c^{\prime}+a+0\right) \\
&=\left(a^{\prime}+b\right)\left(b^{\prime}+c\right)\left(c^{\prime}+a\right)
\end{aligned}
$$

18. If $P(S)$ is the power set of a non-empty $S$, prove that $\{P(S), \square,, \backslash, \phi, S\}$ isa Boolean algebra. (Nov/Dec - 2015)

## Answer:

Let $S$ be the nonempty set and $P(S)$ be its power set.

The set algebra $\left\{P(S), \square, \_, \backslash, S\right\}$ is a Boolean algebra in which the complement of any subset $A \subseteq S$ is $\backslash A \subseteq S-A$, the relative complement of the set A.

If $S$ has $n$ elements, then $P(S)$ has $2^{n}$ elements and the diagram of the Boolean algebra is a $n$ cube.

The partial ordering relation on $\mathrm{P}(\mathrm{S})$ corresponding to the operations and $\square$ is the subset relation $\subseteq$.

If $S$ is an empty set, then $P(S)$ has only one element. That is $\phi$, so that $\phi=0=1$, and the corresponding Boolean algebra is a degenerate Boolean algebra.
19. In a Distributive lattice $\{L, \vee, \wedge\}$ if an element $a \in L$ is a complement then it is unique.
Proof:
Let a be an element with two distinct complement b and c . Then $\mathrm{a} * \mathrm{~b}=0$ and $\mathrm{a}^{*} \mathrm{c}$ = 0
Hence $a^{*} b=a^{*} c$
Also
$a \oplus b=1 \quad$ and $\quad a \oplus c=1$
$\therefore a \oplus b=a \oplus c$
Hence $\mathrm{b}=\mathrm{c}$.
20. In a Boolean algebra prove that $(a \wedge b)^{\prime}=a^{\prime} \vee b^{\prime}$

Proof:

$$
\begin{aligned}
(a \wedge b) \vee\left(a^{\prime} \vee b^{\prime}\right) & =\left\{(a \wedge b) \vee a^{\prime}\right\} \wedge\left\{(a \wedge b) \vee b^{\prime}\right\} \\
& =\left\{\left(a \vee a^{\prime}\right) \wedge\left(b \vee a^{\prime}\right)\right\} \vee\left\{\left(a \vee b^{\prime}\right) \wedge\left(b \vee b^{\prime}\right)\right\} \\
& =\left\{1 \wedge\left(b \vee a^{\prime}\right)\right\} \vee\left\{\left(a \vee b^{\prime}\right) \wedge 1\right\} \\
= & b \vee b^{\prime} \\
& =1
\end{aligned}
$$

$(a \wedge b) \wedge\left(a^{\prime} \vee b^{\prime}\right)=\left\{(a \wedge b) \wedge a^{\prime}\right\} \wedge\left\{(a \wedge b) \wedge b^{\prime}\right\}$
$=\left\{a \wedge a^{\prime} \wedge b\right\} \vee\left\{a \wedge b \wedge b^{\prime}\right\}$
$=\{0 \wedge b\} \vee\{a \wedge 0\}$
$=0$
Hence proved.
21. Show that in any Boolean algebra, $a \bar{b}+b \bar{c}+c \bar{a}=\bar{a} b+\bar{b} c+\bar{c} a$. Solution:
Let $(B,+, 0,1)$ be any Boolean algebra and $a, b, c \in B$.

$$
\begin{aligned}
a \bar{b}+b \bar{c}+c \bar{a} & =a \bar{b} \cdot 1+b \bar{c} \cdot 1+\bar{c} a \cdot 1 \\
& =a \bar{b}(c+\bar{c}+) b \bar{c}(a+\bar{a})+c \bar{a}(b+\bar{b}) \\
& =a \bar{b} c+a \bar{b} \bar{c}+a b \bar{c}+\bar{a} \bar{b} \bar{c}+a b c+\bar{a} b c \\
& =(\overline{a b} c+\bar{a} b c)+(\bar{b} \bar{c}+\overline{a b} c)+(\overline{a b} \bar{c}+a b c) \\
& =(a+\bar{a}) \bar{b} c+(b+\bar{b}) \bar{a} c+(c+c) a b \\
& =1 \cdot \bar{b} c+1 \cdot \overline{a c}+1 . a b \\
& =\bar{a} b+\bar{b} c+\bar{c} a \\
\therefore a b+b \bar{c}+ & c a=\bar{a} b+b c+c a
\end{aligned}
$$

