**B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2012**
**Fifth Semester**
**Computer Science and Engineering**
**MA2265 – DISCRETE MATHEMATICS**
**(Regulation 2008)**

**Part - A**

**1. Define Tautology with an example.**
Solution:
A Statement that is true for all possible values of its propositional variables is called a tautology.
$(P \vee Q) \leftrightarrow (Q \vee P)$ is a tautology.

**2. Define a rule of universal specification.**
Answer:
From $(x)\ A(x)$ one can conclude $A(y)$. If $(x)\ A(x)$ is true for every element $x$ in the universe, then $A(y)$ is true.

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

**3. State pigeonhole principle.**
Solution:
If $k$ pigeons are assigned to $n$ pigeonholes and $n < k$ then there is at least one pigeonhole containing more than one pigeons.

**4. Solve $a_k = 3a_{k-1}$, for $k \geq 1$, with $a_0 = 2$.**
Solution:

$$Let\ G(x) = \sum_{k=0}^{\infty} a_k x^k = a_0 + a_1 x + a_2 x^2 + \cdots \qquad \ldots (1)$$

where $G(x)$ is the generating function for the sequence $\{a_n\}$.
Given $a_k = 3a_{k-1} \Rightarrow 3a_{k-1} - a_k = 0$
Multiplying by $x_k$ and summing from 1 to ∞, we have

$$3\sum_{k=1}^{\infty} a_{k-1}x^k - \sum_{k=1}^{\infty} a_k x^k = 0$$

$$3x\sum_{k=1}^{\infty} a_{k-1}x^{k-1} - \sum_{k=1}^{\infty} a_k x^k = 0$$

$$3x(a_0 + a_1 x + a_2 x^2 + \cdots) - (a_1 x + a_2 x^2 + \cdots) = 0$$

$$3xG(x) - (G(x) - a_0) = 0 \qquad [from\ (1)]$$

$$G(x)(3x - 1) - 2 = 0$$

$$G(x) = \frac{2}{(3x-1)} = -\frac{2}{1-3x}$$

$$\sum_{k=0}^{\infty} a_k x^k = -2\sum_{k=0}^{\infty} 3^k x^k \qquad \left[\because \frac{1}{1-x} = \sum_{n=0}^{\infty} x^n\right]$$

$a_k =$ Coefficient of $x^k$ in $G(x)$

$a_k = -2\,(3^n)$

**5. Define a regular graph. Can a complete graph be a regular graph?**

Ans: A graph is said to be regular if all the vertices are of same degree.

Yes a complete graph is always a regular graph.

**6. State the handshaking theorem.**

Solution:

If $G(V, E)$ is an undirected graph with e edges, then

$$\sum_i \deg v_i = 2e.$$

**7. Prove that the identity of a subgroup is the same as that of the group.**

Solution:

Let $e_1$ be the identity element of a group $G$ and $H$ be the subgroup of $G$.

Let us assume that $e_2 \neq e_1$ be the identity element of $H$.

Since $H \subseteq G$, $e_2 \in G$ which is a contradiction since in a group, identity element is unique.

∴Our assumption is wrong.

$$\therefore e_1 = e_2.$$

**8. State Lagrange's theorem in $\delta$ group theory.**

Solution:

An order of a subgroup $H$ of a group $G$ divides the order of the group $G$.

**9. When is a lattice said to be bounded?**

Solution:

A lattice having least and greatest element is called a bounded lattice.

**10. When is a lattice said to be a Boolean Algebra?**

Solution:

A complemented distributive lattice is called a Boolean Algebra.

**Part - B**

**11. a)i) Show that $\mathbf{P} \vee (\mathbf{Q} \wedge \mathbf{R})$ and $(\mathbf{P} \vee \mathbf{Q}) \wedge (\mathbf{P} \vee \mathbf{R})$ are logically equivalent.**

Solution:

To prove: $S: \big(\mathrm{P} \vee (\mathrm{Q} \wedge \mathrm{R})\big) \leftrightarrow \big((\mathrm{P} \vee \mathrm{Q}) \wedge (\mathrm{P} \vee \mathrm{R})\big)$ is a tautology.

| $\mathbf{P}$ | $\boldsymbol{Q}$ | $\boldsymbol{R}$ | $\mathbf{Q} \wedge \mathbf{R}$ | $\mathbf{P} \vee (\mathbf{Q} \wedge \mathbf{R})$ | $\mathbf{P} \vee \mathbf{Q}$ | $\mathbf{P} \vee \mathbf{R}$ | $(\mathbf{P} \vee \mathbf{Q}) \wedge (\mathbf{P} \vee \mathbf{R})$ | $\boldsymbol{S}$ |
|---|---|---|---|---|---|---|---|---|
| T | T | T | T | T | T | T | T | T |
| T | F | T | F | T | T | T | T | T |
| F | T | T | T | T | T | T | T | T |
| F | F | T | F | F | F | T | F | T |
| T | T | F | F | T | T | T | T | T |
| T | F | F | F | T | T | T | T | T |
| F | T | F | F | F | T | F | F | T |
| F | F | F | F | F | F | F | F | T |

Since all the values in last column are true. $(P \vee (Q \wedge R)) \leftrightarrow ((P \vee Q) \wedge (P \vee R))$ is a tautology.

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

**ii) Show that the hypothesis, "It is not sunny this afternoon and it is colder than yesterday", "we will go swimming only if it is sunny", "If we 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".**

**Solution:**

Let $S$ represents it is sunny this afternoon.
Let $C$ represents it is colder than yesterday.
Let $W$ represents we will go swimming.
Let $T_r$ represents we will take a canoe trip.
Let $H$ represents we will be home by sunset.
The inference is $\sim S \wedge C, W \rightarrow S, \sim W \rightarrow T_r, T_r \rightarrow H \Rightarrow H$

1. $\sim S \wedge C$ — $Rule\ P$
2. $W \rightarrow S$ — $Rule\ P$
3. $\sim W \rightarrow T_r$ — $Rule\ P$
4. $T_r \rightarrow H$ — $Rule\ P$
5. $\sim S$ — $Rule\ T, 1, P \wedge Q \Rightarrow P$
6. $\sim W$ — $Rule\ T, 5,2, Modus\ tollens$
7. $T_r$ — $Rule\ T, 6,3, Modus\ phones$
8. $H$ — $Rule\ T, 7,4, Modus\ phones$

**b) i) Find the principal disjunctive normal form of the statement $(q \vee (p \wedge r)) \wedge \sim ((p \vee r) \wedge q)$.**

**Solution:**

Let S $\Leftrightarrow (q \vee (p \wedge r)) \wedge \sim ((p \vee r) \wedge q)$.

$\Leftrightarrow (q \vee (p \wedge r)) \wedge (\sim (p \vee r) \vee \sim q)$

$\Leftrightarrow (q \vee (p \wedge r)) \wedge ((\sim p \wedge \sim r) \vee \sim q)$

$\Leftrightarrow ((q \vee p) \wedge (q \vee r)) \wedge ((\sim p \vee \sim q) \wedge (\sim r \vee \sim q))$

$\Leftrightarrow (q \vee p \vee F) \wedge (F \vee q \vee r) \wedge (\sim p \vee \sim q \vee F) \wedge (F \vee \sim r \vee \sim q)$

$\Leftrightarrow (q \vee p \vee (r \wedge \sim r)) \wedge ((p \wedge \sim p) \vee q \vee r) \wedge (\sim p \vee \sim q \vee (r \wedge \sim r)) \wedge ((p \wedge \sim p) \vee \sim r \vee \sim q)$

$\Leftrightarrow (q \vee p \vee r) \wedge (q \vee p \vee \sim r) \wedge (p \vee q \vee r) \wedge (\sim p \vee q \vee r) \wedge (\sim p \vee \sim q \vee r)$
$\wedge (\sim p \vee \sim q \vee \sim r) \wedge (p \vee \sim r \vee \sim q) \wedge (\sim p \vee \sim r \vee \sim q)$

$\Leftrightarrow (q \vee p \vee \sim r) \wedge (p \vee q \vee r) \wedge (\sim p \vee q \vee r) \wedge (\sim p \vee \sim q \vee r)$
$\wedge (\sim p \vee \sim q \vee \sim r) \wedge (p \vee \sim r \vee \sim q)$

$\Leftrightarrow (p \vee q \vee \sim r) \wedge (p \vee q \vee r) \wedge (\sim p \vee q \vee r) \wedge (\sim p \vee \sim q \vee r)$
$\wedge (\sim p \vee \sim q \vee \sim r) \wedge (p \vee \sim q \vee \sim r)$ $which\ is\ a\ PCNF$

$\sim S \Leftrightarrow remaining\ max\ terms\ in\ S$

$\sim S \Leftrightarrow (p \vee \sim q \vee r) \wedge (\sim p \vee q \vee \sim r)$

$\sim\sim S \Leftrightarrow \sim [(p \vee \sim q \vee r) \wedge (\sim p \vee q \vee \sim r)]$

$S \Leftrightarrow (\sim p \wedge q \wedge \sim r) \vee (p \wedge \sim q \wedge r)$ $which\ is\ PDNF.$

$S \Leftrightarrow \sim (p \vee \sim q \vee r) \vee \sim (\sim p \vee q \vee \sim r)$

**ii) By indirect method prove that $(x)\ (P(x) \rightarrow Q(x)), (\exists x)P(x) \Rightarrow (\exists x)Q(x)$**

Solution:
Let us assume that $\neg(\exists x)Q(x)$ as additional premise

| | |
|---|---|
| 1. $\neg(\exists x)Q(x)$ | $Additional\ premise$ |
| 2. $(x)\neg Q(x)$ | $Rule\ T, 1, De\ Morgan's\ law$ |
| 3. $\neg Q(a)$ | $Rule\ T, 2, US$ |
| 4. $(\exists x)P(x)$ | $Rule\ P$ |
| 5. $P(a)$ | $Rule\ T, 4, ES$ |
| 6. $P(a) \wedge \neg Q(a)$ | $Rule\ T, 5{,}3\ and\ conjuction$ |
| 7. $\neg(\neg P(a) \vee Q(a))$ | $Rule\ T, 6, De\ Morgan's\ law$ |
| 8. $\neg(P(a) \to Q(a))$ | $Rule\ T, 7, Equivalence$ |
| 9. $(x)(P(x) \to Q(x))$ | $Rule\ P$ |
| 10. $P(a) \to Q(a)$ | $Rule\ T, 9, US$ |
| 11. $\neg(P(a) \to Q(a)) \wedge P(a) \to Q(a)$ | $Rule\ T, 8{,}10\ and\ conjuction$ |
| 12. $F$ | $Rule\ T, 11\ and\ negation\ law$ |

**12.a)i) Use mathematical induction to prove the inequality $n < 2^n$ for all positive integer $n$.**

Proof:

$Let\ P(n): n < 2^n$ ... (1)

$P(1): 1 < 2^1$

$\Rightarrow 1 < 2$

$\therefore P(1)$ is true.

Let us assume that $P(n)$ is true. Now we have to prove that $P(n+1)$ is true.

To prove:

$P(n+1): n+1 < 2^{n+1}$

$n < 2^n \quad (from\ (1))$

$$n+1 < 2^n + 1$$
$$n+1 < 2^n + 2^n \quad [\because 1 < 2^n]$$
$$n+1 < 2.2^n$$
$$n+1 < 2^{n+1}$$

$\therefore P(n+1)$ is true.

$\therefore$ By induction method,

$$P(n): n < 2^n\ is\ true\ for\ all\ positive\ integers.$$

**ii) 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 if there are five possible grades $A, B, C, D$ and $F$.**

Solution:

By Pigeonhole principle, If there are $n$ holes and $k$ pigeons $n \le k$ then there is at least one hole contains at least $\left\lfloor \frac{k-1}{n} \right\rfloor + 1$ pigeons.

Here $n = 5$

$$\left\lfloor \frac{k-1}{5} \right\rfloor + 1 = 6$$
$$\frac{k-1}{5} = 5 \Rightarrow k - 1 = 25 \Rightarrow k = 26$$

The maximum number of students required in a discrete mathematics class is 26.

**b)i) Suppose that there are 9 faculty members in the mathematics department and 11 in the computer science department. How many ways are there to select a committee to develop a discrete**

**mathematics course at a school if the committee is to consist of three faculty member from mathematics department and four from the computer science department?**

Solution:

The number of ways to select 3 mathematics faculty members from 9 faculty members is $9C_3$ ways.

The number of ways to select 4 computer Science faculty members from 11 faculty members is $11C_4$ ways.

The number of ways to select a committee to develop a discrete mathematics course at a school if the committee is to consist of three faculty member from mathematics department and four from the computer science department is $9C_3 . 11C_4$ ways.

$$9C_3 . 11C_4 = \frac{9 \times 8 \times 7}{3!} . \frac{11 \times 10 \times 9 \times 8}{4!} = 27720$$

ii) **Using method of generating function to solve the recurrence relation $a_n + 3a_{n-1} - 4a_{n-2} = 0; n \geq 2$ , given that $a_0 = 3$ and $a_1 = -2$.**

Solution:

$$Let\ G(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots \qquad \ldots (1)$$

where $G(x)$ is the generating function for the sequence $\{a_n\}$.

Given $\quad a_n + 3a_{n-1} - 4a_{n-2} = 0$

Multiplying by $x_n$ and summing from 2 to ∞, we have

$$\sum_{n=2}^{\infty} a_n x^n + 3\sum_{n=2}^{\infty} a_{n-1} x^n - 4\sum_{n=2}^{\infty} a_{n-2} x^n = 0$$

$$\sum_{n=2}^{\infty} a_n x^n + 3x\sum_{n=2}^{\infty} a_{n-1} x^{n-1} - 4x^2\sum_{n=2}^{\infty} a_{n-2} x^{n-2} = 0$$

$$(a_2x^2 + a_3x^3 + a_4x^4 + \cdots) + 3x(a_1x + a_2x^2 + \cdots) - 4x^2(a_0 + a_1x + a_2x^2 + \cdots) = 0$$

$$G(x) - a_0 - a_1x + 3xG(x) - 3xa_0 - 4x^2G(x) = 0 \qquad [from\ (1)]$$

$$G(x)(1 + 3x - 4x^2) - 3 + 2x - 9x = 0$$

$$G(x)(1 + 3x - 4x^2) = 3 - 7x$$

$$G(x) = \frac{3 - 7x}{(1 + 3x - 4x^2)} = \frac{3 - 7x}{(1 + 4x)(1 - x)}$$

$$\frac{3 - 7x}{(1 + 4x)(1 - x)} = \frac{A}{(1 + 4x)} + \frac{B}{(1 - x)}$$

$$3 - 7x = A(1 - x) + B(1 + 4x) \ldots (2)$$

Put $x = -\frac{1}{4}$ in (2)

$$3 - 7\left(-\frac{1}{4}\right) = A\left(1 + \frac{1}{4}\right) \Rightarrow \frac{5}{4}A = 3 + \frac{7}{4} \Rightarrow A = \frac{19}{5}$$

Put $x = 1$ in (2)

$$3 - 7 = B(1 + 4) \Rightarrow 5B = -4 \Rightarrow B = -\frac{4}{5}$$

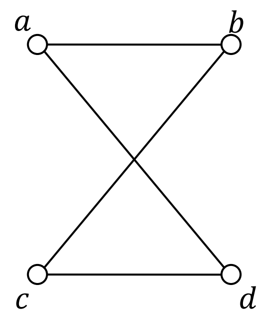
$$G(x) = \frac{\frac{19}{5}}{(1+4x)} - \frac{\frac{4}{5}}{(1-x)}$$

$$\sum_{n=0}^{\infty} a_n x^n = \frac{19}{5}\sum_{n=0}^{\infty}(-4)^n x^n - \frac{4}{5}\sum_{n=0}^{\infty} x^n \qquad \left[\because \frac{1}{1-x} = \sum_{n=0}^{\infty} x^n\right]$$

$a_n$ = Coefficient of $x^n$ in $G(x)$

$$a_n = \frac{19}{5}(-4)^n - \frac{4}{5}$$

**13. a)i) How many paths of length four are there from $a$ to $d$ in the simple graph $G$ given below.**




Solution: The adjacency matrix for the given graph is

$$A = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array}\begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

$$A^2 = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array}\begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 \\ 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 \end{pmatrix} \end{array}$$

$$A^4 = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array}\begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 8 & 0 & 8 & 0 \\ 0 & 8 & 0 & 8 \\ 8 & 0 & 8 & 0 \\ 0 & 8 & 0 & 8 \end{pmatrix} \end{array}$$

Since the value in the $a^{th}$ row and $d^{th}$ column in $A^4$ is 0.

$\therefore$ There is no path from $a$ to $d$ of length 4.

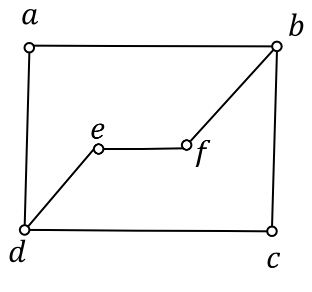
**ii) Show that the complete graph with n vertices $K_n$ has a Hamiltonian circuit whenever $n \geq 3$.**

**Proof:**

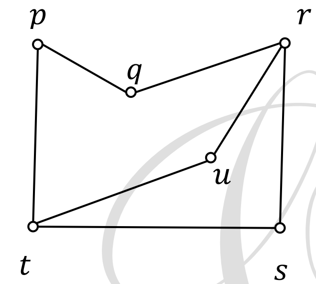
In a complete graph $K_n$, every vertex is adjacent to every other vertex in the graph.

Therefore a path can be formed starting from any vertex and traverse through all the vertices of $K_n$ and reach the same vertex to form a circuit without traversing through any vertex more than once except the terminal vertex. This circuit is called the Hamiltonian circuit.
∴ The complete graph with n vertices $K_n$ has a Hamiltonian circuit whenever $n \geq 3$.

**b) i) Determine whether the graphs $G$ and $H$given below are isomorphic.**




$G$




$H$

Solution:
The two graphs $G$and $H$ have same number of vertices and same number of edges.

$$\deg(a) = 2, \deg(b) = 3, \deg(c) = 2, \deg(d) = 3, \deg(e) = 2, \deg(f) = 2$$
$$\deg(p) = 2, \deg(q) = 2, \deg(r) = 3, \deg(s) = 2, \deg(t) = 3, \deg(u) = 2$$

Here in both the graphs two vertices are of degree three and remaining vertices are of degree two.
The mapping between two graphs are $a \to u, b \to r, c \to s, d \to t, e \to p$ and $f \to q$.
There is one to one correspondence between the adjacency of the vertices between the two graphs.
Therefore the two graphs are isomorphic.

**ii) Prove that an undirected graph has an even number of vertices of odd degree.**
Proof:
By Handshaking theorem, we know that
If the graph G has n vertices and e edges then

$$\sum_{i=1}^{n} \deg(v_i) = 2e \Rightarrow \sum_{i=1}^{n} \deg(v_i) = even\ number$$
$$\sum_{odd} \deg(v_i) + \sum_{even} \deg(v_i) = even\ number$$
$$where \sum_{odd} \deg(v_i)\ \ is\ sum\ of\ vertices\ with\ odd\ degree$$
$$\sum_{even} \deg(v_i)\ \ is\ sum\ of\ vertices\ with\ \ even\ degree$$

$$\sum_{odd} \deg(v_i) + even\ number = even\ number$$

( Since sum of even numbers is an even number)

$$\sum_{odd} \deg(v_i) = even\ number$$

Sum of even number of odd numbers is an even number.
∴ An undirected graph has an even number of vertices of odd degree.

**14.a)i) If $*$ is the operation defined on $S = Q \times Q$, the set of ordered pairs of rational numbers and givenby $(a, b) * (x, y) = (ax, ay + b)$,show that $(S,*)$is a semi group. Is it commutative? Also find the identity element of S.**

Solution:

Closure: $\forall (a, b), (x, y) \in S$

$(a, b) * (x, y) = (ax, ay + b) \in S$ $\quad [\because ax \in Q \text{ and } ay + b \in Q, \forall a, b, x, y \in Q]$

$\Rightarrow (a, b) * (x, y) \in S$

$\forall (a, b), (x, y) \in S \Rightarrow (a, b) * (x, y) \in S$

∴ $S$ is closed under $*$.

Associative: $\forall (a, b), (x, y), (u, w) \in S$

$(a, b) * \big((x, y) * (u, v)\big) = (a, b) * (xu, xv + y)$

$= (axu, a(xv + y) + b) = (axu, axv + ay + b) \ldots (1)$

$\big((a, b) * (x, y)\big) * (u, v) = (ax, ay + b) * (u, v)$

$= (axu, axv + ay + b) \ldots (2)$

From (1) and (2), we get

$(a, b) * \big((x, y) * (u, v)\big) = \big((a, b) * (x, y)\big) * (u, v)$

∴ $S$ satisfies associative property under $*$.

Identity: Let $(e_1, e_2) \in S$ be the identity element.

Then $(a, b) * (e_1, e_2) = (e_1 * e_2) * (a, b) = (a, b), \forall (a, b) \in S$

$$(a, b) * (e_1, e_2) = (a, b)$$
$$\Rightarrow (ae_1, ae_2 + b) = (a, b)$$
$$\Rightarrow ae_1 = a, ae_2 + b = b$$
$$\Rightarrow e_1 = 1, ae_2 = 0$$
$$\Rightarrow e_1 = 1, e_2 = 0$$
$$\Rightarrow (1,0) = \in S$$

∴ $(1,0) \in S$ is the identity element.

∴ $S$ is a semi group under $*$.

$$\forall (a, b), (x, y) \in S, \qquad (a, b) * (x, y) = (ax, ay + b) \ldots (3)$$
$$(x, y) * (a, b) = (xa, xb + y) \ldots (4)$$

From (3) and (4), we get

$$(a, b) * (x, y) \neq (x, y) * (a, b)$$

∴ $S$ is not commutative under $*$.

**ii) Prove that the necessary and sufficient condition for a non empty subset $H$ of a group $\{G,*\}$ to be a subgroup is $a, b \in H \Rightarrow a * b^{-1} \in H$.**

Proof:

Necessary condition:

Let us assume that $H$is a subgroup of $G$.

$H$ itself is a group.

$$a, b \in H \Rightarrow a * b \in H \ldots (1)\ [Closure\ ]$$
$$b \in H \Rightarrow b^{-1} \in H \ldots (2) \quad [Inverse\ property]$$
$$a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a * b^{-1} \in H \quad [from\ (1)\ and\ (2)]$$
$$\therefore a, b \in H \Rightarrow a * b^{-1} \in H.$$

Sufficient condition:

Let $a, b \in H \Rightarrow a * b^{-1} \in H$ and $H$ is a subset of $G$.

Closure property:

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

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

Hence $H$ is closed.

Associative property:

$\because H$ is a subset of $G$. All the elements in $H$ are elements of $G$. Since $G$ is associative under $*$.

$\therefore H$ is associative under $*$.

Identity property:

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

$\therefore e \in H$ be the identity element.

Inverse property:

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

$\therefore a^{-1} \in H$ be the inverse of $a \in H$.

$H$ itself is a group.

$\therefore H$ is a subgroup of $G$.

**b) i) Prove that the set $Z_4 = \{[0], [1], [2], [3]\}$ is a commutative ring with respect to the binary operation addition modulo and multiplication modulo $+_4, \times_4$.**

Solution:

The Cayley table for $(Z_4, +_4)$ and $(Z_4, \times_4)$ is given below

| $+_4$ | **[0]** | **[1]** | **[2]** | **[3]** |
|---|---|---|---|---|
| **[0]** | [0] | [1] | [2] | [3] |
| **[1]** | [1] | [2] | [3] | [0] |
| **[2]** | [2] | [3] | [0] | [1] |
| **[3]** | [3] | [0] | [1] | [2] |

| $\times_4$ | **[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 the above Cayley table, we observe that

All the elements in the table is also an element in $Z_4$ under $+_4$.

$\therefore Z_4$ is closed under binary operation $+_4$.

It is clear from the table that $Z_4$ is associative under $+_4$.

Here $[0] \in Z_4$ is the identity element.

The inverse of $[0], [1], [2]$ and $[3]$ are $[0], [3], [2]$ and $[1]$ respectively.

It is clear from the table that $Z_4$ is commutative under $+_4$.

All the elements in the table is also an element in $Z_4$ under $\times_4$.

$\therefore Z_4$ is closed under binary operation $\times_4$.

It is clear from the table that $Z_4$ is associative under $\times_4$.

It is clear from the table that $Z_4$ is commutative under $\times_4$.
$\therefore (Z_4, +_4, \times_4)$ is a commutative ring.

**ii) If $f: G \to G'$ is a group homomorphism from $(G,*)$ to $(G', \Delta)$ then prove that for any $a \in G$,**

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

Solution:
Since $f$ is a group homomorphism.

$$\forall a, b \in G, \qquad f(a * b) = f(a)\,\Delta\, f(b)$$

Since G is a group, $a \in G \Rightarrow a^{-1} \in G$.

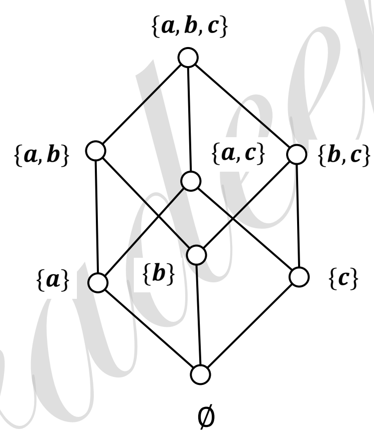
$$f(a)\,\Delta\, f(a^{-1}) = f(a * a^{-1})$$
$$f(a)\,\Delta\, f(a^{-1}) = f(e)$$
$$f(a)\,\Delta\, f(a^{-1}) = e' \qquad [where\ e'\ is\ the\ identity\ element\ in\ G']$$

The inverse of $f(a)$ is $f(a^{-1})$.

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

**15. a)i) Draw the Hasse diagram representing the partial ordering $\{(A, B): A \subseteq B\}$ on the power set $P(S)$ Where $S = \{a, b, c\}$. Find the maximal, minimal, greatest and least elements of the Poset.**

Solution:




The minimal element is $\phi$
The maximal element is $\{a, b, c\}$
The least element is $\phi$
The greatest element is $\{a, b, c\}$

**ii) In a Boolean algebra, prove that $a.(a + b) = a$, for all $a, b \in G$.**

Solution:
We know from the definition of GLB and LUB

$$a.b \leq a \ldots (1)$$
$$a + b \geq a \ldots (2)$$
$$a.(a + b) \leq a \ldots (3) \quad [from\ (1)]$$
$$a.(a + b) = a.a + a.b$$
$$a.(a + b) = a + a.b \geq a\ [from\ (2)]$$

$$\Rightarrow a.(a+b) \geq a \ldots (4)$$

From (3) and (4), we get

$$a.(a+b) = a$$

**b) i) In a distributive Lattice $\{L,\vee,\wedge\}$ if an element $a \in L$ has a complement then it is unique.**

Solution:

Let $b$ and $c$ be the complement of $a \in L$

$$b = b \wedge 1$$
$$b = b \wedge (a \vee c) \quad [\because a \vee c = 1]$$
$$b = (b \wedge a) \vee (b \wedge c) \quad [Distributive\ law]$$
$$b = 0 \vee (b \wedge c) \quad [\because a \wedge b = 0]$$
$$b = b \wedge c \quad \ldots (1) \quad [\because a \vee 0 = a]$$
$$c = 1 \wedge c$$
$$c = (a \vee b) \wedge c \quad [\because a \vee b = 1]$$
$$c = (a \wedge c) \vee (b \wedge c) \quad [Distributive\ law]$$
$$c = 0 \vee (b \wedge c) \quad [\because a \wedge c = 0]$$
$$c = b \wedge c \quad \ldots (2) \quad [\because a \vee 0 = a]$$

From (1) and (2), we get

$$b = c$$

$\therefore$ In a distributive Lattice $\{L,\vee,\wedge\}$ if an element $a \in L$ has a complement then it is unique.

**ii) Simplify the Boolean expression $a'.b'.c + a.b'.c + a'.b'.c'$ using Boolean algebra identities.**

**Solution:**

$$a'.b'.c + a.b'.c + a'.b'.c' = (a' + a).b'.c + a'.b'.c' \quad [Distributive\ law]$$
$$= 1.b'.c + a'.b'.c' \quad [a' + a = 1]$$
$$= b'.c + a'.b'.c' \quad [1.a = a]$$
$$= b'.c + b'.a'.c' \quad [a.b = b.a]$$
$$= b'.(c + a'.c') \quad [Distributive\ law]$$
$$= b'.\big((c + a').(c + c')\big) \quad [Distributive\ law]$$
$$= b'.\big((c + a').1\big) \quad [a' + a = 1]$$
$$= b'.(c + a') \quad [1.a = a]$$
$$= b'.c + b'.a' \quad [Distributive\ law]$$