UNIT – 5

Recurrence Relation

> forward difference operator,

$$\Delta f(x) = f(x+1) - f(x) \quad \text{or}$$
$$\Delta y(x) = y(x+1) - y(x) \quad \text{or}$$

1) $\Delta y_x = y_{x+1} - y_x$

2) $\Delta^2 y_x = \Delta(\Delta y_x) = \Delta(y_{x+1} - y_x) = \Delta y_{x+1} - \Delta y_x$
$$= y_{x+2} - y_{x+1} - (y_{x+1} - y_x)$$
$$= y_{x+2} - 2y_{x+1} + y_x$$

3) $\Delta^3 y_x = \cancel{y_{x+2}}$, $\Delta^4 y_x$

> Shift operator,

$$E\,f(x) = f(x+1) \quad \text{or}$$
$$E\,y(x) = y(x+1) \quad \text{or}$$
$$E\,y_x = y_{x+1}$$

$$E^2 y_x = y_{x+2}$$
$$E^3 y_x = y_{x+3}$$
$$E^n y_x = y_{x+n}$$

y_x

$x \rightarrow$ independent var.

$y \rightarrow$ dependent var.

> Relation b/w Δ and E.

$$\Delta y_x = y_{x+1} - y_x$$
$$\Delta y_x = E\,y_x - y_x$$
$$\Delta y_x = (E-1)y_x$$
$$\Delta = E - 1$$
$$\Rightarrow \boxed{E = \Delta + 1}$$

Let $\{a_n\}$ be a sequence. A recurrence relation of a_n is a relation that expresses a_n in terms of the $a_0, a_1, \ldots, a_{n-1}$.

- Defⁿ: A relation which contain an independent var.(x), dependent variable (y) and one or more differences of dependent variable $(\Delta y, \Delta^2 y, \Delta^3 y, \ldots)$ is called a recurrence relation (difference equⁿ).

Q.) $y_{x+2} - 6y_{x+1} + 2y_x = \cos x$. Solve.

Sol.) Here,

Order of recurrence relation = Highest subscript − lowest subscript

$= x+2-x = 2$

Degree of recurrent relation = ~~Highest power of dependent variable~~

Degree of highest subscript dependent variable $= 1$

Q) $y^2_{x-2} + 6y_{x-1} + 6 \cdot x \cdot y_x = e^x$

Order = 2

Degree = 1

This ~~rr~~ recurrence relation cannot be solved as it does not have constant coeff.

Q.) $a^3_{r+1} - 5a_{r-1} + 6a_{r-3} = \sin r$

Sol.) Order $= (r+1) - (r-3)$

$= 4$

Degree = 3

PAGE NO.:
DATE:

Sol^n of a recurrence relation,

Let $C_0 a_r + C_1 a_{r-1} + C_2 a_{r-2} + \dots + C_n a_{r-n} = f(r)$ — (i)
be a linear recurrence relation of order n with constant coefficient $c_0, c_1, c_2, \dots, c_n$.

Total sol^n = Homogeneous sol^n + Particular sol^n

$$a_r = a_r^{(h)} + a_r^{(P)}$$

- Case 1) If $f(r) = 0$, then equ^n (i) is called homogeneous recurrence relation.

- Case 2) If $f(r) \neq 0$, then equ^n (i) is called non-homogeneous recurrence relation.

Homogeneous solution,

for homogeneous sol^n, put $f(r) = 0$ in equ^n (i)

$\Rightarrow$ $C_0 a_r + C_1 a_{r-1} + C_2 a_{r-2} + \dots + C_n a_{r-n} = 0$ — (ii)

Put $a_r = m^r$ where, $m \neq 0$

$\Rightarrow$ $C_0 m^r + C_1 m^{r-1} + C_2 m^{r-2} + \dots + C_n m^{r-n} = 0$

$\Rightarrow$ $m^{r-n}(C_0 m^n + C_1 m^{n-1} + C_2 m^{n-2} + \dots + C_n) = 0$

$\because$ $m \neq 0$

$\Rightarrow$ $m^{r-n} \neq 0$

So, $C_0 m^n + C_1 m^{n-1} + C_2 m^{n-2} + \dots + C_n = 0$ — (iii)

This equ^n is called auxiliary / characteristic equ^n.

- Case 1) If all roots of equ^n (iii) are real and unequal i.e., $m_1 \neq m_2 \neq m_3 \neq \ldots\ldots \neq m_n$

(i) Sol^n) $q_r^{(h)} = B_1 \cdot m_1^r + B_2 \cdot m_2^r + \ldots\ldots + B_n \cdot m_n^r$

- case 2) If some of the roots are equal.

$$m = \underbrace{m_1 = m_2 = m_3 = \ldots\ldots = m_k} \neq m_{k+1} \neq \ldots\ldots \neq m_n$$

$$q_r^{(h)} = \left(B_1 + B_2 r + B_3 r^2 + \ldots + B_k r^{k-1}\right) m^r + B_{k+1} m_{k+1}^r + \ldots\ldots + B_n \cdot m_n^r$$

- Case 3) If $m_1 = a+ib$, $m_2 = a-ib$, $m_3, \ldots\ldots, m_n$ are real and unequal.

$$q_r^{(h)} = B_1 (a+ib)^r + B_2 (a-ib)^r + B_3 m_3^r + \ldots\ldots + B_n \cdot m_n^r$$

Put $a = R\cos\theta$, $b = R\sin\theta$

$R = \sqrt{a^2+b^2}$, $\theta = \tan^{-1}(b/a)$

(ii) $$(\cos\theta \pm i\sin\theta)^p = \cos p\theta \pm i \sin p\theta$$

$$q_r^{(h)} = R^r B_1 (\cos\theta + i\sin\theta)^r + R^r \cdot B_2 (\cos\theta - i\sin\theta)^r + \ldots$$

$$= R^r B_1 [\cos r\theta + i\sin r\theta] + R^r \cdot B_2 [\cos r\theta - i\sin r\theta] + \ldots$$

$$= R^r [(B_1+B_2)\cos r\theta + (B_1 - B_2) i \sin r\theta] + \ldots$$

$$q_r^{(h)} = R^r [A \cos r\theta + B \sin r\theta] + \ldots$$

PAGE NO.:
DATE:

Particular solⁿ

S.No.	form of $f(r)$	Trial solution
1.	b^r	Ab^r
2.	a pol. of degree K in r.	$A_0 + A_1 r + \cdots + A_K r^K$
3.	b^r[a pol. of deg. K in r]	$b^r[A_0 + A_1 r + \cdots + A_K r^K]$
4.	$\sin br$ or $\cos br$	$A \sin br + B \cos br$
5.	$b^r \sin br$ or $b^r \cos br$	$b^r[A \sin br + B \cos br]$
6.	b^r, when b^r one term of homogeneous solⁿ.	Arb^r.

Solve. $a_r - 5a_{r-1} + 6a_{r-2} = 5^r$. —(i)

solⁿ
$$Ea_{r-2} = a_{r-1}$$
$$E^2 a_{r-2} = a_r$$

from
$$E^2 a_{r-2} - 5Ea_{r-2} + 6E a_{r-2} = 5^r$$

$\Rightarrow$ $\underline{(E^2 - 5E + 6)} a_{r-2} = 5^r$ —(ii)

AE is
$$m^2 - 5m + 6 = 0$$
$$(m-2)(m-3) = 0$$
$$m = 2, 3$$
$$a_r^{(h)} = C_1 2^r + C_2 3^r$$

here, $f(r) = 5^r$

let $a_r^{(P)} = A \cdot 5^r$ be a trial solⁿ of (i).

from (i)

$\Rightarrow$ $A \cdot 5^r - 5 \cdot A\, 5^{r-1} + 6 \cdot A \cdot 5^{r-2} = 5^r$

$\Rightarrow$ $5^{r-2}(A \cdot 5^2 - 5A \cdot 5 + 6A) = 5^r$

$$\Rightarrow \quad 5^{r-2} \cdot 6A = 5^r$$

$$A = 25/6$$

Now,

$$a_5^{(P)} = \left(\frac{25}{6}\right) 5^r = \frac{5^{r+2}}{6}$$

Total sol^n, $a_r = a_r^{(h)} + a_r^{(P)}$

Q) Solve the recurrence relation.

$$a_r - 5a_{r-1} + 6a_{r-2} = 2^r + r, \quad r \geq 2$$

with $a_0 = 1$, $\&$ $a_1 = 1$.

Sol.) $Ea_{r-2} = a_{r-1}$, $E^2 a_{r-2} = a_r$

$$E^2 a_{r-2} - 5Ea_{r-2} + 6a_{r-2} = 2^r + r$$

$$\Rightarrow (E^2 - 5E + 6)a_{r-2} = 2^r + r \quad \text{— (i)}$$

A.E is $m^2 - 5m + 6 = 0$

$$m^2 - 3m - 2m + 6 = 0$$

$$m(m-3) - 2(m-3) = 0$$

$$\Rightarrow (m-2)(m-3) = 0$$

$$m = 2, 3$$

Homogeneous sol^n,

$$a_r^{(h)} = C_1 \cdot 2^r + C_2 \cdot 3^r$$

Here, $f(r) = 2^r + r$

Let $a_5^{(P)} = Ar2^r + A_0 + A_1 r$ be a trial sol^n of (i)

~~from equ^n (i) so~~, the given equ^n

$$\Rightarrow \left[A \cdot r\, 2^r + A_0 + A_1 r\right] - 5\left[A.(r-1).2^{r-1} + A_0 + A_1 . \cancel{r}(r-1)\right]$$
$$+ 6\left[A(r-2)2^{r-2} + A_0 + A_1(r-2)\right] = 2^r + r$$

$$\Rightarrow \left[A \cdot r - \frac{5}{2} A.(r-1) + \frac{3}{2} A(r-2)\right] 2^r + \left[A_1 - 5A_1 + 6A_1\right] r$$

$$+ \left[A_0 - 5A_0 + 5A_1 + 6A_0 - 12A_1\right] = 2^r + r$$

PAGE NO.:
DATE:

$$\Rightarrow \left[Ar - \frac{5}{2}Ar + \frac{5A}{2} + \frac{3}{2}Ar - 3A\right]2^r + \left[2A_1\right]r +$$

$$\left[2A_0 - 7A_1\right] = 2^r + r$$

$$\Rightarrow \left[\cancel{Ar} - \cancel{Ar} + \cancel{\frac{1}{2}} + \frac{5}{2}A - 3A\right]\cancel{r}2^r + \left[2A_1\right]r + \left[2A_0 - 7A_1\right] = 2^r + \cancel{r}$$

$$\left[\left(-\frac{1}{2}\right)A\right]2^r$$

$$\Rightarrow \cancel{\left(-\frac{1}{2}\right)2^r} + (2A_1)r + (2A_0 - 7A_1) = 2^r + r$$

and cons.

Comparing coeff. ↑ both the sides,

$$\cancel{-2^{r-1}}$$

$$\Rightarrow \cancel{\frac{1}{2}} = \cancel{1} \qquad -\frac{1}{2}A = 1 \Rightarrow A = -2$$

$$2A_1 = 1$$

$$A_1 = 1/2 \text{ and}$$

$$2A_0 - 7A_1 = 0$$

$$7\left(\frac{1}{2}\right) = 2A_0 \Rightarrow A_0 = 7/4$$

$$\Rightarrow a_r^{(p)} = -2\cdot 2^r + \frac{7}{4} + \frac{1}{2}r$$

$$\Rightarrow a_r = a_r^{(h)} + a_r^{(p)}$$

$$\Rightarrow a_r = C_1 2^r + C_2\cdot 3^r - 2\cdot r\cdot 2^r + \frac{7}{4} + \frac{1}{2}r$$

Put $r=0$, and $r=1$

$$\Rightarrow a_0 = C_1 + C_2 + \frac{7}{4}$$

$$\Rightarrow 1 = C_1 + C_2 + \frac{7}{4} \Rightarrow C_1 + C_2 = \frac{-3}{4} \quad -(i)$$

And,

$$a_1 = 2C_1 + 3C_2 - 4 + \frac{7}{4} + \frac{1}{2}$$

$\Rightarrow \quad 2C_1 + 3C_2 - \frac{7}{4} = 1$

$\Rightarrow \quad 2C_1 + 3C_2 = \frac{11}{4}$ —(iii)

equ^n (ii) ×2 − equ^n (iii)

$\Rightarrow \quad \cancel{2C_1} + 2C_2 - \cancel{2C_1} - 3C_2 = \frac{-3}{2} - \frac{11}{4}$

$\Rightarrow \quad + C_2 = \frac{+17}{4}$

And, $\quad C_1 = \frac{-3}{4} - \frac{17}{4} = -5$

So, total sol^n,

$a_r = -5 \cdot 2^r + \frac{17}{4} \cdot 3^r - 2r \cdot 2^r + \frac{7}{4} + \frac{1}{2} r$ Ans.

Q.) $a_r - 4a_{r-1} + 4a_{r-2} = (r+1)^2, \quad r \geq 2$
with $a_0 = 0, a_1 = 1$.

Q.) Solve. $a_r + a_{r-2} = 0$ with $a_0 = 0$, $a_1 = 1$.

Sol.) Here, $E^2 a_{r-2} = a_r$

$\Rightarrow E^2 a_{r-2} + a_{r-2} = 0 \qquad f_r = 0$

$\Rightarrow (E^2 + 1) a_{r-2} = 0$

A.E. is $m^2 + 1 = 0$

$\Rightarrow m = \pm i \qquad \Rightarrow m_1 = 0 + i$

—(ii) $\qquad \Rightarrow m_2 = 0 - i$

$\Rightarrow a_r^{(h)} = (0+i)^r + (0-i)^r \qquad a = 0$

$R = \sqrt{0+1} = 1 \qquad b = 1$

$\theta = \tan^{-1}(1/0) = \frac{\pi}{2}$

Scanned by CamScanner

PAGE NO.:
DATE:

$\Rightarrow q_r^{(h)} =$

Q.) Solve the recurrence relation.

$y_{h+2} + y_{h+1} + y_h = h^2 + h + 1$ with $y_0 = 0$, $y_1 = \frac{\pi}{2}$

Sol.) Put $f_h = 0 \Rightarrow h^2 + h + 1 = 0$

$E^2 y_h = y_{h+2}$, $E y_h = y_{h+1}$

$\Rightarrow E^2 y_h + E y_h + y_h = 0$

$\Rightarrow (E^2 + E + 1) = 0$

A.E. is $m^2 + m + 1 = 0$

$\cancel{\left(m + \frac{1}{2}\right)^2 + 3/4 = 0}$

$(A_0 = 1/9,\ A_1 = -1/3,\ A_2 = 1/3)$

$D = b^2 - 4ac$

$1 - 4 = -3$

$m = \frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm \sqrt{3} i}{2}$

$a = -\frac{1}{2}$

$b = \frac{\sqrt{3}}{2}$

Q.) Solve. $y_k + 4 y_{k-1} + 4 y_{k-2} = \cos 3k$

Sol.) Put $f_k = 0$, here $E^2 y_{k-2} = y_k$

$E y_{k-2} = y_{k-1}$

$\Rightarrow E^2 y_{k-2} + 4 E y_{k-2} + 4 y_{k-2} = 0$

$\Rightarrow (E^2 + 4E + 4) y_{k-2} = 0$

$\Rightarrow (E+2)^2 y_{k-2} = 0$

$\Rightarrow$ A.E. is $(m+2)^2 = 0$

$\Rightarrow m_1 = -2,\ m_2 = -2$

Homogeneous solⁿ,

$q_r^{(h)} = C_1 (-2)^r + C_2 (-2)^r$

Here, $f_r = \cos 3k$

$R =$

Scanned by CamScanner

PAGE NO.:
DATE:

$R = \sqrt{a^2+b^2} = \sqrt{\frac{1}{4}+\frac{3}{4}} = 1$

$\theta = \tan^{-1}\left(b/a\right) = \tan^{-1}(-\sqrt{3}) = \tan^{-1}\left(\tan\left(\pi - \frac{\pi}{3}\right)\right)$

$\theta = \frac{2\pi}{3}$

Homogeneous sol^n,

$$y_n^{(H)} = R^n\left(A\cos\frac{2\pi n}{3} + B\sin\frac{2\pi n}{3}\right) \quad \text{—(i)}$$

Now, $f(n) = n^2+n+1$

let $y_n^{(P)} = A_0 + A_1 n + A_2 n^2$ —(ii) be a trial sol^n of equ^n (i)

$\Rightarrow \left[A_0 + A_1(n+2) + A_2(n+2)^2\right] + \left[A_0 + A_1(n+1) + A_2(n+1)^2\right] + \left[A_0 + A_1 n + A_2 n^2\right] = n^2+n+1.$

$\Rightarrow A_0 = 1/9, \quad A_1 = -1/3, \quad A_2 = 1/3$

$\therefore$ from equ^n (ii)

$y_n^{(P)} = \frac{1}{9} - \frac{1}{3}n + \frac{1}{3}n^2$

$A = -1/9$

$B = 1/3\sqrt{3}$

Now,

$y_n = y_n^{(H)} + y_n^{(P)}$

$= A\cos\frac{2\pi n}{3} + B\sin\frac{2\pi n}{3} + \frac{1}{9} - \frac{1}{3}n + \frac{1}{3}n^2$

Put $n=0$

$y_0 = A + \frac{1}{9} \quad \Rightarrow \quad A = -1/9$

Put $n=1$

$y_1 = -\frac{A}{2} +$

Generating function –

A generating f^n for the sequence $\{a_n\}_{n=0}^{\infty}$ is an infinite series:

$$A(t) = \sum_{n=0}^{\infty} a_n t^n = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \text{-----}$$

where the sequence $\{a_n\}_{n=0}^{\infty}$ is called a discrete numeric f^n.

Q.) Find the generating f^n for the sequence $\left\{\frac{1}{n!}\right\}_{n=0}^{\infty}$.

Sol.) Here,

$$a_n = \frac{1}{n!}$$

$$a_0 = 1, \quad a_1 = \frac{1}{1!}, \quad a_2 = \frac{1}{2!}, \quad a_3 = \frac{1}{3!}, \text{---}$$

By def^n

$$A(t) = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \text{----}$$

$$= 1 + \frac{1}{1!}t + \frac{1}{2!}t^2 + \frac{1}{3!}t^3 + \text{---}$$

$$= e^t \quad \text{Ans.}$$

Q.) Find the discrete numeric f^n for $A(t) = \frac{1}{1-t}$.

Sol.)

* Formulas :-

(1) Binomial Theorem

$$(x+a)^n = x^n + {}^nC_1 x^{n-1} a + {}^nC_2 x^{n-2} a^2 + \text{----} + a^n$$

$$(1+x)^n = 1 + nx + \frac{n(n-1)}{2!}x^2 + \frac{n(n-1)(n-2)}{3!}x^3 + \text{---} + x^n$$

$$(1+x)^{-1} = 1 - x + x^2 - x^3 + x^4 \text{----}$$

$$(1-x)^{-1} = 1 + x + x^2 + x^3 + x^4 + \text{----}$$

$(1+x)^{-2} = 1 - 2x + 3x^2 - 4x^3 + \dots$

$(1-x)^{-2} = 1 + 2x + 3x^2 + 4x^3 + \dots$

$(1+x)^{-3} = 1 - 3x + 6x^2 - 10x^3 + \dots$

$(1-x)^{-3} = 1 + 3x + 6x^2 + 10x^3 + \dots$

Given, $A(t) = (1-t)^{-1}$

Using binomial expansion,

$(1-t)^{-1} = 1 + t + t^2 + t^3 + \dots = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \dots$

$\Rightarrow a_0 = 1, \quad a_1 = 1, \quad a_2 = 1, \quad a_3 = 1, \dots, a_n = 1.$

Discrete numeric f^n, $a_r = 1$, $r \geq 0$

Ans.

Q.) Find the ~~numeric~~ generating f^n for the

$$a_r = \begin{cases} 3^r, & \text{if } r \text{ is even} \\ -3^r, & \text{if } r \text{ is odd.} \end{cases}$$

Sol.) Here,

$a_0 = 1, \quad a_1 = -3, \quad a_2 = 3^2, \quad a_3 = -3^3,$

$a_4 = 3^4, \quad a_5 = -3^5, \quad a_6 = 3^6, \quad a_7 = -3^7, \dots$

By def^n,

$A(z) = a_0 + a_1(z) + a_2(z)^2 + a_3(z)^3 + a_4(z)^4 + \dots$

$= 1 - (3z) + (3z)^2 - (3z)^3 + (3z)^4 \dots$

$= (1+3z)^{-1} = \dfrac{1}{1+3z}$ Ans

Q.) If $A(z) = \dfrac{1}{1+3z}$, then find the discrete numeric f^n.

PAGE NO.:
DATE:

Q.) Apply generating f^n technique to solve the initial value problem $y_{n+1} - 2y_n = 0$ with $y_0 = 1$.

Sol.) Let $y(t) = \sum_{n=0}^{\infty} y_n t^n$ be a generating f^n.

Given, $y_{n+1} - 2y_n = 0$

$$\Rightarrow y_{n+1} \cdot t^n - 2y_n t^n = 0$$

$$\Rightarrow \sum_{n=0}^{\infty} y_{n+1} \cdot t^n - 2\sum_{n=0}^{\infty} y_n \cdot t^n = 0$$

$$\Rightarrow \frac{1}{t}\left[y_1 t + y_2 t^2 + y_3 t^3 + y_4 t^4 + \ldots\right] - 2 \cdot y(t) = 0$$

$$\Rightarrow \frac{1}{t}\left[y(t) - y_0\right] - 2y(t) = 0$$

$$\Rightarrow y(t) - 1 - 2t\,y(t) = 0$$

$$\Rightarrow y(t)\left[1 - 2t\right] = 1$$

$$\Rightarrow y(t) = \frac{1}{1-2t}$$

$$\Rightarrow y(t) = (1-2t)^{-1}$$

$$\sum_{n=0}^{\infty} y_n t^n = \sum_{n=0}^{\infty} (2t)^n \qquad \Bigg| \quad (1-x)^{-1} = \sum_{n=0}^{\infty} x^n$$

$$\boxed{y_n = 2^n}$$

PnC :-

Q.) Show that $c(n,r) = c(n, n-r)$.

Sol.) RHS $\Rightarrow$ ${}^nC_{n-r} = \frac{n!}{(n-r)!\,r!}$ $\qquad \binom{n}{r} = \binom{n}{n-r}$

LHS $\Rightarrow$ ${}^nC_r = \frac{n!}{r!\,(n-r)!}$

$\Rightarrow$ LHS = RHS

Q.E.D

PAGE NO.:
DATE:

Combinatorial →

Q.1.) find $f(1), f(2), f(3)$ and $f(4)$ if $f(n)$ is defined is defined recursively by $f(0)=1$ and $n=0,1,2,3,\ldots$

(a) $f(n+1) = f(n)+2$
(b) $f(n+1) = 3f(n)$
(c) $f(n+1) = 2^{f(n)}$
(d) $f(n+1) = (f(n))^2 + f(n) + 1$

Sol.) Put $n=0$

(a) $f(1) = f(0)+2$
$f(1) = 1+2 = \underline{3}$

(b) $f(1) = 3 \times f(0) = \underline{3}$

(c) $f(1) = 2^1 = \underline{2}$

(d) $f(1) = 1+1+1 = \underline{3}$

(a) $f(2) = f(1)+2 = 3+2 = \underline{5}$

(b) $f(2) = 3\times 3 = \underline{9}$

(c) $f(2) = 2^2 = \underline{4}$

(d) $f(2) = 9+3+1 = \underline{13}$

(a) $f(3) = 5+2 = \underline{7}$

(b) $f(3) = 3\times 9 = \underline{27}$

(c) $f(3) = 2^4 = \underline{16}$

(d) $f(3) = 169+14 = \underline{183}$

(a) $f(4) = 7+2 = 9$

(b) $f(4) = 3\times 27 = 81$

(c) $f(4) = 2^{16}$

(d) $f(4) = (183)^2 + 184$

Recursive Algorithm →

Def^n:- An algorithm is called recursive, if it solves a problem by reducing it to an instance of the same problem with smaller input.

PAGE NO.:
DATE:

P-1. Write a recursive algorithm for computing $n!$, where n is a non-negative integer.

Sol.) Procedure factorial (n: non-negative integer)
if $n = 0$ then
factorial $(n) := 1$
else
factorial $(n) := n \cdot$ factorial $(n-1)$

P-2. Write a recursive algorithm for computing a^n, where n is non-negative integer and a is a non-zero real no.

Sol.) Power (a: non-zero real no., n: non-negative integer)

P-3. Write a recursive algorithm for computing $b^n \bmod m$, where b, n and m are integer with $m \geq 2, n \geq 0$, and $1 \leq b \leq m$.

If $n = 0$

$2^0 \equiv 1 \bmod 3$

$2^4 \equiv 1 \bmod 3$ (taking remainder)

$2^4 \bmod 3 = (2 \cdot 2^3 \bmod 3) \bmod 3$

$\therefore \boxed{b^n \bmod m = (b \cdot b^{n-1} \bmod m) \bmod m}$
($n \to$ even)

P-4 Give a recursive algorithm for computing the greatest common divisor of two non-negative integers a and b with $a < b$.

P-5. Construct a recursive version of a binary search algorithm.

PAGE NO.:
DATE:

UNIT - 2

1) Reflexive prop. → $x R x$ → general symbol ..

where, $x \in I^+$

We know that every element divides itself.

i.e., x divides x

$x | x \Rightarrow x \leq x$

Reflexive prop. is valid.

2) Anti-symmetric prop. → $x R y,\ y R x \Rightarrow x = y$

where, $x, y \in I^+$

$x | y,\ y | x$

$\frac{y}{x} = C_1,\quad \frac{x}{y} = C_2$

Treating , as mul^n sign, we get

$\frac{y}{x} \cdot \frac{x}{y} = C_1 \cdot C_2$

$\Rightarrow 1 = C_1 \cdot C_2$

$\Rightarrow \boxed{C_1 = C_2 = 1}$

$\Rightarrow \frac{Y}{x} = \frac{x}{Y} = 1$

$\Rightarrow Y^2 = x^2 \Rightarrow \boxed{x = Y}$

Anti-symmetric prop. is satisfied.

Scanned by CamScanner

GOBOO PAGE NO.: DATE:

3) Transitive prop. $\rightarrow$ $x R y$, $y R z$ $\Rightarrow$ $x R z$
where, $x, y, z \in I^+$

$x | y$, $y | z$

$\frac{y}{x} = c_1$, $\frac{z}{y} = c_2$

$\Rightarrow \frac{y}{x} \cdot \frac{z}{y} = c_1 \cdot c_2 \Rightarrow \frac{z}{x} = c_1 \cdot c_2 = c_3$

$\Rightarrow x | z \Rightarrow x \leq z$
or $\underline{x R z}$

Transitive prop. is satisfied.

Q.) Prove that the relation ("less than equals to") is partial order relation for the set of all positive integers.

~~Sol~~)

Special elements in Partial order set -

(1) Greatest element / unit element / highest element / last / 1

Def^n $\rightarrow$
Any element $a \in P$ is called greatest if $x \leq a$, $\forall x \in P$.

(2) least element / zero / lowest / first / 0 $\Rightarrow$

Def^n $\rightarrow$
Any element $b \in P$ is called least if $b \leq x$, (it precedes remaining element) $\forall x \in P$.

(3) Maximal element $\Rightarrow$
If $m \in P$, then it is called maximal, if $m \leq x$

$\Rightarrow m = x \quad \forall \ x \in P$.

We can also say that no element succeeds m.

(4) Minimal element $\Rightarrow$

Any element $n \in P$ is called minimal, if $x \leq n \Rightarrow x = n$. $\forall \ x \in P$.

We can also say that no element ~~succeeds~~ precedes n.

Wellordered set $\rightarrow$

Any set is said to be well-ordered, if for every subset (non-empty) the set has least elements.

Ex:- set of natural no and whole no. are well ordered set b/s they have a certain min. value.

Bounds $\rightarrow$

(1) Upper bound $\Rightarrow$ let $(P, \leq)$ be a partial order set and $A \subset P$ (proper subset), then u is called upper bound of A if $a \leq u$, $\forall \ a \in A$.
$(u \in P)$

u is also called least upperbound (LUB) / Supremum, if $u \leq v$ where, v is another upper bound.

(2) Lower bound $\Rightarrow$ let $(P, \leq)$ be a partial order set and $A \subset P$, then l is called lower bound of A $(l \in P)$, if $l \leq a$ (l precedes a), $\forall \ a \in A$.

l is also called greatest lower bound (GLB)/ infimum, if $w \leq l$ where, w is another lower bound.

Remark: LUB and GLB behave like binary operators and can be expressed as

GLB $g.l.b\{a,b\} = \inf\{a,b\} = a \cdot b = a \circledast b = a \wedge b$ = meet = product

$l.u.b = \{a,b\} = \sup\{a,b\} = a+b = a \oplus b = a \vee b$ = join = sum

Q.) $P = \{1,2,3,4,5\}$
obtain upper bound.
$1 \leq 2,3,4,5$
$2 \leq 3,4,5$

▷ Lattice – (1) as algebraic system
If L is any non-empty set under two binary operations meet $(\wedge)$ and join $(\vee)$, then algebraic structure $(L, \wedge, \vee)$ is said to be lattice if following prop. is satisfied.

(a) Idempotent $a \wedge a = a$, $a \vee a = a$
(b) Commutative $a \wedge b = b \wedge a$, $a \vee b = b \vee a$
(c) Associative $a \wedge (b \wedge c) = (a \wedge b) \wedge c$; $a \vee (b \vee c) = (a \vee b) \vee c$
(d) Absorption $\left\{ \begin{array}{l} a \wedge (a \vee b) = a \\ a \vee (a \wedge b) = a \end{array} \right.$

(2) Lattice as partial order set.
Any partial order set $(L, \leq)$ is called lattice if for every pair of two elements, the binary opⁿ meet and join can be defined as
$a \vee b = l.u.b\{a,b\}$
$a \wedge b = g.l.b\{a,b\}$

$\leq \rightarrow$ partial order relⁿ

PAGE NO.:
DATE:

such that both are closed. (Closure prop.)

▷ Types of Lattice →

(a) Distributive / Distributed – A lattice is said to be distributive if for all elements it satisfy distributive prop. $(L, \leq, \wedge, \vee) \rightarrow$ structure

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$
$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

(b) Complemented lattice – A lattice $(L, \leq, \wedge, \vee)$ is said to be complemented if it is bounded (it means there exist LB = 0 and UB = 1). And its every element has a complement.

$a \wedge a' = 0$ $\quad$ $a \wedge 0 = 0$ $\quad$ $a \wedge 1 = a$

$a \vee a' = 1$ $\quad$ $a \vee 0 = a$ $\quad$ $a \vee 1 = 1$

Q.) Let N be the set of +ve integers where the meaning of $x \leq y$ is "x divides y", then show that N is a lattice where meet and join defined by

$$a \wedge b = HCF\{a, b\}$$
$$a \vee b = LCM\{a, b\}$$

Sol.) To show that $(N, \leq, \wedge, \vee)$ is a lattice, we have to prove following properties.

I) Reflexive → $x \in N$

x divides x

$x \leq x \Rightarrow x R x$

Anti

(i) Symmetric $\rightarrow$ $x, y \in N$

$$x \leq y , \; y \leq x \Rightarrow x = y$$

$$\frac{y}{x} = C_1 , \quad \frac{x}{y} = C_2$$

$$C_1 C_2 = 1 \Rightarrow \boxed{C_1 = C_2 = 1}$$

$$\frac{y}{x} = \frac{x}{y} \Rightarrow y^2 = x^2$$

$$\Rightarrow \boxed{y = x}$$

(iii) Transitive $\rightarrow$ $x, y, z \in N$

$$x \leq y , \; y \leq z \Rightarrow x \leq z$$

$$\frac{y}{x} = C_1 , \quad \frac{z}{y} = C_2$$

$$\Rightarrow \frac{z}{x} = C_3 \Rightarrow \underline{x \leq z}$$

Closure prop.: $a, b \in N$

$$a \wedge b = HCF\{a, b\}$$

$$a \vee b = LCM\{a, b\}$$

$$a \wedge b , \; a \vee b \in N$$

Clearly for every pair of two elements their HCF & LCM are +ve integer nature.
It means results should belong to N. This is called closure prop. or we can say that structure is closed.
Hence it is proved that N is lattice.

Q. In Boolean algebra $(B, \wedge, \vee, ')$ rel^n is defined by $a \leq b \Rightarrow a \wedge b = a$ or $a \vee b = b$, then prove that rel^n $\leq$ is partial order rel^n and $(B, \leq)$ is lattice

PAGE NO.:
DATE:

Sol.) At first we shew that relⁿ is "partial order relⁿ".

(a) Reflexive → $x R x$

$a \in B$

$a \wedge a = a$ $\quad\quad$ $a \vee a = a$

$a \leq a$ $\quad\quad$ $a \leq a$

$a R a$

Hence, reflexive prop. is satisfied

(b) Anti-symmetric → $x R y, y R x \Rightarrow x = y$

$a, b \in B$

$a \leq b, \quad b \leq a$

$a \wedge b = a, \quad b \wedge a = b$ $\quad\quad$ (Meet)

By comm. law,

$a \wedge b = b \wedge a \quad \Rightarrow \boxed{a = b}$

$a \vee b = b, \quad b \vee a = a$ $\quad\quad$ (Join)

By comm. law

$a \vee b = b \vee a \quad \Rightarrow \boxed{b = a}$

(c) Transitive → $x R y, y R z \Rightarrow x R z$

$a, b, c \in B$

$a \leq b, \ b \leq c$

$a \wedge b = a, \quad b \wedge c = b$ $\quad\quad$ $a \vee b = b, \ b \vee c = c$

$a \wedge (b \wedge c) = a$ $\quad\quad$ $(a \vee b) \vee c = c$

$(a \wedge b) \wedge c = a$ $\quad\quad$ $a \vee (b \vee c) = c$

$a \wedge c = a$ $\quad\quad$ $a \vee c = c$

$a \leq c$ $\quad\quad$ $a \leq c$

$\Rightarrow a R c$

Hence, transitive prop. is satisfied.

PAGE NO:
DATE:

Closure prop. →

For this we will show that

$a \wedge b = g.l.b \{a, b\}$

$a \vee b = l.u.b \{a, b\}$

both are exist.

At first we show $a \wedge b$ is a lower bound.

$a \wedge b \leq a$ $\quad$ $a \wedge b \leq b$

Acc. to absorption law,

$a \vee (a \wedge b) = a$ $\quad$ $b \vee (b \wedge a) = b$

$(a \wedge b) \vee a = a$ $\quad$ $(b \wedge a) \vee b = b$

$(a \wedge b) \vee b = b$

Now, we show that it is greatest lower bound.

for this suppose that there exist another lower bound c.

$c \leq a$ $\quad$ $c \leq b$

$c \wedge a = c$ $\quad$ $c \wedge b = c$

$c \wedge (a \wedge b) = (c \wedge a) \wedge b$

$= c \wedge b$

$= c$

$\boxed{c \leq a \wedge b}$

Q.) Prove that if lattice L is distributive then

$(a \vee b) \wedge (b \vee c) \wedge (c \vee a) = (a \wedge b) \vee (b \wedge c) \vee (c \wedge a)$

Sol.) LHS → By comm. law,

$= (a \vee b) \wedge (c \vee b) \wedge (c \vee a)$

$= [(a \wedge c) \vee b] \wedge (c \vee a)$

$= [(a \wedge c) \wedge (c \vee a)] \vee [b \wedge (c \vee a)]$

$= \{[(a \wedge c) \wedge c] \vee [(a \wedge c) \wedge a]\} \vee \{(b \wedge c) \vee (b \wedge a)\}$

$= (a \wedge c) \vee (a \wedge c) \vee (b \wedge c) \vee (b \wedge a)$

$= (a \wedge c) \vee (b \wedge c) \vee (b \wedge a)$

$= (a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \rightarrow$ RHS

Theo:

➢ In a distribution lattice, if element has complement then show that this complement is unique

→ Let ~~this~~ $(L, \leq, \wedge, \vee)$ be a bounded distribution lattice where element $a \in L$ (non-empty set). Let this element has two different complement elements.

$a \quad b \qquad\qquad a \quad c$

$a \wedge b = 0 \qquad\qquad a \wedge c = 0$

$a \vee b = 1 \qquad\qquad a \vee c = 1$

To prove: $b = c$

$b = b \wedge 1$ (idempotent law)

$= b \wedge (a \vee c)$

$= (b \wedge a) \vee (b \wedge c) = 0 \vee (b \wedge c)$

$= (a \wedge c) \vee (b \wedge c)$

$= (a \vee b) \wedge c = 1 \wedge c = c$

Hence, $\boxed{b = c}$

It is proved that for every element there exist only one complement element.

• Boolean Algebra - $(B, +, \cdot, ')$

Every algebraic structure is called Boolean algebra if following prop. are satisfied.

(1) Closure prop. → $a, b \in B \Rightarrow a + b \in B$

$a \cdot b \in B$

PAGE NO.:
DATE:

(2) Commutative prop. $\rightarrow$ $a+b = b+a$

$a \cdot b = b \cdot a$

(3) Distributive prop. $\rightarrow$ $a \cdot (b+c) = a \cdot b + a \cdot c$

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

(4) Identity prop. $\rightarrow$ $a + 0 = a$

$a \cdot 1 = a$

(5) Inverse prop. $\rightarrow$ $a + a' = 1$

$a \cdot a' = 0$

> Idempotent Theorem/Law — (I) $a + a = a$ (II) $a \cdot a = a$

Proof :- L.H.S $\rightarrow$ $a + a = (a+a) \cdot 1$

$= (a+a) \cdot (a+a')$

(Inverse distributive) $= a + (a \cdot a')$

$= a + 0 = a \rightarrow$ RHS

Q.E.D

> Absorption Theorem — $a + (a \cdot b) = a$; $a \cdot (a+b) = a$

Proof :- L.H.S $\rightarrow$ $a + (a \cdot b) = (a \cdot 1) + (a \cdot b)$

$= a \cdot (1 + b)$ $[\because a + 1 = 1]$

$= a \cdot 1 = a$

> De-Morgan's Theorem — $(a+b)' = a' \cdot b'$

Proof :- We know that, $a + a' = 1$ $\Rightarrow$ $(a+b) + (a+b)' = 1$

$a \cdot a' = 0$ $\Rightarrow$ $(a+b) \cdot (a+b)' = 0$

$(a+b) + (a' \cdot b') = (a+b+a') \cdot (a+b+b')$

$= (a+a'+b) \cdot (a+b+b')$

$= (1+b) \cdot (a+1) = 1 \cdot 1 = 1$

(Idempotent law)

PAGE NO.:
DATE:

$$\Rightarrow (a+b)\cdot(a'\cdot b') = (a\cdot a'\cdot b') + (b\cdot a'\cdot b')$$
$$= (a\cdot a'\cdot b') + (b\cdot b'\cdot a')$$
$$= (0\cdot b') + (0\cdot a')$$
$$= 0 + 0 = 0$$

SOP $\rightarrow (x\cdot y)+(x'\cdot y)+(x\cdot y')+(x'\cdot y')$

Disjuctive normal form / DNF / Canonical

POS $\rightarrow (x+y)\cdot(x'+y)\cdot(x+y')\cdot(x'\cdot y')$

Conjuctive normal form / CNF / dual canonical

Q.) $ab + [(a+b)'\cdot b]'$

$ab + [(a+b) + b']$

$ab + [a + (b+b')] = ab + [a+1] = ab + 1 = 1$

Q.) Convert given ~~structure~~ f^n in form of CNF.

$f(x,y,z) = x$

$= x + 0$ (add identity law)

$= x + y\cdot y' = (x+y)\cdot(x+y')$

$= (x+y+0)\cdot(x+y'+0)$

$= (x+y+zz')\cdot(x+y'+zz')$

$= (x+y+z)\cdot(x+y+z')$

$(x+y'+z)\cdot(x+y'+z')$

Q.) Convert the expression into DNF.

$f(x,y,z) = (x\cdot y') + (x\cdot z) + (x\cdot y)$

Q.) $f(x,y,z) = x\bar{y}z + x\cdot\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z}$ $\quad \bar{y} + \bar{x}\cdot\bar{z}$

Q.) Deduce the following Boolean f^n by using Quine McCluskey method.

$f = \Sigma m(0,1,3,5,7)$

$0 \to 000$ $\qquad$ $5 \to 101$

$1 \to 001$ $\qquad$ $7 \to 111$

$3 \to 011$

$f = \bar{x}\bar{y}\bar{z} + \bar{x}\bar{y}z + \bar{x}yz + x\bar{y}z + xyz$

$y + \bar{x}\bar{z}$ =

	$\bar{x}\bar{y}$	$\bar{x}y$	xy	$x\bar{y}$
$\bar{z}$	1	1	1	0
z	0	1	1	0

= Ans.

$z + \bar{x}\bar{y}$ =

	$\bar{y}\bar{z}$	$\bar{y}z$	yz	$y\bar{z}$
$\bar{x}$	1	1	1	0
x	0	1	1	0

UNIT - 3
GROUP THEORY

- **Binary operation** → Let G be a non-empty set. The op^n $0 : G \times G \to G$ is called a binary op^n on G, defined as, $0(g_1, g_2) = g_1 0 g_2$.

$$G \times G = \{(g_1, g_2) \mid g_1, g_2 \in G\}$$

(a) Closure law
(b) Associative law
(c) Identity law
(d) Inverse law.

Ex. 1) If $G = N = \{1, 2, 3, \ldots\}$

$0 = +$

$+ : N \times N \to N$ defined by

$+(a, b) = a + b$

$+(2,3) = 5$, $+(1,1) = 2$, $+(2,4) = 6$

$+$ is a binary op^n on N and $(N, +)$ is an algebraic structure.

$(G, 0)$

$(a * b) = a + b + 1$

(c) Identity law :-

$a \cdot 0 \cdot e = e \cdot 0 \cdot a = a$

where e is element.

(b) Associative law :- $a + (b + c) = (a + b) + c$

Def^n (Group) → An algebraic structure $(G, 0)$ where G is non-empty with binary operation '0' is called a group, if

PAGE NO.:
DATE:

G_1 closure law $\Rightarrow$

$\forall\ a, b \in G \Rightarrow a o b \in G$

G is closed w.r.t. 'o'.

G_2 Associative law $\Rightarrow$

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

$a o (b o c) = (a o b) o c$

G_3 $\exists$ of an identity element.

$\forall\ a \in G\ \exists\ e \in G$ such that

$a o e = e o a = a$

e is called an identity element w.r.t 'o'.

G_4 Inverse law $\Rightarrow$

for each $a \in G\ \exists\ a' \in G$ such that

$a o a' = a' o a = e$ where,

a' is called inverse of a in G.

1) Groupoid
2) Semi group
3) Monoid (C, A, I)
4) Abelian group

P-1) Show that the set of all integers is an abelian group w.r.t. '+'.

Sol.) I/Z (set of integers) = $\{ \ldots -3, -2, -1, 0, 1, 2, 3, \ldots \}$

G_1 closure law, $\Rightarrow$

We know that sum of two integers is an Integers.

$\forall\ a, b \in I$

$\Rightarrow a + b \in I$

I is closed w.r.t. '+'.

Scanned by CamScanner

PAGE NO.:
DATE:

G_2 : Associative law →

$\forall\ a,b,c \in I$

We have, $a+(b+c) = (a+b)+c$

Associative law hold in I.

G_3 : Existence of an identity element →

If $a \in I$ $\exists$ $e \in I$ such that

$$a+e = e+a = a$$

$$e = 0$$

$\Rightarrow$ $e = 0$ is an additive identity in I.

G_4 : Existence of ~~an~~ inverse of an element →

If $a \in I$ $\exists$ $a' \in I$ such that

$$a+a' = 0 = a'+a$$

$$\Rightarrow a' = -a$$

$\Rightarrow$ $-a$ is an inverse of a in I.

G_5 : Commutative law →

$\forall\ a,b \in I$

we have, $a+b = b+a$

$\Rightarrow$ Commutative law holds in I.

Hence, I is an abelian group under '+'.

Imp

Q.) Show that the set of all non-zero rational numbers, Q is an abelian group under the operation '$*$', defi[ned] as

$$a*b = \frac{ab}{3}, \quad \forall\ a,b \in Q$$

Sol.) G_1 : Closure law →

We know that, mult^n of two rational numbers is a rational no.

Let $a, b \in Q$

To show, $a * b \in Q$

$\because a, b \in Q$

$\Rightarrow a \cdot b \in Q$

$\Rightarrow \frac{ab}{3} \in Q \quad \Rightarrow a * b \in Q$

Q is closed w.r.t '$*$'.

Imp

Q) Show that the set of all rational numbers other than -1 is an abelian group w.r.t. $*$, ~~where~~ defined as $a * b = a + b + ab$, where a, b are rational no. other than -1.

Sol) Let Q' be the set of all rational no. other than -1.

i.e.,

$$Q' = Q - \{-1\}$$

defined $a * b = a + b + ab$, $\forall\ a, b \in Q'$

To prove,

$(Q', *)$ is an abelian group.

(1) G_1 : Closure law $\rightarrow$

If $a, b \in Q'$ are two arbitrary elements.

To show, $a * b \in Q'$

We know that, sum and mul^n of two rational no. is a rational no.

Given, a, b are rational no.

$\Rightarrow a+b,\ ab$ are rational no.

$\Rightarrow a + b + ab$ is a rational no.

$\Rightarrow a * b$ is a rational no.

It remains to show $a * b \neq -1$.

PAGE NO.:
DATE:

Suppose, if possible $a*b=-1$

$$a+b+ab=-1$$

$\Rightarrow$ $(a+1)+b(a+1)=0$

$\Rightarrow$ $(a+1)(b+1)=0$

$\Rightarrow$ $\cancel{a=b=-1}$ $a=-1$ or $b=-1$

which is a contradiction of $a\neq -1$, $b\neq -1$ and ~~so~~ our assumption is wrong.

i.e., $a*b\neq -1$.

$\Rightarrow$ $a*b\in Q'$, $\forall\ a,b\in Q'$

$\Rightarrow$ ~~$a*$~~ Q' is closed w.r.t. $*$.

(2) G_2: Associative law $\rightarrow$

If $a,b,c\in Q'$

To show,

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

LHS $\rightarrow$ $a*(b*c) = a*(b+c+bc)$

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

Applying ~~and distributive~~ associative law w.r.t. $+$

$= a+(b+c+bc)+ab+ac+a(bc)$

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

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

$= (a*b)*c$ $\rightarrow$ R.H.S.

Hence, associative law holds in Q'.

(3) G_3: Existence of an identity element.

$\forall\ a\in Q'$ $\exists$ $e\in Q'$ such that

$$a*e=a=e*a$$

Now, $a*e=a$

$$a+e+ae=a$$

$(-a)$ is inverse of a

$-a + a + e + ae = -a + a$
$0 + e(a+1) = 0$
$e(a+1) = 0$

$e(a+1) = 0$

$\because \quad a \neq -1 \quad$ i.e., $\quad a+1 \neq 0$

$\Rightarrow \quad e = 0$

$\Rightarrow$ $e = 0$ is an identity element in Q'.

(4) G_4 : Inverse law $\rightarrow$

If $a \in Q'$, $\exists$ $a' \in Q'$ such that
$a * a' = e = a' * a$

Now, $\quad a * a' = e$

$\Rightarrow \quad a + a' + a \cdot a' = 0 \qquad \Rightarrow a + a'(a+1) = 0$

$\Rightarrow \quad a' = \dfrac{-a}{a+1}$

Here, $\boxed{a' = \dfrac{-a}{a+1}}$ is an inverse of a.

(5) G_5 : Commutative law $\rightarrow$

If $a, b \in Q'$

To show, $\quad a * b = b * a$

LHS $\rightarrow$ $\quad a * b = a + b + ab$

Applying commutative law w.r.t $+$.

$= b + a + ba$

$= b * a \rightarrow$ RHS

Hence, commutative law holds in Q'.

Thus, Q' is an abelian group under $+$.

Q) Show that the identity element in a group G is unique.

Q) Show that the inverse of an element in a group G is unique.

> Properties of a group →

- Theorem 1: Show that the identity element in a group is unique.

- Proof :- Let $(G, \cdot)$ be a group

Let e_1, e_2 be two identity elements in G

Since e_1 is an identity element

$$e_1 \cdot e_2 = e_2 = e_2 \cdot e_1 \quad \text{—(i)}$$

e_2 is an identity element in G

$$e_2 \cdot e_1 = e_1 = e_1 \cdot e_2 \quad \text{—(ii)}$$

from (i) and (ii)

$$\boxed{e_1 = e_2}$$

- Theorem 2: If $(G, \cdot)$ is a group then show

(i) $ab = ac \Rightarrow b = c$, $\forall\, a, b, c \in G$

(ii) $ba = ca \Rightarrow b = c$

Proof :- Given, $ab = ac$

(i)

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

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$ (pre-mul^n)

Applying associative prop.,

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

$\Rightarrow eb = ec$ $(\because a^{-1}a = e)$

$$\boxed{b = c}$$

(ii) $(ba)a^{-1} = (ca)a^{-1}$

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

$\Rightarrow be = ce$

$\Rightarrow \boxed{b = c}$

PAGE NO.:
DATE:

• Theorem 3 : Show that the inverse of an element in a group is unique.

Proof: Let $(G, \cdot)$ be a group and $a \in G$.
Let b, c be two inverse elements of a in G.
Since, b is an inverse of a in G.
$\Rightarrow \quad b \cdot a = e = a \cdot b \quad$ —— (i)
where, e is an identity element in G.
Since, c is an inverse of a in G.
$\Rightarrow \quad a \cdot c = e = c \cdot a \quad$ —— (ii)
from (i) and (ii)
$\Rightarrow \quad ba = ca$
$\Rightarrow \quad \boxed{b = c}$

• Theorem 4 : If $(G, \cdot)$ is a group then show,
$(ab)^{-1} = b^{-1}a^{-1}, \quad \forall\ a, b \in G$.

Proof: To show that ~~inver~~ $(ab)^{-1} = b^{-1}a^{-1}$, it remains to show that
$(ab) \cdot (b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1}) \cdot (ab)$

if inverse of x is y.
$\Rightarrow x \cdot y = 1 = y \cdot x$
$\Rightarrow y = x^{-1}$

LHS $\rightarrow \quad \underbrace{(ab)}_{x} \cdot (\underbrace{b^{-1}}_{y}\underbrace{a^{-1}}_{z})$

$= [(ab) \cdot b^{-1}] \cdot a^{-1}$
$= [a \cdot (b \cdot b^{-1})] \cdot a^{-1}$
$= [a \cdot 1] \cdot a^{-1} = a \cdot a^{-1} = 1$

RHS $\rightarrow \quad (\underbrace{b^{-1}}_{x}\underbrace{a^{-1}}_{y}) \cdot \underbrace{(ab)}_{z}$

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

$$\Rightarrow \underbrace{(ab)}_{x}\underbrace{(b^{-1}a^{-1})}_{y} = 1 = \underbrace{(b^{-1}a^{-1})}_{y}\underbrace{(ab)}_{x}$$

The inverse of ab is $b^{-1}a^{-1}$

$$\Rightarrow \boxed{(ab)^{-1} = b^{-1}a^{-1}}$$

Similarly, $(abcd)^{-1} = d^{-1}c^{-1}b^{-1}a^{-1}$, $\forall a,b,c,d \in G$

- Order of a group - The no. of distinct elements in a group G is called order of group.
It is denoted by $O(G)$ or $|G|$.

Order of an element in a group.
If $(G, \cdot)$ is a group and $a \in G$.
The least +ve integer n is called an order of 'a' if $a^n = e$, where e is an identity element in G.

IMP
Q.) Show that the cube roots of unity is an abelian group under the opn muln and find the order of each element in group G.

Sol:)
$$x = (1)^{1/3}$$
$$x^3 - 1^3 = 0$$
$$[a^3 - b^3 = (a-b)(a^2+ab+b^2)]$$
$$\Rightarrow (x-1)(x^2+x+1) = 0$$
$$\Rightarrow x = 1, \quad x = \frac{-1 \pm \sqrt{-3}}{2}$$
$$\Rightarrow x = 1, \omega, \omega^2$$
where,
$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

PAGE NO.:
DATE:

let $G = \{1, \omega, \omega^2\}$

Composition Table

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

I) G_1: Closure prop. $\rightarrow$ From the composition table, all the entries in the composition table are the elements of $G \Rightarrow G$ is closed w.r.t '$\cdot$'

II) G_2: Associative prop. $\rightarrow$ Since all the elements of G are complex numbers.
We know that the associative law holds in the set of all complex no.

$\Rightarrow$ The associative law holds in G.

$\Rightarrow$ $a\cdot(b\cdot c) = (a\cdot b)\cdot c \quad , \forall\ a, b, c \in G$

III) G_3: Existence of an identity element.
From the composition table,

$\forall\ a \in G, \ \exists\ 1 \in G$ such that

$a\cdot 1 = 1\cdot a = a$

$\Rightarrow$ 1 is called an identity element in G.

IV) G_4: Inverse law.
From the composition table, we can see that the inverse of $1, \omega, \omega^2$ are $1, \omega^2, \omega$

* Order of an identity element is 1.

PAGE NO.:
DATE:

v) G_5 : Commutative law →
$\forall\, a, b \in G$ we have
$a \cdot b = b \cdot a$
⇒ Comm. law holds in G.
Hence, G is an abelian group.

$O(G) = 3$

$O(1)$	$O(\omega)$	$O(\omega^2)$
$1^1 = 1$	$(\omega)^1 = \omega$	$(\omega^2)^1 = \omega^2$
$O(1) = 1$	$(\omega)^2 = \omega^2$	$(\omega^2)^2 = \omega$
	$(\omega)^3 = 1$	$(\omega^2)^3 = 1$
	$O(\omega) = 3$	$O(\omega^2) = 3$

Q.) Show that 4th roots of unity is an abelian group under mul^n (.) and find order of each element.

Sol.)
$$x = (1)^{1/4}$$
$$x^4 - 1^4 = 0$$
$$(x^2 + 1^2)(x^2 - 1^2) = 0$$
$$(x^2 + 1^2)(x+1)(x-1) = 0$$
$$x = 1, -1, \quad x^2 = -1$$
$$x = \pm\sqrt{-1} = +i, -i$$

Let $G(1, -1, i, -i)$

Composition Table,

•	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	+1
−i	−i	i	+1	−1

Scanned by CamScanner

Addition modulo m ($+_m$) -
If $a, b \in I$

$a +_m b = r$, $0 \le r \le m$, where r is the least non-negative remainder when $(a+b)$ divided by m.

Ex:- $6 +_5 3 = 4$ $(6+3 = 9/5 = \text{rem.})$

$5 +_5 5 = 0$ $(5+5 = 10/5 = 0)$

Multiplication modulo m ($\times_m$) -
If $a, b \in I$

$a \times_m b = r$, $0 \le r < m$, where r is the least non-negative remainder when $(a \times b)$ divided by m.

Ex:- $6 \times_5 3 = 3$ $(6 \times 3 = 18/5 = 3)$

$5 \times_5 5 = 0$ $(5 \times 5 = 25/5 = 0)$

Congruent modulo m -
$a \equiv b \pmod{m}$

iff $m | a-b$

Q.) Show that $G = \{0, 1, 2, 3, 4\}$ is an abelian group w.r.t. $+_5$. Find the order of each element of G.

Sol.) Composition Table →

$0^{-1} = 0$

$1^{-1} = 4$

$2^{-1} = 3$

$3^{-1} = 2$

$4^{-1} = 1$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

PAGE NO.:
DATE:

Here, $O(G) = 5$ $\qquad 1^1 = 1$

$O(0) = 1$ $\qquad 1^2 = 1 +_5 1 = 2$

$O(1) = 5$ $\qquad 1^3 = 1 +_5 1 +_5 1 = 3$

$O(2) = 5$ $\qquad 1^4 = 1 +_5 1 +_5 1 +_5 1 = 4$

$O(3) = 5$ $\qquad 1^5 = 0$

$O(4) = 5$

Q.) Show that $G = \{0, 1, 2, 3, 4\}$, $\times_5$.

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Subgroup – A non-empty subset H of a group G is called a sub-group of G if it is a group for the composition in G.

* A subset consisting of only identity element of a group G is called a subgroup of the composition in G. Each group is a sub-group of itself.

Improper sub-group :

$H = \{e\}$, Group G

* The identity element of the sub-group H is the same as that of G.

GOBOO
PAGE NO.:
DATE:

The inverse of of $a \in H$ is the same as the inverse of the same as an element of G.

Q) Show that, $H = 3Z = \{\ldots -3, 0, 3, 6, \ldots\}$ is a subgroup of $(Z, +)$.

Imp
Sub-group test theorem:
A necessary and sufficient cond. for a non-empty subset H of a group G to be a subgroup is that $a \in H, b \in H \Rightarrow ab^{-1} \in H$, where b^{-1} is the inverse of b in G.

P-1) ~~Show that H~~ Sol. I) Using sub-group test theo.,
$a + (-b) \in H$
$a - b \in H$
If $x, y \in H$
$x = 3K_1, y = 3K_2$
$\Rightarrow x - y = 3K \in H$

Proof:- The necessary cond: If $H \neq 0$ is a sub-group of a group G.
- To show $\Rightarrow a \in H, b \in H \Rightarrow ab^{-1} \in H$, where b^{-1} is the inverse of b in G.

If $a \in H, b \in H$
$\Rightarrow a \in H, b^{-1} \in H$ (by inverse law)
$\Rightarrow ab^{-1} \in H$

Hence, if $a, b \in H \Rightarrow ab^{-1} \in H$.

The sufficient cond. Let $a, b \in H \Rightarrow ab^{-1} \in H$ where b^{-1} is the inverse of b in G. ——(i)
- To show $\Rightarrow H$ is a sub-group of a group G.

PAGE NO.:
DATE:

- G_1 : Existence of an identity element in H.

  if $a \in H$, $a \in H \Rightarrow aa^{-1} \in H$ (by (i))

  Where a^{-1} is the inverse of a in G.

  $\because aa^{-1} = e \Rightarrow e \in H$

  where e is an identity element in ~~G~~ H.

- G_2 : Inverse law.

  If $a \in H$

  Since, $e \in H$, $a \in H \Rightarrow e.a^{-1} \in H$ (by (i))

  where, a^{-1} is the inverse of a in G.

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

  if $a \in H \Rightarrow a^{-1} \in H$, where a^{-1} is the inverse of a in H.

- G_3 : Closure law.

  If $a, b \in H$

  To show $\Rightarrow a.b \in H$

  Since, $a \in H$, $b \in H$

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

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

  $\Rightarrow ab \in H$

  $\Rightarrow H$ is closed under '.'

- G_4 : Associative law.

  If $a, b, c \in H \subseteq G$

  $\Rightarrow a, b, c \in G$

  $\Rightarrow a(bc) = (ab)c$ (by associative in G)

  $\Rightarrow$ Associative law holds in H.

GOBOO
PAGE NO.:
DATE:

Imp

* Theorem : 2 Show that the intersection of two subgroups of a group G is a subgroup of G.

Proof:- Let H_1 and H_2 be two subgroups of a group G.

| $xy^{-1} \in S$ (under '.') |
| $x-y \in S$ (under '+') |

• To show ⇒ $H_1 \cap H_2$ is a subgroup of G.

Since, H_1 and H_2 are subgroups of G

$e \in H_1$ and $e \in H_2$

$e \in H_1 \cap H_2$ ⇒ $H_1 \cap H_2 \neq \phi$

If $x, y \in H_1 \cap H_2$

⇒ $x, y \in H_1$ and $x, y \in H_2$

⇒ $xy^{-1} \in H_1$ and $xy^{-1} \in H_2$.

⇒ $xy^{-1} \in H_1 \cap H_2$

$\forall\ x, y \in H_1 \cap H_2 \Rightarrow xy^{-1} \in H_1 \cap H_2$

⇒ $H_1 \cap H_2$ is a subgroup of G.

> Theorem 3 : Show that the union of two subgroups of a group G need not be a subgroup of a group G.

Proof:- If $H_1 = 3Z = \{ \ldots -3, 0, 3 \ldots \}$

and, $H_2 = 5Z = \{ \ldots -5, 0, 5 \ldots \}$

are subgroups of Z

⇒ $H_1 \cup H_2 = \{ \ldots -5, -3, 0, 3, 5, 6, 9, 10, 12, 15 \ldots \}$

If $3, 5 \in H_1 \cup H_2$ but $3+5 \notin H_1 \cup H_2$.

∴ $H_1 \cup H_2$ does not hold closure law

Hence, $H_1 \cup H_2$ is not a subgroup of a group G.