Unit-4 (Group Theory, Ring Theory, Coding Theory).

GROUP THEORY

→ Group Theory: It deals with the algebraic structures such as semigroup, monoid, groups.

(B.O.)

→ Binary Operation: Let G be a set of $* : G \times G \to G$ defined by $(a,b) \longmapsto a*b \in G \quad \forall a,b \in G$.

then * is called a Binary Op^n.

eg $* : Z \times Z \longrightarrow Z$

(1) $a * b = a + b$ is B.O. ✓

(2) $a * b = \frac{a}{b}$ X

(3) $N \times N \longrightarrow N$

$a * b = a - b$ not B.O X.

→ Associative Binary Op^n :- A B.O. $* : G \times G \to G$ is called associative B.O. iff $\forall a,b,c \in G$

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

Check associative - $Z * Z \longrightarrow Z$

defined by $a * b = a - b$ ← Not B.O

Let $a,b,c \in Z$

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

$a*(b*c) = a*(b-c) = a-(b-c) = a-b+c$ ← Not equal

$$(a * b) * c \neq a * (b * c)$$

→ Existence of Identity Element :-

Let $* : G \times G \to G$ is a B.O.

then an element $e \in G$ is called an identity element if $\forall a \in G$,

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

eg : $+ : Z \times Z \to Z$

then $a + 0 = 0 + a = a \quad \forall a \in Z$

$\Rightarrow e = 0$ is identity element

eg : $* : Z \times Z \to Z$

$a * b = a - b$

$a * e = e * a = a$

$a - e = a$

$e = 0$

eg : $* : R \times R \to R$

$a * b = a + b + \frac{ab}{2} \in R$

$a * e = e * a = a$

$a * e = a$

$a + e + \frac{ae}{2} = a$

$e = 0$

$a = -2 \times$

$e\left(1 + \frac{a}{2}\right) = 0$

$R^* = R - \{0\}$

$* \; R^* \times R^* \longrightarrow R^*$

$a * b = \frac{a}{b}$

$a * e = \frac{a}{e} = a \qquad e = 1.$

→ Existence of inverse - Let $* : G \times G \longrightarrow G$ be a B.O. and $a \in G$. An element $b \in G$ is called inverse of a denoted by a^{-1} if

$$a * a^{-1} = a^{-1} * a = e$$

Commutative B.O. - Let $* : G \times G \longrightarrow G$ be a B.O. Then $*$ is called commutative iff.

$$a * b = b * a \quad \forall a, b \in G.$$

→ Group: Let G be a set and $* : G \times G \to G$ be a map. Then the set $(G, *)$ is called Group if the following condition holds.

(1). $*$ is a B.O. (a closed map)

(2) $*$ is associative & i.e. $\forall a, b, c \in G$

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

] If holds these 2 property. then called semigroup

(3). Existence of identity: i.e. $\exists$ an element $e \in G$ such that $a * e = e * a = a \quad \forall a \in G$.

(4). Existence of Inverse: $\forall a \in G$, $\exists a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

where $e \in G$ is identity of G.

If prop. (1), (2), (3) holds - called moroid

If all (4) holds - group.

→ Abelian group - A group $(G, *)$ is called an abelian group if $*$ is commutative i.e.

$$a * b = b * a.$$

Eg: 1. $(Z, +)$ → abelian group

$$a^{-1} = -a.$$

2. $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}_{2\times 2} \mid ad - bc \neq 0 \right\}$

$*$ = matrix multiplication

Non abelian group because $a \cdot b \neq b \cdot a$ (matrix multiplication)

$$A^{-1} = \frac{1}{|A|} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Q. Is $(R, *)$ is a group where $* : R \times R \to R$ defined by $a * b = a + b + 2ab$.

Ans. (1). $a * b \in R$

Since $a + b + 2ab$ is a real no.

(sum of real no = real)

(2). $*$ is associative

let $a, b, c \in R$

$$(a * b) * c = (a + b + 2ab) * c$$

$$= (a + b + 2ab) + c + 2(a + b + 2ab)c$$

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

~~$= a + b + 2ab + c + 2a$~~

$$= a + b + c + 2(ab + bc + ac) + 4abc$$

$$a * (b * c) = a * (b + c + 2bc)$$

$$= a + (b + c + 2bc) + 2a(b + c + 2bc)$$

$$= a + b + c + 2(ab + bc + ac) + 4abc$$

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

$*$ is associative

(3). Existence of identity element -

Let $e \in G$ is the identity element

then $\forall a \in G \quad a * e = e * a = a$

$$a + e + 2ae = a$$

$$e(1 + 2a) = 0$$

$1 + 2a \neq 0$ $\boxed{e = 0}$ is identity elem

↓

because $a \neq -1/2$

✗ (not fired)

(4). Existence of inverse - Let $a \in G$ and $b \in G$

is inverse of a $\exists \; a * b = b * a = e = 0$

$$a + b + 2ab = 0$$

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

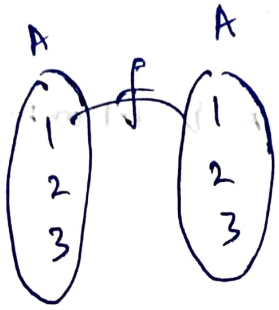
] is inverse of $a \neq -1/2$

$(R, *)$ is not a group

But $(R - \{1/2\}, *)$ is group.

→ Permutation group :-

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



for 1 → 3 choices (1, 2, 3)

2 → (2, 3)

3 → (3)

total ⇒ 3 × 2 × 1

= 6 choices

Total 6 one one onto f^n's possible

$f(1) = 1$

$f(2) = 2$

$f(3) = 3$

$\Rightarrow \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$f(1) = 2$

$f(2) = 1$

$f(3) = 3$

$\Rightarrow \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)$

↓

1 → 2

2 → 1

3 → 3.

$\sigma = (1\ 2\ 3)$

1 → 2

2 → 3

3 → 1

→ Permutation group -

Let $A = \{1, 2, 3, \ldots n\}$ be a set and

$$S_n = \{\sigma \mid \sigma : A \to A \text{ is 1-1 onto fn}\}$$

$$|S_n| = n!$$

Define a map $* : S_n \times S_n \to S_n$

$$\sigma_1 * \sigma_2 = \sigma_1 \circ \sigma_2$$

eg - $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Same

$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$1 \to 2$ and $2 \to 1$

so $1 \to 1$

Check field 1

composition of 1-1, onto map is bijective

therefore $\forall\ \sigma_1, \sigma_2 \in S_n$

$\Rightarrow \sigma_1 \circ \sigma_2 \in S_n$

composition of maps is B.O. on S_n.

check Rule 2 ## $\sigma_1 \circ (\sigma_2 \circ \sigma_3) = (\sigma_1 \circ \sigma_2) \circ \sigma_3$ (Associative)

check Rule 3 ## Identity Element - An identity permutation -

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$ is

identity element of S_n.

check Rule 4 ## Inverse Element :- If $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$$\sigma^{-1} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$\therefore \sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma =$ Identity

Therefore $(S_n, \circ)$ is a group.

Let $\sigma_1 = (1\ 2) \in S_3$ $\quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$\sigma_2 = (2\ 3) \in S_3$ $\quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$$

$\Rightarrow S_n$ is non abelian group.

$n \geq 3$.

→ Order of a group -

Let $(G, *)$ be a finite group then, no. of elements in group is called order of group.

Otherwise it is called of infinite order.

eg : $(Z, +)$, $(R, +)$, $(S, +)$, $(Q, +)$

All are infinite groups.

eg S_n is finite group of order $n!$

→ Order of Element :

Let $(G, *)$ be a group and $a \in G$. Then order of a is least positive integer n (if exists) such that $a^n = e$. where $e \in G$ is the identity element.

otherwise it is called of infinite order.

order of a is denoted by $O(a)$

eg: $(Z, +)$ is a group.

$$Z = \{ \dots \quad 0, \pm 1, \pm 2, \dots \}$$

order of 0 = 1

order of 1 = infinite

2

all infinite

eg: Let $G = \{1, -1, i, -i\}$

$a * b = a.b$

Cayley 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

all elements $\in$ set G.

From calay table - $a * b$ is a B.O because all elem $\in$ set.

- it is clear that- identity element = 1.

Inverse → $a * a^{-1}$ = identity.

	inverse
1	1
-1	-1
i	-i
-i	i

$(G, *)$ is a group.

since calay table is symmetric along its main diagonal therefore it is an abelian group.

order of elements → $o(1) = 1$

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

$o(i) = 4 \rightarrow (i)^4 = 1$

$o(-i) = 4 \rightarrow (-i)^4 = 1$.

Q. If $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \in S_4$

Then find $\alpha\beta$, $\beta\alpha$, α^2 and α^{-1}. Also find order of α, β & $\alpha\beta$.

Sol^n: $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

$\alpha\beta$ (composition)

$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ $\quad \alpha^{-1} = \begin{pmatrix} 3 & 4 & 2 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$

$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1\,3\,2\,4)$ order = 4

$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\,2\,4)$ order = 3

$\alpha^3 = \alpha^2 \cdot \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$

$$\alpha^4 = \alpha^3 \cdot \alpha$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \text{Identity}$$

order = 4.

$O(\alpha) = 4.$

→ Properties of group -

(1). Identity element of $(G, *)$ is unique

(2). Inverse of each element of $(G, *)$ is unique.

(3). Cancellation law in $(G, *)$ holds

i.e. $a * b = a * c \Rightarrow b = c$ (Left cancellation)

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

(4). $(a * b)^{-1} = b^{-1} * a^{-1} \quad \forall a, b \in G$

(5). Only $e \in G$ in the idempotent element of $(G, *)$ G identity

$e * e = e$

→ **Cyclic Group** :- Let $(G, *)$ be a group. Then G is called cyclic group, if there exist an element $a \in G$, such that each element $x \in G$ can be expressed as $x = a^m$ for some integer m.

and 'a' is called generator of G.

and denoted by $G = \langle a \rangle$

eg : $G = \{1, -1, i, -i\}$ $\quad a * b = a.b$

prove that $(G, *)$ is cyclic group.

Sol^n:

$1 = i^4$

$-1 = i^2$

$i = i^1$

$-i = i^3$

} since each element of G can be written as power of 'i' therefore $(G, *)$ is a cyclic group generated by i

i.e. $G = \langle i \rangle$

→ **Properties of cyclic group**:-

1. cyclic group is abelian. (Reverse not true)
2. If a is generator of G then a^{-1} is also generator of G.

$G = \langle a \rangle$, $x = a^m \Rightarrow x = (a^{-1})^{-m}$

2. If $(G, *)$ is a finite cyclic group of order n. Then $\exists$ an element $a \in G$ such that $O(a) = n$.

3. If $(G, *)$ is a finite cyclic group of order n and $G = \langle a \rangle$. Then a^m is also generator of G, iff $\gcd(m, n) = 1$ where $m < n$.

$$O(a^m) = \frac{O(a)}{\gcd(O(a), m)}$$

prop (1). Let G be cyclic, generated by $a \in G$.

Let $x, y \in G$. Then we will prove $x * y = y * x$

$x \in G \Rightarrow x = a^m$
$y \in G \Rightarrow y = a^n$] $\longrightarrow$ for som m, n.

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

commutative $\rightarrow$ abelian

Q prove that $(Z_5, +_5)$ is a finite cyclic group.

Sol $Z_5 = \{0, 1, 2, 3, 4\}$ $\quad Z_m = \{0, 1, 2, \cdots (m-1)\}$

$$a * b = a +_5 b$$

$$3 * 4 = 2. \leftarrow \frac{3+4}{5} = 2 \quad \text{(Remainder.)}$$

Calay Table -

$+_5$	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

→ Subgroup: Let $(G, *)$ be a group. A subset H of G is called subgroup of G if $(H, *)$ ~~is a~~ is itself a group.

and we denote $H \leq G$.

eg: $(Z, +) \leq (Q, +) \leq (R, +) \leq (C, +)$

→ Necessary and sufficient condition for a subset to be a subgroup (One Strip Test).

A subgroup $H \subseteq G$ is called subgroup iff –

(1). $e \in H$, where e is identity of G.

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

Eg: Is $H = \{x \in Z \mid x \text{ is even integer}\}$ is H is subgroup of $(Z, +)$.

(1) 0 is even $\Rightarrow 0 \in H$

i.e. $e = 0$ of Z is an element of H.

(2) Let $x, y \in H \Rightarrow x = 2k_1$

$y = 2k_2$

$y^{-1} = -2k_2$

Now, $x * y^{-1} = 2k_1 + (-2k_2) = 2(k_1 + (-k_2))$

$= 2k$ for some k.

$\in H$

because even integer

$\Rightarrow$ H is subgroup of Z.

Q. Prove that intersection of two subgroups of a group is subgroup but union need not.

proof :- (1) Let $(G, *)$ be a group and H, K are subgroup of G.

$\because$ H and K are subgroup $\Rightarrow$ $e \in H$ & $e \in K$

$\Rightarrow$ $e \in H \cap K$

Let $x, y \in H \cap K \Rightarrow x, y \in H$ and $x, y \in K$

as H and K are subgroups.

$\Rightarrow$ $x * y^{-1} \in H$ and

$x * y^{-1} \in K$

$\Rightarrow$ $x * y^{-1} \in H \cap K$.

$H \cap K \leq G$

(2) union - eg: $(Z, +)$ is a group.

and $H = 2Z = \{0, \pm 2, \pm 4, \ldots\}$

$K = 3Z = \{0, \pm 3, \pm 6, \ldots\}$

are subgroups of $(Z, +)$

$H \cup K = \{0, \pm 2, \pm 3, \pm 4, \pm 6 \ldots\}$

$\left.\begin{matrix} x = 2 \\ y = 3 \end{matrix}\right] \in H \cup K$

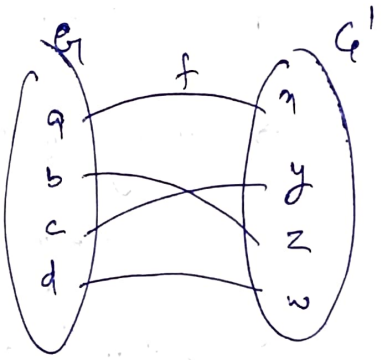
but $x * y^{-1} = 2 + (-3) = -1 \notin H \cup K$

$\Rightarrow H \cup K$ is not a subgroup

→ Group homomorphism –

Let $(G, *)$ and (G', Δ) be two groups and $f: G \to G'$ is a map. Then f is called group homomorphism if

$$f(a * b) = f(a) \Delta f(b) \quad \text{where } \forall a, b \in G$$



Eg:- $f(Z, +) \longrightarrow (Z, +)$

$f(x) = 2x \quad \forall x \in Z$

is a group homo.

Q. Is $f: (Z, +) \longrightarrow (Q, +)$ defined by $f(x) = 2(x-1)$ is a group homo.

Let $x, y \in Z$ then f is group homo.

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

$f(x+y) = 2(x+y-1) = 2x+2y-2$ — (1)

$f(x)+f(y) = 2(x-1)+2(y-1) = 2x+2y-4$ — (2)

(1) $\neq$ (2)

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

$\Rightarrow f$ is not group homo.

→ Kernel of a group homomorphism -

If $f: G \to G'$ be a group homo.

Then $\ker f = \{x \in G \mid f(x) = e' \text{ where } e' \text{ is the identity of } G'\}$

Image of f - $\text{Im} f = \{y \in G' \mid f(x) = y, \text{ for some } x \in G\}$

Q. Show that Kerf is subgroup G and Imf is subgroup of G'.

Q. $f:(R,+) \longrightarrow (R^+,\cdot)$
defined by $f(x) = e^x$

Show that f is a group homo.

Sol" To prove f is group homo, we need to show

$$f(x+y) = f(x)\cdot f(y) \quad \forall\, x,y \in R$$

Let $x,y \in R \Rightarrow f(x) = e^x$, $f(y) = e^y$

Now, $f(x+y) = e^{x+y} = e^x \cdot e^y = f(x)\cdot f(y) \quad \forall\, x,y \in R$

$\Rightarrow$ f is group homo.

Imp.

$\longrightarrow$ Theorem: $f:(G,*) \longrightarrow (G',\Delta)$ is a group homo.

Then (i). $f(e) = e'$, where e and e' are identity of G and G' resp.

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

(iii) If H is subgroup of G, then

$f(H) = \{ f(h) \mid h \in H \}$ is a subgroup of G'

Q. → proof (i) - Let $e \in G$ is identity of $(G, *)$

then $\forall\ a \in G$, $a * e = a$

$\because$ f is a group homo from $G \to G'$

Therefore, $f(a*e) = f(a)$

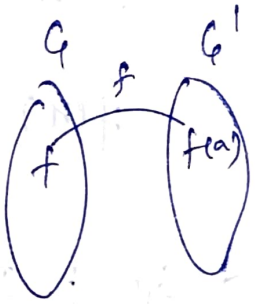
$\Rightarrow f(a) \Delta f(e) = f(a)$

$f(a) \Delta f(e) = f(a) \Delta e'$

$\because e'$ is identity of G'

By cancellation law

$f(e) = e'$



proof -(ii) -

Let a^{-1} is the inverse of $a \in G$.

$\Rightarrow a \times a^{-1} = e$

$\Rightarrow f(a \times a^{-1}) = f(e)$

$f(a) \Delta f(a^{-1}) = e'$

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

→ proof :(iii) As H is subgroup of G

$\Rightarrow e \in H$

$\Rightarrow f(e) = e' \in f(H)$

Let $f(h_1), f(h_2) \in f(H) \Rightarrow h_1, h_2 \in H$ and H is a sub group $\Rightarrow h_1 * h_2^{-1} \in H$

$f(h_1 * h_2^{-1}) \in f(H)$

$f(h_1) \Delta f(h_2^{-1}) \in f(H)$

$f(h_1) \Delta [f(h_2)]^{-1} \in f(H)$

$f(H)$ is subgroups of (G', Δ).

→ Group Isomorphism - Let $(G, *)$ and (G', Δ) are two groups and $f: G \to G'$. Then f is called group isomorphism if (1.) f is homo.

(2) f is 1-1

(3) f is onto.

eg : $G = \{\pm 1, \pm i\}$

$f: (Z_4, +_4) \to (G, \cdot)$

then $f(0) = 1$ $f(3) = -i$

$f(1) = i$ Then f is group iso and

$f(2) = -1$ $Z_4 \cong G$

⇒ If f exist then we call G and G' are isomorphic and write $G \cong G'$.

RING THEORY

(R)
→ Ring: Let R be a set. Consider two binary op^n on R, namely $+$ = addition
& $\cdot$ = multiplication

then $(R, +, \cdot)$ is called ring iff

(1). $(R, +)$ is an abelian group

(2). $(R, \cdot)$ is semigroup.

(3). Multiplication is distributive over addition.

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

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

Eg: $(\mathbb{Z}, +, \cdot)$

$(\mathbb{R}, +, \cdot)$

$(\mathbb{C}, +, \cdot)$

$(\mathbb{Q}, +, \cdot)$ are all rings.

→ Commutative Ring :

Let $(R, +, \cdot)$ is a ring if $\forall\, a, b \in R$

$\Rightarrow a \cdot b = b \cdot a$

then R is called Commutative Ring.

eg: $R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a, b, c, d \in R \right\}$

$+$ = matrix addition

$\cdot$ = matrix multiplication.

Then $(R, +, \cdot)$ is a non-commutative ring

→ Ring with Identity :-(unity)

~~Let $(R, +, \cdot)$ be a ring and $0 \neq$~~

Let $(R, +, \cdot)$ be a ring. Then R is called ring with identity if $\exists$ multiplicative identity (or unity) $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a \;\; \forall\, a \in R$ identity)

→ **Multiplicative inverse** – Let $(R,+,\cdot)$ be a ring and $0 \neq a \in R$. Then an element $b \in R$ is called multiplicative inverse of a $a.b = b.a = 1_R$

→ **Unit element of $(R,+,\cdot)$** – An $a \in (R,+,\cdot)$ is unit element if $\exists\ b \in R$ such that

$$a.b = b.a = 1_R$$

eg: $(R,+,\cdot)$ then $\forall\ a \in R$

$\Rightarrow \frac{1}{a} \in R$ such that $a \otimes \frac{1}{a} = 1_R$

→ **Zero Divisor**:

Let $(R,+,\cdot)$ be a ring then $0 \neq a \in R$ is called zero divisor if $\exists\ b \neq 0 \in R$ such that $a.b = 0$.

Eg: $R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a,b,c,d \in R \right\}$

$+$ = matrix addition.

$\cdot$ = matrix multiplication.

$$A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix}$$

$$A.B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

eg - $(Z_8, +_8, \times_8)$

$2, 4 \in Z_8$ are zero divisor in Z_8

$2 \times_8 4 = 0 \rightarrow \frac{8}{8} = 0$

→ Integral Domain :- A commutative ring with unity ~~identity~~ and without zero divisor is called an ~~ind~~ integral domain.

eg - $(Z, +, \cdot)$ is an integral domain.

→ Field - Let $(F, +, \cdot)$ be a ring. Then it is called field if -

(1). $(F, +)$ is abelian group.

(2). $(F^*, \cdot)$ is abelian group. $(F^* = F - \{0\})$

(3). Multiply is distributive over addition.

An integral domain is called field if every non-zero element has multiplication inverse

Q Prove that $(Z_5, +_5, \times_5)$ is a field.

Sol $Z_5 = \{0, 1, 2, 3, 4\}$ $\quad +_5 = \text{Rem.}\left(\frac{a+b}{5}\right)$

$\times_5 = \text{Rem}\left(\frac{a \times b}{5}\right)$

Calay table for $+_5$

$+_5$	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

(1) all element are $\in Z_5$ so binary op^n.

element	inverse
0	0
1	4
2	3
3	2
4	1

elem + inv. = 0

(2) Let $a, b \in Z_5$. then

$a +_5 (b +_5 c) = (a +_5 b) +_5 c$

Let $a = 2, b = 3, c = 4$.

LHS $= 2 +_5 (3 +_5 4)$

$2 +_5 (2)$

$= 4$

RHS $= 0 +_5 4$

$= 4$ Associative ✓

(3) From 1st row & colm. it is clear that

$0 \rightarrow$ additive identity.

(4) $0+0=0$
$1+4=0$
$2+3=0$
$\vdots$
} inverse of each.

(5) Calay table – symmetric.

$\Rightarrow +_5$ is commutative

i.e. $a +_5 b = b +_5 a$

~~(6)~~ $\Rightarrow (Z_5, +_5)$ is an abelian group.

Calay table for $\times_5$

$\times_5$	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

from calay table.

$(Z_5^*, \times_5) \rightarrow$ abelian group.

0 not included.

$a \times_5 (b +_5 c) = (a \times_5 b) +_5 (a \times_5 c)$

$(a +_5 b) \times_5 c = (a \times_5 c) +_5 (b \times_5 c)$

} Left and Right distributive

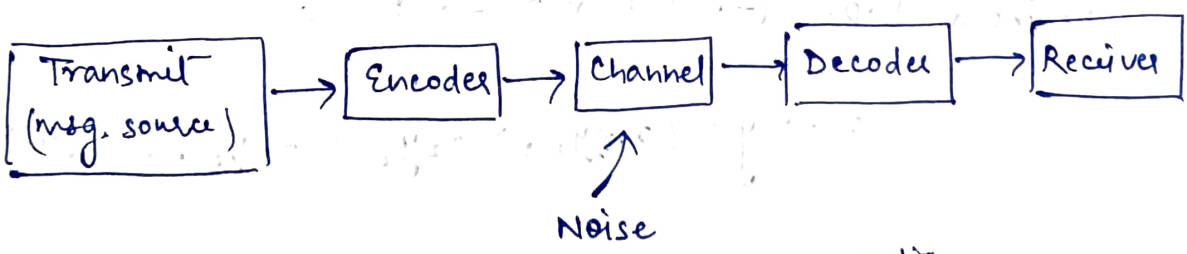
Check by putting $a=2,\ b=3,\ c=4$

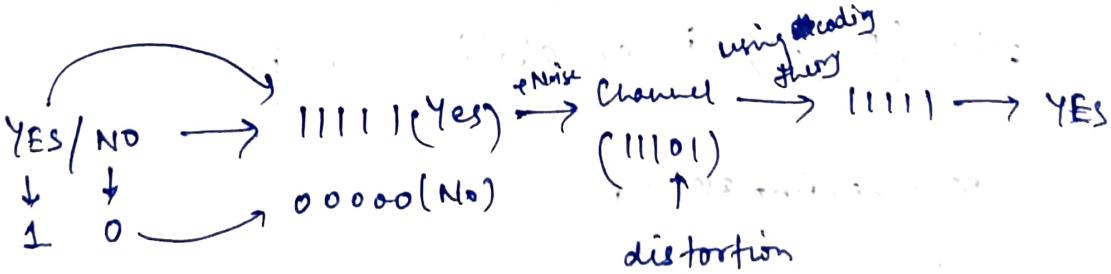
Coding Theory

The process of communication involves transmitting some information carrying signals that is ~~th~~ coverged by a sector to a receiver.

Due to the noise present in channel it may be possible that our message get distorted.

Coding theory deals with minimizing the distortions of the converged message due to the noise and to give the techniqe to receiver to receive the original message.





→ Binary Channel –

In this channel encoder encode the message by using symbols (bit) 0 and 1

→ Group Code –

Let $F = \{1, 0\}$. Then $(F, +_2)$ is an abelian group.

Consider $F^n = \{(x_1, x_2, x_3, \cdots x_n) \mid x_i \in F \ \forall \ i = 1, 2, \cdots n\}$

then let $x = (x_1, x_2, \cdots x_n)$ and

$$y = (y_1, y_2, \cdots y_n) \in F^n$$

Define a B.O. $\oplus : F^n \times F^n \to F^n$ as

$$x \oplus y = (x_1 +_2 y_1, x_2 +_2 y_2, x_3 +_2 y_3 \cdots, x_n +_2 y_n)$$

then $(F^n, \oplus)$ is an abelian group.

~~0 → identity element.~~

~~x inverse = x~~

Any code which is group under the Binary operation $\oplus$ is called group code and elements of F^n are elements.

eg: $(F^3, \oplus)$ is an abelian group.

$F^3 = \{000, 111, 100, 010, 001, 110, 101, 011\}$

↓

(e)

identity

elem.

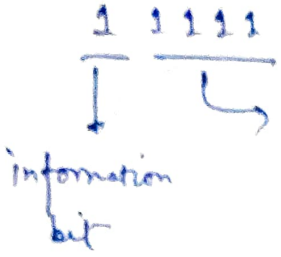
Cayley Table

$\oplus$	000	111	100	010	001	110	101	011
000	000	111	100	010	001	110	101	011
111	111	000	011	101	110	001	010	100
100	100	011	000	110	101	010	001	111
010	010							
001	001							
110	110							
101	101							
011	011							

→ Hamming Code – The code obtained by introducing addition digits called "parity bits", in original message is called Hamming code.

(*). If the original message is a binary string of length m, then the Hamming encoded message is a string of length n ($n > m$). Of the n digits, m digits are used to represent the information called the information bit and remaining $(n-m)$ digits are used to

detect & and correct errors in received ~~memory~~ message.



→ Hamming weight of a codeword :-

Let $x = (x_1, x_2, \dots x_n) \in F^n$.

Then hamming weight of x is the no. of 1's present in the string and is denoted by $|x|$ or wt.(x).

eg: $x = (11001011) \in f^{10}$

$wt(x) = |x| = 6$

→ Hamming Distance :- Let $x, y \in F^n$, then, the hamming distance b/w x and y is the Hamming weight of $x \oplus y$ and denoted by $d(x,y)$

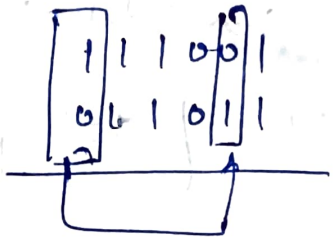
or Hamming distance b/w x and y is the no. of places at which they differ.

eg: $x = 111001 \in F^6$ and $y = 011011 \in F^6$

$$d(x,y) = |x \oplus y| = |1000|0|$$

$$d(x,y) = 2$$

using other method.



at 2 places they differ

$$d(x,y) = 2.$$

→ Hamming distance of a code -

Let C be a code, then Hamming dist. of code C

i.e. $d(C) = \min \{ |x \oplus y| \quad x \neq y \}$

$= \min \{ d(x,y) \mid x \neq y \}$

Imp:

Theorem: If hamming distance = d of code

then it can detect $(d-1)$ errors and correct

$$\left\lfloor \frac{d-1}{2} \right\rfloor \text{ errors.}$$

Coding Theory -

- If minimum distance of a code is d then it can detect atmost $d-1$ errors & correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

Eg if $d=5$ $\left\lfloor \frac{5-1}{2} \right\rfloor$ errors $= 2$

Generator Matrix : Let $e : F^m \to F^n$ (where $m, n \in \mathbb{N}$, $m < n$) be an encoding function.

Then e can be represented by a matrix G over F, called generator matrix for the code, where G, is of form $[I_m : A]_{m \times n}$, where I_m is an identity matrix of order m & A in a $m \times (n-m)$ matrix. If $w \in F^m$, is a message, then $e(w) = wG$ in a codeword & $C = e(F^m) \subseteq F^n$ in a code where $w = [x_1, x_2, \ldots x_m]$.

The matrix $H = \left[A^T \mid I_{n-m} \right]_{(n-m)\times n}$

is called parity check matrix and is useful to decode a codeword to its original message.

Eg: Let $e : F^2 \longrightarrow F^5$ be an encoding fn represented by a Generator matrix $G = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{array}\right]_{2\times 5}$

Then find all the codewords. Also find all the codewords.

Also find parity check matrix and verify that.

Decode the codeword (i) 11101

(ii) 11011

(iii) 11010.

Soln: In $F^2 = \{00, 10, 01, 11\}$

If $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$ is a given matrix.

Then $e(w) = wG$, $w \in F^2$

$e(00) = (00)\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = 00000$

$$e(10) = [10] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = 10110$$

$$e(01) = [01] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = 01011$$

$$e(11) = (11) \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = 11101$$

~~So parity check~~ ∵ H.D. of the code is 3 so it can detect atleast 2 error & correct atleast 1 error.

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

I_m A

so, parity check matrix is $H = [A^T \vdots I_{5-2}]$

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

If H is a parity check matrix and r is received codeword then..

(1). If $H.r^T = [0]$ ⇒ There is no error in transmission and r is the codeword that has been transmitted.

Then the original message is the first 'n' component of received codeword.

(i). r = 11101

$$\text{New } Hr^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

so original msg is 11.

(2) If $H.r^T$ = i^{th} col^m of matrix H, then in the received codeword, there is ~~received~~ an error at i^{th} place. Change the i^{th} component to get a correct codeword c, then the starting 'n' component are original message.

eg (i) r = 11011.

$$Hr^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

↳ 4^{th} col^m

Change 4^{th} bit → 01011.

which is I^{st} col^{n} of H,

$\therefore$ In received codeword, there is error in first place.

$r = 11011 \longrightarrow$ correct is $\longrightarrow 01011$ and original message is 01.

Q. Let $e: F^2 \longrightarrow F^5$ be an encoding f^n given by the matrix $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$

Then find code C generated by G. Show that it is group code. Find min. dist. of C.

$$e(00) = [00]\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [0\ 0\ 0\ 0\ 0]$$

$$e(10) = [10]\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [1\ 0\ 1\ 1\ 0]$$

$$e(01) = [01]\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [0\ 1\ 0\ 1\ 1]$$

(Op^{n} → Add modulo 1+1 = 2 = 0)

$$e(11) = [11]\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [1\ 1\ 1\ 0\ 1]$$

$wt(c) = d(c) = 3 \Rightarrow$ c can detect atmost $(3-1) = 2$ errors and correct $\left\lfloor \frac{3-1}{2} \right\rfloor = 1$

To show, → c is group code -

⊕	00000	10110	01011	11101
00000	00000	10110	01011	11101
10110	10110	00000	11101	01011
01011	01011			
11101	11101			

From Calay table, prove group code.

→ Parity Check Matrix - (PCM.)

Let $e: F^m \to F^n$ be an encoding function and G $G = [I_m \mid A]_{m \times n}$ is a G.M. corresponding to e.

Then the PCM is given by $H = [A^T \mid I_{n-m}]_{(n-m) \times n}$

PCM is useful to decode a message.

How to decode a received vector →

If r is received vector,

(1). If $Hr^T = 0 \Rightarrow$ There is no error in transmission and the receiver vector is same codeword, ~~then~~ that has been sent. Original message is first m components of received vector.

(2). If $Hr^T = i^{th}$ column of the matrix H, then there is error in i^{th} place of received vector. Change the i^{th} component to get original ~~m~~ vector and first m component of this vector are original message.

(3). If it is not of (1) or (2) then more than one error can be detected, but can't correct.

Q Let $e : F^2 \longrightarrow F^5$ be an encoding fⁿ given by matrix. $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$. Find PCM and

$\underbrace{\quad}_{I} \quad \underbrace{\quad\quad}_{A}$

by using it decode → (i). 11101
(ii). 11011
(iii). 11010.

Sol^n. PCM → $H = [A^T \mid I]$

$$H = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

(i) $Hr^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

$Hr^T = 0$. No error. and received vector is correct codeword and 11 is original message

(ii). $r = 11011$

$$Hr^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

Hr^T = 1st column of H.

⇒ There is error at 1st place of received vector.

~~codeword.~~

So correct codeword → 01011.

original message → 01.

(iii). $r = 11010$

$$Hr^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Case-3 ⇒ There is more than one error.

$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ = I^{st} col^{n} + V^{th} col^{n} of H. → There is error at I^{st} & V^{th} place

$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ = II^{nd} + $\underline{IV}^{rd}$ col^{n} of H → Error at II & $\underline{IV}$ place.

↓

Correct codeword ⇒ 01011

original msg = 01

↓

correct codeword ⇒ 10110

original msg = 10.

Qn Find the codiword generated by the encoding function $e: B^2 \longrightarrow B^5$ whose parity check matrix is

$$H = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{matrix} \rightarrow A \\ \\ \\ \\ \end{matrix} \quad I$$

Write H in standard form $H = [A^T : I]_{(5-2)\times 5}$

$$\Rightarrow H = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}_{3\times 5}$$

$$\Rightarrow G = [I_2 : A] = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$B^2 = \{00, 10, 01, 11\}$$

$$e(00) = [00]G = [00]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = 00000$$

$$e(10) = [10]G = [10]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = 10011$$

$$e(01) = [01]G = [01]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = 01011$$

$$e(11) = [11]G = [11]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = 11000$$

$\Rightarrow C = \{00000, 10011, 01011, 11000\}$ are the code generated by e.

(*) $d(C) = 2 \Rightarrow$ C can detect atmost $(2-1) = 1$ error & correct $\left\lfloor \frac{2-1}{2} \right\rfloor = 0$ error.

Qu In previous question, show that the code $C = \{00000, 10011, 01011, 11000\}$ is a group code.

We need to show that $(C, \oplus)$ is an abelian group.

Construct Caley Table.

	00000	10011	01011	11000
00000	00000	10011	01011	11000
10011	10011	00000	11000	01011
01011	01011	11000	00000	10011
11000	11000	01011	10011	00000

∴ all the element of Caley table are member of C ⇒ C is a binary operation.

Also, $\forall\ a, b, c \in C$

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

take $a = 10011$, $b = 01011$, $c = 11000$

$$a \oplus b \oplus c = 10011 \oplus (01011 \oplus 11000)$$
$$= 10011 \oplus (10011)$$
$$= 00000$$

Also $(a \oplus b) \oplus c = 00000$

⇒ $\oplus$ is associative.

From row ① & col ① it is clear that 00000 is identity element of C.

Also inverse of each element exist

Inverse
$00000 = 00000$
$10011 = 10011$
$01011 = 01011$
$11000 = 11000$

Also Caley table is symmetric. Hence C is abelian.

Since C is an abelian group ⇒ C is a group code.

Qus Given the generator matrix $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$

Corresponding to the encoding function $e: B^3 \longrightarrow B^6$. Find corresponding parity check matrix & use it to decode the following received vector & find original message.

(i) 111101 (ii) 100100 (iii) 111100 (iv) 010100

As $G = [I_3 \mid A]_{3\times 6}$

$$H = [A^T \mid I]_{3\times 6} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

(i) $r = 111101$

Now $H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$ = 3rd col of H

⇒ There is error at 3rd component of r. So Correct codeword is = 110101

& Correct messg. is = 110.

(ii) $r = 100100$

$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ = 5th col of H

⇒ There is error at 5th coord. & Hence Correct codeword = 100110

& correct msg = 100

(III) $r = 111100$

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \text{IV}^{th} \text{ col of } H$$

$\Rightarrow$ Error at IVth component of r

$\Rightarrow$ Correct codeword is 111000

& orig. msg = 111

(IV) $r = 010100$

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} =$$ Error can't be corrected

As $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ = Ist + VIth col. = error at Ist & VIth place = Correct codeword = 110101

orig. msg = 110

= IInd + IVth col. = error at II & IVth Place = Correct codeword = 000000

= III + Vth col. = org. msg = 000

= error at III + IVth Place

= Correct codeword = 011010

= org. msg = 011

So there are three possibilities for original message i.e. 110, or 000 or 011

Hence we can't find correct message