Maths

Unit - 4

~~Graph~~ Group Theory

If G is a non-empty set and * is a binary operation of G then the algebric structure $(G, *)$ is called a group if the following condition are satisfied :-

(i) Closure :- $a, b \in G$.

$\Rightarrow a * b \in G$

(ii) Associativity :-

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

(iii) Existence of Identity :-

$a * e = a = e * a$

(iv) Existence of Inverse :-

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

If we add a 5th property of Commutative to the previous 4 property then, the group will be an arbelian group.

(v) Commutative :- $a * b = b * a$

Example :-

If $(I, *)$ is group function for $I = \{-\infty, -3, -2, -1, 0, 1, 2, 3, \infty\}$
Then check whether it is a group or not?

Sol → ① Closure :- $a, b \in G$, $a * b \in G$

$\Rightarrow$ Let 2, 100 be two element $\in G$

$a * b = 2 + 100 = 102 \in G$.

So, it is closed w.r.t operation +.

② Associativity :- $a * (b * c) = (a * b) * c$

Let $a = 1, b = 2, c = 3$

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

$(1 + 2) + 3 = 1 + (2 + 3)$

$6 = 6$

$\Rightarrow$ It is associative

③ Identity :- $a * e = a$

$\Rightarrow a + e = a$

$e = a - a$

$e = 0 \in a$

$\Rightarrow$ Identity exist

④ Inverse :- $a * a^{-1} = e$

$\Rightarrow a + a^{-1} = 0$

$\Rightarrow a^{-1} = -a \in a$.

So, inverse exist.

So, since all 4 condition satisfied So, it is a Group.

Q. Check for group for $(\mathbb{Q}, *)$.

Sol → (1) Closure :- $a * b$

$$= \frac{p}{q} \times \frac{r}{s} = \frac{pr}{qs} \in \mathbb{Q}$$

⇒ It is closed w.r.t ×

(2) Associative :- $a*(b*c) = (a*b)*c$

$$= \frac{p}{q} \times \left(\frac{r}{s} \times \frac{t}{u}\right) = \left(\frac{p}{q} \times \frac{r}{s}\right) \times \frac{t}{u}$$

$$= \frac{prt}{qsu} = \frac{prt}{qsu}$$

⇒ Associative

(3) Identity :- $a * e = a$

$$\frac{p}{q} \times e = a \times e = a$$

$$e = \frac{a}{a} = 1 \in \mathbb{Q}.$$

⇒ Identity exist

(4) Inverse :- $a * a^{-1} = e$

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

$$a^{-1} > \frac{1}{a} \in \mathbb{Q}$$

except $a = 0$

So, inverse exist for all except 0.

⇒ Group

Q. If * is the binary operation on the set R of real numbers defined by $a*b = a+b+2ab$. Check if this is an abelian group or not?

Sol → $(R, *)$ $a*b = a+b+2ab$.

① Closure :- $a, b \in R$, $a*b \in a.$, Let $a=1, b=2 \in R$

$a*b = a+b+2ab$

$1*2 = 1+2+2\times1\times2$

$= 7 \in R$

$\Rightarrow$ It is closed w.r.t $a+b+2ab$.

② Associative :- $(a*b)*c = a*(b*c)$

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

$= a+b+2ab+c+2(a+b+2ab)\times c = a+b+c+2bc+2(b+c+2bc)\times a$

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

$\Rightarrow$ Associative.

③ Identity :- $a*e = a$

$a+e+2ae = a$

$e+2ae = a-a \Rightarrow e(1+2a) = 0$

$e = 0 \in R$

$\Rightarrow$ Identity exist

④ Inverse :-

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

$a+a^{-1}+2aa^{-1} = 0$

$a^{-1}(1+2a) = -a$

$a^{-1} = \frac{-a}{(1+2a)} \in R.$

$\Rightarrow$ Inverse Exist

(5) Commutative :-

$a * b = b * a$

$a + b + 2ab = b + a + 2ba$

$\Rightarrow$ Commutative

Since all 5 condition is satisfied.

$\Rightarrow$ It is an Abelian group.

Q. Show that the set Q^+ of all rational numbers forms an abelian group under the operation * defined by $a * b = \frac{ab}{2}$, $\left[\text{or } \frac{ab}{n} \quad n = 2, 3, \cdots\right]$

Sol → (1) closure :- $a * b = \frac{ab}{2}$.

$\frac{p}{q} * \frac{r}{s} = \frac{\frac{pr}{qs}}{2} \in Q^+$.

$\Rightarrow$ It is closed w.r.t $\frac{ab}{2}$

(2) Associative :- $a * (b * c) = (a * b) * c$

$a * \left(\frac{bc}{2}\right) = \left(\frac{ab}{2}\right) * c$

$= \frac{abc}{4} = \frac{abc}{4}$

$\Rightarrow$ Associative

(3) Identity :- $a * e = a$

$\frac{a \cdot e}{2} = a \Rightarrow e = \frac{2a}{a} = 2$

$\Rightarrow$ Identity exist $\Rightarrow e = 2 \in Q^+$

④ Inverse :- $a * a^{-1} = e$

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

$$= a^{-1} = \frac{1}{a} \in Q \quad [\text{except } a = 0]$$

$\Rightarrow$ Inverse exist for all a except $a = 0$.

⑤ Commutative :- $a * b = b * a$

$$\frac{ab}{2} = \frac{ba}{2}$$

$\Rightarrow$ Commutative.

Since all 5 condition satisfy. It is an abelian group.

Q. Prove that $G = \{0, 1, 2, 3, 4, 5\}$ is a abelian group w.r.t $+_6$.

Sol → $(a, +_6)$.

Comparision Table :-

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4.

① Closure :- Since all element of Composition Table are also belonging to G. So, it is ~~called~~ closed.
~~closure~~

② Associative :- $(a +_6 b) +_6 c = a +_6 (b +_6 c)$

Let $a = 2, b = 3, c = 5$

$(2 +_6 3) +_6 5 = 2 +_6 (3 +_6 5)$

$= 5 +_6 5 = 2 +_6 2$

$= 4 = 4$

$\Rightarrow$ Associative

③ 1st row and 1st column is identical to the elements. So, the element corresponding to it will be it identity.

$\Rightarrow$ 0 is the Identity element

④ a Inverse :- $a * a^{-1} = e$

$= a +_6 a = 0$

for $a = 0$, $a^{-1} = 0$

$a = 1$, $a^{-1} = 5$

$a = 2$, $a^{-1} = 4$

$a = 3$, $a^{-1} = 3$

$a = 4$, $a^{-1} = 2$

$a = 5$, $a^{-1} = 1$

$\Rightarrow$ Inverse exist

$\in$ C.T

⑤ Commutative :- We can see the diagonal elements are symmetric.

$\Rightarrow$ Commutative

Properties of the Group :-

① The identity element of a group $(G, *)$ is unique.

Proof :- If possible Let assume there are 2 identity elements e_1, e_2 of $(G, *)$.

Case I :- when e_1 is an identity element

$$a * e_1 = a = e_1 * a \quad --- ①$$

Case II :- when e_2 is an identity element

$$a * e_2 = a = e_2 * a \quad --- ②$$

from ① and ②.

$$e_1 = e_2$$

which is a contradiction to our assumption.

$\Rightarrow$ The identity element is unique.

② The inverse of each element of a group $(G, *)$ is unique.

Proof :- Let, if possible, there are two inverse a, b, c of the element a.

$$\Rightarrow a * b = e = b * a \quad --- ①$$

$$\Rightarrow a * c = e = c * a \quad --- ②$$

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

which is a contradiction to our assumption.
So, the inverse of an element is unique.

③ $(a*b)^{-1} = b^{-1} * a^{-1} \quad \forall\ a, b \in G$.

Sol → Proof :-

In General :- $a \times b = e$.

$a^{-1} = b$.

$$\frac{(\underbrace{a*b}_{A})^{-1}}{} = \frac{b^{-1} * a^{-1}}{B}$$

We need to prove

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

$\Rightarrow a*b*b^{-1}*a^{-1}$

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

$\Rightarrow (a*e)*a^{-1}$

$\Rightarrow a*a^{-1}$

$= e = LHS$

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

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

4. $(a, *)$ cannot have idempotent element except the identity element.

Sol → Proof :- Let If possible a, b, be an idempotent element except the identity element.

$a * a = a$ — — (1)

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

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

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

$$= a * e = e$$

$$= a = e$$

$$\Rightarrow e = a$$

which is contradiction to our assumption
So, no other idempotent element exist except identity element

* Not → $G = [1, 2, 3]$
order of group $[O(G)$ or $|G| = 3]$
↓
No. of element of group

Cyclic Group :-

A group $(G, *)$ is said to be cyclic if there exist an element $a \in G$ such that every element x of G can be expressed in form of $x = a^n$ for some integer n.

Example :- $G = \{1, -1, i, -i\}$

$1 = i^4$
$-1 = i^2$
$i = i$
$-i = i^3$

Here, $i \rightarrow$ generator.

Since all element can be expressed in form of $(i)^n$ so, it is cyclic group.

For cyclic group :-

$O(a) = 4$

$O(1) = 4$

$O(-1) = 2$

$O(i) = 1$

$O(-i) = 3$

→ Power of $(i)^a$ is (i) ≙ His

Properties of cyclic group :-

① A cyclic group is Abelian.

Proof :- Let $x, y \in G$ are two element of cyclic group with generator a.

Such that $x = a^n$

$y = a^m$

$x * y = a^n * a^m$

$= a^{n+m}$

$= a^{m+n}$

$= a^m * a^n$

$= y * x$

$x * y = y * x$

$\Rightarrow$ Commutative

$\Rightarrow$ Abelian group.

② If a is a generator of a cyclic group $(G, *)$ then a^{-1} is also a generator of that group.

Proof :- a is generator

Let n be element of cyclic group with a as generator

$$\Rightarrow n = a^n$$

$$n = (a^{-1})^{-n}$$

Now, since n and $-n$ both is integer.

n can be expressed as a^{-1} as generator too. with power $-n$.

So, a^{-1} is also a generator if a is generator of a cyclic group.

Permutation Group :-

If the set of permutation of a group is also a group Then it is known as permutation group.

$f : S \to S$ for $S = \{1, 2\}$

element $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ or $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

image

$$S_n = n!$$

Q. If the permutation of the element of $\{1,2,3,4,5\}$ are $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix}$, $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{bmatrix}$

$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{bmatrix}$, $\delta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{bmatrix}$.

find (i) $\alpha\beta$ (ii) α^2, (iii) $\beta\alpha$, (iv) $\gamma\beta$. (v) δ^{-1}

(vi) $\alpha\beta\gamma$. Also. Solve $\alpha n = \beta$.

Sol → (i) $\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{bmatrix}$

$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{bmatrix}$ or $\begin{bmatrix} 2 & 1 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{bmatrix}$ → Same

(ii) $\alpha^2 = \alpha \cdot \alpha$

(iii) $\beta\alpha$ → same as (i)

(iv) $\gamma\beta$

(v) $\delta^{-1} = \begin{bmatrix} 3 & 2 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}$

↳ Just interchange the δ.

(vi) $\alpha\beta\gamma$ → first find $\alpha\beta$ then $(\alpha\beta)\cdot\gamma$.

→ $\alpha x = \beta$

$x = \beta\alpha^{-1}$ → Solve as (i)st.

Sub-group

If $(G, *)$ is a group and $H \subseteq G$ is a non-empty set then H is called subgroup if it satisfy following Condition :-

(i) closure i.e. $a, b \in H$, $a * b \in H$

(ii) Identity i.e. $a * e = a$

(iii) Invuse i.e. $a * a^{-1} = e$

Imp

Theorem :- 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 :-

First we assume that H is a subgroup, then we have to show that $a, b \in H$, $a * b^{-1} \in H$.

$a, b \in H$.

Then, $b^{-1} \in H$. [$\because$ H is a sub group]

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

$a * b^{-1} \in H$ [Closure property]

Now, we assume that $a, b \in H \Rightarrow a * b^{-1} \in H$ (ii) given then we have to show that H is a subgroup.

(1) If $b = a$.

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

$e \in H$.

$\Rightarrow$ Identity exist

(2) $e \in H, a \in H$

$\Rightarrow e * a^{-1} \in H$. [from ii)]

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

$\Rightarrow$ Inverse Exist

(3) $a \in H, b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} \in H$ [from (i)]

$= a * b \in H$

$\Rightarrow$ closure exist

So, from (1) (2) (3), we can say H is a subgroup.

Homomorphism :-

If $(G,*)$ & (G',Δ) are two groups, then a mapping $f: G \to G'$ is called a group homomorphism if for any $a, b \in G$

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

* A group homomorphism f is called group isomorphism if f is one-to-one and onto.

Theorem :- If $f: G \to G'$ is a group homomorphism from $(G,*)$ to (G',Δ). Then

(i) $f(e) = e'$ where e & e' are identity element of G and G' respectively.

(ii) $f(a^{-1}) = [f(a)]^{-1}$ for any $a \in G$.

(iii) If H is a subgroup of G then. $f(H) = \{f(h) : h \in H\}$ is a subgroup of G'.

Proof :-

(i) Since f is a group Homomorphism.

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

$$f(e*e) = f(e) \Delta f(e)$$

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

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

$\Rightarrow$ $f(e)$ is an idempotent element of $[G', \Delta]$

But only identity element can be idempotent.

$\therefore$ $f(e) = e'$ —

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

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

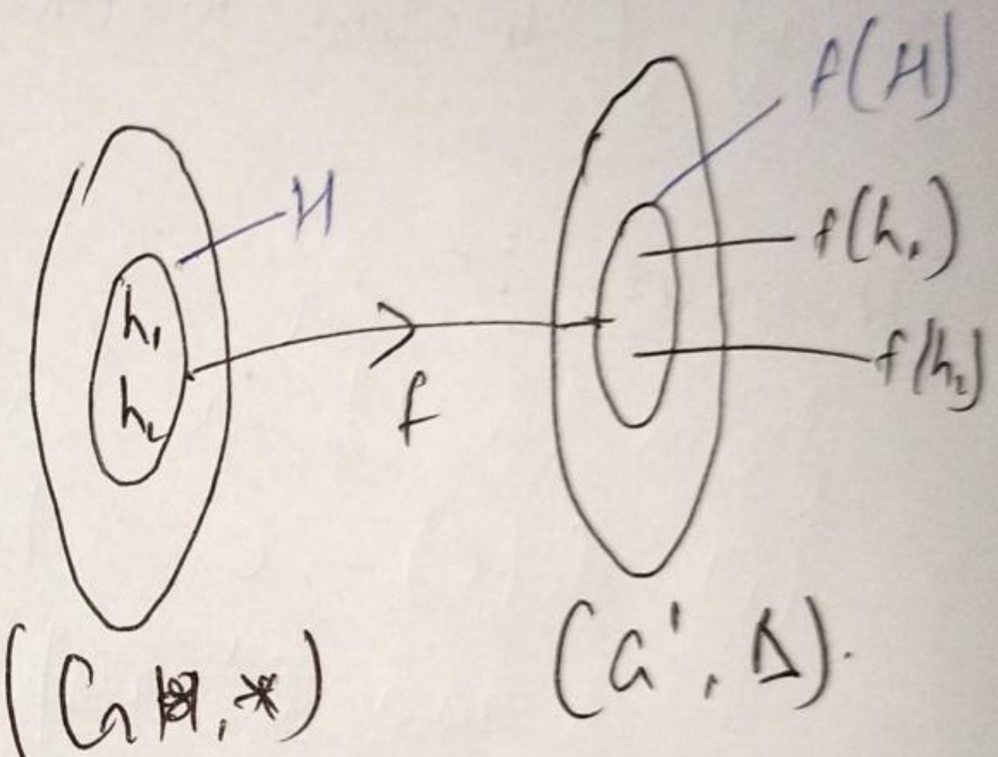
$f(e) = f(a) \Delta f(a^{-1})$

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

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

(iii) Let $h_1, h_2' \in f(H)$

We have to proove $h_1' \Delta (h_2')^{-1} \in f(H)$



$h_1' \Delta (h_2')^{-1}$

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

$= f(h_1) \Delta f(h_2^{-1})$ [By (ii)]

$= f(h_1 * h_2^{-1})$. [By homomorphism]

$\in f(H)$.

Thus, $h_1', h_2' \in f(H) \Rightarrow h_1' \Delta (h_2')^{-1} \in f(H)$

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

Ring Theory :-

An algebric groups $(R, +, \bullet)$ where R is a non-empty set + and $\bullet$ are two closed binary operations (which may be different from ordinary addition and multiplication) is called a ring if following conditions are satisfied :-

(i) $(R, +)$ is an abelian group

(ii) $(R, \bullet)$ is a semi-group.

(iii) The operation $\bullet$ is distributive over + for any $a, b, c \in R$.

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

Condition (i) involves :-
1) Closure
2) Associative
3) Identity
4) Inverse
5) Commutative
→ $(R, +)$

Condition (ii) involves :-
6) Closure
7) Associative
→ $(R, \bullet)$

Condition (iii) involves :-
8) $a \bullet (b+c) = a \bullet b + a \bullet c$.

Q. Check if $(I, +, \bullet)$ is a Ring or not ?

Sol → for $(I, +)$:-

1) Closure ⇒ $a, b \in I$, $a * b \in I$
$\Rightarrow a + b \in I$
⇒ Closed w.r.t I.

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

$\Rightarrow a+b+c = a+b+c$

$\Rightarrow$ Associative

3) Identity :- $a+e = a$

$e = 0 \in I$

$\Rightarrow$ Identity exist

4) Inverse :- $a+a^{-1} = 0$

$a^{-1} = -a \in I$

$\Rightarrow$ Inverse exist

5) Commutative :- $a*b = b*a$

$\Rightarrow a+b = b+a$

$\Rightarrow$ Commutative

So, $(I, +)$ is an abelian group.

Now, for $(I, \cdot)$:

6) closure :- $a, b \in I, \ a \cdot b \in I$

$1, 2 \in I, \ 1 \cdot 2 \in I$

$2 \in I$

$\Rightarrow$ closed w.r.t $\cdot$

7) Associative :- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$\Rightarrow abc = abc$

$\Rightarrow$ Associative

So, $(I, \cdot)$ is a semi-group.

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

$1 \cdot (2+3) = 1 \cdot 2 + 1 \cdot 3$

$5 = 5$

$\Rightarrow$ Distributive

So, $(I, +, \cdot)$ is a ring

Definitions :-

1) If $(R, \cdot)$ is commutative, then the ring $(R, +, \cdot)$ is said to be commutative Ring.

2) If $(R, \cdot)$ has an identity element, then $(R, +, \cdot)$ is called ring with Unity or Identity Ring.

3) If a & b are two non-zero element of a ring R. such that $a \cdot b = 0$ then a and b are divisor of 0 or zero divisor.

Example :- $Z = [0, 1, 2, 3, 4, 5]$

$[Z_6 +_6 X_6]$; $2, 3 \neq 0$

$2 \cdot 3 = 0$

$\therefore$ 2, 3 are Zero-divisor.

* It usually occur in Modulo.

* Without Zero-divisor :-

$a \cdot b = 0$ if $a = 0$ or $b = 0$.

4) If Commutative Ring with unity and without Zero divisor is called integral Domain.

Q. Show that $(Z_5 +_5 X_5)$ is integral Domain.

Sol→ For this first of all we need to draw Commutative 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

X_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

For $[Z_5, +_5]$:

i) Since all element of $C.T \in Z_5$ so, it is closed

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

$(1 +_5 2) +_5 3 = (1 +_5 2) +_5 3$

$1 = 1$

$\Rightarrow$ Associative

3) Since Row 1 & Column 1 is identical to Z_5.
So, 0 is identity element

4) for every element inverse exist.

5) $a +_5 b = a +_5 a \Rightarrow 1 +_5 2 = 2 +_5 1$

$\Rightarrow 3 = 3$

$\Rightarrow$ Commutative

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

For $[Z_5, X_5]$:-

6) Every element of $C.T \in Z_5$ so, it is closed w.r.t X_5.

7) ~~Every~~ $a X_5 (b X_5 c) = (a X_5 b) X_5 c$

$1 X_5 (2 X_5 3) = (1 X_5 2) X_5 3$

$1 X_5 1 = 2 X_5 3$

$1 = 1$

$\Rightarrow$ Associative

$\Rightarrow (Z, X_5)$ is semi-group

8) ~~Commutative~~ Distributive :-

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

$1 X_5 (2 +_5 3) = 1 X_5 2 +_5 1 X_5 3$

$0 = 0$

$\Rightarrow$ Distributive

$\Rightarrow$ $(Z_5, \cdot X_5, +_5)$ is a ring.

9) Commutative :-

$a X_5 b = b X_5 a$

$1 X_5 2 = 2 X_5 1$

$\Rightarrow 2 = 2$

$\Rightarrow$ Commutative

$\Rightarrow$ It is a Commutative Ring.

10) Identity for (Z_5, X_5) :-

Since 2nd Row & 2nd Column is identical to Z_5.

So, 1 is identity element

$\Rightarrow$ It is Commutative ring with Unity.

$In(Z_5, \times_5)$, for any $a, b \neq 0$,

$a \times_5 b = 0$ when $a = 0$ or $b = 0$

$\Rightarrow$ It is without any zero divisor

So, the expression is Integral Domain.

* $(R, +) \rightarrow$ Abelian
  $(R, \cdot) \rightarrow$ Semigroup + Commutative + Identity + Inverse

$\Downarrow$

Multiplicative Inverse

$\Downarrow$

Known as Field.

Properties of Ring :-

1) Identity element of ring w.r.t $+$ is unique
2) Identity element of ring w.r.t $\times$ is unique.
3) Unique Inverse w.r.t $+$.
4) Unique Inverse w.r.t $\times$.
5) A commutative ring with unity is called Integral domain if & only if it satisfy Cancelation Law of Multiplication.

i.e. For all $a, b, c \in R$.

(a) If $a + b = a + c$ then $b = c$ (Left Cancellation)

(b) If $b + a = c + a$ then $b = c$ (Right Cancellation)

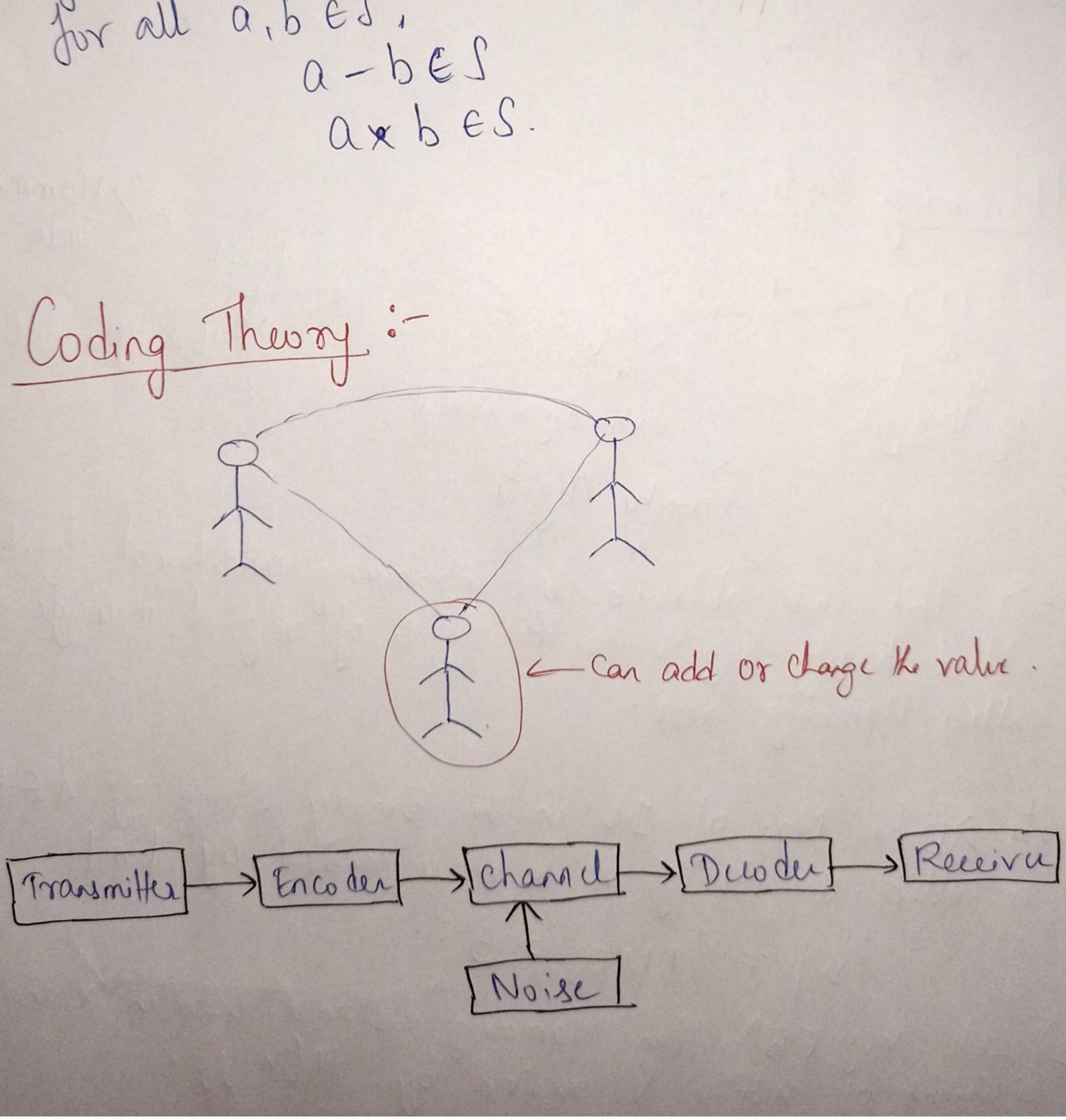
6) Every field is an integral Domain
7) Every finite Integral Domain is field.

SubRing :-

If $(R, +, \times)$ is a ring and S is a non-empty subset of R, then $(S, +, \times)$ is a subring of R if & only if for all $a, b \in S$,

$$a - b \in S$$
$$a \times b \in S.$$

Coding Theory :-

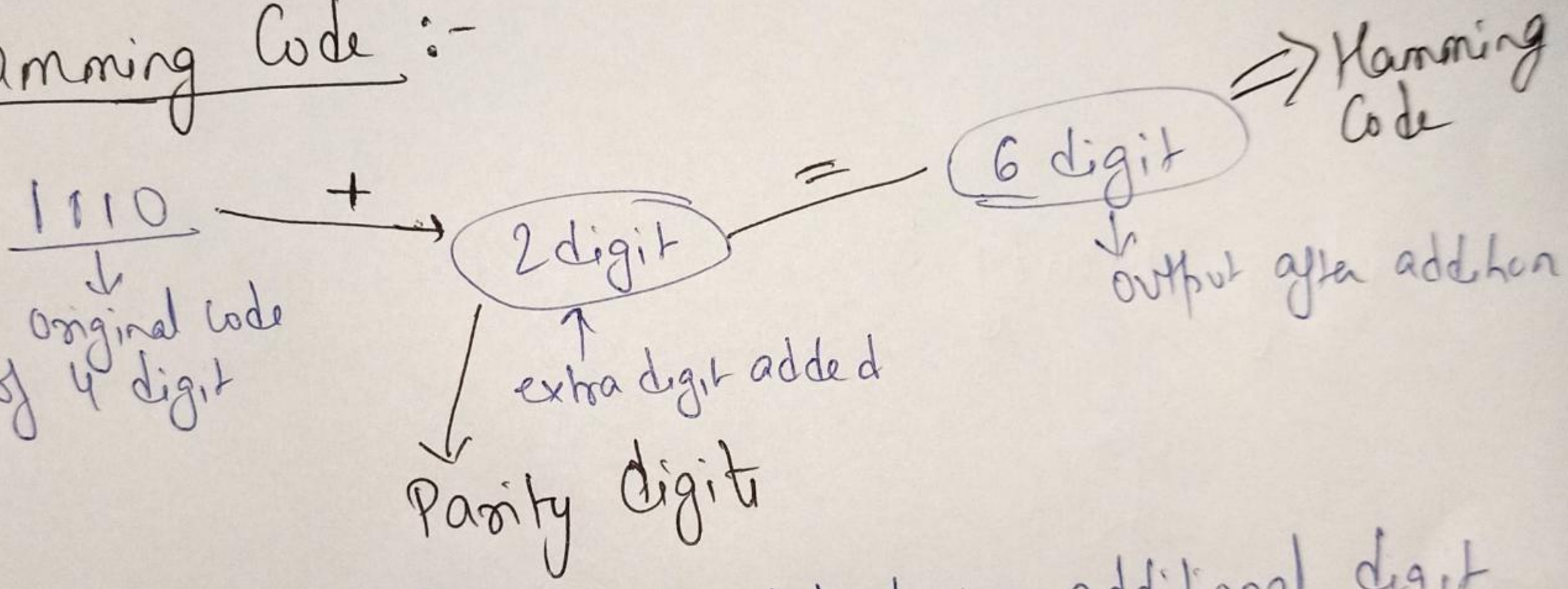


Group Code :-

If $B = \{0, 1\}$, then $B^n = \{x_1, x_2 \cdots x_n \mid x_i \in B$ $i = 1, 2, 3 \cdots n\}$ is a group under the binary operation of addition modulo 2, denoted by $\oplus$. This group $(B^n, \oplus)$ is called a group code.

Ex → $B^4 \Rightarrow$ 1110
0110
4-digit

Hamming Code :-



⇒ The code obtained by introducing additional digit called parity digits to the digit of original message are called Hamming Codes.

Note → ① The No. of 1's in the Binary string of $x \in B^n$ is called weight of x & it is denoted by $|x|$.

$$|x| = |1110| = 3.$$

② Let $x, y \in B^n$. Then Hamming distance between x and y is weight of $x \oplus y$ & denoted by $H(x, y)$.

$$H(x, y) = |x \oplus y|$$

Example → $x = 1011$

$y = 0101$

$H(x,y) = |1011 \oplus 0101|$

$= |1110|$

$= 3$

1	0	1	1
0	1	0	1
1	1	1	0

Q. find the Code word generated by the encoding function $\epsilon: B^2 \rightarrow B^5$ w.r.t parity check Matrix.

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

Sol →

$$H = \left[\begin{array}{cc} 0 & 1 \\ 0 & 1 \end{array}\right] \rightarrow A \qquad \left[\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right] \rightarrow \text{Identity}$$

$H = [A^T] I_{n-m}$

$e : B^2 \rightarrow B^5$

On Comparing with $e: B^m \rightarrow B^n$

$m = 2, \; n = 5$

$H = A^T I_{5-2} = A^T I_3$

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

Generator Matrix = $G = [I_m | A]$

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

Now, $B^2 = [00, 01, 10, 11]$

$e(w) = wG$.

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

$$= [0\,0\,0\,0\,0]$$

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

$$= [0\,1\,0\,1\,1]$$

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

$$= [1\,0\,0\,1\,1]$$

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

$$= [1\,1\,0\,0\,0]$$

Hence code generated by H are.

00000, 01011, 10011 & 11000.

Q. 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 encoding function $e: B^3 \to B^6$, find the corresponding parity check Matrix and use it to decode the following received words and hence to find the original message. Are all words decoded uniquely?

(i) 001111 (ii) 110001 (iii) 110101 (iv) 111111

Sol→ $e: B^3 \to B^6$

$m = 3, n = 3$

$G = [I_m ; A]$

$H = [A^T \mid I_{n-m}]$

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

(i) $H \cdot [\gamma]^T$

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

Since, the syndrome $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ is same as Fifth column of H. The element in 5^{th} position of γ is changed.

∴ Decoded message = 001101

Original message = 001

(ii) $H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$

$\Rightarrow$ ~~first~~ 4th column $\Rightarrow$ 4th element changed

Decoded message = 1 1 0 1 0 1

Original message = 1 1 0

(iii) $H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

Since we get $\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, the decoded message will be same as received message.

Decoded message = 1 1 0 1 0 1

Original message = 1 1 0

(iv) $H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

Since the syndrome is not identical to any column of H, the received word cannot be decoded uniquely.