UNIT-4

GROUP THEORY & CODING THEORY

~~Semigroups~~ Algebric system :-

A non-empty set G together with one or more n-ary operations say * (binary) is called an algebric system or algebric structure.

we denote it by $(G,*)$.

Semigroups & monoids :-

Semigroup :-

If a non-empty set S together with the binary operation '*' satisfying the following two properties

(i) $a*b \in S$ $a,b \in S$ (closure property)

(ii) $(a*b)*c = a*(b*c)$ $a,b,c \in S$ (associative property)

then $(S,*)$ is called a semigroup.

monoid :-

A semigroup $(S,*)$ with an identity element w.r.to '*' is called monoid. It is denoted by $(M,*)$.

In otherwords,

a non-empty set 'M' with respect to '*' is said to be monoid, if * satisfies the following properties.

For $a,b,c \in M$

a) $a*b \in M$ (closure property)

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

c) $\forall\, a \in M$ $\exists\, e \in M$ such that

$a*e = e*a = a$ (identity element)

Groups: -

Group: -

A non-empty set G together with the binary operation '$*$' $(G, *)$ is called a group. If '$*$' satisfies the following conditions.

(i) closure : $a * b \in G$ for all $a, b \in G$

ii) associative : $(a*b)*c = a*(b*c)$ $\forall a, b, c \in G$.

iii) Identity element : There exists an element $e \in G$ called the identity element such that $a*e = e*a = a$ $\forall a \in G$.

iv) Inverse : There exists an element $a^{-1} \in G$ called the inverse of 'a' such that

$a * a^{-1} = a^{-1} * a = e$, $\forall a \in G$.

~~Abelian~~ group: -
Abelian

In a group $(G, *)$, if $a * b = b * a$ $\forall a, b \in G$ then the group $(G,*)$ is called an abelian group.

Ex: $(Z, +)$ is an abelian group.

otherwise $(G, *)$ is called an non abelian group.

Notations: .

Z = the set of all integers

Q = the set of all rational numbers

R = the set of all real numbers

R^+ = the set of all positive real numbers

Q^+ = the set of all positive rational numbers

C = the set of all complex numbers

Z^+ = the set of all positive integers.

1) check whether $(z^+, +)$ is group?

soln:-

$z^+ = 0, 1, 2 \ldots$

i) closure property

$a+b \in z^+$

$0+1 = 1 \in z^+$

$\therefore$ satisfies closure property.

ii) Associative property satisfied $(\because (0+1)+2 = 0+(1+2)$
$3 = 3)$

iii) Identity satisfied (identity element 0)

iv) Inverse not satisfied $(a + a^{-1} = e$

Inverse does not exist. $1 + a^{-1} = 0 \Rightarrow a^{-1} = -1 \notin z^+)$

$\therefore$ $(z^+, +)$ is monoid.

$(z^+, +)$ is not a group.

Properties of a groups:-

1) The identity element of a group is unique.

proof:- let $(G, *)$ be a group.

let e_1 and e_2 be two identity element in G.

Suppose e_1 is the identity then,

$$e_1 * e_2 = e_2 * e_1 = e_2 \longrightarrow ①$$

Suppose e_2 is the identity then,

$$e_2 * e_1 = e_1 * e_2 = e_1 \longrightarrow ②$$

from ① & ② $e_1 = e_2$

$\therefore$ The identity element is unique.

2) The inverse ~~of~~ ~~each~~ element of a group is unique.

proof:- Let $(G,*)$ be a group.

Let $a \in G$ and e be the identity of G. Let a_1^{-1} and a_2^{-1} be the two different inverses of the same element.

$$a_1^{-1} * a = a * a_1^{-1} = e$$

$$a_2^{-1} * a = a * a_2^{-1} = e$$

$$(a_1^{-1} * a) * a_2^{-1} = e * a_2^{-1} = a_2^{-1} \longrightarrow (1)$$

$$a_1^{-1} * (a * a_2^{-1}) = a_1^{-1} * e = a_1^{-1} \longrightarrow (2)$$

from (1) & (2) $a_1^{-1} = a_2^{-1}$

$\therefore$ The inverse ~~of~~ element of group is unique.

3. The cancellation laws are true in a group.

$$a * b = a * c \Rightarrow b = c$$

$$b * a = c * a \Rightarrow b = c$$

4. To prove $(a*b)^{-1} = b^{-1} * a^{-1}$ for any $a, b \in G$.

Proof: - Let $a, b \in G$ and a^{-1}, b^{-1} be their respectively.

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

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

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

$= a * a^{-1}$

$= e$

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

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

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

$\therefore$ The inverse of $(a*b)$ is $b^{-1} * a^{-1}$

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

Show that set Q^+ of all positive rational numbers forms an abelian group under the operation $*$ defined by $a*b = \frac{1}{2}ab$; $a,b \in Q^+$

Soln:-

when $a,b \in Q^+$, $\frac{ab}{2} \in Q^+$

(i) closure: Q^+ is closed under the operation $*$

(ii) Associative:

$(a*b)*c = \frac{ab}{2} * c = \frac{ab}{2} \times \frac{c}{2} = \frac{abc}{4} \rightarrow ①$

$a*(b*c) = a * \frac{bc}{2} = \frac{1}{2} a\left(\frac{bc}{2}\right) = \frac{abc}{4} \longrightarrow ②$

from ① & ② $(a*b)*c = a*(b*c)$ $\forall a,b,c \in Q^+$

$\therefore (Q^+, *)$ is associative.

(iii) Identity:

Let 'e' be the identity element.

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

$a*e = a \Rightarrow \frac{ae}{2} = a$

$\boxed{e=2} \in Q^+$

iv) Inverse: let a^{-1} be the inverse of a.

then $a*a^{-1} = e \Rightarrow$ $a*a^{-1} = 2$

$\frac{aa^{-1}}{2} = 2$

$a^{-1} = 4/a \in Q^+$

$\therefore$ Inverse of $a^{-1} = \underline{4/a} \in Q^+$

5) Commutative:

$$a*b = \frac{ab}{2}$$

$$b*a = \frac{ba}{2} = \frac{ab}{2}$$

$\therefore\ a*b = b*a \quad \forall a,b \in Q^+$

$\therefore\ (Q^+, *)$ is abelian group.

2) If $*$ is the binary operation on the set R of real numbers defined by $a*b = a+b+2ab$.

a) Find if $\{R, *\}$ is semigroup. Is it commutative?

b) Find the identity element, if exists. $(e=0)$

c) when elements have inverses and what are they? $a^{-1} = \frac{-a}{(1+2a)}$

3) If $(G, *)$ is an abelian group, show that $(a*b)^n = a^n * b^n$ for all $a, b \in G$, where n is a positive integer.

Proof:- Since $(G, *)$ is an abelian group

$a*b = b*a \longrightarrow ①$ for $a, b \in G$

To prove $S(1)$ is true, we have $(a*b)^1 = (b*a)^1$ (by ①)

$n=2$

$$(a*b)^2 = (a*b)*(a*b)$$

$$= a*(b*a)*b \quad \text{(by associative)}$$

$$= a*(a*b)*b \quad \text{(by ①)}$$

$$= (a*a)*(b*b) \quad \text{(by associative)}$$

$$(a*b)^2 = a^2*b^2.$$

$\therefore$ $S(2)$ is true.

$\therefore$ Assume that $S(n)$ is true

$$(a*b)^n = a^n*b^n \longrightarrow ②$$

To prove $S(n+1)$ is true.

$$(a*b)^{n+1} = (a*b)^n * (a*b)$$

$$= (a^n * b^n) * (a*b) \quad \text{(by 2)}$$

$$= a^n * (b^n * a) * b \quad \text{(by associative)}$$

$$= a^n * (a * b^n) * b \quad \text{(Since G is abelian)}$$

$$= (a^n * a) * (b^n * b)$$

$$(a*b)^{n+1} = a^{n+1} * b^{n+1}$$

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

$\therefore$ Hence by mathematical induction, the result is true for all positive integer value of n.

HW

2) a) (i) $a, b \in R$ then $a*b = a+b+2ab \in R$

$*$ is closure satisfied.

(ii) Associative :- $a,b,c \in R$ then

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

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

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

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

$$LHS = RHS$$

$\cdot$ $*$ is associative.

Hence $(R,*)$ is a semigroup.

Also $b*a = \cancel{b+a} + 2ba = a+b+2ab = a*b$.

Hence $(R,*)$ is commutative.

b)

b) If Identity element exists, let it be e then for any $a \in R$.

$$a * e = a$$

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

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

$\therefore \boxed{e=0}$ since $1+2a \neq 0 \ \forall a \in R$.

c) let a^{-1} be the inverse of an element $a \in R$

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

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

$$a + a^{-1}(1+2a) = 0$$

$$\boxed{a^{-1} = \frac{-a}{(1+2a)}} \quad (\because a \neq \tfrac{1}{2})$$

Cyclic group:

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

Ex: If $G = \{1, -1, i, -i\}$ then $(G, *)$ is a cyclic group with the generator i,

for $1 = i^4$, $-1 = i^2$, $i = i^1$ and $-i = i^3$

For this cyclic group, $-i$ is also a generator.

Properties of cyclic group:-

1. Every cyclic group is an abelian group.

Proof: - Let $(G,*)$ be a cyclic group with $a \in G$ as a generator. Let $b, c \in G$ then $b = a^m$ and $c = a^n$ where m and n are integers.

now, $b*c = a^m * a^n = a^{m+n}$

$$= a^{n+m}$$

$$= a^n * a^m$$

$$b*c = c*b$$

Hence $(G,*)$ is an abelian group.

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

Proof :- Let $b \in G$, then $b = a^m$ where m is an integer.
Now $b = (a^{-1})^{-m}$ where $-m$ is an integer.

$\therefore$ a^{-1} is also a generator of $(G, *)$.

3. If a cyclic group G is generated by an element of the order n, then a^m is a generator of G iff the gcd of m and n is 1.

Permutation group :-

A permutation is a 1-1 mapping of a non empty set A onto itself.

A group $(G, *)$ is called a permutation group on a non-empty set P if the elements of G are permutations of P and the operation '$*$' is the composition of the two functions.

If $S = \{1, 2, \cdots, n\}$ the permutation group is also called the symmetric group of degree n and denoted by S_n. The number of elements of S_n is $n!$.

Ex: Let $S = \{1, 2, 3\}$ and $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

then $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}; \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix}; \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix}$.

Composition of permutations:-

Let us consider f and g be two arbitrary permutations of like degree, given by

$$f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} \quad g = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}$$

$$f \circ g = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ c_1 & c_2 & c_3 & \cdots & c_n \end{pmatrix}.$$

Ex:- Find the composition of following two permutations

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

Soln:-

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

$$g \circ f : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$\therefore \quad f \circ g \neq g \circ f$

It is not commutative.

Inverse permutation:-

Since a permutation is 1-1, onto and hence it is invertible.

Ex: let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ then $f^{-1} = ?$

$$f^{-1} = \begin{pmatrix} 2 & 3 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

1) If the permutations of the elements of (1, 2, 3, 4, 5) are given by $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$

$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$, $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}$

$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$. Find $\alpha\beta$, $\beta\alpha$, α^2, $\gamma\beta$, δ^{-1} and $\delta\beta\gamma$.

Also solve the equation $\alpha x = \beta$

Soln :-

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

$$\begin{array}{ccccccc} \beta & : & 1 & 2 & 3 & 4 & 5 \\ & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \alpha & : & 1 & 2 & 3 & 5 & 4 \\ & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & & 2 & 3 & 1 & 5 & 4 \end{array} \qquad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

$$\begin{array}{ccccccc} \alpha & : & 1 & 2 & 3 & 4 & 5 \\ & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & & 2 & 3 & 1 & 4 & 5 \\ & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \alpha & : & 3 & 1 & 2 & 4 & 5 \end{array} \qquad \alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$$

$$\begin{array}{ccccccc} & & 1 & 2 & 3 & 4 & 5 \\ \gamma & : & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & & 5 & 4 & 3 & 1 & 2 \\ & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \beta & : & 4 & 5 & 3 & 1 & 2 \end{array} \qquad \gamma\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}.$$

δ^{-1} is obtained by interchanging the two rows of δ and then rearranging the elements of the first row so as to assume the natural order.

$$\delta^{-1} = \begin{pmatrix} 3 & 2 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

$$\begin{array}{lccccc} \alpha\beta : & 1 & 2 & 3 & 4 & 5 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \gamma : & 2 & 3 & 1 & 5 & 4 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 3 & 5 & 2 & 1 \end{array} \qquad \alpha\beta\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix}$$

Solving the eqn. $\alpha x = \beta$

$$x = \alpha^{-1}\beta$$

$$\alpha^{-1} = \begin{pmatrix} 2 & 3 & 1 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$$

$$\begin{array}{lccccc} \alpha^{-1} : & 1 & 2 & 3 & 4 & 5 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 1 & 2 & 4 & 5 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \beta : & 3 & 1 & 2 & 5 & 4 \end{array} \qquad x = \alpha^{-1}\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

2) If α, β are two elements of the symmetric group S_4 and given by $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$; $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ then find $\alpha\beta, \beta\alpha, \alpha^2, \beta^2, \alpha^{-1}$.

Soln: :

$$\begin{array}{lcccc} \alpha : & 1 & 2 & 3 & 4 \\ & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 4 & 2 & 1 \\ & \downarrow & \downarrow & \downarrow & \downarrow \\ \beta : & 3 & 1 & 4 & 2 \end{array} \qquad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

$$\begin{array}{lcccc} \beta : & 1 & 2 & 3 & 4 \\ & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 4 & 3 & 1 \\ \alpha : & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 1 & 2 & 3 \end{array} \qquad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\begin{array}{cccccc} \alpha & : & 1 & 2 & 3 & 4 \\ & & \downarrow & \downarrow & \downarrow & \downarrow \\ & & 3 & 4 & 2 & 1 \\ & & \downarrow & \downarrow & \downarrow & \downarrow \\ \alpha & : & 2 & 1 & 4 & 3 \end{array} \qquad \alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\begin{array}{cccccc} \beta & : & 1 & 2 & 3 & 4 \\ & & \downarrow & \downarrow & \downarrow & \downarrow \\ & & 2 & 4 & 3 & 1 \\ \beta & : & \downarrow & \downarrow & \downarrow & \downarrow \\ & & 4 & 1 & 3 & 2 \end{array} \qquad \beta^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

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

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

Subgroups :-

Defn :- If $(G, *)$ is a group and $H \subseteq G$ is a non-empty subset, that satisfies the following conditions

i) For $a, b \in H$, $a * b \in H$

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

iii) For any $a \in H$, $a^{-1} \in H$ then $(H, *)$ is called a subgroup of $(G, *)$.

Ex:

1) $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$ and

2) $(\mathbb{R}, +)$ is a subgroup of $(\mathbb{C}, +)$.

Subgroups :

If $(G,*)$ is a group and $H \subseteq G$ is a non-empty set that satisfies the following conditions:

i) for $a,b \in H$, $a*b \in H$

ii) $e \in H$, where e is the identity of $(G,*)$.

iii) for any $a \in H$, $a^{-1} \in H$, then $(H,*)$ is called a subgroup of $(G,*)$.

Theorem :-

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

Proof :- (necessary condition)

Let us assume that H is a subgroup of G.

Since H itself is a group, we have for

$a, b \in H \Rightarrow a*b \in H$ (closure)

Since $b \in H \Rightarrow b^{-1} \in H$ ($\because H$ is a subgroup)

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

$\Rightarrow a*b^{-1} \in H$ ($\because H$ is a subgroup)

Sufficient condition :-

Let $a*b^{-1} \in H$ for $a,b \in H$

now we have to prove that H is a subgroup of G

(i) closure : Let $b \in H \Rightarrow b^{-1} \in H$

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

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

$\therefore H$ is closed.

(ii) <u>identity</u> :-

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

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

$\Rightarrow e \in H$

Hence the identity element 'e' $\in H$.

iii) <u>Inverse</u> :-

let $a, e \in H$

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

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

Every element 'a' of H has its inverse a^{-1} is in H.

$\therefore$ H is a subgroup of G.

Theorem: 2 Prove that the intersection of two subgroups of a group G is also a subgroup of G. Give an example to show that the union of two subgroups of G need not be a subgroup of G.

<u>Proof</u> :- Let H_1 and H_2 be any two subgroups of G.

$H_1 \cap H_2$ is a non-empty set.

Since atleast the identity element e is a common to both H_1 & H_2

let $a \in H_1 \cap H_2$ then $a \in H_1$ and $a \in H_2$

let $b \in H_1 \cap H_2$ then $b \in H_1$ and $b \in H_2$

H_1 is a subgroup of G.

$a * b^{-1} \in H_1$, since a and $b \in H_1$

H_2 is a subgroup of G,

$a * b^{-1} \in H_2$, since a and $b \in H_2$

Hence $a * b^{-1} \in H_1 \cap H_2$

Thus, when $a, b \in H_1 \cap H_2$, $a * b^{-1} \in H_1 \cap H_2$

$\therefore$ $H_1 \cap H_2$ is a subgroup of G.

Ex:- Let G be the additive group of integers. then $H_1 = \{\cdots -6, -4, -2, 0, 2, 4, 6 \cdots\}$ and
$H_2 = \{\cdots -9, -6, -3, 0, 3, 6, 9, \cdots\}$ are both sub groups of G.

now $H_1 \cup H_2$ is not closed under addition.

For example: $2 \in H_1 \cup H_2$ and $3 \in H_1 \cup H_2$

$2+3=5 \notin H_1 \cup H_2$.

$\therefore$ $H_1 \cup H_2$ is not a subgroup of G.

$H_1 \cap H_2 = \{-6, 0, 6, 12, \cdots\}$

$-6, 12 \in H_1 \cap H_2 \Rightarrow -6+12=6 \in (H_1 \cap H_2)$

$\therefore$ The intersection of two subgroup is again a subgroup of G.

3. If G is an abelian group with identity e, Prove that all elements x of G satisfying the equation $x^2 = e$ form a subgroup H of G.

Soln:- H is subset of G.

$H = \{x \mid x^2 = e\}$

$e^2 = e$ (the identity element e of $G \in H$)

now, $x^2 = e$

$x^{-1} \cdot x^2 = x^{-1} \cdot e$

$x = x^{-1} \longrightarrow (1)$ (Inverse)

Hence if $x \in H$, $x^{-1} \in H$

let $x, y \in H$

Since G is abelian $xy = yx$ (by (1))

$xy = y^{-1}x^{-1}$

$xy = (xy)^{-1}$ $((ab)^{-1} = b^{-1}a^{-1})$

$\therefore (xy)^2 = e$, $xy \in H$.

Thus if $x, y \in H$ we have $xy \in H$. (closure)

Thus, all the three condition satisfied.

$\therefore$ H is a subgroup of G.

4) If G is the set of all ordered pairs (a,b), where $(a \neq 0)$ and b are real and the binary operations '$*$' on G is defined by $(a,b)*(c,d) = (ac, bc+d)$ show that $(G,*)$ is a non-abelian group. Show also that the subset H of all those elements of G which are of the form $(1,b)$ is a subgroup of G.

Proof:-

To show that $(G,*)$ is an non-abelian group.

(i) Closure property:-

$(a,b) \in G$ such that $a*b \in G$

$a \to (a,b)$, $b \to (c,d) \in G$

$(a*b)*(c*d) = (ac, bc+d) \in G$

satisfied closure property.

(ii) associative property:-

(a,b), (c,d), $(e,f) \in G$

$(a,b)*[(c,d)*(e,f)] = [(a,b)*(c,d)]*(e,f)$

$(a,b) * [ce, ed+f] = [ac, bc+d] * (e, f)$

$(ace, bce+ed+f] = [ace, bce+ed+f)$

$\therefore$ satisfied associative law.

(iii) Identity :-

$a \Rightarrow (a,b)$ & $e = (e_1, e_2) \in G$

$(a * b) * (e_1, e_2) = (a, b)$

$(ae_1, be_1 + e_2) = (a, b)$

$\therefore ae_1 = a \Rightarrow \boxed{e_1 = 1}$

$be_1 + e_2 = b$

$b(1) + e_2 = b$

$b + e_2 = b$ $\qquad \therefore \boxed{e = (1, 0)} \in G.$

$\boxed{e_2 = 0}$

iv) Inverse :-

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

$a = (a, b)$, $a^{-1} = (x, y) \in G$

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

$(a,b) * (x, y) = (1, 0)$

$(ax, bx+y) = (1, 0)$

$ax = 1 \qquad bx + y = 0$

$x = 1/a \qquad y = -bx$

$y = -b \times 1/a = \frac{-b}{a}$

$\therefore a^{-1}$ is $(1/a, -b/a) \in G$.

v) Commutative :- $\quad a * b = b * a$

$(a,b) * (c,d) = (ac, bc+d)$

$(c,d) * (a,b) = (ca, da+b)$

$a * b \neq b * a \quad \therefore G$ is non abelian group.

now $(1, b) * (1, c)^{-1} = (1, b) * (\frac{1}{1}, -\frac{c}{1})$ $\quad (a,b)^{-1} = (\frac{1}{a}, \frac{-b}{a})$

$$= (1, b) * (1, -c)$$

$$= (1, b-c)$$

$(1, b-c) \in H$

$\therefore$ H is a subgroup of G.

Group Homomorphism :-

If $(G,*)$ and (G',Δ) are two groups, then a mapping $f: G \to G'$ is called a group homomor-phism, if for any $a,b \in G$.

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

Theorem :-

If $f: G \to G'$ is a group homomorphism from $(G,*)$ to (G,Δ) then

(i) $f(e) = e'$, where e and e' are the identity elements of G and G' respectively.

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

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

Proof :-

(i) $f(e*e) = f(e) \,\Delta\, f(e)$ (by defn of Homomorphism) $f(a*b) = f(a)\Delta f(b)$

(ie) $f(e) = f(e) \Delta f(e)$ ($a^2 = a$ then a is idempotent)

$f(e)$ is idempotent element of (G',Δ).

$\Rightarrow$ $f(e)$ is identity element of G'.

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

Hence proved.

(ii) G is group for any $a \in G$, $a^{-1} \in G$.

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

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

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

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

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

$$e' = f(a^{-1}) \Delta f(a) \longrightarrow (2)$$

from (1) & (2)

$\therefore f(a^{-1})$ is the inverse of $f(a)$

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

Hence proved.

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

now $h_1' \Delta (h_2')^{-1} = f(h_1) \Delta f(h_2)^{-1}$ (by 2)

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

$= f(h_1 * h_2^{-1})$ (by homomorphism)

$= f(h_3)$ where $h_3 = h_1 * h_2^{-1} \in H$ as H is a subgroup.

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

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

$\therefore f(h)$ is a subgroup.

Kernal of homomorphism :-

Defn :-

If $f : G \to G'$ be a group homomorphism, then the set of elements of G which are mapped into e' (identity of G') is called the kernal of f and it is denoted by $\ker(f)$.

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

Theorem :-

The kernal of a homomorphism f from a group $(G, *)$ to another group (G', Δ) is a subgroup of $(G, *)$.

Proof:-

We know that $\ker f = \{x \in G \mid f(x) = e'\}$

since $f(e) = e'$ is always true, atleast $e \in \ker(f)$

(ie) $\ker(f)$ is a non-empty subset of $(G, *)$

let $a, b \in \ker(f)$

$$f(a) = e' \text{ and } f(b) = e'$$

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

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

$$= e' * e'$$

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

$$a * b^{-1} \in \ker f$$

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

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

Problems :-1

If R and C are additive groups of real and complex numbers respectively and if the mapping $f: C \to R$ is defined by $f(x+iy) = x$, show that f is homomorphism. Find also the kernal of f.

soln:

Soln:- Let $a+ib$ and $c+id$ be any two elements of C. then

$$f[(a+ib)+(c+id)] = f[(a+c)+i(b+d)]$$

$$= a+c \qquad (\because f(a,b)=a)$$

$$= f(a,b)+f(c,d) \qquad f(c,d)=c)$$

$\therefore$ f is group homomorphism from C to R.

The identity of R is real number 0

The images of all complex numbers with real part 0 are each equal to 0, the identity of R

Hence, $\ker(f)$ = the set of all purely imaginary numbers.

2) If $(R,+)$ & $(C,*)$ is two non-empty set with binary operation '+' & '*' then the mapping $f: R \to C$ is defined by $f(x) = e^{ix}$ then show that f is group homomorphism and also find $\ker(f)$.

Soln:-

$f: (R,+) \to (C,*)$

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

given $f(x) = e^{ix}$ $\qquad f(x+y) = e^{i(x+y)}$

$$= e^{ix} \cdot e^{iy}$$

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

f is group homomorphism.

Ring :-

A non-empty $(R,+,\cdot)$ said to be a ring with binary operation '+' and '$\cdot$' is satisfies the following condition.

(i) $(R,+)$ is an abelian group → ⑤ conditions
(ii) $(R,\cdot)$ is a semigroup. → ② conditions
(iii) $(R,\cdot)$ is distributive over +

$a,b,c \in R \Rightarrow a\cdot(b+c) = (a\cdot b)+(a\cdot c)$
$(b+c)\cdot a = (b\cdot a)+(c\cdot a)$

Commutative ring :-

A ring $(R,+,\cdot)$ is said to be then $(R,\cdot)$ is a commutative. (If $ab=ba$ for $a,b\in R$)

ring with Identity (or) Unity :-

If $(R,\cdot)$ is a monoid, then the ring $(R,+,\cdot)$ is called ring with identity.

Zero divisors :-

If a and b be two non-zero elements of a ring R such that $a\cdot b=0$ then a and b are called zero divisors.

Integral domain :-

A Commutative ring with identity $(R,+,\cdot)$ and without zero divisors is called an integral domain.

Ex: $(Z,+,\cdot)$ is integral domain.

Field :-

A Commutative ring with multiplicative identity contain atleast 2 element in the field, then the every non-zero element of R has multiplicative inverse.

A commutative (or) division ring is called a field.

Ex: -

i) $(R, +, \cdot)$ is a field.

ii) $(Q, +, \cdot)$ is a field.

Properties of a rings :-

1) (a) The additive identity or the zero element of a ring $(R, +, \cdot)$ is Unique.

(b) The additive inverse of every element of the rings is unique.

(c) The multiplicative identity of a ring, if it is exists, is unique.

(d) If the ring has multiplicative identity, then the multiplicative inverse of any non-zero element of the rings is Unique.

2) The cancellation laws of addition for all $a, b \in R$.

(a) If $a+b = a+c$ then $b=c$ (left cancellation law)

(b) If $b+a = c+a$ then $b=c$ (Right cancellation law)

3) If $(R, +, \cdot)$ is a ring and $a \in R$ then

$a \cdot 0 = 0 \cdot a = 0$, where 0 is the zero element of R.

4) If $(R,+,\cdot)$ is a ring, then for any $a,b,c\in R$

a) $-(-a)=a$

(b) $a\cdot(-b)=(-a)\cdot b=-(a\cdot b)$

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

(d) $a\cdot(b-c)=(a\cdot b)-(a\cdot c)$

(e) $(a-b)\cdot c=(a\cdot c)-(b\cdot c)$

5) A commutative ring with unity is an integral domain If and only if it satisfies cancellation law of multiplication.

6) * Every field is integral domain.
Converse ~~Every~~ need not be true.

* Every integral domain is not a field.

7) Every finite integral domain is a field.

Subring :-

A non-empty subset $S\subseteq R$, where $(R,+,\cdot)$ ring is called a subring of R.
$(S,+,\cdot)$ is itself is a ring.

Ring homomorphism :-

If $(R,+,\cdot)$ and $(S,+,\cdot)$ be ring then the mapping $f:R\rightarrow S$ is called a ring homomorphism, If for any $a,b\in R$ such that

$f(a+b)=f(a)\oplus f(b)$ &

$f(a\cdot b)=f(a)\odot f(b)$.

Properties:-

1) If $(R,+,\cdot)$ is a ring and S is non_empty subset of R, then $(S,+,\cdot)$ is subring of R, If and only if for all $a,b \in S$, $a-b \in S$ and $a*b \in S$.

2) If $f:(R,+,\cdot) \to (S,\otimes,\odot)$ is a ring homomorphism then a) $f(0)=0'$, where 0 and $0'$ are the additive identities (zeros) of R and S.

b) $f(-a)=-f(a)$ for every $a \in R$.

c) $f(na)=nf(a)$ for every $a \in R$ where n is integer.

d) $f(a^n)=[f(a)]^n$ for every $a \in R$ where n is integer

Problems:-

1) Show that $(Z,\oplus,\odot)$ is a commutative ring with identity, where the operation $\oplus$ and $\odot$ are defined for any $a,b \in Z$ as $a \oplus b = a+b-1$, $a \odot b = a+b-ab$.

Sdn:-

i) To prove $(Z,\oplus)$ is an abelian group.

ii) To prove $(Z,\odot)$ is a monoid & $(Z,\odot)$ is commutative.

iii) To prove $(Z,\odot)$ is distributive over $+$

$a,b,c \in R \Rightarrow a\odot(b\oplus c) = (a\odot b)+(a\odot c)$

1) To prove $(Z,\oplus,\odot)$ is closure under $\oplus,\odot$.

Let $a,b \in Z$ $\quad a\oplus b = a+b-1 \in Z$

$a\odot b = a+b-ab \in Z$

$\therefore (Z,\oplus,\odot)$ closure under $\oplus,\odot$.

2) To Prove $(z, \oplus, \odot)$ is associative under $\oplus$ & $\odot$.

Let $a, b, c \in z \Rightarrow a \oplus (b \oplus c) = (a \oplus b) \oplus c$

$(a \oplus b = a+b-1)$

$a \oplus (b+c-1) = (a+b-1) \oplus c$

$a+b+c-1-1 = a+b+c-1-1$

$a+b+c-2 = a+b+c-2$

Hence proved.

Let $a, b, c \in z \Rightarrow (a \odot (b \odot c) = (a \odot b) \odot c$

$(\because (a \odot b) = a+b-ab)$

$a \odot (b+c-bc) = (a+b-ab) \odot c$

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

$a+b+c-bc-ab-ac+abc = a+b+c-ab-ac-bc+abc$

Hence

$a \odot (b \odot c) = (a \odot b) \odot c$.

3) To find identity $(z, \oplus, \odot)$:-

$a \oplus e = e \oplus a = a$

$\Rightarrow \cancel{a}+e-1 = \cancel{a}$

$\boxed{e=1}$

$a \odot e = e \odot a = a$

$\cancel{a}+e-ae = \cancel{a}$

$e(1-a) = 0$

$e=0$ (or) $(1-a)=0$

$\boxed{e=0}$ (if $a \neq 1$)

4) To find inverse $(z, \oplus, \odot)$

$a \oplus a^{-1} = a^{-1} \oplus a = e$

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

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

$\boxed{a^{-1} = 2-a}$

$a \odot a^{-1} = a^{-1} \odot a = e$

$a + a^{-1} - aa^{-1} = e$

$a + a^{-1}(1-a) = 0$

$a^{-1} = \frac{-a}{1-a}$ (if $a \neq 1$)

(or)

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

6) To prove commutative $(Z, \oplus, \odot)$

$a \oplus b = b \oplus a$

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

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

$a \odot b = b \odot a$

$a+b-ab = b+a-ba$

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

$\therefore$ satisfied commutative $(Z, \oplus, \odot)$.

iii) To prove distributive over +

$a, b, c \in R \quad a \odot (b \oplus c) = a \odot b \oplus (a \odot c)$

LHS:

$a \odot (b \oplus c) = a \odot (b+c-1)$

$= a+b+c-1-a(b+c-1)$

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

$a \odot (b \oplus c) = 2a+b+c-ab-ac-1$

and

$(a \odot b) \oplus (a \odot c) = (a+b-ab) \oplus (a+c-ac)$

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

$= 2a+b+c-ab-ac-1$

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

Hence proved.

$\therefore$ Hence $(Z, \oplus, \odot)$ is a commutative ring with identity.

$\therefore (Z, \oplus, \odot)$ is Field.

HW: Prove that the set S of all ordered pairs (a,b) of real numbers is a commutative ring with zero divisors under the binary operations $\oplus, \odot$ defined by

$(a,b) \oplus (c,d) = (a+c, b+d)$

$(a,b) \odot (c,d) = (ac, bd)$ where a,b,c,d are real.

Coding theory:-

Error detection and error correction techniques play an important role in the design of computer systems. Structure in the design of error-correcting codes is important. It makes easy in finding the properties of a code and it makes to realize the hardware of such practical codes.

Algebraic structures are the basis of the most important codes which have been designed. A communication process may take place in a variety of ways, by making a telephone call, sending a message by a telephone or a letter, using a sign language, etc.

Transmitter → channel → receiver

Encoders and Decoders:-

An encoder is a device which transforms the incoming messages in such a way that the presence of noise in the transformed messages is detectable.

A decoder is a device which transforms the encoded messages into their original form that can be understood by the receiver. The model of a typical data communication system with noise is given as

$$\begin{array}{ccccccccc} \text{Transmitter} & \rightarrow & \text{Encoder} & \rightarrow & \text{channel} & \rightarrow & \text{Decoder} & \rightarrow & \text{Receiver.} \\ & & & & \uparrow & & & & \\ & & & & \text{Noise} & & & & \end{array}$$

Group code :-

If $B = \{0,1\}$, then $B^n = \{x_1, x_2, \ldots x_n / x_i \in B, i = 1,2,3 \ldots n\}$ is a group under the binary operation module 2. This group $(B^n, \oplus)$ is called a group code. $(\because (B^n, \oplus)$ is a group & $(B^n, \oplus)$ is abelian group)

In general, any code which is a group under the operation $\oplus$ is called a group code.

Hamming codes :-

The codes obtained by introducing additional digits called parity digits to the digits in the original messages are called Hamming Codes.

Hamming distance :-

If x and y represent the binary strings $x_1, x_2 \ldots x_n$ and $y_1, y_2 \ldots y_n$ the number of the positions in the strings for which $x_i \neq y_i$ is called Hamming distance between x and y and denoted by $H(x,y)$.

Example :- If $x = 11010$ and $y = 10101$ then to find $H(x,y) = ?$

Soln :- $H(x,y)$ = weight of (x,y)

$H(x,y) = |x \oplus y| = |01111| = \underline{\underline{4}}$

$$\begin{array}{r} 1\,1\,0\,1\,0 \\ 1\,0\,1\,0\,1 \ (+) \\ \hline 0\,1\,1\,1\,1 \\ \hline \end{array}$$

Note :-

1) A code can detect at the most k errors iff the minimum distance between any two code words is atleast $(k+1)$.

2) A code can correct a set of at the most k errors iff the minimum distance between any two code words is atleast $(2k+1)$.

Error Correction Using matrices :-

The encoding function $e : B^m \to B^n$ where $m, n \in Z^+$ and $m < n$, where $B = (0,1)$ is given by a $m \times n$ matrix G over B. This matrix G is called the generator matrix for the code and its of the form $[I_m | A]$. where I_m is the $m \times m$ unit matrix and A is an $m * (n-m)$ matrix.

Example :-

If the message $w \in B^2$, we may assume

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

The words that belong to B^2 are $00, 01, 10, 11$

Then the codes words corresponding to the above messages words are

$$e(w) = wG$$

$$e(00) = (0\ 0)\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (0, 0\ 0\ 0\ 0)$$

$$e(01) = (0\ 1)\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (0+0, 0+1\ \ 0+0\ \ 0+1\ \ 0+1)$$

$$= (0\ 1\ 0\ 1\ 1)$$

$$e(10) = (1\ 0)\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (1\ 0\ 1\ 1\ 0)$$

$$e(11) = (1\ 1)\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (1+0\ \ 0+1\ \ 1+0\ \ 1+1\ \ 0+1)$$

$$e(1,1) = (1\ 1\ 1\ 0\ 1)$$

Parity and Generator matrices:-

The encoding fn. $e: B^m \to B^{m+1}$ is called the parity $(m, m+1)$ check code. If $b = b_1 b_2 \cdots b_m \in B^m$ define $e(b) = b_1 b_2 \cdots b_m b_{m+1}$

where

$$b_{m+1} = \begin{cases} 0 & \text{if } |b| \text{ is even} \\ 1 & \text{if } |b| \text{ is odd.} \end{cases}$$

1. The weight of each of the following words in B^4

Soln: (i) $x = 0100$ (ii) $x = 1110$ iii) $x = 0000$ iv) $x = 1111$

v) $x = 0110$

Soln:-

(i) $x = 0100 \Rightarrow |x| = 1$ ii) $x = 1110 \Rightarrow |x| = 3$

iii) $x = 0000 \Rightarrow |x| = 0$ iv) $x = 1111 \Rightarrow |x| = 4$

v) $x = 0110 \Rightarrow |x| = 2$.

Decoding and error correction:-

An onto function $D: B^n \to B^m$ is called an (n, m) decoding function associated with e. If $D(y) = x_t \in B^m$ and is such that when the transmission channel has no noise then $x_t = x$

$$(D \circ e) = I \quad \text{where } I \text{ is identity function on } B^m.$$

Ex: let $e: B^3 \to B^4$ and $D: B^4 \to B^3$ is the decoding fn.

Code x :	000	010	001	011	100	101	110	111
$y = e(x)$ (even) :	0000	0011	0101	0110	1001	1010	1100	1111
$D(y) = (D \circ e)x$:	000	001	010	011	100	101	110	111

Problems:-

1) Find the code words generated by the encoding function $e: B^2 \to B^5$ with respect to the Parity check matrix.

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

Soln:-

To find encoded words:-

$e(w) = W \cdot G$

G = Generator matrix $= [I_m, A_{m\times(n-m)}]$

Parity check matrix $H = [A^T, I_{n-m}]$

Rewriting the given matrix of $H = [A^T | I_{n-m}]$

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

Here $n = 5$, $m = 2$

The generator matrix G is given by

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

now $B^2 = \{00, 01, 10, 11\}$ and $e(w) = w \cdot G$

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

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

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

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

Hence the code words generated by H are 00000, 01011, 10011 and 11000.

2. Find the code words generated by the parity check matrix

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

when the encoding function is $e : B^3 \to B^6$.

Soln :-

The rewriting the given matrix as $H = [A^T | I_{n-m}]$

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

Here $n=6$
$m=3$

The generator matrix G is given by $(m=3)$

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

To find encode words :-

$$e(w) = w \cdot G$$

now

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

$$e(000) = (000)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (000000)$$

$$e(001) = (001)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (001011)$$

$$e(010) = (010)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (010101)$$

$$e(100) = (100)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (100111)$$

$$e(011) = (011)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (011110)$$

$$e(101)=[1\,0\,1]\begin{bmatrix}1&0&0&1&1&1\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix}=[1\,0\,1\,1\,0\,0]$$

$$e(110)=[1\,1\,0]\begin{bmatrix}1&0&0&1&1&1\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix}=[1\,1\,0\,0\,1\,0]$$

$$e(111)=[1\,1\,1]\begin{bmatrix}1&0&0&1&1&1\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix}=[1\,1\,1\,0\,0\,1]$$

The code words are 000000, 001011, 010101, 100111, 011110, 101100, 110010, and 111001.

3) Decode each of the following received words corresponding to the encoding function $e: B^3 \to B^6$ given by $e(000)=000000$; $e(001)=001011$, $e(010)=010101$; $e(100)=100111$; $e(011)=011110$; $e(101)=101100$. $e(110)=110010$; $e(111)=111001$; assuming that no error or signal error has occured:

011110, 110111, 110000, 111000, 011111.

Soln:-

(i) The word 011110 is identical with $e(011)$. Hence no error has occured and original message is 011.

(ii) The word 110111 differs from $e(100)=100111$ in the second position only. Correcting the single error, the transmitted word is 100111 and the original message is 100.

(iii) The word 110000 differ from $e(110)=110010$ in the ~~fifth~~ position only. Correcting this error, the transmitted word is 110010 and the original message is 110.

(iv) The word $11\cancel{0}000$ differs from $e(111) = 111001$ in the sixth position only. Correcting this error, the transmitted words is $\underline{111}001$, and the original message is 111.

(v) The word 011111 differs from $e(011) = 011110$ in the sixth position only. Correcting this error, the transmitted word is $\underline{011}110$ and the original message is 011.

4) Given the generator matrix $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$

Corresponding to the 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 the words decoded Uniquely? $(G = [I_3 | A])$

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

soln :- $H = [A^T, I_{n-m}]$ $G = [I_m, A_{m \times (n-m)}]$

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

$G = [I_3, A_{3\times 3}]$

$H = [A^T, I_3]$

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

A^T I

∴ Compute the syndrome of each of the received word by using $H \cdot [r]^T$

(i) $r_1 = [1\ 1\ 0\ 1\ 0\ 1]$

$$H \cdot r_1^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1+0+0+1+0+0 \\ 1+1+0+0+0+0 \\ 0+1+0+0+0+1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

r_1 has no error. 3

The Decoded word $= \underline{110}101$

The original message is (word) $= 110$.

(ii) $r_2 = [0\ 0\ 1\ 1\ 1\ 1]$

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0+0+1+1+0+0 \\ 0+0+0+0+1+0 \\ 0+0+1+0+0+1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

$\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ lies on 5^{th} position on H. The element in the ~~fifth~~ position of r is Changed.

∴ The decoded word is $\underline{00}1101$ and the original message is 001.

(iii) $r_3 = (1\ 1\ 0\ 0\ 0\ 1)$

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1+0+0+0+0+0 \\ 1+1+0+0+0+0 \\ 0+1+0+0+0+1 \end{bmatrix}$$

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

$\begin{bmatrix}1\\0\\0\end{bmatrix}$ lies on 4^{th} position on H. ∴ the element in the 4^{th} position of r is changed.

∴ The decoded word is 110101 and the original message is 110.

iv) $r_4 = 111111$

$$H \cdot r^T = \begin{bmatrix}1&0&1&1&0&0\\1&1&0&0&1&0\\0&1&1&0&0&1\end{bmatrix}\begin{bmatrix}1\\1\\1\\1\\1\\1\end{bmatrix} = \begin{bmatrix}1+0+1+1+0+0\\1+1+0+0+1+0\\0+1+1+0+0+1\end{bmatrix}$$

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

Since the syndrome is not identical with any positions of H. The received code cannot be decoded only.

The word $\begin{pmatrix}1\\1\\1\end{pmatrix}$ lies 1^{st} + 6^{th} ⇒ decoded words = 011110 ⇒ The original message is 011

2^{nd} + 4^{th} ⇒ decoded words = 101011 ⇒ The original message is 101.

3^{rd} + 5^{th} ⇒ decoded words = 110101 ⇒ The original message is 110.

H.W: 1) Find the code words generated by the parity check matrix $H = \begin{bmatrix}1&1&1&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&1\end{bmatrix}$ when the encoding fn. $e: B^3 \to B^6$.

2) Find the code words generated by the parity check matrix $H = \begin{bmatrix}1&0&1&0&0\\1&1&0&1&0\\0&1&0&0&1\end{bmatrix}$, when the encoding fn. $e: B^2 \to B^5$.

PART-A

1) The minimum distance of a code (10110, 11110, 10011) is _

Soln:

$$\begin{array}{r} 10110 \\ 11110 \\ \hline 01000 \end{array} (+) \qquad \begin{array}{r} 11110 \\ 10011 \\ \hline 01101 \end{array} (+) \qquad \begin{array}{r} 10011 \\ 10110 \\ \hline 00101 \end{array} (+)$$

1   3   2

∴ Ans 1 (minimum distance)

2) The parity check matrix of the ~~given~~ generator matrix $\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$ is

Soln:

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

$$H = [A^T \cdot I_{n-m}] = [A^T I_3]$$

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

3) The weight of the word 110100l is 4

4) A code can detect a set of atmost 5 errors iff minimum distance between any two code word is . atleast (K+1) $\xrightarrow{\text{Ans}}$ atleast 6