Unit - IV

Binary operation on a set - Groups and axioms of groups - properties of groups - permutation group - equivalence classes with addition modulo m and multiplication modulo m. cyclic groups and properties - Subgroups and necessary and sufficient condition of a subset to be a subgroup.

Group homomorphism and properties - Rings definition and examples - zero divisors - Integral domain - definition, examples and properties - Fields - definition, examples and properties

Coding theory - Encoders and decoders - Hamming codes - Hamming distance - Error detected by an encoding function - examples. Error correction using matrices - Problems on error correction using matrices - Group codes - error correction in group codes - parity check matrix - problems on error correction in group codes - Procedure for decoding group codes - Problems - Applications of groups and coding theory in Engineering.

Groups and Rings.

Binary Operation:

Let S be a non-empty set. A binary operation $*$ on S is a function $*: S \times S \to S$. This image of any ordered pair (a, b) of elements of S under $*$ is denoted by $a * b$.

Cayley Table:

Let $S = \{a_1, a_2, \dots a_n\}$ be a finite set with n-elements and $*$ be a binary operation on S. These n^2 products are arranged in n-rows and n-columns with $a_i * a_j$ occuring in the intersection of the ith row and j^{th} column. Such an operation table is called a Cayley table.

Groups:

A non-empty set G with a binary operation $*$ defined on it is called a group, if the following axioms are satisfied:

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

$$a * b \in G.$$

(ii) Associative: For all $a, b, c \in G$,

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

(iii) Identity: There exists an element $e \in G$, such that

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

(iv) Inverse: For each $a \in G$, $\exists$ an element a' such that,

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

The group is denoted by $(G, *)$.

Abelian group:

A group is said to be abelian or commutative if $a * b = b * a \quad \forall a, b \in G$.

Order of a group:

Let G be a group under the operation $*$. The number of elements in G is called the order of the group G and is denoted by $O(G)$.

If G has n elements, $O(G) = n$. If $O(G)$ has finite number of elements then G is a finite group, otherwise it is called an infinite group.

Elementary properties of a group:

Theorem: Let $(G, *)$ be a group then,

(i) identity element is unique

(ii) For each $a \in G$, inverse is unique.

Proof: Given $(G, *)$ is a group.

(i) Let e and e' be two identity elements of G. Then by identity axiom of a group, we get

$$e * e' = e \quad (\because \text{Treating } e' \text{ as identity})$$

$$e * e' = e' \quad (\because \text{Treating } e \text{ as identity})$$

$\therefore e = e'$

Hence identity element is unique.

(ii) Let e be the identity element of G. Let $a \in G$ be any element. Suppose a' and a'' are two inverses of a, then by inverse axiom,

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

and $a * a'' = a'' * a = e$

Now,

$$a' = a' * e \quad (\because e \text{ is identity})$$
$$= a' * (a * a'') \quad [\because a * a'' = e]$$
$$= (a' * a) * a'' \quad [\because \text{Associat}]$$
$$= e * a'' \quad [\because a' * a = e]$$
$$= a''$$

Theorem: 2

In a group $(G, *)$ the cancellation law hold. For all $a, b, c \in G$,

(i) $a * b = a * c \Rightarrow b = c$ [Left cancellation law]

(ii) $b * a = c * a \Rightarrow b = c$ [Right cancellation law]

Proof:

Given $(G, *)$ is a group. Let e be the identity element of G.

(i) Given, $a * b = a * c$

Let a^{-1} be the inverse of a. Premultiplying by a^{-1}, we get,

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$
$$(a^{-1} * a) * b = (a^{-1} * a) * c \quad (\because \text{by associative})$$
$$e * b = e * c \quad (\because \text{by inverse})$$
$$b = c \quad (\because \text{by identity})$$

(ii) Given, $b * a = c * a$

$$(b * a) * a^{-1} = (c * a) * a^{-1} \quad (\because \text{post multiplying } a^{-1})$$
$$b * (a * a^{-1}) = c * (a * a^{-1}) \quad (\because \text{by associative})$$
$$b * e = c * e$$
$$b = c \quad (\because \text{by identity})$$

Theorem: 3

Let $(G, *)$ be a group. Then (i) for each $a \in G$ $(a^{-1})^{-1} = a$

(ii) for all $a, b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$

Proof:

(i) Let $a \in G$. Then a^{-1} is the inverse of a and $(a^{-1})^{-1}$ is the inverse of a^{-1}.

$\therefore a \star a^{-1} = a^{-1} \star a = e$ ($\because$ by inverse)

$a^{-1} \star (a^{-1})^{-1} = (a^{-1})^{-1} \star a^{-1} = e$ ($\because$ by inverse)

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

$a = (a^{-1})^{-1}$ ($\because$ by left cancellation)

(ii) We have to prove that the inverse of $a \star b$ is $b^{-1} \star a^{-1}$.

Consider, $(a \star b) \star (b^{-1} \star a^{-1})$

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

$= a \star e \star a^{-1}$ ($\because b \star b^{-1} = e$)

$= a \star a^{-1}$ ($\because a \star a^{-1} = e$)

$= e$

Now consider,

$(b^{-1} \star a^{-1}) \star (a \star b)$

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

$= b^{-1} \star e \star b$

$= b^{-1} \star b = e$

Thus,

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

Hence $b^{-1} \star a^{-1}$ is the inverse of $a \star b$.

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

Integral powers of an element a:

Let $(G, \star)$ be a group and $a \in G$. For any positive integers n, we define $a^n = a \star a \star a \cdots \star a$ n-times. We define $a^n = e$

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

$= (a^n)^{-1}$ and $a^{n+1} = a^n \star a$

Theorem: 4

In a group $(G, \star)$ the equation $a \star x = b$ and $y \star a = b$ have unique solutions for the unknowns x and y as $x = a^{-1} \star b$, $y = b \star a^{-1}$ where $a, b \in G$.

Proof: Given $(G, \star)$ is a group. Let e be the identity element of G and a^{-1} be the

inverse of a. Given,

$$a * x = b$$

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

($\because$ premultiplying by a^{-1} on both sides)

$$a^{-1} * a * x = a^{-1} * b$$

($\because$ by associative)

$$e * x = a^{-1} * b \quad (\because \text{by inverse})$$

$$x = a^{-1} * b \quad (\because \text{by identity})$$

Thus, $x = a^{-1} * b \in G$ is a solution. We shall now prove the uniqueness.

Suppose $x_1, x_2 \in G$ be two solutions of $a * x = b$ then,

$$a * x_1 = b \text{ and } a * x_2 = b$$

$$a * x_1 = a * x_2$$

$$x_1 = x_2 \quad (\because \text{by left cancellation})$$

Hence the solution is unique and the unique solution is $x = a^{-1} * b$.

Similarily, we can prove that $y * a = b$ has unique solution $y = b * a^{-1}$.

Now, $y * a = b$

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

($\because$ post multiplying a^{-1})

$$y * (a * a^{-1}) = b * a^{-1} \quad (\text{by associ})$$

$$y * e = b * a^{-1} \quad (\text{by inverse})$$

$$y = b * a^{-1}$$

$\therefore y = b * a^{-1} \in G$ is a solution. We shall now prove the uniqueness.

Let y_1, y_2 be two solutions of $y * a = b$.

$$\therefore y_1 * a = b \text{ and } y_2 * a = b$$

$$\Rightarrow y_1 * a = y_2 * a$$

$$\Rightarrow y_1 = y_2$$

Hence the solution is unique and the unique solution is $y = b * a^{-1}$.

<u>Theorem: 5:</u>

In a group G, if $a^2 = e \ \forall a \in G$, then G is abelian (or)

Show that if every element in a group G is its own inverse, then the group G must be abelian.

Solution:

Let $a, b \in G$ be any two elements, then $a * b \in G$. Given every element is its own inverse.

$$a^{-1} = a \;,\quad b^{-1} = b \;,\quad (a*b)^{-1} = a*b$$
$$\hookrightarrow (1) \qquad \hookrightarrow (2) \qquad \hookrightarrow (3)$$

To prove G is abelian, we have to prove G admits commutative axiom.

From (3), $a*b = (a*b)^{-1}$

$= b^{-1} * a^{-1}$ ($\because$ by Thm 3)

$= b * a$ ($\because$ by (1) & (2))

Hence G is abelian.

Also if $a^2 = e \;\forall\, a \in G$

$$a^{-1} * a^2 = a^{-1} * e$$
$$a^{-1} * (a * a) = a^{-1} * e$$
$$(a^{-1} * a) * a = a^{-1} * e$$
$$e * a = a^{-1} * e$$
$$a = a^{-1} \;\forall\, a \in G.$$

$\Rightarrow$ Every element is its own inverse.

Problems:

1. If $G = \{1, \omega, \omega^2\}$ is the set of cube roots of unity, then prove that G is a group under multiplication.

Solution:

$G = \{1, \omega, \omega^2\}$, where ω is the complex cube root of unity. Since G is a finite set, we form Cayley table.

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

(Since $\omega^3 = 1$, $\omega^4 = \omega$)

(i) closure: The body of the table contains all the elements of G only. $\therefore$ closure axiom is satisfied.

(ii) Associativity: Since multiplication is associative in the complex system, it is true in G. $\therefore$ Associative axiom is satisfied.

(iii) Identity: We have, $1 \cdot 1 = 1$

$\omega \cdot 1 = \omega$

$\omega^2 \cdot 1 = \omega^2$

$\therefore 1$ is the identity element in G.

(iv) Inverse: We have,

$1 \cdot 1 = 1 \Rightarrow 1$ is the inverse of 1

$\omega \cdot \omega^2 = 1 \Rightarrow \omega^2$ is the inverse of ω

$\omega^2 \cdot \omega = 1 \Rightarrow \omega$ is the inverse of ω^2

$\therefore$ The inverse axiom is satisfied.

$\therefore (G, *)$ is a group.

(v) Commutative: For all $a, b \in G$

$a \cdot b = b \cdot a$

$\therefore$ Commutative axiom is true in G.

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

2. The set of fourth roots of unity $\{1, -1, i, -i\}$ is a group under usual multiplication.

<u>Solution</u>: $G = \{1, -1, i, -i\}$

We have to prove that G is a group under usual multiplication. We know $i^2 = -1$.

The cayley table is:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(i) closure: The body of the cayley table contains only the elements of G.

$\therefore$ closure axiom is satisfied.

(ii) Associative: Since multiplication is associative, it is inherited in G.

(iii) Identity: From the table,

$1 \cdot 1 = 1$

$1 \cdot (-1) = -1$

$1 \cdot i = i$

$1 \cdot (-i) = -i$

$\therefore 1$ is the identity element.

(iv) Inverse: From the table,

$1 \cdot 1 = 1 \Rightarrow 1$ is the inverse of 1

$(-1) \cdot (-1) = 1 \Rightarrow -1$ is the inverse of -1

$(i) \cdot (-i) = 1 \Rightarrow -i$ is the inverse of i

$(-i) \cdot i = 1 \Rightarrow i$ is the inverse of $-i$

$\therefore$ Inverse is satisfied.

Hence $(G, *)$ is a group.

Commutative: For all $a, b \in G$

$$a * b = b * a$$

Commutative axiom is satisfied.

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

3. Show that the set, $G = \{0, 1, 2, 3, 4, 5\}$ is a group under addition modulo 6.

Solution:

The Cayley table is:

*	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	6	7
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4
0	0	1	2	3	4	5

+	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

(i) closure: The body of the table contains only elements of G once in each row and column. So, G is closed under addition.

(ii) Associativity: Since usual addition is associative, $+_6$ is associative.

(iii) Identity: 0 is the identity element.

(iv) Inverse: $a + a^{-1} = e$

$0 + 0 = 0 \Rightarrow$ Inverse of 0 is 0

$1 + 5 = 0 \Rightarrow$ " 1 is 5

$2 + 4 = 0 \Rightarrow$ " 2 is 4

$3 + 3 = 0 \Rightarrow$ " 3 is 3

$4 + 2 = 0 \Rightarrow$ " 4 is 2

$5 + 1 = 0 \Rightarrow$ " 5 is 1.

Hence $(G, +_6)$ is a group.

(v) Commutative:

$$a + b = b + a \quad \forall\, a, b \in G$$

Hence $(G, +_6)$ is a abelian group.

4. Prove that non-zero elements of Z_7 is a group under multiplication.

Cayley table:

$\cdot_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Permutation group:

Let S_n is a group under composition of functions as operation. The group S_n is called permutation group on n-symbols and $o(S_n) = n!$

(1) If $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$

and $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix}$

find g on A such that $f \cdot g = h \cdot f$

Solution:

Given $f \cdot g = h \cdot f$

$\Rightarrow g = f^{-1} \cdot h \cdot f$

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

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

(2) Let f and g be given,

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

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

and $g^{-1} f \cdot g \cdot f^{-1}$.

Sol:

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

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

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

Problem on groups:

Show that the identity is the only idempotent element in the group.

Solution:

Let a be an element of a group G such that, $a^2 = a$. Now to prove that $a = e$.

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

Equality of permutations:

Let f and g be two permutations defined on a non-empty set P. Then $f = g$ iff $f(x) = g(x)$, $\forall x \in P$.

Eg: Let $S = \{1, 2, 3, 4\}$ and let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$, $g = \begin{pmatrix} 4 & 1 & 3 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

We see that,

$f(1) = 3 = g(1)$

$f(2) = 1 = g(2)$

$f(3) = 2 = g(3)$

$f(4) = 4 = g(4)$

Thus $f(x) = g(x)$, $\forall x \in S$

$\Rightarrow f = g$.

Permutation Identity:

An identity permutation on S, denoted by I, is defined as $I(a) = a$ $\forall a \in S$.

Eg: Let $S = \{1, 2, 3, 4\}$, then $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ is the identity permutation on S.

Composition of permutations:

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

$$f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$$

$$g = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}, \text{ then}$$

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

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

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

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

$$\Rightarrow f \circ g \neq g \circ f$$

i.e) It is not commutative.

Eg:2: $S_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $S_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$$S_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$S_1 \circ (S_2 \circ S_3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

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

$$(S_1 \circ S_2) \circ S_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

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

$$\Rightarrow S_1 \circ (S_2 \circ S_3) = (S_1 \circ S_2) \circ S_3$$

$\Rightarrow$ It is associative.

Inverse permutation:

If $f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$

then $f^{-1} = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$

Eg: Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

then $f^{-1} = ?$

Sol:

Let $f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ x & y & z & u & v \end{pmatrix}$

Then, $f \circ f^{-1} = I$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ x & y & z & u & v \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ y & z & x & v & u \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$\Rightarrow x = 3, y = 1, z = 2, u = 5, v = 4$

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

Problem:

1. If Z_6 is the set of equivalence class generated by the equivalence relation "Congruence modulo 6", prove that $\{Z_6, \times_6\}$ is a monoid.

Solution: If a non-empty set G satisfies closure, associative and identity law, then G is monoid.

$\times_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	0	0	0	0	0	0
[1]	0	1	2	3	4	5
[2]	0	2	4	0	2	4
[3]	0	3	0	3	0	3
[4]	0	4	2	0	4	2
[5]	0	5	4	3	2	1

(i) The operation $\times_6$ is associative.

(ii) [1] is the identity element of $\{Z_6, \times_6\}$

Hence $\{Z_6, \times_6\}$ is a monoid.

The elements [1] and [5] alone are invertible.

2. Show that the set $\{Z_m\}$ of equivalence classes modulo m is an abelian group under the operation $+_m$ of addition modulo m.

Solution:

$Z_m = \{[0], [1], \ldots [m-1]\}$

closure:

Let $a, b \in Z_m$ such that $a+b = q_1 m + r_1$, $0 \le r_1 < m$ then,

$[a] +_m [b] = [r_1] \in Z_m$

$\therefore Z_m$ is closed.

clearly it is associative, for every $[a] \in Z_m$.

$[a] +_m [0] = [0] +_m [a] = [a]$

[0] is an identity element.

If $[a] \neq [0] \in Z_m$, then $[m-a] \in Z_m$ such that,

$[a] +_m [m-a] = [m] = [0]$

Also,

$[m-a] +_m [a] = [0]$

$[a]^{-1} = [m-a]$

Inverse exists.

Now, $[a] +_m [b] = [b] +_m [a] = [r_1]$

$\therefore Z_m$ is commutative with respect to $+_m$.

Thus, $\{Z_m, +_m\}$ is an abelian group.

Cyclic group:

A group $(G, *)$ is said to be a cyclic group if there exists an element $a \in G$ such that every element $x \in G$ is of the form a^n for some integer n. The element a is called a generator of G and is written as $G = (a)$ or $\langle a \rangle$. It is read as G is cyclic group generated by a.

Eg: The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic group generated by i, since $i^2 = -1$, $i^3 = -i$, $i^4 = 1$. Also $-i$ is another generator.

Theorem: 1 Any cyclic group is abelian.

Proof: Let G be an cyclic group generated by 'a'. Then $G = \{a^n / n \in z\}$.

Let $x, y \in G$ be any two elements then,

$x = a^m$, $y = a^n$ for some m and n.

Now,

$$x * y = a^m * a^n = a^{m+n} \longrightarrow (1)$$

$$y * x = a^n * a^m = a^{n+m}$$
$$= a^{m+n} \longrightarrow (2)$$

From (1) and (2)

$$x * y = y * x \quad \forall x, y \in G$$

Hence G is abelian.

Theorem: 2

If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof: Let $G = \langle a \rangle$ be a cyclic group generated by a. Let a^n be any element of G, where n is some integer.

$a^n = (a^{-1})^{-n}$, $-n$ is integer

So, each element of G, is generated by a^{-1}.

Thus, a^{-1} is also a generator of G.

Theorem: 3

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

Proof: Let a^m is a generator of G. Then, for some integer r, $a = (a^m)^r = a^{mr}$

$$a = a^{mr} * e = a^{mr} * e^s, \text{ for some integers.}$$

$$= a^{mr} * (a^n)^s$$

$$= a^{mr+ns}$$

$\therefore mr + ns = 1$

$\text{Gcd}(m, n) = 1$

To prove, the converse let,

$\text{Gcd}(m, n) = 1$

$\therefore$ There exist two integers p and q such that,

$$mp + nq = 1 \longrightarrow (1)$$

Let H be the set generated by a^m, $H \subseteq G \longrightarrow (2)$

Now, $a^{mp+nq} = a$ ($\because$ by (1))

$$a^{mp} * a^{nq} = a$$

$$(a^m)^p * (a^n)^q = a$$

$$(a^m)^p * e = a$$

$$(a^m)^p = a$$

$\Rightarrow$ Each integral power of 'a' will also be an integral power of a^m.

$$G \subseteq H \longrightarrow (3)$$

From (2) and (3), we get

$$H = G.$$

$\therefore a^m$ is a generator of G.

Subgroup:

Let $(G, *)$ be a group and H be a non-empty subset of G. If $(H, *)$ is itself a group, then $(H, *)$ is called a subgroup of $(G, *)$

Eg: Let $G = \{1, -1, i, -i\}$ be a group then $H = \{1, -1\}$ is a subgroup.

Note: $\{e\}$ and G are trivial subgroups. All other subgroups are proper subgroups.

Theorem: 1

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

Proof: Necessary Condition

Let H be a subgroup. Then if $a, b \in H$, $b^{-1} \in H$

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

Sufficient Condition:

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

If $a = b$, then $a * a^{-1} \in H$

$\Rightarrow e \in H$

For $e, a \in H$, we have $e * a^{-1} \in H$

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

III^{ly} $b^{-1} \in H$

For a and $b^{-1} \in H$, we have

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

$\therefore \{H, *\}$ is a group and hence a subgroup of G.

Group Homomorphism:

Let $(G, *)$ and $(G', \cdot)$ be two groups. A mapping $f: G \to G'$ is called a group homomorphism if for all $a, b \in G$, $f(a * b) = f(a) \cdot f(b)$.

Eg: Consider the groups $(R, +)$ and $(R^*, \cdot)$ where R^* is the set of all non-zero real numbers i.e) $R^* = R - \{0\}$. Let $f: R \to R^*$ be defined by $f(a) = 2^a$, $\forall a \in R$.

For $a, b \in R$ be any two elements then $a + b \in R$.

Now,

$$f(a+b) = 2^{a+b}$$
$$= 2^a \cdot 2^b$$
$$= f(a) \cdot f(b)$$

$\therefore f$ is a homomorphism.

Kernal of homomorphism:

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

Cosets: If $\{H, *\}$ is a subgroup of $\{G, *\}$, then the set aH, where $a \in G$, defined by $aH = \{a * h \mid h \in H\}$ is called the left coset of H in G.

III^{ly} $Ha = \{h * a \mid h \in H\}$ is said as right coset of H in G.

Theorem: 1

If H, K be two subgroups of a group G, then HK is a subgroup of G iff $KH = HK$.

Proof:

Let H, K be any two subgroups of G.

Let $HK = KH$

To prove HK is a subgroup of G, we have to prove that

$$(HK)(HK)^{-1} = HK$$

$$\cancel{(HK)(K^{-1}H^{-1})}$$

Now, $(HK)(HK)^{-1} = (HK)(K^{-1}H^{-1})$

$$= H(KK^{-1})H^{-1}$$
$$= (HK)H^{-1}$$
$$= (KH)H^{-1}$$
$$= K(HH^{-1})$$
$$= KH$$
$$= HK$$

Conversely, HK is a subgroup.

Then $(HK)^{-1} = HK$

$\Rightarrow K^{-1}H^{-1} = HK$

$\Rightarrow KH = HK$

Hence the result.

Theorem: 2 If H and K be two subgroups of G, then $H \cap K$ is also a subgroup of G.

Proof: Let H and K be any two subgroups of G.

$H \cap K \neq \phi$ $\{e\}$ is common to both H and K.

To prove $H \cap K$ is a subgroup

$h \in H \cap K$, $k \in H \cap K$

$\Rightarrow hk^{-1} \in H \cap K$

Now, $h \in H \cap K \Rightarrow h \in H$ and $h \in K$

$k \in H \cap K \Rightarrow k \in H$ and $k \in K$

$h \in H, k \in H \Rightarrow hk^{-1} \in H$

$h \in K, k \in K \Rightarrow hk^{-1} \in K$

$\therefore hk^{-1} \in H \cap K$

Hence $H \cap K$ is a subgroup of G.

Theorem: 3: Fundamental theorem of homomorphism

Let $f: G \to G'$ be a homomorphism. Let H be kernal of f. Then $G/H \simeq G'$.

Proof:

Let $f: G \to G'$ and define $\phi: \frac{G}{H} \to G'$ as

$\phi(Ha) = f(a)$

(i) ϕ is well-defined:

Let $Hb = Ha$

$b = ha, \; h \in H$

$f(b) = f(ha)$

$= f(h) \cdot f(a)$

$= e' f(a)$

$= f(a)$

$\therefore \phi(Hb) = f(b) = f(a) = \phi(Ha)$

(ii) ϕ is 1-1:

$\phi(Ha) = \phi(Hb)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow f(a) \cdot [f(b)]^{-1} = e'$

$\Rightarrow f(ab^{-1}) = e'$

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

$\Rightarrow a \in Hb$

$\Rightarrow Ha = Hb$

(iii) ϕ is onto:

Let $a' \in G'$. Since f is onto, $\exists\, a \in G$ such that $f(a) = a'$. Hence $\phi(Ha) = f(a) = a'$.

ϕ is a homomorphism:

$\phi(Ha\, Hb) = \phi(Hab)$

$= f(ab)$

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

$= \phi(Ha) \cdot \phi(Hb)$

$\therefore G/H \simeq G'$.

Theorem: 4 Lagrange's theorem

The order of a subgroup of a finite group divides the order of the group.

Proof:

Let $G = \{a_1 = e, a_2, \ldots a_n\}$ be a group and H be a subgroup of G.

$O(G) = n$

Consider, $e * H = \{eh \mid h \in H\}$

$a_2 * H = \{a_2 h \mid h \in H\}$

$\vdots$

$a_n * H = \{a_n h \mid h \in H\}$

We know any two left or right cosets are either identical or disjoint.

Also, $O(e * H) = O(H)$

$\therefore O(a_i * H) = O(H), \forall a_i \in G$.

Let there be k-disjoint cosets of H in k and their union equals G.

$$G = (a_1 * H) \cup (a_2 * H) \cup \dots \cup (a_k * H)$$

$$O(G) = O(a_1 * H) + \dots + O(a_k * H)$$

$$O(G) = O(H) + \dots + O(H) \quad [k \text{ times}]$$

$$O(G) = k\, O(H)$$

$$k = \frac{O(G)}{O(H)}$$

The order of a subgroup H divides the order of a group G.

Rings and Fields

Ring: $(R, +, \cdot)$ is said to be a ring if the binary operations + and $\cdot$ on R satisfies the following conditions.

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

(ii) $(R, \cdot)$ is a semigroup

(iii) Distributive law:

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

$(b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in R.$

Note:

1. The additive identity 0 is called the zero element of the ring.
2. Zero of the ring has nothing to do with number 0.

Commutative Ring:

A ring $(R, +, \cdot)$ is said to be commutative if $a * b = b * a \quad \forall a, b \in R$.

Ring with identity:

A ring $(R, +, \cdot)$ is said to be a ring with identity if there exists an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a \quad \forall a \in R$.

Elementary properties of a ring:

Let $(R, +, \cdot)$ be a ring. Then for $a, b, c \in R$,

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$
4. $a \cdot (b - c) = a \cdot b - a \cdot c$

If R has unit element 1,

5. $(-1) \cdot a = -a$
6. $(-1) \cdot (-1) = 1.$

Ring Without Zero-divisors:

In a commutative ring $(R,+,\cdot)$ if for any $a,b \in S$ such that $a \neq 0$, $b \neq 0 \Rightarrow ab \neq 0$ then the ring is without zero divisors.

Integral domain:

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

Field:

A commutative ring $(R,+,\cdot)$ with identity in which every non-zero element has multiplicative inverse is called a field.

Eg: $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ are fields. But $(\mathbb{Z},+,\cdot)$ is an integral domain and not a field.

Subring:

Let $(R,+,\cdot)$ be a ring. A non-empty subset S of R is said to be a subring of R if S itself is a ring w.r.to the same operations $+$ and $\cdot$ of R.

Note:

To verify a subset of a ring is a subring it is enough to verify the conditions.

(i) $(S,+)$ is a subgroup of $(R,+)$

(ii) S is closed under $+$,

ie) for $a,b \in S$, $a-b \in S$ and $a \cdot b \in S$.

Ring Homomorphism:

Let $(R,+,\cdot)$ and $(S,\oplus,\odot)$ be rings. A mapping $f: R \to S$ is called a ring homomorphism if $f(a+b) = f(a) \oplus f(b)$ and $f(a \cdot b) = f(a) \odot f(b)$ $\forall\, a,b \in R$.

Properties of ring homomorphism:

If $f : (R, +, \cdot) \to (S, \oplus, \odot)$ is a ring homomorphism then,

(i) $f(0) = 0'$

(ii) $f(-a) = -f(a)$

(iii) $f(na) = n f(a)$

(iv) $f(a^n) = [f(a)]^n$

(v) If A is a subring of R then $f(A)$ is a subring of S.

(*) Every subgroup of a cyclic group is cyclic.

Proof: Let $(G, *)$ be cyclic. So, $G = \langle a \rangle$. Let H be any subgroup of G.

If $H = \langle e \rangle$ or $H = G$. then nothing to prove. So, assume $H \neq \langle e \rangle$ and $H \neq G$.

Since G is cyclic, $\Rightarrow G = \{a, a^2, \ldots a^n = e\}$.

$H \subseteq G$, so elements of H will be powers of 'a'. Let 'k' be a least positive integer such that $a^k \in H$.

Claim: $H = \langle a^k \rangle$

Let $x \in H$ then $x = a^m$, for some m.

Claim: k / m

If possible $k \nmid m$, then by division algorithm $\exists$ q and r such that,

$$m = kq + r, \quad 0 < r < k.$$

$$m - kq = r$$

$$a^r = a^{m-kq}$$

$$\Rightarrow a^r = a^m \cdot a^{-kq}$$

$$= a^m \cdot (a^k)^{-q} \in H$$

($\because a^k \in H$, $a^m = x \in H$, by closure)

$\Rightarrow a^r \in H$, where $r < k$. which is a contradiction since 'k' is least.

$\therefore k / m$

$\Rightarrow m = kq$

$$x = a^m = a^{kq} = (a^k)^q$$

$\Rightarrow x \in H$ is arbitrary.

So, $\forall x \in H$, written as power of a^k.

So, $H = \langle a^k \rangle$. Hence H is cyclic.

Theorem: Any two left (right) cosets of H in G is either identical or disjoint. Also its partitions the group G ie) $G = \bigcup aH$.

Proof:

Let aH, bH be any two left cosets of H in G. ie) $G = \cancel{bH}$. where $a, b \in G$.

~~Proof: Let aH~~

Claim: Either $aH = bH$ (or) $aH \cap bH \neq \phi$.

Suppose $aH \cap bH \neq \phi$ then there exists $c \in aH \cap bH$.

$\Rightarrow c \in aH$ and $c \in bH$

$\Rightarrow c = a * h_1$ and $c = b * h_2$ ②

① $h_1, h_2 \in H$

$a * h_1 = b * h_2$

$\Rightarrow a = b * h_2 * h_1^{-1}$ ③

Let $x \in aH$

So, $x = a * h_3$, $h_3 \in H$

$x = b * h_2 * h_1^{-1}$ (using ③)

Since $H \leq G$, by closure

$h_1, h_2 \in H \Rightarrow h_2 * h_1^{-1} \in H$

$\therefore x \in bH$

$x \in aH \Rightarrow x \in bH$

$\therefore \boxed{aH \subseteq bH}$

Illy we prove, $\boxed{bH \subseteq aH}$

$\therefore \boxed{aH = bH}$

Hence any two left cosets are either equal or disjoint.

Also $a \in G$, $a = a * e \in aH$

$\Rightarrow a \in aH$

So, $a \notin$ any other left coset

So, these forms a partition.

$$\boxed{G = \bigcup_{a \in G} aH}$$

Order of an element:

Let $(G, *)$ be a group and $a \in G$. The order of 'a' is denoted by $o(a)$. is the least positive integer 'm' such that $a^m = e$.

If it is not possible to find such 'm' then $o(a) =$ infinite.

Eg: 1. $G = \{1, -1, i, -i\}$.

$(G, \cdot)$ is a group with identity $e = 1$.

Always $o(e) = 1$ $\because 1^1 = 1$

$-1 \in G$, $(-1)^1 = -1$, $(-1)^2 = 1$ $\boxed{o(-1) = 2}$

$i \in G$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$

$\boxed{o(i) = 4}$

$-i \in G$, $(-i)^1 = -i$, $(-i)^2 = -1$,
$(-i)^3 = i$, $(-i)^4 = 1 = e$,
$O(-i) = 4$.

<u>Note</u>: $O(a)$ divides $O(G)$.

(2). $G = (Z_6, +_6)$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$O(G) = 6$.

Identity, $e = 0 \Rightarrow \boxed{O(0) = 1}$

$1 \in G$, $1^1 = 1$, $1^2 = 2$, $1^3 = 3$, $1^4 = 4$
$1^5 = 5$, $1^6 = 6 = 0 = e$
$\therefore \boxed{O(1) = 6}$

$2 \in G$, $2^1 = 2$, $2^2 = 2+2 = 4$,
$2^3 = 6 = 0 \Rightarrow \boxed{O(2) = 3}$

$3 \in G$, $3^1 = 3$, $3^2 = 6 \Rightarrow \boxed{O(3) = 2}$

$4 \in G$, $4^1 = 4$, $4^2 = 8 = 2$, $4^3 = 0$
$\Rightarrow \boxed{O(4) = 3}$

$5 \in G$, $5^1 = 5$, $5^2 = 10 = 4$, $5^3 = 15 = 3$
$5^4 = 20 = 2$, $5^5 = 25 = 1$, $5^6 = 30 = 0$
$\boxed{O(5) = 6}$

(3) $G = (Z, +)$

$Z = \{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}$

$e = 0$ $\quad O(0) = 1$

$1 \in G$, $1^1 = 1 \Rightarrow O(1) = 1$

$2 \in G$, $2^1 = 2$, $\cancel{2^2 = 4}$, $\cancel{2^3 = 6}$, $\cancel{2^4}$
$1^2 = 2$, $1^3 = 3 \ldots\ldots$

We never get 0, so
$O(1) =$ infinite.

$|||^{ly}$ all other elements is of order infinite under $+$.

Coding Theory

It is an important branch of mathematics, that is developed to understand the transmission techniques. It was the knowledge of group theory as a base. This theory helps in detecting and correcting errors in transmission.

An ideal communication system can be represented as follows:

Transmitter → Channel → Receiver.

Encoder and Decoder:

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 message into their original form that can be understood by the receiver. The model of a typical data communication system with noise is given as:

Transmitter → Encoder → channel (↑ Noise) → Decoder → Receiver.

Hamming Codes:

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

Hamming distance:

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

Eg: If $x = 11010$, $y = 10101$ then

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

$= |01111|$

$$\begin{array}{r} 11010 \\ 10101 \\ \hline 01111 \end{array}$$

(Hint: $0+0=0$, $1+1=0$, $0+1=1$, $1+0=1$)

Length $= 4$

Note:

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

2. A code can detect at the most k-errors iff the minimum distance is atleast $(k+1)$.

Error correction using matrices:

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

Parity and Generator Matrices:

The encoding function

$$e: B^m \to B^{m+1}$$

is called the parity $(m, m+1)$ check code.

If $b = b_1 b_2 \ldots b_m \in B^m$ define

$$e(b) = b_1 b_2 \ldots b_m b_{m+1}$$

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

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

(i) $x = 01000 \Rightarrow |x| = 1$

(ii) $x = 1110 \Rightarrow |x| = 3$

(iii) $x = 0000 \Rightarrow |x| = 0$

(iv) $x = 1111 \Rightarrow |x| = 4$

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

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

This parity check matrix provides a decoding scheme that corrects a single error in transmission.

If 'r' is the received word and if $Hr^T = [0]$, we conclude no error and r is the code word transmitted.

If $Hr^T =$ the ith column of H, single error has occured during transmission and it has occured in the ith component of 'r'. changing the ith component of r we get the code word.

Eg: $r = 11011$

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

$[0,1]$ is the msg.

01011

If neither case (i) nor case (ii) we conclude more than one transmission error have occured. Though the detection of errors is possible in this case, correction is not possible.

Problems :

1. Find the code words generated by the encoding functions $e: B^2 \to B^5$ w.r.to the parity check matrix.

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

Solution:

Rewriting the given matrix as :

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

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

Here $n > 5$ and $m = 2$.

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 $e(w) = wG$.

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

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

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

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

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

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

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

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

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 $e: B^3 \to B^6$.

Solution:

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

$$= [A^T / I_{n-m}], \quad n > 6, m = 3$$

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

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

$$e(000) = [000] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

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

$$e(001) = [001] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

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

$$e(010) = [010] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

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

$e(100) = [1\ 0\ 0\ 1\ 1\ 1]$

$e(011) = [0\ 1\ 1\ 1\ 1\ 0]$

$e(101) = [1\ 0\ 1\ 1\ 0\ 0]$

$e(110) = [1\ 1\ 0\ 0\ 1\ 0]$

$e(111) = [1\ 1\ 1\ 0\ 0\ 1]$

Thus the code words are 000000, 001011, 010101, 100111, 011110, 101100, 110010, 111001.

3. Decode each of the following received words corresponding to the encoding function. $e: B^3 \to B^6$ given

$e(000) = [0\ 0\ 0\ 0\ 0\ 0]$

$e(001) = [0\ 0\ 1\ 0\ 0\ 1]$

$e(010) = [0\ 1\ 0\ 1\ 0\ 1]$

$e(100) = [1\ 0\ 0\ 1\ 1\ 1]$

$e(011) = [0\ 1\ 1\ 1\ 1\ 0]$

$e(101) = [1\ 0\ 1\ 1\ 0\ 0]$

$e(110) = [1\ 1\ 0\ 0\ 1\ 0]$

$e(111) = [1\ 1\ 1\ 0\ 0\ 1]$

assuming no error or single error occured.

011110, 110111, 110000, 111000, 011111.

<u>Solution:</u>

(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 message is 100.

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

(iv) The word 111000 differs from $e(111) = 111001$ in the sixth position. Correcting this error, the transmitted word is 111001 and original 111

(v) The word 011111 differs from $e(011) = 011110$ in the sixth position. Correcting the error, the transmitted word is 011110 and original is 011.

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

Corresponding to the encoding function $e: B^3 \to B^6$. Find the parity check matrix and use it to decode the following received words and find the original message. Are all the words decoded uniquely?

$G = [I_3 / A]$

(i) 110101

(ii) 001111

(iii) 110001

(iv) 111111

<u>Solution:</u>

$$H = [A^T / I_3]$$

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

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

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

$$= [0 \ 0 \ 0]^T$$

Since $H \cdot [e(w)]^T = (0\ 0\ 0)^T$ The received word is the transmitted word itself. Original message is 110.

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

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

Since the syndrome $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ is the same as fifth column of it, the element in the fifth position of r is changed.

The decoded word is 001101 and original is 001.

(iii) $H \cdot [r]^T = \begin{bmatrix} 101100 \\ 110010 \\ 011001 \end{bmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$

Since the syndrome $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ is the same as fourth column of H, the fourth position of r is changed. The decoded word is 110101 and original is 110.

(iv) $H \cdot [r]^T = \begin{bmatrix} 101100 \\ 110010 \\ 011001 \end{bmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$

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