UNIT-5

Algebraic system consists of a set with an operation on the set and the accompanying properties

Operation: can be unary, binary, ternary ... n-ary ...
Binary operation on a set is a function f from A×A to A. n-ary operations are class of functions having closure properties.

Set A is said to be closed wrt an operation if that operation on members of A always produces another member of A.

Ex:- 1) P(S) - powerset of S. For any sets A, B, C of P(S)
unary opⁿ - complementation.
binary opⁿˢ - ∪, ∩, symmetric difference defined by $A \oplus B = (A \cup B) - (A \cap B)$
ternary opⁿ - $f(A,B,C) = A \cap B \cap C$
⋮
n-ary opⁿ - $f(A_1, A_2 \ldots A_n) = \bigcup_{i=1}^{n} A_i$

2) Z is closed wrt
binary opⁿˢ - +, ×, −

3) Set of odd integers is closed under ×.
but not closed wrt − ∵ diff of two odd integers is even (not odd)
also not closed wrt + ∵ sum of two odd integers is even (not odd).

4) $S = \{A \mid A_{m \times n}$ real matrix$\}$. S is closed wrt
binary opⁿˢ - matrix addition, subtraction
but not
unary opⁿ of transposition ∵ A^T is n×m matrix ∉ S

Defn:-

An algebraic system or an algebra is a system consisting of a non empty set A and one or more n-ary opns on the set A. It is denoted by $\langle A, f_1, f_2 \ldots \rangle$ where $f_1, f_2 \ldots$ are operations on A.

An algebraic structure is an algebraic system $\langle A, f_1, f_2 \ldots, R_1, R_2 \ldots \rangle$ where in addition to operations f_i, the relations R_i are defined on A.

Ex of algebraic system include semigroup, monoid, group, Boolean algebra, ring etc.

General Properties of an algebraic system:-

Let A be a non empty set and + & · are two closed binary operations on A. Then for any two elements a, b, c of A we have

i) Associative property for +: $(a+b)+c = a+(b+c)$

ii) " " for ·: $(a \cdot b) \cdot c = a \cdot (bc)$

iii) Commutative " for +: $a+b = b+a$

iv) " " for ·: $a \cdot b = b \cdot a$

v) Identity element for +: 0 is identity ele.

$a+0 = 0+a = a$, $a \in A$

vi) " " for · : 1 is identity

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

vii) Inverse element under +:

for each $a \in A$, there exists $b \in A$ such that $a+b = b+a = 0$. (b is inverse of a & -a is inverse)

viii) Inverse element under ×:

viii) Distributive law of $\cdot$ over $+$:

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

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

ix) Cancellation property:

$ab = ac \Rightarrow b = c$ provided $a \neq 0$

x) Idempotent property:

$a+a = a$

$a \cdot a = a$

Ex:

1) Algebraic system $\langle Z, +, \cdot \rangle$ with $+, \cdot$ satisfies properties from i to to ix except x.

2) $M_2(Z)$: 2×2 matrices of integers are closed under $+, \cdot$, satisfies commutative & associative properties for $+$. Additive identity element 0 is $0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ for any $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Additive inverse is $-A = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

Matrix multiplication is associative but not commutative. Multiplicative identity is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$:

$AI = IA = A$

ix & x are not satisfied.

3) $P(S)$ powerset of S $\langle P(S), \cup, \cap \rangle$ satisfies except inverse, ix & x.

4) Poly(R) - set of all polynomials in x with real coefficients. $\langle Poly(R), +, \cdot \rangle$ is a commutative ring satisfying all properties from i to ix) except x.

5) S_3 - Set of all permutations with 1,2,3.

$(S_3, \cdot)$ is algebraic system where $\cdot$ is a composition of permutations.

$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$\cdot$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

Binary operation of composition is closed under $\cdot$ on:

$\therefore$ Composition is associative, $\cdot$ is associative.

f_1 is identitity. All elements have inverses.

$f_1^{-1} = f_1$, $f_2^{-1} = f_3$, $f_3^{-1} = f_2$, $f_4^{-1} = f_4$, $f_5^{-1} = f_5$

$f_6^{-1} = f_6$.

$\therefore \langle S_3, \cdot \rangle$ is an algebraic structure known as Group.

i.e., Group satisfies a) closure b) associative & has c) identity d) inverse.

Ex:- Boolean algebra with $A=\{0,1\}$ & two binary ops + and . on A and unary complement is an algebraic system.

$0+0=0, \quad 0+1=1+0=1+1=1$

$0\cdot 0=1\cdot 0=0\cdot 1=0, \quad 1\cdot 1=1$

$0'=1, \quad 1'=0.$

Satisfies all properties from 1 to 8.

Homomorphism & Isomorphism:

Let $(X,\cdot)$ & $(Y,*)$ be two algebraic systems where $\cdot, *$ are n-ary ops. A function $f: X\to Y$ is known as a homomorphism from $(X,\cdot)$ to $(Y,*)$ if for any $x_1, x_2 \in X$ we have

$$f(x_1\cdot x_2) = f(x_1) * f(x_2).$$

Homomorphism is called

i) epimorphism if f is onto (injective)
ii) monomorphism if f is one to one (surjective)
iii) isomorphism if f is one to one & onto (bijecti

When $(X,\cdot)$, $(Y,*)$ are isomorphic then the two algebraic systems are structurally indistinguisha

Thm 1:- If $f: S \to T$ is a homomorphism (epi, mono, iso) from $(S, *)$ to (T, Δ) and $g: T \to P$ is also homomorphism (epi, mono, iso) from (T, Δ) to (P, ∇), then $g \circ f: S \to P$ is a homomorphism (epi, mono, iso) from $(S, *)$ to (P, ∇).

Proof:- $\because$ f is homomorphic then for any $s_1, s_2 \in S$,

$$f(s_1 * s_2) = f(s_1) \Delta f(s_2) .$$

But for $f(s_1) \Delta f(s_2) \in T$

$$g(f(s_1) \Delta f(s_2)) = g(f(s_1)) \nabla g(f(s_2)) \quad \because T \text{ is homo.}$$

Also,

$$\begin{aligned}(g \circ f)(s_1 * s_2) &= g(f(s_1 * s_2)) \\ &= g(f(s_1) \Delta f(s_2)) \quad \because f \text{ is homo.} \\ &= g(f(s_1)) \nabla g(f(s_2)) \quad \because g \text{ is homo.}\end{aligned}$$

$\therefore$ $g \circ f: S \to P$ is homomorphism.

— if f, g are epimorphism, ie, f & g are onto then $g \circ f$ is also onto $\therefore$ it is epimorphism.

if f, g are mono., ie f, g are one to one So is $g \circ f$ is also mono.

Ully when f, g are isomorphic, $g \circ f$ isomorphic.

Ex:-
15.1

2) P.T $\oplus$ is commutative on sets.

Proof:- $A \oplus B = (A \cup B) - (A \cap B)$.

ie $A \oplus B = \{x \mid x \in A \cup B \text{ and } x \notin A \cap B\}$

$= \{x \mid x \in B \cup A \text{ and } x \notin B \cap A\}$

$= B \oplus A$.

3) $*$ on N with $m * n = m + n + k$, k is constant.
S.T. $*$ is a) commutative b) associative.

Proof:- a)

$m * n = m + n + k$

$= n + m + k$

$= n * m$.

b) $(m * n) * p = (m + n + k) * p$

$= (m + n + k) + p + k$

$= m + n + k + p + k$.

$= m + k + (n + p + k)$

$= m + k + (n * p)$

$= m + (n * p) + k$

$= m * (n * p)$.

5) A set of all fns from B to B, $B = \{1, 2\}$.
• is composition. (i) S.T. • is associative
ii) which is identity element iii) find inverse elements

Soln:- 2!

$$f_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \quad f_4 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

•	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_3	f_3	f_3
f_4	f_4	f_4	f_4	f_4

$$f_2 \circ f_3 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

$$f_2 \circ f_4 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

$$f_3 \circ f_2 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

$$f_3 \circ f_4 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

$$f_4 \circ f_2 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

$$f_2 \circ f_2 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

$$f_1 \circ (f_2 \circ f_3) = f_1 \circ f_4 = f_4$$

$$(f_1 \circ f_2) \circ f_3 = f_2 \circ f_3 = f_4.$$

$$f_2 \circ (f_3 \circ f_4) = f_2 \circ f_3 = f_4$$

$$(f_2 \circ f_3) \circ f_4 = f_4 \circ f_4 = f_4.$$

∴ Associative.

f_1 is identity element.

Only f_1, f_2 has inverse. & $f_1^{-1} = f_1$, $f_2^{-1} = f_2$.

It is not commutative ∵ $f_2 \circ f_3 = f_4$ but $f_3 \circ f_2 = f_3$.

Semigroups & monoids.

Semigroup — An algebraic structure satisfying a) closure & b) associative prop.

Monoid - A semigroup with an identity.
i.e., a) closure, b) associative & has c) identity.

If a semigroup $\to (S, \cdot)$ and $\cdot$ satisfies commutative property then $(S, \cdot)$ is called commutative (Abelian) semigroup.
Also a monoid $(M, \cdot, e)$ is commutative (or abelian) monoid when $\cdot$ is commutative.

Note:- In composition table of monoid, no two rows or columns are identical.

Ex:-) $(\mathbb{Z}^+, +)$ is semigroup but not monoid $\because$ identity element $\notin \mathbb{Z}^+$. Also it is abelian semigroup. $\because +$ is commutative.

2) $(N, +)$ is commutative monoid $[N = \{0, 1, 2 \ldots\}]$ with $e = 0$.

3) $(M_n(\mathbb{Z}), +)$ is commutative monoid.

4) $(M_n(\mathbb{Q}), +)$, $(M_n(\mathbb{R}), +) \ldots$ are abelian monoids.

Powers:- of any element $a \in M$ of a monoid $(M, *)$ are defined as $a^0 = e = \text{identity}$, $a^1 = a$, $a^2 = a * a$, $\ldots a^{k+1} = a^k * a$ for $k \in N$.
Raising to powers operation is commutative since for any $m, n \in N$, $a^{m+n} = a^m * a^n = a^n * a^m = a^{n+m}$.

Cyclic monoid:- is a monoid $(M, *, e)$ in which every element of M can be expressed as some powers of a particular element $a \in M$. 'a' is called generator of the cyclic monoid because for any $x \in M$, $x = a^n$, $n \in N$.

A cyclic monoid is an abelian monoid

∵ for any $x, y \in M$, $x = a^m$, $y = a^n$, $x * y = a^m * a^n$.

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

Ex-1) $S = \{00, 01, 02 \ldots 99\}$. $*$ is op^n on S such that for any $x, y \in S$, $x * y$ is string formed by the ~~string~~ for two right most digits of the ordinary product xy i.e., $x * y$ be remainder when xy is divided by 100.

a) S.T $(S, *)$ is an abelian monoid

b) What is identity

c) Determine cyclic monoid generated by 07.

Soln:-

a) $*$ is associative

Ex:- $(08 * 03) * 84 = (24) * 84 = 16$

$(08) * (03 * 84) = (08) * 52 = 16$.

b) It is commutative ∵ ordinary multiplication is commutative. 01 is identity element.

∴ $(S, *)$ is an abelian monoid.

c) $07^2 = 07 * 07 = 49$

$07^3 = 07^2 * 07 = 43$

$07^4 = 07^2 * 07^2 = 01$

$07^5 = 07^4 * 07 = 07$

$07^6 = 07^5 * 07 = 49 = 07^2$.

$\because 07^6 = 07^2$ we have $07^7 = 07^3 = 43$.

$\therefore 07^{6+n} = 07^{2+n}$.

$\therefore$ Cyclic monoid generated by the generator 07 of S is

$\langle 07 \rangle = \{01, 07, 49, 43\}$ which is a finite cyclic monoid

2) $(N, +, 0)$ is an infinite cyclic monoid generated by $1 \in N$.

3) P.T. $(N, *)$ is commutative monoid where $x * y = \max\{x, y\}$

Soln:- $*$ is associative

$\because$ for any $x > y > z \in N$,

$x * (y * z) = x * (\max\{y, z\}) = x * y = \max\{x, y\} = x$.

$(x * y) * z = \max(x, y) * z = x * z = \max\{x, z\} = x$.

$0 \in N$ is identity element $\because x * 0 = 0 * x = x = \max\{x, 0\}$

It is commutative since

$x * y = \max\{x, y\} = \max\{y, x\} = y * x$.

Subsemigroups & Submonoids

Let $(S, *)$ be a semigroup & $T \subseteq S$. Then $(T, *)$ is called subsemigroup of $(S, *)$ if T is closed under $*$

Ily $(M, *, e)$ be a monoid and $T \subseteq M$. Then $(T, *, e)$ is known as a submonoid of $(M, *, e)$ if T is closed under $*$ & $e \in T$.

$(S, *)$ is itself a subsemigroup & $(M, *, e)$ is submonoi

Ex:- For semigroup $(\mathbb{N},+)$, $(\mathbb{Z}^+,+)$ is a subsemigroup ∵ $\mathbb{Z}^+ \subseteq \mathbb{N}$ & $\mathbb{Z}^+$ is closed under +.

$(T,+)$ where T is set of odd integer is not a subsemigroup since T is not closed under +.

2) For monoid $(\mathbb{R},\cdot,1)$, $(\mathbb{N},\cdot,1)$ is a submonoid ∵ $\mathbb{N} \subseteq \mathbb{R}$, $\mathbb{N}$ is closed under $\cdot$ & $1 \in \mathbb{N}$.

$(E,\cdot)$ where E is set of even integers is not submonoid ∵ $1 \notin E$.

3) $A = \{3\}^+ = \{3n \mid n \in \mathbb{Z}^+\} = \{3,6,9,12 \ldots\}$ sums of 3.

$(\{3\}^+,+)$ is a subsemigroup of $(\mathbb{Z},+)$
But it is not submonoid ∵ $e=1 \notin \{3\}^+$.
Also $(\{3\}^+,+)$ is a cyclic semigroup generated by 3.

4) $B = \{2,7\}^+ = \{2^m, 7^n \mid m,n \in \mathbb{N} \ \& \ m+n \geq 1\}$.

$(B,\cdot)$ is a subsemigroup of $(\mathbb{Z},\cdot)$

Here $(B,\cdot)$ is a cyclic group generated by two generators of set $\{2,7\}$. $B = \{2,7,14,28,56 \ldots\}$

Thm: Set of idempotent elements of M for any abelian monoid $(M,*)$ forms a submonoid.

Proof:- Let A be set of identity elements of M.
We have to show that A is closed wrt $*$.
For $a,b \in A$, $a*a = a$ & $b*b = b$ ∴ a,b are idempotent
Now $(a*b)*(a*b) = (a*b)*(b*a)$ ∵ M is abelian
$= a*(b*b)*a$ ∵ $*$ is associative
$= a*b*a$ ∵ b is idempotent
$= (a*a)*b$ ∵ M is abelian
$= a*b$ ∵ a is idempotent

$\therefore$ $a*b$ is an idempotent elements so $a*b \in A$.

$\therefore$ A is closed wrt $*$ & $A \subseteq M$. The identity element e of M is idempotent so $e \in A$. $\therefore (A, *, e)$ is a submonoid of $(M, *, e)$.

Homomorphism & Isomorphism of Semigroup & Monoids.

In design of sequential machines & in formal languages the concept of homomorphism of semigroups & monoids is useful.

Defn:- Let $(S, *)$ and (T, Δ) be any two semigroup. A function $f: S \to T$ is called semigroup homomorphism if for any two elements $a, b \in S$,

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

Thm 3:- Under semigroup homomorphism, properties of i) associativity ii) idempotency iii) commutativity preserved

i) for any $a, b, c \in S$

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

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

$\because$ $*$ is closed under associative

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

$$\therefore (f(a) \Delta f(b)) \Delta f(c) = f(a) \Delta (f(b) \Delta f(c)).$$

$\therefore$ Δ is associative.

ii) for any $a \in S$ which is idempotent,

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

$f(a)$ is idempotent $\in T$.

iii) For any $a, b \in S$

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

$\because$ f is abelian, $f(a*b) = f(b*a)$

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

$\therefore$ Δ is abelian.

Defn:- Let $(M, *, e_M)$ and (T, Δ, e_T) be any two monoids. A function $f: M \to T$ is monoid homomorphism if for any $a, b \in M$,

$$f(a*b) = f(a) \Delta f(b) \quad \& \quad f(e_M) = e_T .$$

—

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

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

Ex:- 1) $(Z^+, +), (Z^+, \cdot)$ are two semigroups.

Define $f: Z^+ \to Z^+$ as $f(m) = 2^m$, $m \in Z^+$.

Then f is a semigroup homomorphism of $(Z^+, +)$ into $(Z^+, \cdot)$ $\because$ $m, n \in Z^+$, $f(m+n) = 2^{m+n} = 2^m \cdot 2^n = f(m) \cdot f(n)$

2) $(N, +, 0)$, $(N, \cdot, 1)$ be two monoids.

$f: N \to N$ as $f(m) = 3^m$, $m \in N$.

Then f is monoid homomorphism of $(N, +)$ into $(N, \cdot)$

$\because$ for any $m, n \in N$

$$f(m+n) = 3^{m+n} = 3^m \cdot 3^n = f(m) \cdot f(n).$$

& $f(0) = 3^0 = 1$.

3) R^+ is set of +ve real nos.

Two semigroup (monoids) $(R^+, \cdot, 1)$, $(R, +, 0)$

Define $f: R^+ \to R$ by $f(x) = \ln x$. Then f is an isomorphism from R^+ onto R.

a) for any $x, y \in R^+$

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

So f is homomorphism.

b) $x \in R$, $e^x (\neq 0) \in R^+$ & $f(e^x) = \ln(e^x) = x$ so f is onto R^+.

c) $x, y \in R^+$, if $f(x) = \ln(x) = f(y) = \ln(y)$

then $e^{\ln x} = e^{\ln y} \Rightarrow x = y$ $\therefore$ f is one to one.

$\therefore$ f is isomorphism.

$\therefore$ $(R^+, \cdot 1)$ is isomorphic to monoid $(R, +, 0)$.

4) E - set of even integers $\{2, 4, \ldots\}$

$f: Z^+ \to E$ by $f(n) = 2n$

f is not semigroup homomorphism from $(Z^+, \cdot)$ into $(E, \cdot)$ $\because$ $m, n \in Z^+$,

$$f(m \cdot n) = 2(m \cdot n) \neq 2m \cdot 2n = f(m) \cdot f(n)$$

Defn:-

If G is a non empty set and $\circ$ is a binary opn on G then $(G, \circ)$ is called a group if following conds are satisfied.

1) Closure - For all $a, b \in G$, $a \circ b \in G$.
2) Associative - $\forall a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$.
3) Identity - $\exists e \in G$ with $a \circ e = e \circ a = a$ $\forall a \in G$.
4) Inverse - $\forall a \in G$, there is an element $b \in G$ such that $a \circ b = b \circ a = e$.

If $\circ$ is commutative ie if $a \circ b = b \circ a$ then G is called an abelian group.

Ex:- Under addition, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are abelian groups. None of them are groups under multiplication as 0 has no inverse. But $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ (non zero $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) are abelian groups under multiplication.

Ring:- $(R, +, \cdot)$ satisfies

a) Commutative law of $+$
b) Associative law of $+$
c) Identity for $+$
d) Inverse for $+$
e) Associative law of $\cdot$
f) Distributive law of $\cdot$ over $+$.

If $(R, +, \cdot)$ is a ring, then $(R, +)$ is an abelian group.

$(R, +, \cdot)$ be a ring.

i) if $ab = ba \quad \forall a, b \in R$, then R is called a commutative ring.

ii) R is said to have no proper divisors of zero if $\forall a, b \in R$,

$ab = z \Rightarrow a = z$ or $b = z$.

iii) if $u \in R$ such that $u \neq z$ & $au = ua = a \quad \forall a \in R$, then u is called a unity or multiplicative identity of R. R is called ring with unity.

Let R be a commutative ring with unity.

a) R is called an integral domain if R has no proper divisors of zero.

b) R is called a field if every non zero element of R is a unit.

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

But Q, R, C under $+, \cdot$ are both integral domains & fields.

Non zero elements of a field $(F, +, \cdot)$ form abelian group $(F^*, \cdot)$.

Ex:- $n \in Z^+, n > 1, (Z_n, +)$ is an abelian group.

$Z_n = \{[0], [1], \ldots [n-1]\}$ Equivalence classes - $[0], [1] \ldots$

p is prime, $(Z_p^*, \cdot)$ is an abelian group.

$(Z_6, +)$

+	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

$(Z_7^*, \cdot)$

·	1	2	3	4	5	
1	1	2	3	4	5	
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

Defn:- For every group G the number of elements in G is called the order of G & is represented by $|G|$.

Exi:- i) $n \in Z^+$, $|(Z_n, +)| = n$ while $|(Z_p^*, \cdot)| = p-1$ for prime

$(Z_9, +, \cdot)$ ring, U_9 - subset $= \{a \in Z_9 \mid a$ is a unit in $Z_9\} = \{a \in Z_9 \mid a^{-1}$ exists $\} = \{1, 2, 4, 5, 7, 8\} = \{a \in Z^+ \mid 1 \le a \le 8$ & $\gcd(a, 9) = 1\}$.

·	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

U_9 is closed under $\cdot$ for ring $(Z_9, +, \cdot)$

1 is identity element & each element has inverse.

$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall\, U_9 \therefore (U_9, \cdot)$ is a group of order 6. $\because$ it is commutative. it is an abelian group.

Defn:- G be a group & $\phi \neq H \subseteq G$. If H is a group under binary operation of G, then H is called a subgroup of G.

Ex:- 1) Every group G has $\{e\}$ and G has subgroups. These are called trivial subgroups. All others are called non trivial or proper.

2) $H=\{0,2,4\}$, $K=\{0,3\}$ are subgroups of $G=(Z_6,+)$

3) $\{1,8\}$, $\{1,4,7\}$ are subgroups of $(U_9,\cdot)$

4) $(Z,+)$ is a subgroup of $(Q,+)$, which is a subgroup of $(R,+)$.

5) $(Z_2,+)$ $(Z_3,+)$ are groups. $G=Z_2 \times Z_3$,
$(a_1,b_1)\cdot(a_2,b_2)=(a_1+a_2, b_1+b_2)$. G is a group of order 6. where $(0,0)$ is identity.

6) $v=\frac{1+\sqrt{3}i}{2}$. $A_6=\{1,v,v^2,v^3,v^4,v^5\}$.
$(A_6,\cdot)$ is a group.

7) S.T G is abelian iff $(ab)^2=a^2b^2$ $\forall\, a,b \in G$.

Proof:- Suppose G is abelian. $(ab)^2=(ab)(ab)=a\cdot(ba)\cdot b$ by associative.

$$(ab)^2 = a(ab)\cdot b \quad \text{(abelian property)}$$
$$= (aa)(bb) \quad \text{(assoc)}$$
$$= a^2b^2$$

Suppose $(ab)^2=a^2b^2$
$(ab)(ab)=a^2b^2$
$a(ba)b=a\cdot abb$ (can)
$(ba)b=abb$ (cancen)
$ba=ab$. $\therefore G$ is abelian

In general, $n \in z^+, n>1$, if $U_n = \{a \in \{Z_n, +, \cdot\} | a \text{ is a unit}\} = \{a \in z^+ | 1 \le a \le n-1 \text{ \& } \gcd(a,n)=1\}$, then $(U_n, \cdot)$ is an abelian group under $\cdot \bmod n$.

Thm:-4:

For every group G,

a) identity of G is unique.

b) inverse of each element of G is unique.

c) if $a,b,c \in G$, $ab=ac \Rightarrow b=c$ (left cancellation)

d) if $a,b,c \in G$, $ba=ca \Rightarrow b=c$ (right cancellation)

Proof:-

a) if e_1, e_2 are both identities in G, then

$e_1 = e_1 e_2 = e_2$

b) Let $a \in G$ & suppose b, c are both inverses of a.

Then $b = b \cdot e = b(ac) = (ba)c = ec = c$.

c) $ab = ac$

multiply b a^{-1},

$a^{-1} \cdot a\, b = a^{-1} a c$

$\Rightarrow b = c$. $\because a^{-1}a = e$ & $e \cdot b = b$.

Ex:- $G = (Z_6, +)$. $H = \{0, 2, 4\}$

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$(H, +)$ is also a group under

8) P.T commutative property is invariant under homomorphism.

Proof:- Let $f: A \to B$ be a group homomorphism onto B. Suppose A is abelian. Since f is onto, for any $a_1, a_2 \in A$, $\exists b_1, b_2 \in B$ such that $f(a_1)=b_1$ & $f(a_2)=b_2$.

Now $b_1 b_2 = f(a_1) f(a_2) = f(a_1 a_2)$

Since f is homomorphism

$b_1 b_2 = f(a_2 a_1)$ $\because$ A is abelian

$= f(a_2) f(a_1)$ $\because$ f is homomorphism

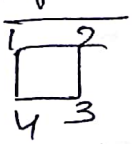
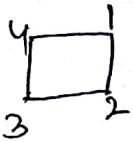
$= b_2 b_1$.

$\therefore$ B is abelian.

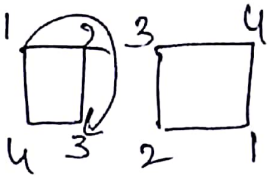
9. S.T set of rigid motions of a square with composition is nonabelian group.

Soln:- Set of all rigid motions of a square (1, 2, 3, 4) is $F = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$. $\circ$ is binary opn on F defined as $(f \circ g)(x) = f(g(x))$.

The Symmetries (rigid motion) of a square

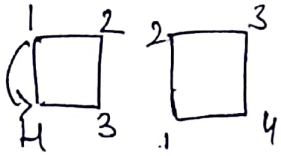
Sl No.	Name	Rigit Motion Before	Rigit Motion After	Perm of Vertices
1.	f_1: identity			$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$
2.	f_2 rotate 90° Clk wise			$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

3 f_3: rotate 180° clk wise



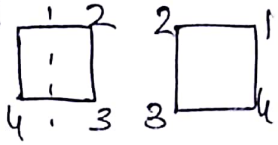
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

4 f_4: rotate 90° counter clk wise



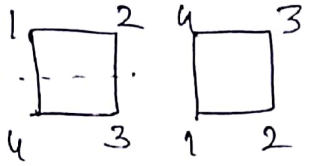
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 4 & 3 \end{pmatrix}$

5 f_5: reflect



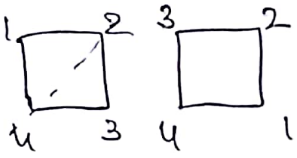
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

6. f_6: reflect



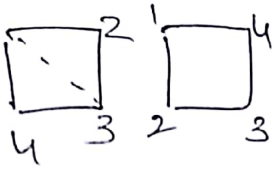
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

7. f_7: reflect



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

8 f_8: reflect



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

Prepare composition table.

Ex: 15.3

1H) In the group S_5, let

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

Determine $\alpha\beta$, $\beta\alpha$, α^3, β^4, α^{-1}, β^{-1}, $(\alpha\beta)^{-1}$, $(\beta\alpha)^{-1}$ & $\beta^4\alpha^{-1}$

Soln:- Do like composition in relation.

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

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

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

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

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

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

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

Homomorphism, Isomorphism & Cyclic groups:-

Defn:- If $(G, \circ)$ and $(H, *)$ are groups and $f: G \to H$, then f is called a group homomorphism if for all $a, b \in G$, $f(a \circ b) = f(a) * f(b)$.

Ex:- $G = (\mathbb{Z}, +)$ $H = (\mathbb{Z}_4, +)$ $f: G \to H$.

$f(x) = [x] = \{x + 4k \mid k \in \mathbb{Z}\}$.

for all $x, y \in G$,

$f(x+y) = [x+y] = [x] + [y] = f(x) + f(y)$

↑ opn in G ↑ opn in H.

Thm:-5

Let $(G, \circ)$, $(H, *)$ be groups with respective identities e_G, e_H. If $f: G \to H$ is a homomorphism, then

a) $f(e_G) = e_H$.

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

c) $f(a^n) = [f(a)]^n$ $\forall a \in G$ & $\forall n \in Z$.

d) $f(S)$ is a subgroup of H for each subgroup S of G.

Proof:-

a) $e_H * f(e_G) = f(e_G) = f(e_G \circ e_G) = f(e_G) * f(e_G)$

$\therefore f(e_G) = e_H$.

d) If S is a subgroup of G, then $S \neq \phi$. So $f(S) \neq \phi$.

Let $x = f(a)$, $y = f(b)$ for some $a, b \in S$. $\because S$ is a subgroup of G, it follows that $a \circ b \in S$, so

$x * y = f(a) * f(b) = f(a \circ b) \in f(S)$

$x^{-1} = [f(a)]^{-1} = f(a^{-1}) \in f(S)$ $\because a^{-1} \in S$ when $a \in S$.

Consequently $f(S)$ is a subgroup of H

b) In G, $a \circ a^{-1} = e_G$ $\therefore f(a \circ a^{-1}) = f(e_G) = e_H = f(a) * f(a^{-1})$ $\therefore f(a^{-1})$ is inverse of $f(a)$

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

Defn:- If $f: (G, \circ) \to (H, *)$ is a homomorphism, f is one isomorphism if it is one to one & onto. Here G, H are called isomorphic groups.

Ex:- i) $f: (R^+, \cdot) \to (R, +)$, $f(x) = \log_{10}(x)$. This function is both one to one and onto. For all $a, b \in R^+$,

$f(ab) = \log_{10}(ab) = \log_{10} a + \log_{10} b = f(a) + f(b)$. $\therefore$ f is isomorphism & group of +ve real nos under multiplication is abstractly the same as the group of all real nos under addition.

2) Let G be group of complex nos $\{1, -1, i, -i\}$ under multiplication.

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

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

With $H = (Z_4, +)$ $f: G \to H$ defined by

$f(1) = [0]$, $f(-1) = [2]$ $f(i) = [1]$ $f(-i) = [3]$.

Then $f((i)(-i)) = f(1) = [0] = [1] + [3] = f(i) + f(-i)$

$f((-1)(-i)) = f(i) = [1] = [1] + [3] = f(i) + f(-i)$

$f((-1)\cdot(-1)) = f(1) = [0] = [4] = [2] + [2] = f(-1) \cdot f(-1)$

$f((i)\cdot(1)) = f(i) = [1] = [1] + [0] = f(i) + f(1)$.

The image under f of subgroup $\{1, -1\}$ of G is $\{[0], [2]\}$, a subgroup of H.

$i^1 = i$ $i^2 = -1$, $i^3 = -i$, $i^4 = 1$ $\therefore$ Every element of G is a power of i. $\therefore$ i generates G.

This is denoted by $G = \langle i \rangle$.

Defn:- A group G is called cyclic if there is an element $x \in G$ such that for each $a \in G$, $a = x^n$ for some $n \in Z$.

Ex:-1) $H = (Z_4, +)$ is cyclic group. $[1]$ and $[3]$ are generators of H. Ex:- $1 \cdot [3] = [3]$, $2 \cdot [3] = [2]$, $3 \cdot [3] = [1]$ & $4 \cdot [3] = [0]$. $\therefore H = \langle [3] \rangle = \langle [1] \rangle$.

$[3+3]$ $[3+3+3]$

2) Multiplicative group $U_9 = \{1,2,4,5,7,8\}$.

$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 7$, $2^5 = 5$, $2^6 = 1$.

$\therefore U_9$ is a cyclic group of order 6. $\{U_9\} = \langle 2 \rangle$.

Also $U_9 = \langle 5 \rangle$ $\because$ $5^1 = 5$, $5^2 = 7$, $5^3 = 8$, $5^4 = 4$, $5^5 = 2$, $5^6 = 1$.

Given group G. if $a \in G$. $S = \{a^k \mid k \in \mathbb{Z}\}$.
Then S is a subgroup of G. This subgroup is called subgroup generated by a, denoted by $\langle a \rangle$.

$U_9 = \langle 2 \rangle$ $(= \langle [2] \rangle) = \langle 5 \rangle$, $\langle 4 \rangle = \{1, 4, 7\}$, $\langle 8 \rangle = \{1, 8\}$ &
$\langle 1 \rangle = \{1\}$.

Defn:- If G is a group & $a \in G$, the order of a, denoted $O(a)$ is $|\langle a \rangle|$.

$O(2) = 6$ $O(4) = 3$ $O(8) = 2$, $O(i) = O(-i) = 4$.

If $|\langle a \rangle|$ is finite. $|\langle a \rangle| = 1$ then $a = e$ because $a = a^1 \in \langle a \rangle$ & $e = a^0 \in \langle a \rangle$. If $|\langle a \rangle|$ is finite but $a \neq e$ then $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$ is finite, so $\{a, a^2, a^3, \ldots\} = \{a^m \mid m \in \mathbb{Z}^+\}$ is also finite. Consequently, $\exists\, s, t \in \mathbb{Z}^+$, $1 \leq s < t$ & $a^s = a^t \Rightarrow a^{t-s} = e$, $t - s \in \mathbb{Z}^+$ $\because e \in \{a^m \mid m \in \mathbb{Z}^+\}$, let n be smallest +ve integer such that $a^n = e$. we claim that $\langle a \rangle = \{a, a^2, a^3 \ldots a^{n-1}, a^n (= e)\}$.

$|\{a, a^2, a^3 \ldots a^n\}| = n$. Otherwise, we have $a^u = a^v$ for +ve integers u, v where $1 \leq u < v \leq n$, & $a^{v-u} = e$ with $0 < v - u < n$. But this contradicts

the minimality of n. WKT $|\langle a\rangle| \geq n$. But for each $k \in \mathbb{Z}$, from division alg $k = qn+r$, $0 \leq r < n$.

So $a^k = a^{qn+r} = (a^n)^q \cdot a^r = e^q a^r = a^r \in \{a, a^2, \ldots a^n\}$

$\therefore \langle a\rangle = \{a, a^2, \ldots a^r (= e)\}$.

Also we can define $O(a)$ as smallest +ve integer n for which $a^n = e$.

Thm:-

Let $a \in G$ with $O(a) = n$. If $k \in \mathbb{Z}$, $a^k = e$ then $n \mid k$.

Proof:- $k = qn+r$, $0 \leq r < n \Rightarrow e = a^k = a^{qn+r} = (a^n)^q \cdot a^r$

$= e^q \cdot a^r = a^r$. If $0 < r < n$, we contradict the definition of n as $O(a)$. $\therefore r = 0$ & $k = qn$.

Ex:- $U_9 = \{1, 2, 4, 5, 7, 8\} = \langle 2\rangle$

define fun $f: U_9 \to (Z_6, +)$

$f(1) = [0]$ $f(2) = [1]$ $f(4) = [2]$

$f(5) = f(2^5) = [5]$ $f(7) = f(2^4) = [4]$ $f(8) = f(2^3) = [3]$.

In general, for each $a \in U_9$, we write $a = 2^k$, for some $0 \leq k \leq 5$ & we have $f(a) = f(2^k) = [k]$.

This is onto & one to one.

$\therefore f(2 \cdot 5) = f(1) = [0] = [1] + [5] = f(2) + f(5)$.

& $f(7 \cdot 8) = f(2) = [1] = [4] + [3] = f(7) + f(8)$

In general, for a, b in U_9 we write $a = 2^m$, $b = 2^n$

$0 \leq m \leq 5$, $0 \leq n \leq 5$.

$f(a \cdot b) = f(2^m \cdot 2^n) = f(2^{m+n}) = [m+n] = [m] + [n] = f(a) + f$

Consequently, f is an isomorphism & groups U_9 & $(Z_6, +)$ are isomorphic.

$g: U_9 \to (Z_6, +)$

$g(1) = [0]$ $\quad g(5) = [1]$ $\quad g(7) = g(5^2) = [2]$

$g(8) = g(5^3) = [3]$ $\quad g(4) = g(5^4) = [4]$ $\quad g(2) = g(5^5) = [5]$.

Thm:-1

Let G be a cyclic group.

a) if $|G|$ is infinite, then G is isomorphic to $(Z, +)$,

b) if $|G| = n$, where $n > 1$, then G is isomorphic to $(Z_n, +)$

Proof:-

a) for $G = \langle a \rangle = \{a^k \mid k \in Z\}$ let $f: G \to Z$ be defined by $f(a^k) = k$. For $a^m, a^n \in G$, $f(a^m \cdot a^n) = a^{m+n} = m+n$

$f(a^m) + f(a^n)$, so f is a homomorphism.

b) If $G = \langle a \rangle = \{a, a^2, \ldots a^n = e\}$, then function $f: G \to Z_n$ defined by $f(a^k) = [k]$ is an isomorphism.

Ex:- If $G = \langle g \rangle$, G is an abelian because $g^m \cdot g^n = g^{m+n} = g^{n+m} = g^n \cdot g^m$, $\forall m, n \in Z$. The converse is false.

Group H is abelian & $O(e) = 1$ $\quad O(a) = O(b) = O(c) = 2$.

∴ No element of H has order 4, H cannot be cyclic.

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Ex: 16.1 State Group or not.

1. a) $\{-1, 1\}$ under multiplication.

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

a) closure ✓
b) associative ✓
c) 1 is identity ✓
d) $-1^{-1} = -1$ $1^{-1} = 1$. ✓

b) $\{-1, 1\}$ under addition

$+$	-1	1
-1	-2	0
1	0	2

a) closure ✗.

c) $\{-1 \quad 0 \quad 1\}$ under addition.

$-1 + (-1) = -2 \notin \{-1, 0, 1\}$

∴ Closure is not satisfied.

d) $\{10n \mid n \in Z\}$ under addition.

$a = 10n \qquad b = 10.n$

$a + b = 10n + 10n = (10n)n \cdot (10n).10n = 10(n \cdot 10)n$

$= 20n \in$ Set.

$=$

Closure ✓

$a + (b + c) = 10.n + (10n + 10n) = 10n + 20n = 30n$

$(a + b) + c = (10n + 10n) + 10n = 30n.$

∴ Associative ✓

$a + b = a$ if $b = 10(0) = 0$

0 is identity.

$\forall$ $a = 10n$.

$\exists$ $b = -10n$ is inverse of a.

$\therefore$ Inverse exists.

$\therefore$ It is a group.

3. Why set Z is not a group under subtraction?

Soln:- Since Associative property does not satisfied by Z under subtraction, it is not a group.

4. Let $G = \{q \in Q \mid q \neq 1\}$. Define binary opⁿ $\circ$ on G by $x \circ y = x + y + xy$. P.T. $(G, \circ)$ is an abelian group.

Soln:-

a) $x \in G$, $y \in G$

$x \circ y = x + y + xy \in G$. $\therefore$ closure satisfied.

b) $x \circ (y \circ z) = x \circ (y + z + yz)$

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

$= x + y + z + yz + xy + xz + xyz$

$= (x + y + xy) + z + xz + yz + xyz$

$= (x \circ y) + z + (x + y + xy)z$

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

$[a + b + a.b]$

$= (x \circ y) \circ z$.

$\therefore$ Associativity is satisfied.

c) 0 is identity.

$\because \quad x \circ 0 = 0 \circ x = x$

ie $x \circ 0 = x$.

d) To find inverse

$x \circ y = 0$.

ie $x + y + xy = 0$.

$x + y(1+x) = 0$.

$y = -\frac{x}{1-x} \in \mathbb{Q}$, is the inverse of x.

e) $\because \quad x \circ y = x + y + xy = y + x + yx$

$= y \circ x$.

$\therefore$ Commutative property is satisfied.

$\therefore (G, \circ)$ is an abelian group.

5) Define binary op^n $\circ$ on $\mathbb{Z}$ by $x \circ y = x + y + 1$. Verify that $(\mathbb{Z}, \circ)$ is an abelian group.

Soln:

a) $x, y \in \mathbb{Z}$, $x \circ y = x + y + 1 \in \mathbb{Z}$.

$\therefore \circ$ is closed under $\mathbb{Z}$.

b) $(x \circ y) \circ z = (x + y + 1) + z + 1$

$= x + (y + z + 1) + 1$

$= x + (y \circ z) + 1$

$= x \circ (y \circ z)$

$\therefore$ Associative property holds.

c) To find identity

$x \circ e = x$.

$x + e + 1 = x$.

$\therefore e = -1$ is identity.

d) To find inverse.

$x \circ y = e = -1$.

ie $x + y + 1 = -1 \Rightarrow y = -2 - x \in \mathbb{Z}$ is inverse of x.

e) Also,

$x \circ y = x + y + 1$

$= y + x + 1 = y \circ x$.

$\therefore$ Commutative property holds.

$\therefore (\mathbb{Z}, \circ)$ is an abelian group.

6. Let $S = R^* \times R$. Define the binary opn $\circ$ on S by $(u,v) \circ (x,y) = (ux, vx+y)$. P.T $(S, \circ)$ is a non abelian group.

Soln:-

a) $(u,v) \circ (x,y) = (ux, vx+y) \in R^* \times R$.

b) $((u,v) \circ (x,y)) \circ (p,q) = (ux, vx+y) \circ (p,q)$

$= (uxp, vxp + yp + q) \rightarrow (1)$

$((u,v) \circ (x,y)) \circ (p,q) = (ux, vx+y) \circ (p,q)$

$= (uxp, vxp + yp + q) \rightarrow (2)$

$(1) = (2)$. $\therefore$ Associative property holds.

c) To find identity.

$(u,v) \circ (x,y) = (u,v)$

ie $(ux, vx+y) = (u,v)$

$\therefore \quad ux = u \Rightarrow x = 1$

$vx + y = v \Rightarrow y = v - vx = 0.$

$\therefore \quad (1,0)$ is the identity.

d) To find inverse.

$(u,v) \circ (x,y) = (1,0)$

ie $(ux, vx+y) = 1,0.$

$ux = 1 \Rightarrow x = \frac{1}{u}.$

$vx + y = 0 \Rightarrow y = -vx = -v \cdot \frac{1}{u} = -\frac{v}{u}.$

$\therefore \left(\frac{1}{u}, -\frac{v}{u}\right)$ is the inverse of (u,v)

$\therefore \quad (S, \circ)$ is a group.

e) $(u,v) \circ (x,y) = (ux, vx+y) \longrightarrow (1)$

$(x,y) \circ (u,v) = (ux, yu+v) \longrightarrow (2)$

From (1) & (2), commutative property does not hold

$\therefore (S, \circ)$ is not an abelian group.

7. Find elements in groups U_{20} and U_{24} - the groups of units for rings $(\mathbb{Z}_{20}, +, \cdot)$ & $(\mathbb{Z}_{24}, +, \cdot)$ resp.

Soln:- $U_{20} = \{a \in \mathbb{Z}^+ \mid 1 \le a \le 19 \text{ and } \gcd(a, 20) = 1\}$.

$= \{1, 3, 7, 9, 11, 13, 17, 19\}$.

$U_{24} = \{a \in \mathbb{Z}^+ \mid 1 \le a \le 23 \text{ and } \gcd(a, 24) = 1\}$

$= \{1, 5, 7, 11, 13, 17, 19, 23\}$.

·	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	13	11	17
7	7	1	9	03	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	13	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

III^ly prepare table for · with U_{24} elements.

9. If G is a group, P.T $\forall a, b \in G$

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

Soln:-

a) W.K.T a^{-1} is the inverse of a & a is the inverse of a^{-1}.

Also we know that inverse is unique.

$\therefore (a^{-1})^{-1}$ is also same as a which is inverse of a^{-1}.

$\therefore$ both $(a^{-1})^{-1}$ and a are same.

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

$= a\cdot(e)a^{-1} = a\cdot a^{-1} = e.$

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

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

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

$\therefore$ $b^{-1}a^{-1}$ is the inverse of (ab).

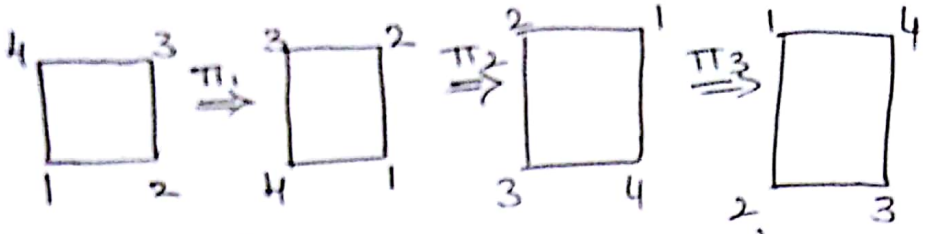
$\therefore$ $(ab)^{-1} = b^{-1}.a^{-1}$.

12) a) How many rigid motions are there for a square?

Soln:- There are 4 rotations & 4 reflections making a total of 8 rigid motions for a square.

b) Make a group table for these rigid motions. What is identity? Describe inverse of each element geometrically.

Soln:-

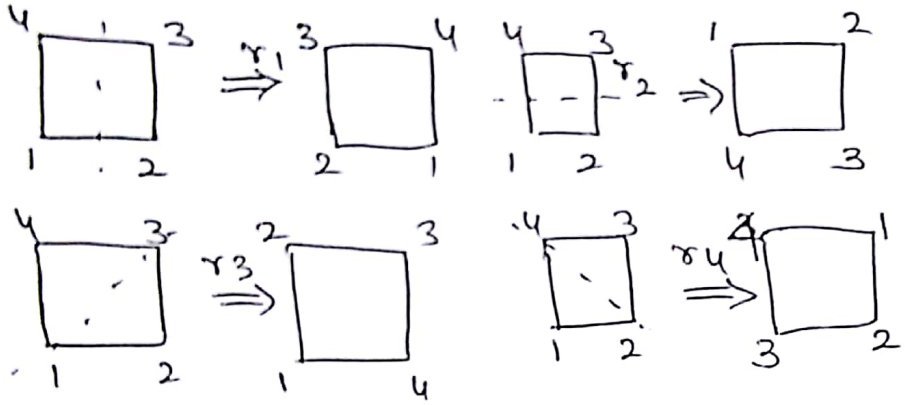


Rotations

$$\pi_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \qquad \pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

Reflections



$$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \qquad r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \qquad r_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\pi_1 \cdot r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \pi_1 .$$

$$\pi_1 \cdot \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \pi_2$$

$$\pi_1 \cdot \pi_2 = \pi_3 .$$

$$\pi_1 \cdot \pi_3 = \pi_0 . \qquad \pi_3 \cdot \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \pi_0$$

$$\pi_2 \cdot \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \pi_3 \qquad \pi_3 \cdot \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \pi_1$$

$$\pi_2 \, \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 4 \end{pmatrix} = \pi_0 . \qquad \pi_3 \cdot \pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \pi_2$$

$$\pi_2 \, \pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \pi_1$$

$r_1 \cdot \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = r_4$, $r_1 \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} =$

$r_1 \cdot \pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = r_3$ $\quad r_1 \cdot r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \pi_0$

$r_1 \cdot r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \pi_2$ $\quad r_1 \cdot r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \pi$

$r_1 r_4 =$

$r_2 \cdot \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = r_3$ $\quad r_2 \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = r_1$

$r_2 \cdot \pi_3 = r_4$ $\quad r_3 \cdot \pi_1 = r_1$ $\quad r_3 \pi_2 = r_4$ $\quad r_3 \cdot \pi_3 = r_2$

$r_3 \cdot r_1 = \pi_1$ $\quad r_3 \cdot r_2 = \pi_3$ $\quad r_3 \cdot r_3 = \pi_0$. $\quad r_3 r_4 = \pi_2$

$r_4 \cdot \pi_1 = r_2$ $\quad r_4 \cdot \pi_2 = r_3$ $\quad r_4 \cdot \pi_3 = r_1$ $\quad r_4 \cdot r_1 = \pi_3$

$r_4 \cdot r_2 = \pi_1$. $\quad r_4 \cdot r_3 = \pi_2$ $\quad r_4 \cdot r_4 = \pi_0$

·	π_0	π_1	π_2	π_3	r_1	r_2	r_3	r_4
π_0	π_0	π_1	π_2	π_3	r_1	r_2	r_3	r_4
π_1	π_1	π_2	π_3	π_0	r_3	r_4	r_2	r_1
π_2	π_2	π_3	π_0	π_1	r_2	r_1	r_4	r_3
π_3	π_3	π_0	π_1	π_2	r_4	r_3	r_1	r_2
r_1	r_1	r_4	r_2	r_3	π_0	π_2	π_3	π_1
r_2	r_2	r_3	r_1	r_4	π_2	π_0	π_1	π_2.
r_3	r_3	r_1	r_4	r_2	π_1	π_3	π_0	π_2
r_4	r_4	r_2	r_3	r_1	π_3	π_1	π_2	π_0.

π_0 is the identity. $\quad \pi_0^{-1} = \pi_0$, $\pi_1^{-1} = \pi_3$, $\pi_2^{-1} = \pi_2$, $\pi_3^{-1} = \pi_1$.

$r_1^{-1} = r_1$, $r_2^{-1} = r_2$, $r_3^{-1} = r_3$, $r_4^{-1} = r_4$.

13. a) No of rigid motions of a pentagon = 5 rotations, 5 reflections. = 10

b) No of rigid motions for a regular poly & n-gon, $n \geq 3$

$= 2 \cdot n$

n-rotations & n reflections.

14) In S_5, let

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

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

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

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

d) $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$ $\quad$ g) $(\beta\alpha)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix}$

e) $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$ $\quad$ h) $= \beta^{-1}\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$

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

Pg 708

19) a) Find all x in $(Z_5^*, \cdot)$ such that $x = x^{-1}$

Soln $Z_5^* = \{1, 2, 3, 4\}$

$1 \cdot 1 = 1$, $2 \cdot 2 = 4$ $3 \cdot 3 = 4$ $4 \cdot 4 = 1$

$\therefore$ 1, 4 are inverses of themselves.

b) Find all x in $(Z_{11}^*, \cdot)$ such that $x = x^{-1}$

$Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$1 \cdot 1 = 1$ $2 \cdot 2 = 4$ $3 \cdot 3 = 9$ $4 \cdot 4 = 5$ $5 \cdot 5 = 3$

$6 \cdot 6 = 3$ $7 \cdot 7 = 5$ $8 \cdot 8 = 9$ $9 \cdot 9 = 4$ $10 \cdot 10 = 1$

$\therefore$ 1 & 10 are inverses of themselves.

c) Let p be a prime. Find all x in $(Z_p^*, \cdot)$ such that $x = x^{-1}$.

Soln:- $x = x^{-1}$

$\therefore$ x by x on both sides,

$x^2 \equiv 1 \bmod p$.

ie $x^2 - 1 \equiv 0 \bmod p$

$\Rightarrow (x+1)(x-1) \equiv 0 \bmod p$.

$\Rightarrow x + 1 = 0$ or $x - 1 = 0$

$\Rightarrow x = -1 \bmod p = p - 1$ $x = 1 \bmod p = 1$.

$\therefore$ $x = \{1, p-1\}$.

d) P.T $(p-1)! \equiv -1 \bmod p$, p is prime.

Soln:

Result is true for $p=2$

$\because (2-1)! = 1 \equiv -1 \bmod 2$.

For $p \geq 3$,

Consider elements $1, 2, 3 \ldots\ldots (p-1)$ in $(\mathbb{Z}_p^*, \cdot)$

Then elements $2, 3, \ldots\ldots (p-2)$ will have

$\frac{p-3}{2}$ pairs of elements of form (x, x^{-1}).

Ex:- when $p=11$, we find $2,3,4 \ldots 9$ yield

4 pairs of $(2,6)$, $(3,4)$, $(9,5)$, $(7,8)$

$\because$ 6 is inverse 2, 4 is inverse of 3, 5 is inverse of 9, 8 is inverse of 7 in mod 11.

$\therefore (p-1)! \equiv (1) \cdot \underbrace{(1)^{\frac{p-3}{2}}}_{1 \cdot \{2 \cdot 3 \cdots p-2\}} \cdot (p-1) \equiv p-1 \equiv -1 \bmod p.$

Qn:- In $(\mathbb{Z}_p^*, \cdot)$ how many have $x = x^{-1}$ & how many have x^{-1} different from x.

Soln:- There are two numbers $\{1, p-1\}$ which have $x = x^{-1}$.

There are $\left(\frac{p-3}{2}\right)$ which have different inverses.

Ex:- In $(Z_{13}^*, \cdot)$, $Z_{13}^* = \{1,2,3,4,5,6,7,8,9,10,11,12\}$

1, 12 have their own inverses of form $x = x^{-1}$

(5,8)

$2^{-1} = 7$ ∴ $(2,7), (3,9), (4,10), (6,11)$ are of form

$3^{-1} = 9$ (x, x^{-1}).

$4^{-1} = 10$ ∴ There are 10 nos which have

$5^{-1} = 8$ diff inverses

$6^{-1} = 11$

$7^{-1} = 2$

$8^{-1} = 5$

$9^{-1} = 3$

$10^{-1} = 4$

$11^{-1} = 6$

~~$12^{-1} = 12$~~

20) Find x in $(U_8, \cdot)$ where $x \neq 1$, $x \neq 7$ but $x = x^{-1}$

Soln:- a) $U_8 = \{a \in Z_8^* \mid 1 \le a \le 7 \text{ \& } \gcd(a,8) = 1\}$

$= \{1, 3, 5, 7\}$

~~$1 \cdot 1 = 1$~~

$3 \cdot 3 = 9 \bmod 8 = 1$

$5 \cdot 5 = 25 \bmod 8 = 1$

~~$7 \cdot 7 = 49 \bmod 8 = 1$~~

∴ Ans is $\{3, 5\}$

b) Find x in U_{16} where $x \neq 1$, $x \neq 15$ but $x = x^{-1}$

$U_{16} = \{1, 3, 5, 7, 9, 11, 13, 15\}$

$5 \cdot 5 = 25 \bmod 16 = 9$

$7 \cdot 7 = 49 \bmod 16 = 1$

$9 \cdot 9 = 81 \bmod 16 = 1$

$11 \cdot 11 = 9$

$13 \cdot 13 = 9$

∴ Ans = $\{7, 9\}$

c) Let $k \in 2^+$, $k \geq 3$. Find x in $(V_{2^k}, \cdot)$ where $x \neq 1$, $x \neq 2^k - 1$ but $x = x^{-1}$.

Soln:- $x = \{ 2^{k-1} - 1 , 2^{k-1} + 1 \}$.

Cosets & Lagrange's Theorem

Defn: If H is a subgroup of G, then for each $a \in G$, the set $aH = \{ah \mid h \in H\}$ is called a left coset of H in G. The set $Ha = \{ha \mid h \in H\}$ is called a right coset of H in G.

If operation in G is addition, then $a+H$ is written in place of aH, where $a+H = \{a+h \mid h \in H\}$.

Ex:- Suppose G is group of motions of equilateral Δ^{le} and $H = \{\pi_0, \pi_1, \pi_2\}$, the coset $r_1 H =$
$\{r_1\pi_0, r_1\pi_1, r_1\pi_2\} = \{r_1, r_2, r_3\}$.
Similarly $r_3 H = r_2 H = \{r_1, r_2, r_3\}$.
$\pi_0 H = \pi_1 H = \pi_2 H = H$.

$|aH| = |H|$ for each $a \in G$ & that $G = H \cup r_1 H$ is a partition of G.
For the subgroup $K = \{\pi_0, r_1\}$, $r_2 K = \{r_2, \pi_2\}$
$r_3 K = \{r_3, \pi_1\}$. $\therefore$ partition of $G = K \cup r_2 K \cup r_3 K$.

Lemma: If H is a subgroup of finite group G, then for all $a, b \in G$ (a) $|aH| = |H|$;
(b) either $aH = bH$ or $aH \cap bH = \phi$.

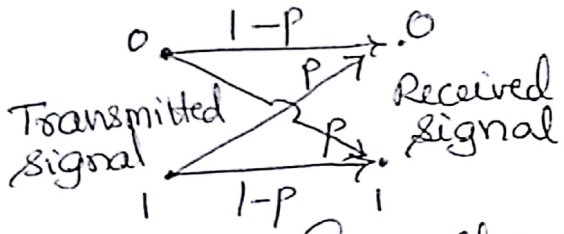
Lagrange's Theorem:-

If G is a finite group of order n with H a subgroup of order m then m divides n.

Elements of Coding Theory

In digital communications, when information is transmitted in the form of strings of 0's & 1's, certain problems arise. As a result of "noise" in the channel, when a certain signal is transmitted a different signal may be received, thus causing the receiver to make a wrong decision. So techniques are developed to detect and even to correct transmission errors. But we can only improve the chances of correct transmission.

The model uses binary symmetric channel.



Binary Symm Channel

Binary - individual signal is represented by one of bits 0 or 1.

When a transmitter sends the signal 0 or 1 in such a channel, associated with either signal is a probability p for incorrect transmission. When the probability is the same for both signals, the channel is called symmetric.

If p is probability of incorrect transmission, then probability of correct transmission is 1-p.

Ex:- Consider string $c = 10110$. c is an element of group Z_2^5, obtained from the direct product

of five copies of $(Z_2, +)$. When sending each bit of c through binary symmetric channel, we assume that probability of incorrect transmission is $p = 0.05$, so that probability of transmitting c with no errors is $(0.95)^5 = 0.77$.

Here assumption is made that the transmission of each signal does not depend on transmission of prior signals. Consequently, the probability of occurrence of all of these independent events is given by product of their individual probabilities

If $c = 10110$, $r = 00110$ then what is probability of sending c and receiving r?

$$p = (0.05) \cdot (0.95)^4 = 0.041.$$

With $e = 10000$, we can write $c + e = r$ ie r is the result of sum of original message c and the particular error pattern $e = 10000$.

$\because c, r, e \in Z_2^5$ and $-1 = 1$ in Z_2, $c + r = e$ & $r + e = c$

In transmitting $c = 10110$, the probability of receiving $r = 00100$ is $(0.05)^2 (0.95)^3 = 0.002$.

($(0.05)^2$: prob. of incorrect bits tran; $(0.95)^3$: prob. of correct bits trans.)

If we transmit $c = 10110$, what is the probabilit that r differs from c in exactly two places?
Here we sum probabilities for each error pattern

consisting of two 1's and three 0's. Each such pattern has probability of 0.002. There are $\binom{5}{2}$ such patterns. So the probability of two errors in transmission is given by

$$\binom{5}{2}(0.05)^2(0.95)^3 = 0.021.$$

Thm 10:-

Let $c \in Z_2^n$. For transmission of c through a binary symmetric channel with probability p of incorrect transmission,

a) The probability of receiving $r = c + e$, where e is a particular error pattern consisting of k 1's and (n-k) 0's is $p^k \cdot (1-p)^{n-k}$.

b) the probability that k errors are made in the transmission is $\binom{n}{k} p^k \cdot (1-p)^{n-k}$.

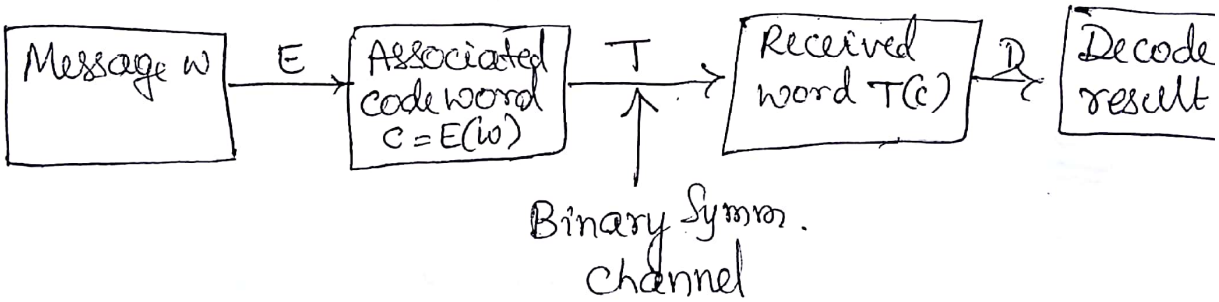
Proof:

Probability of making at most one error in the transmission of $c = 10110$ is sum of probability of making no errors and probability of making one error $= (0.95)^5 + \binom{5}{1}(0.05)(0.95)^4$
$= 0.977$.

A binary symmetric channel is considered good when $p < 10^{-5}$. Always we need $p < \frac{1}{2}$.

To improve accuracy of transmission in a binary symmetric channel, certain types of coding schemes can be used where extra signals are provided.

For $m, n \in Z^+$, let $n > m$. Consider $\phi \neq W \subseteq Z_2^m$.
Set W consists of messages to be transmitted. To each $w \in W$ are appended $n-m$ extra signals to form the code word, where $c \in Z_2^n$. This process is called encoding and is represented by the function $E: W \to Z_2^n$. Then $E(w) = C$ and $E(W) = C' \subseteq Z_2^n$. Since function E simply appends extra bits to (distinct) messages, the encoding process is one-to-one. Upon transmission, c is received as $T(c)$, where $T(c) \in Z_2^n$. But T is not a function because $T(c)$ may be different at different transmission times.



Upon receiving $T(c)$, we want to apply a decoding function $D: Z_2^n \to Z_2^m$ to remove extra signals and we hope obtain the original message w. Ideally $D \circ T \circ E$ should be the identity function on W, with $D: C \to W$. Since this cannot be expected, we use E & D such that there is a high probability of correctly decoding the received word $T(c)$ & recapturing the original message w. Also

we want the ratio $\frac{m}{n}$ to be as large as possible so that an excessive number of signals are not appended to w in getting the code word $c = E(w)$. The ratio measures the efficiency and is called the rate of the code. Also E and D should be electronically implemented Here E and D are called Encoding and Decoding funs of an (n, m) block code.

Ex:- Consider $(m+1, m)$ block code for $m = 8$. Let $W = Z_2^8$. For each $w = w_1 w_2 \ldots w_8 \in W$, define $E: Z_2^8 \to Z_2^9$ by $E(w) = w_1 w_2 \ldots w_8 w_9$, where $w_9 = \sum_{i=1}^{8} w_i$, with the addition performed mod 2.

Ex: $E(11001101) = 110011011$ and
$E(00110011) = 001100110$. [Even parity]

For all $w \in Z_2^8$, $E(w)$ contains an even number of 1's. So for $w = 11010110$ and $E(w) = 110101101$, if we receive $T(c) = T(E(w))$ as 100101101, from the odd number of 1's in $T(c)$ we know that a mistake has occurred in transmission. Here we are able to detect single errors in transmission. But we cannot correct such errors.

The probability of sending the code word 110101101 and making at most one error in transmission is $(1-p)^9 + \binom{9}{1} p \cdot (1-p)^8$.
For $p = 0.001$ this gives $(0.999)^9 + (9)(0.001)(0.999)^8$
$= 0.999964$.

Should an even positive number of errors occur in transmission, $T(c)$ is accepted as correct code word and is interpreted as original message. This scheme is called $(m+1, m)$ parity check code & is appropriate when multiple errors are not likely to occur.

If we send message 11010110 through channel, we have probability $(0.999)^8 = 0.992028$ of correct transmission. By using parity check code, we increase our chances of getting the correct message to 0.999964. Here an extra signal is sent & rate of code has decreased from 1 to 8/9.

Suppose 160 bits are sent, in successive strings of length 8. The chances of receiving correct message without any coding scheme would be $(0.999)^{160} = 0.852076$. With parity check method, we send 180 bits, but chances for correct transmission increases to $(0.999964)^{20}$ $= 0.999280$.

Ex:- The $(3m, m)$-tripple repitition code is one where we can both detect & correct single errors in transmission. With $m=8$ & $W = Z_2^8$, $E: Z_2^8 \to Z_2^{24}$ by $E(w_1 w_2 \ldots w_8) \to$ $w_1 w_2 \ldots w_8 w_1 \ldots w_8 w_1 \ldots w_8$.

So if $W = 10110111$, then $c = E(W) = 101101111011011110110$

The decoding function $D: Z_2^{24} \to Z_2^8$ is carried out by majority rule.

Ex:- T(c) = 101001110011011110110110,

ie
```
101@0011
@0110111
1011011@
--------
r= 101 101 11
   x   x   x
```

then we have three errors occurring in positions 4, 9 and 24. We decode T(c) by examining 1st, 9th, & 17th positions to see which signal appears more times. Here it is 1 (occur twice), So we decode first entry in decoded message as 1. So continuing for remaining positions, the received message is interpreted as 10110111.

Here we have more than one transmission error. But it is ok unless two (or more) errors occur with the second error eight or sixteen spaces after the first - ie if two incorrect transmissions occur for the same bit of original msg

With $p = 0.001$, probability of correctly decoding a single bit is $(0.999)^3 + \binom{3}{1}(0.001)(0.999)^2 = 0.9999$
So probability of receiving & correctly decoding the eight-bit message is $(0.999997)^8 = 0.999976$, just slightly better than parity check method. Here 24 signals are transmitted, & also rate is $8/24 = 1/3$. For this increased accuracy & the ability to detect & now correct single errors

we have to pay with an increased in transmission time.

Ex 16.4 pg 719

1. C be a set of code words, where $C \subseteq Z_2^7$.

a) $c = 1010110 \quad r = 1011111 \quad \therefore e = c + r = 0001001$

b) $c = 1010110 \quad e = 0101101 \quad \therefore r = c + e = 1111011$

c) $e = 0101111 \quad r = 0000111 \quad \therefore c = e + r = 0101000$

2. A binary symmetric channel has probability $p = 0.05$ of incorrect transmission. If code word $c = 011011101$ is transmitted, what is the probability that a) we receive $r = 011111101$?
b) we receive $r = 111011100$? c) single error occurs?
d) a double error occurs? e) a triple error occurs?
f) 3 errors ocur, no two of them consecutive?

Ans:- a) $e = c + r \quad \therefore e =$

$$\begin{array}{r} 011011101 \\ +\ 011111101 \\ \hline 000100000 \end{array}$$

$\therefore p(r) = (0.05) \cdot (0.95)^8 = 0.03317$

$9C_1 = \frac{9!}{8!} = 9$

$9C_2 = \frac{9!}{7! \cdot 2!} = \frac{9 \times 8}{2} =$

$9C_3 = \frac{9 \times 8 \times 7}{3 \times 2} = 84$

b)

$$\begin{array}{r} e = 011011101 \\ +\ 111011100 \\ \hline 100000001 \end{array}$$

$p(r) = (0.05)^2 \cdot (0.95)^7 = 0.01745$

c) $p(\text{Single error}) = 0.03317 \cdot (9) = 0.29853$

d) $p(\text{double error}) = \binom{9}{2} (0.05)^2 \cdot (0.95)^7 = 0.01745 \cdot \binom{9}{2} = 0.06282.$

e) $p(\text{tripple error}) = (0.05)^3 (0.95)^6 \binom{9}{3} = 0.156369$

f)

3) $E: Z_2^3 \to Z_2^9$ be encoding fun for (9,3) tripple repetition code

a) If $D: Z_2^9 \to Z_2^3$ is decoding fun, apply D to decode received words

i) 111101100

decoded msg =
$$\begin{array}{r} 111 \\ +\,101 \\ +\,100 \\ \hline 101 \end{array}$$

ii) 000100011

decoded msg =
$$\begin{array}{r} 000 \\ 100 \\ 011 \\ \hline 000 \end{array}$$

iii) 010011111

decoded msg =
$$\begin{array}{r} 010 \\ 011 \\ 111 \\ \hline 011 \end{array}$$

b) Find 3 diff received words r for which $D(r) = 000$

$r_1 = 000100011$

$r_2 = 000111000$

$r_3 = 000100000$

c) For each $w \in Z_2^3$, what is $|D^1(w)|$?

$|D^1(w)| = 2^6$ (∵ it is majority rule)

Hamming Metric

Defn:- For each element $x = x_1 x_2 \ldots x_n \in Z_2^n$, where $n \in Z^+$, the weight of x, denoted $wt(x)$ is the no of components x_i of x, for $1 \le i \le n$, where $x_i = 1$. If $y \in Z_2^n$, the distance b/n x & y, denoted $d(x,y)$, is the no of components where $x_i \neq y_i$, for $1 \le i \le n$.

Ex:- For $n=5$, $x = 01001$ $y = 11101$.

$wt(x) = 2$ $wt(y) = 4$ $d(x,y) = 2$.

$x+y = 10100$. So $wt(x+y) = 2$.

$d(x,y) = wt(x+y)$.

For each $1 \le i \le 5$, $x_i + y_i$ contributes a count of 1 to $wt(x+y) \iff x_i \neq y_i \iff x_i, y_i$ contribute a count of 1 to $d(x,y)$.

$\therefore \forall n \in Z^+$, $wt(x+y) = d(x,y)$ $\forall x, y \in Z_2^n$.

When $x, y \in Z_2^n$, $d(x,y) = \sum_{i=1}^{n} d(x_i, y_i)$ where

for each $1 \le i \le n$, $d(x_i, y_i) = \begin{cases} 0 & \text{if } x_i = y_i \\ 1 & \text{if } x_i \neq y_i \end{cases}$.

Lemma:- $\forall x, y \in Z_2^n$, $wt(x+y) \le wt(x) + wt(y)$.

Proof:- for each $1 \le i \le n$, examine $x_i, y_i, x_i + y_i$ of $x, y, x+y$ resp. Only situation which could cause inequality to be false: if $x_i + y_i = 1$ while $x_i = y_i = 0$. But this never occurs because $x_i + y_i = 1 \Rightarrow x_i = 1$ or y

Ex:- $x = 01001 \quad y = 11101$.

$wt(x) = 2 \quad wt(y) = 4 \quad wt(x+y) = 2$

$\therefore \quad 2 \leq 2+4$

Thm 11:-

The distance fun d defined on $Z_2^n \times Z_2^n$ satisfies

$\forall\, x, y, z \in Z_2^n$.

a) $d(x,y) \geq 0$.

b) $d(x,y) = 0 \iff x = y$

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

d) $d(x,z) \leq d(x,y) + d(y,z)$. [Triangle inequality].

Proof:-

a) if $x = y \quad d(x,y) = 0$.

if $x \neq y, \quad d(x,y) > 0$.

$\therefore \quad d(x,y) \geq 0$.

b) $d(x,y) = 0$ ie x and y are same.

d) In Z_2^n, $y + y = 0$

$\therefore \quad d(x,z) = wt(x+z) = wt(x+0+z) = wt(x+y+y+z)$.

$= wt((x+y)+(y+z)) \leq wt(x+y) + wt(y+z)$.

$\leq d(x,y) + d(y,z)$ $\quad \because wt(x+z) = d(x,z)$

$wt(y+z) = d(y,z)$.

c) $d(x,y) = wt(x+y) = wt(y+x) = d(y,x)$.

When a function satisfies 4 properties above, it is called a distance fun or metric & we call $(\mathbb{Z}_2^n, d)$ a metric space. Hence d is called Hamming metric.

Defn:- For $n, k \in \mathbb{Z}^+$ & $x \in \mathbb{Z}_2^n$, the sphere of radius k centered at x is defined as $S(x,k) = \{ y \in \mathbb{Z}_2^n \mid d(x,y) \leq k \}$.

Ex:- $n=3$, $x = 110 \in \mathbb{Z}_2^n$, $S(x,1) = \{110, 111, 100, 010\}$ & $S(x,2) = \{110, 111, 100, 010, 000, 011, 101\}$.

Thm 12:-

Let $E: W \to C$ be an encoding function with set of messages $W \subseteq \mathbb{Z}_2^m$ and set of code words $E(W) = C \subseteq \mathbb{Z}_2^n$, where $m < n$. For $k \in \mathbb{Z}_2^+$, we can detect transmission errors of weight $\leq k$ iff the minimum distance b/n code words is atleast $k+1$.

Proof:- The set C is known to both transmitter & receiver, so if $w \in W$ is the message and $c = E(w)$ is transmitted, let $c \neq T(c) = r$. If the minimum distance b/n code words is atleast $k+1$, then the transmission of c can result in as many as k errors and r will not be listed in C. Hence we can detect all errors e where $wt(e) \leq k$. Conversely, let c_1, c_2 be code words with $d(c_1, c_2) < k+1$. Then

$c_2 = c_1 + e$ where $wt(e) \leq k$ If we send c_1 and $T(c_1) = c_2$, then we would feel that c_2 had been sent, thus failing to detect an error of weight $\leq k$.

Thm 13:-

With $E, W, c^{as\ in\ thm12}$ & $k \in \mathbb{Z}^+$, we can construct a decoding function $D: \mathbb{Z}_2^n \to W$ that corrects all transmission errors of weight $\leq k$ iff min distance b/n code words is atleast $2k+1$.

Proof:- Pg 722.

Ex:-

With $W = \mathbb{Z}_2^2$ let $E: W \to \mathbb{Z}_2^6$ be given by

$E(00) = 000000$ $\quad E(10) = 101010$

$E(01) = 010101$ $\quad E(11) = 111111$.

Then min distance b/n code words is 3, so we can detect double errors and correct single ones.

With

$$S(000000,1) = \{x \in \mathbb{Z}_2^6 \mid d(000000, x) \leq 1\}$$

$$= \{000000, 100000, 010000, 001000, 000100, 000010, 000001\},$$

the decoding fun $D: \mathbb{Z}_2^6 \to \mathbb{Z}_2^2$ gives $D(x) = 00$ for all $x \in S(000000,1)$.

III^{ly} $S(010101,1) = \{x \in \mathbb{Z}_2^6 \mid d(010101, x) \leq 1\}$

$= \{010101, 110101, 000101, 011101, 010001, 010111, 010100\}$

and here $D(x) = 01$ for each $x \in S(010101, 1)$. Continuing to define D for another 14 elements in $S(101010)$ and $S(111111, 1)$, there remain 36 other elements. We define $D(x) = 00$ for these 36 other elements & have a decoding function that will correct single errors.

With regard to detection if $c = 010101$ & $T(c) = r = 111101$, we can detect this double error because r is not a code word. But if $T(c) = r_1 = 111111$, a triple error has occurred, so we think that $c = 111111$ & incorrectly decode r_1 as 11, instead of correct message 01.

Parity check & Generator Matrices

Here encoding & decoding funs are given by matrices over Z_2. One of matrices will help to locate the nearest code word for a given received word. This will be especially helpful when set C of code words is larger.

Ex:- Let $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$

be a 3×6 matrix over Z_2. First 3 columns of G form identity matrix of 3×3 ie I_3.

Let A denote matrix formed by last 3 columns of G. We write $G = [I_3 | A]$ to denote its structure. The partitioned matrix G is called a generator matrix.

We use G to define an encoding function $E: Z_2^3 \to Z_2^6$ as follows: for $w \in Z_2^3$, $E(w) = wG$ is the element in Z_2^6 obtained by multiplying w, considered as a three dimensional row vector, by matrix G on its right. In calculation we have $1+1=0$ not $1+1=1$

Ex:-

$$E(110) = (110)G = [110]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [110101]$$

$$\& \quad E(010) = (010)G = [010]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [010001]$$

Note that E(110) can be obtained by adding first two rows of G, where as E(010) is second row itself.

The set of code words obtained by this method is

$C = \{000000, 100110, 010011, 001101, 110101,$
$011110, 101011, 111000\} \subseteq Z_2^6$.

and one can obtain corresponding message by simply dropping the last 3 components of code word

In addition, the minimum distance b/n code words is 3, so we can detect errors of wt ≤ 2 & correct single errors.

For all $w = w_1 w_2 w_3 \in Z_2^3$, $E(w) = w_1 w_2 w_3 w_4 w_5 w_6 \in Z_2^6$.

Since
$$E(w) = [w_1\ w_2\ w_3] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$
$$= [w_1 w_2 w_3 (w_1+w_3)(w_1+w_2)(w_2+w_3)],$$
we have $w_4 = w_1+w_5$ $\quad w_5 = w_1+w_2$ $\quad w_6 = w_2+w_3$.
and these equations are called parity check equations. Since $w_i \in Z_2$ for each $1 \leq i \leq 6$, it follows that $w_i = -w_i$ and so the equations can be rewritten as

$$\begin{aligned} w_1 \quad\quad + w_3 + w_4 \quad\quad\quad &= 0 \\ w_1 + w_2 \quad\quad\quad + w_5 \quad &= 0 \\ w_2 + w_3 \quad\quad\quad + w_6 &= 0 \end{aligned}$$

Thus we find that
$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_5 \\ w_6 \end{bmatrix} = H \cdot (E(w))^{tr} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$
where $E(w)^{tr}$ denotes transpose of $E(w)$.
Consequently, if $r = r_1 r_2 \cdots r_6 \in Z_2^6$, we can

identify r as a code word iff $H \cdot r^{tr} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

Writing $H = [B | I_3]$, we notice $B = A^{tr}$.

Here min distance b/n code words is 3, we should be able to correct single errors.

Suppose we receive $r = 110110$. We want to find code word c that is the nearest neighbour of r. If there is a long list of code words against which to check r, we first examine $H \cdot r^{tr}$, which is called <u>syndrome of r</u>. Here

$$H \cdot r^{tr} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix},$$

so r is not a code word. Hence we at least detect an error. Looking at the list of code words, we see that $d(100110, r) = 1$. For all other $c \in G$, $d(r, c) \geq 2$. Writing $r = c + e = 100110 + 01000$ we find that the transmission error (of wt 1) occurs in second component of r.

Here we are primarily concerned with transmission where multiple errors are rare.

$r = c + e$, e - error pattern of wt 1. Suppose 1 is in ith component of e, $1 \leq i \leq 6$, then $H \cdot r^{tr} = H(c+e)^{tr} = H(c^{tr} + e^{tr})$
$= H \cdot c^{tr} + H \cdot e^{tr}$. $H \cdot c^{tr} = 0$ so $H \cdot r^{tr} = H \cdot e^{tr} = i^{th}$ col of $H \Rightarrow$

Suppose that we receive $r = 000111$. Computing Syndrome

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

→ Thus c and r differ only in ith component & c is determined by simply changing 7th component of r. So for above received msg, correct msg = 100110.

Here result is not one of columns of H. Yet $H \cdot r^{tr}$ can be obtained as sum of two columns of H. If $H \cdot r^{tr}$ came from 1st & 6th columns of H, correcting these components in r results in code word 100110. If we sum 3rd & 5th components of H to get this syndrome, upon changing 3rd & 5th components of r we get a second code word, 001101. So we cannot expect H to correct multiple errors. This is because min distance b/n code words is 3.

In general, for $m, n \in Z^+$, with $m<n$, the encoding function $E: Z_2^m \to Z_2^n$ is given by an $m \times n$ matrix G over Z_2. This matrix G is called the generator matrix for the code & has the form $[I_A | A]$, where A is an $m \times (n-m)$ matrix. Here $E(w) = w \cdot G$ for each message $w \in Z_2^m$ & code $C = E(Z_2^m) \subset Z_2^n$.

The associated parity check matrix H is an $(n-m) \times m$ matrix of form $[A^{tr} | I_{n-m}]$. This matrix is used to define encoding function E, because if $w = w_1 w_2 \ldots w_m \in Z_2^m$, then $E(w) = w_1 w_2 \ldots w_m w_{m+1} \ldots w_n$ where $w_{m+1} \ldots w_n$ can be determined from the set of $n-m$ (parity check) equations that arise from H. $H(E(w))^{tr} = 0$, the column vector of $n-m$ 0's.

This unique parity check matrix H also provid a decoding scheme that corrects single errors in transmission if

a) H does not contain a column of 0's.

b) No two columns of H are same.

When H satisfies these two conditions, we get decoding alg as below. For each $r \in Z_2^n$, if $T(c) = r$ then

i) With $H \cdot r^{tr} = 0$, here transmission is correct & r is code word that was transmitted. Decoded msg consists of first m components of r.

2) With $H \cdot r^{tr}$ equal to i^{th} col of H, there has been a single error in transmission & change i^{th} component of r in order to get code word c. Here first m components of c yield original msg.

3) If neither case 1 nor case 2 occurs, then there has been more than one transmission error has occurred & we can't provide a reliable way to decode.

If we start with a parity check matrix $H = [B \mid I_{n-m}]$ & use it to define E, then we obtain same set of code words that is generated by the unique generator matrix $G = [I_m \mid B^{tr}]$.

Ex:-

1. $W = Z_2^2$ $E: W \to Z_2^6$

$E(00) = 000000$ $E(01) = 010101$ $E(10) = 101010$ $E(11) = 111111$

$S(101010, 1) = \{ x \in Z_2^6 \mid d(101010, x) \leq 1 \}$

$= \{ 101010, 001010, 111010, 100010, 101110, 101000, 101011 \}$.

$S(111111, 1) = \{ x \in Z_2^6 \mid d(111111, x) \leq 1 \}$

$= \{ 111111, 011111, 101111, 110111, 111011, 111101, 111110 \}$.

2) Decode

a) 110101

```
 11
 01
 01
----
 01
```

b) 101011

```
 10
 10
 11
----
 10
```

c) 001111

```
 00
 11
 11
----
 11
```

d) 110000

```
 11
 00
 00
----
 11
```

3) a) If $x \in Z_2^{10}$ determine

$|S(x,1)| = 10+1 = 11$. $= \binom{10}{1} + 1 = 11$

$|S(x,2)| = \binom{10}{1} + \binom{10}{2} + 1 = 10+45+1 = 56$

$|S(x,3)| = \binom{10}{1} + \binom{10}{2} + \binom{10}{3} + 1 = 56+120 = 176$

$\binom{10}{2} = \frac{10!}{8!\cdot 2!} = \frac{10\times 9}{2} = 45$

$\binom{10}{3} = \frac{10\times 9\times 8}{3\times 2} = 120$

4. $E: Z_2^5 \to Z_2^{25}$ be encoding fun where min distance b/n code words is 9. What is largest value of k such that we can detect errors of wt $\le k$?

Soln: Here It can detect $9 = 8+1$ errors of wt ≤ 8.

If we wish to correct errors of wt $\le k$, what is max value of n?

Soln: $q = 2k+1$. $n = 4$. $\therefore k < 6$

6.a) With $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$ decode

i) 111101.

$$H \cdot r^{tr} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = h_3 .$$

By flipping 3rd bit of received msg.

∴ Decoded msg = 110.

ii) 110101

$$H \cdot r^{t} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

∴ Decoded msg = 110.

iii) 001111

$$H \cdot r^{tr} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = h_5$$

∴ Decoded msg = 001.