SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

RAMAPURAM PART- VADAPALANI CAMPUS, CHENNAI – 600 026

Department of Mathematics

Sub Title: DISCRETE MATHEMATICS FOR ENGINEERS

Sub Code: 18MAB 302 T

Unit -III - ALGEBRAIC SYSTEMS -GROUPS

1. $*: A \times A \to A$ is said to be a binary operation if

   a) $a*b \in A$ *for some* $a \in A$ b) $a*b \in A$ *for some* $b \in A$

   c). $a*b \in A$ *for some* $a,b \in A$ d) $a*b \in A$ *for all* $a,b \in A$ **Ans : d**

2. ______ is not a binary operation on the set of natural numbers.

   a) + b) - c) x d) $+_n$ **Ans: b**

3. ______ is not a binary operation on the set of natural numbers.

   a) + b) - c) x d) $\div$ **Ans d**

4. If $a*(b*c) = (a*b)*c \ , \forall a,b,c \in S$ then $*$ is said to be ---------- in S.

   a) Closed b) Commutative c) Associative d) Distributive **Ans c**

5. (S,*) is said to be a semi group if

   a) * is Closed b) * is Associative c) * is both closed and Associative d) it has identity element **Ans: c**

6. The semi-group (S,*) is said to be a monoid if S has

   a) Identity b) inverse c) satisfies commutative law d) satisfies distributive law **Ans a**

7. Let * be a binary operation on S defined by a*b = a+b+2ab then the identity element w.r.to * is

   a) 0 b) 1 c) 2 d) 3 **Ans a**

8. Let $G = Q^+ \text{ and } a*b = \frac{ab}{2}, \forall a,b \in Q^+$ .Then inverse of 'a' is

   a) $\frac{1}{a}$ b) $\frac{2}{a}$ c) $\frac{3}{a}$ d) $\frac{4}{a}$ **Ans : d**

9. The set of all real numbers under the usual multiplication operation is not a group since

   a) Multiplication is not a binary operation b) Multiplication is not associative

   c) Identity elements does not exist d) Zero has no inverse **Ans : d**

10. $G = (Z_5, \times_5)$ is --------

a) Semigroup b) Monoid c) Group d) Abelian group **Ans: b**

11. The identity element In the group G = {2, 4, 6, 8) under multiplication modulo 10 is

a) 5 b) 9 c) 6 d) 12 **Ans : c**

12. If (G, .) is a group such that $(ab)^{-1} = a^{-1}b^{-1}$, $\forall$ a,b$\in$G. Then G is a

a. Commutative semi
b. Abelian group
c. Non-abelian group
d. None of the above **Ans: b**

13. If (G,.) is a group such that $a^2 = e$, $\forall$ a $\in$ G, then G is

a. semi group
b. abelian group
c. non-abelian group
d. none of above **Ans: b**

14. The inverse of – i in the multiplication group {1,-1,i,-i} is

a. 1
b. -1
c. i
d. –I **Ans: c**

15. In the group (G,.), the value of $(a^{-1}b)^{-1}$ is

a. ab^{-1}
b. $b^{-1}a$
c. $a^{-1}b$
d. ba^{-1} **Ans: b**

16. If (G,.) is a group, such that $(ab)^2 = a^2b^2$, $\forall$ a,b$\in$G then G is an

a. Commutative semi group
b. abelian group
c. Non-abelian group
d. None of these **Ans: b**

17. The identity element of a group (G,*) is

a. Unique
b. Uncountable
c. Infinite
d. None of these **Ans: a**

18. If G = {1,-1,i,-i}, then (G,×) is a cyclic group with the generator

a. i and –I
b. i and 1
c.1 and -1
d. –i and 1 **Ans: a**

19. .Every group of prime order is

a.) Cyclic and hence abelian b) Abelian and hence cyclic

b.) c) Not cyclic and abelian d) Not abelian and cyclic **Ans : a**

20. What are the generators of the group (Z,+) ?

a.) 1 and 0 b) -1 and 0 c) 0 alone d) 1 and -1 **Ans : d**

21. The necessary and sufficient condition that a non-empty subset of H of a group G to be a sub-group is

a) a, b $\in$ H => a^{-1}, b^{-1} $\in$ H b) a, b $\in$ H => $a*b^{-1} \in$ H

c) a, b$\in$ H => a*b $\in$ H d) a, b $\in$ H => $(a*b)^{-1} \in$ H **Ans : b**

22.Let G be a group. If a, b € G then inverse of (a*b) is

a) $a^{-1}*b^{-1}$ b) $a*b^{-1}$ c) $a^{-1}*b$ d) $b^{-1}*a^{-1}$ **Ans : d**

23. Which one of subsets of a group G = {1, -1, i, i} is a sub-group of G under multiplication?

a.) {i, -i} b) {i, i} c) {1, -i} d) {1, -1} **Ans : d**

24.Order of a sub-group of a finite group divides the order of the group is called

a.) Lagrange's Theorem b) Group homomorphism

c) Cayley's Theorem d) Fundamental Theorem of homomorphism **Ans : c**

25. A function f : (X, .) -> (Y,*) is said to be homomorphism **Ans : a**

a.) $f(x_1-x_2) = f(x_1) * f(x_2)$ b) $f(x_1*x_2) = f(x_1) . f(x_2)$

c) $f(x_1*x_2) = f(x_1) . 1/ f(x_2)$ d) $f(x_1.x_2) = f(x_1*x_2)$ **Ans : b**

26.Every cyclic group is

a.) Finite b) Abelian c) Normal d) Dihedral **Ans : b**

27.The order of a group G is 13, then the number of sub-groups of G is

a.) 1 b) 2 c) 4 d) 3 **Ans : b**

28.Name the semi-group (M,*) which has an identity element with respect to the operation on *

a.) Group b) Sub-group c) Monoid d) Cyclic **Ans : c**

29.Every sub-group of a cyclic group is

a.) Homomorphic b) Cyclic c) Isomorphic d) Abelian **Ans : b**

30. The minimum order of a non-abelian group is

a.) 3 b) 6 c) 9 d) 4 **Ans : b**

31. Every sub-group of abelian group is

a.) Normal b) Abelian c) Cyclic d) A permutation group. **Ans : a**

32. Which of the following is not an integral domain?

a) (N, +, .) b) (c, +, .) c) (O, +, .) d) (R, +, .) **Ans : a**

33**.** All integral domain S is

a) field when S is finite b) always a field c) never field d) field when S is infinite **Ans : a**

34. if (R, +, .) is a ring then that x.x = x ∀∀ x ∈∈ R, then

a) x + y = 0 ⇒⇒ x = y b) x + x ≠ 0 c) x ≠≠ y ⇒⇒ x + y = 0 d) x + x = 0 **Ans : a**

35**.** A ring of even integers is also a

a) field b) division ring c) integral domain d) ring with unity **Ans : c**

36. The condition for non-existence of zero divisor is

a) $a^2 = a, \ \forall \ a \in R$ b) the cellation law holds for multiplication in R

c) $(a+b)^2 = a^2 + 2ab + b^2, \forall \ a,b \in R$ d) $a^2 \neq a, \ \forall \ a \in R$ **Ans : b**

37. The ring Z of integers (mod p) is an integral domain iff

a) p is a positive integer b) p is purely even numbers c) p is odd d) p is prime **Ans : d**

38. Let $S = \{a_1, a_2, a_3\}, a_i \in Q$. Define addition and multiplication on S by

$(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3)$ and

$(a_1, a_2, a_3).(b_1, b_2, b_3) = (a_1 b_1, a_2 b_1 + a_3 b_2, a_3 b_3)$ then S is

a) A non commutative ring with unity (1, 0, 1) b) A commutative ring without unity

c). A non-commutative ring with unity (1, 0, 0) d) A non-commutative ring without unity **Ans : a**

39. If R is a system such that it is a group under addition and multiplication, obeys the closure and distributive laws, then **Ans : b**

a) R need not be a ring b) R has to be a ring c) R is not a ring d) R is necessarily a field

40. Which one of the following statement is correct?

a) In a ring ab = 0 ⇒⇒ either a = 0 or b = 0 b) Every finite ring is an integral domain

c). Every finite integral domain is a field d) a ring with zero divisors **Ans : c**

41) Let R = {0, l, 2, 3, 4, 5), +6,x6} then R is

a) a ring with zero divisors b) a field c) a division ring d) a ring without zero divisors **Ans : a**

42) . The set of all 2××2 matrices over the field of real number under the usual addition and multiplication of matrices is

a) not a ring b) a ring with unity c) a commutative ring d) an integral domain **Ans : b**

43) If Q and Z are the sets of rational numbers and integers respectively, then which one of the following triples is a field?

a)(Q, +, x)   b) (Q, -, x) c) (Z, +, x)   d) (Z, -, x)   **Ans : a**

44) If $x = 10011 \in B^5$ then weight of x , W(x) =

a) 2   b) 3   c) 5   d) 1   **Ans : b**

45) If $x = 10011 \in B^5$ then the length of x =

a) 2   b) 3   c) 5   d) 1   **Ans : c**

46) The Hamming distance between the codes x = 010000 and y = 000101 is

a) 3   b) 2   c) 6   d) 5   **Ans : a**

47) If $b = b_1 b_2 .....b_{m,}$ $define\ e(b) = b_1 b_2 ....b_m b_{m+1},\ where$ $b_{m+1} = \begin{cases} 0, & if\ \lfloor b \rfloor\ is\ even \\ 1, & if\ \lfloor b \rfloor\ is\ odd \end{cases}$ then

e(01010) =   a) 110100   b) 010101   c) 010110   d) 010100   **Ans : d**

48) The minimum distance of encoding function is 2 then the number of errors it can detect is

a) 1 or less than 1   b) 2 or less than 2   c) 3 or less than three   d) 0 error   **Ans : a**

49) The minimum distance of encoding function is 3 then the number of errors it can correct is

a) 1 or less than 1   b) 2 or less than 2   c) 3 or less than three   d) 0 error   **Ans : d**

50) For an encoding function $e : B^m \to B^n$, $the\ generator\ matrix\ G = \begin{pmatrix} 1 & 0 & 0 & 1\,1\,0 \\ 0 & 1 & 0 & 0\,1\,1 \\ 0 & 0 & 1 & 1\,0\,1 \end{pmatrix}$ and the message

M = (0 1 1) then the code word is

a) [0 1 1 1 1 0]   b) [0 1 0 1 1 0]   c) [0 0 0 1 1 0]   d) [0 1 1 1 0 0]   **Ans: a**

51) In a group code { 00000, 10101 , 01110 , 11011} , the inverse of 11011 is

a) 01110   b) 00000   c) 11011   d) 01110   **Ans: c**

52) The value of $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \oplus \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} =$

a) $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ b) $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ c) $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ d) $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ **Ans: a**

53) Order of B^5 =

a) 5 b) 2 c) 32 d) 10 Ans: c

54) For an encoding function $e : B^m \to B^{3m}$, e(100) =

a) 100001100 b) 100100 001 c) 100100100 d) 100000000 Ans: c

55) The minimum weight of the non-zero code word in a group code is equal to its

a) maximum distance b) minimum distance c) equl distance d) Parity check code **Ans: b**

56.) The encoding function is

a) on-to function b) one to one function c) many to one function d) in to function **Ans: b**

57) The decoding function is

a) on-to function b) one to one function c) many to one function d) in to function **Ans: a**

GROUP CODE

Introduction:

In today's modern world of communication, data items are constantly being transmitted from point to point.

Different devices are used for communication. The basic unit of information is message. Messages can be represented by sequence of dots and dashes.

Let $B = \{0, 1\}$ be the set of bits. Every character or symbol can be represented by sequence of elements of B. Message are coded in O's and 1's and then they are transmitted. These techniques make use of group theory. We will see a brief introduction of group code in this chapter. Also we will see the detection of error in transmitted message.

The set $B=\{0,1\}$ is a group under the binary operation $\oplus$ whose table is as follows :

$\oplus$	0	1
0	0	1
1	1	0

We have seen that B is a group as the $\mathbb{Z}2$, where + is only mod 2 addition.

If follows from theorem - "If G_1 and G_2 are groups then $G=G_1\times G_2$ is a group with binary operation defined by $(a_1,b_1)(a_2,b_2)=(a_1,a_2,b_1,b_2)$. So $B^m=B\times B\times ---\times B$ (m factors) is a group under the operation $\oplus$ defined by $(x_1,x_2--x_m)\oplus(y_1,y_2--y_m)=(x_1+y_1,x_2+y_2,--x_m+y_m)$ observe that B^m has 2^m elements. i.e. order of group B^m is 2^m.

Important Terminology :

Let us choose an integer $n>m$ and one-to-one function $e:B^m\rightarrow B^n$.

1) Encoding Function :

The function e is called an (m, n) encoding function. It means that every word in B^m as a word in B^n.

2) Code word :

If $b\in B^m$ then e(b) is called the code word

3) Weight :

For $x\in B^n$ the number of 1's in x is called the weight of x and is denoted by $|x|$.

e.g. i) $x=10011\in B^5 \therefore w(x)=3$

ii) $x=001\in B^3 \therefore w(x)=1$

4) $x \oplus y \rightarrow$ Let $x, y \in B^n$, then $x \oplus y$ is a sequence of length n that has 1's in those positions x & y differ and has O's in those positions x & y are the same. i.e. The operation + is defined as 0 + 0 = 0   0 + 1 = 1   1 + 1 = 0 1 + 0 = 1

e.g. if $x, y \in B^5$

$$x = 00101, y = 10110$$

$$\therefore x \oplus y = 10011$$

$$\therefore w(x \oplus y) = 3$$

5) Hamming Distance :

Let $x, y \in B^m$. The Hamming Distance $\delta(x, y)$ between x and y is the weight of $x \oplus y$. It is denoted by $|x \oplus y|$. e.g. Hamming distance between x & y can be calculated as follows : if x = 110110, y = 000101 $x \oplus y$ = 110011 so $|x \oplus y|$ = 4.

6) Minimum distance :

Let $x, y \in B^n$.then minimum distance = min $\{d(x, y) / x, y \in B^n\}$.

Let $x_1, x_2 - - x_n$ are the code words, let any $x_i, i = 1 - - - n$ is a transmitted word and y be the corresponding received word. Then $y = x_k$ if $d(x_k, y)$ is the minimum distane for k = 1, 2, --- n. This criteria is known as minimum distance criteria.

7) Detection of errors :

Let $e : B^m \rightarrow B^n\ (m < n)$ is an encoding function then if minimum distane of e is (k + 1) then it can detect k or fewer errors.

8) **Correction of errors :**

Let $e : B^m \to B^n \ (m < n)$ is an encoding function then if minimum distance of e is (2k + 1) then it can correct k or fewer errors.

Weight of a code word : It is the number of 1's present in the given code word.

Hamming distance between two code words : Let $x = x_1 x_2 \ldots x_m$ and $y = y_1 y_2 \ldots y_m$ be two code words. The Hamming distance between them, $\delta(x, y)$, is the number of occurrences such that $x_i \neq y_i$ for $i = 1, m$.

Example:1

Define weight of a codeword. Find the weights of the following.

(a) $x = 010000$ (b) $x = 11100$

(c) $x = 00000$ (d) $x = 11111$

(e) $x = 01001$ (f) $x = 11000$

Solution : Weight of a code word :

(a) $|x| = |010000| = 1$ (b) $|x| = |11100| = 3$

(c) $|x| = |00000| = 0$ (d) $|x| = |11111| = 5$

(e) $|x| = 2$ (f) $|x| = 2$

Example:2

Define Hamming distance. Find the Hamming distance between the codes.

(a) $x = 010000, \quad y = 000101$ (b) $x = 001100, \quad y = 010110$

Solution : Hamming distance :

(a) $\delta(x, y) = |x \oplus y| = |010000 \oplus 000101| = |010101| = 3$

(b) $\delta(x, y) = |x \oplus y| = |001100 \oplus 010110| = |011010| = 3$

Example 7.3 : Let d be the $(4, 3)$ decoding function defined by $d : B^4 \to B^3$. If $y = y_1 y_2 \dots y_{m+1}$, $d(y) = y_1 y_2 \dots y_m$.

Determine $d(y)$ for the word y is B^4.

(a) $\mathrm{y} = 0110$ (b) $\mathrm{y} = 1011$

Solution : (a) $\mathrm{d}(\mathrm{y}) = 011$ (b) $\mathrm{d}(\mathrm{y}) = 101$

Example 7.4 : Let $d : B^6 \to B^2$ be a decoding function defined by for $y = y_1 y_2 \dots y_6$. Then $d(y) = z_1 z_2$.

where

$\mathrm{zi} = 1$ if $\{y_1, y_{i+2}, y_{i+4}\}$ has at least two 1's.

0 if $\{y_1, y_{i+2}, y_{i+4}\}$ has less than two 1's.

Determine $\mathrm{d}(\mathrm{y})$ for the word y in B^6.

(a) $y = 111011$ (b) $y = 010100$

Solution : (a) $d(y) = 11$ (b) $d(y) = 01$

Example 7.5 : The following encoding function $f : B^m \to B^{m+1}$ 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

$$b_{m+1} = 0 \text{ if } |\mathrm{b}| \text{ is even.}$$
$$= 1 \text{ if } |\mathrm{b}| \text{ is odd.}$$

Find $\mathrm{e(b)}$ if (a) $\mathrm{b} = 01010$ (b) $\mathrm{b} = 01110$

Solution : (a) $\mathrm{e(b)} = 010100$ (b) $\mathrm{e(b)} = 011101$

Example 7.6 : Let $e : B^2 \to B^6$ is an (2,6) encoding function defined as

e(00) = 000000, e(01) = 011101
e(10) = 001110, e(11) = 111111

a) Find minimum distance.
b) How many errors can e detect?
c) How many errors can e correts?

Solution : Let $x_0, x_1, x_2, x_3 \in B^6$ where $x_0 = 000000, x_1 = 011101,$ $x_2 = 001110, x_3 = 111111$

$$w(x_0 \oplus x_1) = w(011101) = 4$$
$$w(x_0 \oplus x_2) = w(001110) = 3$$
$$w(x_0 \oplus x_3) = w(111111) = 6$$
$$w(x_1 \oplus x_2) = w(010011) = 3$$
$$w(x_1 \oplus x_3) = w(100010) = 2$$
$$w(x_2 \oplus x_3) = w(110001) = 3$$

Minimum distance = e = 2

d) Minimum distance = 2

An encoding function e can detect k or fewer errors if the minimum distance is k + 1. $\therefore k+1=2 \therefore k=1$

$\therefore$ The function can detect 1 or fewer (i.e. 0) error.

e) e can correct k or fewer error if minimum distance is 2k + 1.

$\therefore 2k + 1 = 2$

$\therefore k = \frac{1}{2}$

$\therefore$ e can correct $\frac{1}{2}$ or less than $\frac{1}{2}$ i.e. 0 errors.

Example 1 : Let e is (2, 4) encoding function defined as

$e(00) = 0000 \qquad e(01) = 1011$

$e(11) = 1100 \qquad e(10) = 0110$

i) Find minimum distance,

ii) How many errors can e detect,

iii) How many errors can e correct.

Solution :

Let $x_0 = 0000,\ x_1 = 1011,\ x_2 = 0110,\ x_3 = 1100$

i) $w(x_0 \oplus x_1) = w(x_1) = 3$

$w(x_0 \oplus x_2) = w(x_2) = 2$

$w(x_0 \oplus x_3) = w(x_3) = 2$

$w(x_1 \oplus x_2) = w(1101) = 3$

$w(x_1 \oplus x_3) = w(0111) = 3$

$w(x_2 \oplus x_3) = w(1010) = 2$

$\therefore$ Minimum distance of e = 2.

Note that minimum distance is not unique. There are three pairs having distance 2.

ii) $\therefore k+1=2 \therefore k=1$,

$\therefore$ e can detect 1 or less than 1 i.e. 0 errors.

iii) $\therefore 2k+1=2 \therefore k=\frac{1}{2}$

$\therefore$ e can correct $\frac{1}{2}$ or less than $\frac{1}{2}$ errors, i.e. e can correct 0 errors.

Example 2 : Let e is (3, 8) encoding function defined as

$e(000)=00000000 \qquad e(011)=01110001$

$e(010)=10011100 \qquad e(110)=11110000$

$e(001)=01110010 \qquad e(101)=10110000$

$e(100)=01100101 \qquad e(111)=00001111$

i) Find minimum distance.

ii) How many errors can e detect?

iii) How many errors can e correct?

Solution :

Let $x_0 = 00000000$, $x_1 = 10011100$, $x_2 = 01110010$, $x_3 = 01100101$, $x_4 = 01110001$, $x_5 = 11110000$, $x_6 = 10110000$, $x_7 = 00001111$.

i) $w(x_0 \oplus x_1) = w(x_1) = 4$, $\qquad w(x_0 \oplus x_2) = w(x_2) = 4$,

$w(x_0 \oplus x_3) = w(x_3) = 4$, $\qquad w(x_0 \oplus x_4) = w(x_4) = 4$,

$w(x_0 \oplus x_5) = w(x_5) = 4$, $\qquad w(x_0 \oplus x_6) = w(x_6) = 3$,

$w(x_0 \oplus x_7) = w(x_7) = 4$

Similarly, $w(x_1 \oplus x_2) = w(11101110) = 6$,

$w(x_1 \oplus x_3)=6,\ w(x_1 \oplus x_4)=6,\ w(x_1 \oplus x_5)=4,\ w(x_1 \oplus x_6)=3,$
$w(x_1 \oplus x_7)=4,\ w(x_2 \oplus x_3)=4, w(x_2 \oplus x_4)=2,\ w(x_2 \oplus x_5)=2,$
$w(x_2 \oplus x_6)=3, w(x_2 \oplus x_7)=6, w(x_3 \oplus x_4)=2, w(x_3 \oplus x_5)=4,$
$w(x_3 \oplus x_6)=5, w(x_3 \oplus x_7)=4,\ w(x_4 \oplus x_5)=2,\ w(x_4 \oplus x_6)=3,$
$w(x_4 \oplus x_7)=6, w(x_5 \oplus x_6)=1,\ w(x_5 \oplus x_7)=8,\ w(x_6 \oplus x_7)=7$

$\therefore$ The minimum distance of e = 1.

ii) $\therefore k+1=1 \therefore k=0$

$\therefore$ e can detect 0 or less than 0 errors i.e. 0 errors.

iii) $\therefore 2k+1=1 \therefore k=0$

$\therefore$ e can correct 0 or less than 0 errors. i.e. 0 errors.

Example 3 : Compute

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

Solution :

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

$\because$ Same digit sum = 0, opposite digit sum = 1

Solution :

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

$\because$ Same digit sum = 0, opposite digit sum = 1

Example 4 : Let B = {0, 1} and + is defined on B as follows.

+	0	1
0	0	1
1	1	0

Then show that (B, +) is a group.

Solution :

Addition is associative. Here B is set of bits and the operation of on B is +. $\therefore$ B with operation + is associative.

Also 0 + 1 = 1 and 0 + 0 = 0

$\therefore$ $0 \in B$ is an identity element. Here inverse of each element is itself. Since 0 + 0 = 0. $\therefore$ $0^{-1} = 0$

and 1 + 1 = 0 $\therefore$ $1^{-1} = 1$

$\therefore$ Inverse of each element exists.

$\therefore$ (B, +) is a group.

Three Cartesian product of groups is again a group.

$\therefore$ $B^n = B \times B \times B \ldots n \text{ times} \ldots \times B$ with + operation defined as $(x_1, x_2, \ldots, x_n) \oplus (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$ is also a group. Here identity element is $(0, 0, \ldots 0) \in B^n$ and every element is its own inverse.

$\therefore$ $(B^n, \oplus)$ is a group. Let $A \subseteq B^n$ such that $(A, \oplus)$ is a group then A is subgroup of B^n. Now we will see the encoding which uses this property of B^n.

GROUP CODES:

An (m, n) encoding function $e : B^m \to B^n \, (m < n)$ is called a group code if range of e is subgroup of B^n. i.e. (Ran.(e), $\oplus$) is a group. Since $\text{Ran.}(e) \subseteq B^n$ and if (Ran.(e), $\oplus$) is a group then Ran.(e) is a subgroup of B^n.

If an encoding function $e : B^m \to B^n \, (m < n)$ is a group code, then the minimum distance of e is the minimum weight of a non zero codeword.

Example 5 : Show that an (3, 7) encoding function $e : B^3 \to B^7$ defined by

$$
\begin{aligned}
&e(000) = 0000000 \qquad && e(011) = 0111110 \\
&e(001) = 0010110 && e(101) = 1010011 \\
&e(010) = 0101000 && e(110) = 1101101 \\
&e(100) = 1000101 && e(111) = 1111011
\end{aligned}
$$

is a group code. Hence find minimum distance.

Solution : Let

$x_0 = 0000000$ $x_4 = 1000101$

$x_1 = 0010110$ $x_5 = 1010011$

$x_2 = 0101000$ $x_6 = 1101101$

$x_3 = 0111110$ $x_7 = 1111011$

$\therefore$ Ran.(e) = $\{x_0, x_1, ..., x_7\}$

$x_0 \oplus x_0 = x_0$, $x_0 \oplus x_1 = x_1$, $x_2 \oplus x_7 = 1010011 = x_5$ like this we can compute and this we will present in table.

The composition Table is,

$\oplus$	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_0	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	x_1	x_0	x_3	x_2	x_5	x_4	x_7	x_6
x_2	x_2	x_3	x_0	x_1	x_6	x_7	x_4	x_5
x_3	x_3	x_2	x_1	x_0	x_7	x_6	x_5	x_4
x_4	x_4	x_5	x_6	x_7	x_0	x_1	x_2	x_3
x_5	x_5	x_4	x_7	x_6	x_1	x_0	x_3	x_2
x_6	x_6	x_7	x_4	x_5	x_2	x_3	x_0	x_1
x_7	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0

Like in Example 4 we can verity that (Ran.(e), $\oplus$) is group and Ran.(e) $\subset B^7$.

$\therefore$ Ran.(e) is subgroup of B^7.

$\therefore$ $e: B^3 \to B^7$ is a group code.

The minimum distance of a group code is the minimum weight of non zero code word.

Consider $w(x_0)=0$, $w(x_1)=w(x_4)=3$, $w(x_2)=2$, $w(x_5)=4$, $w(x_3)=w(x_6)=5$, $w(x_7)=6$.

$\therefore$ Minimum distance = 2.

Example 6 : Show that an (2, 5) encoding function $e: B^2 \to B^5$ defined as

e(00) = 00000   e(10) = 10101

e(01) = 01110   e(11) = 11011

is a group code. Hence find minimum distance and also find how many errors can e detect?

Solution :

$x_0 = 00000$, $x_1 = 01110$, $x_2 = 10101$, $x_3 = 11011$

$\therefore$ Ran.(e) = $\{x_0, x_1, x_2, x_3\}$

$\therefore$ The composition Table

$\oplus$	x_0	x_1	x_2	x_3
x_0	x_0	x_1	x_2	x_3
x_1	x_1	x_0	x_3	x_2
x_2	x_2	x_3	x_0	x_1
x_3	x_3	x_2	x_1	x_0

Addition is associative

$\therefore$ $(\text{Ran.}(e), \oplus)$ is associative. We can see that the first row is same as heading row.

$\therefore$ x_0 is identity element. Also $x_0 \oplus x_0 = x_0$, $\therefore$ $x_0^{-1} = x_0$.

$x_2 \oplus x_2 = x_0$. $\therefore$ $x_2^{-1} = x_2$ so on. i.e. inverse of each element exists which is itself.

$\therefore$ $(\text{Ran.}(e), \oplus)$ is a group and since $\text{Ran.}(e) \subset B^5$.

$\therefore$ Ran.(e) is subgroup of B^5.

$\therefore$ $e : B^2 \to B^5$ is a group code.

Consider,

$w(x_0) = 0$, $w(x_1) = w(x_2) = 3$, $w(x_3) = 4$.

The minimum distance of a group code is the minimum weight of nonzero code word.

$\therefore$ Minimum distance = 3.

Here k + 1 = 3, k = 2.

$\therefore$ e can detect 2 or less than 2 errors. i.e. e can detect 0, 1 or 2 errors.

DECODING AND ERROR CORRECTION :

Consider an (m, n) encoding function $e: B^m \rightarrow B^n$, we require an (n,m) decoding function associate with e as $d: B^n \rightarrow B^m$.

The method to determine a decoding function d is called maximum likelihood technique.

Since $\left|\mathrm{B}^{\mathrm{m}}\right| = 2^{\mathrm{m}}$.

Let $x_k \in B^m$ be a codeword, k = 1, 2, ---^{m} and the received word is y then. Min $1 \le k \le 2^m \{d(x_k, y)\} = d(x_i, y)$ for same i then x_i is a codeword which is closest to y. If minimum distance is not unique then select on priority

MAXIMUM LIKELIHOOD TECHNIQUE :

Given an (m, n) encoding function $e: B^m \rightarrow B^n$, we often need to determine an (n, m) decoding function $d: B^n \rightarrow B^m$ associated with e. We now discuss a method, called the maximum likelihood techniques, for determining a decoding function d for a given e. Since B^{m} has 2^{m} elements, there are 2^{m} code words in B^{n}. We first list the code words in a fixed order.

$$x^{(1)}, x^{(2)}, \ldots, x^{\left(2^m\right)}$$

If the received word is x_1, we compute $\delta\left(x^{(i)}, x_1\right)$ for $1 \leq i \leq 2^m$ and choose the first code word, say it is $x^{(s)}$, such that

$$\min_{1 \leq i \leq 2^m}\left\{\delta\left(x^{(i)}, x_1\right)\right\} = \delta\left(x^{(s)}, x_1\right)$$

That is, $x^{(s)}$ is a code word that is closest to x_1, and the first in the list. If $x^{(s)} = e(b)$, we define the maximum likelihood decoding function d associated with e by

$$d\left(x_t\right) = b$$

Observe that d depends on the particular order in which the code words in $e\left(B^n\right)$ are listed. If the code words are listed in a different order, we may obtain, a different likelihood decoding function d associated with e.

Theorem 7.3 : Suppose that e is an (m, n) encoding function and d is a maximum likelihood decoding function associated with e. Then (e, d) can correct k or fewer errors if and only if the minimum distance of e is at least $2\mathrm{k}+1$.

Example:

Let $m = 2, n = 5$ and $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Determine the group code $e_H : B^2 \to B^5$.

Solution : We have $B^2 = \{00, 01, 10, 11\}$. Then $e(00) = 00x_1x_2x_3$ where

$$x_1 = 0.1 + 0.0 = 0$$
$$x_2 = 0.1 + 0.1 = 0$$
$$x_3 = 0.0 + 0.1 = 0$$
$$\therefore\ e(00) = 00000$$

Now,

$$e(01) = 01x_1x_2x_3$$

where

$$x_1 = 0.1 + 1.0 = 0$$
$$x_2 = 0.1 + 1.1 = 1$$
$$x_3 = 0.0 + 1.1 = 1$$
$$\therefore\ e(01) = 01011$$

Next

$$e(10) = 10x_1x_2x_3$$

$$x_1 = 1.1 + 0.0 = 1$$

$$x_2 = 1.1 + 1.0 = 1$$

$$x_3 = 1.0 + 0.1 = 0$$

$$\therefore\ e(10) = 10110$$

$$e(11) = 11101$$

Example:

: Let $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix. determine

the $(3, 6)$ group code $e_H : B^3 \to B^6$.

Solution : First find $e(000)$, $e(001)$, $e(010)$, $e(011)$, $e(100)$, $e(101)$, $e(110)$, $e(111)$.

$e(000) = 000000$	$e(100) = 100100$
$e(001) = 001111$	$e(101) = 101011$
$e(010) = 010011$	$e(110) = 110111$
$e(100) = 011100$	$e(111) = 111000$

Example:

Consider the group code defined by $e : B^2 \to B^5$ such that

$e(00)=00000 \qquad e(01)=01110 \qquad e(10)=10101 \qquad e(11)=11011$.

Decode the following words relative to maximum likelihood decoding function.

(a) 11110 (b) 10011 (c) 10100

Solution : (a) $x_t = 1110$

Compute

$$\delta\left(x^{(1)}, x_t\right) = |\,00000 \oplus 11110\,| = |\,11110\,| = 4$$

$$\delta\left(x^{(2)}, x_t\right) = |\,01110 \oplus 11110\,| = |\,10000\,| = 1$$

$$\delta\left(x^{(3)}, x_t\right) = |\,10101 \oplus 11110\,| = |\,01011\,| = 3$$

$$\delta\left(x^{(4)}, x_t\right) = |\,11011 \oplus 11110\,| = |\,00101\,| = 2$$

$$\min\left\{\delta\left(x^{(i)}, x_t\right)\right\} = 1 = \delta\left(x^{(2)}, x_t\right)$$

$\therefore$ $e(01)=01110$ is the code word closest to $x_t = 11110$.

$\therefore$ The maximum likelihood decoding function d associated with e is defined by $d(x_t) = 01$.

(b) $x_t = 10011$

Compute $\delta\left(x^{(1)}, x_t\right) = |\,00000 \oplus 10011\,| = |\,11101\,| = 4$

$\delta\left(x^{(2)}, x_t\right) = |\,01110 \oplus 10011\,| = |\,00110\,| = 2$

$\delta\left(x^{(3)}, x_t\right) = |\,10101 \oplus 11110\,| = |\,01011\,| = 3$

$\delta\left(x^{(4)}, x_t\right) = |\,11011 \oplus 10011\,| = |\,01000\,| = 1$

$\min\left\{\delta\left(x^{(i)}, x_t\right)\right\} = 1 = \delta\left(x^{(4)}, x_t\right)$

$\therefore$ e$(11) = 11011$ is the code word closest to $x_t = 10011$.

$\therefore$ The maximum likelihood decoding function d associated with e is defined by $d(x_t) = 11$.

(c) $x_t = 10100$

Compute $\delta\left(x^{(1)}, x_t\right) = |\,00000 \oplus 10100\,| = |\,10100\,| = 2$

$\delta\left(x^{(2)}, x_t\right) = |\,01110 \oplus 10100\,| = |\,11010\,| = 3$

$\delta\left(x^{(3)}, x_t\right) = |\,10101 \oplus 10100\,| = |\,00001\,| = 1$

$\delta\left(x^{(4)}, x_t\right) = |\,11011 \oplus 10100\,| = |\,01111\,| = 4$

$\min\left\{\delta\left(x^{(i)}, x_t\right)\right\} = 1 = \delta\left(x^{(3)}, x_t\right)$

$\therefore$ e$(10) = 10101$ is the code word closest to $x_t = 10100$.

$\therefore$ The maximum likelihood decoding function d associated with e is defined by $d(x_t) = 10$.

Example:

Let $H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix. decode the

following words relative to a maximum likelihood decoding function associated with e_H : (i) 10100, (ii) 01101, (iii) 11011.

Solution : The code words are $e(00) = 00000$, $e(01) = 00101$, $e(10) = 10011$, $e(11) = 11110$. Then $N = \{00000, 00101, 10011, 11110\}$. We implement the decoding procedure as follows. Determine all left cosets of N in B5,

as rows of a table. For each row 1, locate the coset leader ε_i, and rewrite the row in the order.

$\varepsilon_1, \varepsilon_i \oplus$

Example 7.11 : Consider the $(2, 4)$ encoding function e as follows. How many errors will e detect? [May-06]

$e(00) = 0000$, $e(01) = 0110$, $e(10) = 1011$, $e(11) = 1100$

Solution :

$\oplus$	0000	0110	1011	1100
0000	---	0110	1011	1100
0110		---	1101	1010
1011			---	0111
1100				---

Minimum distance between distinct pairs of $e = 2$ $\therefore k + 1 = 2$ $\therefore k = 1$.
$\therefore$ the encoding function e can detect 1 or fewer errors.

Example 7.12 : Define group code. Show that $(2,5)$ encoding function $e: B^2 \to B^5$ defined by $e(00) = 0000$, $e(10) = 10101$, $e(11) = 11011$ is a group code.

Solution : Group Code

$\oplus$	00000	01110	10101	11011
00000	00000	01110	10101	11011
01110	01110	00000	11011	10101
10101	10101	11011	00000	01110
11011	11011	10101	01110	00000

Since closure property is satisfied, it is a group code.

Example 7.13 : Define group code. show that $(2,5)$ encoding function $e: B^2 \to B^5$ defined by $e(00) = 00000$, $e(01) = 01110$, $e(10) = 10101$,

$e(11) = 11011$ is a group code. Consider this group code and decode the following words relative to maximum likelihood decoding function.
(a) 11110 (b) 10011.

Solution : Group Code

$\oplus$	00000	01110	10101	11011
00000	00000	01110	10101	11011
01110	01110	00000	11011	10101
10101	10101	11011	00000	01110
11011	11011	10101	01110	00000

Since closure property is satisfied, it is a group code.

Now, let $x^{(1)} = 00000,\ x^{(2)} = 01110,\ x^{(3)} = 10101,\ x^{(4)} = 11011$.

(a) $x_t = 11110$

$$\delta\left(x^{(1)}, x_t\right) = \left|x^{(1)} \oplus x_t\right| = \left|00000 \oplus 11110\right| = \left|11110\right| = 4$$
$$\delta\left(x^{(2)}, x_t\right) = \left|x^{(2)} \oplus x_t\right| = \left|01110 \oplus 1110\right| = \left|10000\right| = 1$$
$$\delta\left(x^{(3)}, x_t\right) = \left|x^{(3)} \oplus x_t\right| = \left|10101 \oplus 1110\right| = \left|01011\right| = 3$$
$$\delta\left(x^{(4)}, x_t\right) = \left|x^{(4)} \oplus x_t\right| = \left|11011 \oplus 1110\right| = \left|00101\right| = 2$$

$\therefore$ Maximum likelihood decoding function $d(x_t) = 01$.

(b) $x_t = 10011$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = |\, 00000 \oplus 10011 \,| = |\, 10011 \,| = 3$$

$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = |\, 01110 \oplus 10011 \,| = |\, 11101 \,| = 4$$

$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = |\, 10101 \oplus 10011 \,| = |\, 00110 \,| = 2$$

$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = |\, 11011 \oplus 10011 \,| = |\, 01000 \,| = 1$$

$\therefore$ Maximum likelihood decoding function $d\left(x_t\right) = 11$.

Example 7.14 : Let $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix. Determine the $(3,6)$ group code $e_H : B^3 \to B^6$.

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

$e_H(000) = 000000$ $\quad$ $e_H(001) = 001111$ $\quad$ $e_H(010) = 010011$

$e_H(011) = 011100$ $\quad$ $e_H(100) = 100100$ $\quad$ $e_H(101) = 101011$

$e_H(110) = 110111$ $\quad$ $e_H(111) = 111000$

$\therefore$ Required group code = $\{000000, 001111, 010011, 011100, 100100,$ $101011, 110111, 111000\}$

Example : Consider parity check matrix H given by $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Determine the group code $e_H : B_2 \to B_5$. Decode the following words relative to a maximum likelihood decoding function associated with e_H : 01110, 11101, 00001, 11000.

Solution : $B_2 = \{00, 01, 10, 11\}$

$e_H(00) = 00x_1x_2x_3$ where $x_1 = 0.1 + 0.0 = 0$

$x_2 = 0.1 + 0.1 = 0$

$x_3 = 0.0 + 0.1 = 0$ $\quad$ $\therefore e_H(00) = 00000$

$e_H(01) = 01x_1x_2x_3$ where $x_1 = 0.1 + 1.0 = 0$

$x_2 = 0.1 + 1.1 = 1$

$x_3 = 0.0 + 1.1 = 1$ $\quad$ $\therefore e_H(01) = 01011$

$$e_H(10) = 10x_1x_2x_3 \quad \text{where} \quad \begin{aligned} x_1 &= 1.1 + 0.0 = 1 \\ x_2 &= 1.1 + 0.1 = 1 \\ x_3 &= 1.0 + 0.1 = 0 \end{aligned} \qquad \therefore e_H(01) = 10110$$

$$e_H(11) = 11x_1x_2x_3 \quad \text{where} \quad \begin{aligned} x_1 &= 1.1 + 1.0 = 1 \\ x_2 &= 1.1 + 1.1 = 0 \\ x_3 &= 1.0 + 1.1 = 1 \end{aligned} \qquad \therefore e_H(01) = 11101$$

$\therefore$ Desired group code = $\{00000,\ 01011,\ 10110,\ 11101\}$

(1) $x_t = 01110$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = |\,00000 \oplus 01110\,| = |\,01110\,| = 3$$

$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = |\,01011 \oplus 01110\,| = |\,00101\,| = 2$$

$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = |\,10110 \oplus 01110\,| = |\,11000\,| = 2$$

$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = |\,11101 \oplus 01110\,| = |\,10011\,| = 3$$

$\therefore$ Maximum likelihood decoding function $d(x_t) = 01$

(2) $x_t = 11101$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = |\,00000 \oplus 11101\,| = |\,11101\,| = 4$$

$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = |\,01110 \oplus 11101\,| = |\,10110\,| = 3$$

$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = |\,10101 \oplus 11101\,| = |\,01011\,| = 3$$

$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = |\,11011 \oplus 11101\,| = |\,00000\,| = 0$$

$\therefore$ Maximum likelihood decoding function $\mathrm{d}(\mathrm{x_t}) = 11$

(3) $x_t = 00001$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = |\,00000 \oplus 00001\,| = |\,00001\,| = 1$$

$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = |\,01011 \oplus 00001\,| = |\,01010\,| = 2$$

$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = |\,10110 \oplus 00001\,| = |\,10111\,| = 4$$

$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = |\,11101 \oplus 00001\,| = |\,11100\,| = 3$$

$\therefore$ Maximum likelihood decoding function $\mathrm{d}(\mathrm{x_t}) = 00$

(2) $x_t = 11000$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = |\,00000 \oplus 11000\,| = |\,11000\,| = 2$$

$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = |\,01110 \oplus 11000\,| = |\,10011\,| = 3$$

$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = |\,10101 \oplus 11000\,| = |\,01101\,| = 3$$

$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = |\,11011 \oplus 11000\,| = |\,10000\,| = 1$$

$\therefore$ Maximum likelihood decoding function $d(x_t) = 11$

Example : Let $H = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$ be a parity check matrix. decode 0110 relative to a maximum likelihood decoding function associated with e_H.

Solution : $e_H : B_2 \to B_5$

$B_2 = \{00, 01, 10, 11\}$

$e_H(00) = 00x_1x_2$ where $x_1 = 0.1 + 0.0 = 0$

$x_2 = 0.1 + 0.1 = 0$ $\therefore e_H(00) = 0000$

$e_H(01) = 01x_1x_2$ where $x_1 = 0.1 + 1.0 = 0$

$x_2 = 0.1 + 1.1 = 1$ $\therefore e_H(01) = 0101$

$e_H(10) = 10x_1x_2$ where $x_1 = 1.1 + 0.0 = 1$

$x_2 = 1.1 + 0.1 = 1$ $\therefore e_H(01) = 1011$

$e_H(11) = 11x_1x_2$ where $x_1 = 1.1 + 1.0 = 1$

$x_2 = 1.1 + 1.1 = 0$ $\therefore e_H(01) = 1110$

Let $x^{(1)} = 0000,\ x^{(2)} = 0101,\ x^{(3)} = 1011,\ x^{(4)} = 1110$.
Let $x_1 = 0110$.

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = \left| 0000 \oplus 0110 \right| = \left| 0110 \right| = 2$$

$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = \left| 0101 \oplus 0110 \right| = \left| 0011 \right| = 2$$

$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = \left| 1011 \oplus 0110 \right| = \left| 1011 \right| = 3$$

$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = \left| 1110 \oplus 0110 \right| = \left| 1000 \right| = 1$$

$$\therefore Min\,\delta\left(x^{(i)}, x_t\right) = \delta\left(x^{(4)}, x_t\right) \ and \ e(11) = x^{(4)} \qquad \therefore d(x_t) = 11.$$

Example ... **:** Consider the $(2,5)$ group encoding function defined by $e(00) = 00000,\ e(01) = 01101,\ e(10) = 10011,\ e(11) = 11110$ and d be an associated maximum likelihood function. Use d to decode the following words.
(i) 10100 (ii) 01101

Solution : Let $x^{(1)} = 00000,\ x^{(2)} = 01011,\ x^{(3)} = 10110,\ x^{(3)} = 11110$
(1) $x_t = 10100$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = \left| 00000 \oplus 10100 \right| = \left| 10100 \right| = 2$$

$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = \left| 01101 \oplus 10100 \right| = \left| 11001 \right| = 3$$

$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = |10011 \oplus 10100| = |00111| = 3$

$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = |11110 \oplus 10100| = |01010| = 2$

$\therefore Min\, \delta\left(x^{(i)}, x_t\right) = \delta\left(x^{(1)}, x_t\right)$ i.e. $x^{(1)}$ is the code word which is closest to x_t and $1 \le i \le 4$

The first in their list in the list and $e(00) = x^{(1)}$. So we define maximum likelihood decoding function d associated with e by $d(x_t) = 00$.

(2) $x_t = 01100$

$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = |00000 \oplus 01101| = |01101| = 3$

$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = |01101 \oplus 01101| = |00000| = 0$

$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = |10011 \oplus 01101| = |11110| = 4$

$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = |11110 \oplus 01101| = |10011| = 3$

$\therefore \text{Min}\, \delta\left(x^{(i)}, x_t\right) = \delta\left(x^{(2)}, x_t\right)$ i.e. $x^{(2)}$ is the code word which is closest to x_t and $1 \le i \le 4$

The first in their list in the list and $e(01) = x^{(2)}$. So we define maximum likelihood decoding function d associated with e by $d(x_t) = 01$.

Example 7.21 : Let $H = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$ be a parity check matrix.

i) Determine the $(3,5)$ group code $e_H : B^3 \to B^5$.

ii) Construct the decoding table and decode the following words using maximum likelihood technique – 1) 00111, 2) 10111, 3) 11001

Solution : (i) $e_H : B^3 \to B^5$.

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

$e_H(000) = 000x_1x_2$ where $x_1 = 0.1 + 0.0 + 0.1 = 0$

$x_2 = 0.1 + 0.1 + 0.0 = 0 \quad \therefore e_H(000) = 00000$

$e_H(001) = 001x_1x_2$ where $x_1 = 0.1 + 0.0 + 1.1 = 1$

$x_2 = 0.1 + 0.1 + 1.0 = 0 \quad \therefore \mathrm{e_H}(001) = 00110$

$e_H(010) = 010x_1x_2$ where $x_1 = 0.1 + 1.0 + 0.1 = 0$

$x_2 = 0.1 + 1.1 + 0.0 = 1 \quad \therefore \mathrm{e_H}(010) = 01001$

$e_H(011) = 011x_1x_2$ where $x_1 = 0.1 + 1.0 + 1.1 = 1$

$x_2 = 0.1 + 1.1 + 1.0 = 1 \quad \therefore \mathrm{e_H}(011) = 01111$

$e_H(100) = 100x_1x_2$ where $x_1 = 1.1 + 0.0 + 0.1 = 1$

$x_2 = 1.1 + 0.1 + 0.0 = 1 \quad \therefore \mathrm{e_H}(100) = 10011$

$e_H(101) = 101x_1x_2$ where $x_1 = 1.1 + 0.0 + 1.1 = 0$

$x_2 = 1.1 + 0.1 + 1.0 = 1 \quad \therefore \mathrm{e_H}(001) = 10101$

$e_H(110) = 110x_1x_2$ where $x_1 = 1.1 + 1.0 + 0.1 = 1$

$x_2 = 1.1 + 1.1 + 1.0 = 0 \quad \therefore \mathrm{e_H}(110) = 11010$

$e_H(111) = 111x_1x_2$ where $x_1 = 1.1 + 1.0 + 1.1 = 0$

$x_2 = 1.1 + 1.1 + 1.0 = 0 \quad \therefore \mathrm{e_H}(111) = 11100$

Let $x^{(1)} = 00000, \ x^{(2)} = 00110, \ x^{(3)} = 01001, \ x^{(4)} = 01111$

$x^{(5)} = 10011, \ x^{(6)} = 10101, \ x^{(7)} = 11010, \ x^{(8)} = 11100$

(ii) (1) Let $x_t = 00111$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = |00111| = 3$$

$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = |00001| = 1$$

$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = |01110| = 3$$

$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = \left| 01000 \right| = 1$$

$$\delta\left(x^{(5)}, x_t\right) = \left| x^{(5)} \oplus x_t \right| = \left| 10100 \right| = 2$$

$$\delta\left(x^{(6)}, x_t\right) = \left| x^{(6)} \oplus x_t \right| = \left| 10010 \right| = 2$$

$$\delta\left(x^{(7)}, x_t\right) = \left| x^{(7)} \oplus x_t \right| = \left| 11101 \right| = 4$$

$$\delta\left(x^{(8)}, x_t\right) = \left| x^{(8)} \oplus x_t \right| = \left| 11011 \right| = 4$$

(2) Let $x_t = 10111$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = \left| 10111 \right| = 4$$

$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = \left| 10001 \right| = 2$$

$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = \left| 11110 \right| = 4$$

$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = \left| 11000 \right| = 2$$

$$\delta\left(x^{(5)}, x_t\right) = \left| x^{(5)} \oplus x_t \right| = \left| 00100 \right| = 1$$

$$\delta\left(x^{(6)}, x_t\right) = \left| x^{(6)} \oplus x_t \right| = \left| 00010 \right| = 1$$

$$\delta\left(x^{(7)}, x_t\right) = \left| x^{(7)} \oplus x_t \right| = \left| 01101 \right| = 3$$

$$\delta\left(x^{(8)}, x_t\right) = \left| x^{(8)} \oplus x_t \right| = \left| 01011 \right| = 3$$

(3) Let $x_t = 11001$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = |11001| = 3$$
$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = |11111| = 5$$
$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = |10000| = 1$$
$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = |10110| = 3$$
$$\delta\left(x^{(5)}, x_t\right) = \left| x^{(5)} \oplus x_t \right| = |01010| = 2$$
$$\delta\left(x^{(6)}, x_t\right) = \left| x^{(6)} \oplus x_t \right| = |01100| = 2$$
$$\delta\left(x^{(7)}, x_t\right) = \left| x^{(7)} \oplus x_t \right| = |00011| = 2$$

$$\delta\left(x^{(8)}, x_t\right) = \left| x^{(8)} \oplus x_t \right| = |00101| = 2$$

$$\therefore Min\,\delta\left(x^{(i)}, x_t\right) = \delta\left(x^{(3)}, x_t\right) \text{ and } e(010) = x^{(3)} \qquad \therefore d(x_t) = 010.$$

Example 7.22 : Let $H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix. determine the corresponding group code.

i) How many errors will the above group code detect?
ii) Explain the decoding procedure with an example.

Solution : Given H is a parity check matrix of $(3,6)$ group code. $e_H : B^3 \to B^6$.

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

$e_H(000) = 000000,\ e_H(001) = 001011,\ e_H(010) = 010101,\ e_H(011) = 011111$

$e_H(100) = 100110,\ e_H(101) = 101110,\ e_H(110) = 110011,\ e_H(111) = 111000.$

(i) Min distance of a group code = min weight of non-zero code word = 3
$\therefore k+1=3 \qquad \therefore k=2$
$\therefore$ The group code can detect at the most 2 or fewer errors.

(ii) Maximum likelihood decoding procedure :
Let $e_H(000) = x^{(1)},\ e_H(001) = x^{(2)},\ e_H(010) = x^{(3)},\ e_H(011) = x^{(4)}$

$e_H(100) = x^{(5)},\ e_H(101) = x^{(6)},\ e_H(110) = x^{(7)},\ e_H(111) = x^{(8)}$

and let x_t be transmitted codeword. Find $\delta\left(x^{(i)}, x_t\right)$, take minimum.

If $Min\,\delta\left(x^{(i)}, x_t\right) = \delta\left(x^{(s)}, x_t\right)$ then maximum likelihood decoding function d can be defined as $d(x_t) = b$ where $e_H(b) = x^{(s)}$. If two or more $x^{(i)}$ have the same minimum value then we select the $x^{(s)}$ whichever comes first in the list and define the decoding function accordingly.

Example ' : Consider the $(2,9)$ encoding function e defined by

$e(00) = 000\,000\,000$, $e(01) = 011\ 101\ 100$

$e(10) = 101\ 110\ 001$, $e(11) = 110\ 001\ 111$

Let d be an associated maximum likelihood function. How many errors will (e, d) correct.

Solution :

Let $x^{(1)} = 000\ 000\ 000$, $x^{(2)} = 011\ 101\ 100$, $x^{(3)} = 101\ 110\ 001$, $x^{(4)} = 110\ 001\ 111$.

$\oplus$	000 000 000	011 101 100	101 110 001	110 001 111
000 000 000	-	011 101 100	101 110 001	110 001 111
011 101 100		-	110 011 101	101 100 011
101 110 001			-	011 111 110
110001111				

$\therefore$ Minimum distance = 5 $\quad\therefore 2k + 1 = 5 \quad\therefore k = 2$

$\therefore (e, d)$ can correct $k = 2$ or fewer errors.

PART-B

- - -- - - -

Question : 1

Prove that the identity of a subgroup is the same as that of the group.

Solution :

Let G be a group and let H be a subgroup of G.

$\Rightarrow H$ itself is a group under the same operations $*$ on G

Let e be the identity element of G and let e' be the identity element of H

To prove $e = e'$

Since G is a group $\forall a \in G, \exists e \in G$ such that $a * e = e * a = a$..........(1)

Since H is subgroup of G $\forall a \in H, \exists e \in H$ such that $a * e' = e' * a = a$.........(2)

From (1) and (2) $a * e = a * e' \Rightarrow \boxed{e = e'}$ by left cancellation law

Question :

When is a group $(G, *)$ called abelian?

Answer :

A group $(G, *)$ is abelian if $a * b = b * a \;\; \forall a, b \in G$

Question :

Define Homomorphism and isomorphism between two algebraic system.

Answer :

Let G and G' be two groups

A mapping $f : G \to G'$ is called a homomorphism if $f(ab) = f(a) f(b) \;\; \forall a, b \in G$

If $f : G \to G'$ is one-one and onto we say that f is an isomorphism

Question : (

Define a commutative ring

Answer :

If in a ring R, $a \bullet b = b \bullet a \;\; \forall a, b \in R$ then R is called a commutative ring.

Question :

Show that every cyclic group is abelian

Answer :

Let G be a cyclic group generated by an element 'a'

$\Rightarrow \forall x \in G \quad \exists a \in G$ such that $x = a^k$ for some $k \in Z$

Let $b, c \in G$

Since G is cyclic , $b = a^m$, $c = a^n$ for some $m, n \in Z$

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

$= a^n * a^m$

$= c * b$

Hence $b * c = c * b \quad \forall b, c \in G$

Hence G is abelian.

Question :

Prove that if G is abelian group , then for all $a, b \in G$ $(a*b)^2 = a^2 * b^2$

Answer :

Let G be an abelian group

$\Rightarrow a * b = b * a$ for all $a, b \in G$

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

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

$= a*(b*(a*b)) \quad \{\because$ associativity

$= a*((a*b)*b) \quad \{\because a*b = b*a$

$= a*(a*(b*b)) \quad \{\because$ associativity

$= (a*a)*(b*b) \quad \{\because$ associativity

$= a^2 * b^2$

Question

Define a semi group

Answer:

A non – empty set G together with a binary operation $*$ is called a semi group if $a*(b*c) = (a*b)*c \quad \forall a, b, c \in G$.

Question :]

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

Answer :

Let G be a cyclic group generated by a

$\forall x \in G \quad \exists a \in G$ such that $x = a^k$ for some $\mathrm{k} \in Z$

Then $a^k = \left(a^{-1}\right)^{-k} = \left(a^{-1}\right)^l$, where $l = -k$. Thus every element of G is of the form $\left(a^{-1}\right)^l$ for some integer l and G is generated by a^{-1}

Question :

If $(G,*)$ is an abelian group, show that $(a*b)^2 = a^2 * b^2$

Answer :

Let $(G,*)$ is an abelian group

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

Now $(a*b)^2 = (a*b)*(a*b) = a*\left[b*(a*b)\right]$

$= a*\left[(b*a)*b\right] = a*\left[(a*b)*b\right] = a*\left[a*(b*b)\right] = (a*a)*(b*b) = a^2 * b^2$

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

Question:

Let $G = \{1, -1, i, -i\}$ and $(G, \cdot)$ be a group.
Find the order of each element of this group.

Given $G = \{1, -1, i, -i\}$ is a group w.r.to $\cdot$

here identity element $e = 1$.

$o(1) = 1$ $\quad (\because o(e) = 1$

$o(-1) = 2$

$o(i) = 4$

$o(-i) = 4$.

Question:

Prove that the intersection of two subgroups. of a group G is also a Subgroup of G.

Let H_1, H_2 be any two subgroups of G.

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

Since, atleast identity element e is common to both H_1 & H_2.

Let $a \in H_1 \cap H_2$. Then $a \in H_1$ & $a \in H_2$.

Let $b \in H_1 \cap H_2$, Then $b \in H_1$ & $b \in H_2$

H_1 is a Subgroup of G

$\Rightarrow a * b^{-1} \in H_1$

H_2 is a Subgroup of G.

$a * b^{-1} \in H_2$.

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

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

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

Question:

In an abelian group $(G, *)$, Prove by induction that $(a*b)^n = a^n * b^n$. for $n \geq 1$.

Let $P(n)$: $(a*b)^n = a^n * b^n$.

For $n=1$, $P(1)$: $(a*b)^1 = a*b$

$\therefore P(1)$ is true.

Assume $P(n)$ is true for $n = K$.

$P(K)$: $(a*b)^K = a^K * b^K$

To prove: $P(n)$ is true for $n = K+1$.

$$(a*b)^{K+1} = (a*b)^K * (a*b)^1$$
$$= a^K * b^K * (a*b)$$
$$= a^K * b^K * b*a \quad (\because G \text{ is abelian}$$
$$= a^K * (b^K * b) * a$$
$$= a^K * (b^{K+1} * a)$$
$$= a^K * a * b^{K+1}$$
$$(a*b)^{K+1} = a^{K+1} * b^{K+1}$$

$\therefore P(n)$ is true for $n = K+1$.

$\Rightarrow P(n)$ is true for all $n \in N$.

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

Question:

Prove that $(a*b)^{-1} = b^{-1} * a^{-1}$, for any $a, b \in G$.

Let G be a group and $a, b \in G$.

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

$$(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b$$
$$= b^{-1}*(e*b)$$
$$= b^{-1}*b$$
$$\cdot(b^{-1}*a^{-1})*(a*b) = e \quad -(2)$$

From (1) & (2),

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

$\Rightarrow$ $b^{-1}*a^{-1}$ is the inverse of $a*b$.

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

Question:

) Prove that the only idempotent element of a group $(G,*)$ is the identity element.

If possible, let a be an idempotent element of $(G,*)$ other than e.

Then $a*a = a$

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

Hence the only idempotent element of G is its identity element.

(11) If the permutations of the elements of $(1,2,3,4,5)$ are given by $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$ find $\alpha\beta$, α^2, β^2 and α^{-1}.

$$\begin{array}{rccccc} \beta: & 1 & 2 & 3 & 4 & 5 \\ & \downarrow & & & & \\ & 1 & 2 & 3 & 5 & 4 \\ \alpha & \downarrow & & & & \\ & 2 & 3 & 1 & 5 & 4 \end{array}$$

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

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

$$\begin{array}{rccccc} & 1 & 2 & 3 & 4 & 5 \\ \beta & \downarrow & & & & \\ & 1 & 2 & 3 & 5 & 4 \\ \beta & \downarrow & & & & \\ & 1 & 2 & 3 & 4 & 5 \end{array}$$

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

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

Question:

Every group of prime order is cyclic. Prove:

Let $a\ (\neq e)$ be any element of G.

$\therefore$ $o(a)$ is a divisor of $o(G) = p$, a prime number

$o(a) = 1$ or p ($\because$ divisors of p are 1 and p only)

If $o(a) = 1$, then $a = e$ which is not true.

Hence $o(a) = p$.

ie) $a^p = e$

$\therefore$ G can be generated by any element of G other than e and is of order p.

ie) the cyclic group generated by $a \,(\neq e)$ is the entire G.

ie) G is a cyclic group.

PART-C

Question :

Prove that the necessary and sufficient condition for a non – empty subset H of $(G,*)$ to be a subgroup is $a,b \in H$ implies $a*b^{-1} \in H$

Answer :

Necessry part:

Assume that H is a subgroup of G

Let $a\,,b \in H$

Since H is a subgroup of $G\,,\, b \in H \Rightarrow b^{-1} \in H$

Further H is closed under $* \Rightarrow a*b^{-1} \in H$

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

Assume that H is a non-empty subset of G with $a \in H, b^{-1} \in H \Rightarrow a * b^{-1} \in H$

To prove H is a subgroup of $(G,*)$

For $a \in H$, $a^{-1} \in H$ $\{\because H$ is a non-empty subset of G

$\Rightarrow a * a^{-1} \in H$ i.e) $e \in H$ $\therefore$ H contains e

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

Consider $b \in H \Rightarrow b^{-1} \in H$

For $a \in H, b^{-1} \in H,$ $a * \left(b^{-1}\right)^{-1} = a * b \in H$

Hence $e \in H$, $a^{-1} \in H$, and $a * b \in H$ $\forall a, b \in H$

Hence H is closed, H contains e and H contains a^{-1}

$\therefore$ H is a subgroup of G

Question:

(8) Prove that every Subgroup of a cyclic group is cyclic.

Let $G = \langle a \rangle$.

If H is a trivial (Improper) Subgroup of G then H is obviously cyclic.

Let H be a proper Subgroup of G.

Let $a^s \in H$.

Then a^{-s} is also an element of H $\because -s \in Z$

Thus H Contains positive and negative powers of 'a'.

Let m be the least positive integer s.t $a^m \in H$.

$a^m \in H \Rightarrow (a^m)^q \in H$ (by closure law)

$\Rightarrow a^{mq} \in H$

Also $a^{-mq} \in H$

Let a^t be an arbitrary element of H.

By division algorithm, $\exists$ integers q and r s.t

$$t = mq + r \quad , \quad 0 \le r < m$$

$$a^t \in H \ , \ a^{-mq} \in H$$

$$a^t . a^{-mq} \in H \Rightarrow a^{t-mq} \in H$$

$$a^r \in H.$$

$\Rightarrow m$ is the least positive integer s.t $a^m \in H$ and

$0 \le r < m$. $\Rightarrow$ we must have $r = 0$.

$$\therefore \quad t = mq$$

$$a^t = a^{mq} = (a^m)^q$$

ie) every element of H is expressed as an integral powers of a^m.

$\therefore H$ is a cyclic group generated by a^m.

Question:

Prove that every group of prime order is cyclic.

Suppose G is a finite group of order p.

Where p is a prime number.

$\therefore$ G must contain atleast two elements

$\Rightarrow \exists$ an element 'a' s.t $e \neq a \in G$.

and $O(a) = 2$.

Let us assume $O(a) = m$.

$H = \langle a \rangle$ is a cyclic subgroup of G and

$O(H) = m$

By Lagrange's theorem "m" must be a divisor of p.

But p is a prime.

Hence $m = p$.

$\therefore G = H = \langle a \rangle$.

ie) G is a cyclic group which 'a' generator.

Question :

Show that $(Z,+,\times)$ is an integral domain where Z is the set of all integers

Answer :

We must prove that $(Z,+,\times)$ is a ring

That is to prove $(Z,+)$ is an abelilan group, and $(Z,\circ)$ is an semigroup and $a\circ(b+c)=(a\circ b)+(a\circ c)$, $(b+c)\circ a=(b\circ a)+(c\circ a)$

(i). Clearly $a,b\in Z \Rightarrow a+b\in Z$ and hence $(Z,+)$ is closed

(ii). $a+(b+c)=(a+b)+c \ \forall a,b,c\in Z$ is true

(iii). $\exists e=0\in Z$ such that $a+e=e+a=a \quad \forall a\in Z$

(iv). $\forall a\in Z,\ \exists -a\in Z$ such that $a+(-a)=(-a)+a=o=e$

(v). $a+b=b+a \ \forall a,b\in Z$

Hence $(Z,+)$ is an abelilan group

It is clear that , for $\forall a,b\in Z,\ a\circ b\in Z$ and $a\circ(b\circ c)=(a\circ b)\circ c \ \forall a,b,c\in Z$

Hence $(Z,\times)$ is a semigroup

Also $a\circ(b+c)=(a\circ b)+(a\circ c)$, $(b+c)\circ a=(b\circ a)+(c\circ a)$

Hence $(Z,+,\times)$ is a ring, also a commutative ring that is $a\circ b=b\circ a,\ a+b=b+a$

Also Z has a multiplicative identity 1, that is $a\circ 1=1\circ a=a \ \forall a\in Z$

Further , for $a\neq 0, b\neq 0$ implies $a\circ b\neq 0 \ \forall a,b\in Z$

Hence $(Z,+,\times)$ is an integral domain.

Question :

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

(i). Show that $(R,*)$ is a semigroup

(ii). Find the identity element if it exists

(iii). Which elements has inverse and what are they?

Answer :

(i). To prove $(a*b)*c=a*(b*c)$

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

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

$=a+b+c+2ab+2bc+2ca+4abc$.............(1).

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

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

$a*(b*c)=a+b+c+2ab+2bc+2ca+4abc$.............(2)

From (1) and (2) $(a*b)*c=a*(b*c)$

Hence $(R,*)$ is a semigroup

(ii). To prove $a*e=e*a=a \quad \forall a\in R$

Here 0 is the identity since $a*0=a+0+2a(0)=a$

(iii). Now let $a^{-1}\in R$ such that $a*a^{-1}=e=0$

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

$a+a^{-1}[1+2a]=0 \Rightarrow a^{-1}[1+2a]=-a$

Hence $\boxed{a^{-1}=\dfrac{-a}{1+2a}}$

We can check whether $a*a^{-1}=e$ as follows

$$a*a^{-1}=a+a^{-1}+2aa^{-1}=a-\frac{a}{1+2a}+\frac{2a^2}{1+2a}=\frac{a+2a^2-a+2a^2}{1+2a}=0=e$$

Example Prove that the set $Z_4 = (0, 1, 2, 3)$ is a commutative ring with respect to the binary operation $+_4$ and $\times_4$.

The composition tables for addition modulo 4 and multiplication modulo 4 are given in Tables 5.11(a) and 5.11(b).

Table !

$+_4$	[0]	[1]	[2]	[3]
[0]	0	1	2	3
[1]	1	2	3	0
[2]	2	3	0	1
[3]	3	0	1	2

Table !

$\times_4$	[0]	[1]	[2]	[3]
[0]	0	0	0	0
[1]	0	1	2	3
[2]	0	2	0	2
[3]	0	3	2	1

From the composition tables, we observe the following:

1. All the entries in both the tables belong to Z_4. Hence, Z_4 is closed under $+_4$ and $\times_4$.
2. The entries in the first row are the same as those of the first column in both the tables. Hence Z_4 is commutative with respect to both $+_4$ and $\times_4$.
3. If $a, b, c \in Z_4$, it is easily verified that

$$(a +_4 b) +_4 c = a +_4 (b +_4 c) \text{ and}$$
$$(a \times_4 b) \times_4 c = a \times_4 (b \times_4 c)$$

For example, $3 +_4 (1 +_4 2) = 3 +_4 3 = 2$

Also $(3 +_4 1) +_4 2 = 0 +_4 2 = 2$

and $3 \times_4 (1 \times_4 2) = 3 \times_4 2 = 2$

Also $(3 \times_4 1) \times_4 2 = 3 \times_4 2 = 2.$

Thus, associative law is satisfied for $+_4$ and $\times_4$ by Z_4.

4. $0 +_4 a = a +_4 0 = a$, for all $a \in Z_4$

and $1 \times_4 a = a \times_4 1 = a$, for all $a \in Z_4$

Hence 0 and 1 are the additive and multiplicative identities of Z_4.

5. It is easily verified that the additive inverses of 0, 1, 2, 3 are respectively 0, 3, 2, 1 and that the multiplicative inverses of the non-zero elements 1, 2, 3 are respectively 1, 2, 3.

6. If $a, b, c \in Z_4$, then it can be verified that

$$a \times_4 (b +_4 c) = a \times_4 b +_4 a \times_4 c$$

and $$(b +_4 c) \times_4 a = b \times_4 a +_4 c \times_4 a$$

For example,

$$2 \times_4 (3 +_4 1) = 2 \times_4 0 = 0$$

and $$(2 \times_4 3) +_4 (2 \times_4 1) = 2 +_4 2 = 0$$

i.e., $\times_4$ is distributive over $+_4$ in Z_4

Hence, $(Z_4, +_4, \times_4)$ is a commutative ring with unity.

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

When $a, b \in Z$, $a + b - 1 \in Z$ and $a + b - ab \in Z$

Hence, Z is closed under the operations $\oplus$ and $\odot$.

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

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

Hence, Z is commutative with respect to the operations $\oplus$ and $\odot$.

If $a, b, c \in Z$, then

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

and $$a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + b + c - 2$$

Hence, $$(a \oplus b) \oplus c = a \oplus (b \oplus c).$$

Also $$\begin{aligned}(a \odot b) \odot c &= (a + b - ab) \odot c \\ &= a + b - ab + c - (a + b - ab)c \\ &= a + b + c - ab - bc - ca + abc\end{aligned}$$

and $$\begin{aligned}a \odot (b \odot c) &= a \odot (b + c - bc) \\ &= a + b + c - bc - a(b + c - bc) \\ &= a + b + c - ab - bc - ca + abc\end{aligned}$$

Hence, $$(a \odot b) \odot c = a \odot (b \odot c)$$

Thus, associative law is satisfied by $\oplus$ and $\odot$ in Z.

If z is the additive identity of Z, then

$$a \oplus z = z \oplus a, \text{ for any } a \in Z$$

$$a + z - 1 = a \quad \therefore z = 1$$

i.e.,

If u is the multiplicative identity of Z then $a \odot u = u \odot a = a$

$$a + u - au = a$$

i.e., $u(1 - a) = 0$

i.e.,

$\therefore$ if $a \neq 1$, $u = 0$

Hence 1 and 0 are the additive and multiplicative identities of Z under $\oplus$ and $\odot$.

Now $a \oplus b = b \oplus a = 1$,

If $a + b - 1 = 1$

i.e., if $b = 2 - a$

$\therefore$ The additive inverse of $a \in Z$ is $(2 - a)$

Also $a \odot c = c \odot a = 0$,

If $a + c - ac = 0$

i.e., if $a + c(1 - a) = 0$

i.e., if $c = \dfrac{a}{a-1}$, $(a \neq 1)$

$\therefore$ The multiplicative inverse of $a\ (\neq 1) \in Z$ is $\dfrac{a}{a-1}$.

Finally, if $a, b, c \in Z$,

$$\begin{aligned} a \odot (b \oplus c) &= a \odot (b + c - 1) \\ &= a + b + c - 1 - a(b + c - 1) \\ &= 2a + b + c - ab - ac - 1 \end{aligned}$$

and

$$\begin{aligned} (a \odot b) \oplus a \odot c &= (a + b - ab) \oplus (a + c - ac) \\ &= a + b - ab + a + c - ac - 1 \\ &= 2a + b + c - ab - ac - 1 \end{aligned}$$

Thus, $a \odot (b \oplus c) = a \odot b + a \odot c$.

Similarly, it can be verified that

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

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

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

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

and $$(a, b) \odot (c, d) = (ac, bd), \quad \text{where } a, b, c, d \text{ are real.}$$

Since, $a + c$, $b + d$, ac, bd are all real, S is closed under $\oplus$ and $\odot$.

$$\begin{aligned}(a, b) \oplus (c, d) &= (a + c, b + d)\\ &= (c + a, d + b) = (c, d) \oplus (a, b)\\ (a, b) \odot (c, d) &= (ac, bd)\\ &= (ca, db) = (c, d) \odot (a, b)\end{aligned}$$

Hence S is commutative under the operations $\oplus$ and $\odot$.

Let $(a, b), (c, d), (e, f) \in S$.

Now $[(a, b) \oplus (c, d)] \oplus (e, f)$

$$\begin{aligned}&= (a + c, b + d) \oplus (e, f)\\ &= (a + c + e, b + d + f)\\ &= [a + (c + e), b + (d + f)]\\ &= (a, b) \oplus [c + e, d + f]\\ &= (a, b) \oplus [(c, d) \oplus (e, f)]\end{aligned}$$

Thus, S is associative under $\oplus$.

Similarly it is associative under $\odot$. Now $(0, 0) \in S$.

$$\begin{aligned}(a, b) \oplus (0, 0) = (0, 0) \oplus (a, b) &= (a + 0, b + 0)\\ &= (a, b)\end{aligned}$$

$\therefore$ $(0, 0)$ is the additive identity in S.

Also $\qquad (a, b) \odot (1, 1) = (1, 1) \odot (a, b) = (a, b)$

$\therefore$ (1, 1) is the multiplicative identity in S.

If $(a, b) \in S$, $(-a, -b) \in S$, since a, b are real

Now $\qquad (a, b) \oplus (-a, -b) = (-a, -b) \oplus (a, b) = (0, 0)$

$\therefore$ $(-a, -b)$ is the additive inverse of (a, b)

Now
$$\begin{aligned}(a, b) \odot [(c, d) \oplus (e, f)] &\\ &= (a, b) \odot [c + e, d + f] \\ &= a(c + e), b(d + f) \\ &= (ac, bd) \oplus (ae, bf) \\ &= (a, b) \odot (c, d) \oplus (a, b) \odot (e, f)\end{aligned}$$

Thus, the left distributivity holds.

Similarly the right distributivity also holds.

Now $\qquad (a, 0)$ and $(0, b) \in S$, where $a \neq 0$, $b \neq 0$

and $\qquad (a, 0) \odot (0, b) = (a \times 0, 0 \times b)$

$\qquad\qquad = (0, 0)$, which is the zero element of S.

But $(a, 0)$ and $(0, b)$ are not zero elements of S.

$\therefore$ $(a, 0)$ and $(0, b)$ are zero divisors of S.

Hence, $(S, \oplus, \odot)$ is a commutative ring with zero divisors.

Example Prove that the set S of all real numbers of the form $a + b\sqrt{2}$, where a, b are integers is an integral domain with respect to usual addition and multiplication.

We can easily verify that S is closed with respect to addition and multiplication. S is commutative under + and × and S is associative under + and ×.

Let $c + d\sqrt{2}$ be the additive identity (zero) of $a + b\sqrt{2}$ in S.

Then $\qquad (a + b\sqrt{2}) + (c + d\sqrt{2}) = a + b\sqrt{2}$

$\therefore \qquad a + c = a$ and $b + d = b$

$\therefore \qquad c = 0$ and $d = 0$

Hence, the zero element of S is $0 + 0\sqrt{2}$.

Let $e + f\sqrt{2}$ be the multiplicative identity (unity) of $a + b\sqrt{2}$ in S.

Then $$(a + b\sqrt{2})(e + f\sqrt{2}) = a + b\sqrt{2}$$

$\therefore$ $$ae + 2bf = a \text{ and } af + be = b$$

i.e., $$2bf = a(1 - e) \text{ and } b(1 - e) = af \quad (1)$$

Multiplying, we get $$2b^2 f(1 - e) = a^2 f(1 - e)$$

i.e., $$(2b^2 - a^2) f(1 - e) = 0$$

Since, a and b are arbitrary, $2b^2 - a^2 \neq 0$

$\therefore$ $$f(1 - e) = 0$$

$\therefore$ $$f = 0 \text{ or } 1 - e = 0$$

But, from (1), when $f = 0$, $e = 1$

$\therefore$ unity of S is $1 + 0\sqrt{2}$.

We can easily verify the distributive laws with respect to $\times$ and $+$ in S.

$\therefore$ $(S, +, \times)$ is a commutative ring with unity.

Let us now prove that this ring is without zero divisors.

Let $a + b\sqrt{2}$ and $c + d\sqrt{2} \in S$ such that

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = 0 + 0\sqrt{2} \quad (2)$$

$\therefore$ $$ac + 2bd = 0 \text{ and } bc + ad = 0$$

i.e., $$(a - b)c + d(2b - a) = 0 \text{ or}$$
$$(c - d)a + b(2d - c) = 0$$

$\therefore$ Either $a = 0$ and $b = 0$ or $c = 0$ and $d = 0$

$\therefore$ $a + b\sqrt{2} = 0$ or $c + d\sqrt{2} = 0$, when (2) is true.

i.e., the ring has no zero divisors. Thus, $(S, +, \times)$ is an integral dornain.

Example If S is the set of ordered pairs (a, b) of real numbers and if the binary operations $\oplus$ and $\odot$ are defined by the equations

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

and $$(a, b) \odot (c, d) = (ac - bd, bc + ad),$$

prove that $(S, \oplus, \odot)$ is a field.

As usual, the closure, associativity, commutativity and distributivity can be verified with respect to $\oplus$ and $\odot$ in S.

Also the additive and multiplicative identities can be seen to be $(0, 0)$ and $(1, 0)$ respectively.

Hence, $(S, \oplus, \odot)$ is a commutative ring with unity.

Let (a, b) be a non-zero element of S, i.e., a and b are not simultaneously zero.

Let (c, d) be the multiplicative inverse of (a, b).

Then $$(a, b) \odot (c, d) = (1, 0)$$

i.e., $$(ac - bd, bc + ad) = (1, 0)$$

$\therefore$ $$ac - bd = 1 \text{ and } bc + ad = 0$$

Solving these equations for c and d, we get

$$c = \frac{a}{a^2 + b^2} \text{ and } d = -\frac{b}{a^2 + b^2}$$

$a^2 + b^2 \neq 0$, since a and b are not simultaneously zero.

$\therefore$ c or d or both are non-zero real numbers.

$\therefore$ $\left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2} \right)$ is the multiplicative inverse of (a, b)

Hence, $(S, \oplus \odot)$ is a field.