Algebraic Structures (08)

- 7.1 Algebraic structures with one binary operation: semigroup, monoids and groups
- 7.2 Cyclic groups, Normal subgroups
- 7.3 Hamming Code , Minimum Distance
- 7.4 Group codes ,encoding-decoding techniques
- 7.5 Parity check Matrix ,Maximum Likelihood

Algebraic systems

N = $\{1,2,3,4,\ldots,\infty\}$ = Set of all natural numbers.

Z = { 0, \pm 1, \pm 2, \pm 3, \pm 4, ∞ } = Set of all integers.

Q = Set of all rational numbers, R = Set of all real numbers.

 Binary Operation: The binary operator * is said to be a binary operation (closed operation) on a non empty set A, if

 $a * b \in A$ for all $a, b \in A$ (Closure property).

Ex: The set N is closed with respect to addition and multiplication

but not w.r.t subtraction and division.

 Algebraic System: A set 'A' with one or more binary(closed) operations defined on it is called an algebraic system.

Ex: (N, +), (Z, +, -), (R, +, ., -) are algebraic systems.

Properties

- Commutative: Let * be a binary operation on a set A.
 The operation * is said to be commutative in A if
 a * b= b * a for all a, b in A
- Associativity: Let * be a binary operation on a set A. The operation * is said to be associative in A if (a * b) * c = a *(b * c) for all a, b, c in A

(Addition, Subtraction)

- Idempotent : Let * be a binary operation on a set A.
 The operation * is said to be idempotent in A if
 a * a = a
- Identity: For an algebraic system (A, *), an element 'e' in A is said to be an identity element of A if

a * e = e * a = a for all $a \in A$.

Inverse: Let (A, *) be an algebraic system with identity 'e'. Let a be an element in A. An element b is said to be inverse of A if

a * b = b * a = e

Semi group

- **Semi Group:** An algebraic system (A, *) is said to be a semi group if
 - 1. * is closed operation on A.
 - 2. * is an associative operation, for all a, b, c in A.
- Ex. (N, +) is a semi group.
- Ex. (N, .) is a semi group.
- Ex. (N, -) is not a semi group.
- Monoid: An algebraic system (A, *) is said to be a monoid if the following conditions are satisfied.
 - 1) * is a closed operation in A.
 - 2) * is an associative operation in A.
 - 3) There is an identity in A.

Monoid

- Ex. Show that the set 'N' is a monoid with respect to multiplication.
- Solution: Here, N = {1,2,3,4,.....}
 - 1. <u>Closure property</u>: We know that product of two natural numbers is again a natural number.
 - i.e., a.b = b.a for all $a, b \in N$
 - ... Multiplication is a closed operation.
 - 2. <u>Associativity</u>: Multiplication of natural numbers is associative.

i.e., (a.b).c = a.(b.c) for all $a,b,c \in N$

3. Identity : We have, $1 \in N$ such that

a.1 = 1.a = a for all $a \in N$.

: Identity element exists, and 1 is the identity element.

Hence, N is a monoid with respect to multiplication.

Subsemigroup & submonoid- Self read

Subsemigroup : Let (S, *) be a semigroup and let **T** be a subset of **S**.

If T is closed under operation * , then (T, *) is called a subsemigroup of (S, *).

Ex: (N, .) is semigroup and T is set of multiples of positive integer m then (T,.) is a sub semigroup.

Submonoid : Let (S, *) be a monoid with identity e, and let T be a nonempty subset of S. If T is closed under the operation * and $e \in T$, then (T, *) is called a submonoid of (S, *).

Group

- Group: An algebraic system (G, *) is said to be a group if the following conditions are satisfied.
 - 1) * is a closed operation.
 - 2) * is an associative operation.
 - 3) There is an identity in G.
 - 4) Every element in G has inverse in G.
- Abelian group (Commutative group): A group (G, *) is said to be *abelian* (or *commutative*) if a * b = b * a for all a, b belongs to G.

Algebraic systems

Abelian groups	
Groups	
Monoids	
Semi groups	
Algebraic systems	1

Theorems –Self Study

- In a Group (G, *) the following properties hold good
- 1. Identity element is unique.
- 2. Inverse of an element is unique.
- 3. Cancellation laws hold good

 $a * b = a * c \implies b = c$ (left cancellation law) $a * c = b * c \implies a = b$ (Right cancellation law)

- In a group, the identity element is its own inverse.
- Order of a group : The number of elements in a group is called order of the group.
- Finite group: If the order of a group G is finite, then G is called a finite group.

Ex. Show that, the set of all integers is a group with respect to **addition**.

Solution: Let Z = set of all integers.

Let a, b, c are any three elements of Z.

1. **<u>Closure property</u>** : We know that, Sum of two integers is again an integer.

i.e., $a + b \in Z$ for all $a, b \in Z$

2. <u>Associativity</u>: We know that addition of integers is associative.

i.e., (a+b)+c = a+(b+c) for all $a,b,c \in Z$.

3. **Identity**: We have $0 \in Z$ and a + 0 = a for all $a \in Z$.

... Identity element exists, and '0' is the identity element.

Contd.,

4. Inverse: To each $a \in Z$, we have $-a \in Z$ such that

a + (-a) = 0

Each element in Z has an inverse

5. <u>Commutativity</u>: We know that addition of integers is commutative.

i.e., a + b = b + a for all $a, b \in Z$.

Hence, (Z, +) is an abelian group.

Ex. Show that set of all non zero real numbers is a group with respect to multiplication .(Self Study)

Solution: Let R^{*} = set of all non zero real numbers.

Let a, b, c are any three elements of R^* .

1. <u>Closure property</u> : We know that, product of two nonzero real numbers is again a nonzero real number .

i.e., $a \cdot b \in R^*$ for all $a, b \in R^*$.

2. <u>Associativity</u>: We know that multiplication of real numbers is associative.

i.e., (a.b).c = a.(b.c) for all $a,b,c \in R^*$.

- 3. <u>Identity</u>: We have $1 \in R^*$ and $a \cdot 1 = a$ for all $a \in R^*$.
 - .:. Identity element exists, and '1' is the identity element.
- 4. Inverse: To each $a \in R^*$, we have $1/a \in R^*$ such that

a .(1/a) = 1 i.e., Each element in R^* has an inverse.

Contd.,

5.<u>Commutativity</u>: We know that multiplication of real numbers is commutative.
 i.e., a.b = b.a for all a,b ∈ R*.
 <u>Hence, (R*, .) is an abelian group.</u>

- Ex: Show that set of all real numbers 'R' is not a group with respect to multiplication.
- Solution: We have $0 \in R$.

The multiplicative inverse of 0 does not exist.

Hence. R is not a group.

MODULO SYSTEMS

<u>Addition modulo m</u> $(+_m)$

let m be a positive integer. For any two positive integers a and b $a +_m b = a + b$ if a + b < m $a +_m b = r$ if $a + b \ge m$ where r is the remainder obtained by dividing (a+b) with m.

Ex $14 +_6 8 = 22\% 6 = 4$; Ex $9 +_{12} 3 = 12\% 12 = 0$

<u>Multiplication modulo p</u> (\times_p)

let p be a positive integer. For any two positive integers a and b

$$a \times_{p} b = a b$$
 if $a b < p$
 $a \times_{p} b = r$ if $a b \ge p$ where r is the remainder obtained
by dividing (ab) with p.

Ex.
$$3 \times_5 4 = 2$$
 , $5 \times_5 4 = 0$, $2 \times_5 2 = 4$

Ex.The set G = {0,1,2,3,4,5} is a group with respect to addition modulo 6.

Solution: The composition table of G is

+ 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	

1. <u>Closure property</u>: Since all the entries of the composition table are the elements of the given set, the set G is closed under $+_6$.

Contd.,

2. <u>Associativity</u>: The binary operation $+_6$ is associative in G.

for ex. $(2 +_6 3) +_6 4 = 5 +_6 4 = 3$ and

 $2 +_{6} (3 +_{6} 4) = 2 +_{6} 1 = 3$

- 3. <u>Identity</u>: Here, The first row of the table coincides with the top row. The element heading that row , i.e., 0 is the identity element.
- 4. <u>Inverse</u>: From the composition table, we see that the inverse elements of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively.
- 5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation $+_6$ is commutative.

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

Ex.The set G = {1,2,3,4,5,6} is a group with respect to multiplication modulo 7.

Solution: The composition table of G is

× ₇	1	2	3	4	5	6	
1	1	2	3	4	5	6	
2	2	4	6	1	3	5	
3	3	6	2	5	1	4	
4	4	1	5	2	6	3	
5	5	3	1	6	4	2	
6	6	5	4	3	2	1	

1. <u>Closure property</u>: Since all the entries of the composition table are the elements of the given set, the set G is closed under \times_7 .

Contd.,

2. <u>Associativity</u>: The binary operation \times_7 is associative in G.

for ex.
$$(2 \times_7 3) \times_7 4 = 6 \times_7 4 = 3$$
 and

 $2 \times_7 (3 \times_7 4) = 2 \times_7 5 = 3$

- 3. <u>Identity</u>: Here, The first row of the table coincides with the top row. The element heading that row , i.e., 1 is the identity element.
- 4. <u>Inverse</u>: From the composition table, we see that the inverse elements of 1, 2, 3, 4. 5, 6 are 1, 4, 5, 2, 5, 6 respectively.
- 5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation \times_7 is commutative.

Hence, (G, \times_7) is an abelian group.

Normal Subgroup

A subgroup is called a **normal subgroup** if for any $a \in G$, aH = Ha.

Note 1:

aH = Ha does not necessarily mean that a * h = h * a for every $h \in H$.

It only means that a * $h_i = hj * a$ for some h_i , $hj \in H$.

Note2:

Every subgroup of an abelian group is normal.

Hg = gH, for all $g \in G$, if and only if H is a normal subgroup of G.

Let $H=\{[0]_6, [3]_6\}$, Find left and right cosets in group Z_6 Is it a normal subgroup

• It is abelian group , $a +_6 b = b +_6 a$

+	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

Left coset of H, a H = $\{a * h | h \in H\}$

- $0 H = \{ 0 +_{6} 0, 0 +_{6} 3 \} = \{ 0, 3 \}$ $1 H = \{ 1 +_{6} 0, 1 +_{6} 3 \} = \{ 1, 4 \}$ $2 H = \{ 2 +_{6} 0, 2 +_{6} 3 \} = \{ 2, 5 \}$ $3 H = \{ 3 +_{6} 0, 3 +_{6} 3 \} = \{ 3, 0 \}$
- $4 H = \{ 4 +_6 0, 4 +_6 3 \} = \{ 4, 1 \}$ $5 H = \{ 5 +_6 0, 5 +_6 3 \} = \{ 5, 2 \}$

Given

 $H=\{[0]_6, [3]_6\} \text{ w.k.t} \rightarrow a +_6 b = b +_6 a$

H0,H1,H2,H3,H4,H5=0H,1H,2H,3H,4H,5H

Right coset of H, H a={ h * a | h
$$\in$$
 H }
H 0 = { 0 +₆ 0, 3 +₆ 0 } = { 0, 3 }
H 1 = { 0 +₆ 1, 3 +₆ 1 } = { }
H 2 = { 0 +₆ 2, 3 +₆ 2 } = { }
H 3 = { 0 +₆ 3, 3 +₆ 3 } = { }
H 4 = { 0 +₆ 4, 3 +₆ 4 } = { }
H 5 = { 0 +₆ 5, 3 +₆ 5 } = { }

Hamming distance

- The Hamming distance d(x, y) between two words x, y is the weight $|x \oplus y|$ of $x \oplus y$, (bits in which they differ)
- Eg. d(00111, 11001) = 4
- Find the distance between x and y
- x= 110110 ; y=000101
- x = 001100 ; y =010110
- x = 0100100; y = 0011010

Theorems

- The minimum weight of all non zero words in a group code is equal to its minimum distance
- A code can detect all combinations of k or fewer iff the minimum distance between any two code words is at least k +
 1
- A code can correct all combinations of k or fewer errors iff the minimum distance between any two code words is at least 2 k

+ 1

- Consider the (2,4) encoding function , how many errors will 'e' detect ?
- e (00)=0000 e (10)=0111
- e (01)=1011 e (11)=1100
- Soln: Find the Hamming distance between all pairs
- Since $2 \ge k+1$

k<=1,Will detect 1 or fewer errors

- Consider the encoding function B²→B⁶ defined as follows
- e (00)=0010000 e (10)=100010
- e (01)=010100 e (11)=110001

How many errors can it correct and detect?

Error detection 3>=k+1; k <=2 or fewer errors

Error correction 3>=2k+1;k<=1 or fewer errors

Group Codes- Self Read

An (m,n) encoding function $e:B^m \rightarrow B^n$ is called

a group code if e (B^{m}) = {e(b)|b $\in B^{m}$ }=Ran

(e) is a subgroup of Bⁿ

Subgroup if: Identity element of Bⁿ is in N If x and y belong to N, then $x \oplus y \in N$ If x is in N, then its inverse in N Consider the encoding function B²→B⁵ defined as follows

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

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

is a group code

Soln: Let N={ 00000 , 10101, 01110, 11011 } be set of code words

\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

 $a \oplus b \in N$ which is closed operation, associative, identity, inverse

- 1. Closed operation : For any $a, b \in N$, $a \oplus b \in N$, So N is closed under \oplus operation
- 2. Identity element of B⁵ i.e 00000 also belongs to N
- $00000 \oplus 00000 = 00000 \oplus 00000$
- 01110 \oplus 00000= 00000 \oplus 01110
- 10101 \oplus 00000 = 00000 \oplus 10101
- $11011 \oplus 00000 = 00000 \oplus 11011$
- 3. \oplus Associative operation
- $01110 \oplus (00000 \oplus 10101) = (01110 \oplus 00000) \oplus 10101$
- $01110 \oplus 10101 = 01110 \oplus 10101$
- 11011 = 11011
- 4. Inverse
- Ex: 01110 \oplus 01110 = 01110 \oplus 01110 = 00000

Show that (3,5)encoding function e: B³→B⁶ defined as follows

- e (000)=000000
- e (001)=000110
- e (100)=100101
- e (110)=110111

- e (010)=010010
 - e (011)=010100
 - e (101)=100011
- e (111)=110001

PARITY CHECK MATRIX

Consider the parity check matrix given by H;

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

Determine the group code $e_H : B^2 \rightarrow B^5$

Soln: $B^2 = \{00, 01, 10, 11\}$ Then $e(00) = 00 x_1 x_2 x_3 = B^{5}$ $x_1 = 0 \cdot .1 + 0 \cdot 0 = 0$ $x_2 = 0.1 + 0.1 = 0$ $X_{2} = 0.0 + 0.1 = 0$ e (00) = 00000 Next $e(01) = 01 x_1 x_2 x_3 = B^{5}$ $x_1 = 0 \cdot 1 + 1 \cdot 0 = 0$ $x_2 = 0.1 + 1.1 = 1$ $X_3 = 0.0 + 1.1 = 1$ e (01) = 01011

Next $e(10) = 10 x_1 x_2 x_3 = B^{5}$ $x_1 = 1 \cdot 1 + 0 \cdot 0 = 1$ $x_2 = 1.1 + 0.1 = 1$ $X_3 = 1.0 + 0.1 = 0$ e (10) = 10110 Next $e(11) = 11 x_1 x_2 x_3 = B^{5}$ $X_1 = 1.1 + 1.0 = 1$ $x_2 = 1.1 + 1.1 = 0$ $X_3 = 1.0 + 1.1 = 1$ e (11) = 11101 $e_{ii}: B^2 \rightarrow B^5$ is as above for e (00), e (01), e (10), e (11) e(00) = 00000, e(01) = 01011, e(10) = 10110, e(11) = 11101

Problem 1

Consider the parity check matrix given by H; H = 011011 100010 0 0 1

Determine the group code $e_H : B^2 \rightarrow B^5$

```
e (00) = 11000
```

e (00) = 00000

e (01) = 01011

e (00) = 10011

Problem 2

Consider the parity check matrix given by H;

Determine the group code $e_H : B^3 \rightarrow B^6$

```
e (110) = 110111
e (111) = 111000
```

- e (101) = 101011
- e (100) = 100100
- e (011) = 011100
- e (010) = 010011
- e (001) = 001111

e (000) = 000000

MAXIMUM LIKELIHOOD DECODING TECHNIQUE

Consider the encoding function $B^2 \rightarrow B^4$ defined as followse (00)=0000e (10)=1011e (01)=0110e (11)=1101

Decode the foll words relative to MLD function,

(i) **0101 e(01)** (ii) **1010 e(10)**(iii) **1101 e(11)**

Step 1: Construct Decoding Table(Taking various combinations of 4 bit numbers such as 0000[1],then making MSB as 1 thus we get 0001[2] then shift(R→L) to next bit as 1 we get 0010[3] ,etc. BUT before every next combination we need to check if its in the table already like 0100 [4]. As 0100 is already considered we move to 1000[5]accordingly we proceed for unique values till we decode all

words in the question.		0000	0110	1011	1101
	0000[1]	0000	0110	1011	1101
	<mark>0001</mark> [2]	0001	0111	1010	1100
	<mark>0010</mark> [3]	0010	0100 [4]	1001	1111
	1000 [5]	1000	1110	0011	0101

Consider the encoding function B²→B⁵ defined as follows

- e (00)=**00000** e (10)=**10101**
- e (01)=**01110** e (11)=**11011**

Decode the foll words relative to MLD function,

(i) 11110 (ii)10011(iii)10100

	e (00)	e (01)	e (10)	e (11)
	00000	01110	10101	11011
00000	00000	01110	10101	11011
0000 <u>1</u>	00001	01111	<u>10100</u>	11010
000 <u>1</u> 0	00010	01100	10111	11001
00 <u>1</u> 00	00100	01010	10001	11111
0 <u>1</u> 000	01000	00110	11101	<u>10011</u>
<u>1</u> 0000	10000	<u>11110</u>	00101	01011