18MAB302T-DISCRETE MATHEMATICS

UNIT-4 : Group Theory and Group Codes

Topics

- Binary operation on a set- Groups and axioms of groups
- Properties of groups
- Permutation group, equivalence classes with addition modulo m and multiplication modulo m
- Cyclic groups and properties
- Subgroups and necessary and sufficiency of a subset to be a subgroup
- Group homomorphism and properties
- Rings- definition and examples-Zero devisors
- Integral domain- definition , examples and properties.
- Fields – definition, examples and properties
- Coding Theory – Encoders and decoders- Hamming codes
- Hamming distance-Error detected by an encoding function
- Error correction using matrices
- Group codes-error correction in group codes-parity check matrix.
- Problems on error correction in group codes

INTRODUCTION

- INTRODUCTION
- BASIC ALGEBRA
- ALGEBRAIC SYSTEM
- PROPERTIES OF ALGEBRAIC SYSTEM

MODULE-1

SETS

- A Set is a well defined collection of objects. These objects are otherwise called members or elements of the set. The set is denoted by capital letters A, B,C…
- **Examples** : A - The set of all colors in rainbow , S – the set of even numbers
- **Notations :** Sets are represented in two ways .
- **Roster form :** All the elements are listed. Ex. $A = \{1,3,5,7,9\}$
- **Set builder form :** Defining the elements of the set by specifying their common property .
- Example: $V = \{ x / x \text{ is vowel}\}$
- [the elements of V are a,e,i,o,u]
- $S = \{ x / x = n^2, n \text{ is positive integer less than } 30\}$
- $S=\{1,4,9,16,25\}$

BASIC ALGEBRA

Number system

There are common notations for the number system which are

R – the set of all Real numbers, R^+ - the set of Positive real numbers.

Z, Z^+ , Z^- - set of all Integers, Positive integers, Negative integers.

C, C^+, C^- - set of all Complex, Positive complex, Negative complex numbers.

N – set of all Natural numbers i.e N = {1,2,3,…….}

Q, Q^+, Q^- - set of rational, positive rational, negative rational numbers

BASIC ALGEBRA-Number system

- **Congruence modulo n**

Let n be a positive integer. If a and b are two integers and n divides a – b then we say that "a is congruent to b modulo n" and we write a≡ b(mod n). The integer n is called modulus.

Example : 23 ≡ 3 (mod 5) ; 16 ≡ 0 (mod 4)

- **Congruence classes modulo n**

Let a be an integer. Let [a] denote the set of all integers congruent to a (mod n)

i.e [a] = { x : x ∈ $Z, x \equiv a \ mod\ (n)\} = \{x : x \in Z, x = a + kn\ \}$ for some integer k, then [a] is said to be equivalence class, modulo n, represented by [a]. The set of all congruence classes modulo n is denoted by Z_n .

$\therefore\ Z_n = \{[0], [1], [2], \dots [n-1]\}$

BASIC ALGEBRA-Number system

- **Addition of residue classes**

Let [a], [b] ∈ Z_n then their sum is denoted by $+_n$ and is defined as follows:

$[a] +_n [b] = \begin{cases} [a+b] & if\ a+b<n \\ [r] & if\ a+b \geq n \end{cases}$ where r is the least non negative remainder when a+b is divided by n. hence $0 \leq r \leq n$

Ex. $[1] +_5 [2] = [1+2] = 3$

$[3] +_5 [4] = [2]$ for 3+4=7 >5, 7=1x5+2

$[3] +_5 [2] = [0]$

- **Multiplication of residue classes**

Let [a], [b] ∈ Z_n then their product is denoted by $\times_n$ and is defined as follows:

$[a] \times_n [b] = \begin{cases} [ab] & if\ ab<n \\ [r] & if\ a\,b \geq n \end{cases}$ where r is the least non negative integer when ab is divided by n. hence $0 \leq r \leq n$

Ex. $[2] \times_5 [2] = [4]$; $[2] \times_5 [4] = [3]$.

$$Z_n = \{[0], [1], [2], \dots [n-1]\}$$

Algebraic systems

- A binary operation * on a set A is defined as a function from AxA into the set A itself. .
- A non empty set A with one or more binary operations on it is called an algebraic system.

Examples.

- Set : $N = \{1,2,3 \ldots\}$ – the set of natural numbers, Operation : the usual addition '+' which is a binary operation on N, then $(N, +)$ is an algebraic system.
- Similarly, $(Q, +), (Z, .), (R, +), (C, +)$ … are algebraic systems

General properties of algebraic system

Let $(S, *)$ be an algebraic system, $*$ is the binary operation on S .

- **Closure property** – For all $a,b \in S$, $a * b \in S$
- **Associativity** - For all $a, b, c \in S$, $(a * b) * c = a * (b * c)$,
- **Commutativity** - For all $a,b \in S$, $a * b = b * a$
- **Identity element** – There exists an element $e \in S$, such that

  for any $a \in S$, $a * e = e * a = a$
- **Inverse element** – For every $a \in S$, there exists some $b \in S$ such that

  $a * b = b * a = e$, then b is called the inverse element of a.

MODULE 2

- GROUP
- ABELIAN GROUP
- FINITE AND INFINITE GROUP
- EXAMPLES
- ORDER OF GROUP
- ORDER OF ELEMENT

GROUPS

• Definition : Group

If G is a non empty set and * is a binary operation on G, then the algebraic system {G, *} is called a **group** if the following axioms are satisfied:

1) For all a,b ∈ S, $a * b \in S$ [Closure property]

2) For all a, b, c ∈ G, $(a * b) * c = a * (b * c)$ (Associativity)

3) There exists an element e ∈ G such that, for any a ∈ G, $a * e = e * a = a$ (Existence of identity)

4) For every a ∈ G, there exists an element $a^{-1} \in G$ such that

$$a * a^{-1} = a^{-1} * a = e$$ (Existence of inverse)

Abelian group

The group $(G, *)$ which has commutative property ,

for all a,b ∈ S, $a * b = b * a$, is called an abelian group.

- **Finite/Infinite group**

The group $(G, *)$ is said to be finite or infinite according as the underlying set is finite or infinite.

- **Order of a group**

If $(G, *)$ is a finite group , then the number of elements of G is the order of the group written as $O(G)$ or $|G|$

- **Order of an element**

Let $(G, *)$ be a group and $a \in G$, the least positive integer m, such that $a^m = e,$ the identity element of G, is called order of a and is written as $O(a)=m$

Examples for Groups

1) The set $(Z, +)$, of all integers under addition forms a group.

2) The set of all 2 x 2 non singular matrices over R is an abelian group under matrix addition , but not abelian with respect to matrix multiplication as $AB \neq BA$

3) The set {1,-1,i, -i } is an abelian group under multiplication of complex numbers .

Permutation group

Let A be a non empty set, then a function $f: A \to A$ is a permutation of A if f is both one to one and onto, that is f is bijective. Let S_A denotes the set of all permutations on A. Let $f: A \to A$ and $g: A \to A$ be two functions. Then their composition, denoted by $f \circ g$, is the function $f \circ g : A \to A$ defined by $(f \circ g)(a) = g(f(a))$, the composition of function is the binary operation on S_A .

If A ={1,2,3….}, then the permutation p on A can be written as

$$p = \begin{pmatrix} 1 & 2 & \dots & n \\ p(1) & p(2) & \dots & p(n) \end{pmatrix}$$

For example $p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

If A has n elements S_A has $n!$ Permutations.

Permutation group

- Let $p1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ $and\ p2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$, the composition of these two permutations is defined as

$$p1 \circ p2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

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

MODULE 3

- PROPERTIES OF GROUPS
- PROBLEMS ON GROUPS
- PROBLEMS ON ABELIAN GROUPS

Properties of Group

1. **The identity element of the group (G, *) is unique.**

Proof : If possible , let e1 and e2 be two identities of G.

e1 = e2 * e1 [since e2 is the identity]

=e2 [since e1 is the identity]

i.e e1=e2, the identity element is unique

2. **The inverse of each element of (G, *) is unique.**

Proof : If possible , let a' and a'' be two inverses for a in G.

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

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

$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$

$a' = a''$ implies the inverse is unique.

Properties of Group

3. The cancellation laws are true in a group

Viz, $a * b = a * c \Rightarrow b = c$ [left cancellation law]

and $b * a = c * a \Rightarrow b = c$ [right cancellation law]

Proof :

Let $a * b = a * c$ ----(1)

Since $a \in G, a^{-1} \in G$ exists such that $a * a^{-1} = a^{-1} * a = e$

Pre multiplying (1) by a^{-1}, $a^{-1} * (a * b) = a^{-1} * (a * c)$

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

$$e * b = e * c \quad => b = c$$

Let $b * a = c * a \Rightarrow b = c$ -----------(2)

Since $a \in G, a^{-1} \in G$ exists such that $a * a^{-1} = a^{-1} * a = e$

Post multiplying (2) by a^{-1}, $(b * a) * a^{-1} = (c * a) * a^{-1}$

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

$$b * e = c * e \quad => b = c$$

4. $\boldsymbol{Prove}$ $(a * b)^{-1} = b^{-1} * a^{-1}$, for any a, b ∈ G.

Proof:

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

$$= a * \left(b * (b^{-1} * a^{-1})\right) \text{ [Associativity]}$$

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

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

5. If a , b ∈ G, the equation $a * x = b$ has the unique solution $x = a^{-1} * b$.

6. (G, ∗) cannot have an idempotent element except the identity element.

7. If a has inverse b and b has inverse c , then a = c.

Problems on Groups

1. **Show that the set of all non zero real numbers namely R-{0} forms an abelian group with respect to $*$ defined by $a * b = ab/2$ for all a,b ∈ R-{0}**

Proof : [To prove all the four axioms]

- Closure : if a, b ∈ R-{0} then , ab/2 is also a non zero real number ∈ R-{0}
- Associativity : $a * (b * c) = a * (bc/2) = abc/4$ ---------(1)

  $(a * b) * c = ab/2 * c = abc/4$ -----------(2)

  From (1) and (2) , $a * (b * c) = (a * b) * c$
- Identity element : $a * e = a$

  $ae/2 = a$ *implies* $e = 2$ is the identity element .
- Inverse element : for $a \in R - \{0\}$, $a * a^{-1} = e$

  $\frac{aa^{-1}}{2} = 2 \Rightarrow a^{-1} = \frac{4}{a}$ is the inverse of a

Problems on Groups

2. Prove that the set R -{1} forms an abelian group with respect to $*$ defined by

- **$a * b = (a + b - ab)$, for all $a, b \in R-\{1\}$.**

Proof :

- Closure : If a, b $\in$ R -{1} then , $(a + b - ab)$ is also a real number $\in$ R-{1}
- Associativity :

$$a * (b * c) = a * (b + c - bc) = a + b + c - bc - a(b + c - bc)$$
$$= a + b + c - ab - bc - ac + abc$$
$$(a * b) * c = (a + b - ab) * c = a + b - ab + c - (a + b - ab)c$$
$$= a + b + c - ab - bc - ac + abc$$

Hence , $a * (b * c) = (a * b) * c$.

- Identity element : $a * e = a$

$a + e - ae = a \Rightarrow$ $e = 0$ is the identity element .

- Inverse element : For $a \in R - \{0\}$, $a * a^{-1} = e$

$$a + a^{-1} - aa^{-1} = 0$$

$a^{-1} = \frac{a}{a-1}$ is the inverse of 'a' , ($a \neq 1$).

3. Let G = { f_1, f_2, f_3, f_4 } where $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = \frac{1}{x}$, $f_4(x) = -\frac{1}{x}$ *and* $\circ$ be the composition of functions. Prove that (G, $\circ$) is a group.

Proof :

- Closed : From the table it is
- Associativity :

$$f_1 * (f_2 * f_3) = f_1 * f_4 = f_4$$

$$(f_1 * f_2) * f_3 = f_2 * f_3 = f_4$$

Hence , $f_1 * (f_2 * f_3) = (f_1 * f_2) * f_3$.

- Identity element : From the table, we can see that f_1 is the identity element.
- Inverse element : Inverse of every element is the element itself

4. Let A={1,2,3}, S_A be the set of all permutations of A, then prove that with respect to right composition of permutations $\circ$, { $S_A, \circ$ } is an abelian group.

Proof :

Let $S_A = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ where

$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,

$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ and $p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\circ$	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_4	p_3	P_6	p_5
p_3	p_3	p_4	p_1	p_2	P_4	p_1
p_4	p_4	p_3	p_2	p_1	p_3	p_2
p_5	p_5	p_6	p_4	p_3	p_1	p_4
p_6	p_6	p_5	p_1	p_2	p_4	p_1

- From the above table, for any two or three elements we can prove closure and associative property.

- The identity element is p_1 and the inverse of any element is the element itself.

Problems on Groups

4. Let $a \neq 0$ be a fixed real number and $G = \{a^n : n \in Z\}$, Prove that G is an abelian group under multiplication .

Proof :

- Closed : if $a^{n1}, a^{n2} \in$ G then $a * b = a^{n1+n2} \in$ G as n1+n2 $\in$ Z
- Associativity : For $a^{n1}, a^{n2}, a^{n3} \in$ G

$$a^{n1} * (a^{n2} * a^{n3}) = a^{n1} * a^{n2+n3} = a^{n1+n2+n3}$$

$$(a^{n1} * a^{n2}) * a^{n3} = a^{n1+n2} * a^{n3} = a^{n1+n2+n3}$$

- Identity element - $a^n * a^e = a^n$

$a^{n+e} = a^n$ implies e=0 and $a^e = a^0 = 1$ is the identity element

- Inverse element – for $a \in R, a^n * a^{n1} = a^0 => n + n1 = 0 => n1 = -n$

$a^{n1} = a^{-n}$ is the inverse of a^n

5. For any group (G, *) if $a^2 = e$ with $a \neq e$, then prove that G is abelian
[Or, if every element of a group (G, *) is its own inverse, then G is abelian]

Proof:

Let $a^2 = e$.

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

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

implies $a = a^{-1}$

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

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

$b * a = a * b$, G is abelian.

6. Let $(G,*)$ be a group. Prove that G is abelian if and only if $(a*b)^2 = a^2 * b^2$

Proof:

Let G be abelian,

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

$= a*(b*(a*b))$ [Associativity]

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

$= a*(a*b)*b$ [commutativity]

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

Now , suppose $(a*b)^2 = a^2 * b^2$

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

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

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

$(b*a)*b = (a*b)*b$ [Associativity]

$b*a = a*b$ ----commutative.

Thus G is abelian.

- Exercises :

1. The set $\left\{\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}\right\}$ is an abelian group under matrix multiplication.

2. The set $\{0,1,2,3,4\}$ is a finite abelian group of order 5 under addition modulo 5.

3. The set $\{1,3,7,9\}$ is an abelian group under multiplication modulo 10.

MODULE 4

- SUBGROUPS
- EXAMPLES FOR SUBGROUP
- CONDITIONS FOR SUBGROUP
- PROBLEMS ON SUBGROUPS

Problems on subgroups

1. The intersection of two subgroups of a group G is also a subgroup of G .

Proof:

Let H_1 and H_2 be any two subgroups of G. $H_1 \cap H_2$ is a non-empty set, since, at least the identity element e is common to both H_1 and H_2

Let $a \in H_1 \cap H_2, then\ a \in H_1\ and\ a \in H_2$

Let $b \in H_1 \cap H_2, then\ b \in H_1\ and\ b \in H_2$

H_1 is a subgroup of G, $a * b^{-1} \in H_1$ $a\ and\ b\ \in H$

H_2 is a subgroup of G, $a * b^{-1} \in H_2$ $a\ and\ b\ \in H$

$\therefore a * b^{-1} \in H_1 \cap H_2$ implies $H_1 \cap H_2$ is a subgroup of G.

SUBGROUPS

If $\{G, *\}$ is a group and $H \subseteq G$ is a non-empty subset of G, called **subgroup** of G , if H itself forms a group .

Theorem:

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

2. Show that the set $\{a + bi \in C | a^2 + b^2 = 1\}$ is a subgroup f (C, •) where • is the multiplication operator.

Proof:

Let H = $\{a + bi \in C | a^2 + b^2 = 1\}$, consider two elements $x + iy, p + iq \in H$ *such that*

$x^2 + y^2 = 1, p^2 + q^2 = 1$ and the identity element of C is 1+0i

Consider $(x + iy)\ (p + iq)^\wedge(-1) = (x + iy)(p - iq) = xp + yq + i(yp - xq)$

Now $(xp + yq)^2 + (yp - xq)^2 = x^2p^2 + y^2q^2 + 2xpyq + y^2p^2 + x^2q^2 - 2ypxq$

$$= x^2(p^2 + q^2) + y^2(p^2 + q^2) = 1$$

$\therefore\ (x + iy)(p + iq)^{-1} \in H$, H is a subgroup.

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

Proof:

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

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

$x^2 = e$

$x^{-1}.x^2 = x^{-1}.e \implies x = x^{-1}$

Hence, $if\ x \in H, x^{-1} \in H$ [inverse exists]

Let $x, y \in H$, since G is abelian, $xy = yx = y^{-1}x^{-1} = (xy)^{-1}$

∴ $(xy)^2 = e$. i.e $xy \in H$

Thus, if $x, y \in H, we\ have\ xy \in H$ [closed]

Thus H is a subgroup.

4. Union of two subgroups of (G,*) need not be a subgroup of (G,*).

Module 5

- Cyclic groups
- Examples
- Properties
- Problems

Cyclic group

A group (G, $*$) is said to be a **cyclic group** if there exists an element a$\in G$ such that every element of G can be expressed as some integral power of a, **a is called generator of G**.

We write G=(a)

Examples :

1. Let G={1,-1, i, -i} and G is a group under multiplication. It is cyclic with the generator i

   (i.e.) G=(i) or G=(-i)

2. Let G=$\{1, \omega, \omega^2\}$ is a cyclic group under multiplication generated by ω . ω^2 is also a generator.

3. (Z , +) is a cyclic group with generator 1. Note -1 is also a generator.

Properties of cyclic groups

1. Every cyclic group is abelian

Proof:

Let $(G,*)$ be a cyclic group with generator a. Let $x, y \in G$ $such\ that\ x = a^m, y = a^n$

$$x * y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = y * x$$

Therefore $(G,*)$ abelian.

2. Let (G, ∗) be a cyclic group generated by a , then a^{-1} is also a generator of G.

Proof:

Let (G, ∗) be a cyclic group generated by a , then $for\ x \in G\ then\ x = a^n\ for\ some\ n \in Z$

$$x = (a^{-1})^{-n}, -n \in Z$$

$\therefore$ a^{-1} is also a generator of G.

3. Any subgroup of a cyclic group is itself a cyclic group.

Proof :

Let (G, $*$) be a cyclic group generated by a and H be a subgroup of G.

if $a^k \in H$ $then$ $a^{-k} \in H$. Let m be the least positive integer such that $a^k \in H$

we have to prove that $H = (a)^m$. Let $c \in H$. $\therefore c \in G$

$c = a^n$ for some $n \in Z$

Now $n, m \in Z$, there exists integers q and r such that $n = mq + r$, $0 \leq r < m$ by division algorithm.

Now $c = a^n = a^{mq+r} = a^{mq} * a^r$

$a^r = a^{-mq} * c = (a^m)^{-q} * c \in H$

Since $c \in H, (a^m)^{-q} \in H$ and H is a subgroup. But $0 \leq r < m$ and m is the least positive integer such that $a^m \in H$. Therefore r = 0

$\therefore c = a^{mq} = (a^m)^q$

Hence every element of H can be written as an integer power of a^m. $\therefore H = (a^m)$ is a cyclic group.

4. The order of a cyclic group is the same as the order of its generator.

5. A finite group of order n containing an element a of order n is cyclic.

Problems

-

1. Find the number of generators of a cyclic group of order 5.

Let G = (a) be a cyclic group of order 5. Then G = $\{a, a^2, a^3, a^4, a^5 = e\}$.

Since (1,5) =1, (2,5) =1, (3,5) =1, (4,5) =1.

The generators are a, a^2, a^3 *and* a^4.

The number of generators is 4.

2. Find the number of generators of a cyclic group of order 8 .

Let G = (a) be a cyclic group of order 5. Then G=$(a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$.

Since (1,8)=1, (3,8)=1, (5,8)=1, (7,8)=1.

The generators are a, a^3, a^5 *and* a^7.

The number of generators is 4.