DISCRETE STRUCTURES
UNIT III

Group Theory

Algebraic System

If there exists a system such that it consist of a non-empty set and one or more operations on that set, then that system is called an algebraic system. It is generally denoted by (A, o_1,$o_{2,\ldots\ldots}$$o_n$) Where A is a non-empty set and o_1,o_2,……..o_n are operations on A.

An algebraic system is also called an algebraic structure because the operations on the set A define a structure on the elements of A.

Ex. (N,+), (Q,-), (R.+) etc..

all are the example of algebraic system or structure

Operations On Set

Operations are functions which are use to assign a unique element to any given pair of elements.

EX. A+B=C   A∩B=C   A * B=C

Binary Operation Let S be a nonempty set .An operation on S is a function from S X S into S and it will be written by

a*b   or sometimes   ab

In this case the algebraic system is denoted by (S,$_*$)

Unary Operation A function from S into S is called unary operation. For example, the absolute value |n| of an integer n is a unary operation on Z.

Ternary Operation A function from S X S X S into S is called ternary operation

N-ary Operation A function from S X S X S…..X S (up to n factors) in to S is called n-ary operation.

Closed Operation

Suppose we have a non-empty set A.

A function from A X A in to A is said to be a binary operation that is closed if a and b belongs to A then a * b must also belongs to A.

Ex. Let A and B denote, respectively the set of even and odd positive integers. Then A is closed under addition and multiplication since the sum and product of any even numbers are even. But, B is closed under multiplication only not for addition because sum of two odd numbers can be even also.

3+5=8

Ex.Addition(+) and multiplication (*) are closed operation on N. However subtraction(-) and division(/) are not operations on N. 2-9 and 7/3 are not positive integers.

Closed Operation

Example: Let S = {0, 1, -1}. Then addition + is not an operation on S since the sum 1+1 is not an element of S. On the other hand, multiplication is an operation on S.

Properties Of Operation

Suppose I is a set of integers. consider the algebraic system (I,+,*) where + and * are the operation of addition and multiplication on I.

1) Associative

For any a, b, c $\in$ I

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

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

2) Commutative

For any a, b $\in$ I

$a + b = b + a$

$a * b = b * a$

3) Identity Element

For 0, a $\in$ I, a + 0 = 0 + a =a (0 is the identity element for +)

For 1, a $\in$ I , a * 1=1 * a =a (1 is the identity element for s *)

4) Inverse element

For each a ∈ I there exists an element in I denoted by –a and called inverse of a

$$a + (-a)=0$$

5) Distributive

For any a, b, c ∈ I

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

6) Cancellation Property

For any a, b, c ∈ I and a # 0

$$a * b=a * c \Rightarrow b=c$$

Semigroup

Let (A,*) be an algebraic system where * is a binary operation on A . (A,*) is called a semigroup if the following conditions are satisfied:

-- * is closed operation.

-- * is an associative operation.

Ex1. Let A be the set of all positive even integers {2,4,6…} and + be the ordinary addition operation of integers. Since + is a closed operation on A and is also an associative operation that's why (A,+) is a semigroup.

Ex2. (N,X) is a semigroup. For a, b $\in$ N = =>a * b $\in$ N and a, b, c $\in$ N

$$= => \quad (a * b) * c = a * (b * C)$$

SUBSEMI-GROUP

Let A be a nonempty subset of semigroup S. Then A is called a subsemi-group of S if A itself is a semigroup with respect to the operation on S .Since the element of A are also element of S, the associativity law automatically holds for the elements of A. Therefore ,A is a subsemi-group of S if and only if A is closed under the operation on S.

Ex. Let A and B denote respectively the set of even and odd positive integers. Then (A,X) and (B,X) are subsemi-groups of (N,X) since A and B are closed under multiplication.
(A,+) is a subsemi-group of (N,+) since A is closed under addition.
(B,+) is not a subsemi-group of (N,+) since B is not closed under addition.

Monoids

Let (A,*) be an algebraic system where * is a binary operation on A . (A,*) is called a monoid if the following conditions are satisfied:

-- * is closed operation.

-- * is an associative operation.

-- There is an identity.

Ex. Let N be the set of natural numbers. Then (N,+) and (N,X) are semigroups. (N,X) is a monoid since it has identity element 1. However (N,+) is not a monoid since addition in N has no zero element.

Submonoid

Let (S,*) is a monoid with identity e and let T be a nonempty subset of S. If T is closed under operation * And e ∊ T then (T,*) is called a submonoid of (S,*).

Inverse Element

Suppose (A,*) be an algebraic system with an identity e and a be an element in A. An element b is said to be a left inverse of a if

$$b * a = e$$

An element b is said to be a right inverse of a if

$$a * b = e$$

An element b which is both a left and right inverse of a is called an inverse of a and is said to be invertible or regular.

PROPERTIES OF INVERSE ELEMENT

1)The inverse of the identity element e is e

$$e * e = e, e^{-1} = e$$

2) The inverse of the inverse of any element is the element itself.

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

Groups

For a nonempty set G, a Group (G,*) is an algebraic system in which the binary operation * on G satisfies the below four conditions—

1) Operation * must be closed.

2) For all $x, y, z \in G$

$$X * (Y * Z) = (X * Y) * Z \quad \text{(ASSOCIATIVITY)}$$

3) There exists an element $e \in G$ such that for any $x \in g$

$$X * e = e * X = X \qquad \text{(IDENTITY)}$$

4) For every $x \in G$ there exists an element denoted by $x^{-1} \in G$ such that

$$X^{-1} * X = X * X^{-1} = e \quad \text{(INVERSE)}$$

Ex. For algebraic system (I, +) where I is the set of all integers and + is the ordinary addition operation of integers, (I,+) is a group with 0 being the identity and the inverse of n being –n.

Abelian Group

A group (A,*) is called commutative or abelian group if * is a commutative operation.

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

Ex. Group (I,+) is a example of abelian group.

Finite And Infinite Group

- If a group contains a finite number of distinct elements then it is called finite group
- If a group contains an infinite no of elements then it is called infinite group.
- The no of elements in a finite group is called order of group
- An infinite group is said to be of infinite order.

Properties Of Groups

1) The identity element of a group is unique :

Proof)

Suppose e and e’ are two identity elements of group G with respect to operation *.

Then e * e’=e if e’ is identity
e * e’=e’ if e is identity

But e and e’ is unique element of G ,therefore
e * e’ = e and e * e’=e’ = => e= e’

hence the identity element in a group is unique

Properties Of Groups

2) The inverse of each element of a group is unique

means $a^{-1} * a = a * a^{-1} = e$

Let a be any element of group G and let e be the identity element . Suppose there exist a^{-1} and a’ two inverse of a in G then

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

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

Now we have

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

$= a^{-1}$

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

$= a'$

But $a^{-1} *(a * a')=(a^{-1} * a) * a'$ as in a group composition is associative

so $a^{-1} = a'$

3) If the inverse of a is a^{-1} then the inverse of a^{-1} is a

if e is the identity element ,we have $a^{-1} * a = e$

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

$[\,(a^{-1})^{-1} * a^{-1}] * a = (a^{-1})^{-1}$

(composition in G is associative and e is identity element)

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

$a \quad = (a^{-1})^{-1}$

4) The inverse of the product of two elements of a group G is the product of the inverse taken in the reverse order

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

suppose a and b are any two elements of G if a^{-1} and b^{-1} are inverse of a and b respectively then,

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

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

now, $(a * b) * (b^{-1} * a^{-1}) =[(a * b) * b^{-1}] * a^{-1}$ (by associativity)

$= [a *(b * b^{-1})] * a^{-1}$ (by associativity)

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

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

$= e$

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

$$\begin{aligned} &= b^{-1} * [a^{-1} * (a * b)] \\ &= b^{-1} * [(a^{-1} * a) * b] \\ &= b^{-1} * (e * b) \\ &= b^{-1} * b \\ &= e \end{aligned}$$

hence we have,

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

By definition of inverse

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

5) Cancellation law hold good in a group i.e.

$$\mathbf{a*b=a*c == > b=c}$$

$$\mathbf{b*a=c*a == > b=c}$$

Let a $\in$ G then a $\in$ G = => G such that $a^{-1} * a=e=a * a^{-1}$

assume that, $a * b=a*c$

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

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

$e * b=e * c$

$b=c$

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

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

$b*e=c*e$ => $b=c$

6) G is a group with binary operation * and if a and b are any elements of G ,then the linear equation

a* x=b and y * a=b have unique solution in G

$a \in G ==> a^{-1} \in G$

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

Substituting $a^{-1} * b$ for x in the equation a * x=b

we obtain

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

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

$e * b=b$

$b=b$

Thus $x= a^{-1} * b$ is a solution of the equation a * x=b

To show that solution is unique let us suppose that equation $a * x=b$ has two solution given by

$$x= x_1 \text{ and } x= x_2$$

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

$$a * x_1= a* x_2=b$$

$$x_1 =x_2$$

Similarly we can prove that $y * a=b$

has the unique solution $y = b * a_{-1}$

Subgroup

Let (A,*) be a group and B be a subset of A. (B,*) is said to be a subgroup of A if (B,*) is also a group by itself. To check whether B is a subgroup of A or not check:

1) * must be closed operation on B

2) * must be associative operation

3) Since there is only one element e in A such that e*x=x*e=e

for all x in A then e must also in B. or we can say, the identity of (A,*) must be an identity of (B,*).

4) Since the inverse of every element A is unique, for every element b in B its inverse is also in B.

Ex. If (I,+) is an algebraic system, where I is the set of all integers and + is the ordinary addition operation clearly (I,+) is a group. For it (E,+) is a subgroup where E is the set of all even integers.

Cyclic Group

A group G is called cyclic if for some a ∈ G, every element x ∈ G is the form of a^n ,where n is some integer .The element a is called the generator of G .

There may be more then one generator of a cyclic group .

If G is a cyclic group generated by a, then we shell write G={a} or G=(a).the elements of G will be of the form

$\ldots..a^{-3},a^{-2},a^{-1},a^{0}(=e),a,a^{2},a^{3}\ldots..$

Ex. Group G={1,-1,i,-i} is cyclic for it the generators are I and –i.

Properties Of Cyclic Group

Every cyclic group is abelian

The generator of a cyclic group of order n are all the elements a^p , P being prime to n and 0<p<n.

Permutation Group

Suppose P is a finite set having n distinct elements . Then a one one mapping of P onto itself is called a permutation of degree n .

Degree:- the number of elements in the finite set P is known as degree of permutation.

Composition Table

Also known as cayley’s composition table . It is basically use for performing operation on finite set.

STEPS FOR CONSTRUCTING THE COMPOSITION TABLE

1) If we have a set of n elements then make a table of (n+ 1) row and (n+1)column. S={1,-1,i,-i } and operation = multiplication ‘*’Make a table with 5 row and 5 column

*	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

2) (ith entry on the left) . (jth entry on the top) =

(entry on the ith row and jth column intersect)

Imp point:-

1) element of the set should be written in same order both for top and left border.

2) Generally a table which define ‘.’ operation is called multiplication table and a table which define ‘+’ operation is called addition table.

Use Of Composition Table

Composition table is useful in examining the following axioms:-

1) Closure Property :- if all the elements of the table belong to the set G then G is closed under the composition * say . If any of the elements of the table does not belong to the set , the set is not closed.

2) Existence of identity:- The element (in the vertical column) to the left of the row identical to the top row (border row) is called an identity element in the G with respect to operation '*'.

Use Of Composition Table

Composition table is useful in examining the following axioms:-

3) Existence of inverse:- if we mark the identity elements in the table then the element at the top of the column passing through the identity element is the inverse of the element in the extreme left of the row passing through the identity element and vice versa.

4) Commutativity:- if the table is such that the entries in every row coincide with the corresponding entries in the corresponding column then it is commutative.

a) Prove that set of cube root of unity is an abelian finite group with respect to multiplication

b) G={0,1,2,3,4} is a finite abelian group of order 5 w.r.t addition modulo 5

COSETS

Let (A,*) be an algebraic system ,where * is a binary operation . Let a be an element of A and H be a subset of A.

The **left coset** H of with respect to a, which we shell denote a * H ,is the set of elements {a * x for all x ∈ H}.

The **right coset** of H with respect to a, which we shell denote H * a is the set of elements {x * a for all x ∈ H}

NORMAL SUBGROUP

A sub group (H,*) of (G,*) is called a normal subgroup if for any a ∈ G

aH = Ha

Means left and right cosets must be coincide.

ISOMORPHISM

Let (S, o) and (T,*) be two algebraic system. A function f: S --> T is called an isomorphism from (S, o) to (T, *) if it is a one-to-one onto correspondence from S to T , and if

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

If two algebraic system (S, o) and (T,*) are isomorphic then it is denoted by S ~ T

To show that two algebraic structure (S , o) and (T, *) are isomorphic we use the following procedure:

1) Define a function f: S→ T with Dom (f)=S

2) Show that f is one one

3) Show that f is onto

4) Show that f (a o b) = f(a) * f(b)

Automorphism

An isomorphism from an algebraic system (A,*) to (A,*) Is called automorphism on (A,*)

Homomorphism

Let (S, o) and (T,*) be two algebraic system. A function f: S --> T is called an homorphism from (S, o) to (T, *) if it is a onto correspondence from S to T , and if

$$f\,(a \circ b\,) = f\,(a) * f\,(b)$$

To show that two algebraic system (S , o) and (T, *) are homorphic we use the following procedure:

1) Define a function f: S→ T with Dom (f)=S

2) Show that f is onto

) Show that f (a o b) = f(a) * f(b)

Rings

An algebraic structure (R,+,*) where R is a nonempty set and + and * are two defined operations on R that is addition and multiplication ,is called Ring if for all a,b,c in R the following axioms are satisfied:

1) (R,+) is an abelian group

a) $a+b \in R$ (closure law for addition)

b) $(a+b)+c=a+(b+c)$ (Associative law)

c) R must have an identity to be denoted by 0.

d) There must be inverse for each and every element of R

e) $a+b=b+a$

Rings

2) (R,*) is a semigroup

a) $a*b \in R$ (closure law)

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

3) Multiplication is left and right distributive over addition

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

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

Types Of Rings

1) **Commutative Rings** :- if the multiplication composition in R is commutative

$$ab=ba \text{ for all } a,b \in R$$

2) **Rings with unity element**:- A ring R is said to be a ring with unity element If R has a multiplicative identity i.e. if there exists an element in R denoted by 1 ,such that

$$a= a*1=a \quad \text{for all } a \in R$$

Types Of Rings

3) Rings with or without Zero divisor

a) A ring element a is not equal to 0 is called a divisor of Zero if there exists an element b is not equall to zero in the ring such that either

ab=0 or ba=0

We can also say that a ring R is without Zero divisor if the product of no two non zero elements is zero i.e. if

ab=0 either a=0 or b=0 or both a=0 and b=0

b) Cancellation laws in a ring this law holds in a ring if

ab=ac (a $\neq$ o) ==> b=c

ba=ca (a $\neq$ o) ==> b=c

c) Divison Ring:- A ring is called divison Ring if its non-Zero elements form a group under multiplication

d) Pseudo Ring:- A non empty set R with operation addition and multiplication is satisfying all the postulates except distributive law is called psuedo ring.

Integral Domain

A ring is an integral domain if

1) It is commutative
2) It posses an unit element
3) It has at least two elements
4) It is without Zero divisor

Integral Domain

The system (D,+,*) is an integral domain if the following postulates are satisfied

1) (D,+) must be an abelian group

- closure property
- Associativity of addition
- Existence of Zero or additive identity
- Existence of additive inverse or negative
- commutativity of addition

2) The system (D,*) is an abelian semigroup with unity

closure property

associtivity of mutiplication

Existence of unity

commutativity of multiplication

3) Mutiplication composition is right and left distributive with respect to addition.

a*(b+c) = a*b+a*c

(b+c)*a = b*a+c*a

4) If the product of two element is Zero then one of them atleast is Zero.

a * b=0 = => a=0 or b=0

Field

The system (F,+,*) is a field if the following postulates are satisfied:

1) (F,+) must be an abelian group

---closure property
---Associativity of addition
---Existence of Zero or additive identity
---Existence of additive inverse or negative
---commutativity of addition

2) Mutiplication composition is right and left distributive with respect to addition.

a*(b+c) = a*b+a*c
(b+c)*a = b*a+c*a

Field

3) The subset of non zero element of F forms an abelian multiplicative group and so, we have the following properties

---closure property
---Associativity of multiplication
---Existence of multiplicative identity
---Existence of multiplication inverse
---commutativity of multiplication

Factor Group

Let G be a group and H be a normal subgroup of G. Let G/H denotes the set of right (left) cosets of H in G. Then G/H is a group called factor group or quotient group under the coset multiplication defined by

$$(aH)\,(bH) = abH$$