

## LECTURE PLAN

Department: Computer Science

Class: 3<sup>rd</sup> CE 'A' & 'B'

Subject code: MA2311

Subject: Discrete Mathematics

Period 1

### Unit 1      Algebraic Structures

#### Definition 1 - Algebraic System

A non-empty set  $G$  together with one or more  $n$ -ary operations say  $*$  is called an algebraic system or algebraic structure or algebra. i.e.  $(G, *)$

#### Properties of Binary operations -

(i) Closure property:-

$$a * b = x \in G, \text{ for } a, b \in G.$$

(ii) Commutativity:-

$$a * b = b * a, \text{ for all } a, b \in G$$

(iii) Associativity:-

$$(a * b) * c = a * (b * c), \text{ for all } a, b, c \in G$$

(iv) Identity element:-

$$a * e = e * a = a \text{ for all } a \in G$$

(v) Inverse element:-

If  $a * b = b * a = e$ , then  $b$  is called the inverse of  $a$  and is denoted by  $b = a^{-1}$ .

Sub code & Subject : 442311, Discrete Mathematics

Period : 2

### Semigroups and Monoids:-

#### Definition:- Semigroup

If a non-empty set  $S$  together with the binary operation  $*$  satisfying the following two properties

- (a) closure property
- (b) Associative property.

#### Definition:- Monoid

A semigroup  $(S, *)$  with an identity element w.r. to  $*$  is called Monoid.

#### Definition:- cyclic monoids:-

A monoid  $(M, *)$  is said to be cyclic, if every element of  $M$  is of the form  $a^n$ ,  $a \in M$  and  $n$  is an integer.

$$\text{if } x = a^n$$

such a cyclic monoid  $(M, *)$  is said to be generated by the element  $'a'$ . Here  $a$  is called the generator of the cyclic monoid.



Sub code & Subject : MA2311, Discrete Mathematics

Period 3

### Morphism of subgroups:-

#### Definition:- Semigroup Homomorphism:-

Let  $(S, *)$  and  $(T, \circ)$  be any two semigroups with binary operation  $*$  and  $\circ$  respectively.

#### Semigroup Monomorphism:-

A one-one semigroup homomorphism is called a semigroup monomorphism.

#### Semigroup Epimorphism:-

A on-to semigroup homomorphism is called a semigroup epimorphism.

#### Isomorphism:-

A one-one, onto semigroup homomorphism is called an isomorphism.

#### Semigroup Isomorphism:-

Two semigroups  $(S, *)$  and  $(T, \circ)$  are said to be isomorphic, if there exists a semigroup isomorphism between them.

#### Semigroup Endomorphism:-

A homomorphism of a semigroup into itself is called a semigroup endomorphism.

Subject code & Subject : MA 2311 / Discrete Mathematics

Period 4

### Groups:-

Definition:- A non-empty set  $G$  together with the binary operation  $*$ , is  $(G, *)$  is called a group if  $*$  satisfies the following conditions

- (i) closure property  $a * b \in G$ , for all  $a, b \in G$
- (ii) Associative property :  $(a * b) * c = a * (b * c)$ , for all  $a, b, c \in G$
- (iii) Identity property : There exist an element  $e \in G$  called the identity element such that  $a * e = e * a = a$  for all  $a \in G$ .
- (iv) Inverse property : There exist an element  $a^{-1}$  called the inverse of 'a' such that
$$a * a^{-1} = a^{-1} * a = e, \text{ for all } a \in G.$$

### Definition:-

In a group  $(G, *)$ , if  $a * b = b * a$  for all  $a, b \in G$  then the group  $(G, *)$  is called an abelian group.

Eg  $(\mathbb{Z}, +)$  is an abelian group.

### Definition: Order of a group.

The number of elements in a group  $G$  is called the order of the group and is denoted by  $O(G)$ .

It is denoted by  $O(G)$  or  $|G|$ .



### Subgroups

Let  $(G, *)$  be a group. Let  $e$  be the identity in  $G$ .

Let  $H$  be a subset of  $G$ . If  $(H, *)$  itself is a group then  $H$  is called the subgroup of  $G$ .

i.e.  $H$  is itself a group with the same operation  $*$  and the same identity  $e$ .

In other words,  $(H, *)$  is said to be a subgroup of  $(G, *)$  if

- (i)  $e \in H$ , where  $e$  is the identity in  $G$ .
- (ii) For any  $a \in H$ ,  $a^{-1} \in H$
- (iii) For  $a, b \in H$ ,  $a * b \in H$ .

### Theorem

1. The necessary and sufficient condition that a non empty subset  $H$  of a group  $G$  to be a subgroup is

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

2. The intersection of two subgroups of a group is also a subgroup of the group.

Subcode & Subject: MA2311 / Discrete Mathematics

### Morphism of Groups:-

Let  $(G, *)$  and  $(H, \Delta)$  be any two groups. period 6

A mapping  $f: G \rightarrow H$  is said to be a homomorphism if

$$f(a * b) = f(a) \Delta f(b) \text{ for any } a, b \in G.$$

#### Theorem:-

1. Homomorphism preserves identities.
2. Homomorphism preserves inverses.

#### Theorem:-

Let  $f: G \rightarrow G'$  be a group homomorphism and  $H$  is a subgroup of  $G'$ , then  $f^{-1}(H)$  is a subgroup of  $G$ .

#### Theorem:-

Let  $f$  be a homomorphism from  $(G, *)$  into  $(G', \Delta)$ .

Let  $f(G)$  be the homomorphic image of  $G$  into  $G'$ . then  $f(G)$  is a subgroup of  $G'$ .



Sub code & Subject: MA2311 / Discrete Mathematics Period 7

### Kernel of a Homomorphism:-

Let  $f: G \rightarrow G'$  be a group homomorphism. The set of elements of  $G$  which are mapped into  $e'$  (identity in  $G'$ ) is called the kernel of  $f$  and it is denoted by  $\ker(f)$ .

$$\text{i.e. } \ker(f) = \{x \in G / f(x) = e'\}, e' \text{ (identity in } G').$$

### Example:-

1.  $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$  defined by  $f(x) = 2x$ .

Then  $\ker(f) = \{0\}$ .

2.  $f: (\mathbb{R}^*, \cdot) \rightarrow (\mathbb{R}^*, \cdot)$  defined by  $f(x) = \{x\}$

Then  $\ker(f) = \{1, -1\}$ .

### Theorem:-

The kernel of a homomorphism  $f$  from a group  $(G, *)$  to  $(G', *)$  is a subgroup of  $G$

(OR)

Let  $f: (G, *) \rightarrow (G', *)$  be a homomorphism. Then prove that kernel  $f$  is a normal subgroup.

Isomorphism

Definition- A mapping  $f$  from a group  $(G, *)$  to a group  $(G', \Delta)$  is said to be an isomorphism if,

(i)  $f$  is a homomorphism

↳  $f(a * b) = f(a) \Delta f(b)$ , for all  $a, b \in G$ .

(ii)  $f$  is one-one (injective)

(iii)  $f$  is on-to (surjective)

In other words a bijective homomorphism is said to be an isomorphism.

Example

Prove that if  $f: G \rightarrow G'$  is a homomorphism then

$\text{ker } f = \{e\}$  iff  $f$  is 1-1.

Theorem

$\nexists a \in H * b$  then  $H * a = H * b$

and if  $a \in b * H$  then  $a * H = b * H$ .



Theorem 1:-

Any two right (or left) cosets of  $H$  in  $G$  are either disjoint or identical.

Theorem 2:-

If  $(H, *)$  is a subgroup of a group  $(G, *)$  and  $H * a$  is any right coset of  $H$  in  $G$ , then there exists a one-one correspondence (bijective mapping) between the elements of  $H$  and  $H * a$  are equal.

Lagrange's Theorem:-

Let  $G$  be a finite group of order ' $n$ ' and  $H$  be any subgroup of  $G$ . Then the order of  $H$  divides the order of  $G$ .

$$\text{is } |H| \mid |G|$$

The order of each subgroup of a finite group is a divisor of the order of the group.

Normal Subgroups:-

Let  $H$  be a subgroup of  $G$  under  $*$ .

Then  $H$  is said to be a normal subgroup of  $G$ , for every  $x \in G$  and for  $h \in H$

$$\text{if } x * h * x^{-1} \in H$$

$$\text{is } x * H * x^{-1} \subseteq H$$

Alternatively, a subgroup  $H$  of  $G$  is called a normal subgroup of  $G$  if  $x * h = h * x$  for all  $x \in G$ .

Theorem 1:-

The order of any element of a finite group  $G$  divides the order of  $G$ .

Theorem:-

A subgroup  $H$  of a group  $G$  is normal if  $x * h * x^{-1} \in H$  for all  $x \in G$ .

Theorem:-

The intersection of any two normal subgroups of a group is a normal subgroup.



### Index of $H$ :-

#### Definition:-

The number of distinct left (or right) cosets of  $H$  in  $G$  is called the index of  $H$  in  $G$ .

It is denoted by

$$|G:H| = I_G(H) = \frac{|G|}{|H|}.$$

#### Natural Homomorphism:-

Let  $H$  be a normal subgroup of a group  $G$ .

The map  $f: G \rightarrow G/H$  such that

$f(x) = H * x, x \in G$  is called a Natural Homomorphism of a group  $G$  onto the quotient group  $G/H$ .

Theorem:- Fundamental Theorem on Homomorphism of groups.

Every homomorphic image of a group  $G$  is isomorphic to some quotient group of  $G$ .

Subject code & subject: MAR311 / Discrete Mathematics Period 12

### Algebraic Structures with two Binary operations:

#### Ring:-

An algebraic system  $(R, +, \cdot)$  is called a ring if the binary operations  $+$  and  $\cdot$  satisfies the following conditions.

(1)  $(a+b)+c = a+(b+c), a, b, c \in R$

(2) There exists an element  $0 \in R$  called zero element such that  $a+0 = 0+a = a$  for all  $a \in R$ .

#### Definition:-

The ring  $(R, +, \cdot)$  is called a Commutative ring, if  $ab = ba$  for  $a, b \in R$ .

If  $(R, \cdot)$  is a monoid, then the ring  $(R, +, \cdot)$  is called a ring with identity or unity.

If  $a$  and  $b$  are 2 non zero elements of a ring  $R$  such that  $a \cdot b = 0$  then  $a$  and  $b$  are called divisors.



Subject Name / Code : Discrete Mathematics / MA2311

Unit : 5

Period : 1

Lattices And Boolean Algebra.

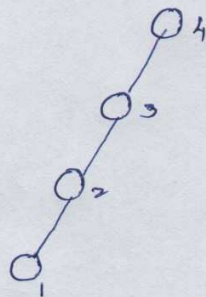
Partial Ordering :

A binary relation  $R$  in a set  $P$  is called a partial order relation or partial ordering in  $P$  iff  $R$  is reflexive, Antisymmetric and transitive.

Hasse Diagram:

A partial ordering  $\leq$  on a set  $P$  can be represented by means of a diagram known as a Hasse diagram.

Ex :- Let  $P = \{1, 2, 3, 4\}$  and  $\leq$  be the relation then the Hasse diagram is,



Subject Name / Code : DISCRETE MATHEMATICS / MA2311

Unit : 5

Period : 2

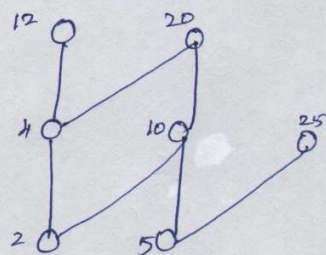
Poset :

A set  $P$  together with a partial ordering  $R$  is called a partially ordered set or a poset.

Ex : Give a relation which is both a partially ordering relation and an equivalence relation on a set.

Soln :- Equality, similarity of triangles are the examples of relation which is both partially ordering and an equivalence relation.

Ex :- Which elts of the poset  $\{2, 4, 5, 10, 12, 20, 25\}$  are maximal and which are minimal?



Maximal elts : 12, 20, 25

Minimal elts : 2 & 5



Subject Name/code : DISCRETE MATHEMATICS / MA 2311

Unit : 5

Period : 3

Lattices as Posets :

Totally Ordered set :

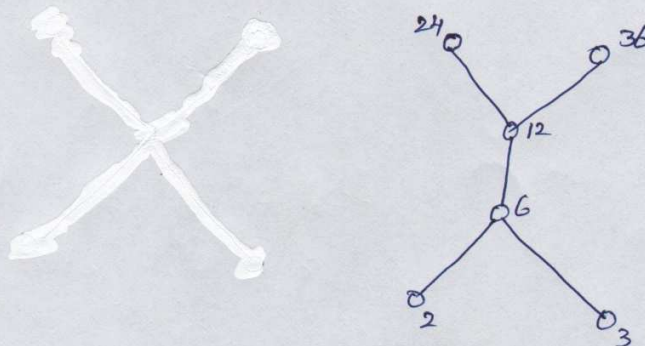
Let  $(P, \leq)$  be a partially ordered set.

If for every  $x, y \in P$  we have either  $x \leq y$  or  $y \leq x$ , then  $\leq$  is called simple ordering or linear ordering on  $P$  and  $(P, \leq)$  is called a totally ordered or simply ordered or a chain.

Ex :- The poset  $(\mathbb{Z}, \leq)$  is totally ordered, since  $a \leq b$  or  $b \leq a$  whenever  $a$  &  $b$  are integers.

Ex :- Let  $X = \{2, 3, 6, 12, 24, 36\}$  and the relation  $\leq$  be such that  $x \leq y$  if  $x$  divides  $y$ . Draw the Hasse diagram of  $(X, \leq)$

Soln:-



Subject Name / Code : DISCRETE MATHEMATICS / MA2311

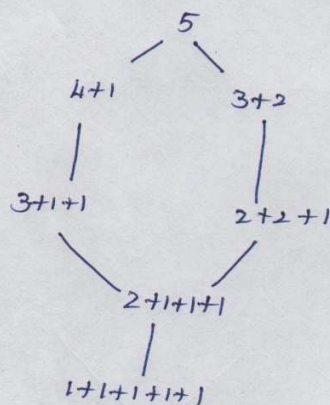
Unit : 5

Period : 4

Ex :- Let  $S$  be a set. Determine whether there is a greatest elt and a least elt in the poset  $(P(S), \subseteq)$ .

Soln :- The least elt is the empty set  $\because \emptyset \subseteq T$  for any subset  $T$  of  $S$ . The set  $S$  is the greatest elt in this poset. Since  $T \subseteq S$  whenever  $T$  is a subset of  $S$ .

Ex :- Draw the Hasse diagram of the set of partitions of 5.



$$5 = 5$$

$$5 = 4+1$$

$$5 = 3+2$$

$$5 = 3+1+1$$

$$5 = 2+2+1$$

$$5 = 2+1+1+1$$

$$5 = 1+1+1+1+1$$



Subject Name / Code : DISCRETE MATHEMATICS / MA2311

Unit : 5

Period : 5

Properties of Lattices :

Lattice :

A Lattice is a partially ordered set  $(L, \leq)$  in which every pair of elts  $a, b \in L$  has a greatest lower bound and a least upper bound.

Property 1 : Idempotent Law

Let  $(L, \leq)$  be a Lattice. For any  $a, b \in L$  we have  $a * a = a$  and  $a \oplus a = a$

Property 2 : S.T the operation of meet and join on a Lattice are associative.

Property 3 : S.T the operation of meet and join on a Lattice are commutative Law.

Property 4 : Absorption Law  $a * (a \oplus b) = a$   
and  $a \oplus (a * b) = a$ .

Subject Name / Code : DISCRETE MATHEMATICS / MA2311

Unit : 5

Period : 6

### Lattices As Algebraic Systems :

Theorem 1 :

Let  $(L, \leq)$  be a Lattice in which  $*$  and  $\oplus$  denotes the operation of meet and join respectively. For any  $a, b \in L$ ,  $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$

Theorem 2 :

Let  $(L, \leq)$  be a Lattice. For any  $a, b \in L$ , the following are equivalent.

(i)  $a \leq b$  (ii)  $a * b = a$  (iii)  $a \oplus b = b$

Theorem 3 :

Let  $(L, \leq)$  be a Lattice. For any  $a, b, c \in L$ , the following inequalities hold,

1) Distributive

2) Modular.

Theorem 4 :

In a Lattice  $(L, \leq)$  s.t (i)  $(a * b) \oplus c * d \leq (a \oplus c) * (b \oplus d)$

(ii)  $(a * b) \oplus (b * c) \oplus (c * a) \leq (a \oplus b) * (b \oplus c) * (c \oplus a)$

$\forall a, b, c \in L$



Subject Name / Code : DISCRETE MATHEMATICS / MA2311

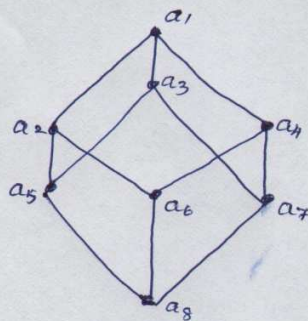
Unit : 5

Period : 7

Sublattice :

Let  $(L, *, \oplus)$  be a lattice and let  $S \subseteq L$  be a subset of  $L$ . The algebra  $(S, *, \oplus)$  is a sublattice of  $(L, *, \oplus)$  iff  $S$  is closed under both operations  $*$  and  $\oplus$

Ex :- Let  $(L, \leq)$  be a lattice in which  $L = \{a_1, \dots, a_8\}$  and  $s_1, s_2$  and  $s_3$  be the sublattices of  $L$  given by  $s_1 = \{a_1, a_2, a_4, a_6\}$   
 $s_2 = \{a_3, a_5, a_7, a_8\}$  and  $s_3 = \{a_1, a_2, a_4, a_8\}$



Defn :- Let  $(L, *, \oplus)$  &  $(S, \wedge, \vee)$  be two lattices. The algebraic system  $(L \times S, \cdot, +)$  in which binary operation  $+$  and  $\cdot$  on  $L \times S$  are such that for any  $(a_1, b_1)$  &  $(a_2, b_2)$  in  $L \times S$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_2, b_1 \wedge b_2)$$

$$(a_1, b_1) + (a_2, b_2) = (a_1 \oplus a_2, b_1 \vee b_2)$$

is called direct product of lattices  $(L, *, \oplus)$  &  $(S, \wedge, \vee)$

Subject Name / Code : DISCRETE MATHEMATICS / MA2311

Unit : 5

Period : 8

Lattice Homomorphism:

Let  $(L, *, \oplus)$  and  $(S, \vee, \wedge)$  be two lattices. A mapping  $g: L \rightarrow S$  is called a lattice homomorphism from the lattice  $(L, *, \oplus)$  to  $(S, \wedge, \vee)$  if for any  $a, b \in L$

$$g(a * b) = g(a) \wedge g(b) \quad \&$$

$$g(a \oplus b) = g(a) \vee g(b)$$

A Homomorphism  $g: L \rightarrow L$  where  $(L, *, \oplus)$  is a lattice is called an Endomorphism.

If a Homomorphism  $g: L \rightarrow S$  of two lattices  $(L, *, \oplus)$  and  $(S, \wedge, \vee)$  is bijective then  $g$  is called isomorphism.

If  $g: L \rightarrow L$  is an isomorphism then  $g$  is called an automorphism.

If  $g: L \rightarrow L$  is an endomorphism then the image set of  $g$  is a sublattice of  $L$ .



Subject Name / Code : DISCRETE MATHEMATICS / MA2311

Period : 9

Unit : 5

Theorem 1: Every chain is a distributive lattice.

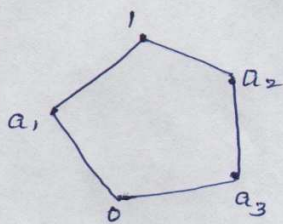
Theorem 2: Let  $(L, *, \oplus)$  be a distributive lattice

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

$$(a * b = a * c) \wedge (a \oplus b = a \oplus c) \Rightarrow b = c$$

Theorem 3: Every distributive lattice is Modular.

Ex :- S.T the lattices given by the diagram are not distributive.



(A)

$$\text{Here, } a_3 * (a_1 \oplus a_2) = a_3 * 1 = a_3 = (a_3 * a_1) \oplus (a_3 * a_2)$$

$$a_1 * (a_2 \oplus a_3) = 0 = (a_1 * a_2) \oplus (a_1 * a_3)$$

$$\text{but, } a_2 * (a_1 \oplus a_3) = a_2 * 1 = a_2$$

$$(a_2 * a_1) \oplus (a_2 * a_3) = 0 \oplus a_3 = a_3$$

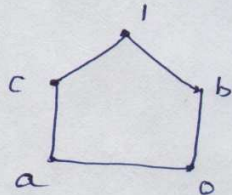
$\therefore$  The lattice A is not distributive.

Subject Name / Code : DISCRETE MATHEMATICS / MA2311

Unit : 5

Period : 10

Ex : P.T the following lattice is not modular



For this Lattice when  $a \leq c$

$$a \oplus (b * c) \neq (a \oplus b) * c$$

$$\therefore a \oplus (b * c) = a \oplus 0 = a$$

$$\text{but } (a \oplus b) * c = 1 * c = c$$

$\therefore$  It is not a modular lattice.

Theorem: state and prove Isotonicity property in a Lattice.

Ex:- If  $(L, \vee, \wedge)$  is a complemented distributive Lattice then the De Morgans Law are valid

$$\text{ie) } \overline{a \vee b} = \bar{a} \wedge \bar{b}$$

$$\overline{a \wedge b} = \bar{a} \vee \bar{b} \quad \forall a, b \in L$$

Theorem:- In a distributive Lattice, s.t

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



Subject Name / Code : DISCRETE MATHEMATICS / MA2311

Lit : 5

Period : 11

Boolean Algebra :

A Boolean Algebra is a complemented distributive Lattice.

It satisfies the following properties :

$(B, *, \oplus)$  is a Lattice in which the operations  $*$  and  $\oplus$  satisfy the identities :

$$a * a = a$$

$$a * b = b * a$$

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

$$a * (a \oplus b) = a$$

$$a \oplus a = a$$

$$a \oplus b = b \oplus a$$

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

$$a \oplus (a * b) = a$$

$(B, *, \oplus)$  is a distributive Lattice & satisfies :

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

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

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

$$a * b = a * c \text{ \& } a \oplus b = a \oplus c \Rightarrow b = c$$

$(B, *, \oplus, 0, 1)$  is a bdd Lattice for any  $a \in B$  the following holds :  $0 \leq a \leq 1$

$$a * 0 = 0$$

$$a * 1 = a$$

Subject Name / Code : Discrete Mathematics

Unit : 5

Period : 12

Theorem :

In a Boolean Lattice, P.T the De-Morgan's

Laws.

Ex :- S.T  $(P(A), \cup, \cap, \subseteq)$  is a Boolean algebra.

Ex :- S.T in any Boolean algebra,

$$(a+b)(a'+c) = ac + a'b + bc$$

Ex :- In any Boolean algebra, S.T  $a=b$

$$\text{iff } a\bar{b} + \bar{a}b = 0$$

Theorem : P.T every finite Boolean algebra

$(B, \vee, \wedge, -)$  has  $2^n$  elts for some positive integer 'n'.

Ex :- P.T  $a \oplus (a' * b) = a \oplus b$

Ex :- P.T  $a * (a' \oplus b) = a * b$

Ex :- S.T Every distributive Lattice is Modular.

Whether the converse is true? Justify your claim.