LECTURE PLAN

Department: Computer Science
Class : 3rd CSE 'A' & 'B'
Subject code : MA2311
Subject : Discrete Mathematics

Period 1

Unit 4 Algebraic Structures

Definition:- 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 : MA2311, 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.

i.e. $x = a^n$

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,Δ) be any two semigroups with binary operation $*$ and Δ 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,Δ) 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 $*$, i.e. $(G,*)$ 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 $a*e = e*a$ 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 $(Z,+)$ 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 otherwords, $(H,*)$ 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:-

period 6

Let $(G,*)$ and (H,Δ) be any two groups.

A mapping $f: G \to H$ 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 $f: G \to G'$ 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 $(G',*)$. Let $f(G)$ be the homomorphic image of G into G'. Then $f(G)$ is a subgroup of G'.

Kernel of a Homomorphism :-

Let $f : G \to G'$ 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 $\ker(f)$.

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

Examples:-

1. $f : (Z, +) \to (Z, +)$ defined by $f(x) = 2x$.
   Then $\ker(f) = \{0\}$.

2. $f : (R^*, \cdot) \to (R^+, \cdot)$ 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 $f : (G, *) \to (G', *)$ 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', Δ) is said to be an isomorphism if

(i) f is a homomorphism

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

(ii) f is one-one (injective)

(iii) f is on-to (Surjective)

In otherwords a bijective homomorphism is said to be an isomorphism.

Examples:-

Prove that if $f: G \to G'$ is a homomorphism then $\ker f = \{e\}$ iff f is 1-1.

Theorem:-

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

Theorem:-

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

Theorem:-

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

i.e. $O(H) / O(G)$

(or)

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 $h \in H$

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

i.e. $x * H * x^{-1} \subseteq H$

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

Theorem :-

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 $x * h * x^{-1} = H$ 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

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

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 : MA2311 / Discrete Mathematics Period 12

Algebraic Structures with two Binary operations:

Rings:-

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.

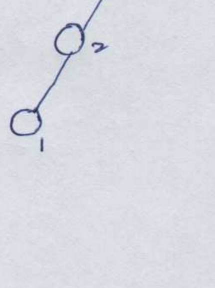
Partial Ordering :

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

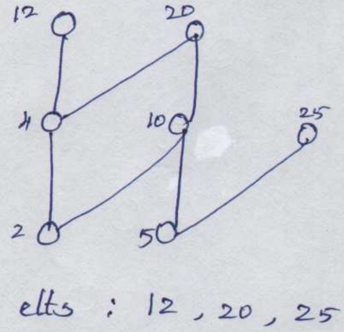
Poset :

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 / MA2311

Unit : 5 Period : 3

Lattices as Posets :

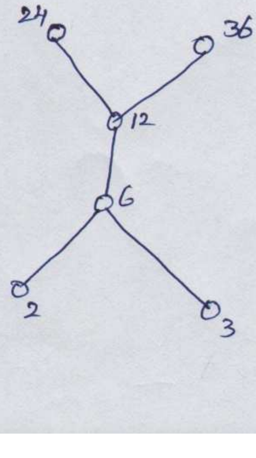
Totally Ordered set :

Let $(P, \leq)$ be a partially ordered set. If for every $x, y \in P$ we have either $x \leq y \vee y \leq x$ 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 $(Z, \leq)$ 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 :-



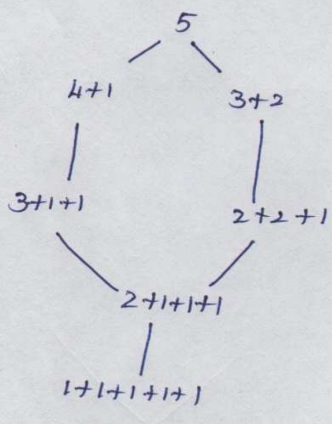
Subject Name / Code : DISCRETE MATHEMATICS / MA2311

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 $\because \phi \subseteq T$ 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 in 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 Algebric Systems :

Theorem 1:

Let $(L, \leq)$ be a Lattice in which $*$ and $\oplus$ denotes the operation of meet and jo[in]

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) Distsibutive

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

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

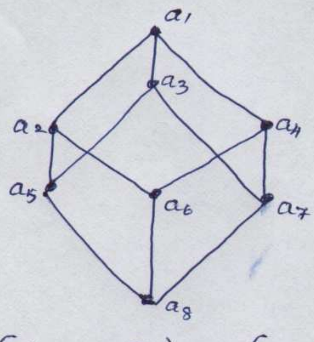
Subject Name / Code : DISCRETE MATHEMATICS / MA2311

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 $L = \{a_1, \cdots a_8\}$ 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 algebric 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 $g : L \to S$ is called a Lattice homomorphism from the Lattice $(L, *, \oplus)$ to $(S, \wedge, \vee)$ if for any $a, b \in L$

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

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

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

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

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

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

Subject Name / Code : DISCRETE MATHEMATICS / MA2311
Period : 9
Unit : 5

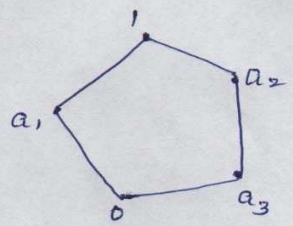
Theorem 1: Every chain is a distributive Lattice.

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)

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

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

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

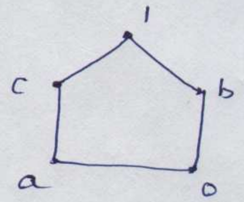
$(a_2 * a_1) \oplus (a_2 * a_3) = 0 \oplus a_3 = a_3$

$\therefore$ 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 $a \leq c$

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

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

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

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

Unit : 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 :

$a * a = a$

$a \oplus a = a$

$a * b = b * a$

$a \oplus b = b \oplus a$

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

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

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

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

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

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

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

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

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

$(B, *, \oplus, 0, 1)$ 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-Morgans 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 $a=b$ 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.