Unit-III : Algebraic Structures

Algebraic Structures:

Algebraic Systems: Examples and General Properties, Semi groups and Monoids, Polish expressions and their compilation, Groups: Definitions and Examples, Subgroups and Homomorphism's, Group Codes.

Lattices and Boolean algebra:
Lattices and Partially Ordered sets, Boolean algebra.

3.1 Algebraic systems

N = {1,2,3,4,….. } = Set of all natural numbers.

Z = { 0, ± 1, ± 2, ± 3, ± 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.

3.1.1 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.

3.1.2 Properties

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

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 $a \in A$.

Note: For an algebraic system (A, *), the identity element, if exists, is unique.

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

$a * b = b * a = e$

3.1.3 Semi groups

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.

3.1.4 **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.

Ex. Show that the set 'N' is a monoid with respect to multiplication.

Solution: Here, N = {1,2,3,4,……}

1. Closure property : 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

$\therefore$ Multiplication is a closed operation.

2. Associativity : 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.

$\therefore$ Identity element exists, and 1 is the identity element.

Hence, N is a monoid with respect to multiplication.

Examples

Ex. Let (Z, *) be an algebraic structure, where Z is the set of integers

and the operation * is defined by n * m = maximum of (n, m).

Show that (Z, *) is a semi group.

Is (Z, *) a monoid ?. Justify your answer.

Solution: Let a , b and c are any three integers.

Closure property: Now, $a * b =$ maximum of $(a, b) \in Z$ for all $a,b \in Z$

Associativity : $(a * b) * c =$ maximum of $\{a,b,c\} = a * (b * c)$

$\therefore$ (Z, *) is a semi group.

Identity : There is no integer x such that

$a * x =$ maximum of $(a, x) = a$ for all $a \in Z$

$\therefore$ Identity element does not exist. Hence, (Z, *) is not a monoid.

Ex. Show that the set of all strings 'S' is a monoid under the operation 'concatenation of strings'.

Is S a group w.r.t the above operation? Justify your answer.

Solution: Let us denote the operation

'concatenation of strings' by + .

Let s_1, s_2, s_3 are three arbitrary strings in S.

Closure property: Concatenation of two strings is again a string.

i.e., $s_1+s_2 \in S$

Associativity: Concatenation of strings is associative.

$$(s_1+ s_2) + s_3 = s_1+ (s_2 + s_3)$$

Identity: We have null string , $l \in S$ such that $s_1 + l = S$.

$\therefore$ S is a monoid.

Note: S is not a group, because the inverse of a non empty string does not exist under concatenation of strings.

3.2 Groups

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

$a * b = b * a$ "a, b $\in$ G.

Properties

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

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

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

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

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.

Ex1 . Show that, the set of all integers is an abelian group with respect to addition.

Solution: Let Z = set of all integers.

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

1. Closure property : We know that, Sum of two integers is again an integer.

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

2. Associativity: 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 $a \in Z$.

   $\therefore$ Identity element exists, and '0' is the identity element.

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. Commutativity: 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.

Ex2 . Show that set of all non zero real numbers is a group with respect to multiplication .

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

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

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

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

2. Associativity: 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. Identity : We have $1 \in R^*$ and $a .1 = a$ for all $a \in R^*$.

$\therefore$ 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.

5. Commutativity: We know that multiplication of real numbers is

commutative.

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

Hence, $(R^* , .)$ is an abelian group.

Note: 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.

Example: Let S be a finite set, and let F(S) be the collection of all functions $f: S \to S$ under the operation of composition of functions, then show that F(S) is a monoid.

Is S a group w.r.t the above operation? Justify your answer.

Solution:

Let f_1, f_2, f_3 are three arbitrary functions on S.

Closure property: Composition of two functions on S is again a function on S.

i.e., $f_1 o f_2 \in F(S)$

Associativity: Composition of functions is associative.

i.e., $(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$

Identity: We have identity function $I : S \to S$

such that $f_1 \circ I = f_1$.

$\therefore$ F(S) is a monoid.

Note: F(S) is not a group, because the inverse of a non bijective function on S does not exist.

Ex. If M is set of all non singular matrices of order 'n x n'.
then show that M is a group w.r.t. matrix multiplication.
Is (M, *) an abelian group?. Justify your answer.

Solution: Let $A,B,C \in M$.

<u>1.Closure property</u> : Product of two non singular matrices is again a non singular matrix, because

½AB½ = ½A½ . ½B½ ^{1} 0 (Since, A and B are nonsingular)

i.e., $AB \in M$ for all $A,B \in M$.

2. <u>Associativity</u>: Marix multiplication is associative.

i.e., $(AB)C = A(BC)$ for all $A,B,C \in M$.

3. <u>Identity</u> : We have $I_n \in M$ and $A\, I_n = A$ for all $A \in M$.

$\therefore$ Identity element exists, and 'I_n' is the identity element.

4. <u>Inverse</u>: To each $A \in M$, we have $A^{-1} \in M$ such that

$A\, A^{-1} = I_n$ i.e., Each element in M has an inverse.

$\therefore$ M is a group w.r.t. matrix multiplication.

We know that, matrix multiplication is not commutative.

Hence, M is not an abelian group.

Ex. Show that the set of all positive rational numbers forms an abelian group under the composition * defined by
$a * b = (ab)/2$.

Solution: Let A = set of all positive rational numbers.

Let a,b,c be any three elements of A.

1. <u>Closure property:</u> We know that, Product of two positive rational numbers is again a rational number.

i.e., $a * b \in A$ for all $a, b \in A$.

2. <u>Associativity</u>: $(a*b)*c = (ab/2) * c = (abc) / 4$

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

3. <u>Identity</u> : Let e be the identity element.

We have $a*e = (a\,e)/2$ ...(1) , By the definition of *

again, $a*e = a$ .....(2) , Since e is the identity.

From (1)and (2), $(a\,e)/2 = a \Rightarrow e = 2$ and $2 \in A$.

∴ Identity element exists, and '2' is the identity element in A.

4. <u>Inverse:</u> Let $a \in A$

let us suppose b is inverse of a.

Now, $a * b = (a\,b)/2$ ....(1) (By definition of inverse.)

Again, $a * b = e = 2$ .....(2) (By definition of inverse)

From (1) and (2), it follows that

$$(a\,b)/2 = 2$$

$$\Rightarrow \quad b = (4 / a) \in A$$

∴ (A ,*) is a group.

Commutativity: $a * b = (ab/2) = (ba/2) = b * a$

Hence, (A,*) is an abelian group.

Ex. Let R be the set of all real numbers and * is a binary operation defined by $a * b = a + b + a\,b$. Show that (R, *) is a monoid.

Is (R, *) a group?. Justify your answer.

Try for yourself.

identity = 0

inverse of $a = -a / (a+1)$

Ex. If $E = \{ 0, \pm 2, \pm 4, \pm 6, \ldots\ldots\}$, then the algebraic structure (E, +) is

a) a semi group but not a monoid

b) a monoid but not a group.

c) a group but not an abelian group.

d) an abelian group.

Ans; d

Ex. Let A = Set of all rational numbers ‘x’ such that 0 < x £ 1.
Then with respect to ordinary multiplication, A is

a) a semi group but not a monoid

b) a monoid but not a group.

c) a group but not an abelian group.

d) an abelian group.

Ans. b

Ex. Let C = Set of all non zero complex numbers .Then with respect to multiplication, C is

a) a semi group but not a monoid

b) a monoid but not a group.

c) a group but not an abelian group.

d) an abelian group.

Ans. d

Ex. In a group (G, *) , Prove that the identity element is unique.

Proof : a) Let e_1 and e_2 are two identity elements in G.

Now, $e_1 * e_2 = e_1$ ...(1) (since e_2 is the identity)

Again, $e_1 * e_2 = e_2$ ...(2) (since e_1 is the identity)

From (1) and (2), we have $e_1 = e_2$

∴ Identity element in a group is unique.

Ex. In a group (G, *) , Prove that the inverse of any element is unique.

Proof: Let a ,b,c ∈G and e is the identity in G.

Let us suppose, Both b and c are inverse elements of a .

Now, a * b = e ...(1) (Since, b is inverse of a)

Again, a * c = e ...(2) (Since, c is also inverse of a)

From (1) and (2), we have

a * b = a * c

$\Rightarrow$ b = c (By left cancellation law)
In a group, the inverse of any element is unique.

Ex. In a group (G, *) , Prove that
$(a * b)^{-1} = b^{-1} * a^{-1}$ for all a,b $\in$G.

Proof : Consider,

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

$= (a * (b * b^{-1}) * a^{-1})$ (By associative property).

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

$= (a * a^{-1})$ (Since, e is identity)

$= e$ (By inverse property)

Similarly, we can show that

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

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

Ex. If (G, *) is a group and a $\in$ G such that a * a = a ,
then show that a = e , where e is identity element in G.

Proof: Given that, a * a = a

$\Rightarrow$ a * a = a * e (Since, e is identity in G)
$\Rightarrow$ a = e (By left cancellation law)
Hence, the result follows.

Ex. If every element of a group is its own inverse, then show that the group must be abelian .

Proof: Let (G, *) be a group.

Let a and b are any two elements of G.

Consider the identity,

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

$\Rightarrow$ (a * b) = b * a (Since each element of G is its own inverse)
Hence, G is abelian.

Note: $a^2 = a * a$
$a^3 = a * a * a$ etc.

Ex. In a group (G, *), if $(a * b)^2 = a^2 * b^2$ "a,b $\in$ G

then show that G is abelian group.

Proof: Given that $(a * b)^2 = a^2 * b^2$

$\Rightarrow$ $(a * b) * (a * b) = (a * a) * (b * b)$
$\Rightarrow$ $a * (b * a) * b = a * (a * b) * b$ (By associative law)
$\Rightarrow$ $(b * a) * b = (a * b) * b$ (By left cancellation law)
$\Rightarrow$ $(b * a) = (a * b)$ (By right cancellation law)
Hence, G is abelian group.

3.2.2 Finite groups

Ex. Show that $G = \{1, -1\}$ is an abelian group under multiplication.

Solution: The composition table of G is

.	1	-1
1	1	-1
-1	-1	1

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.

2. Associativity: The elements of G are real numbers, and we know that multiplication of real numbers is associative.

3. Identity : Here, 1 is the identity element and $1 \in G$.

4. Inverse: From the composition table, we see that the inverse elements of

1 and -1 are 1 and -1 respectively.

Hence, G is a group w.r.t multiplication.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative.

Hence, G is an abelian group w.r.t. multiplication..

Ex. Show that $G = \{1, w, w^2\}$ is an abelian group under multiplication.
Where $1, w, w^2$ are cube roots of unity.

Solution: The composition table of G is

.	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.

2. Associativity: The elements of G are complex numbers, and we know that multiplication of complex numbers is associative.

3. Identity : Here, 1 is the identity element and $1 \in G$.

4. Inverse: From the composition table, we see that the inverse elements of

$1\ w, w^2$ are $1, w^2, w$ respectively.

Hence, G is a group w.r.t multiplication.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative.

Hence, G is an abelian group w.r.t. multiplication.

Ex. Show that G = {1, –1, i, –i } is an abelian group under multiplication.

Solution: The composition table of G is

.	1	–1	i	-i
1	1	-1	i	- i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.

2. Associativity: The elements of G are complex numbers, and we know that multiplication of complex numbers is associative.

3. Identity : Here, 1 is the identity element and $1 \in G$.

4. Inverse: From the composition table, we see that the inverse elements of

1 -1, i, -i are 1, -1, -i, i respectively.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative. Hence, (G, .) is an abelian group.

Modulo systems.

Addition modulo m ($+_m$)

let m is 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 $a + b\ {}^{3}\ m$ where r is the remainder obtained by dividing (a+b) with m.

<u>Multiplication modulo p</u> (*m)

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

$a *m\, b = a\, b$ if $a\, b < p$

$a *m\, b = r$ if $a\, b\ {}^{3}\ p$ where r is the remainder obtained by dividing (ab) with p.

Ex. $3 *_5 4 = 2$, $5 *_5 4 = 0$, $2 *_5 2 = 4$

Example : 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 $+_6$.

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.

Example : 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. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under $*_7$.

2. Associativity: The binary operation $*_7$ is associative in G.

for ex. $(2 *_7 3) *_7 4 = 6 *_7 4 = 3$ and

$2 *_7 (3 *_7 4) = 2 *_7 5 = 3$

3. Identity : 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. . Inverse: 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 $*_7$ is commutative.

Hence, (G, $*_7$) is an abelian group.

More on finite groups

In a group with 2 elements, each element is its own inverse

In a group of even order there will be at least one element (other than identity element) which is its own inverse

The set G = {0,1,2,3,4,…..m-1} is a group with respect to addition modulo m.

The set G = {1,2,3,4,….p-1} is a group with respect to multiplication modulo p, where p is a prime number.

Order of an element of a group:

Let (G, *) be a group. Let 'a' be an element of G. The smallest integer n such that $a^n = e$ is called order of 'a'. If no such number exists then the order is infinite.

Ex. G = {1, -1, i, -i } is a group w.r.t multiplication.The order –i is a) 2 b) 3 c) 4 d) 1

Ex. Which of the following is not true.

a) The order of every element of a finite group is finite and is a divisor of the order of the group.

b) The order of an element of a group is same as that of its inverse.

c) In the additive group of integers the order of every element except 0 is infinite

d) In the infinite multiplicative group of nonzero rational numbers the order of every element except 1 is infinite.

Ans. D

<u>3.3 Sub groups</u>

<u>Def</u>. A non empty sub set H of a group (G, *) is a sub group of G, if (H, *) is a group.

<u>Note</u>: For any group {G, *}, {e, * } and (G, *) are trivial sub groups.

Ex. G = {1, -1, i, -i } is a group w.r.t multiplication.

H_1 = { 1, -1 } is a subgroup of G .

H_2 = { 1 } is a trivial subgroup of G.

Ex. (Z , +) and (Q , +) are sub groups of the group (R +).

<u>Theorem</u>: A non empty sub set H of a group (G, *) is a sub group of G iff

i) $a * b \in H$ " $a, b \in H$

ii) $a^{-1} \in H$ " $a \in H$

Theorem

Theorem: A necessary and sufficient condition for a non empty subset H of a group (G, *) to be a sub group is that

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

Proof: Case1: Let (G, *) be a group and H is a subgroup of G

Let $a,b \in H \Rightarrow b^{-1} \in H$ (since H is is a group)

$\Rightarrow a * b^{-1} \in H.$ (By closure property in H)

Case2: Let H be a non empty set of a group (G, *).

Let $a * b^{-1} \in H$ " a, b ∈ H

Now, $a * a^{-1} \in H$ (Taking $b = a$)

$\Rightarrow e \in H$ i.e., identity exists in H.

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

$\Rightarrow a^{-1} \in H$

∴ Each element of H has inverse in H.

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

$\Rightarrow a * (b^{-1})^{-1} \in H.$

$\Rightarrow a * b \in H.$ ∴ H is closed w.r.t * .

Finally, Let $a,b,c \in H$

$\Rightarrow a,b,c \in G$ (since H Í G)

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

∴ * is associative in H

Hence, H is a subgroup of G.

Theorem: A necessary and sufficient condition for a non empty finite subset H of a group (G, *) to be a sub group is that

$a * b \in H$ for all $a, b \in H$

Proof: Assignment .

Example : Show that the intersection of two sub groups of a group G is again a sub group of G.

Proof: Let (G, *) be a group.

Let H_1 and H_2 are two sub groups of G.

Let $a, b \in H_1 \cap H_2$.

Now, $a, b \in H_1 \Rightarrow a * b^{-1} \in H_1$ (Since, H_1 is a subgroup of G)

again, $a, b \in H_2 \Rightarrow a * b^{-1} \in H_2$ (Since, H_2 is a subgroup of G)

$\therefore$ $a * b^{-1} \in H_1 \cap H_2$.

Hence, $H_1 \cap H_2$ is a subgroup of G .

Ex. Show that the union of two sub groups of a group G need not be a sub group of G.

<u>Proof</u>: Let G be an additive group of integers.

Let $H_1 = \{ 0, \pm2, \pm4, \pm6, \pm8, \ldots\}$

and $H_2 = \{ 0, \pm3, \pm6, \pm9, \pm12, \ldots\}$

Here, H_1 and H_2 are groups w.r.t addition.

Further, H_1 and H_2 are subsets of G.

$\therefore$ H_1 and H_2 are sub groups of G.

$H_1 \cup H_2 = \{ 0, \pm2, \pm3, \pm4, \pm6, \ldots\}$

Here, $H_1 \cup H_2$ is not closed w.r.t addition.

For ex. $2, 3 \in G$

But, $2 + 3 = 5$ and 5 does not belongs to $H_1 \cup H_2$.

Hence, $H_1 \cup H_2$ is not a sub group of G.

Homomorphism and Isomorphism.

Homomorphism : Consider the groups $(G, *)$ and $(G^1, \oplus)$

A function $f : G \to G^1$ is called a homomorphism if

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

Isomorphism : If a homomorphism $f : G \to G^1$ is a bijection then f is called isomorphism between G and G^1 .

Then we write $G \equiv G^1$

Example : Let R be a group of all real numbers under addition and R^+ be a group of all positive real numbers under multiplication. Show that the mapping $f : R \to R^+$ defined by $f(x) = 2^x$ for all $x \in R$ is an isomorphism.

Solution: First, let us show that f is a homomorphism.

Let $a , b \in R$.

Now, $f(a+b) = 2^{a+b}$

$= 2^a \; 2^b$

$= f(a).f(b)$

$\therefore$ f is an homomorphism.

Next, let us prove that f is a Bijection.

For any $a , b \in R$, Let, $f(a) = f(b)$

$\Rightarrow 2^a = 2^b$

$\Rightarrow a = b$

$\therefore$ f is one.to-one.

Next, take any $c \in R^+$.

Then $\log_2 c \in R$ and $f(\log_2 c) = 2^{\log2 c} = c$.

$\Rightarrow$ Every element in R^+ has a pre image in R.

i.e., f is onto.

$\therefore$ f is a bijection.

Hence, f is an isomorphism.

Ex. Let R be a group of all real numbers under addition and R^+ be a group of all positive real numbers under multiplication. Show that the mapping $f : R^+ \to R$ defined by $f(x) = \log_{10} x$ for all $x \in R$ is an isomorphism.

Solution: First, let us show that f is a homomorphism.

Let $a , b \in R^+$.

Now, $f(a.b) = \log_{10} (a.b)$

$= \log_{10} a + \log_{10} b$

$= f(a) + f(b)$

$\therefore$ f is an homomorphism.

Next, let us prove that f is a Bijection.

For any a , b $\in R^+$, Let, f(a) = f(b)

$\Rightarrow \log_{10} a = \log_{10} b$

$\Rightarrow a = b$

$\therefore$ f is one.to-one.

Next, take any $c \in R$.

Then $10^c \in R$ and $f(10^c) = \log_{10} 10^c = c$.

$\Rightarrow$ Every element in R has a pre image in R^+ .

i.e., f is onto.

$\therefore$ f is a bijection.

Hence, f is an isomorphism.

<u>Theorem</u>: Consider the groups $(G_1, *)$ and $(G_2, \oplus)$ with identity elements e_1 and e_2 respectively. If $f : G_1 \to G_2$ is a group homomorphism, then prove that

a) $f(e_1) = e_2$

b) $f(a^{-1}) = [f(a)]^{-1}$

c) If H_1 is a sub group of G_1 and $H_2 = f(H_1)$,

then H_2 is a sub group of G_2.

d) If f is an isomorphism from G_1 onto G_2,

then f^{-1} is an isomorphism from G_2 onto G_1.

<u>Proof</u>: a) we have in G_2,

$e_2 \oplus f(e_1) = f(e_1)$ (since, e_2 is identity in G_2)

$= f(e_1 * e_1)$ (since, e_1 is identity in G_1)

$= f(e_1) \oplus f(e_1)$ (since f is a homomorphism)

$e_2 = f(e_1)$ (By right cancellation law)

b) For any $a \in G_1$, we have

$f(a) \oplus f(a^{-1}) = f(a * a^{-1}) = f(e_1) = e_2$

and $f(a^{-1}) \oplus f(a) = f(a^{-1} * a) = f(e_1) = e_2$

$\therefore$ $f(a^{-1})$ is the inverse of $f(a)$ in G_2

i.e., $[f(a)]^{-1} = f(a^{-1})$

c) $H_2 = f(H_1)$ is the image of H_1 under f; this is a subset of G_2.

Let $x, y \in H_2$.

Then $x = f(a)$, $y = f(b)$ for some $a, b \in H_1$

Since, H_1 is a subgroup of G_1, we have $a * b^{-1} \in H_1$.

Consequently,

$$x \oplus y^{-1} = f(a) \oplus [f(b)]^{-1}$$

$$= f(a) \oplus f(b^{-1})$$

$$= f(a * b^{-1}) \in f(H_1) = H_2$$

Hence, H_2 is a subgroup of G_2.

d) Since $f : G_1 \to G_2$ is an isomorphism, f is a bijection.

$\therefore$ $f^{-1} : G_2 \to G_1$ exists and is a bijection.

Let $x, y \in G_2$. Then $x \oplus y \in G_2$

and there exists $a, b \in G_1$ such that $x = f(a)$ and $y = f(b)$.

$$\therefore f^{-1}(x \oplus y) = f^{-1}(f(a) \oplus f(b))$$

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

$$= a * b$$

$$= f^{-1}(x) * f^{-1}(y)$$

■ This shows that $f^{-1} : G_2 \to G_1$ is an homomorphism as well.

$\therefore$ f^{-1} is an isomorphism.

3.3 Cosets

If H is a sub group of(G, *) and $a \in G$ then the set

$Ha = \{ h * a \mid h \in H\}$ is called a right coset of H in G.

Similarly $aH = \{a * h \mid h \in H\}$ is called a left coset of H is G.

Note:- 1) Any two left (right) cosets of H in G are either identical or disjoint.

2) Let H be a sub group of G. Then the right cosets of H form a partition of G. i.e., the union of all right cosets of a sub group H is equal to G.

3) Lagrange's theorem: The order of each sub group of a finite group is a divisor of the order of the group.

4) The order of every element of a finite group is a divisor of the order of the group.

5) The converse of the lagrange's theorem need not be true.

Ex. If G is a group of order p, where p is a prime number. Then the number of sub groups of G is

a) 1 b) 2 c) p – 1 d) p

Ans. b

Ex. Prove that every sub group of an abelian group is abelian.

Solution: Let (G, *) be a group and H is a sub group of G.

Let $a , b \in H$

$\Rightarrow a , b \in G$ (Since H is a subgroup of G)

$\Rightarrow a * b = b * a$ (Since G is an abelian group)

Hence, H is also abelian.

State and prove Lagrange's Theorem

Lagrange's theorem: The order of each sub group H of a finite group G is a divisor of the order of the group.

Proof: Since G is finite group, H is finite.

Therefore, the number of cosets of H in G is finite.

Let $Ha_1, Ha_2, \dots, Ha_r$ be the distinct right cosets of H in G.

Then, $G = Ha_1 U Ha_2 U \dots, U Ha_r$

So that $O(G) = O(Ha_1)+O(Ha_2) \dots + O(Ha_r)$.

But, $O(Ha_1) = O(Ha_2) = \dots = O(Ha_r) = O(H)$

$\therefore O(G) = O(H)+O(H) \dots + O(H)$. (r terms)

$= r \cdot O(H)$

This shows that O(H) divides O(G).

3.4 **Lattices and Boolean algebra:** Lattices and Partially Ordered sets, Boolean algebra.

Lattice and its Properties:

Introduction:

A lattice is a partially ordered set (L, £) in which every pair of elements a, b Î L has a greatest lower bound and a least upper bound.
The glb of a subset, {a, b} Í L will be denoted by a * b and the lub by a Å b.

.

Usually, for any pair a, b Î L, GLB {a, b} = a * b, is called the **meet** or **product** and LUB{a, b} = a Å b, is called the **join** or **sum** of a and b.

Example1 Consider a non-**empty set S and let P(S) be its power set. The relation Í "contained in" is a partial ordering on P(S). For any two subsets A, BÎ P(S)**
GLB {A, B} and LUB {A, B} are evidently A Ç B and A È B respectively.

Example2 Let I+ be the set of positive integers, and D denote the relation of **"division"** in I+ such that for any a, b Î I+ , a D b iff a divides b. Then (I+, D) is a lattice in which

the join of a and b is given by the least common multiple(LCM) of a and b, that is,
a Å b = LCM of a and b, and the meet of a and b, that is , a * b is the greatest common divisor (GCD) of a and b.

A lattice can be conveniently represented by a diagram.

For example, let Sn be the set of all divisors of n, where n is a positive integer. Let D denote the **relation "division" such that for any a, b Î Sn, a D b iff a divides b.**
Then (Sn, D) is a lattice with a * b = gcd(a, b) and a Å b = lcm(a, b).
Take n=6. Then S6 = {1, 2, 3, 6}. It can be represented by a diagram in Fig(1). Take n=8. Then S8 = {1, 2, 4, 8}

Two lattices can have the same diagram. For example if S = {1, 2, 3} then (p(s), Í) and (S6,D)
have the same diagram viz. fig(1), but the nodes are differently labeled .
We observe that for any partial ordering relation £ on a set S the converse relation ³ is also partial ordering relation on S. If (S, £) is a lattice With meet a * b and join a Å b , then (S, ³) is the also a lattice with meet a Å b and join a * b i.e., the GLB and LUB get interchanged . Thus we have the principle of duality of lattice as follows.

Any statement about lattices involving the operations ^ and V and the relations £ and ³ remains true if ^, V, ³ and £ are replaced by V, ^, £ and ³ respectively.
The operation ^ and V are called duals of each other as are the relations £ and ³..
Also, the lattice (L, £) and (L, ³) are called the duals of each other.

Properties of lattices:

Let (L, £) be a lattice with the binary operations * and Å then for any a, b, c Î L,

- a * a = a   a Ǎ a = a   (Idempotent)
- a * b = b * a   ,   a Å b   = b Å a   (Commutative)
- (a * b) * c = a * (b * c) , (a Å) Å c = a Å (b Å c)

  ○   (Associative)
- a * (a Å b) = a   ,   a Å (a * b) = a   (absorption)

For any a ÎL, a £ a, a £ LUB {a, b} => a £ a * (a Å b). On the other hand, GLB {a, a Å b} £ a i.e., (a Å b) Å a, hence a * (a Å b) = a

Theorem 1

Let (L, £) be a lattice with the binary operations * and Å denote the operations of meet and join respectively For any a, b Î L,

a £ b ó a * b = a ó a Å b = b

Proof

Suppose that a £ b. we know that a £ a, a £ GLB {a, b}, i.e., a £ a * b. But from the definition of a * b, we get a * b £ a.

Hence a £ b => a * b = a .... (1)

Now we assume that a * b = a; but is possible only if a £ b,
that is a * b = a => a £ b   .... (2)
From (1) and (2), we get a £ b ó a * b = a.
Suppose a * b = a.
then b Å (a * b) = b Å a = **a Å b ....** (3)
but b Å (a * b) = b (by iv)**........................** (4)
Hence a Å b = b, from (3) => (4)
Suppose aÅ b = b, i.e., LUB {a, b} = b, this is possible only if a£ b, thus(3) => (1)
(1) => (2) => (3) => (1). Hence these are equivalent.

Let us assume a * b = a.
Now (a * b) Å b = a Å b
We know that by absorption law , (a * b) Å b = b
so that a Å b = b, therefore a * b = a Þ a Å b = b (5)
similarly, we can prove a Å b = b Þ   a * b = a (6)
From (5) and (6), we get
a * b = a Û a Å b = b
Hence the theorem.

Theorem2 For any a, b, c Î L, where (L, £) is a lattice. b
£ c => { a * b £ a * c and
{ a Å b £ a Å c

Proof   Suppose b £ c. we have proved that b £ a ó b * c = b........ (1)

Now consider

(a * b) * (a * c) = (a * a) * (b * c)   (by Idempotent)

= a * (b * c)

= a * b (by (1))

Thus (a * b) * (a * c) = a * b which => (a * b) £ (a * c) Similarly

(a Å b) Å (a Å c) = (a Å a) Å (b Å c)

= a Å (b Å c)

= a Å c

which => (a Å b) £ (a Å c)

note:These properties are known as **isotonicity.**