UNIT - IV

ALGEBRAIC STRUCTURES.

A non empty set G together with 1 or more n-ary operations, say $*$. (Binary). is called an algebraic structures or algebra or system.

We denote it by $[G, *]$

Note:

$+, -, \times, \cdot, *, \cup, \cap$ etc.,. are some of binary operations.

Properties of Binary Operations:-

Let the binary operation be $* : G \times G \to G$.

Then we have the following properties,

1) Closure Properties:-

$a * b = x \in G, \ \forall a, b \in G.$

2) Associative property:

$(a*b)*c = a*(b*c), \ \forall a, b, c \in G.$

3) Identity element :-

$a*e = e*a = a, \ \forall a \in G.$

Here 'e' is called an Identity element.

4) Inverse element:-

If $a*b = b*a = e$ (identity)

then b is called the inverse of a & it is denoted by $b = a^{-1}$.

5) Distributive property:-

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

$(b \cdot c)*a = (b*a) \cdot (c*a) \quad \forall a, b, c \in G.$

6) Commutative property:-

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

7) Cancellation Property:-

$a*b = a*c \Rightarrow b = c$ [Left Cancellation law]

$b*a = c*a \Rightarrow b = c$ [Right Cancellation law]

for all $a, b, c \in G$.

Semi-Group:-

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

1. closure property

$a*b = x \in G, \forall a, b \in G$.

2. Associative property

$(a*b)*c = a*(b*c), \forall a, b, c \in G$.

Then $(G, *)$ is called a semi-group.

Monoid:-

If a non-empty set G with the binary operations * satisfying the following properties

1. closure
2. Associative
3. Identity.

Cyclic monoid:-

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. $x = a^n$ such a cyclic monoid $(M, *)$ is said to be generated by the element a. Here a is called the generated of the cyclic monoid.

Theorem 1:-

Every cyclic monoid (semi group) is commutative.

Proof:-

Let $M, *$ be a cyclic monoid whose generated is $a \in M$. Then for $x, y \in M$, we have $x = a^n$, $y = a^m$ m, n are integers.

Now, $x * y = y * x$ $a^n * a^m$

$= a^{n+m}$

$= a^{m+n}$

$= a^m * a^n$

$= y * x$.

$\therefore M, *$ is commutative.

Group:-

A non empty set G with the binary operation $*$, i.e., $(G, *)$ is called a group if $*$ satisfies the following condition.

1. closure property
2. Associative "
3. Identity "
4. Inverse "

Abelian Group:-

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

Order of a group:-

The no. of elements in a group G is called the order of a group.

It is denoted by $O(G)$. Also it is denoted by $|G|$

If $O(G)$ is finite then G is called a finite ~~too~~ group.

If $O(G)$ is infinite then G is called infinite group.

① Show that $(Q^+, *)$ is an abelian group. where $*$ defined by $a*b = ab/2$.

sol:

Here $(Q^+, *)$ is the set of all positive numbers.

i) closure:-

clearly $a*b = ab/2 \in Q^+$.

ii) Associative:-

$$(a*b)*c = \left(\frac{ab}{2}\right)*c$$

$$= \frac{abc}{4} \longrightarrow Ⓐ$$

$$a*(b*c) = a*\left(\frac{bc}{2}\right)$$

$$= \frac{abc}{4} \longrightarrow Ⓑ$$

from A & B.

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

iii) Identity:

Let e be the identity element

$$a*e = a$$

$$\frac{ae}{2} = a$$

$$\boxed{e = 2}$$

$\therefore$ Identity element is $e = 2 \in Q^+$.

iv) Inverse :-

let a^{-1} be the inverse of a

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

$$\frac{aa^{-1}}{2} = 2.$$

$$aa^{-1} = 4$$

$$a^{-1} = 4/a \in Q^+$$

$\therefore$ Inverse of a is $4/a \in Q^+$.

v) Commutative :

Now $a * b = \frac{ab}{2}$

$$= \frac{ba}{2}$$

$$= b * a. \in Q^+$$

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

2. Show that $(R - \{1\}, *)$ is an abelian group where * is defined by $a*b = a+b+ab.$

sol:

Here $(R-\{1\}, *)$ is the set of all real numbers except

i) closure

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

ii) Associative :-

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

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

$$= a+b+ab+c+ac+bc+abc \quad \text{——} \; (A)$$

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

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

$$= a+b+c+bc+ab+ac+abc \quad \text{——} \; (B)$$

from A & B

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

iii) Identity :-

Let e be an identity element.

$a*e = a$

$\cancel{a} + e + ae = \cancel{a}$

$e(1+a) = 0$

$\boxed{e=0}$

iv) Inverse :-

Let a^{-1} be the inverse of a.

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

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

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

$a^{-1} = \frac{-a}{1+a}$

v) Commutative :-

$a*b = a+b+ab$ — ①

$b*a = b+a+ba$ — ②

$a*b = b*a$.

Hence $(R - \{1\}, *)$ is an abelian group.

2. On Z define $a*b = a+b+1$ where * is the ordinary addition show that $Z, *$ is a group.

Sol:

Here $(Z, *)$ is the set of all integers.

i) closure

clearly $a*b = a+b+1 \in (Z, *)$

ii) Associative :-

$(a*b)*c = (a+b+1)c = a+b+1+c+1$

$= a+b+c+2$ — (A)

$= a+b+c+(a+b+1)c$

$= a+b+c+ac+bc+c$ — (A)

$$a*(b*c) = a*(b+c+1)$$
$$= a+b+c+2+1$$
$$= a+b+c+2 \quad \text{—} (B)$$

from A & B

$$(a*b)*c = a*(b*c) \in Z.$$

3) $a*e = a$

$$a+e+1 = a$$
$$e+1 = 0$$
$$e = -1 \in Z.$$

4) let a^{-1} be the inver of a

$$a*a^{-1} = e$$
$$a+a^{-1}+1 = -1$$
$$a+a^{-1} = -1-1$$
$$a+a^{-1} = -2$$
$$\boxed{a^{-1} = -2-a} \in Z,*$$

$\therefore$ It is a group.

4. Prove that the set $A = \{1, \omega, \omega^2\}$ is an abelian group of order 3 under usual multiplication. where $1, \omega, \omega^2$ are cube roots of units and $\omega^3 = 1$.

sol:

The following is the table of elements in A with usual multiplication.

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

i) closure :-

All the elements in the above table are $\in A$

Hence a is closure.

ii) Associative :-

clearly multiplication of complex numbers are associative.

iii) Identity :-

The Identity element is 1.

iv) Inverse :-

Inverse of 1 is 1

Inverse of ω is ω^2

Inverse of ω^2 is ω.

v) Commutative :-

$1 * \omega = \omega$

$\omega * 1 = \omega$

$\therefore$ A is an abelian group.

5. Show that $\{1, 3, 7, 9\}$ is an abelian group under multiplication modulo 10.

Sol:

Let $G = \{1, 3, 7, 9\}$ and binary operation is $\times_{10}$.

The operation table for $\times_{10}$ is.

$\times_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

~~i) Closure~~:

It is clearly from the table that closure & Associative property are satisfied.

<u>Identity</u>:

Here the identity element is 1.

<u>Inverse</u>:

Inverse of 1 is 1

Inverse of 3 is 7

Inverse of 7 is 3

Inverse of 9 is 9

<u>Commutative</u>:

$a \times_{10} b = b \times_{10} a$ ~~for~~ $\forall\, a, b = 1, 3, 7, 9 \in G$.

$3 * 7 = 1$

$7 * 3 = 1$

$\therefore$ It is abelian.

6. Show that $[Z_5, +_5]$ is an abelian group.

<u>Sol</u>:

The operation table for addition modulo 5 is

$+_5$	0	1	2	3	4
0	$\boxed{0}$	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

It is clearly from that closure & Associative property is true.

Identity:

Here the identity element is 0.

Inverse:

Inverse of 0 is 0
Inverse of 1 is 4.
Inverse of 2 is 3
Inverse of 3 is 2
Inverse of 4 is 1.

Commutative:

$$a +_5 b = b +_5 a \quad \forall a, b \in \{0,1,2,3,4\}$$

$\therefore$ It is abelian.

Show that $(*, R)$ defined by $x * y = x + y + 2xy$ $\forall x, y \in R$. check i) $(R, *)$ is a monoid or not.
ii) Is it commutative.
iii) which elements have inverse and what are they?.

Sol:

i) **Closure:**

$$x * y = x + y + 2xy \in R$$

ii) **Associative:**

$$(x*y)*z = (x+y+2xy)*z.$$

$= \cancel{x+y+2xy+z}$ $\quad x+y+2xy+z+(x+y+2xy)z$

$= \cancel{xz+yz+2xyz}.$

$x*(y*z) = \cancel{x*(x+y+}$ $\quad x+y+2xy+z+$

$(x*y)*z = (x+y+2xy)*z$

$= x+y+2xy+z+2(x+y+2xy)z$

$= x+y+z+2xy+2xz+2yz+4xyz$ — (1)

$x*(y*z) = x*(y+z+2yz)$

$= x+y+z+2yz+2x(y+z+2yz)$

$= x+y+z+2yz+2xy+2xz+4xyz$ — (2)

from (1) & (2)

$(x*y)*z = x*(y*z)$

3) Identity:

$x*e = x$

$x+e+2xe = x$

$e(1+2x) = 0$

$\boxed{e=0} \in R.$

Since *

2) $\therefore (R,*)$ is monoid.

Now $x*y = x+y+2xy$

$= y+x+2yx$

$= y*x.$

$\therefore (R,*)$ is associative.

3) Let a^{-1} be the inverse of an element $a \in R$.

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

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

$x+x^{-1}+2xx^{-1} = 0$

$x^{-1}(1+2x) = -x$

$x^{-1} = \frac{-x}{1+2x}$

Let G denote the set of all matrices of the form $\begin{bmatrix} x & x \\ x & x \end{bmatrix}$ where $x \in R^*$. prove that G is a group under matrix multiplication.

Sol:

Let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$, $x \in R^*$.

i) closure.

Let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$, $B = \begin{bmatrix} y & y \\ y & y \end{bmatrix}$

$$AB = \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \in R^*$$

ii) Associative:

$A = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$, $B = \begin{bmatrix} y & y \\ y & y \end{bmatrix}$ $C = \begin{bmatrix} z & z \\ z & z \end{bmatrix}$

$$(AB)C = \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \begin{bmatrix} z & z \\ z & z \end{bmatrix}$$

$$= \begin{bmatrix} 4xyz & 4xyz \\ 4xyz & 4xyz \end{bmatrix} \text{ — } (1)$$

$$A(BC) = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \begin{bmatrix} 2yz & 2yz \\ 2yz & 2yz \end{bmatrix}$$

$$= \begin{bmatrix} 4xyz & 4xyz \\ 4xyz & 4xyz \end{bmatrix} \text{ — } (2).$$

From (1) & (2)

$$(AB)C = A(BC)$$

iii) Identity:-

Let $E = \begin{pmatrix} e & e \\ e & e \end{pmatrix}$

Then $AE = A$.

$$\begin{bmatrix} x & x \\ x & x \end{bmatrix} \begin{bmatrix} e & e \\ e & e \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$$

$$\begin{bmatrix} 2xe & 2xe \\ 2xe & 2xe \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$$

$$\Rightarrow 2xe = x.$$

$$e = \frac{x}{2x}$$

$$= 1/2$$

$$e = 1/2$$

$$E = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$

$$\therefore AE = E$$

iv) <u>Inverse:</u>

let $\begin{bmatrix} y & y \\ y & y \end{bmatrix}$ be inverse of $\begin{bmatrix} x & x \\ x & x \end{bmatrix}$ of G.

$$\begin{bmatrix} x & x \\ x & x \end{bmatrix}\begin{bmatrix} y & y \\ y & y \end{bmatrix} = \begin{bmatrix} e & e \\ e & e \end{bmatrix}$$

$$\begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$

$$2xy = 1/2$$

$$y = 1/4x$$

$\therefore \begin{bmatrix} 1/4x & 1/4x \\ 1/4x & 1/4x \end{bmatrix}$ is the inverse of G.

$\therefore$ G is a group.

Pg. No 4.10
– 2nd problem.

Properties of Group:-

Property 1

1. The identity element in a group is unique.

Proof:-

Let e_1 & e_2 be two identity element of G.

$e_1 * e_2 = e_1$ taking e_2 as identity and $e_1 * e_2 = e_2$

taking e_1 as identity.

$\therefore e_1 = e_2$.

Property 2

The inverse of a every element in a group is unique.

Proof:-

Let $(G, *)$ be a group with identity element e

Let B & C be inverse of an element $a \in G$

$a * B = B * a = e,$

$a * c = c * a = e.$

$b = b * e$

$= b * (a * c)$

$= (b * a) * c$

$= e * c.$

$\boxed{b = c}$

Property 3:

Let G be a group. If $a, b \in G$. Then $(a * b)^{-1} = b^{-1} * a^{-1}$. or The inverse of the product of 2 elements is equal to the product of the inverses in reverse order.

Proof:-

Let $a, b \in G$ and a^{-1}, b^{-1} be inverse of a, b.

Therefore $a * a^{-1} = e = a^{-1} * \cancel{b^{-1}} a$

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

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

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

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

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

$$= e \quad \text{--- (1)}$$

Similarly we can prove that $(b^{-1}*a^{-1})*(a*b) = e$ — (2)

From (1) & (2) we get

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

(i.e.,) The inverse of $a*b = b^{-1}*a^{-1}$.

Property 4:-

prove that a group $(G, *)$ is abelian if and only if $(a*b)^2 = a^2 * b^2$, $\forall a, b \in G$.

proof:-

Assume that G is an abelian

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

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

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

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

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

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

Conversely,

assume that $(a*b)^2 = a^2 * b^2$.

Implies

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

$\Rightarrow (a*(b*(a*b))) = [a*(a*(b*b))]$

$\Rightarrow b*(a*b) = a*(b*b)$ $\because$ Left Cancellation law

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

$\Rightarrow b*a = a*b$

$\because$ right Cancellation law.

$\therefore$ G is abelian.

Property 5:-

Prove that in an abelian group $(ab)^2 = a^2b^2$.

Proof:-

$(ab)^2 = (ab)(ab)$

$= a(ba)b$ $\because$ G is abelian.

$= a(ab)b$

$= a^2 b^2$

~~Proof~~

~~Show~~

Property 6:-

Show that $(G,*)$ is abelian if and only if

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

Proof:-

Assume that G is abelian.

$\therefore a*b = b*a$. $\forall a,b \in G$.

Taking inverse on b/s,

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

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

Conversely,

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

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

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

$$a*b = b*a$$

$\therefore G$ is an abelian.

Property 7:-

In a group $(G, *)$ the left and right cancellation laws are true.

(i.e.) Left $(a*b = a*c \Rightarrow c = b.)$ $(b*a = c*a \Rightarrow b = c)$. Right.

Proof:

Let G^* be a group.

Let $A \in G$ and hence $A^{-1} \in G$ then $a*a^{-1} = a^{-1}*a = e$.

i) Left Cancellation law,

Let $a*b = a*c$

pre multiply a^{-1} on b/s,

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

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

$$e*b = e*c$$

$$b = c$$

ii) Right Cancellation law,

Let $b*a = c*a$

post multiply a^{-1} on b/s.

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

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

$$b*e = c*e$$

$$b = c.$$

property 8 :-

Show that the set $G = \{1, -1, i, -i\}$ consisting of the 4 roots of unity is a commutative group under multiplication.

proof:-

$\cdot$	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

All the elements in this table belong to G. Hence G is closed. (or) closure.

Here 1 is the Identity Element.

Inverse of 1 is 1

Inverse of -1 is -1

Inverse of i is -i

Inverse of -i is i

obviously,

$$i * -i = 1$$

$$-i * i = 1$$

$\therefore$ commutative is true under multiplication.

Homomorphism:-

Let G and G' be any two groups. A maping ϕ from G to G'.

$\phi : G \to G'$ is called Homomorphism of group G into G' if $\phi(ab) = \phi(a)\phi(b)$, $\forall a,b \in G$.

Isomorphism:-

Let G and G' be any two groups a mapping $\phi : G \to G'$ is called an Isomorphism of G into G'.

If

i) $\phi(ab) = \phi(a)\phi(b)$, $\forall a,b \in G$.

ii) ϕ is ~~are~~ one - one

Semi group Homomorphism:-

Let $(A, *)$ and (B, Δ) be any two semi groups with binary operations $*$ and Δ respectively.

The mapping $f : A \to B$. is called semigroup Homomorphism.

If $f(a*b) = f(a) \Delta f(b)$ $\forall a,b \in f$

Semigroup Monomorphism:-

A one - one semigroup ~~hom~~ homomorphim is called a semigroup monomorphism.

Semigroup Epimorphism:-

A onto semigroup homomorphism is called semigroup Epimorphism.

Theorem:-

Let $[S, *]$ be a semi group. Then there is a homomorphism $g : S \to S^S$.

where $(S^S, \circ)$ is the semigroup of functions from $S \to S$ under the operations of composition.

proof:-

Let $a \in S$. Define a map $f_a : S \to S$ by

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

$$\text{Now } f_{a*b}(c) = (a*b)*c$$
$$= a*(b*c)$$
$$= f_a(b*c)$$
$$= f_a(f_b(c))$$
$$= f_a \circ f_b(c)$$

$$\therefore f_{a*b} = f_a \circ f_b$$

Now define a map $g : S \to S^S$ by $g(a) = f_a$

Let $a, b \in S$

$$\text{Then } g(a*b) = f_{a*b}$$
$$= f_a \circ f_b$$
$$= g(a) \circ g(b)$$

$$\therefore g(a*b) = g(a) \circ g(b)$$

$\therefore g$ is a homomorphism from S into S^S.

Sub group:-

Let $(G,*)$ be a group then $(H,*)$ is said to be sub group of $(G,*)$. If $H \subseteq G$ and $(H,*)$ itself is a group under the operation $*$. (i.e.,) $(H,*)$ is said to be subgroup of $(G,*)$ if

1. $e \in H$ (e is the identity in G)
2. for any $a \in H$, $a^{-1} \in H$.
3. for $a, b \in H$, $a*b \in H$.

For Example

$(Q,+)$ is a subgroup of $(R,+)$ and

$(R,+)$ is a subgroup of $(C,+)$

Note:-

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

Theorem 1:-

1. The intersection of two subgroups of a group is also a subgroup of the group (or) Let G be a group and H_1 and H_2 are subgroup of G then, $H_1 \cap H_2$ is also a subgroup of G.

Proof:-

Since H_1 and H_2 are subgroup of G. Therefore $H_1 \cap H_2 \neq \phi$ (since atleast the identity element is present in H_1 & H_2).

let $a, b \in H_1 \cap H_2$

$\Rightarrow a, b \in H_1$ and $a, b \in H_2$.

$\Rightarrow a * b^{-1} \in H_1$ and $a * b^{-1} \in H_2$.

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

For $a, b^{-1} \in H_1 \cap H_2$. we have $a * b^{-1} \in H_1 \cap H_2$.

$\therefore H_1 \cap H_2$ is a sub-group.

Theorem2:-

The union of two subgroups of a group G is a subgroup if and only if one is contained in the other. (or) let H & K be two subgroups of a group G then $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

proof:-

Assume H & K are two subgroups of G. and $H \subseteq K$ or $K \subseteq H$. $\therefore$

Therefore $H \cup K = K$ or $H \cup K = H$, Hence $H \cup K$ is a subgroup.

Conversely,

Suppose $H \cup K$ is a subgroup of G.

we claim that to prove $H \subseteq K$ or $K \subseteq H$.

Suppose that H is not contained in K. and K is not contained in H.

Then, there exists elements a, b such that

$a \in H$ and $a \notin K$. —(1)

$b \in K$ and $b \notin H$ —(2)

clearly, $a, b \in H \cup K$.

Since $H \cup K$ is a subgroup of G, $ab \in H \cup K$.

Hence

$ab \in H$ (or) $ab \in K$.

Case 1:-

Let $ab \in H$ since $a \in H$, $a^{-1} \in H$

Hence $a^{-1}(ab) = b \in H$ which is contraction $\Rightarrow\Leftarrow$ to ①.

Case 2:

Let $ab \in K$ since $b \in K$, $b^{-1} \in K$.

Hence $b^{-1}(ab) = a \in K$. which is $\Rightarrow\Leftarrow$ to ①.

$\therefore$ Our assumption is wrong

Hence $H \subseteq K$ or $K \subseteq H$.

Morphism of group:-

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

A maping $f : G \rightarrow H$ is said to be a Homomorphism if $f(a * b) = f(a) \Delta f(b)$ for any $a, b \in G$.

Theorem 1:-

Homomorphism preserve identities.

Proof:-

Let $a \in G$.

Let f be a homomorphism from $(G, *)$ int $(G', *)$

Clearly, $f(a) \in G'$.

$f(a) * e^{-1} = f(a)$ [$\because e'$ is the identity in G']

$= f(a * e)$ [$\because e$ is the identity in G]

$= f(a) * f(e)$ [$\because f$ is a homomorphism]

$e' = f(e)$

$\therefore f$ is pres~~ence~~rves identity.

Theorem 2:-

Homomorphism preserves inverse.

proof:-

Let $a \in G$. Since G is a group, $a^{-1} \in G$.

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

$= f(a) * f(a^{-1})$ $\because f$ is homomorphism.

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

$f(a^{-1})$ is the inverse of $f(a) \in G'$.

$\therefore f$ is preserves Inverse.

Kernel of 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 a Kernel of f. And it is denoted by $\ker(f)$

$\ker(f) = \{x \in G \mid f(x) = e'\}$

Isomorphism:

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

1) f is homomorphism.

(i.e.,) $f(a * b) = f(a) \Delta f(b)$ $\forall a, b \in G$.

2) f is one-one.

3. f is onto

Cosets:-

1. Left coset of H in G: Let $(H,*)$ be a subgroup of $(G,*)$. For any $a \in G$, the left coset of H denoted by $a*H$ is the set $a*H = \{a*h, h \in H\}, \forall a \in G$.

2. Right coset of H in G:

The right coset of H denoted by $(H*a)$ is the set $H*a = \{h*a, h \in H\}, \forall \in G$.

Results:-

1. Both left or right coset of H in G is non empty.

2. Since $e \in H$, $e*H = H = H*e$

3. $H*a$ & $a*H$ are also subsets of G.

4. If G is abelian then $a*H = H*a$

5. The union of all left or right cosets of H in G is equal to G.

Theorem:-1

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

Proof:-

Let $a \in H*b$

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

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

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

$\Rightarrow H*(a*b^{-1}) = H$ $[\because a \in H \Rightarrow H*a = H]$

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

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

$\Rightarrow H*a = H*b.$

Similarly

Let $a \in b*H$

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

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

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

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

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

$\Rightarrow a*H = b*H$

Theorem 2:-

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

Proof:-

Let $H*a$ and $H*b$ be two right cosets of a sub group H of G.

Let $a, b \in G$ we have to prove that either $(H*a) \cap (H*b) = \phi$ (or) $H*a = H*b$

Suppose $H*a \cap H*b \neq \phi$

then there exists an element $x \in (H*a) \cap (H*b)$

$\Rightarrow x \in H*a$ and $x \in H*b$

Now $x \in H*a$

$\Rightarrow H*x = H*a$ (by previous theorem) —— ①

and $x \in H*b$

$\Rightarrow H*x = H*b$ —— ②

from ① & ②

$H*x = H*a = H*b$

$\therefore H*a = H*b$

Hence either $(H*a) \cap (H*b) = \phi$ (or) $H*a = H*b$

Theorem:-

Lagrange's theorem:-

Statement:

The order of a sub group of a finite group is a divisor of the order of the group (ie.,) if H is a subgroup of a finite group $(G,*)$ then $o(H)$ divides $o(G)$

Proof:-

Let $(G,*)$ be a finite group of ~~o(n)~~ order n. and H be a subgroup of G with $o(H) = m$. Here, $o(G) = n$.

We have to show that m divides n.

Since H contains m distinct elements, every left coset of H. contains exactly m elements.

We know that left cosets of H are either identical or distinct and collection of distinct left cosets of H is the group G.

Since G is a finite group, G has a finite number of distinct left cosets of H.

Let a_1*H, a_2*H, ... a_k*H. be the distinct left cosets of H.

Then $G = a_1 * H \cup a_2 * H \cup \dots \cup a_k * H$.

$\Rightarrow O(G) = O(a_1 * H) + O(a_2 * H) \dots + (a_k * H)$

$n = m + m + \dots + m$ (K times)

$n = mK$

$\Rightarrow \boxed{\frac{n}{m} = K}$

$\therefore m$ divides n.

This means that $O(H)$ divides $O(G)$

Normal subgroup:-

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

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

Altenately a subgroup $H(G)$ is called a normal subgroup of G if $x * h = h * x$. $\forall x \in G$.

Theorem 1:-

A subgroup H of a group G is normal if and only if $x * h * x^{-1} = H$ $\forall x \in G$.

proof:

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

$\Rightarrow x * H * x^{-1} \subseteq H$

$\therefore H$ is a normal subgroup of G.

Conversely,

Let us assume that H is a normal subgroup of G. $\therefore x * H * x^{-1} \subseteq H$. —— ①

$x \in G \Rightarrow x^{-1} \in G$

$x^{-1} * H * (x^{-1})^{-1} \subseteq H$, $\forall x \in G$.

$\Rightarrow x^{-1} * H * x \subseteq H$

$\Rightarrow x * (x^{-1} * H * x) * x^{-1} \subseteq x * H * x^{-1}.$

$\Rightarrow (x * x^{-1}) * H * (x * x^{-1}) \subseteq x * H * x^{-1}.$

$\Rightarrow H \subseteq x * H * x^{-1}$ —— ②

from ① & ②

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

Theorem 2:-

The intersection of any two normal subgroups of a group is a normal subgroup. (or) If H & K are normal subgroups of G. Then, $H \cap K$ is also a normal subgroup.

Proof:-

Given H & K are normal subgroups

$\Rightarrow$ H & K are subgroups of G.

$\Rightarrow H \cap K$ is a subgroup of G.

Now, we have to prove that $H \cap K$ is normal.

Let $x \in G$ and $h \in H \cap K$.

$x \in G$ and $h \in H$ and $h \in K$.

Now, $x \in G$, $h \in H$ and $x \in G$, $h \in K$.

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

$x * h * x^{-1} \in K$ —— ②

Since H & K are normal subgroup.

$\therefore$ from ① & ②

$x * h * x^{-1} \in H \cap K.$

Hence $H \cap K$ is a normal subgroup of G.

Theorem 3:-

Let G & G' be any two groups with identity element e & e' respectively. If $f: G \to G'$ be a homomorphism then $Ker(f)$ is a normal subgroup.

proof:-

e is an identity in G.

e' is an identity in G'.

Let $K = Ker(f) = \{x \in G / f(x) = e'\}$

W.K.T. $Ker(f)$ is a subgroup of G.

Now to prove: $Ker(f)$ is normal

For, let $a \in G$ and $h \in K$.

$$\therefore f(x * h * x^{-1}) = f(x) * f(h) * f(x^{-1})$$
$$= f(x) * e' * f(x^{-1})$$
$$= f(x) * f(x^{-1})$$
$$= f(x * x^{-1})$$
$$= f(e)$$
$$= e'$$

$$\therefore f(x * h * x^{-1}) = e'$$

$\Rightarrow x * h * x^{-1} \in K$

$\therefore$ For $x \in G$, $h \in K$

we have $x * h * x^{-1} \in K$.

$\therefore Ker(f) = K$ is a normal subgroup of G.

Natural Homomorphism:-

Let H be a normal subgroup of a G. The map $f : G \rightarrow \frac{G}{H}$. such that $f(x) = H * x$, $x \in G$. is called a natural Homomorphism of the group G onto the Quotient group $\frac{G}{H}$

Theorem 1:-

Fundamental theorem on Homomorphism of groups.

Statement:-

Every homomorphic image of a group G is isomorphic to some quotient group of G. Or Let $f : G \rightarrow G'$. be a onto homomorphism of groups with Kernel K. Then $\frac{G}{K} \cong G'$.

Proof:-

Let f be a homomorphism $f : G \rightarrow G'$.

Let G' be the homomorphic image of a group G.

Let K be the Kernel of this homomorphism.

clearly K is a normal subgroup of G.

To prove $\frac{G}{K} \cong G'$

Define $\phi : \frac{G}{K} \longrightarrow G'$ by $\phi(K * a) = f(a)$, $\forall\, a \in G$.

1) ϕ is well defined:-

we have $K * a = K * b$

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

$\Rightarrow f(a * b^{-1}) = e'$ [$\because e'$ identity in G']

$\Rightarrow f(a) * f(b^{-1}) = e'$ [$\because f$ is homomorphism]

$\Rightarrow f(a) * [f(b)]^{-1} = e'$

$\Rightarrow f(a) * [f(b)]^{-1} * f(b) = e' * f(b)$

$$f(a)=f(b)$$
$$\Rightarrow \phi(K*a)=\phi(K*b)$$

$\therefore \phi$ is well defined.

2) ϕ is one-one:-

To prove: $\phi(K*a)=\phi(K*b) \Rightarrow K*a=K*b$

W.K.T

$$\phi(K*a)=\phi(K*b)$$
$$\Rightarrow f(a)=f(b)$$
$$\Rightarrow f(a)*f(b^{-1})=f(b)*f(b^{-1})$$
$$=f(b*b^{-1})$$
$$=f(e)$$

$$f(a)*f(b^{-1})=e'$$
$$\Rightarrow f(a*b^{-1})=e'$$
$$\Rightarrow a*b^{-1}\in K$$
$$\Rightarrow K*a=K*b$$ $\therefore \phi$ is one-one.

3) ϕ is onto:-

Let $y\in G'$. Since f is onto,

there exists $a\in G$ such that $f(a)=y$

Hence $\phi(K*a)=f(a)=y$

$\therefore \phi$ is onto

4.) ϕ is homomorphism.

Now, $\phi(K*a*K*b)=\phi(K*a*b)$
$$=f(a*b)$$
$$=f(a)*f(b)$$
$$=\phi(K*a)*\phi(K*b)$$

$\therefore \phi$ is a homomorphism.

Since, ϕ is one-one, onto and homomorphism.

$\therefore \phi$ is an isomorphism between $\frac{G}{K}$ and G'.

Hence $\frac{G}{K}\cong G'$.

Cyclic groups:-

Let G be a group. Let $a \in G$ then $H = \{a^n / n \in Z\}$ is a subgroup of G. H is called a cyclic subgroup of G generated by a. And it is denoted by $\langle a \rangle$.

Theorem:-

Every cyclic group is an abelian group.

Proof:-

Let $(G, *)$ be cyclic group with generated $a \in G$.

For $x, y \in G \Rightarrow x = a^n, y = a^m$, m and n are integers.

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

$\therefore (G, *)$ is an abelian group.

Rings:-

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

1. $(R, +)$ is an abelian group.
2. $(R, \cdot)$ is a semigroup.
3. The operation multiplication is distributive over addition. (i.e.,) $\forall a, b, c \in R$ $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$

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

Commutative ring:-

If in a ring R, the multiplication operation is also commutative. (i.e.,) $ab = ba$. $\forall a, b \in R$.

Then R is called a commutative ring.

Zero devices:-

If a and b are two non-zero elements of a ring R. such that $a \cdot b = 0$. Then a and b are called zero devices.

Integral domain:-

A commutative ring $(R, +, \cdot)$ with identity and without zero devices is called an integral domain.

Ex:-

$(Z, +, \cdot)$ is an integral domain.

Field:-

A commutative ring with identity $(R, +, \cdot)$ is called a field. If every non-zero elements has a multiplicative inverse. Thus, $(R, +, \cdot)$ is a field if,

1. $(R, +)$ is an abelian group.
2. $\{R - \{0\}, \cdot\}$ is also abelian group.

Ex:-

1. $(R, +, \cdot)$ is a field.
2. $(Q, +, \cdot)$ is a field.
3. $(Z, +, \cdot)$ is not a field.

Permutations functions:-

A bisection from a set A to itself is called a permutation of A.

Note:- Sn has n factorial permutations.

List all the elements of symmetric set S_3 where $S = \{1, 2, 3\}$

sol:

The elements of symmetric set S_3 are

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Cyclic permutation:-

The permutation f defined on $S = \{a_1, a_2, \dots a_r\}$ is said to be cyclic if $f(a_1) = a_2$, $f(a_2) = a_3$, ... $f(a_{r-1}) = a_r$ and $f(a_r) = a_1$. and $f(b) = b$. for all other elements.

Ex:

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

This is a cyclic permutation. It is represented by a cyclic $(1\ 3\ 2)$

2. $$G = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$$

This is cyclic permutation. It is represented by $(1\ 3\ 4)$

Both f and g are represented by a cyclic of length 3.

The no. of elements in the cyclic gives the length of the cyclic.

Transposition:-

A cyclic of length 2 is called a transposition

Even & odd permutations:-

A permutations is said to be an even permutations if it is expressed as a product of even number of transposition. otherwise it is said to be an odd permutation.

1. Show that the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}$ is odd, while the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ is even.

Sol:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}$$

$= (1\ 5)(2\ 6\ 3)$

$= (1\ 5)(2\ 6)(2\ 3)$

= odd.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

$= (1\ 6)(2\ 3\ 4\ 5)$

$= (1\ 6)(2\ 3)(2\ 4)(2\ 5)$

= even.

If $A = (1\ 2\ 3\ 4\ 5)$, $B = (2\ 3)(4\ 5)$ find AB.

Sol:

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$$

$$AB = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

$$= (1\ 3\ 5)$$

2) Let $A = \{1, 2, 3, 4, 5, 6\}$

and $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$

be a permutation of A

1) compute P^{-1}

2) comput P^2.

Sol:

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$$

$$P^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}$$

$$P^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$$

$= P.P.$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}$$

Theorem 6 : *Cayley's Theorem:*

Every finite group of order 'n' is Isomorphic to permutation group of degree 'n'.

Solution :

We shall prove this theorem in 3 steps.

<u>*Step -1:*</u> We shall first find a set G′ of Permutation.

<u>*Step -2:*</u> We prove G′ is a group.

<u>*Step -3:*</u> Exhibit an Isomorphism $\phi : G \to G'$.

<u>*Step -1:*</u>

Let G be finite group of order *n*.

Let $a \in G$.

Define $f_a : G \to G$ by $f_a(x) = ax$

Since $f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y$

f_a is 1 – 1.

Since, if $y \in G$, then $f_a(a^{-1}y) = aa^{-1}y = y$

f_a is onto.

Thus, f_a is a bijection.

Since G has '*n*' elements, f_a is just permutation on '*n*' symbols.

Let $G' = \{f_a / a \in G\}$

<u>*Step -2:*</u>

G′ is a group.

Let $f_a, f_b \in G'$

$$f_a \circ f_b(x) = f_a(f_b(x)) = f_a(bx) = abx = f_{ab}(x)$$

Hence $f_a \circ f_b = f_{ab}$. Hence G′ is closed

$f_e =$ G′ is the identity element.

The inverse of f_a in G′ is f_a^{-1}.

$\therefore$ G′ is a group.

<u>***Step – 3 :***</u>

We prove G and G′ are Isomorphic.

Define $\quad \phi : G \to G'$ by $\phi(a) = f_a$

$$\phi(a) = \phi(b) \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x)$$

$$\Rightarrow ax = bx \Rightarrow a = b$$

Hence ϕ is 1 – 1.

Since f_a is onto ϕ is onto.

Also $\quad \phi(a\,b) = f_{ab} = f_a \circ f_b = \phi(a) \circ \phi(b)$

$\therefore \phi : G \to G'$ is an Isomorphism.

$\therefore \qquad G \simeq G'$

Hence the proof.

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 ker f is a subgroup.

Proof :

We know that

$$ker(f) = \left\{ x \in G \,/\, f(x) = e' \right\}$$

Since $f(e) = e'$ is always true, atleast $e \in ker(f)$.

In otherwords $ker(f)$ is not empty in G.

Let the two elements $a, b \in ker(f)$,

Therefore, $f(a) = e'$ and $f(b) = e'$

Now, $f(a * b^{-1}) = f(a) * f(b^{-1})$ [f is homomorphism]

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

$$= e' * e'$$

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

$$\Rightarrow \quad a * b^{-1} \in ker(f)$$

$$a, b \in ker(f) \Rightarrow a * b^{-1} \in ker(f)$$

$\therefore$ $ker(f)$ is a subgroup of G.