UNIT-2

Algebraic Structure

Lecture No-10

(Ref Pt · 2·1)

Algebraic Structure :-

A non-empty set G equipped with one or more binary operations is called an algebraic structure.

Let symbols $*, +, \cdot, \circ, \oplus, \cup, \cap, \vee, \wedge$ etc denote binary operations on a set G. Then $(G, *), (G, +), (G, *, \circ, \vee, \wedge)$ etc are algebraic structure.

$(N, +)$ $(I, +)$ $(I, -)$ $(R, +)$ $(R, +, \cdot)$ are all algebraic structures.

1. **Semi-Group**

Let G be a non-empty set and $*$ be a binary operation on G. $(G, *)$ is said to be semi-group if the operation $*$ is associative.

OR.

$(G, *)$ is a semi-group if

(i) $x * y \in G \quad \forall\ x, y \in G$

(ii) $(x * y) * z = x * (y * z) \quad \forall\ x, y, z \in G.$

2. **Identity element**

Let $*$ be a binary operation on a non-empty set G. An element $e \in G$ is said to be an identity element for the operation $*$, if

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

It may be observed that a semi-group $(G, *)$ need not have an identity element w.r.to oper^n $*$.

3. **Monoid :-**

A semigroup $(M, *)$ with an identity element w.r.t. operation $*$ is called monoid.

OR

An algebraic system $(M, *)$ is called monoid, if

(i) M is closed w.r. to $*$ ie if $x, y \in M$ then $x * y \in M$.

(ii) $*$ is an associative operation ie for any $x, y, z \in M$
$x * (y * z) = (x * y) * z$.

(iii) Existence of identity element ie. there exist an element $e \in M$ such that
$e * x = x * e = x$, for any $x \in M$

Example Let S be any non-empty set, consider the power set $P(S)$ together with the operation $\cup$ of union of two sets, then $(P(S), \cup)$ is a monoid with empty $\emptyset$ as identity element.

Qu Let $(\{a, b\}, *)$ be a semi-group where $a * a = b$ show that

(i) $a * b = b * a$ (ii) $b * b = b$.

Solution Given that $a * a = b$

(i) $a * b = b a * (a * a)$
$= (a * a) * a$ { ~~Commutative~~ Associative property
$= b * a$ As group is semi-group

$a * b = b * a$ Proved.

(ii) Since $(\{a, b\}, *)$ is a semi-group, it must be closed w.r. to operation $*$. We are given that $a * a = b$ so $a * b$ must be equal to a.

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

Hence $b * b = b$

3. Sol^n Let $(A,*)$ be a semi group. Furthermore, for every a & b in A, if $a \neq b$ then $a*b \neq b*a$.

(i) show that for every $a \in A$, $a*a = a$.

(ii) show that for every $a, b \in A$, $a*b*a = a$.

(iii) show that for every $a, b, c \in A$

$$a*b*c = a*c$$

Sol^n

$$a \neq b \Rightarrow a*b \neq b*a \equiv a*b = b*a \Rightarrow a = b \quad \text{---(1)}$$

(i) By closure property, for any $a \in A$, $a*a \in A$

Again by associative law we have

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

$$a*a = a \qquad [\text{by } 1]$$

$a*a = a$ whenever $a \neq b \Rightarrow a*b \neq b*a$.

(ii) for any $a, b \in A$ we have

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

$$= a*(b*a) \quad \text{---(2)}$$

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

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

$$= a*(b*a) \quad \{\because a*a = a\} \quad \text{---(3)}$$

from (2) & 3 we have

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

$$a*b*a = a \qquad [\text{by } 1] \quad \text{---(4)}$$

(iii) for $a, b, c \in A$ we have

$a*b, c \in A$ and $a, b*c \in A$ by closure property

$(a*b)*c \in A$ and $(a*(b*c) \in A$ " "

$$(a*b)*c = a*(b*c) = a*b*c \in A$$

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

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

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

$= a*(b*c)$ (using 4)

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

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

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

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

$a*b*c = a*c$

Proved

Que Prove that $(A, +)$ is a semi-group, where A be the set of all positive integers and + be ordinary addition operation.

Lecture No-11

Ref Pt - 2.2

Group: An algebraic structure $(G, *)$ where G is a non-empty set and '$*$' is a binary operation defined on G, is called group, if the oper^n $*$ satisfies the following postulates (Group Axioms)

(a) **Closure Property** :-

If a & b belong to G then $a*b$ also belongs to G.

ie $a \in G,\ b \in G \Rightarrow a*b \in G \ \forall\ a, b \in G$.

(b) **Associativity** The binary oper^n $*$ is associative ie if a, b, c are the elements of G then

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

(c) **Existence of Identity** :

There exists an element e in G such that $e*a = a = a*e \ \forall\ a \in G$. The element e is called the identity.

(d) **Existence of Inverse** : for each element $a \in G$, there existence an element of G is called the inverse of a and denoted by a^{-1} such that

$$a^{-1}*a = e = a*a^{-1}$$ { where e is identity element for $*$ }

Abelian Group or Commutative Group

A Group $(G, *)$ is said to be abelian or commutative if in addition to four group axioms the following postulate is also satisfied -

commutativity The binary operation $*$ in G is commutative ie. $a*b = b*a \ \forall\ a, b \in G$.

Order of a finite Group :-

The number of element in a finite group is called the "Order of the Group".

An infinite group is said to be of infinite order.

Que Let $A = \{a, b\}$ which of the following tables define a semi group? which define a monoid on A

*	a	b
a	b	a
b	a	b

(i)

*	a	b
a	b	b
b	a	a

(ii)

*	a	b
a	a	b
b	b	a

(iii)

(i) We have from (i)

Closure since all entries in composition table are in set A. Hence closure property satisfied.

Associativity since there are only two element in the set A. Hence associativity is always satisfied.

Identity $\forall$ elements of A $\exists$ an element $b \in B$ such that $b * a = a$ and $b * b = b$

Hence (i) is semi-group as well as monoid

(ii) Again table (ii) satisfies closure & associativity & there is no identity. Hence it is semigroup but not monoid.

(iii) In table (iii) closure & associativity is satisfied, $\exists$ $\forall$ element of A there exist $a, b \in A$ such that identity of A.

Therefore it is semi-group as well as monoid.

Show that the set of all $(m \times n)$ matrices having their elements as integer is an infinite abelian group with matrix addition as the composition.

Sol" **Closure Property**

Let A & B be two matrices of order $(m \times n)$ and $A, B \in M$. Then $A + B \in M$ because sum of two matrices of the same type is a matrix of same type.

Thus M is closed w.r to Matrix addition

Associative law Let $A, B, C \in M$ & let

$$A = [a_{ij}]_{m \times n} \quad B = [b_{ij}]_{m \times n} \quad C = [c_{ij}]_{m \times n}$$

$$A + (B + C) = [a_{ij}]_{m \times n} + \{[b_{ij}]_{m \times n} + [c_{ij}]_{m \times n}\}$$

$$= [a_{ij}]_{m \times n} + [b_{ij} + c_{ij}]_{m \times n}$$

$$= [(a_{ij}) + (b_{ij} + c_{ij})]_{m \times n}$$

$$= [(a_{ij} + b_{ij}) + c_{ij}]_{m \times n}$$

$$= [(a_{ij} + b_{ij})]_{m \times n} + [c_{ij}]_{m \times n}$$

$$= (A + B) + C$$

Thus oper" of addition of matrix is associative.

Existence of Identity element

If $O = (O_{m \times n})$ is a null matrix in M then $A \in M$, $O \in M \Rightarrow O + A = A$. Thus Null matrix is Identity element

Existence of Inverse: Let $(-A) \in M$ then $A \in M$ where $(-A)$ is the matrix whose elements are the negative of the corresponding elements of A.

Also $A + (-A) = (-A) + A = O$

Thus $(-A)$ is inverse of matrix.

Commutative Law. Let $A = [a_{ij}]_{m \times n} \quad B = [b_{ij}]_{m \times n}$

$$A + B = [a_{ij}]_{m \times n} + [b_{ij}]_{m \times n} \Rightarrow [a_{ij} + b_{ij}]_{m \times n}$$

$$= [b_{ij} + a_{ij}]_{m \times n} = B + A.$$

Thus $(M, +)$ is Abelian Group

Qu The set $P(S)$ of all possible subset of a non empty S under the composition '$*$' defined by the rule. $(A * B) = A \cup B \quad \forall \; A \subseteq S, B \subseteq S$.

Show that $P(S)$ is not a group, but it is monoid.

Solution :-

Closure Property $A \subseteq S, \; B \subseteq S \Rightarrow A \cup B \subseteq S$

$A \cup B \in P(S)$

Therefore $P(S)$ is closed w.r to given composition.

Associativity We know that the union of sets always obey associative law -

$A \cup (B \cup C) = (A \cup B) \cup C$

Existence of Identity since $A \cup \phi = A = \phi \cup A$.

Therefore empty set $\phi \in P(S)$ is identity element for composition '$*$'

Let $A \in P(S)$ and $A = \phi$ & if its inverse is B.

Then $A * B = A \cup B \neq \phi$ {identity element}

Therefore no member of $P(S)$ can be the left inverse of A. Thus $P(S)$ is not a group, but it is monoid under the given composition.

5 c) Show that the set of cube roots of unity is an Abelian group w.r to multiplication.

Hⁿ Cube roots of unity are obtained by solving the following equation.

$$x^3 - 1 = 0$$

$$(x-1)(x^2+x+1) = 0$$

$$x = 1, \quad x = \frac{-1 \pm \sqrt{1-4}}{2} \Rightarrow -\frac{1}{2} \pm \frac{1}{2} i\sqrt{3}$$

$$G_1 = \left\{ 1, -\frac{1}{2} + \frac{i\sqrt{3}}{2}, -\frac{1}{2} - \frac{i\sqrt{3}}{2} \right\}$$

If we put $-\frac{1}{2} + \frac{i\sqrt{3}}{2} = \omega$ then $-\frac{1}{2} - \frac{i\sqrt{3}}{2} = \omega^2$

and $\omega^3 = 1$

$$G_1 = \{1, \omega, \omega^2\}$$

Now we form a composition table

·	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Here $\omega \cdot \omega^2 = \omega^3 = 1$ and $\omega^2\omega^2 = \omega^4 = \omega^3 \cdot \omega = \omega$

1 Closure property: Since all the entries in composition table are the element of G_1, thus G_1 is closed w.r to multiplication.

2. Associativity: Since the elements of G_1 are all complex number & we know that multiplication of complex numbers is associative because -

$(1 \cdot \omega) \cdot \omega^2 = 1 \cdot (\omega \cdot \omega^2)$ etc.

2. Existence of Identity from the composition table we see that - $1(1) \cdot 1$, $1 \cdot (\omega) = \omega = \omega \cdot 1$, $1 \cdot \omega^2 = \omega^2 = \omega^2 \cdot 1$

Therefore 1 is the left identity.

Existence of Inverse -

from composition table, we find that $1 \cdot 1 = 1$ (identity)

Therefore, the inverse of element $1 \in G$ is 1 itself.

ie $\omega \cdot \omega^2 = \omega^2 \cdot \omega = 1$

$\omega^{-1} = \omega^2 \in G$ & $(\omega^2)^{-1} = \omega \in G$.

Thus, the inverse of every element of G exist.

Commutative law We know that the multiplication of Complex number is commutative.

Therefore G is abelian group :

Que Show that the set of fourth roots of unity forms an abelian group w.r.to multiplication

Solution : $x = 1^{1/4} \Rightarrow x^4 - 1 = 0$

$(x^2+1)(x^2-1) = 0$

$x = -1, +1, i, -i$

composition table is given as

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

1. Closure Property

since all entries in the composition table are the element of the set G.

Therefore the set G is closed w.r. to multiplication & the oper^n of multiplication in binary in G.

2. Associativity : The element of G are all complex numbers & the multiplication of complex numbers obeys associative law (ie)

$(1 \cdot i)(-i) = 1 \cdot [i(-i)] = 1$

$(1 \cdot i)(-1) = 1 \cdot [i(-1)] = i$ etc.

Therefore given composition is associative in G.

Existence of identity :-

from composition table we see that the row headed by 1 just coincides with the top row of the composition table. Thus we have:

$$1(1) = 1, \quad 1(-1) = -1, \quad 1(i) = i, \quad 1(-i) = -i$$

Therefore 1 is left identity.

Existence of Inverse: We know that identity element is its own inverse. from the table, it is clear that $(1)^{-1} = 1$, $(-1)^{-1} = -1$, $(-i)^{-1} = i$ and $(i)^{-1} = -i$

Therefore, the inverse of every element of G is in G. Hence, G is a group.

Commutative The multiplication of complex no is commutative ie:

$$1(-1) = (-1)1, \quad (-1)i = i(-1) \text{ etc.}$$

Therefore $(G, \cdot)$ is a finite abelian group.

Theorem 1: The identity element in a group is Unique.

Proof :- Let e & e_1 be two identity elements of group G.

Then we have

$ee_1 = e_1$ if e is identity &

$e \cdot e_1 = e$ if e_1 is identity.

But ee_1 is unique element of G. Therefore

$ee_1 = e$ and $ee_1 = e_1 \Rightarrow e = e_1$

Hence identity is unique.

Theorem 2 The inverse of every element of a group is unique.

Proof: Let a be any arbitrarily element of a group, let e be the identity element. Let b & c are two inverse of a. Then

$$b \cdot a = e = a \cdot b$$

$$c \cdot a = e = a \cdot c$$

We have $b(ac) = be$

$$= b$$

Also $(ba)c = e \cdot c$

$$= c$$

$b(ac) = (ba)c$ (∵ Since composition of multiplication is associative in a group)

Therefore $b = c$

Hence inverse of every element in G is unique.

Theorem 3 If inverse of on element a in a group is a^{-1}, then the inverse of a^{-1} is a. (ie) $(a^{-1})^{-1} = a$.

Proof:- Let e be identity element then,

$a^{-1} \cdot a = e \quad \forall a \in G$.

$\Rightarrow (a^{-1})^{-1} \cdot (a^{-1} \cdot a) = (a^{-1})^{-1} e$ { multiplying both sides by $(a^{-1})^{-1}$ }

$\Rightarrow [(a^{-1})^{-1} a^{-1}] a = (a^{-1})^{-1} e$

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

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

Proved

Theorem-4 The inverse of the product of two element of group is the product of the inverse taken in reverse order.

(IU) 2004

$$(ab)^{-1} = b^{-1}a^{-1} \quad \forall\, a, b \in G.$$

Proof :- Suppose a & b are any element of G and a^{-1}, b^{-1} are respectively the inverse of a & b then

$$a^{-1}a = e = a \cdot a^{-1}$$

and $$b^{-1}b = e = b\,b^{-1}$$

where e is the identity element.

Now
$$\begin{aligned}(ab)\,b^{-1}a^{-1} &= [(ab)\,b^{-1}]\,a^{-1} \\ &= [a(bb^{-1})]\,a^{-1} \\ &= [ae]\,a^{-1} \\ &= aa^{-1} \\ &= e \qquad \text{—(1)}\end{aligned}$$

Similary
$$\begin{aligned}(b^{-1}a^{-1})ab &= b^{-1}[a^{-1}(ab)] \\ &= b^{-1}[(a^{-1}a)b] \\ &= b^{-1}[eb] \\ &= b^{-1}b = e \qquad \text{—(2)}\end{aligned}$$

from (1) & (2)

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

Therefore by the definition of inverse, we see $(ab)^{-1} = b^{-1}a^{-1}$

Theorem 5 Cancellation laws hold in Group.

If $a, b, c \in G$

$$ab = ac \Rightarrow b = c$$
$$ba = ca \Rightarrow b = c.$$

Proof :- Let $a \in G$ and e be the identity element then

$$a \in G \Rightarrow \exists\, a^{-1} \in G \text{ such that } a^{-1}a = e = aa^{-1}$$

Now $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$

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

Similarly $ba = ca$

$$(ba)a^{-1} = (ca)a^{-1}$$
$$b(aa^{-1}) = c(aa^{-1}) \Rightarrow be = ce$$
$$b = c$$

Lecture No-12

Ref Pt - 2.3

Additive Modulo m

Let a & b are two integers then the operation of addition modulo m is defined as the least non-negative remainder when the ordinary sum of a & b divided by m.

This oper^n when applied over the integers a & b is written as $a +_m b$ is defined as -

$$a +_m b = r, \quad 0 \leq r < m$$

Ex $8 +_7 5 = 6$

Que The set $G = \{0, 1, 2, 3 \ldots m-1\}$ of first m non-negative integers is a group w.r to composition addition modulo m.

Sol^n **Closure**: since $a +_m b = r$ where $0 \leq r \leq m-1$

Therefore $\forall a, b \in G \Rightarrow a +_m b \in G$

so G is closed w.r. to composition addition modulo m.

Associativity: $a +_m (b +_m c) = a +_m (b + c)$

Therefore $+_m$ is associative composition in G.

Existence of Indentity $\exists$ an element $0 \in G$ such that $0 +_m a = a = a +_m 0$

Existence of Inverse The inverse of 0 is 0 itself.

If $r \neq 0 \in G$ then there exist an element $(m-r) \in G$ such that

$$(m-r) +_m r = 0 = r +_m (m-r)$$

Therefore $(m-r)$ is inverse of r w.r to given composition.

Thus $(G, +_m)$ is a group.

and it is Abelian also

{since it is commutative also}

Multiplication Modulo m :-

$a \cdot_m b = r, \quad 0 \le r < p$

Ex $8 \cdot_5 4 = 2$.

Que Prove that set $G = \{0, 1, 2, 3, 4, 5, 6\}$ is a finite abelian group of order 6 w.r to multiplication modulo 7.

Soln from Composition table

X_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

Closure property from composition table we see that all entries are from set G. Therefore G is closed w.r to multiplication modulo 7.

Associative :- If $a, b, c \in G$ arbitrarily

$$a X_7 (b X_7 c) = (a X_7 b) X_7 c$$

let $a = 2 \quad b = 4 \quad c = 6$

$$2 X_7 (4 X_7 6) = (2 X_7 4) X_7 6$$

$$2 X_7 3 = 1 X_7 6$$

$$6 = 6$$

Therefore given composition is associative

Identity : $1 \in G$ is identity element.

Inverse :- $1^{-1} = 1, \; 2^{-1} = 4, \; 3^{-1} = 5, \; 4^{-1} = 2, \; 5^{-1} = 3$

$6^{-1} = 6$

Commutative : The composition is commutative as the corresponding rows & columns in the composition table are Identical.

Que Prove that the set $G = \{0, 1, 2, 3, 4, 5\}$ is a finite abelian group of order 6 w.r. to addition modulo 6.

Que Find the order of each element of multiplicative group $G = \{1, -1, i, -i\}$

Soln Since identity element is 1.

therefore $o(1) = 1$

$(-1)^1 = -1$

$(-1)^2 = 1$

so $o(-1) = 2$

$(i)^1 = i$

$(i)^2 = -1$

$(i)^3 = -i$

$(i)^4 = 1$

so $o(i) = 4$

$(-i)^1 = (-i)$

$(-i)^2 = -1$

$(-i)^3 = i$

$(-i)^4 = 1$

so $o(-i) = 4$

Que Find order of each element of group $G = \{0, 1, 2, 3, 4, 5\}$, the composition in G is 'addition modulo 6'

Soln $(G, +_6)$

Identity element is 0, order of this element is 1.

$1^2 = 1$ $\quad 1^2 = 1 +_6 1 = 2$

$1^3 = 1 +_6 1 +_6 1 = 3$

$1^6 = 1 +_6 5 = 0$

so $o(1) = 6$

$2^1 = 2$

$2^2 = 2 +_6 2 = 4$

$2^3 = 2 +_6 2 +_6 2 = 0$

$O(2) = 3$

$3^1 = 3$

$3^2 = 3 +_6 3 = 0$

$O(3) = 2$

$4^1 = 4$

$4^2 = 4 +_6 4 = 2$

$4^3 = 4 +_6 4 +_6 4 = 0$

$O(4) = 3$

$5^1 = 5$

$5^2 = 5 +_6 5 = 4$

$5^3 = 5 +_6 5 +_6 5 = 3$

$5^4 = 5 +_6 5 +_6 5 +_6 5$

$5^6 = 5 +_6 5 +_6 5 +_6 5 +_6 5 +_6 5$

$= 0$

$O(5) = 6$

Qu) Let $(G, *)$ be a group. If it is abelian, show that $a^3 * b^3 = (a*b)^3 \quad \forall a, b \in G$.

Sol) Suppose $(G, *)$ is an abelian group.

then $a * b = b * a \quad \forall a, b \in G$

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

Further

$$(a*b)^3 = (a*b)^2 * (a*b)$$
$$= (a^2 * b^2) * (a*b)$$
$$= [(a^2 * b) * b] * (a*b)$$
$$= [(a^2 * b) * (b*a) * b]$$
$$= [(a^2 * b) * (a*b) * b]$$
$$= a^2 * (b*a) * (b*b)$$
$$= a^2 * (a*b) * b^2$$
$$= (a^2 * a) * (b^2 * b^2)$$
$$= a^3 * b^3$$

Que Prove that if for every element a in group $(G,*)$, $a^2 = e$ then G is abelian group.

Soln $a, b \in G \Rightarrow a*b \in G \quad \forall a, b \in G.$

$\Rightarrow (a*b)^2 = e$

Now $(a*b)(a*b) = e$

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

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

But $a^2 = e \Rightarrow a*a = e$

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

$b^2 = e \Rightarrow b^{-1} = b \quad -(2)$

$\therefore \quad b*a = a*b$

From (1) & (2) Therefore G is an abelian group.

Que Prove that for every element of a group G is its own inverse, then G is abelian.

Soln (Given) $a^{-1} = a, \quad b^{-1} = b$

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

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

$\Rightarrow b*a = a*b$ {Hence G is Abelian}

Order of an element of a Group

By order of an element $a \in G$, we mean the least positive integer n (if it exists) such that $a^n = e$ where e is identity element.

NOTE1 In any group G, the identity element is always of order 1 & it is only element of order 1.

$$\boxed{O(e) = 1}$$

NOTE2 If $a \in G$ & n is 'tve' integer such that $a^n = e$ then $O(a) \leq n$, when n is a least 'tve' integer satisfying $a^n = e$, then $O(a) = n$ & there exists any 'tve' integer $m (< n)$ such that $a^m = e$ then ~~$O(a) \leq m$~~ $O(a) < n$

Theorem The order of an element a of a group G is same as order of a^{-1}.

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

Proof Let $O(a) = n$ & $O(a^{-1}) = m$

$O(a) = n \Rightarrow a^n = e$ — (1)

$O(a^{-1}) = m \Rightarrow (a^{-1})^m = e$ — (2)

from (1)

$a^n = e$

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

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

$O(a^{-1}) \leq n$

$m \leq n$ — (3)

from (2)

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

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

$\{x^{-1} = e \Rightarrow x = e\}$ so $a^m = e$

$O(a) \leq m$

$n \leq m$ — (4)

$m \leq n$ & $n \leq m \Rightarrow m = n$

Proved

Theorem : The order of any integral power of an element can not exceed the order of a.

Proof Let $o(a) = n$ & a^k be any integral power of a, we have to prove $o(a^k) \leq o(a)$

Now $o(a) = n \Rightarrow a^n = e$

$$(a^n)^k = e^k$$

$$a^{nk} = e$$

$$(a^k)^n = e$$

$$o(a^k) \leq n$$

$$o(a^k) \leq o(a)$$ proved

Theorem If $o(a) = n$ for some $a \in G$, then $a^m = e$ iff n is a divisor of m.

Proof The condition is necessary let us suppose that n is a divisor of m. Then there exists an integer q such that $\frac{m}{n} = q$ or $m = nq$.

Now $a^m = a^{nq} = (a^n)^q = e^q = e$

Thus we have established that if $o(a) = n$ & n is divisor of m, then $a^m = e$

The condition is sufficient let $a^m = e \Rightarrow o(a) \leq m$

$\Rightarrow n \leq m$

Since m is an integer & n is a 'the' integer, therefore by division algorithm, there exists integer q & r such that $m = nq + r$ where $0 \leq r < n$

$$a^m = a^{nq+r}$$

$$= a^{nq} \cdot a^r$$

$$(a^n)^q a^r \Rightarrow e^q a^r = a^r$$

$$a^m = e \Rightarrow a^r = e$$

since $0 \le r < n$ therefore $a^r = e$ suggest that r must be equal to zero otherwise $o(a) \neq n$
Thus if $o(a) = n$ then, there exists not positive integer $r < n$ satisfying $a^r = e$
Hence $m = nq \Rightarrow n$ is divisor of m.

Que Prove that $o(a) = o(x^{-1}ax)$.
or The order of element a & $x^{-1}ax$ are same.

Solution We have to prove
$$o(a) = o(x^{-1}ax)$$
Suppose n & m are respectively the orders of a & $x^{-1}ax$ ie $o(a) = n$ & $o(x^{-1}ax) = m$

Now $(x^{-1}ax)^n = (x^{-1}ax)(x^{-1}ax)(x^{-1}ax) \cdots (x^{-1}ax)$
$= x^{-1}aeae \cdots ax$
$= x^{-1}a^n x$
$= x^{-1}ex \Rightarrow x^{-1}x = e$

This means $o(x^{-1}ax) \le n$
ie $m \le n$.

Again $o(x^{-1}ax) = m \Rightarrow (x^{-1}ax)^m = e$
$\Rightarrow x^{-1}a^m x = e = x^{-1}x$
$\Rightarrow a^m x = x$
$\Rightarrow a^m = e$
$o(a) \le m \Rightarrow n \le m$

since $m \le n$ & $n \le m \Rightarrow m = n$

$$o(a) = o(x^{-1}ax)$$

Proved

Lecture No-13

Cyclic Group :-

A group $(G, \cdot)$ is called cyclic if for $a \in G$, every element $x \in G$ is of the form a^n, where n is some integer.

symbolically, $G = \{a^n / n \in I\}$

The element a is called generator of G.

Example 1 The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic.

We can write $G = \{i, i^2, i^3, i^4\}$

Hence G is cyclic group with generator i.

Example 2 $G = (\{0, 1, 2, 3, 4, 5\}, +_6)$ is cyclic group.

Here generators are 1 & 5.

We see that

$1^2 = 1$, $1^2 = 1 +_6 1 = 2$

$1^3 = 1 +_6 1^2 = 3$

$1^4 = 1 +_6 1^3 = 4$

$1^5 = 1 +_6 1^4 = 5$

$1^6 = 1 +_6 1^5 = 0$ or $1 +_6 5 = 0$

Some properties of Cyclic Group

1. Every cyclic group is an Abelian Group.

Proof : Let $G = \{a\}$ be a cyclic group, generated by a.

Let $x, y \in G$ arbitrarily, then there exists integer r such that $x = a^r$, $y = a^s$

$$xy = a^r \cdot a^s = a^{r+s}$$

$$= a^{s \cdot r} = a^s \cdot a^r = y \cdot x$$

$$xy = yx \quad \forall\ x, y \in G$$

Hence G is an abelian group

2. If a is a generator of cyclic group G, then a^{-1} also a generator of G.

Proof Let $G = \{a\}$ be a cyclic group, generated by 'a'. Now, and a^r be an element of G, where r is some integer. We can write $a^r = (a^{-1})^{-r}$ since r is an integer, so $-r$ is also an integer.

Therefore every element of G is generated by a^{-1}.

Thus a^{-1} is also generator of G.

3. Every subgroup of a cyclic group is cyclic

Proof Let $G = \{a\}$ be cyclic group, generated by 'a'

If $H = G$ or (e), then H is cyclic.

Let H be a proper subgroup of G. Then H contains integral power of 'a'. Let $a^s \in H \Rightarrow (a^s)^{-1}$ ie $a^{-s} \in H$.

Let m be a least 'tve' integer such that $a^m \in H$.

Then we will prove that $H = \{a^m\}$ ie H is cyclic group generated by a^m.

Suppose $a^t \in H$ arbitrarily.

By division algo. $\exists$ integer q & r such that

$$t = mq + r, \quad 0 \le r < m$$

$$a^m \in H \Rightarrow (a^m)^q \in H$$

$$\Rightarrow a^{mq} \in H$$

$$\Rightarrow (a^{mq})^{-1} \in H$$

$$a^t \in H \text{ and } a^{-mq} \in H \Rightarrow a^t \cdot a^{-mq} \in H$$

$$a^{t-mq} \in H \Rightarrow a^r \in H$$

Now, m be least +ve integer such that $a^m \in H$ and $0 \le r < m$

Then $r = 0$, therefore $t = mq$

$$a^t = a^{mq} = (a^m)^q$$

Thus every element $a^t \in H$ is of the form of $(a^m)^q$. So H is cyclic group having a^m as its generator.

Cosets :-

Let G be a group on which the group operation is multiplication & H be a subgroup of G.

Let $a \in G$ then, the set

$Ha = \{ha : h \in H\}$ is called right coset of H in G generated by a.

If group operation is addition, then left coset & right coset of H in G generated by a

$H + a = \{h + a : h \in H\}$ Right coset

$a + H = \{a + h : h \in H\}$ left coset

NOTE 1. **If e be identity of G then $He = H = eH$**

2. $e \in H \Rightarrow ae \in H \Rightarrow a \in H, a, e \in H \Rightarrow ae \in aH$

$\Rightarrow a = Ha$

Example If G is an additive group of all integers & H is additive subgroup of all even integers then find all cosets of H in G.

Soln We have $G = \{0, \pm 1, \pm 2 \cdots\}$

& $H = \{0, \pm 2, \pm 4 \cdots\}$

Let $0, 1, 2 \cdots \in G$ then

$H+0 = \{0, \pm 2, \pm 4, \pm 6 \cdots$

$H+1 = \{0+1, \pm 2+1, \pm 4+1 \cdots$

$= \{\cdots -3, -1, 1, 3 \cdots\}$

$H+2 = \{0+2, \pm 2+2, \pm 4+2 \cdots\}$

$= \{\cdots -4, -2, 0, 2, 4 \cdots\} = H$

Hence H & $H+1$ are two distinct cosets.

Theorem: If H is any subgroup of G and $h \in H$ then $Hh = H = hH$.

Proof: let $h \in H \subseteq G$

We have to show $Hh = H$ and $hH = H$

Suppose h' be any arbitrary element of H

Then $h'h \in Hh$

Since H is subgroup then

$h' \in H, h \in H \Rightarrow h'h \in H$

Thus. $h'h \in Hh \Rightarrow h'h \in H$

$\therefore h'h \in Hh$ and $hh' \in H \Rightarrow Hh \subseteq H$ —— (1)

Again $h' = h'e = h'(h^{-1}h)$

$= (h'h^{-1})h \in Hh$

as $h' \in H, h^{-1} \in H \Rightarrow h'h^{-1} \in H \subseteq H$ is subgroup.

$h' \in H \Rightarrow h' \in Hh$

$H \subseteq Hh$ —— (2)

from (1) & (2) we get

$Hh = H$

Similarly we can find $hH = H$

Theorem :- If a & b are any two elements of a group G & H is a subgroup then -

$$Ha = Hb \Leftrightarrow ab^{-1} \in H \text{ and } aH = bH \Leftrightarrow b^{-1}a \in H$$

Proof Let H is a subgroup of G and $a, b \in G$ such that

$$Ha = Hb$$

If e be identity then

$$e \in H \Rightarrow ea \in Ha \Rightarrow a \in Ha$$

But $Ha = Hb \Rightarrow a \in Hb$

$$ab^{-1} \in Hbb^{-1}$$

$$ab^{-1} \in H$$

Conversely : Let H is a subgroup of G and $a, b \in H$ such that $ab^{-1} \in H$

Then show $Ha = Hb$

$$\Rightarrow ab^{-1} \in H \Rightarrow Hab^{-1} = H$$

$$\Rightarrow Hab = Hb \quad \because [h \in H \Rightarrow Hh = H]$$

$$Hae = Hb$$

$$Ha = Hb$$

Therefore $Ha = Hb \Leftrightarrow ab^{-1} \in H$

Theorem :- If a, b are two distinct elements of a group G & H is any subgroup of G, then

$$a \in Hb \Leftrightarrow Ha = Hb$$

and $a \in bH \Leftrightarrow aH = bH$

Proof Let $a \in Hb \Rightarrow ab^{-1} \in Hbb^{-1} \Rightarrow ab^{-1} \in He$

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

$$\Rightarrow Hab^{-1} = H \quad \{\text{since } h \in H \Rightarrow Hh = H\}$$

$$\Rightarrow Hab^{-1}b = Hb$$

$$Hae = Hb \Rightarrow Ha = Hb.$$

Conversely Let $Ha = Hb$

if $a \in Ha \Rightarrow a \in Hb$, $a \in bH \Rightarrow aH = bH$

Theorem: Any two right (left) cosets of a subgroup are either disjoint or identical.

Proof Let H is a subgroup of G and let Ha & Hb any two right coset of H in G.

We need to prove either $Ha \cap Hb = \phi$ or $Ha = Hb$.

Suppose Ha & Hb are not-disjoint, then there exists at least one element c such that $c \in Ha$ & $c \in Hb$.

Let $c = h_1 a$ and $c = h_2 b$ where $h_1, h_2 \in H$

$$h_1 a = h_2 b$$
$$h_1^{-1} h_1 a = h_1^{-1} h_2 b$$
$$e a = h_1^{-1} h_2 b$$
$$a = (h_1^{-1} h_2) b$$
$$Ha = H(h_1^{-1} h_2) b$$
$$Ha = Hb$$

Therefore, either $Ha \cap Hb = \phi$ or $Ha = Hb$.

Lagrange's Theorem :-

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

Proof :- Let G is finite group of order n ie $o(G)=n$

$$G = \{a_1, a_2 \dots a_n\}$$

& H is subgroup of G of order m ie $O(H)=m$

$$H = \{h_1, h_2 \dots h_m\}$$

Let $a_1 \in G$. Then $Ha_1 = \{h_1a_1, h_2a_1, h_3a_1, \dots h_ma_1\}$ be right coset of H in G generated by a_1 having all distinct elements.

Suppose if possible $h_ia = h_ja$

$$\Rightarrow h_i = h_j$$

Therefore each right coset of H in G has m distinct elements but we know the union of all left or right coset of H in G is equal to group ie.

$$G = Ha_1 \cup Ha_2 \cup \dots Ha_k$$

where $Ha_2 = \{h_1a_2, h_2a_2 \dots h_ma_2\}$

$Ha_3 = \{h_1a_3, h_2a_3 \dots h_ma_3\}$

$Ha_k = \{h_1a_k, h_2a_k \dots h_ma_k\}$

Now no. of elements in G = no of elements in Ha_1 + no. of elements in Ha_2 + ... no. of elements in Ha_k

$$n = m + m + \dots (k \text{ times})$$

$$n = km$$

$$k = \frac{n}{m} = \frac{O(G)}{O(H)}$$

$O(H)$ is divisor of $O(G)$

Lecture No-14

Ref Pt-2.5

Subgroup:

A non empty subset H of a group G is called subgroup of G, if -

(i) H is stable for the composition in G.

(ii) H is a group for the composition in G.

NOTE

1. The identity of subgroup H is same as that of G.

If e' & e are identities of H & G respectively

$$a \in H \Rightarrow e'a = a$$

$$a \in G \Rightarrow ea = a$$

$$e'a = ea \Rightarrow \boxed{e' = e}$$

2. The inverse of $a \in H$ is same as the inverse of an element of G.

If b & c are two inverse then

$$ba = e' \text{ and } ca = e$$

$$ba = ca$$

$$b = c \quad \{\text{since } e' = e\}$$

we can write $ba = e' = e = ca$

3. The order of an element $a \in H$ is same as the order of that as an element of G.

4. If H is subgroup of G and K is subgroup of H then K is subgroup of G.

Theorem If H is any subgroup then $HH = H$

Proof let $h_1 \in H$ & $h_2 \in H \Rightarrow h_1 h_2 \in H$

$$h_1 h_2 \in HH \Rightarrow h_1 h_2 \in H$$

$$HH \subseteq H \quad \text{---(1)}$$

$\because h = he$ let $h \in H$ & $e \in H$

$$h \in H \Rightarrow he \in HH$$

$$H \subseteq HH \quad \text{---(2)}$$

$\boxed{HH = H}$ Proved

Theorem If H & K are any elements of a group G then $(HK)^{-1} = K^{-1}H^{-1}$

Proof - Let x be any arbitrary element of $(HK)^{-1}$ then $x = (hk)^{-1}$ $\forall$ $h \in H, k \in K$

$$= k^{-1}h^{-1} \in K^{-1}H^{-1}$$

$$(HK)^{-1} \subseteq K^{-1}H^{-1}$$

Again let y be any arbitrary element of $K^{-1}H^{-1}$ then $y \in k^{-1}h^{-1}$, $k \in K$, $h \in H$

$$= (hk)^{-1} \in (HK)^{-1}$$

$$\Rightarrow K^{-1}H^{-1} \subseteq (HK)^{-1}.$$

Hence $(HK)^{-1} = K^{-1}H^{-1}$

Theorem If H is any subgroup of G, then $H^{-1} = H$ Also show that converse is not true.

Proof Let h^{-1} be any arbitrary element of H^{-1}, then $h \in H$.

Now H is subgroup of G, therefore

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

Thus $h^{-1} \in H^{-1} \Rightarrow h^{-1} \in H$

Therefore $H^{-1} \subseteq H$

Again $h \in H \Rightarrow h^{-1} \in H$

$$\Rightarrow (h^{-1})^{-1} \in H^{-1}$$

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

$H \subseteq H^{-1}$ Hence $H = H^{-1}$

If H is a complex of a group G & $H^{-1} = H$, then it is not necessary that H is a subgroup of G. For example, $H = \{-1\}$ is a complex of multiplicative group $G = \{-1, 1\}$ Also $H^{-1} = \{-1\}$ since -1 is the inverse of 1 in G. But $H = \{-1\}$ is not a subgroup of G. Since $(-1)(-1) = 1 \notin H$

Que If H_1 & H_2 are two subgroups of a group G then $H_1 \cap H_2$ is also a subgroup of G. (UPTU)

Ans Suppose H_1 & H_2 be any two subgroup of G.

Then $H_1 \cap H_2 \neq \phi$

since at least the identity element e is common to both H_1 & H_2

In order to prove $H_1 \cap H_2$ is a subgroup it is sufficient to prove that

$$a \in H_1 \cap H_2 , \; b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$$

Now $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$

$b \in H_1 \cap H_2 \Rightarrow b \in H_1$ and $b \in H_2$

But H_1 & H_2 are subgroups therefore.

$a \in H_1, \; b \in H_1 \Rightarrow ab^{-1} \in H_1$

$a \in H_2, \; b \in H_2 \Rightarrow ab^{-1} \in H_2$

Finally $ab^{-1} \in H_1$, $ab^{-1} \in H_2$

$$ab^{-1} \in H_1 \cap H_2$$

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

Que Union of two subgroup is not necessarily a subgroup.

Soln Suppose G be additive group of integer. Then

$H_1 = \{0, \pm 2, \pm 4, \pm 6 \cdots\}$ & $H_2 = \{0 \pm 3, \pm 6, \pm 9 \cdots\}$

both are subgroup of G.

We have $H_1 \cup H_2 = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9\}$

obviously $H_1 \cup H_2$ is not closed w.r.to addition, since $3 \in H_1 \cup H_2$ is not closed w.r. to addition since $3 \in H_1 \cup H_2$

$4 \in H_1 \cup H_2$ But $3+4 = 7 \notin H_1 \cup H_2$

Therefore $H_1 \cup H_2$ is not a subgroup of G.

Normal Subgroup:

A subgroup H of a group G is said to be a normal subgroup of G if for every $x \in G$ and for every $h \in H$, $xhx^{-1} \subseteq H$.

Theorem: A subgroup H of a group G is normal iff $xHx^{-1} = H \ \forall x \in G$.

Proof Let $xHx^{-1} = H \ \forall x \in G$

$\Rightarrow xHx^{-1} \subseteq H \ \forall x \in G$

$\Rightarrow H$ is normal subgroup of G.

Conversely

H is normal subgroup of G. Then

$xHx^{-1} \subseteq H \ \forall x \in G$ —(1)

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

$\therefore x^{-1}H(x^{-1}) \subseteq H \ \forall x \in G$

$\Rightarrow x^{-1}Hx \subseteq H \ \forall x \in G$

$\Rightarrow x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1}, \forall x \in G$

$H \subseteq xHx^{-1}$ —(2)

from (1) & (2) $xHx^{-1} = H, \forall x \in G$.

Theorem A subgroup H of a group G is a normal subgroup iff left coset of H in G is a right coset of H in G.

Proof Let H be a normal subgroup of G.

Then $xHx^{-1} = H, \forall x \in G \Rightarrow (xHx^{-1})x = Hx \ \forall x \in G$

$xH = Hx \ \forall x \in G$ {each left coset is right coset}

Conversely: assume that $xH = Hx, \forall x \in G$.

$xHx^{-1} = H, \forall x \in G$

H is normal subgroup of G.

Theorem Intersection of any two normal subgroups of a group is normal subgroup.

Proof: Let H & K be two normal subgroup of a group G. Since H & K are subgroup, therefore $H \cap K$ is also a subgroup of G.

Then to show $H \cap K$ is normal subgroup.

Let $x \in G$ and $n \in H \cap K \Rightarrow n \in H, n \in K$

Now $x \in G$, $n \in H$ & $n \in H$.

and H is normal subgroup of $G \Rightarrow xnx^{-1} \in H$

$xnx^{-1} \in H$, $xnx^{-1} \in K \Rightarrow xnx^{-1} \in H \cap K$

Thus $x \in G$, $n \in H \cap K \Rightarrow xnx^{-1} \in H \cap K$

Hence $H \cap K$ is normal subgroup.

Permutation Group :-

Let S be a finite set consisting n elements, then the set of all one-one onto mapping from S to S forms a group w.r.to Composition of mapping.

This group is called permutation group or symmetric Group, of n symbols of degree n & is denoted by S_n.

If $S_n = \{a_1, a_2, a_3 \cdots a_n\}$ then we can write an element $f \in S_n$ as –

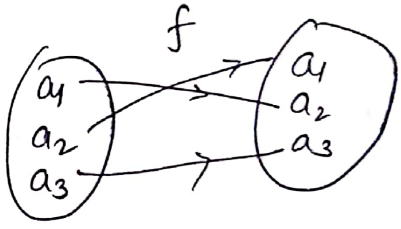
$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ f(a_1) & f(a_2) & f(a_3) & & f(a_n) \end{pmatrix}$$

where $f(a_1), f(a_2) \cdots f(a_n)$ are the f images of $a_1, a_2 \cdots a_n$ respectively.

Permutation : A one-one mapping of a finite set S onto itself is called permutation.

The no. of elements in a finite set S is known

It is denoted by $f = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_1 & a_3 \end{pmatrix}$ or



Equal Permutation :

Let S be non empty set. The permutation f & g defined on S is said to be equal if

$$f(a) = g(a) \quad \forall a \in S.$$

Ex: $S = \{1, 2, 3, 4\}$ and let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ $g = \begin{pmatrix} 4 & 1 & 3 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

Here $f(a) = g(a)$ so these two permutations are equal.

Total No. of Permutations

If there are n elements in set S, then total no of permutations is $\lfloor n$.

Ex Let $S = \{1, 2, 3\}$, then total permutation $= \lfloor 3 = 6$

$$S = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Identity Permutation

Let S be a finite, non empty set, an identity permutation on S denoted by I is defined $I(a) = a \ \forall a \in S$.

Illustration: Let $S = \{a_1, a_2 \dots a_n\}$

Then $I = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ is identity permutation.

Product of Permutation or Composition of Permutation

Let $S = \{a_1\ a_2\ a_3 \dots a_n\}$ and let

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & & a_n \\ f(a_1) & f(a_2) & f(a_3) & \dots & f(a_n) \end{pmatrix}, \quad g = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ g(a_1) & g(a_2) & g(a_3) & \dots & g(a_n) \end{pmatrix}$$

Then composition of f & g is denoted by fg or fog.

$$fog = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ f(g(a_1)) & f(g(a_2)) & f(g(a_3)) & \dots & f(g(a_n)) \end{pmatrix}$$

Example $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

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

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

$fog \neq gof$.

Inverse of Permutation

If f is a permutation on $S = (a_1\ a_2\ a_3 \ldots a_n)$ such that

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_1 & b_2 & b_3 & \cdots & b_n \end{pmatrix}$$

then there exists a permutation called inverse f denoted by f^{-1} such that $fof^{-1} = f^{-1}of = I$.

where $f^{-1} = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$

Cyclic Permutation :

Let $S = \{a_1, a_2 \cdots a_n\}$ be a finite set of n symbols. A permutation f defined on S is said to be cyclic permutation if f is defined such that

$$f(a_1) = a_2,\ f(a_2) = a_3 \cdots f(a_{n-1}) = a_n \text{ and } f(a_n) = a_1$$

Ex Let $S = \{1, 2, 3, 4\}$ then $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ is cyclic permutation. It is written as $f = (1234)$

Ex Let (13426) is cycle of length 5, Suppose it represents a permutation of degree 9 on a set, consisting of element $1, 2 \cdots 9$. Then the permutation is written as -

$$f = \begin{pmatrix} 1 & 3 & 4 & 2 & 6 & 5 & 7 & 8 & 9 \\ 3 & 4 & 2 & 6 & 1 & 5 & 7 & 8 & 9 \end{pmatrix}$$

Disjoint cycle :

Let $S = \{a_1\ a_2\ a_3 \cdots a_n\}$. If f & g are two cycles on S such that they have no element common then f & g are said to be disjoint cycle.

Ex Let $S = \{1, 2, 3, 4, 5, 6\}$ if $f = (145)$ & $g = (236)$ Then f & g are disjoint cycles.

Even & Odd Permutation :-

A permutation f is said to be even permutation if f can be expressed as the product of even no of transpositions.

A permutation f is said to be odd permutation if f can be expressed as the product of odd no. of transposition.

(Transposition : A cycle of length 2 is called transposition).

Que Show that $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 1 & 8 & 5 & 6 & 2 & 4 \end{pmatrix}$ is even

We have $f = \begin{pmatrix} 1 & 7 & 2 & 3 \\ 7 & 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 4 & 8 \\ 8 & 4 \end{pmatrix}\begin{pmatrix} 5 \\ 5 \end{pmatrix}\begin{pmatrix} 6 \\ 6 \end{pmatrix}$

$f = (1723)(48)(5)(6)$

$\Rightarrow f = (17)(12)(13)(48)$

f is expressed as product of 4 transpositions

therefore f is even permutation.

Que Show that $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 6 & 5 & 8 & 7 & 2 \end{pmatrix}$ is odd.

We have $f = \begin{pmatrix} 1 \\ 1 \end{pmatrix}\begin{pmatrix} 2 & 4 & 6 & 8 \\ 4 & 6 & 8 & 2 \end{pmatrix}\begin{pmatrix} 3 \\ 3 \end{pmatrix}\begin{pmatrix} 5 \\ 5 \end{pmatrix}\begin{pmatrix} 7 \\ 7 \end{pmatrix}$

$f = (2468)$

$f = (24)(26)(28)$

f is expressed as product of 3 transpositions.

Hence f is odd.

Define permutation group. Let $A = \{1, 2, 3, 4, 5\}$

Find $(13) \circ (245) \circ (2,3)$

Soln We have $f = \begin{pmatrix} 1 & 3 & 2 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 2 & 4 & 5 & 3 & 1 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 2 & 3 & 1 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$

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

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

$$f = (12453)$$

Lecture No-15
(Ref Pt-2.6)

Homomorphism :

Let $(G, *)$ and (G', Δ) be any two group.
A mapping f from G to G' ie $f: G \to G'$ is called homomorphism of G to G' if

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

* Homomorphism into

A mapping f from a group G into a group G' is said to be a homomorphism of G into G' if

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

Homomorphism onto

A mapping f from a group G onto a group G' is said to be a homomorphism of G onto G' if

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

Ex Let G be a group of integers under addition and $G' = G$ & let $f(x) = 3x \ \forall x \in G$ then

$$f(x+y) = 3(x+y) = 3x+3y = f(x)+f(y)$$

Therefore f is homomorphism.

Isomorphism of Groups :-

Let $(G,*)$ and (G',Δ) be two groups. A mapping $f: G \to G'$ defined by $f(a*b) = f(a) \Delta f(b)$ is called isomorphism, if f is one-one and onto mapping. We can say a one-one onto homomorphism is an isomorphism.

Thus every isomorphism is necessarily a homomorphism But converse is not true.

Properties of Homomorphism & Isomorphism

Let f be a homomorphic mapping of a group G into group G' Then we have three important properties.

(i) The f-image of identity e of G is the identity of G' ie $f(e)$ is the identity of G'.

(ii) The f-image of the inverse of an element a of G is the inverse of the f-image of a ie

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

(iii) The order of the f-image of an element is same as the order of the element.

Proof (i) Let e & e' be identity of G & G' respectively

$$a \in G \Rightarrow f(a) \in G'$$

$$e' \cdot f(a) = f(a) = f(ae)$$

$$= f(e) \cdot f(a)$$

$$e' = f(e)$$

$f(e)$ is identity of G'

(ii) If e is the identity of $G \Rightarrow f(e)$ is identity of G'

If a^{-1} is the inverse of a in G, then

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

Now, $a^{-1}a = e \Rightarrow f(a^{-1}.a) = f(e)$

$$f(a^{-1}) \cdot f(a) = f(e)$$

Again $aa^{-1} = e \Rightarrow f(aa^{-1}) = f(e)$

$$f(a)\, f(a^{-1}) = f(e)$$

$$f(a^{-1})\, f(a) = f(e) = f(a) \cdot f(a^{-1})$$

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

Proved

(iii) Let e be identity of G, then $f(e)$ is identity of G'

Let the order of $a \in G$, be finite and it be equal n ie $O(a) = n$. Then

$$a^n = e \Rightarrow f(a^n) = f(e)$$

$$f(aaa\text{---}n \text{ times}) = f(e)$$

$$f(a)\, f(a) \text{---} f(a) \text{---} n \text{ times} = f(e)$$

$$[f(a)]^n = f(e)$$

$$[f(a)]^n = e'$$

$$O([f(a)]) \leq n \quad \text{---(1)}$$

If possible $O[f(a)] = m$ then

$$f(a)\, f(a) \text{---} m \text{ times} = f(e)$$

$$f(aaa\text{---}m \text{ times}) = f(e)$$

$$f(a^m) = f(e)$$

$$a^m = e$$

$$O(a) \leq m \quad \text{---(2)}$$

from (1) & (2) $m = n$

LECTURE-16

Ring & Types Of Ring

Ms. Sonika Bhatnagar
Assistant Professor
Department of Information Technology

RING

- What is Ring
- Example of Ring
- Types of Ring

RING

Let addition (+) and Multiplication (.) be two binary operations defined on a non empty set R.
Then R is said to form a ring w.r.t addition (+) and multiplication (.) if the following conditions are satisfied:

1.(R, +) is an abelian group (i.e commutative group)
2.(R, .) is a semigroup
3.For any three elements a, b, c $\in$ R the left distributive law a.(b+c) =a.b + a.c and the right distributive property (b + c).a =b.a + c.a holds.

PROPERTIES OF A RING

Therefore a non- empty set R is a ring w.r.t to binary operations + and . if the following conditions are satisfied.

1.For all a, b $\in$ R, a+b$\in$ R,

2.For all a, b, c $\in$ R a+(b+c)=(a+b)+c,

3.There exists an element in R, denoted by 0 such that a+0=a for all a $\in$ R

4.For every a $\in$ R there exists an y $\in$ R such that a+y=0. y is usually denoted by -a

5.a+b=b+a for all a, b$\in$ R.

6.a.b $\in$ R for all a.b $\in$ R.

7.a.(b.c)=(a.b).c for all a, b $\in$ R

8.For any three elements a, b, c $\in$ R a.(b+c) =a.b + a.c and (b + c).a =b.a + c.a. And the ring is denoted by (R, +, .).

R is said to be a commutative ring if the multiplication is commutative.

EXAMPLE OF RING

(Z, +) is a commutative group .
(Z, .) is a semigroup.
The distributive law also holds.
So, ((Z, +, .) is a ring.

Many other examples also can be given on rings like (R, +, .), (Q, +, .) and so on.

TYPES OF RING

1.Null Ring

The singleton (0) with binary operation + and defined by 0 + 0 = 0 and 0.0 = 0 is a ring called the zero ring or null ring.

2. Commutative Ring

If the multiplication in a ring is also commutative then the ring is known as commutative ring i.e. the ring (R, +, .) is a commutative ring provided.

a.b = b.a for all a, b E R

If the multiplication is not commutative it is called non- commutative ring.

TYPES OF RING (CONTINUE…)

3 Ring with unity

If e be an element of a ring R such that e.a = a.e = a for all a then the ring is called ring with unity and the elements e is said to be units elements or unity or identity of R.

4. Ring with zero divisor

A ring (R, +, .) is a said to have divisor of zero (or zero divisor), if there exist two non-zero elements a,b$\in$R such that a.b = 0 or b.a = 0 where 0 is the additive identity in R . here a and b are called the proper divisor of zero.

5. Ring without zero divisor

A ring R is said to be without zero divisor. If the product of no two non zero elements of R is zero i.e. if ab = 0 => a = 0 or b = 0.


Thank You!

LECTURE-17

Integral Domain & Field

Ms. Sonika Bhatnagar
Assistant Professor
Department Of Information Technology

INTEGRAL DOMAIN & FIELD

- What is Integral Domain
- What is Field
- Examples

INTEGRAL DOMAIN

There are two special kinds of ring (with zero divisor & without zero divisor.

If a, b are two ring elements with $a, b \neq 0$ but $ab = 0$ then a and b are called **zero-divisors**.

Example
In the ring $\mathbf{Z}_6$ we have $2.3 = 0$ and so 2 and 3 are zero-divisors.
More generally, if n is not prime then $\mathbf{Z}_n$ contains zero-divisors.

Definition of Integral Domain

An **integral domain** is a commutative ring with an identity ($1 \neq 0$) with no zero-divisors.
That is $ab = 0 \Rightarrow a = 0$ or $b = 0$.

EXAMPLES

Examples of Integral Domain are:-

1. The ring **Z** is an integral domain.

2. The polynomial rings **Z**[x] and **R**[x] are integral domains.

3. The ring $\{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$ is an integral domain.

4. If p is prime, the ring $\mathbf{Z}_p$ is an integral domain.

FIELD

Definition
A **field** is a commutative ring with identity ($1 \neq 0$) in which every non-zero element has a multiplicative inverse.

Examples
The rings **Q**, **R**, **C** are fields.

Remarks
If a, b are elements of a field with $ab = 0$ then if $a \neq 0$ it has an inverse a^{-1} and so multiplying both sides by this gives $b = 0$. Hence there are no zero-divisors and we have:
Every field is an integral domain.

The axioms of a field F can be summarized as:

- $(F, +)$ is an abelian group
- $(F - \{0\}, .)$ is an abelian group
- The distributive law.

THEOREM

Every finite integral domain is a field.

Proof

The only thing we need to show is that a typical element $a \neq 0$ has a multiplicative inverse.

Consider a, a^2, a^3, ... Since there are only finitely many elements we must have $a^m = a^n$ for some $m < n$(say).

Then $0 = a^m - a^n = a^m(1 - a^{n-m})$. Since there are no zero-divisors we must have $a^m \neq 0$ and hence $1 - a^{n-m} = 0$ and so $1 = a(a^{n-m-1})$ and we have found a multiplicative inverse for a.


Thank You!