LECTURE 28 – GROUPS, SYMMETRY,SUBGROUPS

GROUP :

A GROUP < G , *> IS AN ALGEBRAIC SYSTEM IN WHICH * ON G SATISFIES FOUR CONDITION

- **Closure Property**

  For all $x , y \in G$

  $x * y \in G$

- **Associative Property**

  For all $x , y , z \in G$

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

- **Existence of Identity element**

  There exists an element $e \in G$ such that for any $a \in G$

  $x * e = x = e * x$

- **Existence of Inverse Element**

  For every $x \in G$,there exists an element denoted by $a^{-1} \in G$ such that

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

THE ORDER OF A GROUP G IS THE NUMBER OF ELEMENTS IN G AND THE ORDER OF AN ELEMENT IN A GROUP IS THE LEAST POSITIVE INTEGER N SUCH THAT AN IS THE IDENTITY ELEMENT OF THAT GROUP G.

Properties of Group :

THEOREM 1 : LET E BE AN IDENTITY ELEMENT IN GROUP < G , ∗ > , THEN E IS UNIQUE

PROOF :

⇒ LET e AND e\` ARE TWO IDENTITY IN G

⇒ e e\` = e IF e\` IS IDENTITY

⇒ e e\` = e\` IF E IS IDENTITY

⇒ SINCE ee\` IS UNIQUE ELEMENT IN G

⇒ e = e\`

Properties of Group :

THEOREM 2 : INVERSE OF EACH ELEMENT OF A GROUP $< G , * >$ IS UNIQUE

PROOF :

$\Rightarrow$ LET a BE ANY ELEMENT OF G AND E THE IDENTITY OF G

$\Rightarrow$SUPPOSE B AND C ARE TWO DIFFERENT INVERSE OF A IN G.

$\Rightarrow a * b = e = b * a$ (IF b IS AN INVERSE OF a)

$\Rightarrow a * c = e = c * a$ (IF c IS AN INVERSE OF a)

$\Rightarrow$ NOW , $b = b * e$

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

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

$$= e * c = c$$

THUS a HAS UNIQUE INVERSE

Properties of Group :

Theorem 3 : if a^{-1} is the inverse of an element a of group $< G , * >$ then $(a^{-1})^{-1} = a$

Proof :

$\Rightarrow$ Let e be the identity of Group $< G , * >$

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

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

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

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

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

Properties of Group :

Theorem 4 : If < G , $*$ > be a group then for any two elements a and b of < G , $*$ > prove that $(a * b)^{-1} = b^{-1} * a^{-1}$ rule of reversal

Proof :

⇒ Let a^{-1} and b^{-1} are inverse of a and b respectively and e be the identity

⇒ $a * a^{-1} = e = a^{-1} * a$

⇒ $b * b^{-1} = e = b^{-1} * b$

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

⇒ $= [a * (b * b^{-1})] * a^{-1}$

⇒ $= [a * e] * a^{-1}$

⇒ $= a * a^{-1}$

⇒ $= e$

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

⇒ This show that b^{-1} and a^{-1} is inverse of b and a

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

Properties of Group :

Cancellation Property : if a , b and cbe any three elements of a group $< G , \bullet >$ then

$ab = ac \Rightarrow b = c$ left cancellation

$ba = ca \Rightarrow b = c$ right cancellation

Proof :

$\Rightarrow$ Let $a \in G$ and also $a^{-1} \in G$

$\Rightarrow$ $aa^{-1} = e = a^{-1}a$

$\Rightarrow$ where e is identity of G

$\Rightarrow$ Now , $ab = ac$

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

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

$\Rightarrow$ $e . b = e . c$

$\Rightarrow$ $b = c$

$\Rightarrow$ similarly , $ba = ca$

$\Rightarrow$ $b = c$

EXAMPLES :

THE SET OF $N \times N$ NON-SINGULAR MATRICES FORM A GROUP UNDER MATRIX MULTIPLICATION OPERATION.

- THE PRODUCT OF TWO $N \times N$ NON-SINGULAR MATRICES IS ALSO AN $N \times N$ NON-SINGULAR MATRIX WHICH HOLDS CLOSURE PROPERTY.

- MATRIX MULTIPLICATION ITSELF IS ASSOCIATIVE. HENCE, ASSOCIATIVE PROPERTY HOLDS.

- THE SET OF $N \times N$ NON-SINGULAR MATRICES CONTAINS THE IDENTITY MATRIX HOLDING THE IDENTITY ELEMENT PROPERTY.

AS ALL THE MATRICES ARE NON-SINGULAR THEY ALL HAVE INVERSE ELEMENTS WHICH ARE ALSO NON-SINGULAR MATRICES. HENCE, INVERSE PROPERTY ALSO HOLDS.

ABELIAN GROUP :

AN ABELIAN GROUP G IS A GROUP FOR WHICH THE ELEMENT PAIR $(a,b) \in G$ ALWAYS HOLDS COMMUTATIVE LAW.

SO, A GROUP HOLDS FIVE PROPERTIES SIMULTANEOUSLY –

i) CLOSURE

ii) ASSOCIATIVE

iii) IDENTITY ELEMENT

iv) INVERSE ELEMENT

v) COMMUTATIVE.

Example

The set of positive integers (including zero) with addition operation is an abelian group.

$$\boxed{G = \{0, 1, 2, 3, \ldots\}}$$

Here closure property holds as for every pair $(a, b) \in S, (a + b)$ is present in the set S. [For example, $1 + 2 = 2 \in S$ and so on]

Associative property also holds for every element $a, b, c \in S, (a + b) + c = a + (b + c)$ [For example, $(1 + 2) + 3 = 1 + (2 + 3) = 6$ and so on]

Identity property also holds for every element $a \in S, (a \times e) = a$ [For example, $(2 \times 1) = 2, (3 \times 1) = 3$ and so on]. Here, identity element is 1.

Commutative property also holds for every element $a \in S, (a \times b) = (b \times a)$ [For example, $(2 \times 3) = (3 \times 2) = 3$ and so on]

CYCLIC GROUP :

A CYCLIC GROUP IS A GROUP THAT CAN BE GENERATED BY A SINGLE ELEMENT. EVERY ELEMENT OF A CYCLIC GROUP IS A POWER OF SOME SPECIFIC ELEMENT WHICH IS CALLED A GENERATOR. A CYCLIC GROUP CAN BE GENERATED BY A GENERATOR 'g', SUCH THAT EVERY OTHER ELEMENT OF THE GROUP CAN BE WRITTEN AS A POWER OF THE GENERATOR 'g'.

Example

The set of complex numbers $\{1, -1, i, -i\}$ under multiplication operation is a cyclic group.

There are two generators – i and $-i$ as $i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$ and also $(-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1$ which covers all the elements of the group.

Hence, it is a cyclic group.

Note – A **cyclic group** is always an abelian group but not every abelian group is a cyclic group. The rational numbers under addition is not cyclic but is abelian.

SUBGROUP :

A SUBGROUP H IS A SUBSET OF A GROUP G (DENOTED BY H≤G) IF IT SATISFIES THE FOUR PROPERTIES SIMULTANEOUSLY – CLOSURE, ASSOCIATIVE, IDENTITY ELEMENT, AND INVERSE.

A SUBGROUP H OF A GROUP G THAT DOES NOT INCLUDE THE WHOLE GROUP G IS CALLED A PROPER SUBGROUP (DENOTED BY H<G). A SUBGROUP OF A CYCLIC GROUP IS CYCLIC AND A ABELIAN SUBGROUP IS ALSO ABELIAN.

Example

Let a group $G = \{1, i, -1, -i\}$

Then some subgroups are $H_1 = \{1\}, H_2 = \{1, -1\}$,

This is not a subgroup – $H_3 = \{1, i\}$ because that $(i)^{-1} = -i$ is not in H_3

SEMIGROUP & MONOID :

A FINITE OR INFINITE SET 'S' WITH A BINARY OPERATION 'o' (COMPOSITION) IS CALLED SEMIGROUP IF IT HOLDS FOLLOWING TWO CONDITIONS SIMULTANEOUSLY –

- CLOSURE – FOR EVERY PAIR (a,b)∈S,(a o b) HAS TO BE PRESENT IN THE SET S.
- ASSOCIATIVE – FOR EVERY ELEMENT a, b, c∈ S,(a o b) o c=a o (b o c) MUST HOLD.

Example

The set of positive integers (excluding zero) with addition operation is a semigroup. For example, $S = \{1, 2, 3, ...\}$

Here closure property holds as for every pair $(a, b) \in S, (a + b)$ is present in the set S. For example, $1 + 2 = 3 \in S$]

Associative property also holds for every element $a, b, c \in S, (a + b) + c = a + (b + c)$. For example, $(1 + 2) + 3 = 1 + (2 + 3) = 5$

Monoid

A monoid is a semigroup with an identity element. The identity element (denoted by e or E) of a set S is an element such that $(aoe) = a$, for every element $a \in S$. An identity element is also called a **unit element**. So, a monoid holds three properties simultaneously − **Closure, Associative, Identity element**.

Example

The set of positive integers (excluding zero) with multiplication operation is a monoid. $S = \{1, 2, 3, ...\}$

Here closure property holds as for every pair $(a, b) \in S, (a \times b)$ is present in the set S. [For example, $1 \times 2 = 2 \in S$ and so on]

Associative property also holds for every element $a, b, c \in S, (a \times b) \times c = a \times (b \times c)$ [For example, $(1 \times 2) \times 3 = 1 \times (2 \times 3) = 6$ and so on]

Identity property also holds for every element $a \in S, (a \times e) = a$ [For example, $(2 \times 1) = 2, (3 \times 1) = 3$ and so on]. Here identity element is 1.

NORMAL SUBGROUP:

LET G BE A GROUP. A SUBGROUP H OF G IS SAID TO BE A NORMAL SUBGROUP OF G IF FOR ALL H$\in$ H AND X$\in$ G, X H $X^{-1}\in$ H

IF X H X^{-1} = {X H X^{-1}| H $\in$ H} THEN H IS NORMAL IN G IF AND ONLY IF XH $X^{-1}\subseteq$H, $\forall$ X$\in$ G

STATEMENT: IF G IS AN ABELIAN GROUP, THEN EVERY SUBGROUP H OF G IS NORMAL IN G.

PROOF:

LET ANY H$\in$ H, X$\in$ G, THEN
X H X^{-1}= X (H X^{-1})
X H X^{-1}= (X X^{-1}) H
X H X^{-1} = E H
X H X^{-1} = H$\in$ H

HENCE H IS NORMAL SUBGROUP OF G.

ABELIAN GROUP:

DEFINITION OF ABELIAN GROUP

A GROUP < G , * >IN WHICH THE OPERATION ☐ IS COMMUTATIVE IS CALLED ABELIAN GROUP i.e. FOR ALL a,b BELONGS TO G , a * b = b * a

EXAMPLE

< Z , + > IS ABELIAN GROUP

< Q , + > IS ABELIAN GROUP

QUESTIONS :

1. A CYCLIC GROUP CAN BE GENERATED BY A/AN _________ ELEMENT.

A) SINGULAR

B) NON-SINGULAR

C) INVERSE

D) MULTIPLICATIVE

2. HOW MANY PROPERTIES CAN BE HELD BY A GROUP?

A) 2

B) 3

C) 5

D) 4

3. A CYCLIC GROUP IS ALWAYS __________

A) ABELIAN GROUP

B) MONOID

C) SEMIGROUP

D) SUBGROUP

QUESTIONS :

4. {1, I, -I, -1} IS ___________

A) SEMIGROUP

B) SUBGROUP

C) CYCLIC GROUP

D) ABELIAN GROUP

5. A GROUP (M,*) IS SAID TO BE ABELIAN IF ____________

A) (X+Y)=(Y+X)

B) (X*Y)=(Y*X)

C) (X+Y)=X

D) (Y*X)=(X+Y)

QUESTIONS :

6 . Show that in a Group $< G , * >$, if for any $a, b \in G$, $(a * b)^2 = a^2 * b^2$, then $<G , *>$ must be abelian

Solution :

Let $< G , * >$ be a Group and let $a , b \in G$

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

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

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

$\Rightarrow$ By left and right cancellation property

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

$\Rightarrow$ Thus we have $a * b = b * a$. $\forall a,b \in G$

$\Rightarrow$ Hence $< G , * >$ is an abelian Group

QUESTIONS :

7. Show that if every element in a group is its own inverse , then the group must be abelian

Solution :

Let $a , b \in G$

$\Rightarrow$ $a * b \in G$ (by closure property)

Now, $a^{-1} = a$ and $b^{-1} = b$

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

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

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

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

$\Rightarrow$ Thus we have $a * b = b * a , \forall a,b \in G$

$\Rightarrow$ Hence $< G , * >$ is an abelian Group

QUESTIONS :

8. If $< G , * >$ is an abelian group , then for all $a , b \in G$ show that $(a * b)^n = a^n * b^n$

Solution

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

$$(a * b)^{n+1}=a^{n+1} * b^{n+1}$$

$$(a * b)^{n+2}=a^{n+2} * b^{n+2}$$

Now ,

$$(a^n * b^n) (a * b) = (a * b)^{n+1}$$

$$= (a^{n+1} * b^{n+1})$$

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

By cancellation , similarly

$$b^{n+1} * a = a * b^{n+1}$$

Again

$$b^{n+1} * a = b(b^n * a) = b(ab^n)$$

i.e., $ab^{n+1} = b(ab^n)$