UNIT-V

27/06/2022.

Group theory

Binary Operation:-

Let a be any set a mapping $f: A \times A \to A$ is called a binary operation on A

i.e $\exists f(a,b) \in A \ \forall a \in A, b \in A$

we denote a binary operation by a symbol such as $+, -, \%, *, o, \square$ ... so on etc.

example : + is a binary Operation on the set N

Algebraic system or structure:-

A set together with a no. of binary operations on the set is called an algebraic structure or algebraic system

Eg:- $(N, +)$ is an Algebraic system

- $(Z, +, \times)$ is an AS

Properties of binary operation:-

Let $(G, *)$ is an Algebraic system

i. closure: $\forall a, b \in G$; $a*b \in G$

ii. Associative :- $\forall a, b, c \in G$; $a*(b*c) = (a*b)*c$

iii. Identity :- for any $a \in G$, $\exists e \in G$;

Such that $a*e = e*a = e$

iv. Inverse :- for any $a \in G$, $\exists b \in G$; Such that

$a*b = b*a = e$

v. abelian :- $\forall a, b \in G$, $a*b = b*a$ (commutative group)

Groupoid :- A set G with the binary operation * satisfies Closure property then it is called $(G, *)$ Groupoid

Ex:- $(N, +)$ satisfies closure property

i.e Let $1, 2 \in N$

$1+2 = 3 \in N$

$\therefore$ + is closed in N

Semi Group :- A set S with binary operation 'o' satisfies i.e (S, o) closure and associative properties then it is called semi group

ex:- $(N, +)$ is a semi group.

$(Z, +)$ is also a semi group.

Monoid : A set 'M' with binary operation '*' i.e $(M, *)$ is called monoid if it satisfies closure, associative identity properties

ex:- $(Z, +)$ is a monoid

$(Z, \times)$ is also a monoid

Group : An Algebraic structure $(G, *)$ is called a group if * satisfies the following conditions :

closure, associative, identity, inverse.

ex:- $(Z, +)$ is a group

abelian : A Group $(G, *)$ is said to be an abelian group if $a*b = b*a$

finite : A group $(G, *)$ is said to be a finite Group if G contains a finite no.of distinct elements otherwise $(G, *)$ is called as infinite Group.

28/06/2022

1. Let Z be the integers and * be the operation defined by $a*b = a+b+ab \ \forall \ a, b \in Z$, show that $(Z, *)$ is a Semi Group.

Closure : $\forall \ a, b \in Z$

then $a+b \in Z$, $ab \in Z$

$\therefore a+b+ab = a*b \in Z$

$\therefore$ * is closed in Z

Associative $\forall \ a, b, c$

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

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

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

$= a+b+c+ab+ac+bc+abc$

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

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

$= a+b+c+bc+ab+ac+abc$

$\therefore$ LHS = RHS

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

Hence $*$ is associative in Z

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

2. Show that the set of rational number under the binary operation 'o' is defined as $aob = \frac{a+b}{2}$ is not semi group.

Closure : $\forall\ a,b \in Q$

$aob = \frac{a+b}{2} = Q$

$\therefore$ o is closed in Q

Associative : $\forall\ a,b,c \in Q$

To prove $(aob)oc = ao(boc)$

Consider $(aob)oc = \left(\frac{a+b}{2}\right)oc$

$= \frac{a+b+2c}{2}$

Now $ao(boc) = ao\frac{b+c}{2}$

$= \frac{2a+b+c}{2}$

$\therefore ao(boc) \neq (aob)oc$

$\therefore$ o is not associative in Q

Hence (Q,o) is not a semi group.

3. Show that $x*y = x^y$ is not associative $\forall\ x,y \in R$

Associative : $\forall\ x,y,z \in Z$

To prove : $(x*y)*z = x*(y*z)$

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

$= x^{yz}$

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

$= x^{y^z}$

$\therefore *$ is not associative

* composition table

4. Prepare a composition table for the multiplication the set $A = \{1, \omega, \omega^2\}$ where ω is the cube roots of unity. show that $(A, \times)$ is a group.

Sol composition table:-

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Closure: Since all the entries of the composition table are the elements of A.

$\therefore$ $\times$ is closed in A.

Associative: Since multiplication is always associative on the set of complex number

$\therefore$ $(A, \times)$ is associative.

Identity:- from the composition table it is clear that is the multiplication identity with.

$1 \times 1 = 1$
$\omega \times 1 = \omega$
$\omega^2 \times 1 = \omega^2$

Inverse: $1 \times 1 = 1 \Rightarrow 1^{-1} = 1$
$\omega \times \omega^2 = 1 \Rightarrow \omega^{-1} = \omega^2$
$\omega^2 \times \omega = 1 \Rightarrow (\omega^2)^{-1} = \omega$

$\therefore$ 1 is the self inverse & ω, ω^2 are the mutual inverse.

$\therefore$ $(A, \times)$ is the group.

5. Construct composition table of the roots of the equation $x^4 = 1$ and show that it is a group w.r.to general multiplication.

$x^4 = 1$
$x^4 - 1 = 0$
$(x^2)^2 - (1)^2 = 0$
$(x^2+1)(x^2-1) = 0$

$x^2 = -1$ $\quad$ $x^2 = 1$ $\quad$ $\therefore G = \{+1, -1, i, -i\}$
$x^2 = i^2$ $\quad$ $x = \pm 1$ $\quad$ $x = \pm 1$

$\times$	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Closure :- the elements of the non-empty set G are the elements of the composition table
∴ $(G, \times)$ is closed in G

Associative : Since associative multiplication is associative on the set of complex number.
∴ $(G, \times)$ is associative.

Identity :- from the composition table it is clear that 1 is the multiplicative identity

i.e $1 \times 1 = 1$
$-1 \times +1 = -1$
$i \times +1 = +i$
$-i \times 1 = -i$

Inverse :- $1 \times 1 = 1 \Rightarrow 1^{-1} = 1$
$-1 \times -1 = 1 \Rightarrow (-1)^{-1} = -1$
$i \times (-i) = 1 \Rightarrow (i)^{-1} = -i$
$-i \times i = 1 \Rightarrow (-i)^{-1} = i$

1 & -1 are self inverse, -i & i are mutual inverse
∴ $(G, \times)$ is a group.

Addition modulo 'M' and multiplication modulo 'p'

29/06/2022

Let 'm' be a positive Integer ≥ 2 Addition modulo 'm' of a and b is denoted by $a +_m b$ and it is defined by the reminder of $a+b$ with which is divisible by 'm' $3 +_2 4 = 1$ reminder

$2 \overline{)7} ($
(1)

Multiplication modulo 'p':

Let 'p' be a fixed +ve Integer the multiplicative modulo 'p' of a and b is denoted by $a \times_p b$ and it is defined by the reminder of $a \times b$ which is divisible by 'p' $\Rightarrow a \times_p b = r$

$3 \times_2 4 = 0$ $\quad 2 \overline{)12} ($ (0)

$5 \times_5 15 = 0$ $\quad 5 \overline{)75} ($ (0)

1. Prove that $G = \{0,1,2,3,4\}$ is an abelian finite group of order '5' with respect to $+_5$ (Addition modulo 5)

$+_5$	0	1	2	3	4
0	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

Composition closure:
since all entries in the composition table are the elements of G.

Assosiative: since always Addition is Assosiative so Addition modulo 5 is Assosiative in G

Identity: $0+_5 0 = 0$
$1+_5 0 = 1$
$2+_5 0 = 2$
$3+_5 0 = 3$
$4+_5 0 = 4$
From the composition table '0' is the identity element so that

Inverse: $0+_5 0 = 0$
$1+_5 4 = 0$
$2+_5 3 = 0$
$3+_5 2 = 0$
$4+_5 1 = 0$
'0' is self inverse and 1,4 are multual inveres
$|||^{ly}$ 2,3 are multual inveres
there exist all elements have multual inveres so it satisfie inverse property

abelian property (or) commitative:
Since 1,2,3,4 & 5 the rows are equal to the respected columns $\therefore +_5$ is commitative in "G"
$(G, +_5)$ is abelian group.

2. Ex :- $G = \{1, 3, 5, 7\}$ with $\times_8$ is an abelian group.

$\times_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Closure : since all entires in the composition table are elements of G

Assosiative : since always multiplication modulo is Assosiative so $\times_8$ is Assosiative

Identity :- $1 \times_8 1 = 1$

$3 \times_8 1 = 3$

$5 \times_8 1 = 5$

$7 \times_8 1 = 7$

From composition table '1' is the identity element

Inverse :- $1 \times_8 1 = 1$

$3 \times_8 3 = 1$

$5 \times_8 5 = 1$

$7 \times_8 7 = 1$

all 1, 3, 5 & 7 are self inverses.

Abelian (or) commutative :-

since 1, 3, 5 & 7 are rows are columns are same 1, 2, 3, 4 are same

Hence 1, 3, 5 & 7 are Abelian group.

3. Show that Q_1 set of rational numbers other than 1 is an infinite abelian group with respect to the binary operation $*$ is defined by $a*b = a+b-ab$ $\forall$ $a, b \in Q_1$ show that it is an abelian group.

Given $a*b = a+b-ab$

$Q_1 = Q - \{1\}$

Closure :- $\forall\ a, b \in Q_1$

$a+b \in Q_1\ ,\ ab \in Q_1$

$a+b-ab \in Q_1$

$\therefore *$ is closed in Q_1

Associative :- $\forall\ a, b, c \in Q.$

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

$(a*b)*c = \underbrace{(a+b-ab)}_{a} * \underbrace{c}_{b}$

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

$= a+b+c-ab-ac-bc+abc$

$a*(b*c) = \underbrace{a}_{a} * \underbrace{(b+c-bc)}_{b}$

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

$= a+b+c-bc-ab-ac+abc$

Hence * satisfies a+b (assiciative property)

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

Identity :- for any $a \in Q_1\ \exists\ e \in G$

Such that $a*e = a$

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

$e(1-a) = 0$

$e = 0$

$\therefore e = 0$ is the identity element.

Inverse :- For any $a \in Q_1$

$\exists\ a^{-1} \in Q_1$ s.t

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

$a*a^{-1} = e = 0$

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

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

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

there exist a^{-1} element for $\forall\ a \in Q_1$

Inverse exist $\forall\ a \in Q_1$

Abelian property :- $a*b = a+b-ab$
$= b+a-ba$
$= b*a$

$*$ satisfies abelian property.

$(Q_1, *)$ is abelian group.

4. Show that set of all 2×2 non singular matrices under the usual matrix multiplication is a non commutative monoid.

Let A, B are non-singular matrices

1. Closure property : A, B are non-singular matrices. Its product $A\times B = AB$ is also a non-singular matrix

2. Associative :- Since matrix multiplication is always associative.

$A(BC) = (AB)C$

3. Identity property :- $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity matrix which satisfies $AI = IA = A$

$\therefore$ any 2×2

$(G, \times)$ is a monoid

where G is the set of all non-singular 2×2 matrices

4. Commutative :- $\forall A, B \in G$,

$AB \neq BA$

$(G,$ multiplication $\times)$

$= (G, \times)$ is non-commutative monoid.

5. Show that the matrices $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$ where $\alpha \in R$ forms a group w.r.t matrix multiplication.

Let $A_\beta = \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$ $\alpha, \beta \in R$

$G = \{A_\alpha, A_\beta, A_\gamma - -\}$

Closure : $A_\alpha, A_\beta \in G$

$A_\alpha A_\beta = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$

$$A_\alpha A_\beta = \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix}$$

if $\alpha, \beta \in R$, $\alpha+\beta \in R$

$\times$ is closed in G.

Associative :- Matrix multiplication is always associative

$\therefore A_\alpha (A_\beta A_\gamma) = (A_\alpha A_\beta) A_\gamma$

where $\alpha, \beta, \gamma \in R$

Identity :- Identity matrix $I = A_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$A_\alpha I = I A_\alpha = A_\alpha$

Inverse :- $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$

$A_\alpha^{-1} = \dfrac{\operatorname{adj} A_\alpha}{|A_\alpha|}$ $\qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

$|A_\alpha| = 1$

$$\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$$

$A_\alpha A_\alpha^{-1} = A_\alpha^{-1} A_\alpha = I$

$\exists$ inverse matrix $\forall A_\alpha, A_\beta \ldots \in G$

$(G, \times)$ is a group

6. If G is a set of all positive rational numbers then Prove that G is an abelian group under the composition circle (o) $AoB = \dfrac{AB}{3}$ $\forall A, B \in Q$, then prove that (G, o) is a group. $aob = \dfrac{ab}{3}$ $\forall a, b \in Q$.

Closure : $\forall a, b \in G$

$aob = \dfrac{ab}{3} \in G$

Associative $\forall a, b \in G$

too prove $(boc) = (aob)oc$

$ao(boc) = ao\left(\dfrac{bc}{3}\right) = \dfrac{a \times \frac{bc}{3}}{3} = \dfrac{abc}{9}$

$$(a \circ b) \circ c = \frac{ab}{3} \circ c = \frac{\frac{ab}{3} \times c}{3} = \frac{abc}{9}$$

Identity :- For any $a \in G$ $\exists$ $e \in G$ such that

$$a \circ e = e \circ a = a$$

$$a \circ e = a$$

$$\frac{ae}{3} = a \Rightarrow \boxed{e = 3}$$

So that is $e = 3$ is the identity element.

Inverse :- For $a \in G$ $\exists$ $a^{-1} \in G$ such that

Such $a \circ a^{-1} = a^{-1} \circ a = e$.

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

$$\frac{aa^{-1}}{3} = e$$

$$\frac{aa^{-1}}{3} = 3 \Rightarrow a^{-1} = \frac{9}{a}$$

$\therefore$ $\exists$ inverse element $\forall$ $a \in G$

$$a \circ b = \frac{ab}{3} = \frac{ba}{3} = b \circ a$$

$\therefore$ circle is abelian under G

$(G, \circ)$ is an abelian group.

Theorem 1 :-

for a, b, c in a group G.

i. $a.b = a.c \Rightarrow b = c$ (left Cancelation law)

ii. $b.a = c.a \Rightarrow b = c$ (Right Cancelation law)

Proof :- Let $(G, \cdot)$ be a group

Consider $a.b = a.c$

Pre operating with a^{-1} on BHS

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

$$(a^{-1}.a).b = (a^{-1}.a).c \text{ (associative)}$$

$$e.b = e.c \text{ (Inverse } a.a^{-1} = a^{-1}.a = e)$$

$$b = c \text{ (identity property)}$$

left cancelation law

Let $(G, \cdot)$ be a group.

Consider $a.b = a.c$ $\quad b.a = c.a$

post operating with a^{-1} on B.H.S

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

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

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

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

$b.e = c.e$ (Inverse).

$b = c$ (identity property)

right cancelation law

Theorm 2: if G is a group

i. The identity element of 'G' is unique (using Cancelation Law

ii. $\forall a \in G$, $\exists$ unique inverse in G

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

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

Proof :-

1. Let $(G, \cdot)$ is a group

to prove G has unique identity element

we are considering on contradiction there exist two identity element e & e^{-1} for the group G.

for any $a \in G$, $\exists e \in G$ such that

$$a.e = e.a = a \quad \text{—} (1)$$

for any $a \in G$, $\exists e^{-1} \in G$ such that

$$a.e^{-1} = e^{-1}.a = a \quad \text{—} (2)$$

from (1) & (2) $a.e = a.e^{-1}$

$$e = e^{-1} \quad [LCL]$$

2. Let $(G, \cdot)$ is a group

a^{-1}, b To prove for all $a \in G$, $\exists$ unique inverse

on contraduction let us assume that a^{-1} & b are the two different inverses of a.

$$\therefore a.a^{-1} = a^{-1}.a = e \quad \text{—} (1)$$

$a \cdot b = b \cdot a = e$ — (2)

from (1) & (2)

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

$a^{-1} = b$ [LCL]

$\therefore$ their exist unique inverse $\forall a \in G$.

3. $(G, \cdot)$ is a group.

if $a \in G$ then $a^{-1} \in G$

Since $a^{-1} \in G$, $(a^{-1})^{-1} \in G$

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

$a^{-1} \cdot (a^{-1})^{-1} = (a^{-1})^{-1} \cdot a^{-1} = e$ — (2)

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

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

4. $(G, *)$ is a group

Consider

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

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

$= (ae)a^{-1}$ (associative)

$= aa^{-1}$ (identity)

$= e$ (inverse)

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

$\Rightarrow$ (ab) has inverse is $b^{-1}a^{-1}$

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

Homomorphism:- 30/06/2022

Let $(G, *)$ and (H, o) be two groups a mapping $f: G \to H$ is said to be a group homomorphism if it is $f(a * b) = f(a) \, o \, f(b) \ \forall a, b \in G, H$

Homomorphic mapping :-

Homomorphic mapping is 1-1 then it is monomorphism

if $f \mapsto G \to H$ then f is epimaphism

A homomorphic mapping f is 1-1 and onto then it is called isomarphic isomarpism isomorphism

$f: G \to H$ group homomorphism

Let $(G,+)$ $(H,\times)$ be two groups

$f(x) = 3^x$ then $f: G \to H$

$(x+y) = 3^{x+y}$

$= 3^x . 3^y$

$f(x+y) = f(x)+f(y)$ $\forall$ $x,y \in G, H$

with identity element $3^0 = 1$

Theorem 1 :-

Q:- Let $(P,*)$ (Q,Δ) $(R,\oplus)$ be any groups.

$f: P \to Q$, $g: Q \to R$ be group homomorphism

Proof :-

Given that $(P,*)$ (Q,Δ) $(R,\oplus)$ are given group.

$f: P \to Q$, $g: Q \to R$ be group homomorphisms

then prove that $(gof): P \to R$ is also

next group element

Consider $gof(x*y) = g(f(x*y))$

$= g(f(x) \Delta f(y)) \because f(x*y) = f(x) \Delta f(y)$

$= g(f(x)) \oplus g(f(y))$

$= gof(x) \oplus gof(y)$

$\neq$ g(KR.

$gof: P \to R$ is a group homomorphism.

Theorem 2 :-

Prove that under hom group homomorphism the possibilities

i. associativity ii. ideanpotency

iii. commatabvity holds.

Sol :- Let $(G,*)$ (H,o) are two groups
$f: G \to H$ is a group homomarphism

i. associativity :

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

∴ Start Satisfies the associativity.

ii. idenpotency :-

$$f(a) = f(a*a) = f(a) o f(a)$$

∴ H Satisfies idenpontency

iii. Commutabrity :-

$$f(a*b) = f(a) o f(b)$$
$$= f(b) o f(a)$$
$$= f(b*a)$$

∴ H Satisfies commutarvity

Hence two groups are satisfies homomarphism

Cyclic group :-

Let $(G,*)$ is a group. and if $\exists\, a \in G$ the elements of G can be expressed as some powers of a then the group $(G,*)$ is called a cyclic group.

i.e Any element is expressed in the form of a^n where n is a positive integer and a is called generator of G

Ex: $G = \{1, -1, i, -i\}$, $(G, \times)$ is a group

$1 = i^4$

$-1 = i^2$

$i = i$

$-i = i^3$

∴ $(G, \times)$ is a group with i as generator.

Order of an element :-

The order of an element in a group G is the smallest positive integer n such that $a^n = e$

if no such integer exist then we say that a has infinite order

Eg:- Let $G = \{1, -1, i, -i\}$ $(G, \times)$ is a group.

with identity element $e = 1$

$1^1 = 1 \Rightarrow O(1) = 1$

$(-1)^2 = 1 \Rightarrow O(-1) = 2$

$i^4 = 1 \Rightarrow O(i) = 4$

$(-i)^4 = 1 \Rightarrow O(-i) = 4$

Ex:- find the order of every element

$G = \{1, 3, 5, 7\}$ with $\times_8$

$\times_8$	1	3	5	7
1	1	3	5	7
3	3	1	~~7~~	5
5	5	7	1	3
7	7	5	3	1

$1 \times_8 1 = 1 \Rightarrow 1^2 = 1$

$3 \times_8 3 = 1 \Rightarrow 3^2 = 1$

$5 \times_8 5 = 1 \Rightarrow 5^2 = 1$

$7 \times_8 7 = 1 \Rightarrow 7^2 = 1$

$O(1) = O(3) = O(5) = O(7) = 2$