Unit-3

Group theory (advance of set theory)

Algebraic structure :-

A non empty set G along with a binary operator is called Algberic structure (or) Algberic system

here it is written as $(G, *)$

where G is any set

$*$ is any binary operator

ex:-

$(N, +)$

$(Q, -)$

$(S, *\times)$

binary operator:-

Let S be any non empty set if $f: S \times S \to S$ is a mapping then f is called a binary operator in S,

→ we use the symbols $+, -, \times, \div, *, \oplus, \circ$ for binary operator

ex:-

① define a binary operator $*$ as $a+b-ab$ $\forall a, b \in S$

② define a binary operator $\circ$ as $a \circ b = a$ $\forall a, b \in S$

properities :-

1) closer :-

if $a*b \in S$ $\forall a,b \in S$ then we say that it satisfy's the closer property

2) Associative :-

if $(a*b)*c = a*(b*c)$ $\forall a,b,c \in S$

3) existent's of identity :-

$\exists e \in S \Rightarrow a*e = e*a = a$

such that $\forall a \in S$

$\begin{cases} (N, \times) \Rightarrow 1 \times a = a \times 1 = a \\ (Z, +) \Rightarrow 0 + a = a + 0 = a \end{cases}$

4) existents of inverse :-

$\exists b \in S \Rightarrow a*b = b*a = e$ for any $a \in S$

$\begin{cases} 1, 1 \Rightarrow 1-1 = 0 \\ \qquad (\text{additive} = 0) \\ 2 \times \frac{1}{2} \to 1 \Rightarrow (\text{multiplitive} = 1) \end{cases}$

5) ~~co~~mmutative commatitive :-

$\forall a,b \in S \Rightarrow a*b = b*a$

Groupoid :-

Th algebric structure $(G, *)$ which statisf's only closer properity is called groupoid

Semi-group:-

An algebric structure $(G, *)$ is said to semi-group if it statisfy's closer, & associative property

Monoid :-

An algebric structure $(G, *)$ is said to be monoid if it statisfy's closer, associative, existents of identity

** Group:-

An algebric structure $(G, *)$ is said to a group if it statisfy's closer

1) closer $\Rightarrow a * b \in G \quad \forall a, b \in G$

2) Associative $\Rightarrow (a * b) * c = a * (b * c) \quad \forall a, b, c \in G$

3) Existents of Identity

$$\exists e \in G \ni a * e = e * a = a \quad \forall a \in G$$

4) Existents of inverse

$$\exists e \in G \ni a * b = b * a = e \text{ for any } a \in G$$

Abelian Group:-

A group is said to Abelian group if it statisfy commutative property

1Q) Let 'S' be a non-empty set and 'o' is the binary operator defined by $a \circ a = a$ $\forall a, b \in S$ determine whether $\circ$ is commutative & associative in S

1) i) $a \circ b = a$

$b \circ a = b$

$a \circ b \neq b \circ a$

ii) $(a \circ b) \circ c = a \circ c = a$

$a \circ (b \circ c) = a \circ b = a$

$(a \circ b) \circ c = a \circ (b \circ c)$

2Q) circle top 'o' operation is defined on Z as $a \circ b = a + b - ab$ $\forall a, b \in Z$ is the operation 'o' is binary operation in Z if so is it associative & commutative

i) $a \circ b = a + b - ab \in Z$

ii) $(a \circ b) \circ c = (a + b - ab) \circ c$

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

$\Rightarrow a + b + c - ab - ac - bc + abc$

$a \circ (b \circ c) \Rightarrow a \circ (b + c - bc)$

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

$\Rightarrow a + b + c - bc - ab - ac + abc$

iii) $a \circ b = a + b - ab$

$b \circ a = b + a - ba$

3Q) prove that $(P(S), \cap)$ is a semi-group where $P(S)$ is power set of S and '$\cap$' intersection

i) if $A, B \in P(S)$

$\Rightarrow A \cap B \in P(S)$

it statisfy's closer

ii) we know that

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

so the it statisfy's associative property

Hence it is a semi-group

4Q) determine wheather (Q, o) is semi-group where Q is a set of rational numbers and binary operater is defined as

$a o b = a - b + ab$

i) if $A, B \in Q$

$\Rightarrow A o B \in Q$

ii) $(a o b) o c \Rightarrow (a - b + ab) o c$

$\Rightarrow (a - b + ab) - c - (a - b + ab)c$

$\Rightarrow a - b - c - abc - bc - ac - bc + ac + bc$

$\Rightarrow a - b - c - 2ac - 2bc$

$a \circ (b \circ c) \Rightarrow a \circ (b - c + bc)$

$\Rightarrow a - (b - c + bc) - a(b - c + bc)$

$\Rightarrow a - b - c - ab - ac - ab + ac - ab - ac$

$\Rightarrow a - b - c - 3ab - ac$

5a) prove that $(\mathbb{Z}, \cdot)$ is abelian group where $\cdot$ is usual multiplication

i) closer $\forall a, b \in \mathbb{Z} \Rightarrow a \cdot b \in \mathbb{Z}$

ii) Associative

$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in \mathbb{Z}$

iii) Identity

$\exists\, 1 \in \mathbb{Z} \ni a \cdot 1 = 1 \cdot a = a, \quad \forall a \in \mathbb{Z}$

iv) Inverse

there is no inverse of $\frac{1}{2} \in \mathbb{Z}$

$\therefore (\mathbb{Z}, \cdot)$ is not abelian group but monoid

6) $(\mathbb{Z}, +)$

i) $\forall a, b \in \mathbb{Z} \Rightarrow a \cdot b \in \mathbb{Z}$ closer

ii) $a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{Z}$ Associative

iii) $\exists\, 0 \in \mathbb{Z} \ni a + 0 = 0 + a = a \quad \forall a \in \mathbb{Z}$ (Identity)

iv) $\exists\, -a \in \mathbb{Z} \ni a + (-a) = (-a) + a = 0$ for any $a \in \mathbb{Z}$ (Inverse)

v) $a+b=b+a \quad \forall a, b, \in \mathbb{Z}$

$(\mathbb{Z}, +)$ is A.G

7) prove that $G_4 = \{1, \omega, \omega^2\}$ is a A.G with represtive multiplication where $1, \omega, \omega^2$ are cubic root of unity

composition table (CT)

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

$\therefore \omega^3 = 1$

$\omega^4 = \omega$

1) closer :-

All the values in the table are in G_2 so it statisfy closer

2) Associative :-

usual multiplication is associative so it statisfy's associative

3) Identity :-

the value against 1 i.e 1st row & col are same so Identity element is 1

4) Inverse :-

1 is 1

ω is ω^2

ω^2 is ω

5) commitative :-

the table is symmetric so it is commitative

8) show that $G_2 = \{1, -1, i, -i\}$ is A.G with ropeetive multiplication where $i = \sqrt{-1}$

C.T

•	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) closer

2) Associative

3) Identity

4) Inverse

$1 \Rightarrow 1$

$-1 = -1$

$i = -i$

$-i = i$

5) Sommitative

9) prove that a set Z of all integers with binary operation * defined by $a * b = a + b + 1$ $\forall a, b \in Z$ is an A.G

i) closer

$a * b = a + b + 1 \in Z \quad \forall a, b \in Z$

ii) Associative

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

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

$= a+b+c+2$

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

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

$= a+b+c+2$

iii) Identity :-

$a*e = a \Rightarrow a+e+1 = a$

$\Rightarrow e = -1$

iv) inverse

$a*b = e \Rightarrow a+b+1 = -1$

$\Rightarrow a+b = -2$

$\Rightarrow b = -2-a$

$\Rightarrow b = -(a+2)$

$\in Z \ \forall a \in Z$

$\therefore -(a+2)$ is inverse of $a \in Z$

v) commutative :-

$a*b = a+b+1$

$b*a = b+a+1$

$\therefore a*b = b*a$

10) show that $(Q^+, \circ)$ is an AG where Q^+ is all positive rational numbers & operator $\circ$ is defined by $a \circ b = ab/3$

i) closer

$a \circ b = ab/3 \quad \forall a, b \in Q^+$

ii) Associative

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

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

iii) identity

$(a \circ e) = a \Rightarrow \frac{ae}{3} = a$

$e = 3$

iv) Inverse

$(a \circ b) = e$

$\Rightarrow \frac{ab}{3} = 3$

$\Rightarrow ab = 9$

$\Rightarrow b = 9/a$

$\Rightarrow a = 9/b$

v) $(a \circ b) = \frac{ab}{3}$

$(b \circ a) = \frac{ba}{3}$

Addition modulo m:-

If a, b are any two integer & r is the least non-negative number obtained by dividing the ordinary sum a & b by m then the addition modulo m of a & b is r

→ Symbolically $a +_m b = r \quad (0 \le r < m)$

ex:-

$m = 5$

$3 +_5 2 = 5 = 0$

$7 +_5 2 = 4 \Rightarrow m = 5$

$r = 4$

5) 9 (1
5
(4)

multiplication modulo p:-

if a & b are two integers and r is the least non-negative remainder obtained by dividing ordinary product of a and b by p then the multiplication modulo p of a & b is r

→ symbolically $a \times_p b = r \quad (0 \le r < p)$

ex:-

$5 \times_3 2 = 1$

11@) Show that set 'G' is AG where G is the set of addition modulo 5

$G = \{0, 1, 2, 3, 4\}$

$+_5$	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

so it is

closer => all the values are in G_5

Associative => $1 +_5 (3 +_5 4) = 1 +_5 2 = 3$

$(1 +_5 3) +_5 4 = 4 +_5 4 = 3$

Identity (co) => 1st row & 1st col are same as in G_5

Inverse => $0^{-1} = 0$

$1^{-1} = 4$

$2^{-1} = 3$ all the elements have

$3^{-1} = 2$ inverses

$4^{-1} = 1$

commutitive

the table is symmetric so set G_5 is commutitive

∴ set G_5 is A-G

12) show that the set G_5 of multiplication modulo 5 is an A-G

$G_5 = \{1, 2, 3, 4\}$

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

So it is

closer :-

all the values are in G_5

associative

$2 \times_5 (3 \times_5 4) = 2 \times_5 2 = 4$

$(2 \times_5 3) \times_5 4 = 1 \times_5 4 = 4$

Identity

$e = 1$

Inverse

$1^{-1} = 1$

$2^{-1} = 3$

$3^{-1} = 2$

$4^{-1} = 4$

commitative

the table is symmetric so set is commitative

∴ set G is AG

13) $G = \{1, 5, 7, 11, 13, 17\}$ $\times_{18}$ find construct composition table & find inverse of all elements

SOL:-

$\times_{18}$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

$12^{-1}/_{18} = 6.72$

-6

0.72×18

$= 13$

Inverse

$1^{-1} = 1$

$5^{-1} = 11$

$7^{-1} = 13$

$11^{-1} = 5$

$13^{-1} = 7$

$17^{-1} = 17$

14) If G_2 is set of even numbers i.e $G_2 = \{\ldots -4, -2, 0, 2, 4, \ldots\}$ then prove that G_2 is ΔG_2 with usual addition as an operator

Sol) Let $a = 2x$, $b = 2y$, $c = 2z$

$a, b, c \in G_2$ & $x, y, z \in Z$

i) $a+b = 2x+2y = 2(x+y) \in G_2$

ii) $a+(b+c) = 2x + (2y+2z)$

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

$= (a+b) + c$

iii) $a+e = a \quad e = 0 \in G_2$

iv) $a+d = 0 \Rightarrow d = -a \in G_2$

v) $a+b = 2x+2y = 2(x+y)$

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

$= b+a$

15) State $G = \{x \mid x = 2^a 2^b$ for $a, b \in Z\}$ under multiplication is Group

Let $x = 2^a 2^b$, $y = 2^c 2^d$, $z = 2^e 2^f$

$x, y, z \in G$ & $a, b, c, d, e, f \in \mathbb{Z}$

i) $x \cdot y = 2^a 2^b \cdot 2^c \cdot 2^d$

$= 2^{a+c} \cdot 2^{b+d}$

$a+c, b+d \in \mathbb{Z}$

$\therefore x, y \in G$

ii) $x(y \cdot z) = 2^a 2^b (2^c 2^d 2^e 2^f)$

$= (2^a \cdot 2^b \cdot 2^c \cdot d^d) 2^e 2^f$

$= (x \cdot y) \cdot z$

iii) Let $e = 2^i \cdot 2^j \in G \Rightarrow a \cdot e = a$

$\Rightarrow (2^a \cdot 2^b)(2^i \cdot 2^j) = 2^a \cdot 2^b$

$\Rightarrow 2^{a+i} \cdot 2^{b+j} = 2^{a \cdot b}$

i.e $a+i = a \Rightarrow j = 0$

$b+i = b \Rightarrow j = 0$

$\therefore e = 2^0 \cdot 2^0 \in G$ is an identity

iv) Let $y = 2^c 2^d \Rightarrow x \cdot y = 2^0 2^0$

$2^a \cdot 2^b \cdot 2^c \cdot 2^d = 2^0 \cdot 2^0$

$2^{a+c} \; 2^{b+d} = 2^0 \cdot 2^0$

$= a+c = 0$ & $b+d = 0$

$c = -a$ & $d = -b$

$\therefore 2^{-a}\ 2^{-b}$ is inverse of $2^a \cdot 2^b$

Hence $-a, -b \in \mathbb{Z}$

$2^{-a} \cdot 2^{-b} \in G$

16Q) Show that a set of order pair (a, b) of Real numbers for which $a \neq 0$ w.r.t the operator defined by $(a,b) * (c,d) = (ac, bc+d)$ is a group is this commutative

$(a, b) * (c, d) = (ac, bc+d)$

i) clearly $a, b, c, d, \in \mathbb{Z}$

$\Rightarrow ac, bc+d \in \mathbb{Z}$

moreover since $a \neq 0$

$c \neq 0 \Rightarrow ac \neq 0$

$\therefore (a, b) * (c, d) \in G$

ii) $(a, b) * [(c, d) * (e, f)]$

$(a, b) * (ce, d, e+f)$

$(ace, bec + de + f)$

$[(a,b) * (c,d)] * (e,f)$

$= (ac, bc+d) * (e, f)$

$\Rightarrow (aec, bce, + de + f)$

LHS = RHS

iii) Let $(a,b) * (c,d) = (a,b)$

$\Rightarrow (ac, bc+d) = (a,b)$

$\therefore ac = a \;\&\; bc+d = b$

$\Rightarrow c = 1 \;\&\; b+d = b \Rightarrow d = 0$

$\therefore (1,0) \in G_1$ is an identity

iv) $(a,b) * (x,y) = (1,0)$

$(ax, bx+y) = (1,0)$

$ax = 1 \qquad bx+y = 0$

$x = 1/a \qquad y = -b/a$

since $a \neq 0 \Rightarrow x \neq 0$

$\therefore (1/a, -b/a)$ is inverse ele- of (a,b)

v) $(a,b) * (c,d) = (ac, bc+ad)$

$(c,d) * (a,b) = (ac, ad+b)$

$\therefore bc+d \neq ad+b$

$(a,b) * (c,d) \neq (c,d) * (a,1)$

$\therefore$ Hence it is not commutative

Sub-group :-

Let $(G,*)$ be a group & H be non-empty subset of G_1 if $(H,*)$ is its self is a Group then it is called subgroup of $(G,*)$

ex :-

$(\mathbb{Z}, +)$ subgroup of $(\mathbb{Q}, +)$

17) Let $G_1 = \{1, -1, i, -i\}$, $H = \{1, -1\}$ check whether H is subgroup of G_1

·	1	-1
1	1	-1
-1	-1	1

i) closer
it statisfy's closer

2) it statisfy Associative

3) identity 1 is in G_1

4) inverse
$1^{-1} = 1$
$-1^{-1} = -1$
∴ H is a group

∴ H is a subgroup of G_1

18) prove that $H = \{0, 2, 4\}$ is a subgroup of $(Z_6, +_6)$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

i) closer
it statisfy closer

ii) Associative statisfy

iii) identity 0 is in Z_6

iv) inverse
$0^{-1} = 0$
$2^{-1} = 4$
$4^{-1} = 2$

∴ H is a group
∴ H is a subgroup of Z_6

19) Let S be a set of ordered pair (a, b) of real number such that $a \neq 0$, binary operator '$\times$' is defined by $(a, b) \times (c, d) = (ac, bc + d)$ prove that $(H, \times)$ is a subgroup of $(S, \times)$ given that $H = \{(1, b) / b \in R\}$

i) $(1, a), (1, b) \in H$

$(1, a) \times (1, b) = (1, a + b) \in H$

ii) Associative

it also statisfy is associative

iii) $(1, b) \times (1, e) = (1, b)$

$\Rightarrow (1, b + e) = (1, b)$

$\Rightarrow b + e = b$

$\Rightarrow e = 0$

$\therefore (1, 0)$ is identity

iv) $(a, b)^{-1} = (1/a, -b/a)$

$(1, b)^{-1} = (1, -b) \in H$

$\therefore$ H is a group

$\therefore$ H is a subgroup of S.

order of an element:-

Let $(G, *)$ be a group and $a \in G$ then if their exists least positive integer $n \Rightarrow a^n = e$ where e is the identity element in G then 'n' is order of a & written as $O(a) = n$

ex:-

$G = \{1, -1, i, -i\}$

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

$1^2 = 1$

$(-1)^1 = -1 \times$

$(-1)^2 = 1 \checkmark \quad O(-1) = 2$

$i^1 = i \times$

$i^2 = -1 \times$

$i^3 = -i \times \quad O(i) = 4$

$i^4 = 1 \checkmark$

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

$(-i)^2 = -1 \times$

$(-i)^3 = i \times$

$(-i)^4 = 1 \checkmark$

$O(-i) = 4$

order of a group:-

the order of a group is no. of elements in the group

ex:-

1) $G = \{1, -1, i, -i\}$

$O(G) = 4$

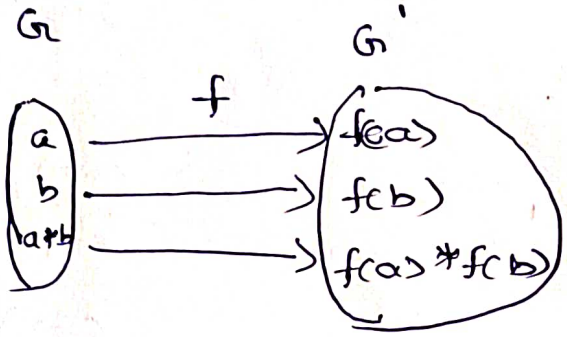
2) $(\mathbb{Q}^+, +_5)$

then $O(\mathbb{Q}^+, +_5) = 5$

functions of group:-

i) Homomorphism:-

A function $f:(G,*) \to (G',\cdot)$ it said to homomorphism if $f(a*b) = f(a).f(b)$ where $a,b \in G$ & $f(a), f(b) \in G'$



ii) Endomorphism:-

A homomorphism for a group G to itself is called endomorphism i.e

$f:(G, *) \to (G, *)$

iii) Monomorphism:-

A homomorphism $f:G \to G'$ is said to monomorphism if it is one-one function

iv) Epimorphism:-

A homomorphism $f:G \to G'$ is said to epimorphism if it is onto function.

v) isomorphism

A homomorphism $f: G \to G'$ is said to be isomorphism if it is one-one & onto function.

vi) automorphism

An isomorphism f for G to it-self is called automorphism.

1) Let $(\mathbb{Z}, +)$ be a group & $(G, *)$ be another group where $G = \{2^n / n \in \mathbb{Z}\}$ A function $f: \mathbb{Z} \to G$ defined by $f(n) = 2^n \ \forall\ n \in \mathbb{Z}$ prove that f is a homomorphism

Let $n_1, n_2 \in \mathbb{Z} \Rightarrow f(n_1) = 2^{n_1}$, $f(n_2) = 2^{n_2}$

$f(n_1+n_2) = 2^{n_1+n_2}$

$= 2^{n_1} * 2^{n_2}$

$= f(n_1) * f(n_2)$

$\therefore$ f is homomorphism

2) Let $(G, *)$ defined by $G = \{1, -1, i, -i\}$ & $(\mathbb{Z}, +)$ be other group prove that $f: \mathbb{Z} \to G$ is homomorphism where $f(n) = i^n \ \forall\ n \in \mathbb{Z}$

Let $n_1, n_2 \in \mathbb{Z} \Rightarrow f(n_1) = i^{n_1}$, $f(n_2) = i^{n_2}$

$f(n_1+n_2) = i^{n_1+n_2} = i^{n_1} * i^{n_2}$

$= f(n_1) * f(n_2)$

$\therefore$ f is homomorphism

Note

If f is a homomorphism $f: G \to G'$ then we write $G \cong G'$. This is read as G is isomorphic to G'

a) Let $(R, +)$ be the additive group & $(R^+, *)$ be the multiplicative group then the function $f: R \to R^+$ defined by $f(x) = e^x$ is isomorphism

i) Let $f(a) = f(b)$ for $a, b \in R$

$\Rightarrow e^a = e^b$

$\Rightarrow a = b$

$\therefore f$ is one-one.

ii) Let $y \in R^+$ $\quad f(x) = y$

Let $f(x) = y$

$\Rightarrow e^x = y \Rightarrow \ln e^x = \ln y$

$\Rightarrow x \ln e = \ln y$

$= x = \ln y \in R$

for every $y \in R^+$ $\exists \ln y \in R$

$\ni f(\ln y) = y$

$\therefore f$ is onto

iii) $f(a+b) = e^{a+b} = e^a * e^b$

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

$\therefore f$ is homomorphism

$\therefore f$ is iso-morphism

a) Let $(\mathbb{Z}, +)$ be a group and $(G, *)$ be other group where $*$ is usual multiplication and $G = \{2^n / n \in \mathbb{Z}\}$ define $f: \mathbb{Z} \to G$ by $f(n) = 2^n \; \forall \; n \in \mathbb{Z}$ show that $\mathbb{Z}$ is isomorphic to G $(\mathbb{Z} \cong G)$

i) Let $f(a) = f(b)$ for $a, b \in \mathbb{Z}$

$\Rightarrow 2^a = 2^b$

$\Rightarrow a = b$

$\therefore f$ is one-one

ii) Let $y \in G \Rightarrow f(x) = y$

$\Rightarrow 2^x = y$

$\Rightarrow \log 2^x = \log y$

$\Rightarrow x \log 2 = \log y$

$x = \frac{\log y}{\log 2} \Rightarrow \log_2 y \in \mathbb{Z}$

$\therefore$ for $y \in G \; \exists \log_2 y \in \mathbb{Z} \Rightarrow$

$f(\log_2 y) = 2^{\log_2 y} = y$

$\therefore f$ is onto

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

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

$\therefore f$ is homomorphism

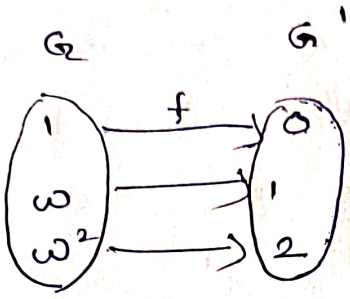
$\therefore f$ is isomorphism

Q) Let $(G, *)$ & $(G', +_3)$ be two groups where $*$ is usual multiplication, $G = \{1, \omega, \omega^2\}$ & $G' = \{0, 1, 2\}$ define $f: G \to G'$ ∋ $f(\omega^n) = n$ prove that $G \cong G'$

i) $f(1) = f(\omega^0) = 0$

$f(\omega) = f(\omega^1) = 1$

$f(\omega^2) = 2$



∴ f is one-one

ii) for $n \in G'$ ∃ ω^n ∋

$f(\omega^n) = n$

∴ f is onto

iii) Let $\omega, \omega^2 \in G$

LHS = $f(\omega * \omega^2) = f(\omega^3) = f(\omega^0) = 0$

RHS = $f(\omega) +_3 f(\omega^2) = 1 +_3 2 = 0$

∴ LHS = RHS.

∴ f is homomorphism.

∴ f is isomorphism.

***

Theorems:-

1) If G is a group then

i) the identity element 'e' is unique $e \in G$

Let $e \in G$ be the identity element then

$$e \cdot a = a \cdot e = a \quad \forall a \in G \rightarrow (1)$$

Let $e' \in G$ be the other identity element then

$$e' \cdot a = a \cdot e' = a \quad \forall a \in G \rightarrow (2)$$

Take $a = e'$ in (1) $\Rightarrow e \cdot e' = e' \cdot e = e' \rightarrow (3)$

Take $a = e$ in (2) $\Rightarrow e' \cdot e = e \cdot e' = e \rightarrow (4)$

from (3) & (4) $\Rightarrow e' \cdot e = e'$ &

$e' \cdot e = e$

$\Rightarrow e' = e$

$\therefore$ Identity element is unique.

ii) the inverse element is unique

Let there are two inverses a_1 & a_2 for $a \in G$

Since a_1 is the inverse of a we get

$$a \cdot a_1 = a_1 \cdot a = e \rightarrow (1)$$

Since a_2 is the inverse of a we get

$$a_1 \cdot a_2 = a_2 \cdot a = e \rightarrow (2)$$

(1) & (2) $\Rightarrow a \cdot a_1 = a \cdot a_2$

pre multi by a_1 on both sides

$$a_1(a \cdot a_1) = a_1(a \cdot a_2)$$

$$(a_1 \cdot a) \cdot a_1 = (a_1 \cdot a) \cdot a_2$$

$$\Rightarrow e \cdot a_1 = e \cdot a_2$$

$$\Rightarrow a_1 = a_2$$

iii) prove that a inverse $(a^{-1})^{-1} = a$

a^{-1} is a inverse of a

$\therefore a a^{-1} = a^{-1} . a = e \rightarrow ①$

also $(a^{-1})^{-1}$ is a inverse of a^{-1}

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

① & ②

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

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

Since inverse is unique $(a^{-1})^{-1} = a$

iv) for all $a, b \in G \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$

for $a, b \in G$ w.k.T

$ab \in G$

w.k.T

$(ab)^{-1}$ is the inverse of ab

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

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

that is $b^{-1}a^{-1}$ is also inverse of ab

since inverse is unique

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

2) for $abc \in G$ where G is a group then prove that

i) $a.b = a.c \Rightarrow b = c$ [left cancellation law]

ii) $b.a = c.a \Rightarrow b = c$ [Right cancellation law]

i) $a \cdot b = a \cdot c$

pre multiply by $\bar{a}^1$

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

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

$e \cdot b = e \cdot c$

$b = c$

ii) $b \cdot a = c \cdot a$

post multiply by $\bar{a}^1$

$(b \cdot a) \cdot \bar{a}^1 = (c \cdot a) \bar{a}^1$

$b(a \cdot \bar{a}^1) = c(a\bar{a}^1)$

$be = c \cdot e$

$b = c$

3) Let G be a group $a, b \in G$ which commutate show that

i) $\bar{a}^1$ & b commutate, ii) $\bar{b}^1$ & a commutate

ii) $\bar{a}^1$ & $\bar{b}^1$ commutate

i) Given that a, b commute

$a \cdot b = b \cdot a$ ⟶ post multiply by $\bar{a}^1$

$\Rightarrow (ab)\bar{a}^1 = (ba)\bar{a}^1$

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

$\Rightarrow a(b\bar{a}^1) = b \cdot e = b$

pre multiply by $\bar{a}^1$

$(\bar{a}^1 a)(b\bar{a}^1) = \bar{a}^1 b$

$e(b\bar{a}^1) = \bar{a}^1 b$

$b\bar{a}^1 = \bar{a}^1 b$

$\therefore \bar{a}^1 b$ commute

ii) Given that a, b commute

$a \cdot b = b \cdot a$

post multiply with b^{-1}

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

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

$(a) e = a \cdot e$

$(a) = a$

pre multiply with b^{-1}

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

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

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

(or)

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

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

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

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

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

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

iii) $ab = ba$

$(ab)^{-1} = (ba)^{-1}$

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