Course - BMG4CC1D 4th Sem
Algebra (marks 75) (General)

1) Defination and Examples of groups :- First we discuss about binary composition for discussion of group.

Binary composition :- Let A be a non empty set. A binary composition on A is a mapping $f: A \times A \to A$. Therefore a binary composition f assigns to each ordered pair of elements of A a definite element. This mapping is generally denoted by the symbol '$\circ$'. For a pair of elements a, b in A, the image of (a, b) under the binary composition '$\circ$' is $a \circ b$.

Note:- The symbols like $*, +, \cdot, \odot, \oplus$ are also used to denote a binary composition.

Groups :-

A non empty set G is said to ~~be~~ form a group with respect to a binary composition '$\circ$' if

(i) G is closed under the composition $\circ$,

(ii) '$\circ$' is associative

iii) there exists an element e in G such that $e \circ a = a \circ e = a$ for all a in G.

iv) for each element a in G, there exists an element a' in G such that $a' \circ a = a \circ a' = e$.

The group is denoted by the symbol $(G, \circ)$.

Abelian Group :- A group $(G, \circ)$ is said to be a commutative group or an abelian group if $\circ$ is commutative.

i.e. $\forall\ a, b \in G$.

$a \circ b = b \circ a$ holds.

some discussions :-

1) The set Z' forms a commutative group with respect to addition.

I) Let $a, b \in Z'$, then clearly $(a+b) \in Z'$. This shows that the set Z' is closed under addition.

b) Addition is associative on the set $\mathbb{R}$. Z' being a subset of $\mathbb{R}$, so addition is associative on Z'.

c) clearly $0 \in Z'$ and $(0+a) = (a+0) = a\ \forall\ a \in Z'$ so, 0 is the identity element.

d) Let $a \in Z'$, then $-a \in Z'$ such that $a + (-a)$ $= (-a) + a = 0$ (identity element in Z'), this shows that inverse of each element of Z' exists in Z'.

e) Addition is commutative on $\mathbb{R}$, Z' being subset of $\mathbb{R}$ so addition is commutative on Z'.

$\therefore (Z', +)$ is a commutative group.

H.W Check yourself that $(2Z', +)$ is a commutative group.

(2) $(Z, \cdot)$ is not a group.

clearly ~~inverse~~ 1 being identity element since $a \cdot 1 = 1 \cdot a = a \ \forall\ a$ in Z. But the inverse of no element other than 1 and -1 in Z exists in Z. So inverse property does not hold.

$\therefore (Z, \cdot)$ is not a group.

Similarly $(Q, \cdot)$ is not a group since inverse of 0 does not exist.

In the same way $(\mathbb{R}, \cdot)$ is not a group as inverse of 0 does not exist in $\mathbb{R}$.

Note:- But $Q^* = Q - \{0\}$ forms a commutative group.

** Let $M_2(\mathbb{R})$ be the set of all 2×2 matrices whose elements are real numbers. We prove that $M_2(\mathbb{R})$ forms a commutative group with respect to matrix addition.

Proof:- (i) Let $A, B \in M_2(\mathbb{R})$, then $A + B \in M_2(\mathbb{R})$

$\therefore$ the set $M_2(\mathbb{R})$ is closed under '+'.

(ii) we know that matrix addition is associative on $M_2(\mathbb{R})$.

iii) The null matrix $O_2 \in M_2(\mathbb{R})$ and $O_2 + A = A + O_2 = A$ for all A in $M_2(\mathbb{R})$. So O_2 is the identity matrix.

iv) Let $A \in M_2(\mathbb{R})$ then $-A \in M_2(\mathbb{R})$ and $-A + A = A + (-A) = O_2$. This shows that $(-A)$ is the inverse of A. This shows that each elements of $M_2(\mathbb{R})$ has its own inverse in $M_2(\mathbb{R})$.

v) matrix addition is commutative on $M_2(\mathbb{R})$. This shows that $(M_2(\mathbb{R}), +)$ is a commutative group.

Note:- The set $M_2(\mathbb{R})$ does not form a group under matrix multiplication.

Let A be a singular matrix in $M_2(\mathbb{R})$ $\therefore |A| = 0$. clearly I_2 being identity element of $M_2(\mathbb{R})$ under matrix multiplication. Then there does not exist a matrix B in $M_2(\mathbb{R})$ such that $A \cdot B = B \cdot A = I_2$ holds. Therefore A has no inverse.

$\therefore (M_2(\mathbb{R}), \cdot)$ is not a group.

** Let S be the set of all (2×2) non-singular matrices whose elements are real numbers. S is a proper subset of $M_2(\mathbb{R})$. We prove that S forms a non-commutative group under matrix multiplication.

Proof :- (i) Let $A, B \in S$ then $\det A \neq 0$; $|B| \neq 0$

now $\det(AB) = \det(A) \cdot \det(B) \neq 0$

$\therefore AB \in S$.

$\therefore$ S is closed under matrix multiplication.

(ii) matrix multiplication is associative on $M_2(\mathbb{R})$ so it is also associative in S; as S is a subset of $M_2(\mathbb{R})$.

(iii) $I_2 \in S$ since $\det(I_2) = 1 \neq 0$ and $I_2 \cdot A = A \cdot I_2 = A$ for all A in S. So, I_2 is the identity element of S.

(iv) Let $A \in S$ so $|A| \neq 0$ and hence A^{-1} is a (2×2) matrix; $\det(A^{-1}) = \frac{1}{\det(A)} \neq 0$

$\therefore A^{-1} \in S$

$\therefore$ each elements of S has its own inverse in S.

$\therefore (S, \cdot)$ is a group.

[H] This group is called the general linear group of degree 2 over $\mathbb{R}$ and denoted by

$GL(2,\mathbb{R})$.

Note:- 1) $GL(2,\mathbb{R})$ is non commutative group as for two arbitrary matrices $A, B \in GL(2,\mathbb{R})$ $A \cdot B \neq B \cdot A$, in general.

2) The group $GL(n,\mathbb{R})$ is the group of all non-singular $(n \times n)$ matrices under matrix multiplication

Let's do yourself

(1) Examine if the following systems are group

(1) $(\mathbb{Z}', o)$ where $a o b = a + b + ab$; $a, b \in \mathbb{Z}'$

(2) $(\mathbb{R}^*, o)$ where $a o b = |ab|$; $a, b \in \mathbb{R}^* = \mathbb{R} - \{0\}$.

(3) $(\mathbb{R}, o)$ where $a o b = 2(a+b)$; $a, b \in \mathbb{R}$.

(4) prove that the set H forms a commutative group with respect to matrix multiplication. where

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \text{ and } ad - bc = 1 \right\}.$$

(5) prove that the set of all complex numbers of unit modulus forms a commutative group with respect to multiplication.

(6) prove that the set $\{2^n : n \in \mathbb{Z}'\}$ forms a commutative group with respect to multiplication.

Proof of (6)

Let A denotes the set of all complex numbers of unit modulus.

now $A = \{ a+ib : a,b \in \mathbb{R} \text{ and } a^2+b^2 = 1 \}$

(i) now let $x+iy$ and $(p+iq) \in A$ where $x,y,p,q \in \mathbb{R}$ and $x^2+y^2 = 1$ and $p^2+q^2 = 1$

now $(x+iy)\cdot(p+iq)$

$= (xp-yq) + i(xq+yp)$

now, $(xp-yq)^2 + (xq+yp)^2$

$= x^2p^2 - 2xypq + y^2q^2 + x^2q^2 + 2xypq + y^2p^2$

$= x^2(p^2+q^2) + y^2(p^2+q^2)$

$= x^2+y^2 = 1$

$\therefore (x+iy)\cdot(p+iq) \in A.$

$\therefore$ closure property holds.

(ii) clearly multiplication is associative on A.

(iii) clearly $(1+0\cdot i) \in A$.

now let $(a+ib) \in A$ where $a,b \in \mathbb{R}$. $a^2+b^2 = 1$

and $(a+ib)\cdot(1+0\cdot i) = (1+0\cdot i)\cdot(a+ib) = (a+ib)$

this shows that $(1+0\cdot i)$ is the identity element of A (under multiplication).

(iv) Let $(a+ib)$ be an arbitrary element of A where $a^2+b^2=1$ and $a,b \in \mathbb{R}$

clearly $(a-ib) \in A$ since $|a-ib| = \sqrt{a^2+b^2} = 1$

now
$(a+ib).(a-ib) = (a-ib).(a+ib) = 1+0.i$

this shows that each elements of A has its own inverse in A.

(v) This shows that $(A,\cdot)$ forms a group.

commutative property

Let $a+ib$ and $c+id \in A$ where $a^2+b^2=1$ and $c^2+d^2=1$; $a,b,c,d \in \mathbb{R}$.

now
$(a+ib).(c+id)$
$=(ac-bd)+i(be+ad)$

and
$(c+id).(a+ib)$
$=(ac-bd)+i(ad+bc)$

$\therefore \forall (a+ib),(c+id) \in A$ where $a^2+b^2=1$; $c^2+d^2=1$
$a,b,c,d \in \mathbb{R}$

$(a+ib).(c+id) = (c+id).(a+ib)$

$\therefore (A,\cdot)$ is a commutative group.

Some theorems

(1) A group $(G,0)$ contains only one identity element

(2) ~~In a group $(G,0)$~~

proof: Let e, f be two identity elements in a group $(G,0)$.

Then $e \circ a = a \circ e = a \quad \forall a \in G$: [since e being identity element]

and $f \circ a = a \circ f = a \quad \forall a \in G$ [since f being identity element]

We have

$e \circ f = f$ when [e being identity element]

and $e \circ f = e$ when [f being identity element]

$\therefore e = f$ and this proves uniqueness of identity element.

(2) In a group $(G, \circ)$ each element has only one inverse.

proof:- Let $a \in G$ and a', a'' be two inverses of a.

Then $a' \circ a = a \circ a' = e$ [e being identity element]

and $a'' \circ a = a \circ a'' = e$

We have, $a' \circ (a \circ a'') = (a' \circ a) \circ a''$ [since $\circ$ is associative]

$\therefore a' \circ (a \circ a'') = e \circ a'' = a'' \quad \text{---(i)}$

also $a' \circ (a \circ a'') = a' \circ e = a' \quad \text{---(ii)}$

from (i) and (ii) we have $a'' = a'$ and this proves that the inverse of a is unique.

(3) In a group $(G, \circ)$

(i) $a \circ b = a \circ c$ implies $b = c$ [left cancellation law]

(ii) $boa = coa \Rightarrow b = e$ [right cancellation law]
for all $a, b, c \in G$.

proof:-

(i) since $a \in G$ so $\bar{a}^1 \in G$.

now $aob = aoc$

$\Rightarrow \bar{a}^1 o (aob) = \bar{a}^1 o (aoc)$

$\Rightarrow (\bar{a}^1 oa) ob = (\bar{a}^1 oa) oc$ [since 'o' is associative]

$\Rightarrow eob = eoc$ [e being identity element]

$\Rightarrow b = c$

ii) $boa = coa$ (check yourself)

$\Rightarrow b = c$

(4) In a group (G, o): $(aob)^{-1} = (\bar{b}^1 o \bar{a}^1)$ $\forall a, b \in G$.

proof:- Let $a, b \in G$ then $\bar{a}^1, \bar{b}^1, aob, \bar{b}^1 o \bar{a}^1$ all belong to G.

now, $(\bar{b}^1 o \bar{a}^1) o (aob)$

$= [\bar{b}^1 o (\bar{a}^1 oa)] ob$ (since 'o' is associative)

$= (\bar{b}^1 o e) ob$ (e being identity element)

$= \bar{b}^1 ob$

$= e$.

and $(aob) o (\bar{b}^1 o \bar{a}^1)$

$= [a o (bo\bar{b}^1)] o \bar{a}^1$ [since 'o' is associative]

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

$\therefore$ we get

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

now from defination of inverse we have

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

8 (1) If each element in a group be its own inverse then prove that the group is abelian or commutative.

proof:- Let $(G, \circ)$ be a group and $a, b \in G$.

By condition $a = a^{-1}$ and $b = b^{-1}$

Since $(G, \circ)$ be a group so $a \circ b \in G$ [from closure property]

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

we know that $(a \circ b)^{-1} = b^{-1} \circ a^{-1} \quad \forall a, b \in G$.

$= b \circ a$ (since $b^{-1} = b$ and $a^{-1} = a$)

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

$\therefore a \circ b = b \circ a \quad \forall a, b \in G$.

this shows that $(G, \circ)$ be an abelian group.

(2) prove that a group $(G, \circ)$ is abelian if and only if $(a \circ b)^{-1} = a^{-1} \circ b^{-1} \quad \forall a, b \in G$.

proof:- let us assume that $(G, \circ)$ is an abelian group.

Then $\forall a, b \in G$; $a \circ b = b \circ a$ holds.

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

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

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

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

taking inverse both side we get

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

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

$\forall a,b \in G$.

$\therefore (G,*)$ is abelian. (proved).

(3) Let $(G,*)$ be a group and a be an element of G. Define a mapping $\rho_a : G \to G$ by $\rho_a(x) = x*a$ where $x \in G$. prove that ρ_a is a bijection.

proof:- Let $x, y \in G$ Then $\rho_a(x) = x*a$ and $\rho_a(y) = y*a$ where $a \in G$.

now $\rho_a(x) = \rho_a(y)$

$\Rightarrow x*a = y*a$

$\Rightarrow x = y$ [by right cancellation law]

therefore $x \neq y \Rightarrow \rho_a(x) \neq \rho_a(y)$, proving that ρ_a is injective.

Let p be an arbitrary element in the codomain set G. Since $a \in G$ and $p \in G$, there exists a unique element y in G such that $y*a = p$.

therefore y is a pre-image of p; $\therefore \rho_a$ is surjective

$\therefore \rho_a$ is injective as well as surjective

$\Rightarrow \rho_a$ = bijective.