Dr.D Radhakrishna
Associate Professor of Mathematics
Vijaya College, RV Road, Bangalore-04

II SEMESTER GROUPS

Defn of a Group: A non-empty set X with an operation $*$ is a group if it satisfies (i) Closure axiom (ii) Associative axiom (iii) Identity axiom and (iv) Inverse axiom.

OR

Defn of a Group: An algebraic structure (X, $*$) is a group if it satisfies (i) Associative axiom (ii) Identity axiom and (iii) Inverse axiom.

Defn of a Semi-Group: A nonempty set X with an operation $*$ satisfying closure and associative axioms is a semigroup.

Abelian Group: A non-empty set X with an operation $*$ is an abelian group if it satisfies (i) Closure axiom (ii) Associative axiom (iii) Identity axiom (iv) Inverse axiom and (v) commutative axiom.

EX: 1. (N,+) is a semi-group but not a group.
2. (N,·) is a semi-group but not a group.
3. (Z,+) is an abelian group
4. (Z,·) is a semi-group but not a group.
5. (Q,+), (R,+), (C,+) are all abelian groups,
6. (Q,·), (R,·), (C,·) are semi-groups but not groups, these are groups by deleting 0 in the set.

Problems on Groups:

1. Prove that the set {2^n/n€Z} is a group w r t multiplication.

soln: Let G={2^n/n€Z}

closure axiom:

let 2^x, 2^y€G

$2^x\ 2^y=2^{x+y}$€G

Associative axiom:

let 2^x, 2^y, 2^z€G

$2^x(2^y\ 2^z)= 2^x(2^{y+z})=2^{x+y+z}$

$(2^x 2^y)\ 2^z=2^{x+y}2^z=2^{x+y+z}$

Identity axiom:

$1=2^0$ is identity in G

Inverse axiom:

$\forall 2^x$€G, then 2^{-x} is the inverse of 2^x.

therefore, (G,·) is a group.

2. Prove that the set {a+ $\sqrt{2}$b/a,b€R} is an abelian group w r t addition.

soln:

let G={a+ $\sqrt{2}$b/a,b€R}

closure axiom:

let $a_1+\sqrt{2}b_1$, $a_2+\sqrt{2}b_2$€G

$(a_1+\sqrt{2}b_1)+(a_2+\sqrt{2}b_2)= a_1+a_2+\sqrt{2}\ (b_1+b_2)$ €G

Associative axiom:

$a_1+\sqrt{2}b_1,\ a_2+\sqrt{2}b_2,\ a_3+\sqrt{2}b_3$ €G

$a_1+\sqrt{2}b_1+(a_2+\sqrt{2}b_2+ a_3+\sqrt{2}b_3)= a_1+\sqrt{2}b_1+(a_2+ a_3+\sqrt{2}\ (b_2+b_3)$

$=a_1+a_2+a_3+\sqrt{2}(b_1+b_2+b_3)$ €G

$(a_1+\sqrt{2}b_1+ a_2+\sqrt{2}b_2)+(a_3+\sqrt{2}b_3)= (a_2+ a_2+\sqrt{2}\ (b_1+b_2)+ (a_3+\sqrt{2}b_3)$

$= a_1+a_2+a_3+\sqrt{2}(b_1+b_2+b_3)$ €G

Identity axiom:

$0=0+\sqrt{2}\ 0$ is identity in G

Inverse axiom:

for every $a+\sqrt{2}b$€G, $-a-\sqrt{2}b$€G is the inverse of $a+\sqrt{2}b$€G

commutative axiom:

let $a_1+\sqrt{2}b_1$, $a_2+\sqrt{2}b_2$€G

$(a_1+\sqrt{2}b_1)+ (a_2+\sqrt{2}b_2)=a_1+a_2+\sqrt{2}(b_1+b_2) = a_2+a_1+\sqrt{2}(b_2+b_1)= (a_2+\sqrt{2}b_2)+ (a_1+\sqrt{2}b_1)$

therefore, (G,+) is an abelian group.

3. Prove that the set of matrices in the form $\left\{\begin{bmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{bmatrix} / \theta\in R\right\}$ is group w r t matrix multiplication.

soln: let M= $\left\{\begin{bmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{bmatrix} / \theta\in R\right\}$

closure axiom:

let A= $\begin{bmatrix}\cos\theta_1 & \sin\theta_1\\ -\sin\theta_1 & \cos\theta_1\end{bmatrix}$, B= $\begin{bmatrix}\cos\theta_2 & \sin\theta_2\\ -\sin\theta_2 & \cos\theta_2\end{bmatrix}$€M now, $AB=\begin{bmatrix}\cos\theta_1 & \sin\theta_1\\ -\sin\theta_1 & \cos\theta_1\end{bmatrix}\begin{bmatrix}\cos\theta_2 & \sin\theta_2\\ -\sin\theta_2 & \cos\theta_2\end{bmatrix}=$

$$\begin{bmatrix}\cos\theta_1\cos\theta_2-\sin\theta_1\sin\theta_2 & \sin\theta_1\cos\theta_2+\cos\theta_1\sin\theta_2\\ -\sin\theta_1\cos\theta_2-\cos\theta_1\sin\theta_2 & \cos\theta_1\cos\theta_2-\sin\theta_1\sin\theta_2\end{bmatrix}=$$

$$\begin{bmatrix}\cos(\theta_1+\theta_2) & \sin(\theta_1+\theta_2)\\ -\sin(\theta_1+\theta_2) & \cos(\theta_1+\theta_2)\end{bmatrix}$$ €M

Associative axiom:

let $A=\begin{bmatrix}\cos\theta_1 & \sin\theta_1\\ -\sin\theta_1 & \cos\theta_1\end{bmatrix}$, $B=\begin{bmatrix}\cos\theta_2 & \sin\theta_2\\ -\sin\theta_2 & \cos\theta_2\end{bmatrix}$, $C=\begin{bmatrix}\cos\theta_3 & \sin\theta_3\\ -\sin\theta_3 & \cos\theta_3\end{bmatrix}$€M

$$A(BC)=\begin{bmatrix}\cos\theta_1 & \sin\theta_1\\ -\sin\theta_1 & \cos\theta_1\end{bmatrix}\begin{bmatrix}\cos(\theta_2+\theta_3) & \sin(\theta_2+\theta_3)\\ -\sin(\theta_2+\theta_3) & \cos(\theta_2+\theta_3)\end{bmatrix}=$$

$$\begin{bmatrix}\cos(\theta_1+\theta_2+\theta_3) & \sin(\theta_1+\theta_2+\theta_3)\\ -\sin(\theta_1+\theta_2+\theta_3) & \cos(\theta_1+\theta_2+\theta_3)\end{bmatrix}=(AB)C$$

Identity axiom:

$$\begin{bmatrix}\cos 0 & \sin 0\\ -\sin 0 & \cos 0\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\in M$$ is an identity element

Inverse axiom:

let $A=\begin{bmatrix}\cos\theta_1 & \sin\theta_1\\ -\sin\theta_1 & \cos\theta_1\end{bmatrix}$€M

$A^{-1}=\frac{\text{adj}A}{|A|}=\begin{bmatrix}\cos(\theta_1) & -\sin(\theta_1)\\ \sin(\theta_1) & \cos(\theta_1)\end{bmatrix}=\begin{bmatrix}\cos(-\theta_1) & \sin(-\theta_1)\\ -\sin(-\theta_1) & \cos(-\theta_1)\end{bmatrix}$€M

therefore, M is a group w r t matrix multiplication.

4. Prove that the set of complex numbers of the form {cosϴ+i sinϴ/ϴ€R} is a group w r t multiplication.

soln: let C={cosϴ+i sinϴ/ϴ€R}

closure axiom:

let $\cos\theta_1+i\sin\theta_1$, $\cos\theta_2+i\sin\theta_2$€C

$(\cos\theta_1+i\sin\theta_1)(\cos\theta_2+i\sin\theta_2)=\cos(\theta_1+\theta_2)+i\sin(\theta_1+\theta_2)$€C, **using Demoivrs' thm.**

Associative axiom:

let $\cos\theta_1+i\sin\theta_1$, $\cos\theta_2+i\sin\theta_2$, $\cos\theta_3+i\sin\theta_3$€C

$[(\cos\Theta_1+i\sin\Theta_1)(\cos\Theta_2+i\sin\Theta_2)](\cos\Theta_3+i\sin\Theta_3)$

$= [\cos(\Theta_1+\Theta_2)+i\sin(\Theta_1+\Theta_2)](\cos\Theta_3+i\sin\Theta_3)= \cos(\Theta_1+\Theta_2+\Theta_3)+i\sin(\Theta_1+\Theta_2+\Theta_3)$

also, $(\cos\Theta_1+i\sin\Theta_1)[(\cos\Theta_2+i\sin\Theta_2)(\cos\Theta_3+i\sin\Theta_3)]$

$= (\cos\Theta_1+i\sin\Theta_1)[\cos(\Theta_2+\Theta_3)+i\sin(\Theta_2+\Theta_3)]= \cos(\Theta_1+\Theta_2+\Theta_3)+i\sin(\Theta_1+\Theta_2+\Theta_3)$

Identity axiom:

1=cos0+isin0€M is identity

Inverse axiom:

for every cosΘ+i sinΘ€M

inverse is cos(-Θ)+i sin(-Θ)€M

therefore, C is a group w r t matrix multiplication.

5. Prove that the set of integers Z is an abelian group w r t ∗ defined by a∗b=a+b+3,∀a,b€Z

soln:

closure axiom:

let a,b€Z, a∗b=a+b+3€Z

Associative axiom:

let a,b,c€Z

a∗(b∗c)=a∗(b+c+3)=a+b+c+3+3=a+b+c+6

(a∗b)∗c=(a+b+3) ∗c =a+b+3+c+3=a+b+c+6

Identity axiom:

∀a€Z and e be identity

then by identity axiom a∗e=a

a+e+3=a

e+3=0

e=-3€Z is identity

Inverse axiom:

∀a€Z, let a^{-1} be the inverse of a

by inverse axiom

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

$a+a^{-1}+3=-3$

$a^{-1}=-6-a$€Z

commutative axiom:

a∗b=a+b+3=b+a+3=b∗a

therefore, (Z, ∗) is an abelian group.

6. Prove that the set Q_{-1} of rational numbers other than'-1' is an abelian group

w r t ∗ defined by a∗b=a+b+ab,∀a,b€Q_{-1}

soln:

closure axiom:

let a,b€Q_{-1}, a∗b=a+b+ab€Q_{-1}

Associative axiom:

let a,b,c€Q_{-1}

a∗(b∗c)=a∗(b+c+bc)=a+b+c+bc+a(b+c+bc)=a+b+c+bc+ab+ac+abc

(a∗b)∗c=(a+b+ab) ∗c =a+b+ab+c+(a+b+ab)c=a+b+c+ab+ac+bc+abc

Identity axiom:

∀a€Z and e be identity

then by identity axiom a∗e=a

a+e+ae=a

e+ae=0

e(1+a)=0

e=0€Q_{-1} is identity, because a≠-1

Inverse axiom:

∀a€ Q_{-1}, let a^{-1} be the inverse of a

by inverse axiom

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

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

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

$a^{-1}=\frac{-a}{1+a}$ €Q_{-1}

commutative axiom:

a∗b=a+b+ab=b+a+ba=b∗a

therefore, (Q_{-1}, ∗) is an abelian group.

Assignments:

1. Prove that the set of complex numbers {x+iy/x,y€R} is a group under addition.
2. Prove that the set of even integers is an abelian group under addition.

let G={2n/n€}

(G,+)

3. Prove that the set of integers Z is a group w r t ∗ defined by a∗b=a+b+1∀a,b€Z is an abelian group.

let a,b,c**€**

a∗(b∗ c)=a∗(b+c+1)=a+b+c+1+1=a+b+c+2

let a€Z and e be identity

by identity axiom

$a*e=a$

$a+e+1=a$

$e+1=0$

$e=-1$ €Z is identity

let a€Z and $e=-1$ be identity

let a^{-1} be inverse of a

by inverse axiom

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

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

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

$a^{-1}=-2-a$€Z

commutative axiom

$a*b=a+b+1=b+a+1=b*a$

$(Z, *)$ is an abelian group

4. Prove that the set Q_1 of rational numbers other than 1 is an abelian group w r t $*$ defined by $a*b=a+b-ab,\forall a,b$€Q_1

5. Prove that the set of positive rationals Q_+ is a group w r t $*$ defined by $a*b=\frac{ab}{5}$ $\forall a,b$€ Q_+ is a group.

let a,b,c€ Q_+

$$a*(b*c)=a*\frac{bc}{5}=\frac{a\frac{bc}{5}}{5}=\frac{abc}{25}$$

Identity axiom:

let a€Q_+ and e be identity

by identity axiom

$a*e=a$

$\frac{ae}{5}=a$

$e=5$€Q_+

Inverse axiom

let a€Q_+ and $e=5$ is identity

let a^{-1} be inverse of a

by inverse axiom

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

$\frac{aa^{-1}}{5}=5$

$a^{-1}=\frac{25}{a}$

$a*b=\frac{ab}{5}=\frac{ba}{5}= b*a$

Properties of Group

Thm1: Identity element in a group is unique.

Proof:

Let (G, ∗) be the group

If possible, let e & d be two identity elements in G

let a€G is arbitrary, then by identity axiom

a∗e=e∗a=a-----(1)

a∗d=d∗a=a-----(2)

from (1)and (2)

e=d

thus, identity element in G is unique.

Thm2: Inverse of an element in a group is unique.

Proof:

Let (G, ∗) be the group and e be identity.

let a€G is arbitrary.

If possible, let b and c by two inverses of a

then, by inverse axiom,

a∗b= b∗a= e-------(1)

also,

a∗c= c∗a= e-------(2)

now, b=b∗e

b=b∗(a∗c), using (2)

b= (b∗a)∗c, by associative axiom

b=e∗c, using (1)

b=c

Thm3: Inverse of an inverse element is an element itself.

Proof:

Let (G, $*$) be the group and e be identity.

let a€G is arbitrary, then its inverse exist denoted by a^{-1}.

let $a^{-1}=x$

by inverse axiom,

$a*x=x*a=e$

a and x are inverses to each other

therefore, $a=x^{-1}$

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

Thm4:In a group (G, $*$), $(a*b)^{-1}=b^{-1}*a^{-1}$, ∀a,b€G.

Proof:

Let (G, $*$) be the group and e be identity.

∀a,b€G, consider

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

also,

$(b^{-1}*a^{-1})*(a*b)= b^{-1}*(a^{-1}*a)*b=b^{-1}*e*b= b^{-1}*b=e$-----(2)

from (1) and (2), $a*b$ and $b^{-1}*a^{-1}$ are inverses to each other

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

note: this property can be extended to more than two elements

i.e $(a*b*c*d)^{-1}=d^{-1}*c^{-1}*b^{-1}*a^{-1}$

Thm5:In a group (G, $*$), (i) if $a*b=a*c$, then b=c(left cancellation)
(ii) if $b*c=a*c$, then b=a,(right cancellation) ∀a,b,c€G.

Proof:

(i) consider, $a*b=a*c$

pre operating a^{-1}, we get

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

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

$e*b=e*c$

$b=c$

(ii) consider, $b*c=a*c$

post operating c^{-1}, we get

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

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

$b*e=a*e$

$b=a$

Thm6:In a group (G, $*$), the equation $x*a=b$, ∀a,b€G has unique solution.

Proof:

consider, $x*a=b$-----(1)

post operate a^{-1} both the sides

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

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

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

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

$x= b*a^{-1}$ is the solution in G

To show the solution is not unique, let x_1 and x_2 be two solutions of (1)

therefore, $x_1*a=b$ and $x_2*a=b$

then, $x_1*a= x_2*a$

$x_1=x_2$ by right cancellation law

continuation of problems on groups(finite groups):

1. Prove that the set of cube roots of unity is an abelian group under multiplication.

soln:

let **G={1,ω,ω²}** be the cube roots of unity.

[where $\omega=\frac{-1+i\sqrt{3}}{2}$, $\omega^2=\frac{-1-i\sqrt{3}}{2}$ such that $\omega^3=1$ and $1+\omega+\omega^2=0$]

construct the composition table

.	**1**	**ω**	**ω²**
1	**1**	**ω**	**ω²**
ω	**ω**	**ω²**	1
ω²	**ω²**	1	**ω**

1. closure axiom: All the elements in the table are in set G.

2. Associative axiom: $1\ (\omega\ \omega^2)=1.1=1$

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

3. Identity axiom: 1 is identity element in G

4. Inverse axiom: $1^{-1}=1$, $\omega^{-1}= \omega^2$, $(\omega^2)^{-1}= \omega$

5. commutative axiom: the table is symmetric about the diagonal elements

therefore, (G, .) is an abelian group.

2. Prove that the set of fourth roots of unity is an abelian group under multiplication.

soln:

let **G={1,-1,i,-i}** be the fourth roots of unity.

construct the composition table

.	**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 axiom: All the elements in the table are in set G.
2. Associative axiom: 1 (i . -i)=1.1=1

   (1. i) -i= i. -i=1

3. Identity axiom: 1 is identity element in G
4. Inverse axiom: 1^{-1}=1, -1^{-1}=1, $(i)^{-1}$= -i, $(-i)^{-1}$= i
5. commutative axiom: the table is symmetric about the diagonal elements

therefore, (G, .) is an abelian group.

1. Prove that the set of integers Z is an abelian group under addition modulo4.

soln:

let **G={0,1,2,3}** be the set of integers modulo4

construct the composition table

$\oplus_4$	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

1. closure axiom: All the elements in the table are in set G.
2. Associative axiom: $1 \oplus_4 (2 \oplus_4 3)= 1 \oplus_4 1=2$

   $(1 \oplus_4 2) \oplus_4 3= 3 \oplus_4 3=3$

3. Identity axiom: 0 is identity element in G
4. Inverse axiom: 0^{-1}=0, 1^{-1}=3, 2^{-1}= 2, 3^{-1}= 1
5. commutative axiom: the table is symmetric about the diagonal elements

therefore, (G, $\oplus_4$) is an abelian group.

2. Prove that the set of integers Z is an abelian group under addition modulo6.

soln:

let **G={0,1,2,3,4,5}** be the set of integers modulo6

.

construct the composition table

$\oplus_6$	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

1. closure axiom: All the elements in the table are in set G.
2. Associative axiom: $1 \oplus_6 (4 \oplus_6 5) = 1 \oplus_4 3 = 4$

$$(1 \oplus_6 4) \oplus_6 5 = 5 \oplus_4 5 = 4$$

3. Identity axiom: 0 is identity element in G
4. Inverse axiom: $0^{-1}=0$, $1^{-1}=5$, $2^{-1}= 4$, $3^{-1}= 3$, $4^{-1}=2$, $5^{-1}=1$
5. commutative axiom: the table is symmetric about the diagonal elements

therefore, (G, $\oplus_6$) is an abelian group.

3. Prove that the set of non-zero integers Z is an abelian group under multiplication modulo7.

soln:

let **G={1,2,3,4,5,6}** be the set of non-zero integers modulo7

construct the composition table

$\otimes_7$	**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

1. closure axiom: All the elements in the table are in set G.
2. Associative axiom: $1 \otimes_7 (4 \otimes_7 5) = 1 \otimes_7 6 = 6$

$$(1 \otimes_7 4) \otimes_7 5 = 4 \otimes_7 5 = 6$$

3. Identity axiom: 1 is identity element in G
4. Inverse axiom: $1^{-1}=1$, $2^{-1}=4$, $3^{-1}= 5$, $4^{-1}= 2$, $5^{-1}=3$, $6^{-1}=6$
5. commutative axiom: the table is symmetric about the diagonal elements

therefore, (G, $\otimes_7$) is an abelian group.

4. Prove that the set of non-zero integers Z is an abelian group under multiplication modulo5.

5. Prove that the set {2,4,6,8} multiplication modulo10.

soln:

let **G={2,4,6,8}**

construct the composition table

$\otimes_{10}$	**2**	**4**	**6**	**8**
2	2	4	6	8
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

1. closure axiom: All the elements in the table are in set G.
2. Associative axiom: $2 \otimes_{10} (4 \otimes_{10} 6) = 2 \otimes_{10} 4 = 8$

   $(2 \otimes_{10} 4) \otimes_{10} 6 = 8 \otimes_{10} 6 = 8$
3. Identity axiom: 1 is identity element in G
4. Inverse axiom: $2^{-1}=8$, $4^{-1}=4$, $6^{-1}= 6$, $8^{-1}= 2$
5. commutative axiom: the table is symmetric about the diagonal elements

therefore, (G, $\otimes_{10}$) is an abelian group.

6. Prove that the set {1, 5,7,11} multiplication modulo12.

soln:

let **G={1, 5,7,11}**

construct the composition table

$\otimes_{12}$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

1. closure axiom: All the elements in the table are in set G.
2. Associative axiom: $5 \otimes_{12} (7 \otimes_{12} 11) = 5 \otimes_{12} 5 = 1$

   $(5 \otimes_{12} 7) \otimes_{12} 11 = 11 \otimes_{12} 11 = 1$
3. Identity axiom: 1 is identity element in G
4. Inverse axiom: $1^{-1}=1$, $5^{-1}=5$, $7^{-1}= 7$, $11^{-1}= 11$
5. commutative axiom: the table is symmetric about the diagonal elements

therefore, (G, $\otimes_{12}$) is an abelian group.

Assignments:

1. Prove that the square roots of unity is an abelian group under multiplication.

1. Prove that the set of integers Z is an abelian group under addition modulo7.

2. Prove that the set {1, 3,4,5,9} multiplication modulo11.

3. Prove that the set $\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$ **form a group under matrix multiplication.**