

(a) If possible, let there be two identity elements  $e$  and  $e'$  in  $(S, \cdot)$ . Hence  $eoe' = e'oe = e'$ , since  $e$  is an identity element and  $e' \in S$ . Again  $e'oe = eoe' = e$ , since  $e'$  is an identity element and  $e \in S$ . Therefore  $e = e'$ , that is, the identity element of a groupoid is unique.

(b) Let  $M_2 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ , where  $a, b, c, d \in \mathbb{R}$ .

We know that the matrix sum of two real matrices is a real matrix of the same order.

Also the matrix addition is associative.

Hence  $\{M_2, +\}$  is a semi-group.

Similarly, it can be shown that  $\{M_2, \cdot\}$  is a semi-group.

Ex. 2. Show that the set of cube roots of unity is a finite abelian group with respect to multiplication. [B.H. 2001]

The set of cube roots of unity is  $S = \{1, \omega, \omega^2\}$ .

(i) Closure axiom is satisfied, since

$$1 \cdot \omega = \omega, \quad \omega \cdot \omega^2 = 1, \quad \omega^2 \cdot 1 = \omega^2.$$

(ii) Associative axiom is satisfied, since

$$(1 \cdot \omega) \cdot \omega^2 = 1 \cdot (\omega \cdot \omega^2), \text{ etc.}$$

(iii) Identity axiom is satisfied, since

$$1 \cdot \omega = \omega, \quad 1 \cdot \omega^2 = \omega^2, \quad 1 \cdot 1 = 1. \quad 1 \text{ is the identity element}$$

(iv) Inverse axiom is satisfied, since

$$1 \cdot 1 = 1 = \omega \cdot \omega^2 = \omega^2 \cdot \omega$$

(inverse of each element exists in the set).

(v) Commutative property is satisfied, since

$$1 \cdot \omega = \omega \cdot 1, \quad \omega \cdot \omega^2 = \omega^2 \cdot \omega, \text{ etc.}$$

Moreover the number of elements of  $S$  is finite.

Hence the set  $S$  forms a finite abelian group with respect to multiplication.

Ex. 3. Check the following multiplication table for the set of fourth roots of unity, namely  $\{1, -1, i, -i\}$  for its group properties:

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

[B.H. 1983; C.H. 1994]

We see from the composition table that

(i) the closure property holds, since

$$1 \times 1 = 1, \quad -1 \times i = -i, \quad i \times (-i) = 1, \text{ etc.}$$

(ii) the operation is associative, since

$$(1 \times i) \times (-i) = 1 \times [i \times (-i)] = 1, \text{ etc.}$$

(iii) the set has 1 as the identity element with respect to the given operation, since  $1 \times (-1) = -1$ ,  $1 \times i = i$ ,  $1 \times (-i) = -i$ , etc.;

(iv) each element has an inverse, since

$$1 \times 1 = 1, \quad (-1) \times (-1) = 1, \quad -i \times i = 1, \quad i \times (-i) = 1, \text{ etc.}$$

Hence the set forms a multiplicative group. The set is commutative with respect to multiplication; for,  $1 \times (-1) = (-1) \times 1$ ,  $(-1) \times i = i \times (-1)$ , etc.

Hence it forms an abelian group.

Note. It is seen that a group is commutative, if the composition table with the corresponding operation has a symmetry across its leading diagonal.

Ex. 4. If  $a$  be an element of a multiplicative group with identity element  $e$  and  $a^2 = a$ , then show that  $a = e$ .

Since  $a$  is an element of the group, it has its inverse, say  $a^{-1}$ , in the group.

Operating both sides of the given equation by  $a^{-1}$  on the right, we have

$$(a^2)a^{-1} = aa^{-1}$$

that is,

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

or,

$$a(aa^{-1}) = e, \text{ the identity element}$$

or,

$$ae = e, \text{ which gives } a = e, \text{ since } a^2 = a.$$

(d) Prove that the set  $R \times R$  together with the operation  $\circ$  defined by  $(a, b) \circ (c, d) = (a + c, b + d + 2bd)$  is a commutative semi-group with identity. [N.B.H. 2002]

3. Prove that the set of even integers (including zero) forms an additive group.

Show further that the group is abelian. If the set be of odd integers, then prove that it does not form a group with respect to the composition addition.

4. (a) Show that the set of all rational numbers does not form a group with respect to multiplication. [C.H. 1983]

[It does not contain the inverse of 0.]

(b) If, in a group  $G$ ,  $x^2 = e$  (identity) for every  $x \in G$ , then prove that  $G$  is abelian. [K.H. 1990]

5. Show that the set of all non-zero integers does not form a group with the binary operations multiplication and subtraction.

6. Show that the set  $S = \{-1, 0, 1\}$  does not form a group with respect to operations addition and multiplication, while the set  $T = \{-1, 1\}$  is an abelian group under multiplication and does not form a group under addition.

7. Show that the set  $S = \{-3, -2, -1, 0, 1, 2, 3\}$  is not a group with the operation addition.

8. Show that the set of positive integers does not form a group under the composition addition and the set of negative integers does not form a group with addition and multiplication.

9. Show that the set of non-zero complex numbers forms a group with respect to multiplication. Show that the set of non-zero complex numbers with unity element, then show that

is an abelian group under [B.H. 1985]

$0, 1, 2, \dots, (n-1)$ .

$e^{\frac{2\pi ir}{n}}$  is  $e^{\frac{2\pi i(n-r)}{n}}$ .



## Examples III (A)

1. (a) Satisfy yourself that

- (i) in the groupoid  $(I, \cdot)$ , 1 is both left and right identity element.
- (ii)  $(R, +)$  is a semi-group, where  $R$  is the set of all real numbers.
- (iii) the system  $S = (Z, o)$ , where  $aob = a + b + ab$ , for all  $a, b \in Z$ , is a monoid.

(iv) the set of even integers forms a semi-group under the composition multiplication but does not form a monoid.

(v) the systems  $(M_2, +)$  and  $(M_2, \cdot)$  are monoids, where  $M_2$  denotes the set of all real  $2 \times 2$  matrices;  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  is the identity of the former and  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  is that of the latter.

(vi) the power set  $P(S)$  is a monoid with respect to the composition  $A \circ B = A \cap B$  and  $A \cup B$ .

[K.H. 1977]

(b) If  $M$  be the set of all real matrices  $\left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} ; a+b \neq 0 \right\}$ , then

show that  $(M, \cdot)$  is a semi-group, where  $\cdot$  denotes matrix multiplication.

Show further that it has no left identity and  $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$  is the right identity.

2. (a) Show that the set of all real numbers is a groupoid but not a semi-group under the operation  $o$  defined by

$$aob = a + 3b \quad \forall a, b \in R.$$

But, if the binary operation  $o$  be defined by

$$aob = b \quad \forall a, b \in R,$$

then the set of real numbers forms a semi-group.

(b) Show that a quasi-group, in which the associative property holds is a group. [K.H. 1980]

(c) If  $(S, o)$  be a semi-group and  $a \in S$ , then prove that

$$a^{m+n} = a^m o a^n, \text{ for all } m, n \in N.$$

## GROUP THEORY

(d) Prove that the set  $R \times R$  together by  $(a, b) o (c, d) = (a + c, b + d + 2bd)$  is a commutative identity.

3. Prove that the set of even integers (including 0) forms a group.

Show further that the group is abelian. If  $G$  is a group, prove that it does not form a group with respect to addition.

4. (a) Show that the set of all rational numbers forms a group with respect to multiplication.

[It does not contain the inverse of 0.]

(b) If, in a group  $G$ ,  $x^2 = e$  (identity), then  $G$  is abelian.

5. Show that the set of all non-zero integers forms a group under the binary operations multiplication and addition.

6. Show that the set  $S = \{-1, 0, 1\}$  does not form a group under operations addition and multiplication. Show that the set of non-zero integers forms an abelian group under multiplication and addition.

7. Show that the set  $S = \{-3, -2, -1, 0\}$  does not form a group under operation addition.

8. Show that the set of positive integers does not form a group under composition addition and the set of non-zero integers forms a group with addition and multiplication.

9. Show that the set of non-zero real numbers forms a group under multiplication. Show that this is also true for complex numbers.

10. If  $G = \{0\}$  be a singleton with 0 as identity, show that it forms a group with additive property.

11. Show that the  $n$ -th roots of unity form a group under ordinary multiplication.

[By De Moivre's theorem,  $1^n = e^{2\pi i n} = 1$ ]

Identity element is  $e^{2\pi i n} = 1$  and inverse of  $a$  is  $a^{-1}$ .

Examples III (A)

self that  
poid  $(I, \cdot)$ , 1 is both left and right identity element.  
semi-group, where  $R$  is the set of all real numbers.  
 $S = (Z, \circ)$ , where  $a \circ b = a + b + ab$ , for all  $a, b \in Z$  is

even integers forms a semi-group under the  
on but does not form a monoid.

$(M_2, +)$  and  $(M_2, \cdot)$  are monoids, where  $M_2$   
 $2 \times 2$  matrices;  $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$  is the identity of the  
of the latter.

$S$  is a monoid with respect to the composition  
and  $A \circ B = A \cup B$ .

real matrices  $\left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix}; a+b \neq 0 \right\}$ , then  
[K.H. 1977]

up, where  $\cdot$  denotes matrix multiplication.

identity and  $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$  is the right identity.

all real numbers is a groupoid but not a  
o defined by

R.  
be defined by

a semi-group.

in which the associative property holds,  
[K.H. 1990]

d  $a \in S$ , then prove that  
 $m, n \in N$ .

(d) Prove that the set  $R \times R$  together with the operation  $\circ$  defined  
by  $(a, b) \circ (c, d) = (a+c, b+d+2bd)$  is a commutative semi-group with  
identity. [N.B.H. 2002]

3. Prove that the set of even integers (including zero) forms an additive  
group.

Show further that the group is abelian. If the set be of odd integers, then  
prove that it does not form a group with respect to the composition addition.

4. (a) Show that the set of all rational numbers does not form a group  
with respect to multiplication. [C.H. 1983]

[It does not contain the inverse of 0.]

(b) If, in a group  $G$ ,  $x^2 = e$  (identity) for every  $x \in G$ , then prove that  
 $G$  is abelian. [K.H. 1990]

5. Show that the set of all non-zero integers does not form a group with  
the binary operations multiplication and subtraction.

6. Show that the set  $S = \{-1, 0, 1\}$  does not form a group with respect to  
operations addition and multiplication, while the set  $T = \{-1, 1\}$  is an  
abelian group under multiplication and does not form a group under  
addition.

7. Show that the set  $S = \{-3, -2, -1, 0, 1, 2, 3\}$  is not a group with the  
operation addition.

8. Show that the set of positive integers does not form a group under the  
composition addition and the set of negative integers does not form a  
group with addition and multiplication.

9. Show that the set of non-zero real numbers forms a group with respect  
to multiplication. Show that this is also true for a set of non-zero complex  
numbers.

10. If  $G = \{0\}$  be a singleton with 0 as its unity element, then show that  
it forms a group with additive property.

11. Show that the  $n$ -th roots of unity form an abelian group under  
ordinary multiplication. [B.H. 1985]

[By De Moivre's theorem,  $1^n = e^{\frac{2\pi i r}{n}}$ , where  $r = 0, 1, 2, \dots, (n-1)$ .

Identity element is  $e^{\frac{2\pi i 0}{n}} = 1$  and inverse of  $e^{\frac{2\pi i r}{n}}$  is  $e^{\frac{2\pi i (n-r)}{n}}$ .]

is  
even  
Pho



12. Prove that the set of all  $m \times n$  matrices having their elements as integers (rationals, reals) is an infinite abelian group with matrix addition as composition.

13. (a) Prove that the set of all  $2 \times 2$  non-singular matrices  $M_2$  having their elements as real numbers is a non-abelian group with matrix multiplication as composition.

Show further that if some elements of  $M_2$  be non-singular, then  $\{M_2, \cdot\}$  is not a quasi-group, where  $\cdot$  denotes matrix multiplication.

(b) Show that the set  $M$  of all  $2 \times 2$  matrices  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ , where  $a, b, c, d$  are integers and  $ad - bc = 1$ , is a non-commutative group with respect to matrix multiplication.

14. (a) Show that the set  $\{a + \sqrt{2}b : a, b \in Q\}$ , where  $Q$  is the set of rational numbers, forms a group under ordinary addition as composition. [C.H. 1993]

(b) On the set of integers  $Z$ , the binary operation  $*$  is defined as  $a * b = a + b - 2$ , for all  $a, b \in Z$ . Show that  $\langle Z, * \rangle$  is a group.

15. Show that the set

$$(i) \dots, 2^{-4}, 2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3, 2^4, \dots$$

forms a multiplicative group;

$$\text{and } (ii) \dots, -3m, -2m, -m, 0, m, 2m, 3m, \dots,$$

where  $m$  is a fixed integer, forms an additive group.

16. Show that in the first two composition tables, the underlying sets do not form groups because in the first there is no inverse of  $a$  and in the second there is no identity element; but the set of the third table forms a group with composition  $\circ$ .

$\times$	$a$	$b$	$c$
$a$	$a$	$a$	$a$
$b$	$a$	$b$	$c$
$c$	$a$	$c$	$b$

$\cdot$	$a$	$b$	$c$	$d$
$a$	$c$	$d$	$b$	$a$
$b$	$a$	$b$	$c$	$d$
$c$	$d$	$c$	$a$	$b$
$d$	$b$	$c$	$a$	$d$

$\circ$	$a$	$b$	$c$	$d$
$a$	$b$	$d$	$a$	$c$
$b$	$d$	$c$	$b$	$a$
$c$	$a$	$b$	$c$	$d$
$d$	$c$	$a$	$d$	$b$

17. Prove that the six matrices

$$\begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix}, \begin{bmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{bmatrix} \text{ for } \theta = 0, \frac{2}{3}\pi, \frac{4}{3}\pi$$

form a group with respect to usual matrix multiplication.

18. (a) Show that the set of matrices

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

where  $\alpha$  is a real number, form a group with respect to matrix multiplication.

(b) Prove that the set of all matrices  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  where  $a, b, c, d$  are integers and  $ad - bc = 1$  forms a group with respect to matrix multiplication.

(c) Show that the set of all matrices  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  where  $a, b, c, d$  are integers and  $ad - bc = 1$  forms a commutative group.

(d) Show that the set

$$M = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}$$

forms an abelian group under matrix multiplication.

(e) If  $G = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \text{ is an integer} \right\}$ , show that  $G$  forms a commutative group under matrix multiplication.

(f) Let  $G$  be the set of all  $2 \times 2$  matrices  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  where  $a, b, c, d$  are integers and  $ad - bc = 1$  and  $a, d$  are not zero simultaneously. Show that  $G$  forms a group with respect to multiplication.

(g) Show that the set of all matrices  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  where  $a, b, c, d$  are integers and  $ad - bc = 1$  forms a group with respect to multiplication.

19. (a) Show that the set  $Q$  of all rational numbers forms a group under the binary operation  $*$  defined by

$$a * b = a + b - a \cdot b$$

(b) In the set  $Q$  of rational numbers, show that  $(Q, *)$  has no identity element.

(c) Prove that the set  $Z_6$  of integers modulo 6 forms a group with respect to the composition  $*$  defined by

$$a * b = a + b - 3$$

set of all  $m \times n$  matrices having their elements as numbers is an infinite abelian group with matrix addition as composition.

if some elements of  $M_2$  be non-singular, then the set of all  $2 \times 2$  non-singular matrices  $M_2$  having their elements as numbers is a non-abelian group with matrix multiplication as composition.

if some elements of  $M_2$  be non-singular, then the set of all  $2 \times 2$  matrices  $M_2$  having their elements as numbers is a non-abelian group with matrix multiplication as composition.

if some elements of  $M_2$  be non-singular, then the set of all  $2 \times 2$  matrices  $M_2$  having their elements as numbers is a non-abelian group with matrix multiplication as composition.

$2, 2^2, 2^3, 2^4, \dots$

$m, 2m, 3m, \dots$

is an additive group.

composition tables, the underlying sets of the first two tables are the same, but the set of the third table forms a group.

$b$	$c$	$d$	$a$
$d$	$b$	$a$	$c$
$a$	$c$	$d$	$b$
$c$	$a$	$b$	$d$

matrix multiplication.

18. (a) Show that the set of matrices

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

where  $\alpha$  is a real number, forms a group under matrix multiplication.

(b) Prove that the set of all real orthogonal matrices of order  $n$  forms a group with respect to matrix multiplication. [B.H. 1993]

(c) Show that the set of all real matrices of the form  $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$ , where

$a \neq 0$ , forms a commutative group with respect to matrix multiplication.

(d) Show that the set

$$M = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\}$$

forms an abelian group under matrix multiplication.

[T.H. 2007]

(e) If  $G = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \text{ is any non-zero real number} \right\}$ , then show that

$G$  forms a commutative group under matrix multiplication.

(f) Let  $G$  be the set of all  $2 \times 2$  matrices  $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ , where  $a, b$  are real

numbers and are not zero simultaneously. Show that  $G$  is a group with respect to multiplication.

(g) Show that the set of all complex numbers  $z$  with  $|z| = 1$  is a group with respect to multiplication.

19. (a) Show that the set  $Q$  of all rational numbers, other than 1, forms a group under the binary operation  $*$  defined by

$$a * b = a + b - ab, \quad a, b \in Q.$$

(b) In the set  $Q$  of rational numbers, the operation  $*$  is defined by  $a * b = a - b + a \cdot b$ , where  $+$ ,  $\cdot$ ,  $-$  denote the usual operations in  $Q$ . Show that  $(Q, *)$  has no identity. [C.H. 1984]

(c) Prove that the set  $Z_0$  of all odd integers forms a group with respect to the composition  $*$  defined by

$$a * b = a + b - 3, \quad a, b \in Z_0.$$

[B.H. 2002]

4.6/ If in then prove photo



(d) Show that the set  $G$  of all ordered pairs  $(a, b)$  with  $a \neq 0$ , of rational numbers  $a, b$  is a group with operation  $*$  defined by

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

[Identity =  $(1, 0)$  and  $(a^{-1}, -ba^{-1})$  is the inverse of  $(a, b)$ .] [C.H. 1990, 1996]

20. Show that the set  $Q$  of all rational numbers, other than  $(-1)$ , forms a group under the binary operation  $*$  defined by

$$a * b = a + b + ab, \quad a, b \in Q.$$

With the same definition of the operation  $*$ , when  $a, b \in R$ , show that  $(R, *)$  is a monoid, but not a quasi-group.

21.  $*$  is a binary operation in  $Q$  defined by  $a * b = \frac{ab}{3}$ ,  $a, b \in Q$  (the set of all positive rational numbers). Show that  $(Q, *)$  is a commutative group.

[V.H. 1987; B.H. 1995; N.B.H. 2006]

22. Show that the positive rationals do not form a group  $G$  with respect to the binary operation  $*$  defined by  $x * y = \frac{x}{y}$ ,  $x, y \in G$ .

23. (a) If, in a group  $(G, o)$ , the elements  $a$  and  $b$  of  $G$  commute, then show that (i)  $a^{-1} o b^{-1} = b^{-1} o a^{-1}$ , (ii)  $a^{-1} o b = b o a^{-1}$ .

(b) Prove that the group  $(G, o)$  is abelian, if  $a, b \in G$ ,  $b^{-1} o a^{-1} o b o a = i$ , where  $i$  is the identity of the group.

(c) If  $G$  be a group with binary operation  $*$ , then show that  $(a * b^{-1} * c)^{-1} = c^{-1} * b * a^{-1}$ , for all  $a, b, c \in G$ .

(d) Prove that a group with four elements is necessarily abelian under any binary operation. [V.H. 1997]

(e) If the set  $\{1, x, y\}$  forms a multiplicative group, then show that  $(xy)^{-1} = xy$  and  $x^3 = y^3 = 1$ . [B.H. 1990]

24. Show that the set  $G = \{0, 1, 2, 3\}$  forms a group with respect to addition modulo 4; but it does not form a group under multiplication modulo 4 as some of the elements have no inverses.

25. Show that the set  $S = \{0, 1, 2, 3, 4, 5\}$  forms a finite abelian group under addition modulo 6.

Drop the element 0 from the set  $S$  and form the table for addition modulo 6. Verify that the set does not form a group for want of closure property.

Note. The above set is sometimes written as  $S = \{[0, 1, 2, 3, 4, 5], +_6\}$ .

## GROUP THEORY

26. Form the operation table  $S = \{1, 2, 3, 4, 5\}$  under multiplication modulo 5. Does it form a group under multiplication modulo 5?

Note. This set is sometimes written as  $S = \{1, 2, 3, 4, 5\}$ .

27. Show that the set  $S = \{0, 1, 2, 3, 4, 5\}$  modulo 5 and the set  $S = \{1, 2, 3, 4, 5\}$  modulo 7.

28. Show that the set of integers forms a group under multiplication modulo 12.

29. Show that the residue class modulo 5 forms a group with respect to addition modulo 5.

30. Show that the residue class modulo 5 forms a group with respect to multiplication modulo 5.

31. Show that the set  $I_n = \{0, 1, 2, \dots, n-1\}$  of integers forms a group under addition modulo  $n$ .

32. Show that, if  $p$  be a prime, the set  $I_p = \{1, 2, \dots, p-1\}$  of integers forms an abelian group under multiplication modulo  $p$ .

33. Show that the residue class modulo  $p$  forms an abelian group under multiplication modulo  $p$ .

34. Show that the non-zero residue class modulo  $p$  forms a group with multiplication of residue modulo  $p$ .

35. Show that the non-zero residue class modulo  $p$  forms a group under multiplication modulo  $p$ .

integer  $n$  do not form a group under multiplication modulo  $n$ .

3.8. Permutations.

Permutation of a non-empty finite set onto itself (a bijective mapping of the set of integers onto itself).

The symbol

$$p = \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}$$

means: replace 1 by  $a$ , 2 by  $b$ , 3 by  $c$ . That is, we get a one-one mapping of the set of integers onto itself. Such a symbol denotes permutation.



all ordered pairs  $(a, b)$  with  $a \neq 0$ , of rational numbers, other than  $(-1)$ , forms a group under  $*$  defined by  $(a, b) * (c, d) = (ac, bc + d)$ .  $(a, b)^{-1}$  is the inverse of  $(a, b)$ .

[C.H. 1990, 1996]

on  $*$  defined by  $ab, a, b \in \mathbb{Q}$ . The operation  $*$ , when  $a, b \in \mathbb{R}$ , show that  $(\mathbb{R}, *)$  is a group.

defined by  $a * b = \frac{ab}{3}$ ,  $a, b \in \mathbb{Q}$  (the set of rational numbers). Show that  $(\mathbb{Q}, *)$  is a commutative group.

[V.H. 1987; B.H. 1995; N.B.H. 2006]

do not form a group  $G$  with respect to  $*$  defined by  $x * y = \frac{x}{y}$ ,  $x, y \in G$ . Elements  $a$  and  $b$  of  $G$  commute, then  $(ii) a^{-1} \circ b = b \circ a^{-1}$ .

abelian, if  $a, b \in G$ ,  $b^{-1} \circ a^{-1} \circ b \circ a = i$ .

operation  $*$ , then show that for all  $a, b, c \in G$ .

elements is necessarily abelian under  $*$ .

[V.H. 1997]

multiplicative group, then show that  $(G, *)$  is a group.

[B.H. 1990]

forms a group with respect to addition under multiplication modulo 4 as

forms a finite abelian group under

form the table for addition modulo 6 for want of closure property.

as  $S = \{[0, 1, 2, 3, 4, 5], +6\}$ .

26. Form the operation table for the set  $S = \{1, 2, 3, 4, 5\}$  under multiplication modulo 6 and show that the set does not form a group under this operation.

Note. This set is sometimes written as  $S = \{[1, 2, 3, 4, 5], \times 6\}$ .

27. Show that the set  $S = \{0, 1, 2, 3, 4\}$  forms a group under addition modulo 5 and the set  $S = \{1, 2, 3, 4, 5, 6\}$  forms an abelian group under multiplication modulo 7.

28. Show that the set of integers  $\{1, 5, 7, 11\}$  forms a group under multiplication modulo 12.

29. Show that the residue classes modulo 4 do not form a group with respect to multiplication of residue classes. Show further that it forms a group with respect to addition of residue classes.

30. Show that the residue classes  $[1], [3], [5], [7]$  modulo 8 form a group with respect to multiplication of residue classes.

31. Show that the set  $I_n = \{0, 1, 2, \dots, (n-1)\}$  of first  $n$  non-negative integers forms a group under addition modulo  $n$ .

32. Show that, if  $p$  be a prime number, then the set

$$I_p = \{1, 2, \dots, (p-1)\}$$

forms an abelian group under multiplication modulo  $p$ .

33. Show that the residue classes modulo  $n$  form a finite group with respect to addition of residue classes.

34. Show that the non-zero residue classes modulo a prime  $p$  form a group with multiplication of residue classes.

35. Show that the non-zero residue classes modulo a composite integer  $n$  do not form a group under multiplication of residue classes.

### 3.8. Permutations.

Permutation of a non-empty finite set is defined to be a one-one mapping of a finite set onto itself (a bijective mapping). Let  $a, b, c, \dots, k$  be any arrangement of the set of integers  $1, 2, 3, \dots, n$ .

The symbol

$$p = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a & b & c & \dots & k \end{pmatrix}$$

means: replace 1 by  $a$ , 2 by  $b$ , 3 by  $c$ , etc. until finally  $n$  is replaced by  $k$ . That is, we get a one-one mapping of the finite set  $\{1, 2, 3, \dots, n\}$  onto itself. Such a symbol denotes permutation.

*Handwritten notes:*  
 (2) is eq  
 group  
 → photo  
 4.6 If in a  
 den prove the  
 photo



Ex. 5. Show that the following four matrices form a group under matrix multiplication:

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad D = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

We see that  $A$  is a unit matrix.

Hence  $AA = A$ ,  $AB = BA = B$ ,  $AC = CA = C$ ,  $AD = DA = D$ .

$$\text{Also } BC = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = D \text{ and } BD = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = C.$$

Similarly,  $CB = D$  and  $DB = C$ .

Again  $DC = CD = B$ .

Also  $BB = CC = DD = A$ .

Hence we find the composition table as

$\times$	$A$	$B$	$C$	$D$
$A$	$A$	$B$	$C$	$D$
$B$	$B$	$A$	$D$	$C$
$C$	$C$	$D$	$A$	$B$
$D$	$D$	$C$	$B$	$A$

The set of four matrices is thus closed with respect to matrix multiplication. The elements are associative for the operation.  $A$  is the identity element and every element is its own inverse as seen from the table. Thus the set of the four matrices forms a multiplicative group which is commutative as well.

Ex. 6. Show that if every element of a group  $(G, o)$  be its own inverse, then it is an abelian group. [B.H. 1987]

Is the converse true?

Let  $a, b \in G$ ; then  $a o b \in G$  (closure).

Hence, by the given condition, we have

$$\begin{aligned} a o b &= (a o b)^{-1} \\ &= b^{-1} o a^{-1} \\ &= b o a, \text{ since } a^{-1} = a \text{ and } b^{-1} = b. \end{aligned}$$

Thus  $a o b = b o a$ , for every  $a, b \in G$ .

Therefore it is an abelian group.



Ex. 5. Show that the following four matrices form a group under matrix multiplication:

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad D = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

We see that  $A$  is a unit matrix.

Hence  $AA = A$ ,  $AB = BA = B$ ,  $AC = CA = C$ ,  $AD = DA = D$ .

$$\text{Also } BC = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = D \text{ and } BD = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = C.$$

Similarly,  $CB = D$  and  $DB = C$ .

Again  $DC = CD = B$ .

Also  $BB = CC = DD = A$ .

Hence we find the composition table as

$\times$	$A$	$B$	$C$	$D$
$A$	$A$	$B$	$C$	$D$
$B$	$B$	$A$	$D$	$C$
$C$	$C$	$D$	$A$	$B$
$D$	$D$	$C$	$B$	$A$

The set of four matrices is thus closed with respect to matrix multiplication. The elements are associative for the operation.  $A$  is the identity element and every element is its own inverse as seen from the table. Thus the set of the four matrices forms a multiplicative group which is commutative as well.

Ex. 6. Show that if every element of a group  $(G, o)$  be its own inverse, then it is an abelian group. [B.H. 1987]

Is the converse true?

Let  $a, b \in G$ ; then  $a o b \in G$  (closure).

Hence, by the given condition, we have

$$\begin{aligned} a o b &= (a o b)^{-1} \\ &= b^{-1} o a^{-1} \\ &= b o a, \text{ since } a^{-1} = a \text{ and } b^{-1} = b. \end{aligned}$$

Thus  $a o b = b o a$ , for every  $a, b \in G$ .

Therefore it is an abelian group.