KHARAGPUR COLLEGE

DEPARTMENT OF MATHEMATICS

STUDY MATERIALS

SUBJECT: MATHEMATICS HONOURS

CLASS: B. Sc. Hons.

SEMESTER: 3 RD

PAPER: C6T [GROUP THEORY- I]

UNIT: I & II

Dr. Sangita Chakraborty

Associate Professor
Department of Mathematics
Kharagpur College

Email:
sangita@kharagpurcollege.ac.in

MTMH GROUP THEORY 1 3RD SEM Lecture #1.

S. Chakraborty

- **BINARY COMPOSITION :—**

A binary composition on a non-empty set A is a mapping '$\circ$' : $A \times A \to A$.

$\therefore$ To each ordered pair of elements $(a, b) \in A \times A$, '$\circ$' assigns a definite element $a \circ b \in A$.

i.e., A binary composition '$\circ$' is said to be defined on A if $a \circ b \in A$, $\forall\, a, b \in A$. A is said to be closed w.r.t. '$\circ$'.

- **EXAMPLES :—**

① The sets : $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \cdots$ are closed w.r.t. addition (+), subtraction (−), multiplication (·).

② The set $\mathbb{N}$ is closed w.r.t. '+' but not closed w.r.t. '−'. Because $a - b \notin \mathbb{N}$ for some $a, b \in \mathbb{N}$.

③ The set $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$ be the set of residue classes, $n \in \mathbb{Z}^+$.
$\mathbb{Z}_n$ is closed w.r.t. the b.c. $\oplus$, called addition modulo n, defined on $\mathbb{Z}_n$ by $\bar{a} \oplus \bar{b} = \overline{a+b}$.
Also, $\mathbb{Z}_n$ is closed w.r.t. the b.c. $\odot$, called multiplication modulo n, defined by $\bar{a} \odot \bar{b} = \overline{a.b}$, for $\bar{a}, \bar{b} \in \mathbb{Z}_n$.

④ The set $M_n(\mathbb{R})$ be the set of all $n \times n$ real matrices. The b.c. 'addition of matrices' and 'multiplication of matrices' both are defined on $M_n(\mathbb{R})$.

GROUPOID :— When on a non-empty set G on which a b.c. '$\circ$' is defined, $(G, \circ)$ becomes an algebraic system, called a groupoid.

SEMIGROUP :— A groupoid $(G, \circ)$ is said to be a semigroup if $a \circ (b \circ c) = (a \circ b) \circ c$, $\forall\, a, b, c \in G$. ('$\circ$' is associative)

MONOID :— A groupoid $(G, \circ)$ is said to be monoid if (i) $a \circ (b \circ c) = (a \circ b) \circ c$, $\forall\, a, b, c \in G$,
(ii) $\exists$ an element $e \in G$ s.t. $e \circ a = a \circ e = a$, $\forall\, a \in G$.
(e is the identity element in G).

Examples :

$(\mathbb{Z}, +)$ is a monoid, 0 being the identity element
$(\mathbb{Z}, \cdot)$ " " " , 1 " " " "
$(\mathbb{Z}_n, \odot)$ " " " , $\bar{1}$ " " " "

Some Definitions on Groupoid (G, o).

① Commutative groupoid → If the b.c. 'o' is commutative in a groupoid (G, o), i.e.,
$a o b = b o a$, $\forall\, a, b \in G$.

② Right identity (e_R) → if $a o e_R = a$, $\forall\, a \in G$
Left identity (e_L) → if $e_L o a = a$, $\forall\, a \in G$.
Identity element (e) exists in (G, o) if both e_R and e_L exist and $e_R = e_L = e$.
e is unique, if it exists.

③ Left inverse (a_L) → (G, o) contains e.
if $a_L o a = e$ for $a_L \in G$, $a \in G$.
Right inverse (a_R) → if $a o a_R = e$ for $a_R, a \in G$.
Invertible → a is invertible if both a_L and a_R exist and $a_L = a_R = a'$ (say).

④ In a monoid an invertible element is said to be a unit.

⑤ In a semigroup, an element x is said to be an idempotent element if $x o x = x$.

Examples:

① $(\mathbb{Z}, +)$ is a commutative groupoid, But $(\mathbb{Z}, -)$ is NOT "
② 0 is the identity element in $(\mathbb{Z}, +)$
0 is NOT " " in $(\mathbb{Z}, -)$, [as 0 is not the left identity]
③ 2 is not invertible in the monoid $(\mathbb{Z}, \cdot)$.
④ 2 is a unit in the monoid $(\mathbb{Q}, \cdot)$
⑤ 0, 1 are the idempotent elements in the semigroup/monoid $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$.
⑥ $\bar{0}, \bar{1}, \bar{3}, \bar{4}$ are the idempotent elements in the monoid $(\mathbb{Z}_6, \odot_6)$.

If (S, o) be a semigroup and $a \in S$.
Then $a^{m+n} = a^m o a^n$, $\forall m, n \in \mathbb{N}$.

$a^{m+n} = \underbrace{a o a o \cdots o a}_{(m+n) \text{ times}}$ [$\because a o (a o a) = (a o a) o a = a o a o a$]

$= (\underbrace{a o a o \cdots o a}_{m \text{ times}}) o (\underbrace{a o a o \cdots o a}_{n \text{ times}})$

$= a^m o a^n$.

Quasigroup → A groupoid (G, o) is said to be a quasigroup if for any two elements $a, b \in G$, each of the equations $a o x = b$ and $y o a = b$ has a unique solution in G.

Examples:

① $(\mathbb{Z}, +)$ is a groupoid. Let $a, b \in \mathbb{Z}$.
The equation $a + x = b$ has unique solution $x = b - a \in \mathbb{Z}$.
Also " " $y + a = b$ " " " " "

② $(\mathbb{Z}, -)$ is a groupoid. Let $a, b \in \mathbb{Z}$
The eqn $a - x = b$ has the unique soln $x = a - b \in \mathbb{Z}$.
" " $y - a = b$ " " " $y = a + b \in \mathbb{Z}$.
But it is not a semigroup.
∴ $(\mathbb{Z}, +)$ and $(\mathbb{Z}, -)$ are both quasigroups.

③ $(\mathbb{Z}, \cdot)$ is NOT a quasigroup, since the equation $2 \cdot x = 3$ has no solution in $\mathbb{Z}$.
[Because, $x = 3/2 \notin \mathbb{Z}$].

④ $(M_2(\mathbb{R}), \cdot)$ is a groupoid. The eqn $AX = B$, for $A, B \in M_2(\mathbb{R})$, has no solution in $M_2(\mathbb{R})$, if A is a singular matrix [$\det A = 0$].
∴ $(M_2(\mathbb{R}), \cdot)$ is NOT a quasigroup.

GROUP: A non-empty set G is said to form a group (G,o) w.r.t. a b.c. 'o' if

(i) $aob \in G, \forall a,b \in G$ [closure property]

(ii) $ao(boc) = (aob)oc, \forall a,b,c \in G$ [Associative "]

(iii) $\exists$ an element $e \in G$ s.t. $eoa = aoe, \forall a \in G$ [Identity(e) "]

(iv) For each $a \in G$, $\exists$ an element $a' \in G$ s.t. $a'oa = aoa' = e$ [Inverse "]

Commutative Group / Abelian Group:
A group (G,o) is said be an abelian group if $aob = boa, \forall a,b \in G$ [commutative property].

Properties of Groups:

① The identity element in a group (G,o) is unique.

→ If possible, let e and f be two identity elements in (G,o). Then $eoa = aoe = a$ & $foa = aof = a$ $\} \forall a \in G$.

$\therefore eof = e$, by the identity property of f.

& $eof = f$, " " " " " e.

$\Rightarrow e = f$ (Uniqueness property)

② In a group (G,o), each element has only one inverse.

→ Let a' and a'' be two inverses of $a \in G$.

Then, $a'oa = aoa' = e$ & $a''oa = aoa'' = e$ $\}$ e is the identity in (G,o).

Now, $(a'oa)oa'' = a'o(aoa'')$, by associative property

$\Rightarrow eoa'' = a'oe \Rightarrow a'' = a'$ [Uniqueness of Inverse]

③ In a group (G,o), cancellation laws hold.

→ Let $a,b,c \in G$, and let $aob = aoc$, $boa = coa$

$a \in G \Rightarrow \bar{a}^1 \in G$. Then $\bar{a}^1o(aob) = \bar{a}^1o(aoc)$

$\Rightarrow (\bar{a}^1oa)ob = (\bar{a}^1oa)oc$

$\Rightarrow eob = eoc \Rightarrow b = c$

$\therefore aob = aoc \Rightarrow b = c$ [Left cancellation]

Again, $boa = coa \Rightarrow (boa)o\bar{a}^1 = (coa)o\bar{a}^1$

$\Rightarrow bo(aoa^{-1}) = co(aoa^{-1})$

$\Rightarrow boe = coe$

$\Rightarrow b = c$ [Right cancellation]

④ In a group (G, o), each of the equations $a o x = b$, and $y o a = b$ has a unique solution in G, $\forall\, a, b \in G$.
Then (G, o) is also called a quasigroup.

$\longrightarrow \bar{a}^{1} o (a o x) = \bar{a}^{1} o b \Rightarrow (\bar{a}^{1} o a) o x = \bar{a}^{1} o b$
$\Rightarrow e o x = \bar{a}^{1} o b$
$\Rightarrow x = \bar{a}^{1} o b \in G.$

Also, $(y o a) o \bar{a}^{1} = b o \bar{a}^{1} \Rightarrow y o (a o \bar{a}^{1}) = b o \bar{a}^{1}$
$\Rightarrow y o e = b o \bar{a}^{1}$
$\Rightarrow y = b o \bar{a}^{1} \in G.$

Uniqueness of solutions :-
If possible, let $x_1, x_2 \in G$ be two solutions of $a o x = b \Rightarrow a o x_1 = b = a o x_2$
$\Rightarrow x_1 = x_2$ [by left cancellation].
Similarly for the solution of $y o a = b$.

⑤ In a group (G, o), $(a o b)^{-1} = b^{-1} o a^{-1}$, $\forall\, a, b \in G$.

$\longrightarrow$ Let $a, b \in G$. Then $a o b, a^{-1}, b^{-1}, b^{-1} o a^{-1}, \in G$.

$(b^{-1} o a^{-1}) o (a o b) = [b^{-1} o (a^{-1} o a)] o b = (b^{-1} o e_G) o b$
$= b^{-1} o b = e_G.$

$(a o b) o (b^{-1} o a^{-1}) = [a o (b o b^{-1})] o a^{-1} = (a o e_G) o a^{-1}$
$= a o a^{-1} = e_G.$

$\therefore (b^{-1} o a^{-1}) o (a o b) = (a o b) o (b^{-1} o a^{-1}) = e_G$
$\Rightarrow b^{-1} o a^{-1}$ is the inverse of $a o b$.
i.e., $(a o b)^{-1} = b^{-1} o a^{-1}$.

EXAMPLES OF GROUPS :-

1. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ are commutative groups.
2. $m\mathbb{Z} = \{0, \pm m, \pm 2m, \cdots\}$, the set of all integral multiples of m, where $m \in \mathbb{Z}^+$. $(m\mathbb{Z},+)$ is a commutative group.
3. $M_2(\mathbb{R})$ be the set of all 2×2 matrices of real nos. $M_2(\mathbb{R})$ forms a commutative group w.r.t. 'matrix addition (+)'. $O_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the identity element.
4. $(\mathbb{Z},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R},\cdot)$, $(\mathbb{C},\cdot)$ are not groups.
5. $M_2(\mathbb{R})$ does not form a group w.r.t. 'matrix multiplication'
6. Let $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, forms a commutative group w.r.t. multiplication. i.e., $(\mathbb{Q}^*,\cdot)$ is a commutative group.
7. Let $\mathbb{R}^* = \mathbb{R} - \{0\}$ and $\mathbb{C}^* = \mathbb{C} - \{0\}$ $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$ are commutative groups.
8. Let $S \subset M_2(\mathbb{R})$, be the set of all 2×2 non-singular matrices of real numbers. S forms a group w.r.t. 'matrix multiplication'. This group is not commutative, since matrix multiplication is not commutative in general. This group is called the general linear group of degree 2 over $\mathbb{R}$ and is denoted by $GL(2,\mathbb{R})$. $GL(n,\mathbb{R})$ is the group of all non-singular $n\times n$ real matrices under matrix multiplication.

9. FINITE GROUPS :-

(i) The set $\mathbb{Z}_n$, the classes of residues of integers modulo n $(n \in \mathbb{Z}^+)$ forms an abelian group w.r.t. 'addition (modulo n)'.

(ii) $(\mathbb{Z}_n, \odot)$ is not a group since $\bar{0}$ has no inverse

(iii) $(\mathbb{Z}_n - \{\bar{0}\}, \odot)$ is an abelian group of order $n-1$ w.r.t. multiplication (mod n) when n is a prime.
BUT, Not group when n is a composite number. Since, if $n = pq$ then $\bar{p}, \bar{q} \in \mathbb{Z}_n$, but $\bar{p} \odot \bar{q} = \overline{pq} = \bar{n} = \bar{0} \notin \mathbb{Z}_n - \{\bar{0}\}$. $\therefore$ $\mathbb{Z}_n - \{\bar{0}\}$ is not closed w.r.t. $\odot$

(iv) **GROUP U_n:** The set of all units in the monoid $(Z_n, \odot)$, $n>1$, forms an abelian group w.r.t. multiplication (mod n).

$\bar{u} \in Z_n$ is a unit in the monoid $(Z_n, \odot)$ iff u is less than n and prime to n, i.e., $\gcd(u,n)=1$.

$\longrightarrow$ Let $\bar{u}$ be a unit. Then $\exists\ \bar{v} \in Z_n$ s.t.
$\bar{u} \odot \bar{v} = \bar{1} \Rightarrow uv - 1 = kn \Rightarrow uv - kn = 1$; $v, k \in Z$.
$\Rightarrow \gcd(u,n) = 1$.

Conversely, let $\gcd(u,n)=1$ and $u<n$.
$\exists\ p, q \in Z$ s.t. $up + nq = 1 \Rightarrow up - 1 = -qn$
$\Rightarrow up \equiv 1 \pmod n \Rightarrow p$ is not multiple of n.
Let $p \equiv r \pmod n$, $0<r<n$. Then $\bar{r} \in Z_n$.
$r \equiv p \pmod n \Rightarrow ur \equiv up \pmod n$
$\Rightarrow ur \equiv 1 \pmod n \Rightarrow \bar{u} \odot \bar{r} = \bar{1}$
Since the monoid $(Z_n, \odot)$ is commutative,
$\bar{u} \odot \bar{r} = \bar{r} \odot \bar{u} = \bar{1} \Rightarrow \bar{u}$ is a unit.

To prove the properties of Groups, $U_n = \{\bar{u} : \gcd(u,n)=1\}$

- Let $\bar{u}, \bar{v} \in U_n$. Then $\gcd(u,n)=1$, $\gcd(v,n)=1$
  $\Rightarrow \gcd(uv,n)=1 \Rightarrow \bar{u} \odot \bar{v}$ is a unit,
  $\Rightarrow \bar{u} \odot \bar{v} \in U_n$
  $\therefore U_n$ is closed w.r.t. multiplication (mod n).
- $\odot$ multiplication (mod n) is associative on Z_n and $U_n \subset Z_n$, $\therefore$ Associative prop. holds in $(U_n, \odot)$.
- $\bar{1} \in U_n$ and $\bar{1} \cdot \bar{u} = \bar{u} \cdot \bar{1} = \bar{u}$, $\forall\ \bar{u} \in U_n$.
  $\Rightarrow \bar{1}$ is the identity element in $(U_n, \odot)$
- For each $\bar{u} \in U_n$, $\exists\ \bar{v} \in Z_n$ s.t. $\bar{u} \cdot \bar{v} = \bar{1} = \bar{v} \cdot \bar{u}$
  $\Rightarrow \bar{v}$ is the inverse of $\bar{u}$ and $\bar{v} \in U_n$.
- $\odot$ is commutative on the set Z_n and hence so in U_n.

$\therefore$ $(U_n, \odot)$ Forms an abelian group under multiplication (mod n).

Note: $U_n = \{\bar{u} : \gcd(u,n)=1\}$, is a group of $\phi(n)$ elements, where $\phi(n)$ = The number of integers less than n and prime to n.

eg: The group U_8, U_{10} contains 4 ($=\phi(8)$) elements.
$U_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, $U_{10} = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$.

Note: If n be prime, $U_n = \{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{n-1}\}$, which is a group of order $n-1$. [Every integer $<n$ is prime to n]

COMPOSITION Table :- If G be a non-empty finite set, a b.c. 'o' on G can be defined by the composition table, having n rows and n columns, where n is the number of elements in G.
If $G = \{a_1, a_2, \cdots, a_n\}$, then $a_i \circ a_j$ appears on the table in the ith row and jth column. The n^2 entries of the table are all elements of G, since G is closed under o.
For example, Let us consider the composition table for the b.c. of 'addition modulo 5' on the set Z_5.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\bar{0}$ is the identity element.
inverse of $\bar{1}$ is $\bar{4}$
" " $\bar{2}$ " $\bar{3}$
" " $\bar{3}$ " $\bar{2}$
" " $\bar{4}$ " $\bar{1}$

(3)

The table is symmetric about the principal diagonal, therefore b.c. '$\oplus$' is commutative.
Now, for $\bar{a}, \bar{b}, \bar{c} \in Z_5$, $\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + \overline{b+c}$
$= \overline{a+b+c}$
Also $(\bar{a} + \bar{b}) + \bar{c} = \overline{a+b} + \bar{c} = \overline{a+b+c}$.
$\therefore$ $\oplus$ is associative on Z_5.
$\therefore$ $(Z_5, \oplus)$ forms an abelian group.

② Let us consider the o-composition table for the set $G = \{a, b, c\}$ as follows —

o	a	b	c
a	a	b	c
b	b	a	b
c	c	b	a

Here (G, o) can not form a group because, both the row & the column of b contains b twice. (which is not true for a finite groups)

Here for testing (G, o) as quasigroup, we see the row of b contains b twice.
∴ the equation $b \circ x = b$ has two solutions given by $x = a$ and $x = c$.
Moreover, the row of b does not contain c.
∴ the equation $b \circ x = c$ has no solution in G.
Again, the column of b contains b twice.
∴ The equation $y \circ b = b$ has two solutions; $y = a$ and $y = c$.
Moreover, the column of b does not contain c.
∴ the equation $y \circ b = c$ has no solution in G.
∴ (G, o) is not a quasigroup too.

FINITE GROUP:

A group (G, o) is said to be a finite group if G contains a finite number of elements.
i.e., if $O(G)$ is finite OR, $|G|$ is finite

If (G, o) be a finite group then in every row/column of the composition table each element of G appears exactly once.

Let $a_1, a_2, \ldots, a_n$ be the n elements of G in the order in which they appear in the topmost row and the leftmost column. Let $O(G) = n$ (finite)

Let us consider the ith row of the table.
The entries of ith row are $a_i \circ a_1, a_i \circ a_2, \ldots, a_i \circ a_n$
These all belong to G. And no two of these are equal. If so, then $a_i \circ a_r = a_i \circ a_s \Rightarrow a_r = a_s$.
where $(r, s = 1, 2, \ldots, n)$. This is not possible.

Similar arguments for column hold.

Ex-9.

Ex.8 (S.K. Mapa): The following table defines a b.c. * on the set $S=\{a,b,c\}$.

*	a	b	c
a	a	b	c
b	b	a	c
c	c	a	b

Here we see, each element of S occurs exactly once in every row but not in every column.
a is the identity element.
b has the self inverse, $b^{-1}=b$.
Again $b \circ c = c$, $c \circ b = a \Rightarrow$ c has the right inverse b.
Also $a \circ c = c$.
But c does not have left inverse.

$\therefore$ $(S,*)$ does not form a group.

Ex.9. A binary composition * is defined on the set $S=\{a,b,c\}$ such that $a*a=b*b=c*c=c$. Can you complete the composition table in order that $(S,*)$ may be a group?

Here c must be the identity element $a*c=c*a=a$, $b*c=c*b=b$

*	a	b	c
a	c	b	a
b	a	c	b
c	a	b	c

In order to have exactly one element in every row & column, we must write $b*a=a$, $a*b=b$. Not possible.
$\Rightarrow$ b is the left identity, a is the left identity. But Not a Commutative group.

$\therefore$ $(S,*)$ does not form a group.

Ex.10. Complete the following composition table for the set $S=\{a,b,c\}$ so that $(S,*)$ may be a group.

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Here a is the identity element.
$b*c=c*b=a \Rightarrow b^{-1}=c$, $c^{-1}=b$.
$b*b=c$, $c*c=b$. $(S,*)$ forms a group.
Otherwise, if $b*c=c$, & $b*b=a$
or, if $c*b=b$, then
& $c*c=a$, then
every column will not have exactly one element, & $(S,*)$ would not form a group.

Ex.11. Let $(G,\circ)$ be a finite abelian group with elements $a_1, a_2, \ldots, a_n$ and $x = a_1 \circ a_2 \circ \cdots \circ a_n$. Show that $x \circ x = e$.

Since $a_i \in G$, $a_i^{-1} \in G$ for $\forall\, i = 1, 2, \ldots, n$
And each $a_i^{-1} \in G$ is some $a_i \in G$, which are all distinct n elements of G.
$\therefore$ $x \circ x = (a_1 \circ a_2 \circ \cdots \circ a_n) \circ (a_1 \circ a_2 \circ \cdots \circ a_n)$
Can be form a pair (a_i, a_j) such that each is the inverse of the others. Then $x \circ x = e$.

Ex. 12. Let (G, o) be a finite group containing an even number of elements. Prove that $\exists$ at least one element $a (\neq e)$ in G s.t. $a o a = e$ holds.

Let the elements be $e, a_1, a_2, \cdots, a_{2n-1}$.

$e^{-1} = e$. $a_i \in G \Rightarrow a_i^{-1} \in G$, $\forall i = 1, 2, \cdots, 2n-1$.

Let $a_i^{-1} = a_j$. Then $a_j^{-1} = a_i$, $\forall i, j = 1, 2, \cdots, 2n-1$.

Therefore the elements (a_i, a_j) form a pair such that each is the inverse of the other. This pairing leaves at least one element, say $a_k \in G$ s.t. $(a_k)^{-1} = a_k$. Then $a_k o a_k = e$.

Ex-9 (S. K. Mapa).

③ Let G be the set of four functions f_1, f_2, f_3, f_4 on $\mathbb{R} - \{0\}$ defined by:

$f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = -x$, $f_4(x) = -\frac{1}{x}$.

Show that (G, o) is a commutative group w.r.t. functional composition 'o'.

The composition table:

o	f_1	f_2	f_3	f_4
f_1	x (f_1)	$\frac{1}{x}$ (f_2)	$-x$ (f_3)	$-\frac{1}{x}$ (f_4)
f_2	$\frac{1}{x}$ (f_2)	x (f_1)	$-\frac{1}{x}$ (f_4)	$-x$ (f_3)
f_3	$-x$ (f_3)	$-\frac{1}{x}$ (f_4)	x (f_1)	$\frac{1}{x}$ (f_2)
f_4	$-\frac{1}{x}$ (f_4)	$-x$ (f_3)	$\frac{1}{x}$ (f_2)	x (f_1)

All the entries of the table belong to G. $\Rightarrow G$ is closed w.r.t. o.

identity element $= f_1$

Since functional composition is associative, o is associative on G.

Every element has the self inverse, as the main diagonal contains only the identity f_1.

Also the table is symmetric w.r.t. the principal / main diagonal. So 'o' is commutative.

Hence (G, o) forms a commutative group.

⑥ Let G be the set of six functions f_i $(i=1,2,\cdots,6)$ on $R-\{0,1\}$ defined by:
$f_1(x)=x$, $f_2(x)=\frac{1}{x}$, $f_3(x)=1-x$, $f_4(x)=1-\frac{1}{x}$, $f_5(x)=\frac{x}{x-1}$, $f_6(x)=\frac{1}{1-x}$. Show that $(G,\circ)$ is a non-abelian group.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_5	f_6	f_2	f_1
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_2	f_1	f_3	f_4

(i) All entries of the table belong to the set G.
∴ G is closed w.r.t. $\circ$

(ii) Associative property holds in $(G,\circ)$ as the functional composition is associative in general.

(iii) Identity element $= f_1$
Every f_i has a inverse.

(iv) Inverse of $f_1 = f_1$
" " $f_2 = f_2$
" " $f_3 = f_3$
" " $f_4 = f_6$
" " $f_5 = f_5$
" " $f_6 = f_4$

∴ $(G,\circ)$ forms a group.

(v) But it is a non-abelian group as the table about the principal diagonal is not symmetric, $\because$ $\circ$ is not commutative.

⑤ Let the addition $(+)$ be defined on the set $Z_2 \times Z_2$ by $(a,b)+(c,d)=(a\oplus_2 c, b\oplus_2 d)$. Show that $Z_2\times Z_2$ is a commutative group under '+'.

$Z_2\times Z_2 = \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{1},\bar{1})\}$,

$+$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$
$(\bar{0},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{0})$
$(\bar{1},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$
$(\bar{1},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{0})$

(i) All entries of the table $\in Z_2\times Z_2$, $\Rightarrow$ '+' is closed on $Z_2\times Z_2$.

(ii) '+' and $\oplus_2$ both associative on $Z_2\times Z_2$

(iii) $(\bar{0},\bar{0})$ is the identity element.

(iv) Principal diagonal contains the identity element only
∴ each element is its own inverse.

(v) Table is symmetric about Principal diagonal

∴ $(Z_2\times Z_2,+)$ is a Commutative group.

Exercises – 10 (S. K. Mapa)

② In a group (G, o), $(a o b)^2 = a^2 o b^2$ holds $\forall\, a, b \in G$. Prove that the group is abelian.

$(a o b)^2 = a^2 o b^2$ holds in a group (G, o)

$\Rightarrow (a o b) o (a o b) = (a o a) o (b o a)$

$\Rightarrow a o (b o a) o b = a o (a o b) o a$, by associative prop.

$\Rightarrow b o a = a o b$, by left & right cancellation laws.

$\therefore$ The group (G, o) is abelian.

③ In a group (G, o), $(a o b)^3 = a^3 o b^3$, $(a o b)^5 = a^5 o b^5$ hold $\forall\, a, b \in G$. Prove that the group is abelian.

$(a o b)^3 = a^3 o b^3 \longrightarrow$ (i) $\quad (a o b)^5 = a^5 o b^5 \longrightarrow$ (ii)

$\Rightarrow (a o b) o (a o b) o (a o b) = a^3 o b^3$

$\Rightarrow a o [(b o a) o (b o a)] o b = a o (a^2 o b^2) o b$

$\Rightarrow (b o a)^2 = a^2 o b^2 \longrightarrow$ (iii)

[Using Associative & Cancellation laws]

Now $(a o b)^5 = a^5 o b^5$

$\Rightarrow (a o b) o (a o b)^3 o (a o b) = a o (a^4 o b^4) o b$

$\Rightarrow a o [b o (a o b)^3 o a] o b = a o (a^4 o b^4) o b$

$\Rightarrow b o (a^3 o b^3) o a = a^4 o b^4$ [by (i), using Cancellation laws].

$\Rightarrow (b o a)(a^2 o b^2) o (b o a) = a^4 o b^4$

$\Rightarrow (b o a)(b o a)^2 o (b o a) = a^4 o b^4$ [by (iii)]

$\Rightarrow (b o a)^2 o (b o a)^2 = a^4 o b^4$

$\Rightarrow (a^2 o b^2) o (a^2 o b^2) = a^2 o (a^2 o b^2) o b^2$

$\Rightarrow a^2 o (b^2 o a^2) o b^2 = a^2 o (a^2 o b^2) o b^2$

$\Rightarrow b^2 o a^2 = a^2 o b^2$ [by cancellation laws]

$\Rightarrow b^2 o a^2 = (b o a)^2$ [by (iii)] $\longrightarrow$ (iv)

From (iv), we obtain,

$b o (b o a) o a = (b o a) o (b o a) = b o (a o b) o a$

$\Rightarrow b o a = a o b$ [by cancellation laws]

$\therefore$ The group (G, o) is abelian.

④ In a group G, for all $a, b \in G$, $(ab)^n = a^n b^n$ holds for 3 consecutive integers n. Prove that the group is abelian.

Let us take p be any integer. Then

$(ab)^p = a^p b^p \longrightarrow$ (i), $(ab)^{p+1} = a^{p+1} b^{p+1} \longrightarrow$ (ii),

$(ab)^{p+2} = a^{p+2} b^{p+2} \longrightarrow$ (iii)

From (ii), $ab(ab)^p = (a a^p)(b b^p)$

$\Rightarrow ab(a^p b^p) = a(a^p b) b^p$ [by (i)]

$\Rightarrow a(ba^p)b^p = a(a^p b)b^p$, by associative law.

$\Rightarrow ba^p = a^p b$, by cancellation laws. $\longrightarrow$ (1).

From (iii), $ab(ab)^{p+1} = a(a^{p+1} b) b^{p+1}$

$\Rightarrow ab(a^{p+1} b^{p+1}) = a(a^{p+1} b) b^{p+1}$ [by (ii)]

$\Rightarrow a(ba^{p+1}) b^{p+1} = a(a^{p+1} b) b^{p+1}$

$\Rightarrow ba^{p+1} = a^{p+1} b \longrightarrow$ (2), by cancellation law

From (2), $(ba^p)a = a^p(ab)$

$\Rightarrow (a^p b)a = a^p(ab)$ [using (1)]

$\Rightarrow a^p(ba) = a^p(ab)$

$\Rightarrow \underline{ba = ab}$, by left cancellation law.

$\therefore$ The group G is <u>abelian</u>.

⑤ In a group G, $a^2 b^2 = b^2 a^2$ and $a^3 b^3 = b^3 a^3$ hold $\forall a, b \in G$. Prove that the group is abelian.

From, $a^2 b^2 = b^2 a^2$

$\Rightarrow a^2 = b^2 a^2 b^{-2} \longrightarrow$ (1), $\quad a^2 b^2 = b^2 a^2$

$\Rightarrow b^2 = a^{-2} b^2 a^2 \longrightarrow$ (2).

From, $a^3 b^3 = b^3 a^3$

$\Rightarrow a^2(ab)b^2 = b^2(ba)a^2$

$\Rightarrow (ab)b^2 = a^{-2}[b^2(ba)]a^2 = b^2(ba)$ [by (2)]

$\Rightarrow ab = b^2(ba)b^{-2} = ba$ [by (1)].

$\therefore ab = ba$

The group is abelian.

Ex-7 (S.K. Mapa)

① Define a b.c. 'o' on Q by $a o b = 2a+b$; $a, b \in Q$. Show that (Q, o) is a quasigroup but not a semigroup. Does there exist an identity element in (Q, o)?

Let us consider two equations:
$a o x = b$ and $y o a = b$, for $a, b \in Q$.
So that $2a+x=b$ & $2y+a=b$
$\Rightarrow x = 2a-b \in Q$; $y = \frac{b-a}{2} \in Q$.
$\therefore$ x & $y \in Q$ and they are unique for $a, b \in Q$.
$\therefore$ (Q, o) is a quasigroup. (proved)

To show: (Q, o) is not a semigroup, let us take $a, b, c \in Q$.
$a o (b o c) = a o (2b+c) = 2(a)+(2b+c)$
And $(a o b) o c = (2a+b) o c = 2(2a+b)+c$
$\Big\} \neq$
$\therefore$ 'o' is not associative on Q.

To find identity element in (Q, o):
For left identity, let us consider an equation:
$x o a = a$ for $a \in G$.
$\Rightarrow 2x+a=a \Rightarrow x=0 \in Q \Rightarrow 0$ is a left identity in (Q, o).
For right identity, let us consider an equation:
$a o y = a$ for $a \in G$. $\Rightarrow 2a+y=a \Rightarrow y=-a \in Q$.
Here $y(=-a)$ depends on the element, i.e., y is different for different elements of Q.
Hence y cannot be a right identity.
$\therefore$ Right identity does not exist in (Q, o)
$\therefore$ No identity element exists in (Q, o).

② Let $R^* = R - \{0\}$. Define a b.c. 'o' on R^* by $a o b = |ab|$; $a, b \in R^*$. Show that (R^*, o) is a semigroup but not a quasigroup.

Let $a, b, c \in R^*$. Then $a o (b o c) = a o |bc| = |abc|$
Also $(a o b) o c = |ab| o c = |abc|$
$\therefore$ $a o (b o c) = (a o b) o c \Rightarrow$ 'o' is associative
$\Rightarrow (R^*, o)$ is a semigroup.

To show $(\mathbb{R}^*, o)$ a quasigroup:

Let us consider the equations:

$a o x = b$ and $y o a = b$ for $a, b \in G$

$\Rightarrow |ax| = b$ & $|ya| = b$

$\Rightarrow |x| = \frac{b}{|a|}$ & $|y| = \frac{b}{|a|}$.

{For negative b, the R.H.S. quantity $\frac{b}{|a|}$ becomes negative, whereas the L.H.S. is a +ve quantity}

So the solutions for x & y do not exist for (-ve) $b \in \mathbb{R}^*$.

$\therefore$ $(\mathbb{R}^*, o)$ cannot be a quasigroup.

③ Let $M = \left\{ \begin{pmatrix} a & a \\ b & b \end{pmatrix} : a+b \neq 0, a, b \in \mathbb{R} \right\}$. Show that (i) there is no left identity, (ii) $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ is a right identity.

(i) Let $\begin{pmatrix} x & x \\ y & y \end{pmatrix} o \begin{pmatrix} a & a \\ b & b \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix}$, where $a, b \in \mathbb{R}$, and $a+b \neq 0$.

$\Rightarrow \begin{pmatrix} ax+bx & ax+bx \\ ay+by & ay+by \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix} \Rightarrow ax+bx = a;\ ay+by = b$

$\Rightarrow x = \frac{a}{a+b}, \ y = \frac{b}{a+b}$.

Here the values of x & y depend on a & b.
i.e., For different a & b, we will have different x & y.
$\therefore$ there does not exist a left identity.

(ii) For right identity, let us take

$\begin{pmatrix} a & a \\ b & b \end{pmatrix} o \begin{pmatrix} x & x \\ y & y \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix}$

$\Rightarrow \begin{pmatrix} ax+ay & ax+ay \\ bx+by & bx+by \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix} \Rightarrow \begin{matrix} ax+ay=a \\ \& \ bx+by=b \end{matrix}$

Now, $ax + ay = a \Rightarrow x+y=1$, if $a \neq 0$

$bx + by = b \Rightarrow x+y=1$, if $b \neq 0$.

Now, $x+y=1$ and $a+b \neq 0$ may give us

$x=1, y=0$.

$\therefore$ $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ is a right identity. (proved)