Sol. : W

Planar Graphs

ome Algebraic Structures

1. Introduction

In this chapter we shall define groups, rings, fields and prove some of their elementary properties. These concepts are as basic to Modern Mathematics as the operations of addition and multiplication are to school mathematics. In fact the basic operations in arithmetic are generalised in Modern Mathematics to abstract level.

2. Binary Operation

(a) Definition : Let A be a non-empty set. A function $f : A \times A \to A$ is called a **binary** operation.

Examples of Binary Operation

It should be noted that since a binary operation is a function, one and only one element of A is assigned to one ordered pair of $A \times A$. Further, we shall denote binary operations by $*$ or $(+)$ instead of f. Since, a binary operation is a function to **each** $(a, b) \in A \times A$, there exists a **unique** element $a * b \in A$. We describe this property by saying that ***A* is closed under** $*$.

Example 1 : Let $A = Z$ and $a * b$ be $a + b$. Then $*$ is a binary operation on Z.

Example 2 : Let $A = Z^+$ and $a * b$ be $a - b$.

Then $*$ is not a binary operation on Z^+ since $a - b$ may not be an element of A for some a, b in A. *e.g.* $3 * 7 = 3 - 7 = -4$ does not belong to Z^+.

Example 3 : Let $A = R$ and $a * b$ be a / b.

Then $*$ is not a binary operation on R since a / b may not be an element of R for some a, b in A. *e.g.* $5 * 0 = 5 / 0 \notin A$.

However, if $A = R \sim \{0\}$ then $a * b = a / b$ is a binary operation.

Example 4 : Let L be a lattice and $a * b$ be $a \wedge b$ (GLB of a, b).

Then $a * b$ is a binary operation because for every ordered pair a, b of L, there exists a unique $a \wedge b$.

Example 5 : Let L be a lattice $a * b$ be $a \vee b$ (LUB of a, b).

Then $a * b$ is a binary operation for the reason given above.

(b) Identity and Inverse

Definition : Given a non-empty set A and a binary operation $\oplus$ if there is an element $e \in A$, such that for **every** $a \in A$, $a \circledast e = e \circledast a = a$, then e is called the **identity** element for the operation $\circledast$.

For example, in the set of real numbers, zero is identity element for usual addition because $a + 0 = 0 + a = a$ for every $a \in R$.

In the set of real numbers, unity is identity element for usual multiplication because $a \times 1 = 1 \times a = a$ for every $a \in R$.

Definition : Given a non-empty set A and a binary operation $\circledast$ if A has an identity element e and if for any two element $a, b \in S$, $a \circledast b = b \circledast a = e$, then b is called the **inverse** of a and is denoted by a^{-1}.

Example : "If a binary operation in Q^+ (set of positive rational numbers) is defined by $a \circledast b = ab/2$ then 2 is an identity and $4/a$ is the inverse of a under $\circledast$".

State true or false with proper justification.

Sol. : If e is an identity element under $\circledast$, we must have **(M.U. 2004)**

$$a \circledast e = e \circledast a = a$$

But by data, $a \circledast e = \frac{ae}{2}$

$$\therefore \frac{ae}{2} = a \quad \therefore e = 2 \text{ is identity.}$$

If b is the inverse of a, we must have

$$a \circledast b = b \circledast a = 2 \quad \text{(identity)}$$

But by data, $a \circledast b = \frac{ab}{2}$

$$\therefore \frac{ab}{2} = 2 \quad \therefore b = \frac{4}{a} \quad \therefore a^{-1} = \frac{4}{a}$$

Hence, the statement is true.

3. Properties of Binary Operations

1. Commutativity

Definition : A binary operation on set A is called **commutative** if

$$\boxed{a * b = b * a} \quad \text{for all element } a \text{ and } b \text{ of } A.$$

Example 1 : The binary operation of usual addition in Z is commutative ?

Example 2 : The binary operation of usual subtraction (division) on Z is not commutative.

2. Associativity

Definition : A binary operation $*$ on a set A is said to be **associative**, if

$$\boxed{a * (b * c) = (a * b) * c} \quad \text{for all } a, b, c \in A.$$

Example 1 : Is the binary operation of usual addition on Z associative ?

Sol. : Because $a + (b + c) = (a + b) + c$ for all $a, b, c \in Z$, the operation of addition is associative.

Example 2 : Show that the relation $*$ given by $a * b = a^b$ on the set of natural numbers is a binary operation. Is it associative? **(M.U. 2005, 07)**

Sol. : If a and b are natural numbers, then a^b is also a natural numbers.

Hence, $a * b$ is binary.

Since, $a^{bc} \neq a^{cb}$, the operation is not associative.

Example 3 : Is the binary operation of usual subtraction (division) on Z associative ? Commutative ? (M.U. 2003)

Sol. : Because $a - (b - c) \neq (a - b) - c$ *e.g.* $5 - (6 - 4) = 5 - (2) = 3$ and $(5 - 6) - 4 = -1 - 4 = -5$, the usual subtraction is **not** associative on Z.

Also $5 - 8 \neq 8 - 5$.

It is **not** commutative on Z.

Example 4 : Is the operation $*$ on $A = (a, b, c)$ defined by the adjoining table associative ?

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

Sol. : Although $(a * c) * b = c * b = a$ and $a * (c * b) = a * a = a$ but $a * (b * c) = a * a = a$ and $(a * b) * c = a * c = c$, the operation $*$ is **not** associative.

Example 5 : Is the operation $a * b = a \times |b|$, associative on R ?

Sol. : Because $(a * b) * c = (a \times |b|) * c = a \times |b| \times |c|$

and $a * (b * c) = a * (b \times |c|) = a \times |b \times |c|| = a \times |b| \times |c|$

We see that $*$ is associative. (But note that $*$ is **not** commutative).

Example 6 : Is the operation $a * b = ab / 5$ on R associative ?

Sol. : Because $(a * b) * c = (ab / 5) * c = abc / 25$

and $a * (b * c) = a * (bc / 5) = abc / 25$,

the operation $*$ is associative. (Note that $*$ is also commutative.)

Example 7 : Let L be a lattice and let $a * b = a \wedge b$ (the greatest lower bound). Then $*$ is associative.

Sol. : Since $(a * b) * c = (a \wedge b) \wedge c$ and $a * (b * c) = a \wedge (b \wedge c)$

But, $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.

Hence, the result.

Similarly, we can prove that $a * b = a \vee b$ (the least upper bound of a and b) is also associative.

EXERCISE - I

1. Show that $\circ$ given by $a \circ b = a^b$ is a binary operation on the set of natural numbers. (M.U. 2005, 07)

2. Verify whether the following binary operations are commutative and associative.

   (a) Usual subtraction / division on Z. [**Ans.** : Neither commutative nor associative]

   (b) $a * b = a + b + 3$ on Z^+. [**Ans.** : Commutative and Associative]

   (c) $a * b = a / b$ on non-zero real numbers. [**Ans.** : Neither commutative, nor associative]

   (d) $a * b = ab$ on Z. [**Ans.** : Commutative and Associative]

   (e) $a * b$ = maximum (minimum) of a and b on R. [**Ans.** : Commutative and Associative]

   (f) $a * b = ab / 7$. [**Ans.** : Commutative and Associative]

   (g) $a * b = ab + 3b$ on R. [**Ans.** : Neither Commutative nor Associative]

3. Consider the set $A = \{0, 1, 2, 3\}$. Give one example for each of the following.

(i) A relation R on A that is neither symmetric, nor anti-symmetric.

(ii) A relation R on A that is symmetric, transitive but not reflexive.

(iii) A binary operation on A that is commutative but not associative. **(M.U. 2005)**

*	0	1	2	3
0	1	2	3	0
1	2	3	2	2
2	3	2	0	2
3	0	2	2	1

[**Ans. :** (i) $R = \{(1, 3), (1, 0), (2, 0), (0, 1)$.

(ii) $R = \{(0, 1), (1, 0), (1, 2), (2, 1), (2, 3), (3, 2), (0, 0), (1, 3), (3, 1)\}$

(iii) See adjoining Table.

4. Semi-Group

(a) Definition

(M.U. 2000, 10, 13)

A non-empty set S together with a (i) **binary** and (ii) **associative operation**, $*$ is called a **semi-group**.

We denote the semi-group by $(S, *)$. Thus, a non-empty set S is a semi-group if

(i) $*$ is binary *i.e.* $a * b \in S$ for every $a, b \in S$.

(ii) $*$ is associative *i.e.* $a * (b * c) = (a * b) * c$ for every $a, b, c \in S$.

Definition : A semi-group $(S, *)$ is called **commutative semi-group** if $*$ is commutative.

Thus, $(S, *)$ will be a commutative semi-group if $*$ is (i) binary, (ii) associative and (iii) commutative.

Examples of Semi-groups

Example 1 : $(Z, +)$ is a commutative semi-group.

Example 2 : If A is a set and $\wp(A)$ is its power set then $\wp(A)$ with the operation of union is a commutative semi-group.

Example 3 : Prove that the set Q of rational numbers with the binary operation $*$ defined by $a * b = a + b - ab$; $a, b \in Q$ is a semi-group. Is it commutative ? **(M.U. 2005)**

Sol. : With usual multiplication addition and subtraction for any two rational numbers $a * b = a + b - ab$ belongs to Q. Hence, $*$ is a binary operation.

Now, $(a * b) * c = (a + b - ab) * c$

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

$= a + b - ab + c - ac - bc + abc$

$= a + b + c - ab - bc - ca + abc.$

Also, $a * (b * c) = a * (b + c - bc)$

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

$= a + b + c - bc - ab - ac + abc$

$= a + b + c - ab - bc - ca + abc.$

Hence, $*$ is associative.

Further, $b * a = b + a - ba = a + b - ab$

Hence, $a * b = b * a$. $\therefore$ $*$ is also commutative.

Example 4 : Let $Z_n = \{0, 1, 2, ..., (n-1)\}$ and $*$ be the operation on Z_n such that $a * b$ = the remainder when ab is divided by n.

(a) Construct the table for the operation $*$ when $n = 4$.

(b) Show that $(Z_4, *)$ is a semigroup. **(M.U. 1997, 99, 2017)**

Sol. : (a) We have $Z_4 = \{0, 1, 2, 3\}$ and $a * b$ = remainder when ab is divided by 4.

With this understanding, we get the adjoining table.

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(b) **(i)** From the table it is clear the Z_n is closed under $*$ because $a * b$ belongs to Z_n.

(ii) Now consider associativity. Let $a = 1$, $b = 2$, $c = 3$ then using the table we see that

$$(a * b) * c = 2 * 3 = 2$$

$$a * (b * c) = 1 * 2 = 2$$

$$\therefore \quad (a * b) * c = a * (b * c)$$

It can be verified for all the elements.

Hence, $*$ is associative. Hence, $(Z_n, *)$ is a semigroup for any n.

Example 5 : Let $(A, *)$ be a semigroup. Consider a binary operation + on A such that for x and y in A, $x + y = x * a * y$ where a is in A.

Show that + is an associative operation. **(M.U. 1997)**

Sol. : To prove associativity, we shall prove that

$$(x + y) + z = x + (y + z) \quad \text{where } x, y, z \in R$$

Now, $\quad L.H.S. = (x + y) + z = (x * a * y) + z$

$$= (x * a * y) * a * z = x * a * y * a * z$$

And $\quad R.H.S. = x + (y + z) = x + (y * a * z)$

$$= x * a * (y * a * z) = x * a * y * a * z$$

$$\therefore \quad L.H.S. = R.H.S.$$

$\therefore$ + is an associative operation.

(b) Product of Semi-groups

Let $(S_1, *_1)$ and $(S_2, *_2)$ be two semi-groups. We can obtain a new semi-group $S = S_1 \otimes S_2$ called the product of S_1 and S_2 as follows.

(i) The elements of S come from $S_1 \times S_2$ *i.e.* if the ordered pair (a, b) is an element S, then $a \in S_1$ and $b \in S_2$.

(ii) The operation $*$ on S is defined on the two components as

$$(a, b) * (a', b') = (a *_1 a', b *_2 b')$$ [See Ex. 1, page 16-11]

5. Monoid

(a) Definition : A **semi-group** $(S, *)$ which has **identity** is called a **monoid**. **(M.U. 2000, 10)**

Thus, we can say that there are semi-groups which have identity (in which case we call them monoids) and there are semi-groups without identity element.

(b) Theorem : The identity element of a semi-group is unique.

Proof : If possible let e' be another identity element of the semi-group $(S, *)$. Since e' is an identity, $a * e' = e' * a = a$ for each a.

In particular, let $a = e$. $\therefore$ $e * e' = e' * e = e$

Also since e is an identity, $a * e = e * a = a$ for each a. ..... (1)

In particular let $a = e'$, $\therefore$ $e' * e = e * e' = e$

From (i) and (ii), it follows that $e = e'$. ..... (2)

$\therefore$ The identity element is unique.

Examples of Monoid

Example 1 : The semi-group $(Z, +)$ is a monoid because 0 is the identity element.

But note that the semi-group $(Z^+, +)$ is not a monoid as it has no identity element.

Example 2 : The semi-group $(Z^+, \times)$ is a monoid because 1 is its identity element.

Example 3 : Let S be a finite set. Let $F(S)$ be the set of all functions $f : S \to S$ and let $*$ be operation of composition of functions.

$F(S)$ is a monoid because $*$ is associative and identity function is the identity of this semi-group.

Example 4 : Verify that if A is any set then the power set $\mathcal{P}(A)$ with the operation of union is a monoid.

Sol. : As seen before in Ex. 2, page 16-4 for union $(\mathcal{P}(A), \cup)$ is a commutative semi-group.

If Φ is the null-set then Φ is the identity element because

$$\Phi * A = \Phi \cup A = A \quad \text{and} \quad A * \Phi = A \cup \Phi = A$$

Hence, $(\mathcal{P}(A), \cup)$ is a monoid.

Note that $\mathcal{P}(S)$ with $*$ as intersection of two subsets of $\mathcal{P}(S)$ is also a monoid with $\mathcal{P}(S)$ itself as identity. It is also commutative.

Example 5 : If $a * b = a$ and S is the set of all positive integers $Z^+ = \{1, 2, 3, ...\}$, verify whether $(S, *)$ is a semi-group or a monoid.

Sol. : Since for every a, b, $a * b = a$ is in S, $*$ is binary.

Further, $(a * b) * c = a * c = a$ and $a * (b * c) = a * b = a$

$\therefore$ $*$ is associative.

Hence, $(S, *)$ is a semi-group.

But $a * 1 = a$ and $1 * a = 1$.

Hence, $(S, *)$ has no identity element. $\therefore$ $(S, *)$ is not a monoid.

8. Isomorphism, Automorphism And Homomorphism

We have already studied isomorphism between two posets. In general, two algebraic systems are called isomorphic if they preserve special characteristics of the system. We shall now consider isomorphism between two semi-groups.

Isomorphism

Definition : Let $(S, *)$ and $(S', *')$ be two semi-groups. A function $f : S \to S'$ is called an isomorphism from $(S, *)$ to $(S', *')$ if f is one-to-one and onto and if

$$\boxed{f(a * b) = f(a) *' f(b)} \quad \text{for all } a, b \text{ in } S.$$

Note carefully the $*$ on the left side and $*'$ on the right side.

Theorem 1 : If $(S, *)$ and $(S', *')$ are two semi-groups and if $f : S \to S'$ is a isomorphism from $(S, *)$ to $(S', *')$ then $f^{-1} : S' \to S$ is also an isomorphism from $(S', *')$ to $(S, *)$.

Proof : Since by definition of isomorphism, f is a one-to-one correspondence hence f^{-1} exists and is a one-to-one correspondence from $(S', *')$ to $(S, *)$.

Let a' and b' be any two elements of S'. Since f is onto there exist elements a and b in S such that $f(a) = a'$ and $f(b) = b'$.

$\therefore \quad a = f^{-1}(a')$ and $b = f^{-1}(b)$

Now, $f^{-1}(a' *' b') = f^{-1}(f(a) *' f(b)) = f^{-1}(f(a * b))$

[$\because$ f is a isomorphism $f(a * b) = f(a) *' f(b)$ by definition above.]

$\therefore \quad f^{-1}(a' *' b') = (f^{-1} \circ f)(a * b)$

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

Hence, f^{-1} is an isomorphism.

Procedure To Prove An isomorphism

To prove an isomorphism between two semi-groups $(S, *)$ and $(S', *')$ we shall follow the following procedure.

(i) **Step 1 :** We define the function $f : S \to S'$ with domain of $f = S$.

(ii) **Step 2 :** We shall show that f is one-to-one.

(iii) **Step 3 :** We shall show that f is onto.

(iv) **Step 4 :** We shall show that $f(a * b) = f(a) *' f(b)$.

Example 1 : Let S be the set of all even integers. Show that the semi-groups $(Z, +)$ and $(S, +)$ are isomorphic. **(M.U. 2016)**

Sol. : We shall follow the above procedure.

Step 1 : We define the function $f : Z \to S$ where $f(a) = 2a$.

Step 2 : Suppose $f(a_1) = f(a_2)$. Then $2a_1 = 2a_2$. Hence, f is one-to-one.

Step 3 : Suppose b is an even integer.

Then $a = b/2 \in Z$ and $f(a) = f(b/2) = 2(b/2) = b$. Hence, f is onto.

Step 4 : We have $f(a + b) = 2(a + b) = 2a + 2b$

$= f(a) + f(b)$

Hence, $(Z, +)$ and $(S, +)$ are iso-morphic semi-groups.

Example 2 : Let R^+ be the set of all positive real numbers. Show that the function $f : R^+ \to R$ defined by $f(x) = \log x$ is an isomorphism from the semigroup $(R^+, \times)$ to the semigroup $(R, +)$ where $\times$ and $+$ are the usual multiplication and addition respectively. **(M.U. 2004, 05)**

Sol. : Step 1 : The function is defined by $f(x) = \log x$.

Step 2 : If $f(a_1) = f(a_2)$, then $\log a_1 = \log a_2$

$\therefore \quad a_1 = a_2$. f is one-to-one.

Step 3 : Suppose b is a real number then

$e^b \in R$ and $f(e^b) = \log e^b = b \in R^+$.

$\therefore$ Each element of R is an f-image of some element of R^+.

$\therefore$ f is onto.

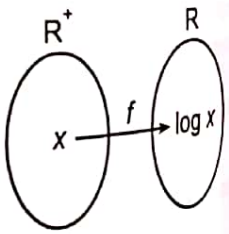

Fig. 16.1

Step 4 : We have $f(ab) = \log ab = \log a + \log b = f(a) + f(b)$

$\therefore$ f is an isomorphism.

Example 3 : Let $S = \{a, b, c\}$ and $S' = \{p, q, r\}$ and consider the following operations.

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

$*'$	p	q	r
p	r	p	q
q	p	q	r
r	q	r	p

Let $f(a) = q$, $f(b) = p$, $f(c) = r$. Show that S and S' are isomorphic.

Sol. : Step 1 : The function f is defined by $f(a) = q$, $f(b) = p$, $f(c) = r$.

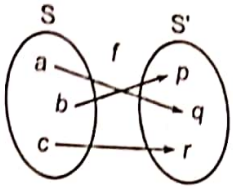

Fig. 16.2

Step 2 : Clearly f is one-to-one.

Step 3 : Clearly f is onto.

Step 4 : Now, from the first table above since $a * b = b$

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

Also, since $f(a) = q$, $f(b) = p$,

$$f(a) *' f(b) = q *' p = p \qquad \therefore \; f(a * b) = f(a) *' f(b)$$

This can be shown to be true for all possible products of a, b and c. In fact we can obtain the table of operation $*$ on $f(a)$, $f(b)$ and $f(c)$ by replacing in the first table, the images of a, b, c *i.e.* by replacing a by $f(a) = q$, b by $f(b) = p$ and c by $f(c) = r$. Thus, we get

$*$	q	p	r
q	q	p	r
p	p	r	q
r	r	q	p

Interchanging the first and second rows we get the left table. Then interchanging the first and second columns we get the table on the right which is the same as the table given for $*'$ on S'. This shows that S and S' are isomorphic.

$*$	q	p	r
p	p	r	q
q	q	p	r
r	r	q	p

$*$	p	q	r
p	r	p	p
q	p	q	r
r	q	r	p

Example 4 : Let $S = \{a, b, c, d\}$ and $S' = \{p, q, r, s\}$ and consider the following operations.

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

$*'$	p	q	r	s
p	p	q	r	s
q	q	p	p	r
r	q	s	s	r
s	p	q	r	s

Let $f(a) = p$, $f(b) = q$, $f(c) = r$, $f(d) = s$. Show that f is an isomorphism.

Sol. : Step 1 : The function is defined by $f(a) = p$, $f(b) = q$, $f(c) = r$, $f(d) = s$.

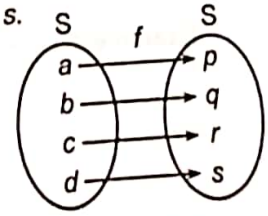

Fig. 16.3

Step 2 : Clearly f is one-to-one.

Step 3 : Clearly f is onto.

Step 4 : Now $a * b = b$. $\therefore \; f(a * b) = f(b) = q$

Since $f(a) = p$ and $f(b) = q$

$$f(a) *' f(b) = p *' q = q \qquad \therefore \; f(a * b) = f(a) *' f(b)$$

Theorem 2 : Let $(S, *)$ and $(S', *')$ be monoids with identity elements e and e' respectively. Let $f : S \to S'$ be an isomorphism from $(S, *)$ to $(S', *')$. Prove that $f(e) = e'$. **(M.U. 2003)**

Proof : Let b be any element of S'.

Since f is onto there is an element a in S such that b is the image of a i.e. $f(a) = b$.

Now, $b = f(a) = f(a * e) = f(a) *' f(e)$

because S and S' are isomorphic. ..... (1)

But $f(a) = b$.

$\therefore$ From (1), we get $b = b *' f(e)$

Similarly, since $a = e * a$ ..... (2)

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

because S and S' are isomorphic.

$\therefore$ $b = f(e) *' b$ ..... (3)

From (2) and (3), we see that $f(e)$ is the identity element of S'.

But since identity element is unique, we get, $f(e) = e'$.

Corollary : If $(S, *)$ and $(S', *')$ are two semi-groups such that S has an identity element while S' does not have the identity element then $(S, *)$ and $(S', *')$ cannot be isomorphic.

Proof : For isomorphism of two semi-groups we must have, for all a, b, S,

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

If we take $b = e$, the identity element in S, then we must have,

$$f(a * e) = f(a) *' f(e) = f(a) *' e'$$

where, e' is the identity element of S' by the above theorem.

Since, by data e' does not exist, S and S' cannot be isomorphic.

Example : Let Z be the set of all integers and S' be the set of all even integers. If X is the usual multiplication then prove that (Z, X) and (S, X) are semi-groups which are not isomorphic.

Sol. : We can easily prove that (Z, X) and (S', X) are semi-groups because multiplication is binary and associative in both Z and S'.

But $Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ has multiplicative identity 1

and $S' = \{\ldots, -6, -4, -2, 2, 4, 6, \ldots\}$ has no multiplicative identity.

Hence, by the above corollary (Z, X) and (S', X) are not isomorphic.

Automorphism

Definition : An isomorphism from a semigroup $(S, *)$ to $(S, *)$ itself is called an **automorphism** (auto = self) on $(S, *)$.

Example 1 : Let $S = \{a, b, c, d\}$ and consider the following operations $*$.

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

Let $f(a) = d$, $f(b) = c$, $f(c) = b$ and $f(d) = a$.

Show that f is an automorphism.

Sol. : Step 1 : The function is defined by

$f(a) = d$, $f(b) = c$, $f(c) = b$, $f(d) = a$.

Step 2 : Clearly f is one-to-one.

Step 3 : Clearly f is onto.

Step 4 : From the table

$a * b = b$ $\quad\therefore\quad f(a * b) = f(b) = c$

Since $f(a) = d$, $f(b) = c$

$f(a) * f(b) = d * c = c$ $\quad\therefore\quad f(a * b) = f(a) * f(b)$

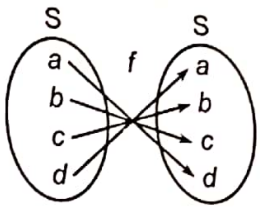

Fig. 16.4

This can be shown to be true for all products of a, b, c and d.

Hence, f is isomorphic.

$\therefore$ $(S, *)$ is an automorphism.

If we drop the conditions of one-to-one and onto from the definition of isomorphism we get another property, called homomorphism of the algebraic structures of two semi-groups.

Homomorphism

Definition : Let $(S, *)$ and $(S', *')$ be two semi-groups. A function $f : S \to S'$ is called a **homomorphism** from $(S, *)$ to $(S', *')$ if

$$\boxed{f(a * b) = f(a) *' f(b)}$$ for all a, b in S.

Further if f is also onto S' is called a **homomorphic image** of S.

We note that for isomorphism as well as for homomorphism, **the image of the product is equal to the product of the images**

i.e., $f(a * b) = f(a) *' f(b)$

And the difference is that, in isomorphism f is one-to-one and also onto.

Theorem 3 : Let $(S, *)$ and $(S', *')$ be monoids with identity elements e and e' respectively. Let $f : S \to S'$ be homomorphism from $(S, *)$ to $(S', *')$.

Prove that $f(e) = e'$.

Proof : Similar to the proof of Theorem 2, page 16-9 and as such is left to you.

Theorem 4 : If f is a homomorphism from a commutative semi-group $(S, *)$ onto a semi-group $(S', *')$ then $(S', *')$ is also commutative.

Proof : Let s_1' and s_2' be any two elements of S'. Since f is onto there exist two elements s_1 and s_2 in S whose images are s_1' and s_2' respective *i.e.* $f(s_1) = s_1'$ and $f(s_2) = s_2'$.

$$\therefore \quad s_1' *' s_2' = f(s_1) *' f(s_2)$$
$$= f(s_1 * s_2) = f(s_2 * s_1)$$

[$\because$ $(S, *)$ is a commutative semi-group.]

$$= f(s_2) *' f(s_1)$$
$$= s_2' *' s_1'$$

$\therefore$ $(S', *')$ is also commutative.

Example 1 : Let $S = N \times N$. Let $*$ be the operation on S defined by $(a, b) * (a', b') = (a + a', b + b')$. Further, let $f : (S, *) \to (Z, +)$ defined by $f(a + b) = a - b$. Show that $(S, *)$ is a semi-group and f is a homomorphism. **(M.U. 2004)**

Sol. : (a) Let $x = (a, b),\ y = (c, d),\ z = (e, f)$ where $a, b, c, d, e, f \in N$.

(i) $$x * y = (a, b) * (c, d)$$
$$= (a + c,\ b + d)$$

But $a + c \in N$ and $b + d \in N$

$\therefore\ (a + c,\ b + d) \in N \times N$. $*$ is binary.

(ii) $$x(yz) = (a, b) * [(c, d) * (e, f)]$$
$$= (a, b) * (c + e,\ d + f)$$
$$= [\,a + (c + e),\ b + (d + f\,)]$$
$$(xy)\,z = [(a, b) * (c, d)] * (e, f)$$
$$= (a + c,\ b + d) * (e, f)$$
$$= [(a + c) + e,\ (b + d) + f]$$

But as $a, b, c, d, e, f \in N$.

$$a + (c + e) = a + c + e = (a + c) + e$$
$$b + (d + f) = b + d + f = (b + d) + f$$

$\therefore$ $*$ is associative. Hence, $(S, *)$ is a semi-group.

(b) Further, we have

$$f(x * y) = f(a + c, b + d)$$
$$= (a + c) - (b + d) = (a - b) + (c - d)$$
$$= f(a, b) + f(c, d) = f(x) + f(y)$$

But $f : S \to Z$ is not onto. Hence, f is homomorphism.

Example 2 : Let $S = N \times N$ and $*$ be the operation on S defined by $(a, b) * (a', b') = (aa', bb')$. Show, that $(S, *)$ is a semi-group. If f is defined by $f : (S, *) \to (Q, *)$ by $f(a, b) = a / b$. show that f is homomorphism.

Sol. : Left to you.

If $x = (a, b),\ y = (c, d),\ z = (e, f)$, note that

$$f(x * y) = f(ac, bd) = (ac) / (bd)$$
$$= (a / b)\,(c / d) = f(x) \times f(y).$$

7. Group

(M.U. 2000, 01, 10)

Definition : An ordered pair $(G, *)$ is called a **group**, if G is a non-empty set and $*$ is a **binary operation** on G satisfying the following axioms.

$G\,1$: For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$.

(*i.e.*, $*$ is **associative** in G)

$G\,2$: There exists an element $e \in G$, such that $e * a = a * e = a$ for all $a \in G$. The element e is called **identity** for $*$.

(*i.e.*, **Identity** e for $*$ exists in G.)

$G3$: For every $a \in G$ there exists an element $b \in G$ such that $a * b = b * a = e$. The element b is called the **inverse** of a and is denoted by a' or by a^{-1}.

(*i.e.*, for every element in G **inverse** exists.)

Abelian or Commutative Group : A group $(G, *)$ is called commutative or Abelian if $a * b = b * a$ for all $a, b \in G$. **(M.U. 2002)**

Most of the groups that we shall be dealing with are commutative *i.e.* Abelian groups. But all groups are not commutative. If M is the set of non-singular $n \times n$ matrices then the set forms a non-commutative group under multiplication. You might have noticed that in general $A \times B = B \times A$ where A and B are non-singular square matrices of the same order.

Examples of Groups

Example 1 : Let $G = \{ x \mid x$ is a real number$\}$ and $a * b = a + b$, the usual addition. Then $(G, *)$ is an Abelian group with 0 as identity and $-a$ as a^{-1}.

Example 2 : Let $G = \{x \mid x$ is a rational number excluding zero$\}$ and $a * b = a \times b$, the usual multiplication.

G is group with 1 as identity and q / p as inverse of p / q.

Example 3 : Let $G = \{0, \pm 1, \pm 2, ...\}$ and $a * b = a + b$ the usual sum of integers. Then $(G, *)$ is an Abelian group with 0 as identity and $-a$ is a^{-1}.

Example 4 : Let $G = \{ x \mid x$ a non-zero real number $\}$ and $a * b = a \times b$, the usual multiplication. Then $(G, *)$ is an Abelian group with 1 as identity and $1/a$ as a^{-1}.

Example 5 : Let $G = \{ z \mid z$ is a complex number $\}$ and $a * b = a + b$, the addition of complex numbers. Then $(G, *)$ is an Abelian group with $0 + i0$ an identity and $-x - iy$ as the inverse of $x + iy$.

Example 6 : Let $G = \{ z \mid z$ is a non-zero complex number $\}$ $a * b = a \times b$, the multiplication of complex numbers. Then $(G, *)$ is an Abelian group with $1 + i \cdot 0$ as identity and $(x - iy) / (x^2 + y^2)$ as inverse of $x + iy$.

Example 7 : Let $G = \{ z \mid z = e^{i0} \}$ and $a * b = a \times b$ usual multiplication of complex numbers. Then $(G, *)$ is an Abelian group with e^{i0} as unity and $e^{-i\theta}$ as inverse of $e^{i\theta}$.

Example 8 : Let $G = \{1, -1\}$ and $a * b = a \times b$ with usual multiplication. Then $(G, *)$ is a group with 1 as identity and each element is inverse of itself.

Examples of Non-Commutative Groups

Example 1 : Let $G = \{ M \mid M$ is a 2×2 non-singular matrix $\}$ and $A * B$ be the usual matrix multiplication. Then $(G, *)$ is a group but **not** an Abelian group. (We shall discuss this problem in detail on page 16-18 in Ex. 12.)

Example 2 : Let $G = \{ (a, b) \mid (a, b)$ is an ordered pair of real numbers, $a \neq 0 \}$ and $(a, b) * (c, d) = (ac, bc + d)$. Then $(G, *)$ is a group but **not** an Abelian group. (See Ex. 11, page 16-17).

To prove that G is a group

Example 1 : Prove that $G = \{1, -1, i, -i\}$ is a group under usual multiplication $*$ of complex numbers. **(M.U. 2002, 05)**

$*$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	1

Sol. : The adjoining table shows the result of multiplication of elements of G.

Since for every pair $a, b \in G$ there exists a unique element $a * b$ in G, $*$ is a binary operation in G.

G 1 : Since multiplication of complex numbers is associative, the multiplication $*$ is associative in G.

G 2 : From the first column (or row) we see that 1 is an identity element. Hence, $1 \in G$ is an identity element.

G 3 : Since $1 * 1 = 1$, $(-1) * (-1) = 1$, $(i) * (-i) = 1$, $(-i) \times (i) = 1$, inverse exists for every elements in G. We have $1^{-1} = 1$, $-1^{-1} = -1$, $i^{-1} = -i$, $-i^{-1} = i$.

Hence, G is a group under multiplication.

Example 2 : Prove that the set of cube-roots of unity is a group under multiplication of complex numbers. **(M.U. 2005)**

$*$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Sol. : We know that the three cuberoots of unity are 1, ω, ω^2, where $\omega = e^{2\pi i/3}$, $\omega^2 = e^{4\pi i/3}$.

The multiplication table is given on the right. The table shows that G is closed under $*$.

G 1 : Since multiplication of complex numbers is associative, multiplication is associative in G

G 2 : From the first row (or column) we find that 1 is the identity element.

G 3 : Since the identity element 1 appears in each row (column) each element has its inverse

$\therefore \quad (1)^{-1} = 1, \quad (\omega)^{-1} = \omega^2, \quad (\omega^2)^{-1} = \omega.$

$\therefore$ Cube-roots of unity is a group under multiplication.

Example 3 : Prove that the set of real numbers is a group under $*$ defined by

$$a * b = a + b - 2.$$

Sol. : Since for every $a, b \in R$, there exists a unique element $a * b = a + b - 2$ in R, $*$ is a binary operation in R.

G 1 : $(a * b) * c = (a + b - 2) * c = (a + b - 2) + c - 2$

$= a + b + c - 4$

And $a * (b * c) = a * (b + c - 2) = a + (b + c - 2) - 2$

$= a + b + c - 4$

$\therefore \quad (a * b) * c = a * (b * c)$ for all $a, b, c \in R$.

$\therefore \quad *$ is associative in R.

G 2 : To find identity e, consider $a * e = a$

But $a * e = a + c - 2$

$\therefore \quad a + e - 2 = a \quad \therefore \quad e = 2. \quad \therefore$ 2 is the identity element.

G 3 : To find inverse of a. Let b be the inverse. Then $a * b = e = 2$

$\therefore \quad a + b - 2 = 2 \quad \therefore \quad b = 4 - a.$

$\therefore \quad 4 - a$ is the inverse of a. $\therefore$ Hence, G is a group under $*$.

Example 4 : Determine whether the following set together with the binary operation $*$ is a semi-group, monoid or a group. Justify your answer.

(a) Set of real numbers with $a * b = a + b + 2$.

(b) The set of $m \times n$ matrices under the operation of multiplication. **(M.U. 2000)**

Sol. : (a) Since for every $a, b \in R$, there exists a unique element $a * b = a + b + 2$ in R, $*$ is a binary operation.

G1 : $(a * b) * c = (a + b + 2) * c = (a + b + 2) + c + 2 = a + b + c + 4$

and $a * (b * c) = a * (b + c + 2) = a + (b + c + 2) + 2 = a + b + c + 4$

$\therefore$ $(a * b) * c = a * (b * c)$ $\therefore$ $*$ is associative in R.

G2 : To find identity, consider $a * e = a$.

$\therefore$ $a + e + 2 = a$ $\therefore$ $e = -2$

$\therefore$ -2 is the identity element.

G3 : To find the inverse. Let b be the inverse of a. Then by definition of the inverse

$a * b = e$ $\therefore$ $a + b + 2 = -2$ $\therefore$ $a + b = -4$ $\therefore$ $b = -4 - a$

Hence, $-4 - a$ is the inverse of a.

$\therefore$ G is a group under $*$.

(b) If A and B are two $m \times n$ matrices, then we know that AB is not defined.

$\therefore$ The operation of multiplication is not binary and hence the set of $m \times n$ matrices under multiplication is not a monoid, a subgroup or a group.

Example 5 : Let G be the set of rational numbers different from 1.

Let $a * b = a + b - ab$ for all $a, b \in G$. Prove that $(G, *)$ is a group. **(M.U. 2005, 13)**

Sol. : Let $a, b \in G$. We shall prove that $a * b = a + b - ab$ is a rational number different from 1 by reduction-ad-absurdum method.

If possible, let $a + b - ab = +1$

$\therefore$ $a - b + b - ab = 0$ $\therefore$ $(a - 1) - b(a - 1) = 0$

$\therefore$ $(a - 1)(-b + 1) = 0$.

Hence, $a = +1$, $b = +1$ which is absurd since $a, b \in G$, the set of rational numbers different from 1.

$\therefore$ $a * b$ is a rational number different from 1 *i.e.* $a * b \in G$.

$\therefore$ $*$ is a binary operation.

G1 : $a * (b * c) = a * (b + c - bc) = a + (b + c - bc) - a(b + c + bc)$

$= a + b + c - bc - ab - ac - abc$

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

$= a + b + c - ab - ac - bc - abc.$

Hence, $a * (b * c) = (a * b) * c$. $\therefore$ $*$ is associative.

G2 : Now $a * 0 = a + 0 + a0 = a$

Also $0 * a = 0 + a + 0a = a$ $\therefore$ $0 \in G$ is the identity element.

G3 : For a given $a, b \in G$ consider the equation $a * b = 0$

i.e., $a + b - ab = 0$. $\therefore$ $b = -\dfrac{a}{1 - a}$.

Since $a * b = a + b - ab = 0$, b is the inverse of G. Since $a \in G$, $a \neq 1$.

$\therefore$ b is rational. Further $b = -\dfrac{a}{1 - a} \neq 1$ because if $b = -\dfrac{a}{1 - a} = 1$

i.e., $-a = 1 - a$ *i.e.*, $0 = 1$ which is absurd.

Hence, b is different from one.

$\therefore \quad b = -\frac{a}{1-a} \in G \qquad \therefore$ b is the inverse of a.

$\therefore \quad a^{-1} = -\frac{a}{1-a}$. Hence, G is a group under $*$.

Example 6 : Prove that if G is the set of all subsets of A, a non-empty set A and $*$ the operation of union, then $(G, *)$ is not a group. **(M.U. 2001)**

Sol. : If A, B are the subsets of A then $A \cup B$ is also a subset of A.

$\therefore$ G is closed under $*$.

G 1 : $A \cup (B \cup C) = (A \cup B) \cup C$.

$\therefore$ $*$ is associative.

G 2 : If Φ denotes empty set.

$A \cup \Phi = A$ and $\Phi \cup A = A \qquad \therefore \quad \Phi \in G$ is identity element.

G 3 : But the inverse of a set $A \in G$ does not exist because we cannot find a non-empty set B such that $A \cup B = \Phi$.

$\therefore$ Inverse does not exist. $\therefore$ $(G, *)$ is not a group.

Example 7 : Let G be a set of all square matrices of type $\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$ where $m \in Z$. Prove that G is a group under multiplication. Is it a Abelian group ? **(M.U. 2002, 03)**

Sol. : Let $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$

$\therefore \quad AB = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix} \in G$

$\therefore$ Multiplication is binary operation.

G 1 : Since matrix multiplication is associative, multiplication in the example is associative.

G 2 : Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$AI = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$. Also $IA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$

$\therefore$ I is identity element.

G 3 : Since $|A| = 1 \neq 0$, inverse of A exists for every $A \in G$.

$\therefore$ $(G, *)$ is a group under multiplication.

Now, $AB = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$ as seen above and $BA = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$

$\therefore \quad AB = BA. \qquad \therefore$ $(G, *)$ is an Abelian group.

Example 8 : Let G be the set of complex numbers for which $|z| = 1$. Is $(G, *)$ a group where $*$ is multiplication of complex numbers ? **(M.U. 2002)**

Sol. : Let $z_1 = x_1 + i y_1$, $z_2 = x_2 + i y_2$ where $|z_1| = 1$, $|z_2| = 1$ *i.e.* $x_1^2 + y_1^2 = 1$, $x_2^2 + y_2^2 = 1$.

$$z_1 z_2 = (x_1 + i y_1)(x_2 + i y_2) = (x_1 x_2 - y_1 y_2) + i (x_1 y_2 + x_2 y_2)$$

Now, $|z_1 z_2|^2 = (x_1 x_2 - y_1 y_2)^2 + (x_1 y_2 + x_2 y_1)^2$

$\therefore$ $= x_1^2 x_2^2 + y_1^2 y_2^2 - 2x_1 x_2 y_1 y_2 + x_1^2 y_2^2 + x_2^2 y_1^2 + 2x_1 x_2 y_1 y_2.$

$= x_1^2 x_2^2 + x_1^2 y_2^2 + y_1^2 x_2^2 + y_1^2 y_2^2$

$= x_1^2 (x_2^2 + y_2^2) + y_1^2 (x_2^2 + y_2^2)$

$= (x_1^2 + y_1^2)(x_2^2 + y_2^2) = 1 \times 1 = 1$

$\therefore$ $|z_1 z_2| = 1$

$\therefore$ $*$ is a binary operation.

$\therefore$ $*$ is associative.

G1 : Multiplication of complex numbers is associative.

$\therefore$ $*$ is associative.

G2 : For any complex number $z = x + iy$, $(x + iy)(1 + i0) = x + iy$

$\therefore$ $(1 + i0)$ whose modulus 1 is the identity element.

G3 : Let $z = x + iy$ and $z^{-1} = x - iy$

$\therefore$ $z * z^{-1} = (x + iy)(x - iy) = x^2 + y^2 = 1$

$\therefore$ For every $z \in G$ the inverse exist.

$\therefore$ Further, since for complex numbers $z_1 z_2 = z_2 z_1$.

$\therefore$ $(G, *)$ is an Abelian group.

Example 9 : If R is the set of all real numbers other than zero and if $a * b = 2ab$, prove that $(R, *)$ is an Abelian group. **(M.U. 2002, 03, 08, 14)**

Sol. : Since $a * b = 2ab \in R$, $*$ is a binary operation in R.

G1 : $a * (b * c) = a * (2bc) = 2a(2bc) = 4abc$

And $(a * b) * c = (2ab) * c = 2(2ab)(c) = 4abc.$

$\therefore$ $*$ is associative.

G2 : Let $a * e = a$ $\therefore$ $2ae = a$ $\therefore$ $e = \frac{1}{2}$

Now, $a * \frac{1}{2} = 2a \cdot \frac{1}{2} = a$, $\frac{1}{2} * a = 2 \cdot \frac{1}{2} a = a.$

$\therefore$ $\frac{1}{2}$ is identity element.

G3 : Let $a * b = e = \frac{1}{2}$ $\therefore$ $2ab = \frac{1}{2}$ $\therefore$ $b = \frac{1}{4a}$

Hence, $\frac{1}{4a}$ is the inverse of a *i.e.* $a^{-1} = \frac{1}{4a}$.

$\therefore$ For every $a \in R$, inverse exists.

Further, $a * b = 2ab$ and $b * a = 2ab$.

$\therefore$ $a * b = b * a.$ $\therefore$ $(R, *)$ is an Abelian group.

Example 10 : Let G be the set of all non-zero real numbers and let $a * b = \frac{ab}{2}$. Show that $(G, *)$ is an Abelian group. **(M.U. 2003, 09, 14)**

Sol. : Since $a * b = \frac{ab}{2}$ and $\frac{ab}{2} \in R$, if $a, b \in R$, $*$ is a binary operation in R.

G 1 : $a * (b * c) = a * \frac{bc}{2} = \frac{a(bc)}{4} = \frac{abc}{4}$ and $(a * b) * c = \frac{ab}{2} * c = \frac{(ab)c}{4} = \frac{abc}{4}$.

$\therefore$ $*$ is associative.

G 2 : Let $a * e = a$ $\therefore$ $\frac{ae}{2} = a$ $\therefore$ $ae = 2a$ $\therefore$ $e = 2$

Now, $a * 2 = \frac{a2}{2} = a$ $\therefore$ 2 is identity element.

G 3 : Let $a * b = e = 2$ $\therefore$ $\frac{ab}{2} = 2$ $\therefore$ $ab = 4$ $\therefore$ $b = \frac{4}{a}$

$\therefore$ $\frac{4}{a}$ is the inverse of a *i.e.*, $a^{-1} = \frac{4}{a}$.

Further $a * b = \frac{ab}{2}$ and $b * a = \frac{ba}{2}$,

$\therefore$ $a * b = b * a$ $\therefore$ $(R, *)$ is an Abelian group.

Example 11 : Determine whether the set A of all ordered pairs (a, b) of real numbers $(a \neq 0)$ under $*$ defined by $(a, b) * (c, d) = (ac, bc + d)$ is an Abelian group. **(M.U. 2003)**

Sol. : If a, b, c, d are real number, we have

$(a, b) * (c, d) = (ac, bc + d)$ and $ac \in R, bc + d \in R$.

$\therefore$ $*$ is a binary operation.

G 1 : Consider

$$[(a, b) * (c, d)] * (e, f) = (ac, bc + d) * (e, f)$$
$$= (ace, bce + de + f)$$
$$(a, b) * [(c, d) * (e, f)] = (a, b) * [(ce, de + f)]$$
$$= (ace, bce + de + f)$$

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

$\therefore$ $*$ is associative.

G 2 : Let $(a, b) * (x, y) = (a, b)$ so that (x, y) is identity element.

$\therefore$ $(ax, bx + y) = (a, b)$

This equality will hold if $x = 1$ and $y = 0$.

$\therefore$ $(1, 0)$ is identity element.

G 3 : Let $(a, b) * (x, y) = (1, 0)$

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

$\therefore$ $x = \frac{1}{a},\ y = -bx = -\frac{b}{a}$ $\therefore$ $(a, b)^{-1} = (x, y) = \left(\frac{1}{a}, -\frac{b}{a}\right)$.

It can be verified that

$$(a, b)\left(\frac{1}{a}, -\frac{b}{a}\right) = \left(1, \frac{b}{a} - \frac{b}{a}\right) = (1, 0)$$

Further, $(a, b) * (c, d) = (ac, bc + d)$ and $(c, d) * (a, b) = (ca, da + b)$

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

$\therefore$ $(R, *)$ is a group but **not** a Abelian group.

Example 12 : Let M be the set of all 2×2 non-singular matrices. Prove that M is a non-commutative group under usual multiplication of matrices. Is M a group under addition of matrices ? Is M a group under matrix multiplication if the condition of non-singularity is removed ?

(M.U. 2007)

Sol. : If $A, B \in M$ then clearly AB is defined and is a 2×2 matrices. Further, $(AB)^{-1} = B^{-1} A^{-1}$. Since the inverse of AB exists, AB is non-singular.

$\therefore$ Multiplication is a binary operation on M.

G1 : The matrix multiplication is associative.

G2 : The identity matrix is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. It is non-singular.

Also $I \in M$, $AI = A = IA$ for all $A \in M$.

G3 : By definition of a non-singular matrix, for $A \in M$ there exist A^{-1} ($\in M$) the inverse of A is such that

$$AA^{-1} = A^{-1}A = I. \qquad \therefore \ M \text{ is a group under multiplication.}$$

Now, to demonstrate that it is a non-abelian group, let

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Since $|A| = |B| = -1$, both A, B are non-singular.

But $AB = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and $BA = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$\therefore \ AB \neq BA. \qquad \therefore \ G$ is **not** Abelian.

For the last part, let $A \in M$ be any matrix. Then $|A| \neq 0$. Also $|-A| = -|A| \neq 0$.

$\therefore (-A)$ is also a non-singular matrix. But $(A) + (-A) = 0$. Hence, the determinant of the sum is zero. The sum is not non-singular and does **not** belong to M *i.e.* M is not closed under addition.

$\therefore$ M is not a group under addition (where M is the set of **non-singular** matrices.)

If M is any matrix then $(M, \times)$ is not a group because inverse does not exist always.

Example 13 : Prove that the set of matrices $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$ where α is real, forms a group under usual matrix production. Is the group Abelian ?

(M.U. 1997, 98, 2004, 05)

Sol. : Let $A_\alpha, A_\beta \in G$.

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

$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} = A_{\alpha+\beta} \in G$$

$\therefore$ $*$ is a binary operation.

G1 : We know that matrix multiplication is associative.

G2 : The unit matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix}$ is identity element.

G 3 : Since $|A_\alpha| = \cos^2\alpha + \sin^2\alpha = 1$, A_α is non-singular, inverse exists.

$$A^{-1} = \frac{1}{|A_\alpha|}\text{adj. } A = \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} = \begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{bmatrix} = A_{(-\alpha)} \in G$$

Further, matrix multiplication is commutative.

$\therefore$ $(A_\alpha, *)$ is an Abelian group.

Example 14 : Let $(G, *)$ be a group. Prove that G is an Abelian group if and only if $(a * b)^2 = a^2 * b^2$ where a^2 stands for $a * a$. **(M.U. 1999, 2002, 08, 14, 16)**

Sol. : (i) Let $(G, *)$ be an Abelian group.

Hence, $a * b = b * a$. ..... (1)

Now, consider

$$\begin{aligned} (a * b)^2 &= (a * b) * (a * b) \\ &= (a * b) * (b * a) && \text{[By (1)]} \\ &= a * (b * b) * a \\ &= a * b^2 * a = a * a * b^2 && \text{[By (1)]} \\ &= a^2 * b^2. \end{aligned}$$

(ii) Let $(a * b)^2 = a^2 * b^2$

Pre-multiplying by a^{-1} and post-multiplying by b^{-1}.

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

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

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

$\therefore$ $e * (b * a) * e = e * (a * b) * e$

$\therefore$ $b * a = a * b$. $\therefore$ G is an Abelian group.

Example 15 : If $(G, *)$ is an Abelian group, then prove that $(a * b)^n = a^n * b^n$ where $a, b \in G$. **(M.U. 2001, 13, 15)**

Sol. : We shall prove the result by the method of mathematical induction.

Step 1 : By data $(a * b)^1 = a^1 * b^1$ $\therefore$ $a * b = a * b$.

$\therefore$ The result is true for $n = 1$.

Step 2 : Let the result be true for $n = k$.

$\therefore$ $(a * b)^k = a^k * b^k$.

Now, multiply both sides by $a * b$.

$\therefore$ $(a * b)^k * (a * b) = a^k * b^k * a * b$

$\therefore$ $(a * b)^{k+1} = a^k * a * b^k * b$ [$\because$ $G, *$ is an Abelian group]

$= a^{k+1} * b^{k+1}$

Hence, the result is true for $n = k + 1$.

Step 3 : Since it is true for $n = 1$, by step 2, it is true for $n = 2$ and since it is true for $n = 2$ again by step 3, it is true for $n = 3$ and so on.

It is true for all n.

Example 16 : Prove that a set of 2×2 rook matrices form a group under matrix multiplication. Is the group abelian ?

Sol. : A rook matrix is a square matrix which has only two elements, 0 and 1 such that each row or each column has exactly one 1.

Obviously there will be only two 2×2 rook matrices given below.

$$M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

There will be four products of the above matrices.

$$M_1 \cdot M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = M_1$$

$$M_1 \cdot M_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = M_2$$

$$M_2 \cdot M_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = M_2$$

$$M_2 \cdot M_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = M_1$$

Thus, we have the following multiplication table.

$*$	M_1	M_2
M_1	M_1	M_2
M_2	M_2	M_1

The table show that M_1 is the identity element.

G 1 : Since there are only two elements, $*$ is trivially associative.

G 2 : M_1 is the identity element.

G 3 : Since $M_1 \cdot M_1 = M_1$ (Identity), M_1 is the inverse of M_1.

Since $M_2 \cdot M_2 = M_1$ (Identity), M_2 is the inverse of M_2.

Further, since $M_2 \cdot M_1 = M_1 \cdot M_2$. $\therefore$ $(M, *)$ is an Abelian Group.

Example 17 : Prove that a set of bijective functions from A to A where $A = (1, 2)$ is a group under composition of functions. Is it Abelian ?

Sol. : Let $A = (1, 2)$ then we have the following two bijective functions on A.

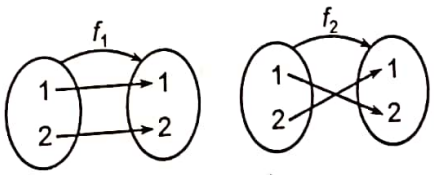

Fig. 16.5

We can obtain four compositions from f_1 and f_2 viz. $f_1 \circ f_1$, $f_1 \circ f_2$, $f_2 \circ f_1$, $f_2 \circ f_2$. Now, prove the remaining part as above.

Example 18 : Prove that z_4 where z_4 denotes the set of integers z modulo 4 is a group under addition but is not a group under multiplication.

Sol. : We first prepare the addition and multiplication tables.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(1) For $(z_4, \oplus)$ se see that

(i) $\oplus$ is associative.

For example, $(1 \oplus 2) \oplus (3) = 3 \oplus 3 = 2$

and $1 \oplus (2 \oplus 3) = 1 \oplus 1 = 2$

(ii) 0 is the identity element.

This, can be seen to be true from the first row or the first column.

$0 + 0 = 0, \quad 1 + 0 = 1, \quad 2 + 0 = 2, \quad 3 + 0 = 3.$

(iii) Additive inverse exists for each element

$0^{-1} = 0, \quad 1^{-1} = 3, \quad 2^{-1} = 2, \quad 3^{-1} = 1$

Hence, $(z_4, \oplus)$ is a group.

(2) For $(z_4, \otimes)$, we see that multiplicative inverse does not exist.

For example, $2 \times 0 = 0, \quad 2 \times 1 = 2, \quad 2 \times 2 = 0, \quad 2 \times 3 = 2$

The product of 2 with no element of z_4 is unity.

Hence, 2^{-1} does not exist. $\therefore$ $(z_4, \otimes)$ is not a group.

In general, if z_m denotes the set of integers modulo m, then z_m is a group under addition but it is not a group under multiplication.

However, if U_m denotes a reduced residue system modulo m which consists of **those integers which are relatively prime to m** (*i.e.* which are not factors or multiples of factors of m), then U_m is a group under multiplication. See the next example.

Example 19 : Show that $U_{12} = \{1, 5, 7, 11\}$ which denotes the reduced residue system modulo 12 is a group under multiplication.

Sol. : We first prepare the multiplication table.

$\otimes$	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) $(u_{12}, \otimes)$ is associative.

For example, $5 \times (7 \times 11) = 5 \times (5) = 1$

and $(5 \times 7) \times 11 = (11) \times 11 = 1$

(2) 1 is the identity element.

This is clear from the first row or from the first column.

(3) Every element has the inverse and the element itself is its inverse.

This is so because all diagonal elements are unity.

$\because \quad 5 \otimes 5 = 1, \quad 5^{-1} = 5$

$\because \quad 7 \otimes 7 = 1, \quad 7^{-1} = 7$

Similarly, $1^{-1} = 1, \quad 11^{-1} = 11.$

Hence, $(u_{12}, \otimes)$ is a group.

Example 20 : Let $S = \{ x \mid x \text{ is real and } x \neq 0, x \neq -1 \}$.

Consider the following functions $f_i : S \to S$, $i = 1, 2, \ldots\ldots, 6$

$$f_1(x) = x, \quad f_2(x) = \frac{1}{x}, \quad f_3(x) = 1 - x, \quad f_4(x) = \frac{x}{1-x}, \quad f_5(x) = \frac{1}{1-x}, \quad f_6 = \frac{x-1}{x}.$$

Show that $G = \{ f_1, f_2, f_3, \ldots\ldots, f_6 \}$ is a group under the operation of composition. Give the multiplication table for G. **(M.U. 2003, 05, 15)**

Sol. : We shall first obtain $f_i \circ f_j$ for all i and j.

$$f_1 \circ f_1 = f_1 \circ (x) = x = f_1$$

$$f_1 \circ f_2 = f_1 \circ \left(\frac{1}{x}\right) = \left(\frac{1}{x}\right) = f_2$$

$$f_1 \circ f_3 = f_1 \circ (1-x) = 1 - x = f_3$$

$$f_1 \circ f_4 = f_1 \circ \left(\frac{x}{1-x}\right) = \frac{x}{1-x} = f_4$$

$$f_1 \circ f_5 = f_1 \circ \left(\frac{1}{1-x}\right) = \frac{1}{1-x} = f_5$$

$$f_1 \circ f_6 = f_1 \circ \left(\frac{x-1}{x}\right) = \frac{x-1}{x} = f_6$$

Further, $f_2 \circ f_1 = f_2 \circ (x) = \frac{1}{x} = f_2$

$$f_2 \circ f_2 = f_2 \circ \left(\frac{1}{x}\right) = \frac{1}{1/x} = x = f_1, \qquad f_2 \circ f_3 = f_2 \circ (1-x) = \frac{1}{1-x} = f_5$$

$$f_2 \circ f_4 = f_2 \circ \left(\frac{x}{x-1}\right) = \frac{x-1}{x} = f_6$$

$$f_2 \circ f_5 = f_2 \circ \left(\frac{1}{1-x}\right) = \frac{1}{1/(1-x)} = 1 - x = f_3$$

$$f_2 \circ f_6 = f_2 \circ \left(\frac{x-1}{x}\right) = \frac{1}{(x-1)/x} = \frac{x}{x-1} = f_4$$

Further since $f_3 = 1 - x$,

$$f_3 \circ f_1 = f_3 \circ (x) = 1 - x = f_3$$

$$f_3 \circ f_2 = f_2 \circ \left(\frac{1}{x}\right) = 1 - \frac{1}{x} = \frac{x-1}{x} = f_6$$

$$f_3 \circ f_3 = f_3 \circ (1-x) = 1 - (1-x) = x = f_1$$

$$f_3 \circ f_4 = f_3 \circ \left(\frac{x}{x-1}\right) = 1 - \frac{x}{x-1} = \frac{-1}{x-1} = \frac{1}{1-x} = f_5$$

$$f_3 \circ f_5 = f_3 \circ \left(\frac{1}{1-x}\right) = 1 - \frac{1}{1-x} = \frac{-x}{1-x} = \frac{x}{x-1} = f_4$$

$$f_3 \circ f_6 = f_3 \circ \left(\frac{x-1}{x}\right) = 1 - \frac{x-1}{x} = \frac{1}{x} = f_2$$

Also since $f_4 = \frac{x}{x-1}$,

$$f_4 \circ f_1 = f_4 \circ (x) = \frac{x}{x-1} = f_4$$

$$f_4 \circ f_2 = f_4 \circ \left(\frac{1}{x}\right) = \frac{1/x}{(1/x)-1} = \frac{1}{1-x} = f_5$$

$$f_4 \circ f_3 = f_4 \circ (1-x) = \frac{1-x}{(1-x)-1} = \frac{1-x}{-x} = \frac{x-1}{x} = f_6$$

$$f_4 \circ f_4 = f_4 \circ \left(\frac{x}{x-1}\right) = \frac{x/(x-1)}{x/(x-1)-1} = x = f_1$$

$$f_4 \circ f_5 = f_4 \circ \left(\frac{1}{1-x}\right) = \frac{1/(1-x)}{1/(1-x)-1} = \frac{1}{x} = f_2$$

$$f_4 \circ f_6 = f_4 \circ \left(\frac{x-1}{x}\right) = \frac{(x-1)/x}{(x-1)/x-1} = \frac{x-1}{-1} = 1-x = f_3$$

To find $f_5 \circ f_1$ ..... $f_5 \circ f_6$ and $f_6 \circ f_1$ ..... $f_6 \circ f_6$ is left to you.

Now we shall see the following.

G_1 : Associativity

$$f_2 \circ f_3 = f_2 \circ (1-x) = \frac{1}{1-x}, \qquad f_1 \circ (f_2 \circ f_3) = f_1 \circ \left(\frac{1}{1-x}\right) = \frac{1}{1-x}$$

Also, $f_1 \circ f_2 = f_2 \circ \frac{1}{x} = \frac{1}{x}$ $\quad \therefore \quad (f_1 \circ f_2) \circ f_3 = (f_1 \circ f_2) \circ (1-x) = \frac{1}{1-x}$

Hence, $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$ $\quad \therefore$ $\circ$ is associative in G.

G_2 : Identity

From the above calculations, we find that f_1 is the identity.

G_3 : Inverse

From the above calculations, we see that every element has an inverse.

For instance inverse of f_1 is f_1, inverse of f_2 is f_2, inverse of f_3 is f_3 and so on. Hence, G is a group under composing.

You can prepare the multiplication table.

Example 21 : Write down all permutations taken 3 at a time of the elements of the set {1, 2, 3}.

Show that this set of permutations of the elements of {1, 2, 3} forms a group under the composition of permutations. **(M.U. 1997, 99, 2000)**

Sol. : The permutations of the elements of the set {1, 2, 3} are

(i) (1, 2, 3); (ii) (1, 3, 2); (iii) (2, 1, 3);

(iv) (2, 3, 1); (v) (3, 1, 2), (vi) (3, 2, 1).

With A = {1, 2, 3} we define the six (functions) permutations as follows.

$P_1(A) = 1, 2, 3$; $P_2(A) = 1, 3, 2$; $P_3(A) = 2, 1, 3$;

$P_4(A) = 2, 3, 1$; $P_5(A) = 3, 1, 2$; $P_6(A) = 3, 2, 1$.

$P_1(A)$ means keeping the same order

e.g., if A = {3, 2, 1} then $P_1(A) = 3, 2, 1$.

$P_6(A)$ means interchanging the first and the last elements

e.g., if A = {3, 2, 1} as above, then $P_6(A)$ = {1, 2, 3}.

Let us denote the set of six permutations (functions) by P.

$\therefore \quad P = \{ P_1(A), P_2(A), ..., P_6(A) \}$

With A = {1, 2, 3} and P_i defined as above we consider the following.

G_1 : Associativity

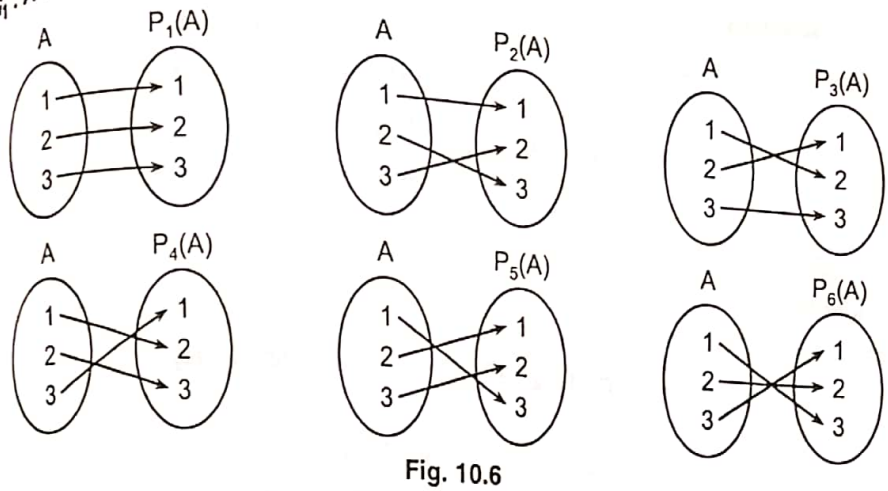

Fig. 10.6

We have, if $A = \{1, 2, 3\}$, then

$P_1(A) = \{1, 2, 3\}$, $P_2(A) = \{1, 3, 2\}$, $P_3(A) = \{2, 1, 3\}$

$P_1(A) \circ P_2(A) = \{1, 3, 2\}$ [$\because$ P_1 maintains the order]

Thus, if $A = \{1, 2, 3\}$, $P_1(A) \cdot P_2(A) = \{1, 3, 2\}$.

$P_1 \circ P_2$ interchanges the last two.

But $P_3(A) = 2, 1, 3.$

$\therefore$ $(P_1 \circ P_2) \circ P_3 = 2, 3, 1$

Now, $P_2(A) \circ P_3(A) = 2, 3, 1$ [$\because$ P_2 interchange the last two]

$\therefore$ $P_1 \circ (P_2 \circ P_3) = 2, 3, 1$ [$\because$ P_1 maintains the order]

$\therefore$ $(P_1 \circ P_2) \circ P_3 = P_1 \circ (P_2 \circ P_3)$

$\therefore$ $\circ$ is associative.

G_2 : Identity

Since, if $A = \{1, 2, 3\}$, $P_1(A) = \{1, 2, 3\}$, we see that P_1 maintains the order

$\therefore$ $P_1 \circ P_2 = P_2$, $P_1 \circ P_3 = P_3$, ..., $P_1 \circ P_k = P_k$.

G_3 : Inverse

We see that $P_1 \circ P_1 = P_1$

$P_2 \circ P_2 = P_2 \circ (1, 3, 2) = (1, 2, 3)$

$= P_1$ [$\because$ P_2 interchanges the last two elements]

$P_3 \circ P_3 = P_3 \circ (2, 1, 3) = (1, 2, 3)$ [$\because$ P_3 interchanges the first two elements]

and so on.

Each function is the inverse of itself. $\therefore$ $(G, \circ)$ is a group.

Example 22 : Let Q be the set of all positive rational numbers which can be expressed as $2^a 3^b$ where a, b are integers.

Prove that $(Q, *)$ is a group where $*$ is usual multiplication. **(M.U. 2002, 06, 12)**

Sol. : We have $2^{a_1} 3^{b_1} * 2^{a_2} 3^{b_2} = 2^{a_1+a_2} 3^{b_1+b_2} = 2^a 3^b$

$\therefore$ G is closed under $*$.

G_1 : Associativity

Consider $(2^{a_1} 3^{b_1}) * (2^{a_2} 3^{b_2} * 2^{a_3} 3^{b_3}) = (2^{a_1} 3^{b_1}) * (2^{a_2 + a_3} 3^{b_2 + b_3})$

$= 2^{a_1 + a_2 + a_3} 3^{b_1 + b_2 + b_3} = 2^a 3^b$

Again $(2^{a_1} 3^{b_1} * 2^{a_2} 3^{b_2}) * 2^{a_3} 3^{b_3} = (2^{a_1 + a_2} 3^{b_1 + b_2}) * 2^{a_3} 3^{b_3}$

$= 2^{a_1 + a_2 + a_3} 3^{b_1 + b_2 + b_3} = 2^a 3^b$

$\therefore$ $(G, *)$ is associative.

G_2 : Identity

If $a = 0, b = 0$, $2^0 3^0 = 1$

$\therefore$ $(2^a 3^b) * (2^0 3^0) = 2^a 3^b \cdot 1 = 2^a 3^b$ $\therefore$ $2^0 3^0$ is an identity.

G_3 : Inverse

Consider $(2^a 3^b) \times (2^{-a} 3^{-b}) = 2^{a-a} 3^{b-b} = 2^0 3^0 = 1$

$\therefore$ $2^{-a} 3^{-b}$ is the inverse of $2^a 3^b$. $\therefore$ $(Q, *)$ is a group.

Example 23 : If S is a non-empty set, prove that the $P(S)$ (power set of S) with $*$ where $A * B$ is defined as symmetric difference is an Abelian group. **(M.U. 2006)**

Sol. : Clearly, if $A, B \in S$, then $A * B$ also belongs to S.

$\therefore$ $P(S)$ is closed under $*$.

G_1 : Associativity

$(A * B) = \{ x \mid x$ belongs to A or $B \}$

$(A * B) * C = \{ x \mid x$ belongs to A or B or $C \}$

$(B * C) = \{ x \mid x$ belongs to B or $C \}$

$A * (B * C) = \{ x \mid x$ belongs to A or B or $C \}$

$\therefore$ $(A * B) * C = A * (B * C)$

$\therefore$ $*$ is associative.

G_2 : Identity

Φ is an identity element.

$A * \Phi = \{ x \mid x$ belongs to A or $\Phi \}$

$= \{ x \mid x$ belongs to $A \}$ [$\because$ Φ has no elements]

$\therefore$ $A * \Phi = A$ for each A.

G_3 : Inverse

Since

$A * \overline{A} = \{ x$ belong to A or $\overline{A} \}$

$= \Phi$ [$\because$ No element belongs to A and $\overline{A}$ simultaneously]

$\therefore$ $\overline{A}$ is the inverse of A.

G_4 : Commutativity

Clearly $A * B = B * A$

$\therefore$ $(G, *)$ is an Abelian group.

Example 24 : Let $(A, *)$ be a monoid such that for every $x \in A$, $x * x = e$ where e is the identity (*i.e.*, every element is its own inverse). Show that $(A, *)$ is an Abelian group. **(M.U. 2000, 01)**

OR If every element in a group is its own inverse then the group is Abelian. **(M.U. 2013, 15)**

Sol. : **(i)** Since $(A, *)$ is a monoid, $*$ is associative over A.

(ii) Since $(A, *)$ is a monoid, it has an identity element.

(iii) Since $x * x = e$ and e is the identity element, for every x, its inverse exists and every element is its inverse.

$\therefore$ $(A, *)$ is a group.

Since by data e is the identity $\quad x * e = e * x = x$

But by data $\quad y * y = e$ ..... (1)

Let us denote $\quad y * y = b.$ ..... (2)

Then from (2), $b = e$ and then from (1), $x * b = b * x$ for all $x \in A$.

$\therefore$ $(A, *)$ is an Abelian group.

(a) Congruence Relation

Definition : If m is any positive integer and if a, b are any integers then a is said to be **congruent to b modulo m** if m divides $(a - b)$ (*i.e.* if $\left(\frac{a-b}{m}\right)$ has zero remainder). **(M.U. 2009)**

We write this as $a \equiv b \pmod{m}$. If the remainder is not zero we write it as $a' \not\equiv b' \pmod{m}$. For example,

(i) $81 \equiv 21 \pmod 5$ $\quad \because$ 5 divides $81 - 21 = 60$.

(ii) $58 \equiv 16 \pmod 7$ $\quad \because$ 7 divides $58 - 16 = 42$.

(iii) $34 \not\equiv 12 \pmod 3$ $\quad \because$ 3 does not divide $34 - 12 = 22$.

(iv) $25 \not\equiv 7 \pmod 4$ $\quad \because$ 4 does not divides $25 - 7 = 18$.

Theorem : Congruence modulo m is an equivalence relation in Z.

Proof : Let m be a positive integer.

(i) If a is any integer $a - a = 0$, is divisible by m.

$\therefore$ $a \equiv \pmod m$ (Reflexivity)

(ii) If $a \equiv b \pmod m$ *i.e.* if $(a - b)$ is divisible by m then $(b - a) = -(a - b)$ is also divisible by m.

$\therefore$ If $a \equiv b \pmod m$, then $b \equiv a \pmod m$ (Symmetry)

(iii) If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $(a - b)$ is divisible by m and $(b - c)$ is divisible by m.

$\therefore$ The sum $(a - b) + (b - c) = a - c$ is also divisible by m.

$\therefore$ If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$ (Transitivity)

$\therefore$ Congruence is an equivalence relation.

Remarks ....

(i) If a is congruent to an integer in the set $S = \{0, 1, 2, ..., (m - 1)\}$ then that integer is **unique**. In other words a cannot be congruent to two integers of the set S.

(ii) If $a \equiv b \pmod m$ then a and b when divided by m leave the same remainder.

(iii) The set obtained from Z modulo m is denoted by Z_m, the operation of addition on Z_m is denoted by $+_m$ and operation of multiplication on Z_m is denoted by $\times_m$.

Sol. : Consider the set { –1, 0, 1 } and prepare the two tables addition modulo 2 and multiplication modulo 2.

$+_2$	–1	0	1
–1	0	–1	0
0	–1	0	1
1	0	1	0

$\times_2$	–1	0	1
–1	1	0	–1
0	0	0	0
1	–1	0	1

Example 2 : Prove that the set $A = \{0, 1, 2, 3, 4, 5\}$ is a finite Abelian group under addition modulo 6. **(M.U. 2004, 05, 07, 09, 13, 16)**

Sol. : We first prepare the table of addition modulo 6 denoted by $\oplus$.

From the table, it is obvious that $\oplus$ is a binary operation.

***G* 1 :** From the table we see that $\oplus$ is associative.

e.g., $2 \oplus (3 \oplus 5) = 2 \oplus (2) = 4$ and $(2 \oplus 3) \oplus 5 = (5) \oplus 5 = 4$.

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	6 = 0
2	2	3	4	5	6 = 0	7 = 1
3	3	4	5	6 = 0	7 = 1	8 = 2
4	4	5	6 = 0	7 = 1	8 = 2	9 = 3
5	5	6 = 0	7 = 1	8 = 2	9 = 3	10 = 4

***G* 2 :** The first column or the first row shows that 0 is the identity for $\oplus$.

***G* 3 :** The positions of 0 the additive inverse in every row (and every column) show that every element of A has the additive inverse. *e.g.,* $1 \oplus 5 = 0$.

Hence, inverse of 1 is 5 and inverse of 5 is 1.

Also $\because\ 3 \oplus 3 = 0 \quad \therefore\ (3)^{-1} = 3$

Further, $2 \oplus 4 = 0 \quad \therefore\ (2)^{-1} = 4$ etc.

$\therefore$ G is a group under addition modulo 6.

***G* 4 :** Further $a \oplus b = b \oplus a$. *e.g.,* $4 \oplus 5 = 3$ and $5 \oplus 4 = 3$

$\therefore\ 4 \oplus 5 = 5 \oplus 4. \quad \therefore$ G is an Abelian group.

Example 3 : Prove that $A = \{ 1, 2, 3, 4, 5, 6 \}$ is a finite Abelian group under multiplication modulo 7. **(M.U. 2010, 11, 12, 14, 15, 17)**

Sol. : We first prepare the table of multiplication modulo 7 denoted by $\otimes$. From the table it is clear that $\otimes$ is a binary operation.

$\otimes$	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

***G* 1 :** From the table, we see that $\otimes$ is associative.

e.g. $2 \otimes (3 \otimes 5) = 2 \otimes 1 = 2$

and $(2 \otimes 3) \otimes 5 = 6 \otimes 5 = 2$

***G* 2 :** The first column (or the first row) show that 1 is the identify for $\otimes$.

G 3 : The positions of the multiplicative identity 1 in every row (and every column) show that every element of A has the multiplicative inverse.

e.g. $2 \otimes 4 = 1$ and $4 \otimes 2 = 1$

$\therefore (2)^{-1} = 4$ and $(4)^{-1}\ 2$

$\therefore$ G is a group modulo 7.

G 4 : Further, $a \otimes b = b \otimes a$

e.g. $4 \otimes 5 = 6$ and $5 \otimes 4 = 6$

$\therefore$ G is an Abelian Group.

Example 4 : Let Z_4 *i.e.*, $G = \{ 0, 1, 2, 3 \}$. (i) Prepare the composition table with respect to X_4. (ii) Is it a group ? **(M.U. 2008)**

Sol. : X_4 denotes the operation of multiplication modulo 4 and composition table means the table in which this operation is shown. (See the adjoining table.)

X_4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

From the table, we see that G is closed under the operation X_4 as all elements in the adjoining table are elements of G.

G 1 : From the table, we see that $\otimes$ is associative.

e.g., $2 \otimes (3 \otimes 1) = 2 \otimes (3) = 2 \otimes 3 = 2$

and $(2 \otimes 3) \otimes 1 = 2 \otimes (1) = 2 \otimes 2 = 2$

G 2 : From the second row (or second column) we see that, 1 is the identity element.

$0 \otimes 1 = 0, \quad 1 \otimes 1 = 1, \quad 2 \otimes 1 = 3, \quad 3 \otimes 1 = 3$

G 3 : In the row (or column) of 2, we see that, $2 \otimes 0 = 0, 2 \otimes 1 = 2, 2 \otimes 2 = 0, 2 \otimes 3 = 2$. Thus, we do not get an identity element and hence, 2 does **not** have a inverse.

$\therefore$ G under multiplication modulo 4 is not a group.

(b) Residue Classes

Since congruence is an equivalence relation, it partitions Z, the set of integers into disjoint equivalence classes called the **residue classes modulo** m. The residue class of a is the set of integers which are congruent to a modulo m. The residue class of a is denoted by $[a]$. Thus, $[a] = \{x \mid x \in Z \text{ and } x \equiv a\}$.

For example, if $m = 5$, we have

$[0] = \{ \ldots\ldots, -10, -5, 0, 5, 10, \ldots\ldots \}$

$[1] = \{ \ldots\ldots, -9, -4, 1, 6, 11, \ldots\ldots \}$

$[2] = \{ \ldots\ldots, -8, -3, 2, 7, 12, \ldots\ldots \}$

$[3] = \{ \ldots\ldots, -7, -2, 3, 8, 13, \ldots\ldots \}$

$[4] = \{ \ldots\ldots, -6, -1, 4, 9, 14, \ldots\ldots \}$

(c) Congruence Relation On Semi-group

Definition : An equivalence relation R on the semi-group $(S, *)$ is called a **congruence relation on the semi-group** if $a\ R\ a'$ and $b\ R\ b'$, then $(a * b)\ R\ (a' * b')$.

Example : Consider the semi-group $(Z, +)$ and the relation R defined by $a\ R\ b$ if and only if $a \equiv b \pmod 3$.

Prove that R is a congruence relation on the semi-group S.

Sol. : Considering the above definition we have to prove that if $a, a', b, b' \in G$ and if $a \, R \, b$ a $a' \, R \, b'$, then $(a * a') \, R \, (b * b')$ *i.e.* we have to prove that if $a \equiv a' \pmod 3$ and $b = b' \pmod 3$ th $a + b = a' + b' \pmod 3$. Now, since $a \equiv a' \pmod 3$, $(a - a') = 3m$ say and since $b \equiv b' \pmod$ $(b - b') = 3n$, say, where m and n are integers.

$$\therefore \quad a - a' + b - b' = 3m + 3n$$

$$\therefore \quad (a + b) - (a' + b') = 3 (m + n)$$

$$\therefore \quad (a + b) \equiv (a' + b') \pmod 3$$

Hence, the result.

(d) Cyclic Group

(M.U. 2000, 1

Definition : A group $(G, *)$ is said to be a **cyclic group** if there exists an element $a \in G$ su that every element of G can be written as some power of a *viz.* a^k for some integer k where by a^k v mean $a \times a \times a \ldots\ldots a$ (k times).

Then G is said to be generated by a or a generates G.

A cyclic group is always Abelian because commutativity is observed,

$\because$ if $a^r, a^s \in G$, then $a^r \times a^s = a^s \times a^r$.

Example 1 : The cube roots of unity form a cyclic group under multiplication of comple numbers.

Sol. : In Example 2, page 16-13, we have proved that the cube roots of unity is a group unde multiplication.

Now, we shall prove that it is cyclic *i.e.*, every element of the group $1, \omega, \omega^2$ can be expresse as integral power of some element $a \in G$.

We note that $\omega^0 = 1, \ \omega^1 = \omega, \ \omega^2 = \omega^2$.

Thus, the element $1, \omega, \omega^2$ are expressed as 0^{th}, 1^{st} and 2^{nd} power of ω. Hence, the group is cyclic with ω as a generator.

Also, $(\omega^2)^0 = 1, \ (\omega^2)^1 = \omega^2, \ (\omega^2)^2 = \omega^4 = \omega^3 \cdot \omega = \omega$.

Thus, $1, \omega, \omega^2$ are expressed as 0^{th}, 1^{st} and 2^{nd} power of ω^2.

Hence, the group is cyclic with ω^2 as a generator.

Example 2 : Prove that the group $G = \{ 0, 1, 2, 3, 4, 5 \}$ is a finite, abelian, cyclic group under addition modulo 6.

Sol. : We have proved in Example 2, page 16-27 that G is an Abelian group.

Now, we shall prove that it is a cyclic group *i.e.*, every element of the group G can be expressed as integral power of some element $a \in G$.

We note that $1^1 = 1, \quad 1^2 = 1 +_6 1 = 2, \quad 1^3 = 1 + 1_6 \, 1^2 = 1 +_6 2 = 3,$

$1^4 = 1 +_6 1^3 = 1 +_6 3 = 4, \quad 1^5 = 1 +_6 1^4 = 1 +_6 4 = 5,$

$1^6 = 1 +_6 1^5 = 1 +_6 5 = 0.$ [See the table on page 16-27]

Hence, $G = \{ 1^6, 1^1, 1^2, 1^3, 1^4, 1^5 \}$.

$\therefore$ G is a cyclic group with 1 as a generator.

(It can be shown that 5 is another generator.)

(e) **Subgroup**

Definition : Let H be a subset of group G, such that (M.U. 2002, 04, 05, 10)

(i) the identity element e of G belongs to H.

(ii) if a, b belong to H then $a * b$ also belongs to H.

(iii) if $a \in H$ then $a^{-1} \in H$. Then H is called a **subgroup** of G.

In short a subgroup is a subset of G having all the properties of a group.

Illustrations : (i) Let G be the group of all non-zero complex numbers $a + ib$ where a, b are real under multiplication.

Let $H = \{ a + ib \mid a^2 + b^2 = 1 \}$ then H is a subgroup of G.

(ii) Let G be the group of 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $ad - bc \neq 0$ under matrix multiplication.

Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix},\ ad \neq 0 \right\}$, then H is a subgroup of G.

Example 1 : Consider the group Z of integers under addition.

Let $H = \{....., -3m, -2m, -m, 0, m, 2m, 3m, ...\}$ where m is a positive integer.

Show that H is a subgroup of Z.

Sol. : **(i)** The identity of element of G is 0 and 0 belongs to H.

(ii) If km and lm are any two elements of H, then

$(km + lm) = (k + l)\, m$ is also an element of H.

(iii) If km is an element of H, then its negative (inverse) km is also an element of H.

$\therefore$ H is a subgroup.

Example 2 : Find the subgroups of $(Z_5, \oplus)$ where $\oplus$ is the operation addition modulo 5. (M.U. 1998)

Sol. : The operation addition modulo 5 is given by the adjoining table.

Addition Modulo 5

$\oplus$	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

From the first row and first column we see that 0 is the identity element.

$\because$ $1 \oplus 4 = 0$, inverse of 1 is 4.

$\because$ $4 \oplus 1 = 0$, inverse of 4 is 1.

Also $2 \oplus 3 = 0$, inverse of 2 is 3.

and $3 \oplus 2 = 0$, inverse of 3 is 2.

Hence, we consider two subgroups of $(Z_5, \oplus)$ viz. $G_1 = \{0, 1, 4\}$ and $G_2 = \{0, 2, 3\}$.

Now, by definition of subgroup H is a subgroup if

(i) the identity element e belongs to H.

(ii) if a, b belongs to H then $a \oplus b$ belongs to H.

(iii) if a belongs to H then a^{-1} belongs to H.

The above properties are satisfied by {0, 1, 4} and {0, 2, 3} under $\oplus$ and hence they are subgroups.

Example 3 : Consider the set $A = \{1, 2, 3, 4, 5, 6\}$ under the multiplication modulo 7.

(i) Construct the multiplication table.

(ii) Find the inverses of 2, 3, 5 and 6.

(iii) Prove that A is a cyclic group.

(iv) Find the subgroups generated by {3, 4} and {2, 3} and state their orders. **(M.U. 1999, 2000, 16)**

$*$	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

Sol. : (i) The multiplication tables is given by the adjoining table.

From the first column and the first row we see that 1 is the identity element.

(ii) From the table we see that $2 * 4 = 1$ and $4 * 2 = 1$.

$\therefore$ Inverse of 2 is 4.

Also since $3 * 5 = 1$ and $5 * 3 = 1$ $\therefore$ Inverse of 3 is 5.

Since $5 * 3 = 1$ and $3 * 5 = 1$ $\therefore$ Inverse of 5 is 3.

Since $6 \times 6 = 1$, inverse of 6 is 6.

(iii) We observe that

$3^1 = 3$, $3^2 = 9_7 = 2$, $3^3 = 27_7 = 6$,

$3^4 = 81_7 = 4$, $3^5 = 243_7 = 5$, $3^6 = 729_7 = 1$.

Thus, each element of A can be written as 3^k.

Hence, (H, $*$ is a cyclic a group) and 3 is its generator.

(iv) The subgroup generated by {3, 4} is denoted by $\langle \{3, 4\} \rangle$.

Clearly the elements (3, 4) belong to the subgroup $\langle \{3, 4\} \rangle$.

The inverse of 3 is 5 and inverse of 4 is 2 and they belong to the subgroup $\langle \{3, 4\} \rangle$.

The identity element 1 belongs to the subgroup.

Thus, the elements 1, 2, 3, 4, 5 belong to the subgroup $\langle \{3, 4\} \rangle$.

Let us check whether the remaining element 6 also belongs to the subgroup.

Now, since $4 \in \langle \{3, 4\} \rangle$ and $5 \in \langle \{3, 4\} \rangle$

$4 * 5$ must belong to the subgroup.

But $4 * 5_7 = 6$. Hence, $6 \in \langle \{3, 4\} \rangle$

$\therefore$ The subgroup of {3, 4} is {1, 2, 3, 4, 5, 6} the set A. Its order *i.e.* the number of elements is 6.

Similarly, you can prove that the subgroup of {2, 3} is the set A itself.

Example 4 : Let G be a reduced system modulo 15 *i.e.*, $G = \{1, 2, 4, 7, 8, 11, 13, 14\}$ (*i.e.*, the set of integers between 1 and 15 which are relatively prime to 15 *i.e.* the integers which are not the factors of 15 or the multiples of the two factors 3, 5 from 1 to 15).

Then, G is a group under multiplication modulo 15.

(1) Construct the multiplication table.

(2) Find 2^{-1}, 7^{-1}, 11^{-1}.

(3) Is G cyclic ?

(4) Find the order and the sub-groups generated by 2, 7, 11.

Sol. : (a) To prepare the multiplication table we find the remainder when the product of any two elements ab is divided 15. We thus get the following table.

⊛	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

From the first row (or the column), we find that 1 is the identity element.

(b) Since 1 is the multiplicative identity b is the inverse of a if $a \otimes b = 1$.

From the table, we find that $2^{-1} = 8$, $7^{-1} = 13$, $11^{-1} = 11$.

(c) Since $2^2 = 4$, $2^3 = 8$, $2^4 = 1$, the sub-group generate by $2 = \{1, 2, 4, 8\}$.

The number of elements in this group *i.e.* the order of this group $| 2 | = 4$.

Since $7^2 = 7 * 7 = 4$, $7^3 = (7 * 7) * 7 = 4 * 7 = 13$, $7^4 = (7 * 7 * 7) * 7 = 13 * 7 = 1$, the sub-group generated by $7 = \{1, 4, 7, 13\}$. The number of elements in the sub-group *i.e.*, $| 7 | = 4$.

Since $11^2 = 1$, the sub-group generate by 11 is $\{1, 11\}$ and $| 11 | = 2$.

(d) Since no element generates G, G is not cyclic.

Example 5 : Consider $G = \{1, 5, 7, 11, 13, 17\}$ a reduced system modulo 18 (*i.e.* the set of integers between 1 and 18 which are relatively prime to 18). Then G is a group under multiplication.

(i) Construct the multiplication table.

(ii) Find $5^{-1}, 7^{-1}, 17^{-1}$.

(iii) Find the order and the sub-groups generated by 5, 7, 17.

(iv) Is G cyclic ?

Sol. : (i) The multiplication table is as shown in adjoining table.

⊗	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

1 is the identity.

(ii) $5^{-1} = 11$, $7^{-1} = 13$, $17^{-1} = 17$.

(iii) Now $5^2 = 5 \circledast 5 = 7$,

$5^3 = 5 \circledast 5 \circledast 5 = 7 \circledast 5 = 17$,

$5^4 = 17 \circledast 5 = 13$,

$5^5 = 13 \circledast 5 = 11$,

$5^6 = 11 \circledast 5 = 1$

$\therefore$ Sub-group of $5 = \{1, 5, 7, 11, 13, 17\} = G$

and $| 5 | = 6$.

i.e., the number of elements in sub-group of 5 is 6. Hence, the order is 6.

Since $7^2 = 7 \circledast 7 = 13$, $7^3 = 13 \circledast 7 = 1$.

Sub-group of $7 = \{1, 7, 13\}$ and $| 7 | = 3$

Since $17^2 = 17 \circledast 17 = 1$, sub-group of $17 = \{1\}$ and $| 17 | = 1$.

(iv) The group G is cyclic. Sub-group of $5 = G$.