5.1 GROUP

5.1.1 Binary Operation.

Let A be a non-empty set. Then $A \times A = \{(a,b) : a, b \in A\}$.

A mapping $f : A \times A \to A$ is called a *binary operation or binary composition* on the set A. In general a binary operation is denoted by $\circ$ or $*$ etc.. The image of the ordered pair (a,b) under the binary operation is denoted by $a \circ b$. Thus if '$\circ$' is a binary operation, then $a \circ b \in A \ \forall \ a, b \in A$ and A is said to be *closed* under the binary operation '$\circ$'.

Illustration. (i) The operation addition is a binary operation on the set of integers Z, as $2 + 5 = 7 \in Z$, $9 + (-1) = 8 \in Z$ and in general $a + b \in Z \ \forall \ a, b \in Z$

(ii) The operation subtraction is not a binary operation on the set of all natural numbers N as $2, 3 \in N$ but $2 - 3 = -1 \notin N$

(iii) The operation '$\circ$' defined by $a \circ b = \frac{ab}{7}$ is a binary operation on the set of all rational numbers Q, as $3 \circ 5 = \frac{3 \times 5}{7} = \frac{15}{7} \in Q$ etc.

Uniary Operation. Let A be a non-empty set.

A mapping $f : A \to A$ is called a uniary operation on the set A. In general a uniary operation is denoted by ' or ~ or – etc.

Illustration.

(i) Let S be a set and $P(S)$ be its power set. i.e. $P(S)$ is set of all subset of S. Let ' (')' be defined as $A' =$ complement of A w.r.t S. Now we see if $A \in P(S)$, $A' \in P(S)$ also.

So $' : P(S) \to P(S)$ is a mapping. So ' is an uniary operation.

(ii) Let $D_{12} = \{1, 2, 3, 4, 6, 12\}$ be the set of all factors of 12. Let '–' be defined as $\bar{n} = \frac{12}{n}$. We see if $n \in D_{12}$ then $\frac{12}{n} \in D_{12}$ also. So $^-$ is a mapping from D_{12} to D_{12}.

So, $^-$ is a uniary Operation.

Commutative Operation. A binary operation $\circ$ is said to be commutative on a set A if $a \circ b = b \circ a \ \forall \ a, b \in A$.

The opertaion addition is commutative on any set but the operation subtraction is not so.

Associative Operation. A binary operation $\circ$ is said to be associative on a set A if $a \circ (b \circ c) = (a \circ b) \circ c \; \forall \; a, b, c \in A$.

The operation multiplication is associative on the set of natural numbers but not the operation subtraction.

5.1.2 Algebraic Structure. A non-empty set A equipped with one or more binary operations is called an *algebraic structure*. We shall denote an algebraic structure with binary operation $\circ$ as $(A, \circ)$ or, $\langle A, \circ \rangle$.

Illustration. $(N, +), (Z, -), (R, +, \bullet)$ are all algebraic structure where $(R, +, \circ)$ is an algebraic structure equipped with two binary operation addition $(+)$ and multiplication $(\bullet)$.

Groupoid. An algebraic structure in which a non-empty set G is equipped with a binary operation say $\circ$ is called a *Groupoid* and is denoted by $(G, \circ)$ or $\langle G, \circ \rangle$.

Thus $(N, +), (Q, \circ), (Z, -)$ and $(Z, +)$ are groupoid.

Composition table. The binary operation $\circ$ defined on a non-empty finite set A can be described by a table, called the *composition table*. If the number of elements of A be n then the table has n rows and n columns. All elements of A are placed in a row at the top and in a column at the left of the table in the same order. Now, if $x, y \in A$ and x lie at the i-th position in the left column of the table, y lie at the j-th position in the top row of the table, then the element $x \circ y$ lie in the table at the intersection of i-th row and j-th column of the table.

Illustration. A composition table of the groupoid $(A, \circ)$ where $A = \{a, b, c\}$ is given below :

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

← top row

↑ left column

Table - 1

It follows from Table–1 that $a \circ a = a$, $a \circ b = b$, $a \circ c = c$, $b \circ a = b$, $b \circ b = c$, $b \circ c = a$, $c \circ a = c$, $c \circ b = a$, $c \circ c = b$.

Identity element : An element e in G is said to be an identity element in the groupoid $(G, \circ)$ if

$$a \circ e = e \circ a = a \quad \forall\, a \in G.$$

If $a \circ e = a \;\forall\, a \in G$ then e is said to be right identity in the groupoid $(G, \circ)$. If $e \circ a = a \;\forall\, a \in G$ then e is said to left identity in the groupoid $(G, \circ)$.

Illustration. In the groupoid $(Q, +)$, 0 is the identity element since $a + 0 = a \;\forall\, a \in Q$ and in the groupoid $(Q, \cdot)$, 1 is the identity element since $a \cdot 1 = a \;\forall\, a \in Q$.

Inverse element : Let e be an identity element of a groupoid $(G, \circ)$ and $a \circ b = b \circ a = e$, then b is called the inverse of a and is denoted by a^{-1}.

If $a \circ b = e$, then b is called the right inverse of a.

Again, if $b \circ a = e$ then b is called left inverse of a.

Illustration. In the groupoid $(Z, +)$, the inverse of any element $x \in Z$ is $-x$, as $x + (-x) = (-x) + x = 0$ (the identity element)

5.1.3 Semi-Group : A groupoid $(G, \circ)$ is said to be a semi-group if the binary operation $\circ$ is associative, i.e. if $a \circ (b \circ c) = (a \circ b) \circ c \;\forall\, a, b, c \in G$.

Illustration. The groupoid $(N, +)$ is a semi-group as $a + (b + c) = (a + b) + c$ holds $\forall\, a, b, c \in N$. But the groupoid $(N, -)$ is not a semi-group, as $a - (b - c) \neq (a - b) - c$.

5.1.4 Monoid : A semi-group with an identity element is called a monoid. Thus 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) there exist an element e in G called identity element such that $a \circ e = e \circ a = a \;\forall\, a \in G$.

Illustration. (i) The groupoid $(Z, \cdot)$ is a monoid, as $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ holds $\forall\, a, b, c \in Z$ and 1 is the identity element belonging to Z.

(ii) The groupoid $(E, \cdot)$ where E is set of all even integers is a semi-group but not a monoid because $1 \notin E$.

5.1.5 Group : A non-empty set G is said to form a *group* with respect to a *operation* $\circ$, if

(i) G is closed under the operation i.e. $a \circ b \in G \;\forall\, a, b \in G$

(ii) $\circ$ is associative i.e., $a \circ (b \circ c) = (a \circ b) \circ c \ \forall\ a, b, c \in G$.

(iii) there exist an identity element e in G such that $a \circ e = a \ \forall\ a \in G$. ($e$ is called right identity element).

(iv) for each element a in G, there exist an inverse element a^{-1} in G such that $a \circ a^{-1} = e$ (a^{-1} is called right inverse of a).

This group is denoted by $(G, \circ)$ or $\langle G, \circ \rangle$.

Abelian Group or Commutative Group.

A group $(G, \circ)$ is said to be *abelian* or *commutative* if $\circ$ is commutative i.e. $a \circ b = b \circ a \ \forall\ a, b \in G$

Otherwise the group is said to be *non-abelian*.

Finite Group & Its Order.

If in a group $(G, \circ)$, the underlying set G consists of a finite number of distinct elements, then the group is called a *finite group* or otherwise *an infinite group*.

The number of elements in a finite group is called the *order* of the group and is denoted by $o(G)$ or $|G|$.

Illustrative Examples.

Ex. 1. *Show that the set of all rational numbers is an abelian group w.r.t addition.*

Let us consider the set of all rational numbers Q with the binary operation addition. Then for any $a, b, c \in Q$ we have,

(i) $a + b \in Q$, as the sum of two rational number is rational

(ii) $a + (b + c) = (a + b) + c$, as the operation addition is associative for all numbers.

(iii) $a + 0 = 0 + a = a \ \forall\ a \in Q$. So, $0 \in Q$ is the identity element.

(iv) $a + (-a) = (-a) + a = 0 \ \forall\ a \in Q$. So the inverse element $(-a)$ exist for each element $a \in Q$.

Hence the set of all rational numbers form a group with respect to addition i.e., $(Q, +)$ is a group.

Again $a + b = b + a \ \forall\ a, b \in Q$. So $(Q, +)$ is an abelian group.

Ex. 2. *Show that the set of all natural numbers is not a group w.r.t multiplication.*

Let us consider the set of all natural numbers N on which operation multiplication is defined. Obviously N is closed with respect to multiplication and the operation multiplication of natural numbers is associative. Also $1 \in N$ is an identity element, as $1 \cdot a = a \cdot 1 = a \; \forall \; a \in N$.

Again $\frac{1}{a} \cdot a = a \cdot \frac{1}{a} = 1 \; \forall \; a \in N$.

So, $\frac{1}{a}$ is the inverse of a but $\frac{1}{a} \notin N$ for $a \neq 1$.

Thus inverse element $\frac{1}{a}$ does not exist for each element $a \in N$. Hence $(N, \cdot)$ is not a group.

5.1.6 Elementary Properties of Groups.

Porperty 1. (Right Cancellation property). If a, b, c are any elements of a group $(G, \circ)$ then

$$b \circ a = c \circ a \Rightarrow b = c$$

Proof. Now $a \in G \Rightarrow a^{-1} \in G$ such that $a \circ a^{-1} = e$, the right identity element.

$$\therefore b \circ a = c \circ a$$

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

$$\Rightarrow b \circ (a \circ a^{-1}) = c \circ (a \circ a^{-1}), \text{ by Associative law}$$

$$\Rightarrow b \circ e = c \circ e \qquad \because a \circ a^{-1} = e$$

$$\Rightarrow b = c \qquad \because e \text{ is right identity element.}$$

Property 2. In a group $(G, \circ)$ the right identity element. is also left identity.

Proof. Let e be the right identity element in $(G, \circ)$.

Then for arbitrary element a $a \circ e = a \; \forall \; a$ in G.

Let a^{-1} be the right inverse of a i.e. $a \circ a^{-1} = e$

Now $(e \circ a) \circ a^{-1} = e \circ (a \circ a^{-1})$, using Assoc. prop.

$$= e \circ e = e = a \circ a^{-1}$$

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

$\therefore e \circ a = a$ by right cancellation property

so e is left identity element.

Property 3. In a group $(G, \circ)$ the right inverse of an element is also its left inverse.

Proof. Let $a \in G$ and e be the right identity element. a^{-1} be the right inverse of a, i.e. $a \circ a^{-1} = e$

Now, $(a^{-1} \circ a) \circ a^{-1} = a^{-1} \circ (a \circ a^{-1})$ by Associative law

$= a^{-1} \circ e = a^{-1} = e \circ a^{-1}$ $\because e$ is left identity

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

or, $a^{-1} \circ a = e$ by Right cancellation property

$\therefore a^{-1}$ is left inverse of a.

An Important Note.

In view of Property 2 and Property 3 we see in a group the right identity and the left identity are same. Henceforth we call them **identity** element in the group. Thus if e is identity element in the group then

$a \circ e = e \circ a = a \; \forall \; a$ in G.

Similarly a^{-1} is called **inverse** of a in G and $a \circ a^{-1} = a^{-1} \circ a = e$

Property 4. In a group $(G, \circ)$

(i) the identity element is unique.

(ii) the inverse of an element is unique.

Proof. (i) Let e and e' be two identity elements of $(G, \circ)$. Then

$e \circ e' = e' \circ e = e'$ [$\because e$ is an identity element and $e' \in G$]

and $e' \circ e = e \circ e' = e$ [$\because e'$ is an identity element and $e \in G$]

Hence $e = e'$ i.e. the identity element is unique.

(ii) Let a' and a'' be two inverses of an element a in G and e be the identity element. Then $a \circ a' = a' \circ a = e$ and $a \circ a'' = a'' \circ a = e$

$\therefore a' \circ a = a'' \circ a$ $\therefore a' = a''$ by right cancellation property

Thus the inverse of an element is unique.

Property 5. In a group $(G, \circ)$, $\left(a^{-1}\right)^{-1} = a \; \forall \; a \in G$

Proof. Let e be the identity element of $(G, \circ)$.

Then $a^{-1} \circ a = a \circ a^{-1} = e$

$[\because a^{-1}$ is the inverse of $a]$. (1)

Again, since $a^{-1} \in G$ and $\left(a^{-1}\right)^{-1}$ exist

so, $(a^{-1})^{-1} \circ a^{-1} = e$ (2)

Thus we have $(a^{-1})^{-1} \circ a^{-1} = a \circ a^{-1}$, by (1) and (2)

$\therefore \left(a^{-1}\right)^{-1} = a$ by right cancellation property.

Note. $e^{-1} = e$, *e being the identity element*

Property 6. In group $(G, \circ)$, $(a \circ b)^{-1} = b^{-1} \circ a^{-1} \; \forall \; a, b \in G$ i.e., the inverse of the product of two elements of a group G is the product of the inverse taken in the reverse order.

[*W.B.U.T. 2008*]

Proof. We have $(a \circ b) \circ \left(b^{-1} \circ a^{-1}\right)$

$= \left[(a \circ b) \circ b^{-1}\right] \circ a^{-1}$ ($\because \circ$ is associative)

$= \left[a \circ \left(b \circ b^{-1}\right)\right] \circ a^{-1}$ (again by associativity)

$= (a \circ e) \circ a^{-1}$ where e is the identity element.

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

Hence $b^{-1} \circ a^{-1}$ is right inverse i.e. inverse of $a \circ b$.

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

Property 7. (Left Cancellation property). If a, b, c are any elements of a group $(G, \circ)$ then

$$a \circ b = a \circ c \Rightarrow b = c$$

Proof. Now $a \in G \Rightarrow a^{-1} \in G$ such that $a \circ a^{-1} = e$

($\because a^{-1}$ is left inverse of a)

$\therefore a \circ b = a \circ c$

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

$\Rightarrow (a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c$ by Associativity

$\Rightarrow e \circ b = e \circ c$

$\Rightarrow b = c$ $\because e$ is left identity also.

Property 8. In a group $(G, \circ)$ for all $a, b \in G$ the equations $a \circ x = b$ and $y \circ a = b$ have unique solutions which are $x = a^{-1} \circ b$ and $y = b \circ a^{-1}$ [*W.B.U.T. 2005*]

Proof. Since $a, b \in G \Rightarrow a^{-1} \in G$ and $b \in G \Rightarrow a^{-1} \circ b \in G$.

We have $a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b$ [$\because \circ$ is associative]

$= e \circ b$, where e is the identity element

$= b$

which shows that $x = a^{-1} \circ b$ is a solution of the equation $a \circ x = b$ in G.

To prove the uniqueness let $x = x_1$ and $x = x_2$ be two solutions of the equation $a \circ x = b$. Then $a \circ x_1 = b$ and $a \circ x_2 = b$

$\therefore a \circ x_1 = a \circ x_2 \Rightarrow x_1 = x_2$, by left cancellation law.

Therefore the solution of the equation $a \circ x = b$ is unique.

Similarly we can prove that $y = b \circ a^{-1}$ is a unique solution of the equation $y \circ a = b$.

Property 9. Let $(G, \circ)$ be a semi-group and for all $a, b \in G$ each of the equations $a \circ x = b$ and $y \circ a = b$ has a solution in G. Then $(G, \circ)$ is a group.

Proof. Since $(G, \circ)$ is a semi-group, G is closed under the binary operation $\circ$ and $\circ$ is associative. So, in order to prove that $(G, \circ)$ is a group, we should show that the identity element exist and each element of G has inverse element.

Since the equation $a \circ x = b$ has a solution $\forall a, b$, so the equation $a \circ x = a$ has a solution say e. Then $a \circ e = a \; \forall a$. Next let c be the solution of $y \circ a = b$. Then $c \circ a = b$

Therefore e is the right identity

Again since $a \circ x = b$ has a solution $\forall b$ in G, so let a' be the solution of the equation $a \circ x = e$ where e is the identity element. Then $a \circ a' = e$ so that a' becomes right inverse of a. Since a is an arbitrary element of G, so right inverse of each element of G exist. Thus $(G, \circ)$ is a group.

Property 10. Let $(G, \circ)$ be a finite semi-group in which both the two cancellation laws hold. Then $(G, \circ)$ is a group.

Proof. Since G is finite set we can suppose

$G = \{a_1, a_2, a_3, \ldots a_n\}$ all a_i s' are distinct.

Let $a, b \in G$ be arbitrary. So $a = a_p$ and $b = a_q$ for some intigers p and q lying between 1 and n.

We shall show the equation $a \circ x = b$ has a solution in G.

Since $a \in G$ so $a \circ a_1, a \circ a_2, a \circ a_3 \ldots a \circ a_n$ all belong to G by closure property of semi - group.

Further they all are distinct because,for $i \neq j$, $a \circ a_i = a \circ a_j \Rightarrow a_i = a_j$, by left cancellation law, which is not possible as $a_1, a_2, a_3, \ldots a_n$ are distinct.

So $a \circ a_1, a \circ a_2, a \circ a_3 \ldots a \circ a_n$ are n distinct elements of G. Since b is an element of G

$\therefore a \circ a_k = b$ for some a_k

i.e. $a \circ x = b$ has a solution which is a_k in G.

Similarly, as Right Cancellation law hold in G, it can be shown that the equation $y \circ a = b$ has a solution in G.

So, by Property 9, $(G, \circ)$ is a group.

Note. *The above theorem is not true if G is infinite. For example, $(N, \cdot)$ is a semi-group in which both cancellation laws hold but $(N, \cdot)$ is not a group.*

Illustrative Examples.

Ex. 1. *Prove that the set of even integers forms an additive abelian group.*

Let E be the set of all even integers. Then

$$E = \{0, \pm 2, \pm 4, \pm 6, \cdots\}$$

Now for any $a, b, c \in E$, we have

(i) $a+b \in E$, as the sum of any two even integers is an even integer.

(ii) $a+(b+c)=(a+b)+c$, as the operation addition is associative for all numbers.

(iii) since $0 \in E$ and $a+0=0+a=a \ \forall \ a \in E$, so 0 is the identity element.

(iv) If $a \in E$, then $-a \in E$ and $a+(-a)=(-a)+a=0$. So $-a$ is the inverse of a. Thus inverse of every element exists.

(v) Again $a+b=b+a \ \ \forall \ a, b \in E$.

Hence E is an abelian group w.r.t the binary operation addition.

Ex. 2. *Show that the set of all odd integers does not form a group* w.r.t *the composition addition.*

As the sum of any two odd integers is an even integer, so the set of all odd integers is not closed w.r.t the composition addition. Hence the set of all odd integers does not form a group w.r.t the composition addition.

Ex. 3. *Show that all roots of the equation* $x^4=1$ *forms a commutative group under the operation multiplication.*

[*W.B.U.Tech 2005, 2007*]

All the roots of the equation $x^4=1$ are $\pm 1, \pm i$.

So we now show that the set $G=\{-1, 1, -i, i\}$ forms a group under the operation multiplication.

Let us form the following composition table :

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(i) From the above table, it is clear that the product of any two elements of G is an element of G. So G is closed.

(ii) Again $(i \cdot 1) \cdot (-i) = i \cdot (-i) = 1$ and $i \cdot (1 \cdot (-i)) = i \cdot (-i) = 1$

$\therefore\ (i \cdot 1) \cdot (-i) = i \cdot (1 \cdot (-i))$ and so on.

Hence the operation multiplication is associative.

(iii) Since $1 \cdot i = i \cdot 1 = i$, $1 \cdot (-1) = (-1) \cdot 1 = -1$ etc., so 1 is the identity element in G.

(iv) From the above table, it is obvious that the inverse of $1, -1, i, -i$ are $1, -1, -i, i$ respectively. Hence inverse of every element of G exists.

(v) As $i \cdot (-i) = (-i) \cdot i$ etc, so the multiplication is commutative.

Hence $(G, \cdot)$ forms a commutative group.

Ex. 4. *Show that the set of rational numbers other than 1, Q' forms a group under the binary operation $*$ defined by* $a * b = a + b - ab\ ;\ a, b \in Q'$

Let $Q' = Q - \{1\}$. Then for $a, b, c \in Q'$ we have

(i) $a * b = a + b - ab \in Q'$.

So Q' is closed under the operation $*$.

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

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

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

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

$$= (a + b - ab) + c - (a + b - ab)\, c$$

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

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

So, the operation $*$ is associative.

(iii) Let e be an identity element in G. Then

$$a * e = a\ \forall\ a \in Q'$$

$\Rightarrow a + e - ae = a$

$\Rightarrow e(1 - a) = 0 \quad \Rightarrow e = 0\ [\because\ a \neq 1]$.

We also see $0 \in Q'$.

So 0 is the identity element

(iv) Let a' be an element in Q' such that $a * a' = 0$.

Then $a + a' - aa' = 0 \quad \Rightarrow a' = \frac{a}{a-1} \in Q' \quad \because a \neq 1$.

So, $\frac{a}{a-1}$ is the inverse of a. Thus inverse of every element in Q' exist.

Hence $Q - \{1\}$ forms a group under the operation $*$.

Ex. 5. *Show that the set G of all ordered pairs (a, b) with $a \neq 0$, of real numbers a, b forms a group with operation '$\circ$' defined by $(a,b) \circ (c,d) = (ac, bc + d)$* [*W.B.U.T. 2007, 2015*]

(i) Let $(a, b), (c, d) \in G$, Then $a \neq 0, \ c \neq 0 \quad \therefore \ ac \neq 0$.

Therefore $(a, b) \circ (c, d) = (ac, bc + d) \in G$, as $ac \neq 0$ and $ac, bc + d$ are real numbers.

So, G is closed under the operation $\circ$.

(ii) Next let $(a, b), (c, d), (e, f) \in G$. Then

$\{(a, b) \circ (c, d)\} \circ (e, f)$

$= (ac, \ bc + d) \circ (e, f) = \{a\, c\, e, (bc + d)e + f\}$

$= (ace, \ bce + de + f)$

and

$(a,b) \circ \{(c,d) \circ (e,f)\} = (a, b) \circ (ce, de + f) \ = (ace, bce + de + f)$

$\therefore \ \{(a, b) \circ (c, d)\} \circ (e, f) = (a, b) \circ \{(c,d) \circ (e,f)\}$

So the operation $\circ$ is associative.

(iii) Let $(x, \ y)$ be the identity element in G. Then

$(x, \ y) \circ (a, b) = (a, b) \ \forall \ (a, b) \in G \quad \Rightarrow (xa, ya + b) = (a, \mathrm{b})$

$\Rightarrow xa = a, ya + b = b \Rightarrow x = 1, \ y = 0 \ [\because a \neq 0]$

So $(1, 0) \in G$ is the identity element.

(iv) Let $(a', \ b')$ be the inverse of $(a, b) \in G$.

Then $(a', b') \circ (a, b) = (1, 0)$

$\Rightarrow (aa', b'a + b) = (1, 0) \Rightarrow aa' = 1, b'a + b = 0$

$\Rightarrow a' = \frac{1}{a}, \ b' = -\frac{b}{a} \ [\because \ a \neq 0]$

So, $\left(\frac{1}{a}, -\frac{b}{a}\right)$ is the inverse of (a, b). Thus the inverse of every element in G exist.

Hence $(G, \circ)$ forms a group.

Note. *Since* $(a,b)\circ(c,d)=(ac,\ bc+d)$ *and*

$(c,d)\circ(a,b)=(ca,da+b)$, *so* $(a,b)\circ(c,d)\neq(c,d)\circ(a,b)$

Thus, $(G,\circ)$ is a non-abelian group.

Ex. 6. *Determine as to whether the set* $P(X)$ *of all subsets of a non-empty set* X, *under the composition* $*$ *defined by the relation*

$A * B = A \cup B,\ A, B \in P(X)$ *constitute group.*

(i) Let $A, B \in P(X)$. Then $A \subseteq X,\ B \subseteq X$

$\therefore\ A \cup B \subseteq X \cup X = X \quad \therefore\ A \cup B \in P(X)$

Hence $A * B = A \cup B \in P(X)$. So $P(X)$ is closed w.r.t the given composition.

(ii) We know that the union of sets is an associative operation. So $A \cup (B \cup C) = (A \cup B) \cup C \ \ \forall\ A, B, C \in P(X)$ and hence

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

Therefore the composition $*$ is associative.

(iii) The empty set ϕ is a subset of X. So $\phi \in P(X)$

Now $A \cup \phi = \phi \cup A = A\ \forall A \in P(X)$

$\therefore\ A * \phi = \phi * A = A\ \ \forall A \in P(X)$

Therefore ϕ is the identity element of $P(X)$

(iv) Let A be any non-empty element of $P(X)$

i.e., let $A \subseteq X$ and $A \neq \phi$. Then for every element A' of $P(X)$, we have $A' * A = A' \cup A \neq \phi$ So inverse element of A does not exist.

Hence $P(X)$ is not a group under the given composition.

Ex. 7. *Show that the set* $G = \left\{a + b\sqrt{2} : a, b \in Q\right\}$ *is a group w.r.t. addition*

(i) Let $x = a + b\sqrt{2} \in G$ and $y = c + d\sqrt{2} \in G$

Then $a, b, c, d \in Q \Rightarrow a+c, b+d \in Q$

$\therefore\ x+y=(a+c)+(b+d)\sqrt{2} \in G \quad \forall\ x, y \in G$

$\therefore$ G is closed w.r.t addition.

(ii) The elements of G are all real numbers and the addition of real numbers is associative.

(iii) As $0 \in Q$ so, $0=0+0\sqrt{2} \in G$. Now if $a+b\sqrt{2} \in G$, then $0+\left(a+b\sqrt{2}\right)=\left(a+b\sqrt{2}\right)$. Therefore 0 is the identity element.

(iv) Since $a, b \in Q \Rightarrow -a, -b \in Q$, so $a+b\sqrt{2} \in G$

$\Rightarrow (-a)+(-b)\sqrt{2} \in G$. Now,

$$\left[(-a)+(-b)\sqrt{2}\right]+\left(a+b\sqrt{2}\right)=(-a+a)+(-b+b)\sqrt{2}=0+0\sqrt{2}=0$$

So, $(-a)+(-b)\sqrt{2}$ is the inverse of $a+b\sqrt{2}$. Hence inverse of every element of G exists. Therefore G is a group w.r.t. addition.

Ex. 8. *Show that the set of all $n \times n$ non-singular real matrices forms a non-abelian group under matrix multiplication.*

Let M be the set of all non-singular $n \times n$ real matrices.

(i) Let $A, B \in M$. Then $|A| \neq 0, |B| \neq 0$

Now $|AB| = |A||B|$ and so $|AB| \neq 0 \quad \therefore\ AB \in M$

$\therefore$ M is closed under matrix multiplication.

(ii) Matrix multiplication is associative on M, as it is defined between any two $n \times n$ real matrices.

(iii) Let I be the unit matrix. So $I \in M$ as $|I| = 1 \neq 0$. Now, $A \cdot I = A\ \forall\ A \in M$. Therefore I is the identity element in M.

(iv) Let $A \in M$. Then $|A| \neq 0$ and so A^{-1} exist.

$$\therefore\ A \cdot A^{-1} = I \quad \Rightarrow \left|AA^{-1}\right| = |I| \quad \Rightarrow |A|\left|A^{-1}\right| = 1.$$

$$\Rightarrow \left|A^{-1}\right| = \frac{1}{|A|} \neq 0 \quad \therefore\ A^{-1} \text{ is non-singular. So, } A^{-1} \in M.$$

Therefore the inverse of every element of M exist.

(v) Again as the matrix multiplication is not in general commutative, so matrix multiplication in M is not commutative.

Hence $(M, \cdot)$ is a non-abelian group.

Note. *When the elements of the matrices are integers, then M is not a group under matrix multiplication because the inverse of every element does not exist.*

For example, the inverse of non-singular matrix $\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$ is $\begin{pmatrix} -2 & \frac{3}{2} \\ 1 & -\frac{1}{2} \end{pmatrix} \notin M$, as all elements of $\begin{pmatrix} -2 & \frac{3}{2} \\ 1 & -\frac{1}{2} \end{pmatrix}$ are not integers.

Ex. 9. *Find the identity element and inverse of an element in the groupoid $(M, \cdot)$ where $M = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \text{ is a non-zero real number} \right\}$.*

Let $E = \begin{bmatrix} e & e \\ e & e \end{bmatrix} \in M$ be such that $EA = A \; \forall A \in M$

Let $A = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$. Then $EA = A \Rightarrow \begin{bmatrix} e & e \\ e & e \end{bmatrix}\begin{bmatrix} a & a \\ a & a \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 2ae & 2ae \\ 2ae & 2ae \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \quad \Rightarrow 2ae = a \Rightarrow e = \frac{1}{2} \; [\because \; a \neq 0]$

Thus $E = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \in M$ and is such that $EA = A \;\; \forall \;\; A \in M$.

Therefore $E = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ is the identity element

Next let $B = \begin{bmatrix} b & b \\ b & b \end{bmatrix} \in M$ be the inverse of $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in M$.

Then $BA = E \Rightarrow \begin{bmatrix} b & b \\ b & b \end{bmatrix}\begin{bmatrix} a & a \\ a & a \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \Rightarrow 2ab = \frac{1}{2} \quad \Rightarrow b = \frac{1}{4a} \; [\because \; a \neq 0]$

Then $B=\begin{bmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{bmatrix} \in M$ is the inverse of $A=\begin{bmatrix} a & a \\ a & a \end{bmatrix}$.

Ex. 10. *Let S be set of all real matrices* $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a^2+b^2=1\right\}$. *Show that S forms a commutative group under matrix multiplication.*

(i) Let $A=\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \in S,\ B=\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \in S$

$\therefore\ a_1^2+b_1^2=1$ and $a_2^2+b_2^2=1$

Now $AB=\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}=\begin{pmatrix} a_1a_2-b_1b_2 & a_1b_2+b_1a_2 \\ -(a_1b_2+a_2b_1) & (a_1a_2-b_1b_2) \end{pmatrix}$

$=\begin{pmatrix} c_1 & c_2 \\ -c_2 & c_1 \end{pmatrix}$ (say)

Since $c_1^2+c_2^2=(a_1a_2-b_1b_2)^2+(a_1b_2+a_2b_1)^2$

$=(a_1^2+b_1^2)(a_2^2+b_2^2)=1\cdot 1=1$. So $AB \in S$.

(ii) Matrix multiplication is associative on S, as it is hold for all $n\times n$ real matrices.

(iii) Now $I=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$ and $AI=A\ \forall\ A \in S$

Therefore $I=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element in S.

(iv) Next let $B=\begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix}$ be the inverse of $A=\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}$

Then $BA=E \Rightarrow \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix}\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\Rightarrow \begin{pmatrix} x_1a_1-y_1b_1 & x_1b_1+y_1a_1 \\ -(a_1y_1+x_1b_1) & x_1a_1-y_1b_1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\Rightarrow\ x_1a_1-y_1b_1=1,\ x_1b_1+y_1a_1=0 \quad \Rightarrow\ x_1=a_1,\ y_1=-b_1$

$\Rightarrow\ B=\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \in S$, as $a_1^2+b_1^2=1$

$\therefore \quad B = \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \in S$ is the inverse of $A = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \in S$. Thus inverse of each element of S exist.

(v) It is obvious by (i) that $AB = BA \; \forall \; A, \; B \in S$. So matrix multiplication is commutative in S.

Hence S forms a commutative group under matrix multiplication.

Ex. 11. *Show that if every element of a group $(G, \circ)$ be its own inverse, then it is an abelian group. Is the converse true ?*

Let $a, b \in G$. Then $a^{-1} = a, \; b^{-1} = b$

Also, $a \circ b \in G$, as G is closed under operation $\circ$.

$\therefore \quad (a \circ b)^{-1} = a \circ b$ or, $b^{-1} \circ a^{-1} = a \circ b$ or, $b \circ a = a \circ b$

Thus, $a \circ b = b \circ a \; \forall \; a, b \in G \quad \therefore (G, \circ)$ is an abelian group.

But the converse is not true. For example $(R, +)$ where R is the set of all real numbers, is an abelian group but no element except 0 is its own inverse.

Ex. 12. *Prove that a group $(G, \circ)$ is abelian if and only if $(a \circ b)^{-1} = a^{-1} \circ b^{-1} \quad \forall \; a, b \in G$*

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

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

$\Rightarrow a \circ b = \left(b^{-1}\right)^{-1} \circ \left(a^{-1}\right)^{-1} \left[\because \left(a^{-1}\right)^{-1} = a \; \forall \; a \in G \right]$

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

Hence $(G, \circ)$ is an abelian group.

Next let $(G, \circ)$ is an abelian group. Then $a \circ b = b \circ a \; \forall \; a, b \in G$

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

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

5.1.7 Integral Power of an element of a Group

Let $(G, \circ)$ be a group and $a \in G$. Then, if n is a positive integer, we define $a^n = a \circ a \circ a \cdots$ to n factors.

Obviously $a^n \in G$, as G is closed. Also we define $a^0 = e$, the identity element of G. As $a^n \in G$, so $\left(a^n\right)^{-1} \in G$. So, we define

$a^{-n} = \left(a^n\right)^{-1}$ where n is a positive integer.

Thus $a^{-n} = (a \circ a \circ a \cdots \text{to } n \text{ factors})^{-1}$

$= a^{-1} \circ a^{-1} \cdots \circ a^{-1}$ to n factors $= \left(a^{-1}\right)^n$.

Illustration

In additive group $(Z, +)$, if n is a positive integer,

we have $a^n = a + a + a + \cdots$ to n terms $= na$; $a^0 =$ the identity element $= 0$ and $a^{-n} = (-a) + (-a) + \cdots + (-a) = -na$

Theorem. In a group $(G, \circ)$

(i) $a^m \circ a^n = a^{m+n}$, (ii) $\left(a^m\right)^n = a^{mn}$, $\forall a \in G$ and $\forall\, m, n \in Z$

Proof. Obvious.

5.1.8 Order of an element of a Group

Let $(G, \circ)$ be a group and $a \in G$. Then the order of a is the least positive integer n such that $a^n = e$, the identity element of G and is denoted by $0(a)$. If there exists no positive integer n such that $a^n = e$, then the order of a is said to be infinity or zero.

For example, we consider the group $(G, \circ)$ where $G = \{1, -1, i, -i\}$. Here 1 is the identity element.

$\therefore\ 0(1) = 1$ as $1^1 = 1$, $0(-1) = 2$ as, $(-1)^2 = 2$, $0(i) = 4$, as $i^4 = 1$, $0(-i) = 4$ as $(-i)^4 = 1$.

Theorem 1. The order of every element of a finite group is finite and is less than or equal to the order of the Group.

Proof. Beyond the scope of the book.

Theorem 2. The order of an element a of a group is the same as that of its inverse a^{-1} i.e., $0(a) = 0\left(a^{-1}\right)$

Proof. Let n and m be the finite orders of a and a^{-1} respectively. Then $0(a) = n \Rightarrow a^n = e$, e being the identity

element.

$$\Rightarrow (a^n)^{-1} = e^{-1} \Rightarrow (a^{-1})^n = e \quad [\because e^{-1} = e]$$

$$\Rightarrow 0(a^{-1}) \leq n \Rightarrow m \leq n \quad \ldots \text{(i)}$$

Also, $0(a^{-1}) = m \Rightarrow (a^{-1})^m = e \Rightarrow (a^m)^{-1} = e$

$$\Rightarrow a^m = e^{-1} \Rightarrow a^m = e \Rightarrow 0(a) \leq m \Rightarrow n \leq m \quad \ldots \text{(ii)}$$

In virtue of (i) and (ii), we have, $n = m$

i.e., $0(a) = 0(a^{-1})$

Next let the order of a be infinite. Then the order of a^{-1} is infinite. Because, if not, then $0(a^{-1}) = m$ (finite)

$\Rightarrow (a^{-1})^m = e \Rightarrow (a^m)^{-1} = e$.

$\Rightarrow a^m = e \Rightarrow o(a) = m \Rightarrow$ order of a is finite. Hence order of a^{-1} is infinite.

Theorem 3. Let a be an element of a group $(G, \circ)$ of order n. Then $a^m = e$ if and only if n is a divisor of m.

Proof. Let n be a divisor of m. Then there exists an integer q such that $nq = m$.

Now, $a^m = a^{nq} = (a^n)^q = e^q = e \quad [\because 0(a) = n \Rightarrow a^n = e]$

Conversely let $a^m = e$.

Since $0(a) = n$, so n is the least positive integer such that $a^n = e$. Again m is an integer. Then by division algorithm, there exist integers q and r such that $m = nq + r, \ 0 \leq r < n$

$$\therefore \ a^m = e \Rightarrow a^{nq+r} = e \Rightarrow a^{nq} \cdot a^r = e \Rightarrow (a^n)^q \cdot a^r = e \Rightarrow e^q \cdot a^r = e.$$

$$\Rightarrow a^r = e$$

Now n is the least positive integer such that $a^n = e$. Since $r < n$, above result is possible if $r = 0$, $\therefore \ m = nq \Rightarrow n$ is a divisor of m.

Theorem 4. If $0(a) = n$, then $a, a^2, a^3, \ldots, a^n (= e)$ are distinct elements of G.

Proof. Left as an exercise.

Theorem 5. Let a be an element of a group $(G, \circ)$ of order n and p is prime to n. Then the order of a^p is also n i.e. $0(a^p) = n$.

Proof. Let $0(a^p) = m$

Then $0(a) = n \Rightarrow a^n = e \Rightarrow (a^n)^p = e^p \Rightarrow (a^p)^n = e$

$\Rightarrow 0(a^p) \le n \Rightarrow m \le n$ ... (i)

Again, since p, n are prime to each other, so there exist integers x and y such that $px + ny = 1$

$$\therefore a = a^{px+ny} = a^{px} \cdot a^{ny} = a^{px} \cdot (a^n)^y = a^{px} \cdot e^y = a^{px} \cdot e = a^{px}$$

$$\therefore a^m = (a^{px})^m = \left[(a^p)^m\right]^x = e^x = e$$

$$\left[\because 0(a^p) = m \Rightarrow (a^p)^m = e\right]$$

$\Rightarrow 0(a) \le m \Rightarrow n \le m$ ... (ii)

In virtue of (i) and (ii) we get $m = n$.

Illustrative Examples.

Ex. 1. *If $x, y \in (G, \circ)$, then show that $0(y)$ and $0(x \circ y \circ x^{-1})$ are same. Hence or otherwise prove that $0(a \circ b) = 0(b \circ a)$.*

Let $0(y) = n$ $\therefore y^n = e$, the identity element.

Now, $(x \circ y \circ x^{-1})^2 = (x \circ y \circ x^{-1}) \circ (x \circ y \circ x^{-1})$

$= x \circ y \circ (x^{-1} \circ x) \circ y \circ x^{-1}$, by associative property

$= x \circ y \circ e \circ y \circ x^{-1} = x \circ y \circ y \circ x^{-1} = x \circ y^2 \circ x^{-1}$

Similarly $(x \circ y \circ x^{-1})^3 = x \circ y^3 \circ x^{-1}$

In general $(x \circ y \circ x^{-1})^n = x \circ y^n \circ x^{-1} = x \circ e \circ x^{-1} = x \circ x^{-1} = e$

If possible; let $(x \circ y \circ x^{-1})^m = e$ where $m < n$

Then $(x \circ y \circ x^{-1})^m = e \Rightarrow x \circ y^m \circ x^{-1} = e$

$\Rightarrow (x^{-1} \circ x) \circ y^m \circ (x^{-1} \circ x) = x^{-1} \circ e \circ x$

$e \circ y^m \circ e = x^{-1} \circ x \Rightarrow y^m = e$ which is impossible as $0(y) = n$ and $m < n$.

Hence n is the least positive integer such that $\left(x \circ y \circ x^{-1}\right)^n = e$.

$\therefore \quad 0\left(x \circ y \circ x^{-1}\right) = n$

Now $a \circ (b \circ a) \circ a^{-1} = (a \circ b) \circ \left(a \circ a^{-1}\right) = (a \circ b) \circ e = a \circ b$

$\therefore \quad 0\left(a \circ (b \circ a) \circ a^{-1}\right) = 0(a \circ b) \Rightarrow 0(b \circ a) = 0(a \circ b)$.

Ex. 2. *If y be an element of a group $(G, \circ)$ and $0(y) = 20$, find the order of y^8.*

Since $0(y) = 20$, $y^{20} = e$, the identity element.

Let $0\left(y^8\right) = n$

$\therefore \quad \left(y^8\right)^n = e$ i.e $y^{8n} = e$ where n is the least positive integer.

Hence 20 is a divisor of $8n$ i.e. 5 is a divisor $2n$

$\therefore \quad n = 5$, as n is the least positive integer $\therefore \quad 0\left(y^8\right) = 5$.

Ex. 3. *If in a group $(G, \circ)$, $a^5 = e$ and $aba^{-1} = b^2 \ \forall \ a, b \in G$ find the order of b.*

Now $\left(aba^{-1}\right)^2 = \left(aba^{-1}\right)\left(aba^{-1}\right) = ab\left(a^{-1}a\right)ba^{-1} = ab\, e\, ba^{-1}$

$= abba^{-1} = ab^2a^{-1} = a\left(aba^{-1}\right)a^{-1} \quad \left[\because b^2 = aba^{-1}\right]$

$= a^2ba^{-2}$

$\therefore \quad \left(aba^{-1}\right)^4 = \left(aba^{-1}\right)^2\left(aba^{-1}\right)^2 = \left(a^2ba^{-2}\right)\left(a^2ba^{-2}\right)$

$= a^2b\left(a^{-2}a^2\right)ba^{-2} = a^2ba\ ba^{-2} \quad \left[\because a^m \cdot a^n = a^{m+n}\right]$

$= a^2bba^{-2} \quad \left[\because a^\circ = e\right]$

$= a^2b^2a^{-2} = a^2\left(aba^{-1}\right)a^{-2} = a^3ba^{-3}$

In this way $\left(aba^{-1}\right)^8 = a^4ba^{-4}$ and

$\left(aba^{-1}\right)^{16} = \left(aba^{-1}\right)^8\left(aba^{-1}\right)^8$

$= \left(a^4ba^{-4}\right)\left(a^4ba^{-4}\right)$

$= a^4ba^{-4}\ a^4ba^{-4}$

$= a^4bba^{-4} = a^4b^2a^{-4} = a^4(aba^{-1})a^{-4} = a^5ba^{-5}$

$= ebe^{-1}$ $[\because\ a^5 = e]$

$= be$ $[\because\ e^{-1} = e] = b$

Thus $(b^2)^{16} = b$ or, $b^{32} = b$ or, $b^{31}bb^{-1} = bb^{-1}$

or, $b^{31} \cdot e = e$

or, $b^{31} = e \Rightarrow 0(b) = 1$ or 31, as 31 is a prime integer.

So if $b = e$, then $0(b) = 1$ and if $b \neq e$, then $0(b) = 31$.

Ex. 4. *Let G be a group. If $a, b \in G$ such that $a^4 = e$, the identity element of G and $ab = ba^2$, prove that $a = e$.* [*W.B.U. Tech 2007*]

We have $ab = ba^2$

$\therefore\ b^{-1}ab = b^{-1}ba^2$

i.e., $b^{-1}ab = ea^2$ $\quad [\because\ b^{-1}b = e]$

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

$\therefore\ (b^{-1}ab)(b^{-1}ab) = a^2 \cdot a^2$

or, $b^{-1}a(bb^{-1})ab = a^4$

or, $b^{-1}a\,e\,ab = e$ $\quad [\because\ a^4 = e, \text{given}]$

or, $b^{-1}a^2b = e$

or, $bb^{-1}a^2b = be$

or, $ea^2b = b$

or, $ba^2b = bb$

or, $(ba^2)b = bb$

or, $ab \cdot b = b \cdot b$ $\quad [\because\ ab = ba^2]$

or, $ab = b$, by right cancellation law

or, $ab = eb$

$\therefore\ a = e$, by right cancellation law.

Ex. 5. *If $(G, \circ)$ is a group such that $(a \circ b)^n = a^n \circ b^n$ for three consecutive integers n and for all $a, b \in G$ then show that G is abelian*

According to the problem, we have

$(a \circ b)^n = a^n \circ b^n$ ... (i)

$(a \circ b)^{n+1} = a^{n+1} \circ b^{n+1}$ ... (ii)

$(a \circ b)^{n+2} = a^{n+2} \circ b^{n+2}$ ... (iii)

Now $(a \circ b)^{n+2} = (a \circ b)^{n+1} \circ (a \circ b)$

$\Rightarrow a^{n+2} \circ b^{n+2} = a^{n+1} \circ b^{n+1} \circ (a \circ b)$ by (ii) and (iii)

$\Rightarrow a \circ \left(a^{n+1} \circ b^{n+1}\right) \circ b = a \circ \left(a^n \circ b^n\right) \circ (b \circ a) \circ b$

$\Rightarrow a^{n+1} \circ b^{n+1} = \left(a^n \circ b^n\right) \circ (b \circ a)$,

by left and right canellationlaw

$\Rightarrow (a \circ b)^{n+1} = (a \circ b)^n \circ (b \circ a)$, by (i) and (ii)

$\Rightarrow (a \circ b)^n \circ (a \circ b) = (a \circ b)^n \circ (b \circ a)$

$\Rightarrow a \circ b = b \circ a$, by left cancellation law

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

Ex. 6. *Prove that a group with three elements is necessarily commutative.*

Let $G = \{a, b, e\}$ form a group under the operation '$\circ$', e being the identity element. Then obviously $e^{-1} = e$. Further, let $a^{-1} = a$, $b^{-1} = b$. So every element of G is its own inverse. Hence

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

$\Rightarrow a \circ b = b^{-1} \circ a^{-1} \quad \Rightarrow a \circ b = b \circ a$

Next let $a^{-1} \neq a$, $b^{-1} \neq b$.

Then, obviously $a^{-1} = e$ or $a^{-1} = b$ and $b^{-1} = e$ or $b^{-1} = a$.

But, $a^{-1} = e \Rightarrow \left(a^{-1}\right)^{-1} = e^{-1} \Rightarrow a = e \quad \left[\because e^{-1} = e\right]$

which is impossible. So $a^{-1} = b$.

Similarly we have $b^{-1} = a$

Now, $a \circ b = a \circ a^{-1} = e$ and $b \circ a = b \circ b^{-1} = e$

$\therefore\ a \circ b = b \circ a$

Also we have $a \circ e = a = e \circ a$ and $b \circ e = b = e \circ b$.

Thus every pair of elements commute.

Hence G forms an abelian group.

Ex. 7. *Show that a group* $(G, \circ)$ *is abelian if and only if* $(a \circ b)^2 = a^2 \circ b^2 \quad \forall\, a, b \in G$. [*W.B.U.T. 2006, 2014*]

First let $(G, \circ)$ be abelian.

Then $(a \circ b)^2 = (a \circ b) \circ (a \circ b)$

$= a \circ (b \circ a) \circ b = a \circ (a \circ b) \circ b$ [$\because$ G is abelian, $a \circ b = b \circ a$]

$= (a \circ a) \circ (b \circ b) = a^2 \circ b^2$

Next let $(a \circ b)^2 = a^2 \circ b^2 \quad \forall\ a, b \in G$

Then $(a \circ b)^2 = a^2 \circ b^2$

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

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

$\Rightarrow b \circ a = a \circ b \ \forall a, b \in G$ [by left and right cancellation law]

Hence $(G, \circ)$ is abelian.

5.1.9. Congruent Modulo *m*. Two integers a and b are said to be congruent modulo m if $a - b$ is divisible by the fixed positive integer m and then we write $a \equiv b \pmod{m}$ which is read as "a is congruent to b modulo m"

For example, $18 \equiv 3 \pmod{5}$ as $18 - 3$ is divisible by 5.

Similarly, $7 \equiv 7 \pmod{7}$, $-22 \equiv 2 \pmod{6}$

Theorem 1. The "congruence modulo m" is an equivalence relation in the set of integers.

Proof. Let Z be the set of all integers and $a \in Z$

Then $a - a = 0$ and 0 is divisible by m.

$\therefore\ a \equiv a \pmod{m} \quad \forall a \in Z$

So the congruence modulo m is reflexive.

Again let $a, b \in Z$ and $a \equiv b \pmod{m}$

Then $a - b$ is divisible by $m \Rightarrow -(b - a)$ is divisible by m

$\Rightarrow (b - a)$ is divisible by m. $\Rightarrow b \equiv a \pmod{m}$

Thus the congruence modulo m is symmetric.

Next let $a, b, c \in Z$ and $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$.

Then $(a-b)$ and $(b-c)$ both are divisible by $m \Rightarrow \{(a-b)+(b-c)\}$ is divisible by $m \Rightarrow (a-c)$ is divisible by $m. \Rightarrow a \equiv c \pmod{m}$

Therefore the congruence modulo m is transitive.

Hence the congruence modulo m is an equivalence relation in the set of integers.

Residue Classes modulo m.

As the congruence modulo m is an equivalence relation in Z, so it forms a partition Z into m disjoint equivalence classes which are called *residue classes modulo m* or *congruence classes modulo m* .

They are denoted by $[0], [1], [2] \cdots [m-1]$, or, $\overline{0}, \overline{1}, \overline{2}, \cdots \overline{m-1}$

where $[a]$(or $\overline{a}$) $= \{x : x \in Z$ and $x - a$ is divisible by $m\}$.

We denote the set of all residue classes modulo m in Z by Z_m. Thus $Z_m = \{ [0], [1], \cdots [m-1] \}$.

The residue class $[0]$ is called the zero residue class.

For example $Z_4 = \{ [0], [1], [2], [3] \}$

where $[0] = \{ 0, \pm 4, \pm 8, \cdots \}$

$[1] = \{ 1, 1 \pm 4, 1 \pm 8, \cdots \}$

$[2] = \{ 2, 2 \pm 4, 2 \pm 8, \cdots \}$

$[3] = \{ 3, 3 \pm 4, 3 \pm 8, \cdots \}$

Theorem 2. The residue classes modulo m, $[0], [1], [2], \cdots [m-1]$ are all distinct and for $n \geq m$, $[n] = [r]$ where r is the least non-negative remainder when n is divided by m.

Proof. Beyond the scope of the book.

Corollary : The class modulo m, $[m] = [0]$.

Addition and Multiplication of Residue Classes.

Let $[a_1], [a_2] \in Z_m$. Then we define $[a_1]+[a_2]=[a_1+a_2]=[a_3]$ where a_3 is the least non-negative remainder when $a_1 + a_2$ is divided by m.

Also we define $[a_1][a_2]=[a_1a_2]=[a_4]$ where a_4 is the least non-negative remainder when a_1a_2 is divided by m.

Theorem 3. The set of residue classes modulo m is an abelian group with respect to addition of residue classes.

Proof. Let Z_m be the set of all residue classes modulo m in Z. Then $Z_m = \{[0], [1], [2], \cdots, [m-1]\}$.

(i) Let $[a_1], [a_2] \in Z_m$ and $[a_1]+[a_2]=[a_1+a_2]=[a_3]$ where a_3 is the least non-negative remainder when $a_1 + a_2$ is divided by m.

$\therefore\ 0 \le a_3 < m \quad \therefore\ [a_3] \in Z_m$

Then Z_m is closed w.r.t addition of residue classes.

(ii) Next let $[a_1], [a_2], [a_3] \in Z_m$. Then $[a_1]+([a_2]+[a_3])$

$=[a_1]+[a_2+a_3]=[a_1+(a_2+a_3)]$

by definition of addition of residue classes

$=[(a_1+a_2)+a_3] \quad =[a_1+a_2]+[a_3] \quad =([a_1]+[a_2])+[a_3]$

So the composition is associative.

(iii) We have $[0] \in Z_m$ and $[0]+[a_1]=[0+a_1]=[a_1]\ \forall [a_1] \in Z_m$.

Therefore [0] is the identity element.

(iv) Let $[r] \neq [0] \in Z_m$. Then $[m-r] \in Z_m$ and $[m-r]+[r]=[m]=[0]$. So, $[m-r]$ is the inverse of $[r]$. Again $[0]+[0]=[0]$. So $[0]$ is the inverse of $[0]$ itself. Thus inverse of each element of Z_m exist.

(v) Again $[a_1]+[a_2]=[a_1+a_2]=[a_2+a_1]=[a_2]+[a_1]$

$\forall [a_1], [a_2] \in Z_m$. So the composition is commutative.

Hence $(Z_m, +)$ is an abelian group.

Theorem 4. The set of non-zero residue classes modulo p forms an abelian group with respect to multiplication of residue classes, where p is a prime integer.

Proof. Let Z_p be the set of all non-zero residue classes modulo p, a prime integer, in Z. Then $Z_p = \{[1], [2], \cdots, [p-1]\}$

(i) Let $[a_1], [a_2] \in Z_p$ and $[a_1]\,[a_2] = [a_1 a_2] = [a_3]$ where a_3 is the least non-negative remainder when $a_1 a_2$ is divided by p.

Since $1 \le a_1 \le p-1$, $1 \le a_2 \le p-1$, and p is prime, so $a_1 a_2$ is not divisible by p. Hence $1 \le a_3 \le p-1$

Consequently $[a_1][a_2] = [a_3] \in Z_p$

$\therefore$ Z_p is closed.

(ii) Let $[a_1], [a_2], [a_3] \in Z_p$.

Then, $([a_1]\,[a_2])[a_3] = [a_1 a_2][a_3] = [(a_1 a_2)a_3] = [a_1(a_2 a_3)]$

[$\because$ multiplication of integers is associative]

$= [a_1][a_2 a_3] = [a_1]([a_2][a_3])$

So the multiplication of residue classes is associative.

(iii) Since $[a_1] \in Z_p$ and $[1][a_1] = [1 \cdot a_1] = [a_1] = [a_1][1]$, $\quad \forall [a_1] \in Z_p$, so $[1]$ is the identity element in Z_p.

(iv) Let $[a] \in G$. Then $1 \le a \le p-1$

Now $[1][a], [2][a], \cdots [p-1]\,[a] \in Z_p$. We shall now show that they are distinct. For this, let $[a_1], [a_2] \in Z_p$ and $a_1 > a_2$ such that $[a_1][a] = [a_2][a]$.

$\Rightarrow [a_1 a] = [a_2 a] \Rightarrow a_1 a - a_2 a$ is divisible by p

$\Rightarrow (a_1 - a_2)a$ is divisible by p

$\Rightarrow a_1 - a_2$ is divisible by p, as a is not divisible by p

But $1 \le a_1 \le p-1$, $\quad 1 \le a_2 \le p-1$

$\Rightarrow 1 \le a_1 - a_2 \le p-1$

So, $a_1 - a_2$ cannot be divisible by p, as p is prime.

So, $[a_1][a] \neq [a_2][a]$. Therefore $[1][a],[2][a],\cdots[p-1][a]$ are distinct elements of Z_p. Hence, one of these elements must be equal to $[1]$. Let $[b][a]=[1]$ for some $[b] \in Z_p$. Then $[b]$ is the inverse of $[a]$. So inverse of each element of Z_p exist.

(v) Now $[a_1][a_2]=[a_1a_2]=[a_2a_1]=[a_2][a_1] \quad \forall\ [a_1],[a_2] \in Z_p$. So the composititon is commutative.

Hence $(Z_p, \times)$ is an abelian group.

Note. (i) *If we include* $[0]$ *in* Z_p, *then* Z_p *will not form a group, as* $[0]$ *has no inverse.*

(ii) *If p is not prime but composite, then there exist two integers a and b such that* $1 < a \leq p-1$, $1 < b \leq p-1$ *and* $ab = p$

Now $ab = p \Rightarrow [ab]=[p] \Rightarrow [a][b]=[0]$, $[\because [p]=[0]]$

$\Rightarrow [a][b] \notin Z_p$

Hence Z_p is not closed under the multiplication of residue classes.

Illustrative Examples.

Ex. 1. *Show that the set of residue classes modulo 5 forms a group of order 5 w.r.t addition of residue classes.*

Let Z_5 denote the set of all residue classes modulo 5. Then $Z_5 = \{[0],[1],[2],[3],[4]\}$.

We construct the following composition table :

+	[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 above table it is seen that

(i) all the entries are elements of the set Z_5. So Z_5 is closed w.r.t addition of residue classes.

(ii) the operation addition of residue classes is associative for example

$([1]+[3])+[4]=[4]+[4]=[3]$ and $[1]+([3]+[4])=[1]+[2]=[3]$

(iii) Since $[0]\in Z_p$ and $[a]+[0]=[a]\ \forall [a]\in Z_p$, so $[0]$ is the identity element in Z_5.

(iv) From the table, we see that the inverse of $[0],[1],[2],[3],[4]$ are $[0],[4],[3],[2],[1]$ respectively. For example $[2]+[3]=[5]=[0]$, the identity element. So $[2]$ is the inverse of $[3]$. Thus inverse of each element of Z_p exist.

Again the number of elements in Z_5 is 6.

Therefore Z_5 forms a group of order 6 w.r.t addition of residue classes.

Note. *It can be easily verified that* $[a]+[b]=[b]+[a]\ \forall [a],[b]\in Z_5$

So addition of residue classes is commutative.

Hence the above group $(Z_5,+)$ is an abelian group.

Ex. 2. *Show that the set of non-zero residue classes modulo 4 does not form a group w.r.t multiplication of residue classes.*

Let Z_4 be the set of all non-zero residue classes. Then $Z_4=\{[1],[2],[3]\}$. Omitting the brackets, we construct the following composition table

×	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

From the above we see that $[2][2]=[0]\notin Z_4$.

So Z_4 is not closed w.r.t multiplication of residue classes. Hence $(Z_4, +)$ does not form a group.

Ex. 3. *Verify whether the set Z_5 of all residue classes modulo 5 form a group w.r.t multiplication of residue classes.*

Here we have $Z_5 = \{[0], [1], [2], [3], [4]\}$

Omitting the bracket, we constract the composition table as given below:

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

From the above table, it is seen that 1 is the identity element in Z_5. But the element 0 has no inverse, as $0 \cdot a \neq 1 \quad \forall\, a \in Z_5$. Hence the set Z_5 does not form a group w.r.t multiplication of residue classes.

EXERCISE

I. SHORT ANSWER QUESTIONS

1. Show that the set S of all real numbers form a semi-group under the operation defined by $a * b = a + b + 2ab \quad \forall\, a, b, \in R$.
2. Construct a composition table of the groupoid $(P, \times_4)$ where $P = \{1,2,3\}$.
3. Show that the identity element of a group is the only element whose order is 1.
4. Show that (Z^+, o) where o is defined by $aob = a \quad \forall a, b, \in Z^+$ is a semi-group . Is it a monoid?
5. If a is an element of a group with identity e such that $a^2 = a$, prove that $a = e$.
6. Prove that the inverse of the inverse of an element of a group is equal to the element itself.
7. Show that $(Q, \cdot)$ does not form a group.

8. Find the order of every element of the group $\{(1,-1,i,-i),\times\}$.

9. Prove that in a group identity element is unique

10. Prove that in a group $(G, *)$ the equation $a*x=b$ has unique solution

11. Prove the set of residue classes modulo 5 form a group w.r.t addition.

12. Show that the set of all residue classes modulo 3 do not form a group w.r.t multiplication of residue classes.

13. If $G=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \text{ is any non-zero real number}\right\}$, then show that G is a commutative group under matrix multiplication.

14. If G be a group such that $(ab)^2 = a^2b^2 \ \forall a,b \in G$ show that the group G is abelian. [*W.B.U. Tech.2006*]

15. Show that the set Z of all integers is an abelian group with the operation '$\circ$' defined by $a \circ b = a+b+2,\ a,b \in Z$.

16. Verify whether the operation '$*$' defined by $a*b = a+b+ab \ \ a,b \in Z$ satisfies all the group axioms ?

17. The non-zero rational numbers form an abelian group under multiplication. What is the identity element and what are its inverse ? [*W.B.U.Tech 2003*]

18. M is the set of matrices of the form $\begin{pmatrix} a & b \\ a & b \end{pmatrix}$ where $a,b \in R$, $a+b \neq 0$. Does $(M, \cdot)$ follow the group axiom ?

19. Let R_0 be the set of all real numbers except zero. Define a binary operation $*$ on R_0 by $a*b = |a|b \ \ \forall \ a,b \in R_0$. Show that (i) $*$ is associative on R_0 (ii) there exists a left identity for $*$ and a right inverse for each element in R_0
Is $(R_0, *)$ a group ?
[Hints : 1 and -1 are both left identity]

20. Prove that if $x^2 = e \ \ \forall x \in G$, then G is a commutative group.

21. In a group G, prove that $(ab)^2 = a^2b^2$ if and only if