Unit 3 Modern Algebra

Structure:

3.1 Introduction

The theory of groups which is a branch of Abstract Algebra is of paramount importance in the development of mathematics.

The idea of group was first given by the French Mathematician Evariste Galois in 1832 who died at the age of 21 years in a duel. The group theory was later developed by an English Mathematician Arthur Cayley. He defined the notion of an abstract group with a general structure which could be applied to numerous particular cases. The theory of groups has applications in Quantum Mechanics and other branches of mathematics.

Objectives:

At the end of the unit you would be able to

- apply the concepts of Algebraic Structure in practical problems
- understand Binary Operations
- Apply Binary Operations in group theory

3.2 Binary Operation

Let G be a non-empty set. Then$G \times G = \{(x, y): x, y \in G\}$. A function f from $G \times G$ in to G is said to be a binary operation on the set G. The image of an ordered pair (x, y) under f is denoted by $x\ f\ y$.

The symbols +*, x, 0, *, ….* are very often used as the binary operations on a set.

Thus,"*" is a binary operation on the set *G* if for every $a, b \in G$ implies $a * b \in G$.

Hence a binary operation * combines any two elements of *G* to give an element of the same set *G.*

Examples:

1. If *Z* is the set of integers then usual addition *(+)* is the binary operation on *Z.* For if *m* and n are two integers then $m + n$ is again an integer i.e. for every $m, n \in Z, m + n \in Z.$
   In particular $-5, 3 \in Z,$ implies $-5 + 3 = -2 \in Z,$ etc.

   Similarly, the usual multiplication is the binary operation on the set Q of rationals, for the product of two rational numbers is again a rational number.
2. Let *E* be the set of even integers. i.e., $E = \{0, \pm 2, \pm 4, \pm 6, ….\}$ and *O* be the set of odd integers i.e. $O = \{\pm 1, \pm 3, \pm 5, ….\}$. Clearly, the usual addition is the binary operation on E whereas it is not a binary operation on *O.* Because the sum of two even integers is even but the sum of two odd integers is not an odd integer.

   Also the usual subtraction is not a binary operation on the set *N* of natural numbers.

Algebraic Structure

A non-empty set with one or more binary operations is called an algebraic structure. If * is a binary operation on *G* then *(G, *)* is an algebraic structure.

For example, the set of integers *Z* is an algebraic structure with usual addition as the binary operation. Similarly *(Q, .), (E, +)* are algebraic structures.

Group

A non-empty set *G* is said to be a group with respect to the binary operation * if the following axioms are satisfied :

1. Closure law. For every $a, b \in G, a * b \in G.$
2. Associative law. For every $a, b, c \in G$
   $a * (b * c) = (a * b) * c$

3. Existence of identity element. There exists an element e $\in$ G such that $a * e = e * a = a$, for every $a \in G$.
   Here "e" is called the identity element
4. Existence of inverse. For every $a \in G$ there exists an element $b \in G$ such that
   $a * b = b * a = e$. Here b is called the inverse of a and is denoted by $b = a^{-1}$. A group G with respect to the binary operation * is denoted by (G, *). If in a group *(G, *)*, $a * b = b *$a for every $a, b, \in G$ then G is said to be commutative or Abelian group named after Norwegian mathematician NielsHenrik Abel *(1802 – 1820).*

Finite and Infinite Groups

A group *G* is said to be finite if the number of elements in the set *G* is finite, otherwise it is said to be an infinite group. The number of elements in a finite group is said to be the order of the group *G* and is denoted by *O(G).*

Example: Prove that the set *Z* of integers is an abelian group with respect to the usual addition as the binary operation.

1. Closure law. We know that the sum of two integers is also an integer. Hence, for every $m, n \in Z, m + n \in Z$.
2. Associative law. It is well known that the addition of integers is associative. Therefore $(m + n) + p = m + (n + p)$ for every $m, n, p \in Z$.
3. Existence of identity element. There exists $0 \in Z$ such that $m + 0 = 0 + m = m$ for every $m \in Z$. Hence *0* is called the additive identity.
4. Existence of inverse. For every $m \in Z$ there exists $– m \in Z$ such that $m + (–m) = (–m) + m = 0$.

   Here – *m* is called the additive inverse of m or simply the negative of m. Therefore *(Z, +)* is a group.
5. Commutative law. We know that the addition of integers is commutative i.e., $m + n = n + m$ for every $m, n \in Z$. Hence *(Z, +)* is an abelian group.
   Since there are an infinite elements in *Z, (Z, +)* is an infinite group.
   Similarly, we can prove that the set *Q* of rationals, the set *R* of reals and the set *C* of complex numbers are abelian groups with respect to usual addition.

Example: Prove that the set Q_0 of all non-zero rationals forms an abelian group with respect to usual multiplication as the binary operation.
Now $Q_0 = Q - \{0\}$

Solution:

1. Closure law. Let $a, b \in Q_0$ i.e. a and b are two non-zero rationals. Then their product $a\ b$ is also a non-zero rational. Hence $a\ b \in Q_0$.

   Since a, b are two arbitrary elements of Q_0, we have for every $a, b, \in Q_0, ab \in Q_0$.
2. Associative law. We know that the multiplication of rationals is associative. i.e.,, $a(b\ c) = (a\ b)\ c$ for every $a, b, c \in Q_0$.
3. Existence of identity element. There exists $1 \in Q_0$ such that $a.1 = 1\ .\ a = a$ for every $a \in Q_0$. Here 1 is called the multiplicative identity element.
4. Existence of inverse. Let $a \in Q_0$. Then "*a*" is a non-zero rational. Therefore $\frac{1}{a}$ exists and is also a rational $\neq 0$.

   Also $a.\frac{1}{a} = \frac{1}{a}.a = 1$ for every $a \in Q_0$.

   $\therefore \frac{1}{a}$ is the multiplicative inverse of *a.*

   Therefore $(Q_0, .)$ is a group.

   Further, it is well-known that the multiplication of rationals is commutative i.e., $ab = ba$ for every $a, b \in Q_0$.
   Hence $(Q_0, .)$ is an abelian group.

   Similarly we can show that the set R_0 of non-zero reals and the set C_0 of non-zero complex numbers are abelian groups w.r.t. usual multiplication.

1. The set *N* of natural numbers is not a group w.r.t. usual addition, for there does not exist the identity element *0* in *N* and the additive inverse of a natural number is not a natural number i.e., for example $2 \in N$ but $-2 \notin N$. Also *N* is not a group under multiplication because $5 \in N$ but $\frac{1}{5} \notin N$.

2. The set of integers is not a group under multiplication for $2 \in Z$ but $\frac{1}{2} \notin Z$.
3. The set of rationals, reals and complex numbers (including 0) do not form groups under multiplication for multiplicative inverse of 0 does not exist.

SAQ 1: Prove that the fourth roots of unity form an abelian group with respect to multiplication.

3.3 Addition Modulo *n*

Let n be a positive integer a and b be any two integers. Then "addition modulo n of two integers a and b", written $a +_n b$, is defined as the least non-negative remainder when $a + b$ is divided by n. If r is the remainder when $a + b$ is divided by n, then

$a +_n b = r$, where $0 \leq r < n$.

In other words, *if* $a + b \equiv r \pmod n$, $0 \leq r < n$. Then $a +_n b = r$.

For example,

$7 +_5 10 = 2$ *since* $7 + 10 = 17 \equiv 2 \pmod 5$

$15 +_7 11 = 5$ *since* $15 + 11 = 26 \equiv 5 \pmod 7$

$17 +_8 21 = 6$ *since* $17 + 21 = 38 \equiv 6 \pmod 8$

$12 +_5 8 = 0$ *since* $12 + 8 = 20 \equiv 0 \pmod 5$

$1 +_7 1 = 2$ *since* $1 + 1 = 2 \equiv 2 \pmod 7$

Properties:

1. Commutative, since $a + b$ and $b + a$ leave the same remainder when divided by n, $a +_n b = b +_n a$.
   For example $5 +_7 6 = 4 = 6 +_7 5$
2. Associative, since $a + (b + c)$ and $(a + b) + c$ leave the same remainder when divided by n, $a +_n (b +_n c) = (a +_n b) +_n c$.
   For example $4 +_6 (3 +_6 5) = (4 +_6 3) +_6 5$

Example: Prove that the set $Z_4 = \{0, 1, 2, 3\}$ is an abelian group w.r.t. addition modulo 4.

Solution: Form the composition table w.r.t. addition modulo *4* as below:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Since $1 + 3 = 4 \equiv 0 \pmod 4$, $3 + 3 = 6 \equiv 2 \pmod 4$ $2 + 3 = 5 \equiv 1 \pmod 4$ etc.

1. Closure law. From the above composition table for all $a, b \in G$, $a +_4 b$ also belongs to Z_4.
2. Associative law. Since $a + (b + c)$ and $(a + b) + c$ leave the same remainder when divided by *4,* we have
   $a +_4 (b +_4 c) = (a +_4 b) +_4 c.$
3. Existence of identity element. From the above table, we observe that $0 \in Z_4$satisfies $a +_4 0 = 0 +_4 a = a$ for every $a \in Z_4$.
   $\therefore$ *0* is the identity element.
4. Existence of inverse. From the above table, the inverses of *0, 1, 2, 3* are respectively *0, 3, 2, 1* because $0 +_4 0 = 0$, $1 +_4 3 = 0$, $2 +_4 2 = 0$, and $3 +_4 1 = 0$.
   Hence $(z_4, +_4)$ is a group
   Further, since $a + b$ and $b + a$ leave the same remainder when divided by *4*, $a +_4 b = b +_4 a$.
   $\therefore$ $(Z_4, +_4)$ is an abelian group.
   Similarly, we can show that the set of remainders of *5* viz.
   $Z_5 = \{0, 1, 2, 3, 4\}$ from an abelian group under addition (mod *5*).
   In general the set of remainders of a positive integer m.
   $Z_m = \{0, 1, 2, \ldots. (m - 1)\}$ form an abelian group under addition (mod *m).*

3.4 Multiplication modulo *n*

Let *n* be a positive integer and*a, b* any two integers. Then multiplication modulo n of two integers a and b, written $a \times_n b$, is defined as the least non-negative remainder when ab is divided by *n.* If r is the remainder when ab is divided by n then $a \times_n b = r$, where $0 \leq r < n$. In other words, if $ab \equiv r \pmod{n}$, $0 \leq r < n$ then $a \times_n b = r$.

For example,
$7 \times_5 3 = 1$ *since* $7 . 3 = 21 \equiv 1 \pmod{5}$
$9 \times_7 5 = 3$ *since* $9 . 5 = 45 \equiv 3 \pmod{7}$
$12 \times_8 7 = 4$ *since* $12 . 7 = 84 \equiv 4 \pmod{8}$
$2 \times_7 3 = 6$ *since* $2 . 3 = 6 \equiv 6 \pmod{7}$
$14 \times_4 6 = 0$ *since* $14 . 6 = 84 \equiv 0 \pmod{4}$

Properties

1. **Commutative:** Since *ab* and *ba* leave the same remainder when divided by *n*,
   $a \times_n b = b \times_n a$
   For example $5 \times_7 4 = 4 \times_7 5$
2. **Associative:** Since *a(bc)* and *(ab)c* leave the same remainder when divided by *n*
   $a \times_n (b \times_n c) = (a \times_n b) \times_n c$
   For example $3 \times_7 (4 \times_7 5) = (3 \times_7 4) \times_7 5$

Example: Prove that the set $Z'_5 = \{1, 2, 3, 4\}$ is an abelian group under multiplication modulo *5.*

Solution: Form the composition table w.r.t. multiplication modulo *5* as below:

x_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Since $2 . 3 = 6 \equiv 1 \pmod{5}$
$2 . 4 = 8 \equiv 3 \pmod{5}$
$4 .4 = 16 \equiv 1 \pmod{5}$ etc.

1. Closure law. Since all the elements entered in the above table are the elements of Z'_5, closure law holds good i.e. for all *a, b* $\in$ *G, a* $\times_5$ *b* also belongs to Z'_5.
2. Associative law. Since *a (bc) and (ab) c* leaves the same remainder when divided by *5,* we have for every *a, b, c* $\in Z'_5$,

   $a \times_5 (b \times_5 c) = (a \times_5 b) \times_5 6.$
3. Existence of identity element. From the above table, we observe that $1 \in Z'_5$ satisfies $a \times_5 1 = 1 \times_5 a = a$ for every $a \in Z'_5$.

   $\therefore$ *1* is the identity element.
4. Existence of inverse. Also the inverses of *1, 2, 3, 4* are respectively *1, 3, 2, 4* because $1 \times_5 1 = 1$, $2 \times_5 3 = 1$, $3 \times_5 2 = 1$, and $4 \times_5 4 = 1.$

   Therefore $(Z'_5\ x_5)$ is an abelian group.

   Similarly, we can show that the non-zero remainders of *7 viz.* $Z'_7 = \{1, 2, 3, 4, 5, 6\}$ form an abelian group under multiplication (mod 7). In general, the non-zero remainders of a positive integer *p* viz. $Z'_p = \{1, 2, 3, \ldots\ldots (p - 1)\}$ form *a* group under multiplication *(mod p)* if and only if *p* is a prime number.

Note: The set $Z'_6 = \{1, 2, 3, 4, 5\}$ does not form a group under multiplication *(mod 6)* for *2, 3* $\in$*G, but* $2 \times_6 3 = 0 \notin G.$ This is because *6* is not a prime number.

3.5 Semigroup

A non-empty set *G* is said to be a semigroup w.r.t. the binary operation if the following axioms are satisfied.

1. **Closure:** For every *a, b,* $\in$ *G, a * b* $\in$ *G*
2. **Associative:** For every *a, b, c* $\in$ *G, a * (b * c) = (a * b) * c.*

Examples:

1. The set N of all natural numbers under addition is a semigroup because for every *a, b, c* $\in$ *N*

   (i) $a + b \in N$, *and (ii)* $a + (b + c) = (a + b) + c.$ The set, *N* is semigroup under multiplication also.
2. The set *Z* of integers is a semigroup under multiplication because for every *a, b* $\in$ *Z, a .b*$\in$ *Z* and for every *a, b, c* $\in$ *Z, a(bc) = (ab) c.* Note

that every group is a semigroup but a semigroup need not be a group. For example, the set *N* of all natural numbers is a semigroup under multiplication (also under addition) but it is not a group. Similarly *Z,* the set of integers is an example of a semigroup but not a group under multiplication.

3.6 Properties of Groups

For the sake of convenience we shall replace the binary operation * by dot"". in the definition of the group. Thus the operation dot .may be the operation of addition or multiplication or some other operation. In what follows by *ab* we mean *a .b or a * b.* With this convention, we rewrite the definition of the group.

Definition: A non-empty set *G* is said to be a group w.r.t. the binary operation. if the following axioms are satisfied.

1. Closure property: For every $a, b \in G, ab \in G$
2. Associative property: For every $a, b, c \in G, a (bc) = (ab) c.$
3. Existence of identity element: There exists an element $e \in G$ such that $ae = ea = a$ for every $a \in G.$ Here *e* is called the identity element.
4. Existence of inverse: For every $a \in G$ there exists an element $b \in G$ such that $ab = ba = e.$ Here *b* is called the inverse of *a i.e.,* $b = a^{-1}$ Further,
5. If $ab = ba$ for every $a, b \in G$ then *G* is said to be an abelian group or a commutative group.

Theorem: The identity element in a group is unique.

Proof: Let e and e' be the two identity elements of a group *G.*Then by definition, for every $a \in G.$

$ae = ea = a$ (1)

and $ae' = e'a = a$ (2)

Substitute $a = e'$ *in (1) and a = e in (2).* Then we obtain

$e'e = ee' = e'$

and $ee' = e'e = e$

Hence $e' = ee' = e'e = e$

$\therefore$ The identity element in a group is unique.

Theorem: In a group *G,* the inverse of an element is unique

Proof: Let b and *c* be the two inverses of an element a in *G.*

Then by definition $ab = ba = e$

$ac = ca = e$

Now consider, $b = be$

$= b(ac)$

$= (ba)\,c$

$= ec$

$= c$

Therefore, inverse of every element in a group is unique

Theorem: If *a* is any element of a group *G,* then $(a^{-1})^{-1} = a.$

Proof: Since a^{-1} is the inverse of a, we have $aa^{-1} = a^{-1}a = e$

This implies that a is an inverse of a^{-1}, but inverse of every element is unique

$\therefore \left(a^{-1}\right)^{-1} = a$

Thus the inverse of the inverse of every element is the same element.

Theorem: If a and b are any two elements of a group G then $\left(ab\right)^{-1} = b^{-1}\,a^{-1}$.

Proof:

Consider, $(ab)\,(b^{-1}\,a^{-1}) = a\left[b\left(b^{-1}\,a^{-1}\right)\right]$

$= a\left[\left(bb^{-1}\right)a^{-1}\right]$

$= a\left[ea^{-1}\right]$

$= aa^{-1}$

$= e$

Similarly we can prove that $\left(b^{-1}\,a^{-1}\right)\left(ab\right) = e$

Hence $\left(ab\right)\left(b^{-1}\,a^{-1}\right) = \left(b^{-1}\,a^{-1}\right)\left(ab\right) = e$

Therefore $b^{-1}\,a^{-1}$ is the inverse of *ab,*

i.e., $\left(ab\right)^{-1} = b^{-1}\,a^{-1}$.

Corollary: If *a, b, c* belong to a group *G* then $(abc)^{-1} = c^{-1}\,b^{-1}\,a^{-1}$etc.

Note: If $(ab)^{-1} = a^{-1}\,b^{-1}$ for all $a, b \in G$, then *G* is abelian.

For, $(ab)^{-1} = a^{-1}\,b^{-1}$ implies $\left[\left(ab\right)^{-1}\right]^{-1} = \left[a^{-1}\,b^{-1}\right]^{-1}$

i.e. $ab = \left(b^{-1}\right)^{-1}\left(a^{-1}\right)^{-1}$

$= ba$ *for all a, b* $\in G$

Hence *G* is abelian.

Theorem: (Cancellation laws).

If *a, b, c*are any three elements of a group G, then

ab = *ac* implies *b* = *c* (left cancellation law)

ba = *ca* implies *b* = *c* (right cancellation law)

Proof: Since a is an element of a group *G,* there exists $a^{-1} \in$ G such that $aa^{-1} = a^{-1}a = e$, the identity element

Now ab = ac

$\Rightarrow$ $a^{-1}(ab) = a^{-1}(ac)$

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

$\Rightarrow$ *eb* = *ec*

$\Rightarrow$ *b* = *c*

Similarly *ba* = *ca*

$\Rightarrow$ $(ba)a^{-1} = (ca)\,a^{-1}$

$\Rightarrow$ $b\left(aa^{-1}\right) = c\left(aa^{-1}\right)$

$\Rightarrow$ *be* = *ce*

$\Rightarrow$ *b* = *c*

Theorem: If a and b are any two elements of a group *G*, then the equations *ax* = *b* and *ya* = *b* have unique solutions in *G*.

Proof:

i) Since $a \in G, a^{-1} \in G.$

Now $a^{-1} \in G$ and *b* $\in$ *G* implies $a^{-1}\,b \in G$ (closure axiom) and $a\left(a^{-1}b\right) = \left(aa^{-1}\right)b = eb = b.$

Hence, $x = a^{-1}$ b satisfies the equation *ax* = *b* and hence is a solution. *If* x_1, x_2 are the two solutions of the equation, *ax* = *b* then $ax_1 = b$ and $ax_2 = b$.

$ax_1 = ax_2$

$x_1 = x_2$ *(By left cancellation law)*

Hence the solution is unique.

ii) Also $b \in G$, $a^{-1} \in G$ implies $ba^{-1} \in G$ and $(ba^{-1})a = b(a^{-1}a) = be = b$

y = ba^{-1} satisfies the equation ya = b and hence is a solution. If y_1, y_2 are two solutions of the equation ya = b then $y_1a = b$ and $y_2a = b$

$\therefore y_1a = y_2a$

$\therefore y_1 = y_2$ *(By right cancellation law)*

Therefore the solution is unique

SAQ 2: Prove that in a group *G* if $a^2 = a$ then $a = e$, the identity element.

Note: Any element a which satisfies $a^2 = a$ is called the idempotent element in a group. Thus e is the only idempotent element in G.

Example: If in group *G*, $(ab)^2 = a^2b^2$ for every $a, b \in G$ prove that *G* is abelian.

Solution:

Now $(ab)^2 = a^2b^2$

$\Rightarrow$ $(ab)(ab) = (a . a)(b . b)$

$\Rightarrow$ $a[b(ab)] = a[a(bb)]$ *(Associative)*

$\Rightarrow$ $b(ab) = a(bb)$ *(Left cancellation law)*

$\Rightarrow$ $(ba)b = (ab)b$ *(Associative)*

$\Rightarrow$ $ba = ab$ *(Right cancellation law)*

Hence *G* is an abelian group.

Example: Show that if every element of a group *G* is its own inverse then *G* is abelian.

Solution: Let $a, b \in G$ then $a^{-1} = a$ and $b^{-1} = b$

Clearly $ab \in G$ $\therefore (ab)^{-1} = ab$ by hypothesis

i.e. $b^{-1}a^{-1} = ab$

i.e. $ba = ab$ since $b^{-1} = b$, $a^{-1} = a$

$\therefore$ *G* is abelian.

3.7 Subgroup

A non-empty subset H of a group *G* is said to be a subgroup of G if under the operation of *G, H* itself forms a group.

If e be the identity element of a group *G*,then *H = { e }* and *H = G* are always subgroups of *G.* These are called the trivial or improper subgroups of G. If *H* is a subgroup of G and $H \neq \{e\}$ and $H \neq G$ then H is called a proper subgroup of G.

Examples:

1. We know that the set Z of integers forms a group under addition. Consider a subset $E = \{2x : x \in Z\} = \{0, \pm 2, \pm 4, \ldots.\}$ of Z. Then E also forms a group under addition.
   Therefore, E is a subgroup of Z.
   Similarly,$F = \{3x : x \in Z\} = \{0, \pm 3, \pm 6, \pm 9, \ldots..\}$ is a subgroup of z.
2. Clearly, the multiplicative group $H = \{1, -1\}$ is a subgroup of the multiplicative group $G = \{1\ -1, i, -i\}$.
3. Let $G = \{1, 2, 3, 4, 5, 6\}$ be a subset of G. *Let* $H = \{1,2,4\}$ Now it is clear from the following composition table that H also forms a group under x_7.

X_7	1	2	4
1	1	2	4
2	2	4	1
4	4	1	2

   Therefore H, is a subgroup of G.

Theorem: A non-empty subset H of a group G is a subgroup of G if and only if

i) for every $a, b \in H$ implies $ab \in H$

ii) for every $a \in H$ implies $a^{-1} \in H$

Note: Union of two subgroups need not be subgroups for, let $H = \{0, \pm 2,, \pm 4, \ldots.\}$ and $K = \{0, \pm 3, \pm 6, \ldots.\}$ be two subgroups of the group of integers Z, so that $H \cup K = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \ldots.\}$.

Now $2, 3 \in H \cup K$ *but* $2 + 3 = 5 \notin H \cup K$ because 5 is neither a multiple of 2 nor a multiple of 3.

3.8 Summary

In this unit we studied that a set which satisfies certain rules is called as a group. Here we studied sub group, semi group etc. with well-illustrated examples.

3.9 Terminal Questions

1. Prove that a non-empty subset *H* of a group *G* is a subgroup of *G* if and only if for every $a, b \in H$ implies $ab^{-1} \in H.$
2. Prove that the intersection of two subgroups of *a* group is again *a* subgroup.

3.10 Answers

Self-Assessment Questions

1. Roots of the equation $x^4 = 1$ are called the fourth roots of unity and they are *1, –1, i, – i. Let G = {1, – 1 i, –i }.*

   From the composition table w.r.t. usual multiplication as follows:

.	1	–1	i	– i
1	1	–1	i	– i
–1	–1	1	– i	i
i	i	– i	–1	1
– i	– i	i	1	–1

1. Closure Law. Since all the elements written in the above composition table are the elements of *G,* we have for all $a, b, \in G,\ ab \in G.$
2. Associative Law. We know that the multiplication of complex numbers is associative and *G* is a subset of the set of complex numbers

   Hence $a(bc) = (ab)\,c$ for all a, b, c $\in$ G.
3. Existence of identity element. From the composition table, it is clear that there exists $1 \in G$ satisfying $a \,.\, 1 = 1 \,.\, a = a$ for every $a \in G.$

   Therefore *1* is the identity element.
4. Existence of inverse. From the composition table we observe that the inverses of *1, – 1, i – i are 1, -1, -i, i.*

   Thus for every $a \in G$ there exists $a^{-1} \in$ G such that $a\, a^{-1} = a^{-1}a = 1,$ the identity element. Hence *(G, .)* is a group.

   Further multiplication of complex numbers is commutative.

   Therefore *ab* = *ba*for every a, b $\in$ G.

Also we observe that the elements are symmetric about the principal diagonal in the above composition table. Hence commutative law holds good.

Therefore *(G, .)* is an abelian group.

Note that *G* is a finite group of order *4*.

2. Now $a^2 = a \Rightarrow a\,.\,a = a\,.\,e$ since $a = ae \Rightarrow a = e$ *(by right cancellation law.)*