**UNIT-III**

**GROUPS**

**BINARY OPERATION:** Let S be a non-empty set. Then any function o : S  SS is called a binary operation in S. If a, b, S, then we write o (a, b) = a o b.

**CLOSURE PROPERTY:** A non-empty set S is said to be closed under an operation ‘o’ if (a, b) S  aobS. Every non-empty set is closed under the binary operation defined on it.

**GROUPOID:** A non-empty set S together with a binary operation o on it is called a groupoid and is denoted by (S, o).

**EXAMPLES:** (N, +), (N, . ), (Z, +), (Z, . ), (Z, –), (Q, +), (Q, –), (Q, . ), (Q, – {0}, ), (R+, +), (R, –), (R, . ), (R – {0}, ), (C, +), (C, –), (C, . ), (C, ) are examples of groupoid (N, –) is not a groupoid because 5, 7 N but 5 – 7 N.

**SEMI-GROUP:** Let S be a non-empty set and o be a binary operation in S. Then (S, o) is called a semi-group if ao(boc) = (aob) oc  a, b, c S [Associative Law].

**EXAMPLES:** (N, +), (N, . ), (Z, +), (Z, . ), (Q, +), (Q, . ), (R, +), (R, . ), (C, +), (C, . ) are all examples of semi-group.

**GROUP:** A non-empty set G with a binary operation o is called a group if the following conditions are satisfied:

(i) a o (boc) = (aob) oc  a, b, c G [Associative Law].

(ii) There exists an element e G such that aoe = a = eoa a G [Existence of identity element].

(iii) For each a G,  b G such that aob = e = boa [Existence of inverse].

**ABELIAN GROUP:** A group (G, o) is said to be abelian if aob = boa a, b G.

**FINITE GROUP:** A group (G, o) is said to be finite if the set G is finite.

**EXAMPLES OF GROUPS**

**Examples 1:** (Z, +) is an abelian group.

**Solution:**

**(i)** **Closure property:** We know that the addition of two integers is an integer. Thus, a, b Z  a + b Z.

**(ii)** **Associative law:** We know that addition of integers is associative. Thus, a + (b +c) = (a + b) + c a, b, c Z.

**(iii)** **Existence of identity element:** The number 0Z and a + 0 = a = 0 + a a Z.

  0 is the identity element.

**(iv) Existence of Inverse:** Let a Z. Then – a Z and a + (–a) = Z = (–a) + a. Thus, –a is the inverse of a. Hence, (Z, +) is a group.

**(Z, +) is abelian:** Since, a + b = b + a  a, b  Z.

 (Z, +) is abelian. Hence (Z, +) is an abelian group.

**Examples 2:** (Q, +) is an abelian group.

**Examples 3:** (R, +) is an abelian group.

**Example 4:** Let C be the set of all complex numbers. Then C is an abelian group under addition of complex numbers.

**Solution:**

**(i)** **Closure property:** We know that addition of two complex numbers is a complex number. Thus, z1, z2,  C  z1 + z2 C.

**(ii)** **Associative law:** We know that addition of complex numbers is associative. Thus, z1 + (z2 + z3) = (z1 + z2) + z3  z1, z2, z3  C.

**(iii)** **Existence of Identity:** The number 0 = 0 + i 0  C and for all z = a + i bC

 z + 0 = (a + ib) + (0 + i0)

 = a + ib

 = (0 + i0) (a + ib)

 = 0 + z

 Thus, 0 = 0 + i 0 is the identity element.

**(iv)** **Existence of Inverse:** Let z = a + ibC. Their – z = – a – ib C and z + (–z) = 0 + i0 = (–z) + z

  – z is the inverse of z. Thus, (C, +) is a group.

**(C, +) is abelian:** Since z1 + z2 = z2 + z1  z1, z2 C.

 (C, +) is abelian. Hence (C, +) is an abelian group.

**Examples 5:** The set of all non-zero rational numbers is a group under multiplication.

**Solution:** Let Q\* denote the set of all non-zero rational numbers.

**(i)** **Closure property:** We know that multiplication of two non-zero rational numbers is a non-zero rational number. Thus, a, b Q\*  a . b Q\*.

**(ii)** **Associative law:** We know that multiplication of rational numbers is associative. Thus, a. (b.c) = (a.b). c  a, b, c Q\*.

**(iii)** **Existence of identity:** The number 1Q\* and a . 1 = a = 1 . a  a Q\*. Thus, 1 is the identity element.

**(iv)** **Existence of inverse:** Let a Q\*. Then Q\* and a. = 1 =  . a. Thus,  is the inverse of a.

  (Q\*, . ) is a group.

**(Q\*, . ) is abelian:** Since a . b = b . a a, b Q\* so (Q\*, . ) is an abelian group.

**Examples 6:** The set R\* of all non-zero real numbers is a group under multiplication.

**Example 7:** The set C\* of non-zero complex numbers is an abelian group under multiplication of complex numbers.

**Solution:**

**(i)** **Closure property:** We know that multiplication of two non-zero complex numbers is a non-zero complex number. Thus z1, z2 C\*  z1 . z2 C\*.

**(ii)** **Associative law:** We know that multiplication of complex numbers is associative. Thus, z1. (z2 . z3) = (z1 . z2) . z3  z1, z2, z3 C.

**(iii)** **Existence of identity:** Since 1 + i0 C\* and (a + ib) . (1 + i0) = a + ib

 = (1 + i0) (a + ib)  a + ib C\*. Thus, 1 + i0 is the identity element of C\* under multiplication.

**(iv)** **Existence of inverse:** Let z = a + ib C\*. Then w =  + i  C\* and

 z.w = (a + ib) . 

 = 

 =

 = 

 Similarly w.z = 1 + i0.

 Thus, z.w = 1 + i0 = w.z

  w is the inverse of z

 Thus (C\*, . ) is a group.

**(C\*, .) is abelian:** Since z1, z2 = z2 . z1  z1, z2 C, so (C\*, . ) is abelian. Hence (C\*, . ) is an abelian group.

**Examples 8:** Let M2 (Z) be the set of all 22 matrices over integers. Then M2 (Z) is an abelian group under addition of matrices.

**Solution:** We have M2 (Z) =  .

**(i)** **Closure property:** Let A, B M2 (Z). Then A =  B =  where a, b, c, d, p, q, r, s Z.

  A + B =   M2 (Z), because a + p, b + q, c + r, d + s  Z.

 Thus M2­ (Z) is closed under matrix addition.

**(ii)** **Associative law:** Since addition of matrices is associative it follows that A + (B + C) = (A + B) + C  A, B, C  M2 (Z).

**(iii) Existence of identity:** We have 0 =  M2 (Z) because 0Z.

 and A + 0 =  +  =  = A

 0 + A =  = A

  A + 0 = A = 0 + A A M2 (Z)

 Thus, 0 =  is the identity element.

**(iv)** **Existence of inverse:** Let A =  M2(Z). Then – A =  M2 (Z) and

 A + (– A) =  = 0

 Similarly (–A) + A = 0.

 Thus, A + (–A) = 0 = (–A) + A

  – A is the inverse of A.

 Thus, (M2 (Z), +) is a group.

**(M2 (z), +) is abelian:** Since matrix addition is commutative, so A + B = B + A A, B M2 (Z).

Thus, (M2 (Z), + ) is an abelian group.

**Example 9:** Let M2 (Q) be the set of all 22 non-singular matrices over rationals. Then M2 (Q) is a non-abelian group under multiplication of matrices.

**Solution:** M2 (Q) = 

**(i)** **Closure property:** Let A, B M2 (Q). Then A = , B = , where a, b, c, d, p, q, r, s Q.

  AB =  M2 (Q) because ap + br, aq + bs, cp + dr, cq + ds Q and |AB| = |A| |B| 0. Thus, M2 (Q) is closed under matrix multiplication.

**(ii)** **Associative Law:** Since multiplication of matrices is associative, it follows that A. (B.C) = (A.B). C  A, B, C M2 (Q).

(iii) **Existence of identity:** We have I =  M2 (Q) because 0, 1 Q and |I| == 1 0.

 AI = 

 IA = 

  AI = A = IA  A M2 (Q)

  I is the identity element.

**Existence of inverse:**

Let A =  M2 (Q)

Let B = . Then B M2 (Q) because  ,  ,  ,  Q and |B| =  [ ad – bc 0]

Also AB =   = 

Similarly BA = I

Thus, AB = I = BA

 A–1 = B M2 (Q). Thus (M2 (Q), . ) is a group.

**(M2 (Q), .) is non-abelian:**

Let A = 

Then AB = 

and BA = 

Thus AB  BA and so (M2 (Q), . ) is non-abelian.

**Example 10:** Let M2(Z) denote the set of all 2  2 non-singular matrices over integers. Is (M2 (Z), . ) a group?

**Solution:** (M2 (Z), ) is not a group because if A =  M2 (Z),

then A–1 =  M2 (Z), (since entries of A–1 may not be integers).

**ORDER OF A GROUP:** Let (G, o) be a group. Then the number of elements in G is called the order of the group (G, o) and is denoted by o(G). If the number of elements in a group is finite, then it is called a group of finite order. If a group is not a finite order then it is said to be group of infinite order.

**Example 11:** Show that 4 = {1, , 2}, where, , 2 are cube roots of unity, forms a group under multiplication of complex numbers. (G is a finite group of order).

**Solution:** We have the following composition table.

|  |  |  |  |
| --- | --- | --- | --- |
|  | 1 |  | 2 |
| 1 | 1 |  | 2 |
|  |  | 2 | 1 |
| 2 | 2 | 1 |  |

**(i)** **Closure property:** Since all the elements in the composition table are elements of G, so G is closed under multiplication.

**(ii)** **Associative law:** Since multiplication of complex numbers is associative, so associative law holds in G.

**(iii)** **Existence of identity:** If follows from the table, that a. 1 = a = 1 . a  a G. Thus, 1G is the identity element.

**(iv)** **Existence of inverse:** From table, it is clear that 1.1 = 1 = 1.1, . 2 = 1 = 2. 

 So, inverse of 1 is 1

 inverse of  is 2

 inverse of 2 is 

 Thus, (G, . ) is a group.

**(G, . ) is abelian:** Since multiplication of complex is commutative, so a . b = b . a  a, b G. Hence (G, . ) is an abelian group.

**Example 12:** Show that G = { 1, i} where i =  is an abelian group under multiplication of complex numbers.

**Solution:** We have the following composition table:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| . | –1  | 1 | –i | i  |
| –1 | 1 | –1 | i  | –i |
| 1 | –1 | 1 | –i | i |
| i  | –i | I | 1 | –1 |

**(i)** **Closure property:** Since all the elements in the composition table are elements of G, so G is closed under multiplication.

**(ii)** **Associative law:** Since multiplication of complex numbers is associative, so associative law holds in G.

**(iii)** **Existence of identity:** If follows from the table, that a . 1 = a = 1 . a  a G. Thus, 1G is the identity element.

**(iv)** **Existence of inverse:** From the table, it is clear that 1.1 = 1 = 1.1; (–1).(–1) = 1 = (–1).(–1); (–i).(i) = 1 = (i) (–i);

 Thus, inverse of 1 is 1

 inverse of –1 is –1

 inverse of i is – i

 inverse of –i is i

 Thus, (G, . ) is a group.

**(G, . ) is abelian:** Since multiplication of complex numbers is commutative so a.b = b.a a, b G. Hence, (G, . ) is an abelian group.

**Example 13:** Let G = {1, i, j, k}. Then show that G is a non-abelian group under the usual multiplication ‘ . ‘ and i . i = j . j = k . k = –1

 i . j = – j . i = k ; j . k = – k . j = i

 k . i = – i . k = j

This group is called HAMILTONIAN Group or the group of Unit Quarternions. Its order is 8.

**Solution:** The composition table for G is as follows:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| . | 1 | –1 | i  | –i | j | –j | k | –k |
| 1 | 1 | –1 | i  | –i | j  | –j | k  | –k |
| –1 | –1 | 1 | –i | i  | –j  | j  | –k | k  |
| i  | i  | –i  | –1 | 1 | k  | –k | –j | j  |
| –i | –i | i  | 1 | –1 | –k | k | j  | –j |
| j  | j  | –j | –k | k  | –1 | 1 | i  | -i |
| –j | –j | J | k | –k | 1 | –1 | –i | i  |
| k  | k  | –k | j  | –j | –i  | i  | –1 | 1 |
| –k | –k | k | –j | j | i  | –i | 1 | –1 |

**(i)** **Closure property:** Since all the elements in the composition table are elements of G so G is closed under the given operation.

**(ii)** **Associative law:** From the table, we can easily verify that a . (b . c) = (a . b) . ca, b, cG

**(iii)** **Existence of identity:** If follows from the table, that a.1 = a = 1.a  a G, so 1G is the identity element.

**(iv)** **Existence of identity:** It is clear from the table that

 inverse of 1 is i

 inverse of –1 is –1

 inverse of i is –i

 inverse of –i is i

 inverse of j is –j

 inverse of –j is j

 inverse of k is –k

 inverse of –k is k

 Thus, (G, . ) is a group.

**(G, . ) is non-abelian:** Since j.k = i and k.j = –i so j.k  k.j. Thus (G, . ) is a non-abelian group.

**ADDITION MODULO m:** Let a and b be any two integers and m be a positive integer. Then the addition modulo m, denoted by a  b is defined as a b = r, where r is the least non-negative remainder when a + b is divided by m e.g.

(i) 9 6 = 0 (ii) 12 8 = 6

(iii) –10 4 = 2 (iv) –3  5 = 2

(v) 2 3 = 5 (vi) –6  2 = 0

**MULTIPLICATION MODULO n:** Let a and b be any two integers and n be a positive integer. Then the multiplication modulo n, denoted by a b is defined as ab = r, where r is the least non-negative remainder when ab is divided by n. e.g.

(i) 4 7 = 4 (ii) 8 5 = 4

(iii) 7 5 = 0 (iv) 2 9 = 4

(v) –3 20 = 4 (vi) –6 2 = 0

**Example 14:** Let G = {0, 1, 2, 3, 4, 5}. Show that (G, ) is an abelian group.

**Solution:** The composition table for (G, ) is as under:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 |
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

**(i)** **Closure property:** Since all the elements in the composition table are elements of G so G is closed under .

**(ii)** **Associative law:** From the table, we can easily verify that a (b c) = (ab) c  a, b, c G. e.g. (34) 5 = 0 = 3  (45).

**(iii) Existence of identity:** It follows from the table that a0 = a = 0 a  a G. These 0 is the identity element for (G, ).

**(iv)** **Existence of inverse:** From the table, it is clear that

 inverse of 0 is 0

 inverse of 1 is 5

 inverse of 2 is 4

 inverse of 3 is 3

 inverse of 4 is 2

 inverse of 5 is 1. Thus, (G, ) is a group.

**(G, ) is abelian:** From the table, it is clear that a b = b a  a, b G. Thus (G, ) is an abelian group.

**Example 15:** Prove that the set G = {1, 2, 3, 4, 5, 6} is a finite abelian group of order 6 under multiplication modulo 7.

**Solution:** The composition table for (G, ) is as under:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 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 |

**(i)** **Closure property:** Since all the elements in the composition table are the elements of G, so G is closed under .

**(ii) Associative law:** From the table, we can easily very that a (b c) = (a b)  c  a, b, c  G.

 e.g. 3 (5  4) = 3 6 = 4

 and (35)  4 = 1 4 = 4.

**(iii) Existence of identity:** It follows from the table that a1 = a = 1 a  a  G. Thus, 1 is the identity element for (G, )

**(iv)** **Existence of inverse:** From the table it is clear that

 inverse of 1 is 1

 inverse of 2 is 4

 inverse of 3 is 5

 inverse of 4 is 2

 inverse of 5 is 3

 inverse of 6 is 6

 Thus, (G, ) is a group.

**(G, ) is abelian:** From the table, it is clear that a b = b a  a, b  G. Hence, (G, ) is an abelian group.

**THEOREM 1:** Let (G, o) be a group. Then cancellation laws hold in G i.e. aob = aoc  b = c [left cancellation law) and boa = coa  b = c  a, b, c  G [right cancellation law].

**Proof:** Since a  G, so a–1  G.

 aob = aoc  a–1 o(aob) = a–1 o(aoc)

  (a–1oa) ob = (a–1oa) oc

  eob = eoc  b = c.

Also,

 boa = coa

  (boa) oa–1 = (coa) oa–1

  bo (aoa–1) = co (aoa–1)

  boe = coe  b = c.

Thus, cancellation laws hold in G.

**THEOREM 2:** Let (G, o) be a group. Then identity element in G is unique.

**Proof:** Let e and  be two identity elements of G.

Then eo = e = oe -(1) [ is the identity element]

and oe =  = eo -(2) [ e is the identity element]

from (1) and (2) e = 

Thus, identity of (G, o) is unique

 OR

Let e and  be two identity elements of G.

Then aoe = a = eoa  a G -(1)

 ao = a = oa  a G -(2)

from (1) and (2) aoe = ao

 e =  [By left cancellation law]. Thus, identity of (G, 0) is unique.

**THEOREM 3:** Let (G, o) be a group. Then inverse of each element of G is unique.

**Proof:** Let b and c be two inverses of ‘a’ in G.

Then aob = e = boa -(1)

and aoc = e = coa -(2)

Now b = boe

 = bo(aoc) [using (2)]

 = (boa) oc [Associative law]

 = eoc [using (1)]

 = c

Thus, b = c. Hence inverse of ‘a’ is unique

 OR

Let b and c be two inverses of a in G.

Then aob = e = boa -(1)

 aoc = e = coa -(2)

from (1) and (2) aob = aoc  b = c [By left cancellation law]

Hence inverse of ‘a’ is unique.

**THEOREM 4:** Let (G, o) be a group.

Then (i) (a–1)–1 = a  a  G

 (ii) (aob)–1 = b–1 o a–1  a, b G

**Proof:** (i) We know that

 a–1 o a = e = a–1 oa  a, b G

  a is the inverse of a–1

  (a–1)–1 = a

 (ii) We have

 (aob) o (b–1 o a–1)

 = [(aob) ob–1] oa–1 [Associative law]

 = [ao (bob–1)] oa–1 [Associative law]

 = [aoe] oa–1

 = aoa–1 = e.

Also (b–1o a–1) o (aob)

 = [(b–1 o a–1) oa] ob [Associative law]

 = [b–1 o (a–1 o a)] ob [ Associative law]

 = (b–1 o e) ob = b–1 ob = e.

Thus,

 (aob) o (b–1 o a–1) = e = (b–1 o a–1) o (aob)

  b–1 o a–1 is the inverse of aob

  (aob)–1 = b–1 o a–1.

**THEOREM 5:** Let (G, o) be a group. Then for every a, b  G, each of the equations a o x = b, yoa = b have unique solutions in G.

**Proof:** We have

|  |  |
| --- | --- |
|  aox = b -(1) a–1o (aox) = a–1ob (a–1oa) ox = a–1ob eox = a–1 ob x = a–1 o b G | yoa  b -(2)(yoa) oa–1 = boa–1yo (aoa–1) = boa–1yoe = boa–1y = boa–1 G |

Thus the given equations have solution in G.

**UNIQUENESS:** Let x1 and y1 be solutions of (1) and (2) respectively.

Then aox1 = b –(3) and y1oa = b –(4)

From (1) and (3), we have

 aox = aox1

 x = x1 [By left cancelation law]

From (2) and (4), we have

 yoa = y1 o a

 y = y1 [By right cancelation law]

Hence x = x1 and y = y1. This proves uniqueness of solution.

**LEFT IDENTITY ELEMENT:** Let (G, o) be a group. Then an element e G is called left identity element if e o a = a  a G.

**RIGHT IDENTITY ELEMENT:** Let (G, o) be a group. Then e G is called right identity element if aoe = a  a G.

**LEFT INVERSE:** Let (G, o) be a group and aG. Then bG is called left inverse of a if boa = e.

**RIGHT INVERSE:** Let (G, o) be a group and a G. Then b G is called right inverse of a if aob = e.

**THEOREM 6:** Let G be a set with binary operation o. Suppose

(i) o is associative

(ii) there is a left identity in G

(iii) each element of G has a left inverse in G.

Then (G, o) is a group.

**Proof:** To show that (G, o) is a group, it is sufficient to show that G has identity element and each element of G has inverse in G.

**EXISTENCE OF IDENTITY ELEMENT:** Let e be the left identity. Let a G. Since a has left inverse so  a–1 G s.t.

 a–1 o a = e -(1)

Now

 a–1o (aoe) = (a–1oa) oe

 = eoe [using (1)]

 = e

 = a–1oa [using (1)]

  a–1 o (aoe) = a–1 o a

  aoe = a [By left cancellation law]

  e is the right identity also.

  e is the identity element.

**EXISTENCE OF INVERSE:** Let a  G and a–1 be the left inverse of a in G.

Then a–1 oa = e. –(2)

Now a–1 o (aoa–1) = (a–1oa) oa–1

 = eoa–1 [using (2)]

 = a–1

 = a–1oe

 a–1o (aoa–1) = a–1oe

 aoa–1 = e [By left cancellation law]

 a–1 is the right inverse of a

 a–1 is the inverse of a in G.

Hence (G, o) is a group.

**THEOREM 7:** Let G be a set a set with binary operation o. Suppose

(i) ao (boc) = (aob) oc  a, b, c  G.

(ii)  e G such that aoe = a  a G [right identity]

(iii) For each aG,  b G such that aob = e [right inverse].

Then (G, o) is a group.

**Proof:** Try as in theorem 6.

**THEOREM 7:** A semi-group (G, o) is a group if and only if the equations aox = b and yoa = b  a, b G are solvable in G.

**Proof:** First suppose (G, o) is a group. Then we have to show that the equations aox = b ; yoa = b are solvable in G.

Now, aox = b yoa = b

 a–1o(aox) = a–1 ob (yoa) oa–1 = boa–1

 (a–1oa) ox = a–1 ob yo (aoa–1) = boa–1

 eox = a–1 ob yoe = boa–1

 x = a–1 ob G y = boa–1 G.

Thus, the given equations are solvable in G. Conversely, suppose (G, o) is a semi-group such that the equations aox = b (1)

 and yoa = b (2)

are solvable in G. Then we have to prove that (G, o) is a group.

**EXISTENCE OF RIGHT IDENTITY:** From (1)

 aox = b  a, b G

 aox = a [Taking b = a]

 aoea = a [x = ea G]

Let b G be any element. Then from (2) b = coa for some c G.

 boea = (coa) oca

 = co (aoea)

 = coa

 = b b G

 ea is right identity of G.

**EXISTENCE OF RIGHT INVERSE:** Let a G. Then from (1)

 aox = b  b G

 aox = ea [ea = b G]

 x is the right inverse of a.

Thus, each element of G has right inverse in G. Hence (G, o) is a group.

**THEOREM 9:** A finite semi-group (G, o) is a group if and only if the cancellation laws hold in G.

**Proof:** First suppose (G, o) be group. Then we have to show that cancellation laws hold in G.

Let a, b, c G such that

 aob = aoc

 a–1o (aob) = a–1 o(aoc)

 (a–1oa) ob = (a–1oa) oc

 eob = eoc

 b = c

Thus, left cancellation law hold in G.

Next, let a, b, c G such that

 boa = coa

 (boa) oa–1 = (coa) oa–1

 bo(aoa–1) = co (aoa–1)

 boe = coe  b = c

Thus, right cancellation law holds in G.

Conversely, suppose (G, o) is a finite semi-group in which cancellation laws hold. Then we have to show that (G, o) is a group. To show that (G, o) is a group, we shall show that the equations aox = b ; yoa = b ; a, b G are solvable in G. Fix a, b G.

Define f: G G by f(x) = aox

Then f(x1) = f(x2)

 aox1 = aox2

 x1 = x2 [By left cancellation law]

 f: G G is one-one

 f: G G is onto since G is a finite set.

Thus, for b G  x0 G such that f(xo) = b

 aoxo = b

 The equation ax = b has a solution in G. Similarly, we can show that the equation yoa = b has a solution in G. Hence (G, o) is a group.

**Remark:** The condition on the set G being a finite set is essential. For example (N, +) is a semi-group in which cancellation laws sold but it is not a group.

**EXAMPLE OF A FINITE SEMI-GROUP WHICH IS NOT A GROUP:** Let G = {0,1, 2, 3}. Then G under multiplication modulo 4 is a finite semi-group, which is not a group because there is no inverse of 2 in G. (here 1 is the identity element)

**EXPONENTS:** Let (G, o) be a group. For each a G, we define

 ao = e

 a1 = a

 a2 = aoa

 a3 = aoaoa

 an =  n N.

If n is a negative integer, we define an = = (a–1)–n.

Thus an is defined for all integers n.

**LAWS OF EXPONENTS:**

(i) am . an = am + n

(ii) (am)n = amn  m, n z.

**Example:** (1) If G = (R, +), then 3o = 0 (identity): 32 = 3 + 3 = 6

 34 = 3 + 3 + 3 + 3 = 12

(2) If G = (R\*, . ) be the multiplicative group of non-zero reals,

 then 3o = 1 (identity) 33 3.3.3 = 27; 34 = 3.3.3.3 = 81.

**EXERCISE**

1. Let  be the set of rational numbers other than 1. Then show that  is an abelian group under the operation o defined by aob = a + b – ab for all a, b .

2. Let G = {(a, b) : a, b R, a  0}. Then show that G is a group under the operation \* defined by (a, b) \* (c, d) = (ac, bc + d)

3. Prove that the set of nth roots of unity forms an abelian group under multiplication of complex numbers.

4. Prove that the set of complex numbers of modulus 1 forms a group under multiplication of complex numbers.

5. Prove that a group in which every element is its own inverse is an abelian group.

6. Prove that a group G is abelian if and only if (ab)2 = a2 b2 for all a, b G.

7. Let G be an abelian group. Then show that (ab)n = an bn for all a, b G and n Z.

8. Prove that every group G with identity e such that x2 = e for all x G is abelian.

9. If G is a group of even order, then prove that there exists an element a  e in G such that a2 = e.

10. Prove that the set of matrices  where  is a real number forms an abelian group under matrix multiplication.