Group Theory.

In this chapter we introduce the concept of binary operation and study few algebraic structures like, semi group, group and few of its properties.

Let A be a non empty set. A binary operation $*$ over A is a function $*: A \times A \to A$.

That is a binary operation $*$ on a non empty set A, associates each pair (a, b) of elements of A to a unique element, say $c \in A$. This is denoted by $a * b = c$.

If $*$ is a binary operation on the set A, then we say that the set A is closed under the operation $*$.

examples:

1. The set N of natural numbers is closed under addition. whereas usual subtraction is not a binary operation on N.
2. On the set $\mathbb{Q}$ of all rational numbers, the operation $*$ defined by $a * b = \frac{ab}{2}$, $\forall a, b \in \mathbb{Q}$ is a binary operation on $\mathbb{Q}$.
3. The usual matrix multiplication is a binary operation on the set of all $n \times n$ matrices over the set of real numbers.
4. Let n be a fixed positive integer, a and b be any two integers. Define $a +_n b = r$, where r is the least positive non negative remainder obtained when the usual sum $a + b$ is divided by n. Clearly $+_n$ is a binary operation on $Z_n = \{0, 1, 2, \ldots, n-1\}$

Binary algebra:

A non empty set A together with a binary operation $*$ defined on it, is called a binary algebra or groupoid and it is denoted by $\langle A, * \rangle$.

example:

The set E of all even numbers, is closed under usual addition and also under usual multiplication. Thus $\langle E, + \rangle$ and $\langle E, \times \rangle$ are binary algebra. whereas, the set of all odd numbers, do not form a binary algebra under usual addition, since the sum of two odd numbers is not odd.

Semi group.

A non empty set S, together with the binary operation $*$ is called a semigroup if $*$ is associative in S. ie, $\forall x, y, z \in S$, $x * (y * z) = (x * y) * z$.

Monoid

A non empty set S, together with the binary operation $*$ is called a monoid if $*$ is associative in S and if there exists a unique element e in S such that for every element x in S, $x * e = x = e * x$. e is called the identity element.

examples

1. The set Z of all integers together with usual addition is a semi group. In fact it is also a monoid, with 0 as the identity element.
2. The set N of all natural numbers with usual addition is a semi group. But it is not a monoid, as 0 the identity element does not belong to N.

Groups

A binary algebra $\langle G, * \rangle$ is said to be a group, if the following axioms hold.

(i) Associativity:

$\forall\ a, b, c \in G,\ a * (b * c) = (a * b) * c$

(ii) Existence of identity:

$\exists$ an element $e \in G$, such that $\forall a \in G$, $a * e = a = e * a$. The element e is called an identity element of G.

(iii) Existence of inverse

$\forall\ a \in G$, $\exists$ an element $b \in G$ such that $a * b = e = b * a$. The element b is called an inverse of the element of a in G.

Note: A group $\langle G, * \rangle$ is a monoid in which every element has an inverse in G w.r.t the binary operation $*$.

A group $\langle G, * \rangle$ is said to be an abelian or a commutative group if the binary composition is commutative. ie, $\forall\ a, b \in G$, $a * b = b * a$

A group $\langle G, * \rangle$ is said to be a finite group if the set G is finite, otherwise it is called an infinite group.

The number of elements in the group $\langle G, * \rangle$ is called the order of the group and it is denoted by $O(G)$.

examples:

1. $\langle Z, + \rangle$, $\langle Q, + \rangle$, $\langle R, + \rangle$, $\langle C, + \rangle$ are abelian groups.
2. If R^*, Q^* and C^* denote respectively the sets of non zero real numbers, non zero rational numbers and non zero complex numbers, then $\langle R^*, \cdot \rangle$, $\langle Q^*, \cdot \rangle$ and $\langle C^*, \cdot \rangle$ are abelian groups.
3. The set $G = \{ na \mid a \in Z \}$ is an abelian group under usual addition, where n is a non-zero integer.
4. The set $\{1, \omega, \omega^2\}$ of cube roots of unity is abelian group under usual multiplication.
5. The set $G = \{1, -1, i, -i\}$ of fourth roots of unity is an abelian group under usual multiplication.
6. The set of even integers is an abelian group under usual addition.
7. The set M of all $n \times n$ non singular matrices of real numbers is a non-abelian group under usual matrix multiplication.
8. The set M of all $m \times n$ matrices over the set of real numbers is an abelian group under usual matrix addition.
9. The set G of all unimodular complex numbers is a group under usual multiplication of complex numbers.
10. The set $\{ \pm 1, \pm i, \pm j, \pm k \}$ is a non-abelian group under the quaternion multiplication, defined by $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$, $ik = -j$

The set $Q_8 = \{ \pm 1, \pm i, \pm j, \pm k \}$ is called a quaternion group.

examples

1. Show that the set of all integers is a group under addition.

Sol'n (i) $\forall\ a,b \in \mathbb{Z} \quad a+b \in \mathbb{Z}$.

Hence $\langle \mathbb{Z}, + \rangle$ is closed under addition.

(ii) $\forall\ a,b,c \in \mathbb{Z} \quad (a+b)+c = a+(b+c)$

Hence $\langle \mathbb{Z}, + \rangle$ is associative

(iii) $\forall\ a \in \mathbb{Z}, \quad a+0 = a = 0+a$.

Hence 0 is the identity element of $\langle \mathbb{Z}, + \rangle$

(iv) $\forall\ a \in \mathbb{Z}, \quad a+(-a) = 0 = (-a)+a$

Hence $-a$ is the inverse element of a in $\langle \mathbb{Z}, + \rangle$

Therefore $\langle \mathbb{Z}, + \rangle$ is a group.

2. Show that the set of all non-zero complex numbers $(\mathbb{C}^*)$ is a group under multiplication.

Sol'n (i) $\forall\ a_1+ib_1,\ a_2+ib_2 \in \mathbb{C}^*, \quad (a_1+ib_1)\times(a_2+ib_2)$

$(a_1a_2-b_1b_2)+i(a_1b_2+b_1a_2) \in \mathbb{C}^*$

Hence $\langle \mathbb{C}^*, \cdot \rangle$ is closed under multiplication.

(ii) $\forall (a_1+ib_1), (a_2+ib_2), (a_3+ib_3) \in \mathbb{C}^*$

$$(a_1+ib_1)\times[(a_2+ib_2)\times(a_3+ib_3)] = (a_1+ib_1)\times(a_2a_3-b_2b_3+i(b_2a_3+a_2b_3))$$

$$= a_1a_2a_3 - a_1b_2b_3 - b_1b_2a_3 - b_1a_2b_3 + i(a_1b_2a_3 + a_1a_2b_3 + b_1a_2a_3 - b_1b_2b_3)$$

$$= ((a_1a_2-b_1b_2)+i(a_1b_2+b_1a_2))\times(a_3+ib_3)$$

$$= [(a_1+ib_1)\times(a_2+ib_2)]\times(a_3+ib_3)$$

Hence $\langle \mathbb{C}^*, \cdot \rangle$ is associative

(iii) $\forall\ a_1+ib_1 \in \mathbb{C}^*, \quad (a_1+ib_1)\times 1 = a_1+ib_1 = 1\times(a_1+ib_1)$

Hence 1 is the identity element of $(\mathbb{C}^*, \cdot)$

(iv) $\forall\ a_1+ib_1 \in \mathbb{C}^*, \quad (a_1+ib_1)\times\frac{1}{(a_1+ib_1)} = 1 = \frac{1}{(a_1+ib_1)}\times(a_1+ib_1)$

Here $\frac{a_1-ib_1}{(a_1^2+b_1^2)} = \frac{1}{a_1+ib_1}$ is the inverse of (a_1+ib_1) in $(\mathbb{C}^*, \cdot)$

Therfore $(\mathbb{C}^*, \cdot)$ is a group

3. Show that $\langle N, + \rangle$ where N is the set of natural numbers is a semigroup and not a group.

Sol:

(i) $\forall\ a, b, c \in N,\ (a+b)+c = a+(b+c)$.

Hence $\langle N, + \rangle$ is associative.

Therefore $\langle N, + \rangle$ is a semigroup.

(ii) $\forall\ a \in N,\ a+0 = a = 0+a$,

but $0 \notin N$, Hence identity element doesnot exist for $\langle N, + \rangle$.

Therefore $\langle N, + \rangle$ is not a group.

4. Show that $\langle Z^+, \times \rangle$ where Z^+ is the set of positive integers, is not a group.

Sol:

$Z^+ = \{1, 2, 3, \ldots\}$

(i) $\forall\ a, b, c \in Z^+,\ (a \times b) \times c = a \times (b \times c)$

Hence $\langle Z^+, \times \rangle$ is associative.

(ii) $\forall\ a \in Z^+,\ a \times 1 = a = 1 \times a$

Hence 1 is the identity element of $\langle Z^+, \times \rangle$

(iii) $\forall\ a \in Z^+,\ a \times \frac{1}{a} = 1 = \frac{1}{a} \times a$,

but $\frac{1}{a} \notin Z^+$, Hence inverse element does not exist for $\langle Z^+, \times \rangle$.

Therefore $\langle Z^+, \times \rangle$ is not a group.

5. On the set $\mathbb{Q}^+$ of positive rational numbers the binary operation is defined by $a * b = \frac{ab}{2}$. Show that $\langle \mathbb{Q}^+, * \rangle$ is an abelian group.

Sol^n (i) $\forall\ a, b, c \in \mathbb{Q}^+$, $(a*b)*c = \left(\frac{ab}{2}\right)*c = \frac{abc}{4} = a*\left(\frac{bc}{2}\right)$
$= a*(b*c)$

Hence $\langle \mathbb{Q}^+, * \rangle$ is associative.

(ii) $\forall\ a \in \mathbb{Q}^+$, $a * 2 = a = 2 * a$

Hence 2 is the identity element of $\langle \mathbb{Q}^+, * \rangle$

(iii) $\forall\ a \in \mathbb{Q}^+$ $a * \frac{4}{a} = 2 = \frac{4}{a} * a$.

Hence $\frac{4}{a}$ is the inverse element of a in $\langle \mathbb{Q}^+, * \rangle$

(iv) $\forall\ a, b \in \mathbb{Q}^+$ $a * b = \frac{ab}{2} = b * a$.

Hence $\langle \mathbb{Q}^+, * \rangle$ is commutative.

Hence $\langle \mathbb{Q}^+, * \rangle$ is an abelian group.

6. On the set $\mathbb{R}$ of real numbers $*$ is defined by $a * b = a + a^2 b$, $\forall\ a, b \in \mathbb{R}$. Show that $\langle \mathbb{R}, * \rangle$ is not a group.

Sol^n $\forall\ a, b, c \in \mathbb{R}$, $(a*b)*c = (a+a^2b)*c$
$= a + a^2b + (a+a^2b)^2 c$
$= a + a^2b + a^2c + 2a^3bc + a^4b^2c$

and $a*(b*c) = a*(b+b^2c)$
$= a + a^2(b+b^2c)$
$= a + a^2b + a^2b^2c$.

$\therefore (a*b)*c \neq a*(b*c)$, $\langle \mathbb{R}, * \rangle$ is not associative
Hence $\langle \mathbb{R}, * \rangle$ is not a group.

7. Verify whether $\langle \mathbb{R}, * \rangle$ with $a * b = a - b$ a group.

Sol^n $\forall\ a, b, c \in \mathbb{R}$ $(a*b)*c = (a-b)*c = a-b-c$
and $a*(b*c) = a*(b-c) = a-b+c$
Since $(a*b)*c \neq a*(b*c)$, $\langle \mathbb{R}, * \rangle$ is not associative
Hence $\langle \mathbb{R}, * \rangle$ is not a group.

Exercise

1. Show that the set of all $m \times n$ matrices over real numbers is a group under matrix addition.
2. Show that $G = \{a + b\sqrt{2} \mid a, b \in \mathbb{R}, a \neq 0\}$ is a group under multiplication.
3. Show that the set $G = \{A, B, C, D\}$ where $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $D = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ is a group under matrix multiplication.
4. Show that the set of all non zero real numbers is a group under multiplication.
5. Show that the set $G = \{2n \mid n \in \mathbb{Z}\}$ is an abelian group under addition.
6. In the set G of rational numbers $\neq 1$, define $*$ by $a * b = a + b - ab$. Show that $(G, *)$ is an abelian group.
7. Show that $\langle \mathbb{Z}, * \rangle$ where $\mathbb{Z}$ is the set of integers and $a * b = a + b - 1 \ \forall \ a, b \in \mathbb{Z}$ is a group.
8. Show that the following are not groups. Give reasons.
   (i) $\langle \mathbb{Z}, * \rangle$ with $a * b = ab$.
   (ii) $\langle \mathbb{Q}^*, * \rangle$ with $a * b = a^b$, where $\mathbb{Q}^*$ is the set of non zero rational numbers.
   (iii) $\langle \mathbb{Z}^+, + \rangle$ where $\mathbb{Z}^+$ is the set of positive integers.
   (iv) $\langle \mathbb{R}, * \rangle$ where $a * b = a + b + a^2 b$

Properties of a Group.

Theorem 1:
The identity element of a group is unique

Proof: Let $\langle G, * \rangle$ be a group.
If possible let e and e' be two identity elements
Since e is an identity element,
we have $e' * e = e'$ and $e * e' = e' \quad -(1)$
Again as e' is an identity element,
we have $e * e' = e$ and $e' * e = e \quad -(2)$
From (1) and (2) it follows $e = e'$
Hence the identity element in a group is unique.

Theorem 2:
The inverse of an element of a group is unique.

Proof: Let e be the identity element and
a be an element of the group $\langle G, * \rangle$.
Let if possible b and c be two inverses of a in G.
Since b is an inverse of a, we have $a * b = e = b * a \quad -(1)$
Again as c is an inverse of a, we have $a * c = e = c * a \quad -(2)$
Now, $b = b * e$ [$\because e$ is the identity element]
$\Rightarrow b = b * (a * c)$ [from (2)]
$\Rightarrow b = (b * a) * c$ [associative law]
$\Rightarrow b = e * c$ [from (1)]
$\Rightarrow b = c$ [$\because e$ is the identity element]
Hence the inverse of an element is unique.

Theorem 3:

If a is an element of the group $\langle G, * \rangle$, then $(a^{-1})^{-1} = a$.

Theorem 4:

Let $\langle G, * \rangle$ be a group and $a, b \in G$, then

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

Theorem 5:

In a group $\langle G, * \rangle$ for all $a, x, y \in G$.

(i) $a * x = a * y \Rightarrow x = y$ [left cancellation law]

(ii) $x * a = y * a \Rightarrow x = y$ [right cancellation law].

Theorem 6:

Given two elements a and b of the group $\langle G, * \rangle$, then there exists unique solution for $a * x = b$ and $y * a = b$.

Examples.

1. In the group $\mathbb{R}^*$ of non zero real numbers the binary operation $*$ is defined by $a*b=\frac{ab}{5}$. Solve $2*x*5=10$ in $\mathbb{R}^*$.

Sol^n $2*x*5=10 \Rightarrow 2*(x*5)=10$

$\Rightarrow 2*\left(\frac{5x}{5}\right)=10$

$\Rightarrow 2*x=10$

$\Rightarrow \frac{2x}{5}=10$

$\Rightarrow x=25$

2. In the set G of all rational numbers except -1, the binary operation $*$ defined by $a*b=a+b+ab$. Solve $3*4*x=0$ in $\mathbb{R}^*$.

Sol^n $3*4*x=0 \Rightarrow (3*4)*x=0$

$\Rightarrow (3+4+12)*x=0$

$\Rightarrow 19*x=0$

$\Rightarrow 19+x+19x=0$

$\Rightarrow 20x=-19$

$\Rightarrow x=-\frac{19}{20}$.

3. If every element of a group G is its own inverse, show that G is abelian.

Sol^n. By data, $\forall\ a\in G$, $a^{-1}=a$.

Consider $(x*y)^{-1}=y^{-1}*x^{-1}$ [By Theorem 4.]

$\Rightarrow (x*y)^{-1}=y*x$ [$\because y^{-1}=y,\ x^{-1}=x$]

$\Rightarrow x*y=y*x$ [$\because x*y\in G,\ (x*y)^{-1}=x*y$]

Hence G is abelian.

4. If in a group $\langle G, * \rangle$, $a * a = a \ \forall \ a \in G$, show that $a = e$ where e is the identity element.

Sol^n Given $(a * a) = a$

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

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

$\Rightarrow e * a = e$

$\Rightarrow a = e$

5. Show that the groups of order 1, 2 and 3 are abelian

Sol^n (i) Let G be a group of order 1.

That is G contains only one element say e.

Consider $e * e = e$

$e * e = e * e$

There fore G is abelian

(ii) Let G be a group of order 2.

That is G contains two elements one of which acts as the identity element e and another element distinct from e, say a.

Let $G = \{e, a\}$.

The inverse of a is itself (as inverse of e is itself).

Consider $a * e = a$

$a * e = e * a$

Therfore G is abelian

(iii) Let G be a group of order 3 and $G = \{e, a, b\}$

case(i) If $a^{-1} = a$ and $b^{-1} = b$

i.e, inverse of each element is itself. Hence G is abelian

case(ii) If $a^{-1} \neq a$ and $b^{-1} \neq b$, then $a^{-1} = b$ and $b^{-1} = a$

Consider $a * b = a * a^{-1} = e = b^{-1} * b = b * a$.

Therefore G is abelian.

6. If $(G, *)$ is a group of even order, (such that $a*b=ab$), then show that there exists an element $a \in G$, [where $a \neq e$] such that $a^2 = e$ [i.e, $a^{-1} = a$].

Soln Given G is a group of even order.

Since e is its own inverse, when e is eliminated, then G will have odd number of elements.

We know that each element of G has unique inverse, thus there exists an element $a (\neq e) \in G$, s.t $a^{-1} = a$.

Now, $a = a^{-1} \Rightarrow a*a = a^{-1}*a \Rightarrow a^2 = e$.

7 Show that a group $\langle G, * \rangle$ (s.t. $a*b=ab$) is abelian if and only if $(ab)^2 = a^2b^2$, $\forall\ a, b \in G$

Soln Let G be abelian, and we need to prove $(ab)^2 = a^2b^2$.

Consider $(ab)^2 = (ab)(ab)$

$\Rightarrow$ $= a(ba)b$ (associative law)

$\Rightarrow$ $= a(ab)b$ ($\because$ G is abelian)

$\Rightarrow$ $= (aa)(bb)$ (associative law)

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

Conversely let $(ab)^2 = a^2b^2$, we need to show that G is abelian.

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

$\Rightarrow (ab)(ab) = (aa)(bb)$

$\Rightarrow a(ba)b = a(ab)b$ (associative law)

$\Rightarrow (ba)b = (ab)b$ (left cancellation law)

$\Rightarrow (ba) = (ab)$ (right cancellation law)

$\Rightarrow$ G is abelian.

Exercise

1. In the group $\langle Q^+, * \rangle$, where Q^+ is the set of all positive rationals and $a * b = \frac{ab}{2}$, find the solution of the equations $6 * x = 3$ and $y * 5 = 7$.
2. In the set of all rational numbers except 1, define $*$ by $a * b = a + b - ab$. Solve the equations $y * 3 * 2 = -5$ and $4 * z * 3 = -7$.
3. In the set $\mathbb{Z}$ of integers the binary operation $*$ is defined by $a * b = a + b + 1$. Solve $4 * 3 * x = 2$ and $7 * y * (-3) = 7$.
4. If $*$ is defined by $a * b = \frac{ab}{7}$ on the set of rational numbers, find the solution of the equations $7^{-1} * x * 3 = 4$ and $4 * y * 3^{-1} = 2$.

Modular System

Addition modulo m

Let m be a fixed positive integer and a and b are any two integers. The binary composition called addition modulo m, denoted by $+_m$ is defined as $a +_m b$ = least non negative remainder obtained by dividing the usual sum $a+b$ by m.

eg under addition modulo 7, $4 +_7 6 = 3$, since the usual sum $4+6=10$ leaves 3 as remainder when divided by 7.

similarly $4 +_4 5 = 1$, $3 +_2 7 = 0$, $2 +_5 7 = 4$.

Multiplication modulo m

Let m be a fixed positive integer and a and b any two integers. The binary composition called multiplication modulo m, denoted by $\times_m$ is defined as $a \times_m b$ = least non negative remainder obtained by dividing the usual product $a \times b$ by m.

eg under multiplication modulo 6, $4 \times_6 6 = 0$, since the usual product $4 \times 6 = 24$ leave 0 as remainder when divided by 6.

similarly $4 \times_3 5 = 2$, $3 \times_4 7 = 1$, $2 \times_5 7 = 4$.

Example

1. Form the addition modulo 6 table for the set $\{0, 1, 2, 3, 4, 5\}$.

Sol^n

$+_6$	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

2. Form the table of multiplication modulo 10 of the set $\{1, 3, 7, 9\}$.

Soln

$\times_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

3. Show that $\langle Z_4, +_4 \rangle$, where $Z_4 = \{0, 1, 2, 3\}$ is an abelian group.

Soln

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

(i) Consider $3 +_4 (2 +_4 1) = 3 +_4 3 = 2$

$(3 +_4 2) +_4 1 = 1 +_4 1 = 2$

$\therefore 3 +_4 (2 +_4 1) = (3 +_4 2) +_4 1$

Similarly with any other three elements of Z_4,

$(a +_4 b) +_4 c = a +_4 (b +_4 c)$.

$\therefore \langle Z_4, +_4 \rangle$ is associative.

(ii) $\forall\ a \in Z_4$, $(a +_4 0) = a = 0 +_4 a$

Hence 0 is the identity element of $\langle Z_4, +_4 \rangle$.

(iii) 0 is the inverse of 0 $\because 0 +_4 0 = 0 = 0 +_4 0$

3 is the inverse of 1 $\because 1 +_4 3 = 0 = 3 +_4 1$

2 is the inverse of 2 $\because 2 +_4 2 = 0 = 2 +_4 2$

1 is the inverse of 3 $\because 3 +_4 1 = 0 = 1 +_4 3$

Hence the inverse of each element exists.

(iv) Since the table is symmetric about the principle diagonal, $a +_4 b = b +_4 a$, $\forall\ a, b \in Z_4$.

Hence $\langle Z_4, +_4 \rangle$ is commutative.

Therefore $\langle Z_4, +_4 \rangle$ is an abelian group.

4. Show that $G=\{1,2,3,4\}$ is an abelian group under multiplication modulo 5.

Sol^n

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(i) From the table it follows that G is closed under multiplication modulo 5.

(ii) $3 \times_5 (4 \times_5 2) = 3 \times_5 3 = 4$

$(3 \times_5 4) \times_5 2 = 2 \times_5 2 = 4$

$\therefore 3 \times_5 (4 \times_5 2) = (3 \times_5 4) \times_5 2$

Similarly with any other three elements of G,

$a \times_5 (b \times_5 c) = (a \times_5 b) \times_5 c$. $\therefore \langle G, \times_5 \rangle$ is associative.

(iii) $\forall a \in G$, $a \times_5 1 = a = 1 \times_5 a$

Hence 1 is the identity element of $\langle G, \times_5 \rangle$.

(iv) 1 is the inverse of 1 $\because 1 \times_5 1 = 1 = 1 \times_5 1$

3 is the inverse of 2 $\because 2 \times_5 3 = 1 = 3 \times_5 2$

2 is the inverse of 3 $\because 3 \times_5 2 = 1 = 2 \times_5 3$

4 is the inverse of 4 $\because 4 \times_5 4 = 1 = 4 \times_5 4$.

$\therefore$ inverse of each element exists in $\langle G, \times_5 \rangle$.

(v) Since the table is symmetric about the principal diagonal $a \times_5 b = b \times_5 a \ \forall a, b \in G$.

Hence $\langle G, \times_5 \rangle$ is commutative.

Therfore $\langle G, \times_5 \rangle$ is an abelian group.

Exercise

1. Write the addition modulo 6 table for the set $\{0,2,4\}$
2. Write the multiplication modulo 12 table for the set $\{1,5,7,11\}$
3. Show that $\langle Z_5, +_5 \rangle$, where $Z_5 = \{0,1,2,3,4\}$ is an abelian group
4. Show that $\langle G, \times_7 \rangle$, where $G = \{1,2,3,4,5,6\}$ is an abelian group.
5. Show that the set $G = \{1,2,3\}$ is not a group under $\times_4$.

Permutation and Symmetric group of order 3

A one-one, onto mapping of a finite set onto itself is called permutation and the number of elements in the set is called the degree of permutation.

Consider a set $S=\{a,b,c\}$ of three distinct elements. Let f be a one-one onto mapping from S onto itself. Then f is called a permutation.

Suppose $f(a)=b$, $f(b)=a$, $f(c)=c$. This permutation is denoted by two line notation. In this notation we write the elements of S in the first row and under each element of the first row, we put down its images under the mapping f. Thus f is denoted by $f=\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$

Let $S=\{1,2,3\}$. There are $3!$ different ways of arranging the elements of S. Thus the total number of distinct one-one and onto functions which can be defined on S is $3!=6$. That is the total number of distinct permutations of order 3 is 6.

All the 6 distinct permutations of order 3 for the set $S=\{1,2,3\}$ are as follows.

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Note: The permutations $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ is same as the permutation $\begin{pmatrix} 3 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix}$ because the mapping is same in both the cases.

Equality of two permutations

Two permutations f and g of degree 3 on the set $S=\{1,2,3\}$ are said to be equal if $f(x)=g(x)\ \forall\ x\in S$.

$f=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ and $g=\begin{pmatrix}2&1&3\\1&3&2\end{pmatrix}$ are equal as $f(1)=g(1)=3$, $f(2)=g(2)=1$, $f(3)=g(3)=2$.

Identity permutation

The identity mapping I on the set $S=\{1,2,3\}$ onto itself is called the identity permutation of degree 3. ie, $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ is the identity permutation of order 3.

Product or Composition of two permutations

Given two permutations of same order, they can be combined by means of composition of two functions. This is called the product of two permutations.

Let $f=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ and $g=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ be two permutations of degree 3. fog is the product of permutations f and g such that

$fog(1)=f(g(1))=f(3)=1$

$fog(2)=f(g(2))=f(1)=2$ Thus $fog=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

$fog(3)=f(g(3))=f(2)=3$.

i.e., $f=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ and $g=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

Also fog can be found as: $g:\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $f:\ 3\ 1\ 2$ $\therefore fog=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

Similarly gof can be found as: $f:\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $g:\ 2\ 3\ 1$ $\therefore gof=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

Observe that $fog\neq gof$.

Inverse of a permutation

Consider a permutation $f=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ of degree 3 on the set $S=\{1,2,3\}$.

Since f is a one-one onto mapping from the set S onto S, the inverse of f exists and it is

$$f^{-1}=\begin{pmatrix}3&1&2\\1&2&3\end{pmatrix} \text{ or } = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}.$$

Further f^{-1} is a permutation of degree 3.

The inverse permutation f^{-1} is written by interchanging the rows and writing in an order.

Further, $f\circ f^{-1}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=I$, the identity permutation

Also $f^{-1}\circ f=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=I$.

S_3 – the set of all permutations of degree 3.

Let $S=\{1,2,3\}$. The number of permutations of degree 3 are 6 and these are:

$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $f=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $g=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $h=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, $i=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$, $j=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$

Thus $S_3=\{e,f,g,h,i,j\}$

Theorem: The set S_3 of all permutations of degree 3, is a finite non-abelian group of order 6, under the product of permutations.

Symmetric group of degree 3

The group S_3 of all permutations of degree 3 is called the symmetric group of degree 3.

Examples.

1. If $f=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ and $g=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ are two elements of S_3, find fog^{-1}, gof^{-1}.

Soln Given $f=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$, $g=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

$$f^{-1}=\begin{pmatrix}3&2&1\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad g^{-1}=\begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$fog^{-1}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

$$gof^{-1}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

2. If $f=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, $g=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ and $h=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, in S_3 find $fogoh$ and $hogof$.

Soln Given

$$fogoh=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

$$hogof=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

Exercise.

1. If $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ is an element of S_3 find g^{-1}.

2. If $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ are in S_3, find (i) $f \circ f$ and (ii) $g \circ g$.

3. In the symmetric group of S_3 of $S = \{a, b, c\}$, $f^{-1} = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$, $g = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$.

Find (i) $f \circ g$, (ii) $g \circ f$, (iii) $f \circ g^{-1}$.

Subgroups

A subset H of a group $\langle G, * \rangle$ is called a subgroup of G, if it is a group by itself w.r.t. the same binary operation defined in G.

Every group $\langle G, * \rangle$ will have atleast two subgroups, one is the group G itself and the other is the subset $\{e\}$, where e is the identity element of G. These two subgroups of G are called trivial or improper subgroups of G. All other subgroups if it exist are called proper subgroups.

The following theorems give the necessary and sufficient conditions for a subset H of a group G to be a subgroup of G.

Theorem 1:
A non empty subset H of a group $\langle G, * \rangle$ is a subgroup of G if and only if,
(i) $a, b \in H \Rightarrow a * b \in H$, (ii) $a \in H \Rightarrow a^{-1} \in H$.

Theorem 2:
A non empty subset H of a group $\langle G, * \rangle$ is a subgroup of G if and only if $\forall\, a, b \in H$, $a * b^{-1} \in H$.

Examples

1. Show that the set of even integers including 0 is a subgroup of additive group of the set $\mathbb{Z}$ of integers.

Sol: Let H be the set of even integers including 0.
Let $a, b \in H$. Thus $a = 2n$ and $b = 2m$ for some $n, m \in \mathbb{Z}$.
Consider, $a + b = 2n + 2m = 2(n+m)$, which is even.
Hence $a + b \in H$.
Consider $a^{-1} = -a = -2n$, which is even,
Hence $a^{-1} \in H$
Hence H is a subgroup of $\mathbb{Z}$.

2. Show that the set of square roots of unity is a subgroup of the group of fourth roots of unity under multiplication.

Sol^{n} Let $H = \{1, -1\}$, the set of square roots of unity.

Let $G = \{1, -1, i, -i\}$, the set of fourth roots of unity.

Clearly $H \subset G$.

Now, $1 \in H,\ 1 \in H \Rightarrow 1 \cdot 1^{-1} = 1 \cdot 1 = 1 \in H$

$-1 \in H,\ -1 \in H \Rightarrow (-1)(-1)^{-1} = (-1)\cdot(-1) = 1 \in H$

$1 \in H,\ -1 \in H \Rightarrow 1 \cdot (-1)^{-1} = 1 \cdot (-1) = -1 \in H$

$-1 \in H,\ 1 \in H \Rightarrow (-1) \cdot 1^{-1} = (-1) \cdot 1 = -1 \in H$

Thus $\forall\ a, b \in H,\ a \cdot b^{-1} \in H$.

Hence H is a subgroup of G.

3. Show that $H = \{0, 2, 4\}$ is a subgroup of the group $\langle G, +_6 \rangle$, where $G = \{0, 1, 2, 3, 4, 5\}$

Sol^{n}

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

(i) $\forall\ a, b \in H,\ a +_6 b \in H$

(ii) $0^{-1} = 0 \in H$

$2^{-1} = 4 \in H$

$4^{-1} = 2 \in H$

Hence H is a subgroup of G.

4. Show that the intersection of two subgroups of a group G is again a subgroup.

Sol^{n} Let H and K be any two subgroups of G.

(i) Let $x, y \in H \cap K \Rightarrow x, y \in H$ and $x, y \in K$.

$\Rightarrow x * y \in H$ and $x * y \in K$ [$\because$ H and K are subgroups of G].

$\Rightarrow x * y \in H \cap K$.

(ii) Let $x \in H \cap K \Rightarrow x \in H$ and $x \in K$

$\Rightarrow x^{-1} \in H$ and $x^{-1} \in K$ [$\because$ H and K are subgroups of G]

$\Rightarrow x^{-1} \in H \cap K$

From (i) and (ii) $H \cap K$ is a subgroup of G.

5. Let G be a group and $a \in G$. Then the set $N(a) = \{x \in G \mid xa = ax\}$ is a subgroup of G.

Sol^n The set $N(a)$ is the set of all elements of G which commute with the fixed element a.

Let $x, y \in N(a)$, then $xa = ax$ and $ya = ay$.

Consider $ya = ay \Rightarrow y^{-1}(ya)y^{-1} = y^{-1}(ay)y^{-1}$

$\Rightarrow (y^{-1}y)(ay^{-1}) = (y^{-1}a)(yy^{-1})$

$\Rightarrow e(ay^{-1}) = (y^{-1}a)e$

$\Rightarrow ay^{-1} = y^{-1}a \quad -(1)$

We shall show that $\forall x, y \in N(a)$, $xy^{-1} \in N(a)$

Consider $(xy^{-1})a = x(y^{-1}a)$

$= x(ay^{-1})$ from (1)

$= (xa)y^{-1}$

$= (ax)y^{-1}$ [$\because xa = ax$]

$(xy^{-1})a = a(xy^{-1})$

$\therefore xy^{-1} \in N(a)$.

Hence $N(a)$ is a subgroup of G.

6. Show that the union of two subgroups of a group need not be a subgroup of G.

Sol^n Consider the groups $\langle Z_6, +_6 \rangle$, where $Z_6 = \{0,1,2,3,4,5\}$

Let $H = \{0,3\}$ and $K = \{0,2,4\}$, Clearly H and K are subgroups of Z_6.

Consider $H \cup K = \{0,2,3,4\}$.

~~Consider~~ let $3,4 \in H \cup K$, $3 +_6 4 = 1 \notin H \cup K$.

i.e, $H \cup K$ is not closed under addition modulo 6.

Hence $H \cup K$ is not a subgroup of Z_6.

Exercise

1. Show that $\langle \mathbb{R}^+, \times \rangle$ is a subgroup of $\langle \mathbb{R}^*, + \rangle$
2. Show that $\langle \mathbb{R}, + \rangle$ is a subgroup of $\langle \mathbb{C}, + \rangle$
3. Let G be the multiplicative group of all non singular matrices over complex numbers. Let H be the set of following matrices.
   $\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $\pm \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$, $\pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.
   Show that H is a subgroup of H.
4. Consider the group $\langle Z_8, +_8 \rangle$, where $Z_8 = \{0,1,2,3,4,5\}$ Show that $H = \{0,2,4\}$ is a subgroup of Z_8.
5. Show that $H = \{1,9\}$ is a subgroup of $\langle G, \times_{10} \rangle$, where $G = \{1,3,7,9\}$.
6. Consider the additive group $\langle \mathbb{Z}, + \rangle$ of all integers and let $H = \{3a \mid a \in \mathbb{Z}\}$. Show that H is a subgroup of $\mathbb{Z}$.

Integral powers of an element of a group.

Let a be an element of a group G. Then for every integer n, by the element a^n, we mean,

(i) $a^n = a.a.a.\ldots.a$, n times, if n is positive integer.

(ii) $a^{-n} = (a^n)^{-1}$, i.e., a^{-n} is the inverse of a^n.

(iii) $a^0 = e$, the identity element of G.

Note: If the group operation is denoted by $+$, then we write (i) $a+a+\ldots+a$ by na instead of a^n (n is positive integer)

(ii) $(-n)a = -na$

(iii) $0.a = 0$, the identity element of a group.

Eg: In $(Z_5^*, \times_5)$, where $Z_5^* = \{1,2,3,4\}$

$3^4 = 3 \times_5 3 \times_5 3 \times_5 3 = 1$.

In $(Z_4, +_4)$, where $Z_4 = \{0,1,2,3\}$

$6(3) = 3 +_4 3 +_4 3 +_4 3 +_4 3 +_4 3 = 2$,

here $3 \in Z_4$ and 6 is the integer by which times the element 3 is composed with itself.

Order of an element

The order of an element a of a group G, is the least positive integer m such that $a^m = e$. If there exists no such integer for which $a^m = e$, we say the element a is of infinite order.

The order of an element a is denoted by $O(a)$, read as order of a.

Note: 1. For any group, the identity element is the only element of order 1.

2. If for $a \in G$, where G is a group, $a^m = e$, for some positive integer n, then $O(a) \leq n$.

3. If $O(a) \geq n$, then $a^m \neq e$ for $0 < m < n$.

Examples

1. Find the orders of the elements of the multiplicative group $G = \{1, -1, i, -i\}$ of fourth root of unity

Sol^n. Since 1 is the identity element, $O(1) = 1$.

$(-1)^2 = 1 \quad \therefore O(-1) = 2$.

$i^4 = 1 \quad \therefore O(i) = 4$

$-i^4 = 1 \quad \therefore O(-i) = 4$

2. Find the orders of the elements of the multiplicative group $G = \{1, \omega, \omega^2\}$ of cube roots of unity. [where $\omega = (-1 + i\sqrt{3})/2$]

Sol^n Since 1 is the identity element $O(1) = 1$.

$\omega^3 = 1 \quad \therefore O(\omega) = 3$

$(\omega^2)^3 = 1 \quad \therefore O(\omega^2) = 3$

3. Find the orders of the elements of the group.

$G = \langle Z_4, +_4 \rangle$.

Sol^n $Z_4 = \{0, 1, 2, 3\}$.

since 0 is the identity element $O(0) = 1$

$4(1) = 1 +_4 1 +_4 1 +_4 1 = 0 \quad \therefore O(1) = 4$

$2(2) = 2 +_4 2 = 0 \quad \therefore O(2) = 2$

$4(3) = 3 +_4 3 +_4 3 +_4 3 = 0 \quad \therefore O(3) = 4$

Note:

1. In the group $\langle Z, + \rangle$ of integers, every element except identity 0, is of infinite order.
2. In the multiplicative group of positive rational numbers, every element except the identity element 1, is of the infinite order.

Properties related to order of an element of a group

1. In a group G, $O(a) = O(a^{-1})$, for every $a \in G$.
2. If a is an element of the group G, is of order n, then $a^m = e$, for any integer m, if and only if n dives m.
3. If a and x be any two elements of the group G, then $O(a) = O(xax^{-1})$.
4. In a group G, $O(ab) = O(ba)$, $\forall\ a, b \in G$.
5. In a group G, the order of any element a cannot exceed that of the group. That is $O(a) \leq O(G)$.
6. Let G be a group and $a \in G$. If $O(a) = n$ and $(m, n) = 1$, then $O(a^m) = n$.
7. The order of any power of an element of a group cannot exceed the order of the element. ie, $O(a^k) \leq O(a)$.
8. If $O(a) = n$, where a is an element of the group G and $d = (n, m)$ then $O(a^m) = \frac{n}{d}$.

Examples

1. Give an example of a group to show that $O(ab)$ need not be equal to $O(a).O(b)$.

Sol: Consider the group $G = \{1, -1, i, -i\}$ of fourth roots of unity under multiplication.

$\because (-1)^2 = 1 \Rightarrow O(-1) = 2$ and $\because (-i)^4 = 1 \Rightarrow O(-i) = 4$.

Now $(-1).(-i) = i$ and $\because i^4 = 1 \Rightarrow O[(-1)(-i)] = 4$.

But $O(-1).O(-i) = 2 \cdot 4 = 8$

Thus $O[(-1)(-i)] \neq O(-1).O(-i)$.

Cyclic Groups

If G is a group and $a \in G$, the subset $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and is known as the cyclic subgroup of G generated by the element a. In this subgroup for every element $b \in H$, there exists an integer $m \in \mathbb{Z}$, such that $b = a^m$.

That is every element of H can be expressed as an integral power of a. For this reason, H is called the "subgroup generated by a".

If this property of expressing every element as an integral power of a single element, say a, holds good for the whole group, then such group is called a cyclic group generated by the element a.

A group G is said to be a cyclic group generated by the element $a \in G$ if $G = \{a^n \mid n \in \mathbb{Z}\}$ and is denoted by $G = \langle a \rangle$.

Note:

1. If the binary operation for the cyclic group $G = \langle a \rangle$ is $+$, then every element of G is of the form na for some $n \in \mathbb{Z}$.
2. A cyclic group may have more than one generator.
3. A cyclic group is said to be finite cyclic group, if the group is finite, otherwise it is said to be infinite cyclic group.

Examples

1. Show that the multiplicative group of fourth roots of unity is a cyclic group.

Sol^n $G_1 = \{1, -1, i, -i\}$

Now $(i)^1 = i$, $(i)^2 = -1$, $(i)^3 = -i$, $(i)^4 = 1$

Therefore i is a generator of G_1.

Thus G_1 is a cyclic group generated by the element i.

The element $-i$ is another generator of G_1.

2. Show that the group $\langle Z_5, +_5 \rangle$ is a cyclic group and every non zero element of Z_5 is a generator.

Sol^n $Z_5 = \{0, 1, 2, 3, 4\}$.

Consider $4 \in Z_5$ $\quad 4 = 1.4$

$$4 +_5 4 = 3 \Rightarrow 3 = 2.4$$

$$4 +_5 4 +_5 4 = 2 \Rightarrow 2 = 3.4$$

$$4 +_5 4 +_5 4 +_5 4 = 1 \Rightarrow 1 = 4.4$$

$$4 +_5 4 +_5 4 +_5 4 +_5 4 = 0 \Rightarrow 0 = 0.4$$

Thus every element of Z_5 can be expressed as some integral multiple of the element $4 \in Z_5$.

Therefore Z_5 is a cyclic group with 4 as a generator.

Similarly, one can verify other non zero element of Z_5 is also a generator.

Note

1. $\langle Z, + \rangle$ is an infinite cyclic group with 1 as a generator.
2. $\langle Z_n, +_n \rangle$ is a finite cyclic group with 1 as a generator.
3. $\langle Q, + \rangle$ is not a cyclic group.

[Let $\langle Q, + \rangle$ be a cyclic group generated by $m \in Q$.

Then $m = \frac{p}{q}$, $p, q \in Z$, $q \neq 0$.

Let $\frac{1}{2q} \in Q \Rightarrow \frac{1}{2q} = n.m$, $n \in Z \Rightarrow \frac{1}{2q} = n.\frac{p}{q} \Rightarrow \frac{1}{2} = n.p$.

It is impossible as the product of two integers is not equal to a fraction. Thus $\langle Q, + \rangle$ is not cyclic].

Properties of Cyclic Groups.

Theorem 1:

Every cyclic group is abelian.

Proof: Let G be a cyclic group with a as a generator.

Thus $G = \langle a \rangle = \{a^n / n \in Z\}$.

Let $x, y \in G$ be arbitrary.

Then there exists two integers m and n, such that

$$x = a^m \text{ and } y = a^n.$$

Consider $x \cdot y = a^m \cdot a^n$

$\Rightarrow x \cdot y = a^{m+n}$

$\Rightarrow x \cdot y = a^{n+m}$

$\Rightarrow x \cdot y = a^n \cdot a^m$

$\Rightarrow x \cdot y = y \cdot x$

Hence G is abelian.

Note: The converse of the above theorem is not true. That is every abelian group is not necessarily cyclic.

Consider $G = \{v_1, v_2, v_3, v_4\}$ and the associative binary composition $*$, given by the following table.

$*$	v_1	v_2	v_3	v_4
v_1	v_1	v_2	v_3	v_4
v_2	v_2	v_1	v_4	v_3
v_3	v_3	v_4	v_1	v_2
v_4	v_4	v_3	v_2	v_1

(i) v_1 is the identity element, since $v_1 * v_i = v_i = v_i * v_1 \quad \forall v_i \in G$.

(ii) $v_1^{-1} = v_1$, $v_2^{-1} = v_2$, $v_3^{-1} = v_3$, $v_4^{-1} = v_4$. Each element is inverse of itself.

(iii) The table is symmetric, Hence G is commutative.

Hence G is an abelian group.

This group $\langle G, * \rangle$ is known as the Klein's 4 group.

Here: $\langle v_1 \rangle = \{v_1\}$, $\langle v_2 \rangle = \{v_1, v_2\}$, $\langle v_3 \rangle = \{v_1, v_3\}$, $\langle v_4 \rangle = \{v_1, v_4\}$

Thus no element of G, generates the whole group G.

Hence G is not cyclic.

Theorem 2:
If a is a generator of a cyclic group G, then a^{-1} is also a generator.

Theorem 3:
If a is a generator of a cyclic group G, then $O(a) = O(G)$.

Theorem 4:
If G is a finite group of order n, containing an element of order n, then G is cyclic.

Theorem 5:
Let G be a cyclic group of order k and a be a generator. If $a^m = a^n (m \neq n)$, then $m \equiv n \pmod{k}$ and conversely.

Theorem 6:
Let G be a cyclic group of order d and a be a generator. The element $a^k (k < d)$ is also a generator of G, if and only if $(k, d) = 1$.

Theorem 7:
Every ~~cyclic~~ subgroup of a cyclic group is cyclic.

* Let d be any positive integer. The number of positive integers less than d and prime to d, is denoted by $\phi(d)$.
Any integer n can be decomposed into product of prime factors. i.e., $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, where $p_1, p_2 \ldots$ are prime factors
Then $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$

Theorem 8:
A cyclic group of order d has $\phi(d)$ generators.

Examples

1. Find the number of generators of the cyclic group of order 60.

Sol^n: Given $O(G)=60$

and $60 = 2^2 \times 3 \times 5$

$\therefore \varphi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 16$.

Thus G has 16 generators.

2. How many generators are there for the cyclic group of order 10. If a is a generator, what are the other generators?

Sol^n $10 = 2\times 5 \Rightarrow \varphi(10) = 10\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 4$.

Thus there are 4 generators.

By data a is a generator. The other generators are of the form a^k, with $(k,10)=1$.

Hence $k=1,3,7,9$. Thus the generators are a, a^3, a^7, a^9.

Note:

If the group operation is in addition form, and a is one of the generator, then other generators are of the form $k\cdot 1$ with $(k,n)=1$, where $O(G)=n$.

3. Find the number of generators of the cyclic group $(Z_{18}, +_{18})$. Write all the generators.

Sol^n $O(Z_{18})=18$ and $18 = 2\times 3^2 \Rightarrow \varphi(18) = 18\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=6$

Thus there are 6 generators.

We know that 1 is a generators.

$(k,18)=1 \Rightarrow k=1,5,7,11,13,17$.

Thus the generators are 1, 5, 7, 11, 13 and 17.

Coset Decomposition of a group.

Let $\langle G, * \rangle$ be a group and H be a subgroup of G. For $a, b \in G$ "a is said to be congruent to b modulo H" or aRb, if and only if $a.b^{-1} \in H$.

If a is congruent to b mod H, then we write $a \equiv b (\text{mod } H)$

The relation $a \equiv b (\text{mod } H)$ is an equivalence relation. Hence this relation gives a partition of G, into disjoint classes. Each member in the partition is a non-empty subset of G and any two distinct members of the the partition are disjoint.

If $a \in G$, we denote the equivalent class generated by a by $[a]$. i.e., $[a] = \{x \in G \mid x \equiv a (\text{mod } H)\}$

$= \{x \in G \mid x a^{-1} \in H\}$

Cosets of a subgroup H in a group G

Let H be a subgroup of a group $\langle G, * \rangle$ and a be any element of G.

The set Ha defined by $Ha = \{ha \mid h \in H\}$ is called the right coset of H in G w.r.t. a.

The set aH defined by $aH = \{ah \mid h \in H\}$ is called the left coset of H in G w.r.t. a.

Note

1. $Ha \neq \phi$ [$\because e \in H$ and $e.a = a \in Ha$]

   $aH \neq \phi$ [$\because e \in H$ and $a.e = a \in aH$]

2. $He = \{he \mid h \in H\} = \{h \mid h \in H\} = H$

   Similarly $eH = H$, and $He = H$.

   Thus every subgroup H itself is a right coset and as well left coset of H in G.

3. If G is abelian, then every right coset Ha is equal to corresponding left coset aH.

   i.e., if G is abelian $Ha = aH$. But in general $Ha \neq aH$

Results related to Cosets.

1. If H is a subgroup of a group G, then for all $a \in G$, $[a] = Ha$.

2. From the above theorem, we have $\forall a \in G$, $Ha = [a]$. Thus any two distinct cosets of H in G are disjoint and the union of all the right cosets of H is whole of G. In other words the collection of all distinct right cosets of H in G form a partition of the group G. This decomposition of the group G is called the "right coset decomposition" of the group G, w.r.t. the subgroup H.

   Similarly if one defines a relation called "congruence modulo H" on G by $a \equiv b \pmod H$ if and only if $b^{-1}a \in H$. It can be shown that $[a] = aH$ and hence the collection of all distinct left cosets of H in G form a partition of the group G. This decomposition of the group G is called the "left coset decomposition" of the group w.r.t. the subgroup H.

3. If H is a subgroup of G, then there exists a one-to-one correspondence between any two right (left) cosets of H in G.

4. There is one-to-one correspondence between the set of all right cosets and the set of all left cosets of a subgroup of a group.

Index of a subgroup:

The number of distinct right (left) cosets of a subgroup H of a group G is called the index of the subgroup H in G and is denoted by $[G : H]$ and read as "the index of H in G".

Lagrange's Theorem

If G is any finite group and H is any subgroup of G, then $O(H)$ divides $O(G)$.

Proof: Let $O(G) = n$ and $O(H) = m$.

We shall show that $m \mid n$ i.e., $n = km$, for some $k \in Z$

Since the group G is finite, there are finite number of right (left) cosets of H in G.

Let G have k distinct right (left) cosets of H and these are $Ha_1, Ha_2, \ldots, Ha_k \Rightarrow [G:H] = k$.

We know that any two right (left) cosets of H have the same number of elements.

In particular H itself is a right (left) coset of H in G.

Since $O(H) = m$, each right (left) coset of H will have m elements.

Also $G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_k$

$\therefore O(G) = O(Ha_1) + O(Ha_2) + \ldots + O(Ha_k)$

$\Rightarrow n = O(H) + O(H) + \ldots + O(H)$ (k cosets)

$\Rightarrow n = m + m + \ldots + m$ (k times)

$\Rightarrow n = km$

or $m \mid n$ i.e, $O(H) \mid O(G)$.

Note

1. The index of any subgroup of a finite group is a divisor of the order of the group.
   [i.e, if $O(G) = n$, $[G:H] = k$ then $k \mid n$ [It follows from Lagrange's theorem]]
2. The converse of Lagrange's theorem need not be true. i.e, If G is a finite group of order n and m is a positive integral divisor of n, then G need not have a subgroup of order m.
3. If $O(G) = n$, $O(H) = m$, & $[G:H] = k$, then the number of right (left) cosets of H in G is equal to $\frac{O(G)}{O(H)}$

Consequences of Lagrange's Theorem

1. If G is a finite group and $a \in G$, then $O(a)$ divides $O(G)$.
2. If G is a finite group of order n then $\forall a \in G$, $a^n = e$, where e is the identity element of G.
3. A finite group of prime order is cyclic and hence abelian.
4. If G is a cyclic group of prime order then G has no proper subgroup.
5. Every finite group of composite order has proper subgroups.
6. Any group of order five or less than five is abelian.
7. If G is a finite cyclic group of order k, then for every divisor n of k, there exists a unique subgroup of G of order n.

Examples

1. Consider the multiplicative group $G = \{1, -1, i, -i\}$ of fourth roots of unity and $H = \{-1, 1\}$ be a subgroup of G. Write all the right cosets of H in G.

Sol^n Here $O(G) = 4$, $O(H) = 2$

The number of distinct right cosets of H in G is $[G:H] = \frac{O(G)}{O(H)} = \frac{4}{2} = 2$.

The right cosets are $H.1 = \{-1, 1\}$ and $H.i = \{-i, i\}$

2. Find all the left cosets of $H = \{0, 4, 8\}$ in $\langle Z_{12}, +_{12} \rangle$

Sol^n Here $O(Z_{12}) = 12$ and $O(H) = 3$.

$\therefore$ number of distinct left cosets of H in $G = \frac{12}{3} = 4$.

These are

$0 +_{12} H = \{0, 4, 8\}$

$1 +_{12} H = \{1, 5, 9\}$

$2 +_{12} H = \{2, 6, 10\}$

$3 +_{12} H = \{3, 7, 11\}$.

3. List all the subgroups of the cyclic group of fourth roots of unity.

Sol^n $G = \{1, -1, i, -i\}$.

Here $O(G) = 4$ and i is a generator.

The divisors of 4 are 1, 2 and 4.

$\therefore$ The subgroups of G are the only subgroups generated by i, $i^2 = -1$ and $i^4 = 1$.

$\therefore$ The subgroups are

$\langle i \rangle = \{1, -1, i, -i\}$, $\langle -1 \rangle = \{1, -1\}$, $\langle 1 \rangle = \{1\}$.

4. List all the subgroups of a cyclic group G of order 24 and whose generator is g.

Sol^n Here $O(G) = 24$, $O(g) = 24$.

The divisors of 24 are 1, 2, 3, 4, 6, 8, 12 and 24.

$\therefore$ The subgroups of G are the only subgroups generated by $g, g^2, g^3, g^4, g^6, g^8, g^{12}$ and $g^{24} = e$.

5. Find all the subgroups of $\langle Z_{18}, +_{18} \rangle$.

Sol^n: 1 is a generator of Z_{18}.

The divisors of 18 are 1, 2, 3, 6, 9, 18.

∴ The generators of the subgroups are

$1 \cdot 1 = 1$, $1 \cdot 2 = 2$, $1 \cdot 3 = 3$, $1 \cdot 6 = 6$, $1 \cdot 9 = 9$, $1 \cdot 18 = 0$

Subgroups are $\langle 1 \rangle = Z_{18}$

$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$

$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\}$

$\langle 6 \rangle = \{0, 6, 12\}$

$\langle 9 \rangle = \{0, 9\}$

$\langle 0 \rangle = \{0\}$.

Exercise.

1. Find all the right cosets of the subgroup $H = \{0, 3\}$ in the group $\langle Z_6, +_6 \rangle$.
2. Find all the right cosets of the subgroup $H = \{1, 3, 9\}$ in the group $\langle Z_{13} - \{0\}, \times_{13} \rangle$.
3. List all the subgroups of $\langle Z_9, +_9 \rangle$.
4. Find all the subgroups of $\langle Z_6, +_6 \rangle$.
5. Find the number of elements in the cyclic subgroup of $\langle Z_{12}, +_{12} \rangle$ generated by 3 and 8.

[Hint: If g is a generator of a cyclic group G of order n, then g^m generates a subgroup H of G of order $\frac{n}{d}$, where $d = (n, m)$]

6. Find all the left cosets of $H = \{0, 3, 6, 9\}$ in $\langle Z_{12}, +_{12} \rangle$ and verify Lagrange's theorem in each case.

Homomorphism:

Let $\langle G, \cdot \rangle$ and $\langle G', * \rangle$ be two groups. A mapping $f: G \to G'$ is said to be a homomorphism if

$$f(g_1 \cdot g_2) = f(g_1) * f(g_2) \quad \forall\ g_1, g_2 \in G.$$

That is the mapping f is said to be a homomorphism, if f maps the composition of any two elements of G into the composition of the images of the elements. By this we say that f preserves composition. If f is a homomorphism from the group G into G', we say G is homomorphic to the group G'.

Isomorphism

A homomorphism f from a group G into G' is said to be isomorphism if f is a bijection. i.e., f is both one-one and onto.

Two groups G and G' are said to be isomorphic, if there exists an isomorphism $f: G \to G'$. This we denote it by $G \approx G'$.

Endomorphism

A homomorphism f from a group G into itself is called Endomorphism.

Automorphism

An isomorphism f from a group G onto itself is called Automorphism.

Note: The identity map $I_G: G \to G$ from the group G onto itself, defined by $I_G(g) = g$ is a homomorphism. This shows that there exists atleast one homomorphism from G into itself. Further $I_G(g) = g$ is an automorphism.

Examples

1. Let $\langle G, \cdot \rangle$ and $\langle G', * \rangle$ be two groups and e' be the identity element of G'. Define $f: G \to G'$ by $f(g) = e' \ \forall \ g \in G$. Show that f is a homomorphism.

Sol^n Consider, $f(g_1 \cdot g_2) = e'$, $g_1 \cdot g_2 \in G$.

Also, $f(g_1) * f(g_2) = e' * e' = e'$

$\therefore f(g_1 \cdot g_2) = f(g_1) * f(g_2)$.

Hence f is a homomorphism.

This homomorphism is called a trivial homomorphism.

2. Consider the additive group $\langle Z, + \rangle$ of all integers and the group $H = \{1, -1\}$ under multiplication. Define $\varphi: Z \to H$ by $\varphi(n) = \begin{cases} 1 & \text{if } n \text{ is even or zero} \\ -1 & \text{if } n \text{ is odd} \end{cases}$

Show that φ is a homomorphism.

Sol^n let $m, n \in Z$

Case (i) Let m and n are both even.

Then $m+n$ is even $\Rightarrow \varphi(m+n) = 1$.

Also $\varphi(m) = 1$ and $\varphi(n) = 1$.

$\therefore \varphi(m+n) = \varphi(m) \cdot \varphi(n)$.

Case (ii) Let one of m and n be even, say m be even and n be odd. Then $m+n$ is odd $\Rightarrow \varphi(m+n) = -1$,

Also $\varphi(m) = 1$ and $\varphi(n) = -1$

$\therefore \varphi(m+n) = \varphi(m) \cdot \varphi(n)$.

Case (iii) Let m and n are both odd.

Then $m+n$ is even $\Rightarrow \varphi(m+n) = 1$.

Also $\varphi(m) = -1$ and $\varphi(n) = -1$

$\therefore \varphi(m+n) = \varphi(m) \cdot \varphi(n)$.

Hence φ is an homomorphism.

3. Let $M_n(\mathbb{R})$ be the group of all non-singular $n \times n$ matrices with real entries under matrix multiplication. Let $\mathbb{R}^*$ be the multiplicative group of non-zero real numbers. If $\varphi: M_n(\mathbb{R}) \to \mathbb{R}^*$ is defined by $\varphi(A) = |A|, \forall A \in M_n(\mathbb{R})$, show that φ is a homomorphism.

Sol^n Consider $\varphi(AB) = |AB|, \forall A, B \in M_n(\mathbb{R})$

$$= |A| \cdot |B|$$

$$\varphi(AB) = \varphi(A) \cdot \varphi(B).$$

Hence φ is a homomorphism.

4. Consider the multiplicative group $\langle \mathbb{R}^*, \cdot \rangle$ of all non-zero real numbers. Define $f: \mathbb{R}^* \to \mathbb{R}^*$ by $f(x) = 2^x \ \forall x \in \mathbb{R}^*$. Verify if f is a homomorphism.

Sol^n Consider $f(xy) = 2^{xy}$

and $f(x) = 2^x$, $f(y) = 2^y$ $\therefore f(x) \cdot f(y) = 2^x \cdot 2^y = 2^{x+y}$

$\therefore f(xy) \neq f(x) \cdot f(y)$

Hence f is not a homomorphism.

5. Define $f: \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}, + \rangle$ by $f(x) =$ greatest integer $\leq x$. Is f a homomorphism?

Sol^n By definition of f, $f(1) = 1$, $f(\frac{1}{2}) = 0$, $f(\frac{3}{2}) = 1$, ... so on

Consider $f(\frac{3}{2}) = 1$ and $f(\frac{5}{2}) = 2$

$$f(\tfrac{3}{2} + \tfrac{5}{2}) = f(4) = 4$$

Also $f(\frac{3}{2}) + f(\frac{5}{2}) = 1 + 2 = 3$

$\therefore f(\frac{3}{2} + \frac{5}{2}) \neq f(\frac{3}{2}) + f(\frac{5}{2})$

$\therefore f$ is not a homomorphism.

Elementary properties of Homomorphism

1. Let $f: G \to G'$ be a homomorphism from the group $\langle G, \cdot \rangle$ into the group $\langle G', * \rangle$. Then
   (i) $f(e) = e'$ where e and e' are the identity elements of the group G and G' respectively.
   (ii) $f(a^{-1}) = [f(a)]^{-1}$, $\forall\ a \in G$.
2. If f is a homomorphism of a group G into G', then the range $f(G) = \{f(g) \mid g \in G\}$ is a subgroup of G'. The set $f(G) = \{f(g) \mid g \in G\}$ is called the homomorphic image of G in G'.
3. If $f: G \to G'$ is a homomorphism of a group G into G' and H is a subgroup of G, then $f(H)$ is again a subgroup of G'.
4. If $f: G \to G$ be a homomorphism from the group G into itself and H is a cyclic subgroup of G, then $f(H)$ is again a cyclic subgroup of G.

Kernel of a Homomorphism:

Let $f: G \to G'$ be a homomorphism from the group G into G' and e' be the identity element of G'. The subset K of G defined by $K = \{a \in G \mid f(a) = e'\}$ is called the Kernel of the Homomorphism f and is denoted by $\ker f$.

Examples

1. If $f: \mathbb{C}^* \to \mathbb{C}^*$ is a homomorphism defined by $f(a+ib) = a-ib \ \forall\ a+ib \in \mathbb{C}^*$, find $\ker f$.

Sol^n

$$\ker f = \{x \in \mathbb{C}^* \mid f(x) = e'\}$$
$$= \{a+ib \mid f(a+ib) = 1\} \quad [\because e' = 1]$$
$$= \{a+ib \mid a-ib = 1\}$$
$$= \{a+ib \mid a=1, b=0\}$$
$$\ker f = \{1\}$$

2. Consider the homomorphism $f: \langle \mathbb{R}^+, \cdot \rangle \to \langle \mathbb{R}, + \rangle$, where $\langle \mathbb{R}^+, \cdot \rangle$ is the multiplicative group of all positive real numbers and $\langle \mathbb{R}, + \rangle$ is the additive group of all real numbers, defined by $f(x) = \log_{10} x$. Find $\ker f$.

Sol^n

$$\ker f = \{x \in \mathbb{R}^+ \mid f(x) = 0\}$$
$$= \{x \in \mathbb{R}^+ \mid \log_{10} x = 0\}$$
$$= \{x \in \mathbb{R}^+ \mid x = 1\}$$
$$= \{1\}$$

Results related to Isomorphism

1. If $f: G \to G'$ be an isomorphism of a group G onto a group G' and a is any element of G, then the order of $f(a)$ equals the order of a.
2. Let $f: G \to G'$ be an isomorphism. If G is abelian, then G' is also abelian.
3. Any infinite cyclic group is isomorphic to the group $\mathbb{Z}$ of integers, under addition.
4. Any finite cyclic group of order n is isomorphic to additive group of integers modulo n.

Examples

1. Show that the additive group $\langle \mathbb{R}, + \rangle$ of all real numbers and the multiplicative group $\langle \mathbb{R}^+, \cdot \rangle$ of all positive real numbers are isomorphic.

Sol^n Define $f: \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}^+, \cdot \rangle$ by $f(x) = e^x \; \forall x \in \mathbb{R}$.

Now $f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$

$\therefore f$ is a homomorphism.

Again, $f(x) = f(y) \Rightarrow e^x = e^y$

$\Rightarrow e^{x-y} = 1 = e^0$

$\Rightarrow x - y = 0$

$\Rightarrow x = y$

$\therefore f$ is one-one.

Let $y \in \mathbb{R}^+$, Consider $f(\log_e^y) = e^{\log_e^y} = y$

$\therefore \forall y \in \mathbb{R}^+ \; \exists \; \log_e^y \in \mathbb{R}$ such that $f(\log_e^y) = y$

$\therefore f$ is onto

Hence f is a isomorphism.

2. Let $G=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R}^*\right\}$. show that $f:\langle G,\cdot\rangle \to \mathbb{R}^*$ defined by $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}=a$ is an isomorphism.

Sol:

$$f\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}\right)=f\begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}=ab=f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\cdot f\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$$

$\therefore f$ is a homomorphism.

Let $f(a)=f(b) \Rightarrow \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow a=b$.

$\therefore f$ is one-one.

Let $a \in \mathbb{R}^*$, Consider $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}=a$.

$\therefore \forall\, a \in \mathbb{R}^*$, $\exists \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in \langle G,\cdot\rangle$ such that $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}=a$.

$\therefore f$ is onto.

Hence f is an isomorphism.

Exercise!

1. Verify if the following maps are homomorphisms. If the map is a homomorphism, find its kernel.

(i) $f:\langle \mathbb{R},+\rangle \to \langle \mathbb{R}^+,\cdot\rangle$ defined by $f(x)=e^x \;\forall\, x \in \mathbb{R}$

(ii) $f:\langle \mathbb{Z},+\rangle \to \langle \mathbb{Z}_n,+_n\rangle$ defined by $f(a)=r, \forall a \in \mathbb{Z}$, where r is the unique least non negative remainder when a is divided by n.

(iii) $g:\langle \mathbb{C}^*,\cdot\rangle \to \langle \mathbb{C}^*,\cdot\rangle$ defined by $g(z)=|z|, \forall z \in \mathbb{C}^*$.

(iv) $f:\langle \mathbb{R},+\rangle \to \langle \mathbb{R},+\rangle$ defined by $f(x)=3x+1, \forall x \in \mathbb{R}$

2. Show that the following mappings are isomorphisms.

(i) $T:\langle G,+\rangle \to \langle G,+\rangle$, where $G=\{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$, defined by $T(a+b\sqrt{2})=a-b\sqrt{2}$.

(ii) G is any group & g a fixed element of G.
$T:G \to G$ defined by $T(x)=gxg^{-1}$.