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 semi group 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 $*$.

Note: 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 vector cross product.

examples

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

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

Hence $\frac{1}{a_1+ib_1}$ 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) $\forall\ a \in N,\ a+0 = a = 0+a$,

~~Hence 0 is the identity element.~~

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

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

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

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

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

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

$\therefore (a*b)*c \neq a*(b*c)$, $\langle \mathbb{R}, * \rangle$ 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 $e * e' = e'$ — (1)

Again as e' is an identity element, we have $e * e' = e$ and $e' * e = e$ — (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 $a * b = e = b * a$ — (1)

Again as c is an inverse of a, we have, $a * c = e = c * a$ — (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 $(a^{-1})^{-1} = a$.

Proof:

Let $x = a^{-1}$. We shall show that $x^{-1} = a$.

To show that $x^{-1} = a$ we have to establish $a * x = e = x * a$.

Now consider, $a * x = a * a^{-1} = e$ — (1)

Again, $x * a = a^{-1} * a = e$ — (2)

$\therefore$ by (1) & (2), $x^{-1} = a \Rightarrow (a^{-1})^{-1} = a$ $[\because x = a^{-1}]$

Theorem 4:

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

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

Proof:

We need to show that $b^{-1} * a^{-1}$ is the inverse of $a * b$.

Let $x = b^{-1} * a^{-1}$ and $y = a * b$.

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

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

$= (b^{-1} * e) * b$ $[\because a^{-1}$ is the inverse of $a]$

$= b^{-1} * b$ $[\because e$ is the identity$]$

$x * y = e$ — (1)

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

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

$= (a * e) * a^{-1}$ $[\because b^{-1}$ is the inverse of $b]$

$= a * a^{-1}$ $[\because e$ is the identity$]$

$y * x = e$ — (2)

From (1) and (2) $\Rightarrow x$ is the inverse of y

i.e., $x = y^{-1}$

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

This result is called the reversal law.

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]

Proof:

(i) Consider $(a * x) = (a * y)$

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

$\Rightarrow (a^{-1} * a) * x = (a^{-1} * a) * y$ (associative law)

$\Rightarrow e * x = e * y$ [$\because a^{-1}$ is the inverse of a]

$\Rightarrow x = y$ [$\because e$ is the identity]

Hence $a * x = a * y \Rightarrow x = y$

(ii) Consider $(x * a) = (y * a)$.

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

$\Rightarrow x * (a * a^{-1}) = y * (a * a^{-1})$ associative law.

$\Rightarrow x * e = y * e$ [$\because a^{-1}$ is the inverse of a]

$\Rightarrow x = y$ [$\because e$ is the identity.

Hence $x * a = y * a \Rightarrow x = y$.

$\longrightarrow$

Theorem 6:

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

Proof:

Consider the equation $a * x = b$

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

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

$\Rightarrow e * x = a^{-1} * b$

$\Rightarrow x = a^{-1} * b$

Hence the solution of $a * x = b$ is $x = a^{-1} * b$.

To show that the solution is unique, we shall assume that there are two solutions say x_1 and x_2

ie, $a * x_1 = b$ and $a * x_2 = b$

$\Rightarrow a * x_1 = a * x_2$.

$\Rightarrow x_1 = x_2$ (by left cancellation law)

Hence the solution is unique.

Consider $y * a = b$

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

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

$\Rightarrow y * e = b * a^{-1}$

$\Rightarrow y = b * a^{-1}$

Hence the solution of $y * a = b$ is $y = b * a^{-1}$

To show that the solution is unique, we shall assume that there are two solutions say y_1 and y_2.

ie, $y_1 * a = b$ and $y_2 * a = b$

$\Rightarrow y_1 * a = y_2 * a$

$\Rightarrow y_1 = y_2$ (by right cancellation law)

Hence the solution is unique.

Examples.

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

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, $a^{-1} = a$].

Sol^n 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 $(ab)^2 = a^2b^2$, $\forall\ a, b \in G$

Sol^n 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 $\langle \mathbb{Q}^+, * \rangle$, where $\mathbb{Q}^+$ 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 $\{0, 1, 2, 3, 4, 5\}$.

Soln

$+_6$	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) $3 \times_5 (4 \times_5 2) = 3 \times_5 3 = 4$

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

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

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.

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

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

(iii) 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 $\because 4 \times_5 4 = 1 = 4 \times_5 4$.

$\therefore$ In $\langle G, \times_5 \rangle$, the inverse of each element exists

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

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

Therefore $\langle G, \times_5 \rangle$ 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 $\times_4$.

Sub groups

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) $a \in H \Rightarrow a^{-1} \in H$.

Proof (a) Let H be a subgroup of G. We shall show the conditions (i) and (ii) are true.

Since H is a subgroup of G, H is a group by itself.

Hence H is closed under the binary operation $*$.

ie, $\forall\ a, b \in H,\ a * b \in H$.

Again, as H is a subgroup under $*$, by the existence of inverse axiom, $a \in H \Rightarrow a^{-1}$ exists and $a^{-1} \in H$.

Hence (i) and (ii) are true.

(b) Conversely let H be a subset of G such that (i) and (ii) are true. We shall show that H is a group by itself under the binary operation $*$.

By condition (i) $\forall\ a, b \in H \Rightarrow a * b \in H$, Hence H is closed under $*$.

Since $*$ is associative in G, $*$ is associative in particular in H.

By condition (ii) $a \in H \Rightarrow a^{-1} \in H$, the inverse exists in H

This implies $a * a^{-1} \in H$ i.e, $e \in H$, the identity exists in H.

Hence H is a group by itself and hence a subgroup of G.

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

Proof.
(a) Let H be a subgroup of $\langle G, * \rangle$. We shall show that $\forall a, b \in H, a * b^{-1} \in H$.
Since H is a subgroup of G, H is a group by itself.
$\therefore b \in H \Rightarrow b^{-1} \in H$.
Now $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a * b^{-1} \in H$.
(b) Conversely, let H be a non empty subset of G such that $\forall a, b \in H \Rightarrow a * b^{-1} \in H$.
we shall show that H is a group by itself under the binary operation $*$.
Now let $a \in H, a^{-1} \in H \Rightarrow a * a^{-1} \in H \Rightarrow e \in H$.
Hence H contains the identity element.
Now, $e \in H, a \in H \Rightarrow e * a^{-1} \in H \Rightarrow a^{-1} \in H$.
Thus inverse of a exists in H.
let $a, b \in H$, then $a \in H, b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} \in H \Rightarrow a * b \in H$.
Hence H is closed under $*$.
Since $*$ is associative in G, $*$ is associative in particular in H.
Hence H is a group by itself and hence a subgroup of G.

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 integers n and m.
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, $1 \in H, 1 \in H \Rightarrow 1.1^{-1} = 1.1 = 1 \in H$
$-1 \in H, -1 \in H \Rightarrow (-1).(-1)^{-1} = (-1).(-1) = 1 \in H$
$1 \in H, -1 \in H \Rightarrow 1.(-1)^{-1} = 1.(-1) = -1 \in H$
$-1 \in H, 1 \in H \Rightarrow (-1).1^{-1} = (-1).1 = -1 \in H$

Thus $\forall\ a, b \in H,\ a.b^{-1} \in H$
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) $0^{-1} = 0, 2^{-1} = 4 \in H, 4^{-1} = 2 \in H$.

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 $x, y \in K$
$\Rightarrow xy \in H$ and $xy \in K$ [$\because$ H and K are subgroups of G]
$\Rightarrow (xy) \in H \cap K$.

(ii) let $x \in H \cap K \Rightarrow x^{-1} \in H$ 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 $\langle Z_6, +_6 \rangle$, where $Z_6 = \{0,1,2,3,4,5\}$ Show that $H = \{0,2,4\}$ is a subgroup of Z_6.
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 $\mathbb{Z}$.