# CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY

## FACULTY OF APPLIED SCIENCES

## DEPARTMENT OF MATHEMATICAL SCIENCES

## SEMESTER 3 B.Tech CE, IT, CSE

## DISCRETE MATHEMATICS AND ALGEBRA

## MA253

## UNIT 5

## ABSTRACT ALGEBRA

**<u>OUTLINE OF UNIT 5 – ABSTRACT ALGEBRA</u>**

- **BINARY OPERATIONS**
- **COMPOSITION TABLE/ COMPOSITE TABLE**
- **ALEGBRAIC STRUCTURE**
- **GROUPOID, SEMI GROUP, MONOID**
- **GROUP AND ABELIAN GROUP**
- **ORDER OF THE GROUP AND ELEMENT**
- **SUBGROUP, LAGRANGE’ S THEOREM**
- **CYCLIC GROUP, PERMUTATION GROUP**
- **PERMUTATION GROUP**

**BINARY OPERATION/BINARY COMPOSITION:** A binary composition or binary operation on a non empty set A is a mapping $f: A \times A \to A$. Suppose $a, b \in A$, then the image of (a,b) under a binary composition/operation $*$ defined by $a * b$ has to be in A.

**ALEGBRAIC STRUCTURE**: A non empty set G with one or more binary operations is called an algebraic structure. Suppose * is a binary operation on G. Then $(G,*)$ is an algebraic structures.

$(N, +), (Z, +), (Q, +), (R, +) (N, -), (Z, -), (Q, -), (R, -)$
$(N,*), (Z,*), (Q,*), (R,*), (N,/)$, (Z,/), $(Q,/)$, (R,/). .

**COMPOSITION TABLE :** A binary composition (operation) on the non empty finite set A can be defined by table is called a composition table.

**Example: The composition table for multiplication modulo 7 on the set G={0,1,2,3,4,5,6}. $(\mathbb{Z}_7, \times_7)$ is an Algebraic Structure.**

| $\times_7$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

# GROUP

**Identity Element:** There exist an element $e \in G$ such that

$$a * e = a = e * a, \forall a \in G.$$

The element e is called the identity.

**Inverse Element :** There exist an element $a^{-1} \in G$ such that

$$a * a^{-1} = e = a^{-1} * a, \forall a \in G$$

**GROUP:** Let G be a non-empty set with a binary operator denoted by $*$ .Then this algebraic structure $(G,*)$ is a group, if the binary $*$ satisfies the following properties:

1. **Closure property:** $a * b \epsilon G \quad \forall a, b \epsilon G$
2. **Associativity:** $(a * b) * c = a * (b * c) \forall a, b, c \epsilon G$
3. **Existence of Identity:** There exist an identity element $e \in G$ such that
$$a * e = a = e * a, \forall a \epsilon G.$$
4. **Existence of Inverse:** Each element of G possesses inverse i.e.,
$$a * a^{-1} = e = a^{-1} * a, \forall a \in G$$

**ABELIAN GROUP:** A group is said to be abelian or commutative if in addition to the above four properties the following properties is also satisfied i.e.

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

**FINITE GROUP & INFINITE GROUP:** If in a group G the underlying set G consists of a finite number of distinct elements then the group is called a finite group otherwise an infinite group.

## EXAMPLES OF GROUP

**Example: Show that the set $\mathbb{Z}$ of all integers $\mathbb{Z} = \{\dots\dots -\mathbf{4}, -\mathbf{3}, -\mathbf{2}, -\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \dots\dots\}$ is a group with respect to the operation of addition of integers.**

**Solution: Closure property:** We know that the sum of two integers is also an integer.

i.e., $a + b \in \mathbb{Z}$. Thus $\mathbb{Z}$ is closed w.r.t to addition.

**Associativity:** We know that addition of integers is an associative .Therefore

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

**Existence of Identity:** The number $0 \in \mathbb{Z}$. Also we have

$$0+a=a=a+0.$$

Therefore 0 is the identity element.

**Existence of Inverse:** If $a \in \mathbb{Z}$, then $-a \in \mathbb{Z}$. Also we have

$$(-a) + a = 0 = a + (-a).$$

Thus every integer possesses additive inverse. Therefore $\mathbb{Z}$ is group with respect to addition . Since addition of integer is a commutative operator.

$\mathbb{Z}$ is an abelian group.

**Example:** Show that the set of all positive rational number forms an abelian group under the composition defined by

$$a * b = \frac{ab}{2}$$

**Solution:** Let $Q_+$ denote the set of all positive rational number. To show: ($Q_+$, *) is a group.

**Closure Property:** We know that multiplication and division of two rational number is a rational number therefore $\boldsymbol{\frac{ab}{2}}$ is a rational number. Thus for every a, b ∈ $Q_+ \Rightarrow$ a*b∈ $Q_+$

Thus $Q_+$ is closed with respect to the operator *.

**Associativity:** Let a,b,c ∈ $Q_+$. Then

L.H.S: a*(b*c)=$a * \left(\frac{bc}{2}\right) = \frac{abc}{4}$

R.H.S: (a*b)*c=$\left(\frac{ab}{2}\right) * c = \frac{abc}{4}$

L.H.S=R.H.S

* is associative.

**Commutativity:** Let a,b∈ $Q_+$. Then

$$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$$

**Existence of Identity:** Let e be the identity element in $Q_+$.
By definition of identity element

$$a * e = a = e * a \,, \forall\, a \epsilon Q_+$$

**Now**

$$a * e = a \Longrightarrow \frac{ae}{2} = a \Longrightarrow \left(\frac{a}{2}\right)(e-2) = 0 \Longrightarrow e = 2 \;\; since\ a\epsilon Q_+ \Longrightarrow a \neq 0$$

$$e * a = a \Longrightarrow \frac{ea}{2} = a \Longrightarrow \left(\frac{a}{2}\right)(e-2) = 0 \Longrightarrow e = 2 \;\; since\ a\epsilon Q_+ \Longrightarrow a \neq 0$$

Therefore 2 is identity element.

**Existence if Inverse:** Let a be any element of $Q_+$. Let b be inverse of a then by definition of inverse

$$a * b = e = b * a$$

**Now** $\quad a * b = e \Longrightarrow \frac{ab}{2} = 2 \Longrightarrow b = \frac{4}{a}$

Now $a\epsilon Q_+ \Longrightarrow \frac{4}{a}\ \epsilon Q_+$

Now $\quad a * \frac{4}{a} = 2 = \frac{4}{a} * a$. Therefore $\frac{4}{a}$ is inverse of a .Thus each element of $Q_+$is invertible. Hence ($Q_+$, *) is a group.

**Example: Check whether the set $\boldsymbol{G} = \left\{\boldsymbol{a} + \boldsymbol{b}\sqrt{\mathbf{2}} : \quad \boldsymbol{a}, \boldsymbol{b}, \in \boldsymbol{Q}\right\}$ is group with respect to addition or not.**

**Solution: Closure Property:** Let x, y be any two elements of G. Then

$$x = a + b\sqrt{2}\,;\; y = c + d\sqrt{2}$$

Now

$$x + y = a + b\sqrt{2} + c + d\sqrt{2}$$
$$= (a + c) + (c + d)\sqrt{2}$$

Since a+c and c+d are elements of Q, therefore $(a + c) + (c + d)\sqrt{2} \in G$ .

Thus $x + y \epsilon G, \;\; \forall x, y \epsilon G$

Thus G is closed with respect to addition.

**Associativity:** The element of G are all real numbers and addition of real numbers is associative. Hence associativity holds true.

**Existence of Identity:** Observe that $0 + 0\sqrt{2} \in G$ since $0 \in Q$. If $a + b\sqrt{2}$ is any element of G, then

$$(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = a + b\sqrt{2} = 0 + 0\sqrt{2} + (a + b\sqrt{2})$$

$0 + 0\sqrt{2}$ is the identity element.

**Existence of Inverse:** Since $a, b, \in Q \Rightarrow -a, -b, \in Q$ and hence

$a + b\sqrt{2}\,\epsilon G \Rightarrow (-a) + (-b)\sqrt{2}\,\epsilon G$

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

$$= (-a) + (-b)\sqrt{2} + (a + b\sqrt{2})$$

Therefore $(-\boldsymbol{a}) + (-\boldsymbol{b})\sqrt{\mathbf{2}}$ is the inverse element.

***Thus, tht set G*** $= \{\boldsymbol{a} + \boldsymbol{b}\sqrt{\mathbf{2}} : \ \boldsymbol{a}, \boldsymbol{b}, \in \boldsymbol{Q}\}$ **is a group with respect to addition.**

**Example: Show that the set of all matrices of the form $\begin{bmatrix} \boldsymbol{x} & \boldsymbol{x} \\ \boldsymbol{x} & \boldsymbol{x} \end{bmatrix}$, where x is a non zero real number, is a group of singular matrices for multiplication. Find the identity and inverse of an element.**

**Solution:** Let $M = \left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} : x \text{ } is \text{ } a \text{ } non \text{ } zero \text{ } real \text{ } number \right\}$.

**Closure Property**: Let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \in M, B = \begin{bmatrix} y & y \\ y & y \end{bmatrix} \in M$, where x and y are non zero real numbers.

Now $AB = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \begin{bmatrix} y & y \\ y & y \end{bmatrix} = \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \in M$, because "2xy" is also a non zero real number.

**Associativity:** Matrix Multiplication is always associative. $(i.e. (AB)C = A(BC))$

- **Existence of identity:** Let $E = \begin{bmatrix} e & e \\ e & e \end{bmatrix}$ be such that $E \cdot A = A, \forall A \in M$.
- Let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \in M$. Then
- $E \cdot A = A \Rightarrow \begin{bmatrix} e & e \\ e & e \end{bmatrix} \begin{bmatrix} x & x \\ x & x \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \Rightarrow \begin{bmatrix} 2ex & 2ex \\ 2ex & 2ex \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \Rightarrow 2ex = x \Rightarrow$ $e = \frac{1}{2}$,
- $since \text{ } x \neq 0$.

Thus $E = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \in M$ as $\frac{1}{2} \neq 0$ and is such that $E \cdot A = A = A \cdot E, \forall A \in M$.

**Existence of inverse:** If $C = \begin{bmatrix} c & c \\ c & c \end{bmatrix}$ be the inverse then $C \cdot A = E, \forall A \in M$.

Let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \in M$.

$$\therefore CA = E \Rightarrow \begin{bmatrix} c & c \\ c & c \end{bmatrix}\begin{bmatrix} x & x \\ x & x \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \Rightarrow \begin{bmatrix} 2cx & 2cx \\ 2cx & 2cx \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \Rightarrow 2cx = \frac{1}{2} \Rightarrow c = \frac{1}{4x}$$

Thus $C = \begin{bmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{bmatrix} \in M$ as $x \neq 0$ such that $C \cdot A = E = A \cdot C, \forall A \in M$.

Thus $C = \begin{bmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{bmatrix} \in M$ is the inverse of A.

Hence M is a group w.r.t. matrix multiplication.

**Example: Check whether the set S of all ordered pairs (a,b) of real numbers for which $\boldsymbol{a \neq 0}$ with respect to the operation $*$ defined by $(\boldsymbol{a}, \boldsymbol{b}) * (\boldsymbol{c}, \boldsymbol{d}) = (\boldsymbol{ac}, \boldsymbol{bc} + \boldsymbol{d})$ is a group w.r.t $*$ or not.**

**Solution: Closure Property:** Let $(a, b)$ and $(c, d)$ be any two element of S. Then

$a \neq 0$ and $c \neq 0$.

Now $(\boldsymbol{a}, \boldsymbol{b}) * (\boldsymbol{c}, \boldsymbol{d}) = (\boldsymbol{ac}, \boldsymbol{bc} + \boldsymbol{d}) \in \boldsymbol{S}$ (because $a \neq 0$ and $c \neq 0 \Rightarrow ac \neq 0$)

Hence S is closed with respect to the given composition( binary operation)

**Associativity:** Let $(a, b), (c, d), (e, f)$ be any three element of S.

L.H.S. $[(a, b) * (c, d)] * (e, f)$

$=(ac, bc + d) * (e, f) = (ace, (bc + d)e + f) = (ace, bce + de + f)$

R.H.S. $(a, b) * [(c, d) * (e, f)]$

$=(a, b) * (ce, de + f)$

$=(ace, b(ce) + de + f) = (ace, bce + de + f)$

Hence the given composition $*$ is associative.

**Existence of Identity:** Let $(x, y)$ be identity element of S such that

$$(x, y) * (a, b) = (a, b) = (a, b) * (x, y) \Rightarrow (xa, ya + b) = (a, b)$$

$$\Rightarrow xa = a; ya + b = b$$

We get $x = 1$ and $y = 0$.

Therefore (1,0) is the identity element.

**Existence of inverse:** Let $(c, d) \in S, c \neq 0$ be inverse of $(a, b) \in S$.

Now

$$(a, b) * (c, d) = (1,0) = (c, d) * (a, b)$$

$$\Rightarrow (ac, bc + d) = (1,0)$$

$$\Rightarrow ac = 1, bc + d = 0$$

$$\Rightarrow c = \frac{1}{a} \neq 0; d = -\frac{b}{a}$$

Hence $\left(\frac{1}{a}, -\frac{b}{a}\right)$ is an inverse of element (a,b).

**Hence the set S of all ordered pairs (a,b) of real numbers for which $\boldsymbol{a \neq 0}$ with respect to the operation $*$ defined by $(\boldsymbol{a}, \boldsymbol{b}) * (\boldsymbol{c}, \boldsymbol{d}) = (\boldsymbol{ac}, \boldsymbol{bc} + \boldsymbol{d})$ is a group**

- **GROUPOID**: Suppose G is non empty set and $*$ is a binary operation then (G,$*$) is called a groupoid if $*$ is closed in G, that is, given any two elements

$$a, b \in G \Rightarrow a * b \in G$$

- **SEMI GROUP**: A non empty set G together with binary operation $*$, $(G,*)$ is a semi group if binary operation $*$ is associative.
- **MONOID**: A non empty set G together with a binary operation $*$, $(G,*)$ is called a monoid if it satisfies the following properties:

  (1) $*$ is closed in $(G,*)$

  (2) $*$ is associative in $(G,*)$

  (3) There exist an identity element in $(G,*)$

**Example: The set of all integers $\mathbb{Z}$ with operation defined by $\boldsymbol{a * b = a + b + 1}$.**

**(1) Is $\mathbb{Z}$ Groupoid?**

**(2) Is $\mathbb{Z}$ a Semi Group?**

**(3) Is $\mathbb{Z}$ a monoid?**

## Solution:

**Groupoid:** To prove G is groupoid , prove that G is closed w.r.t $*$, let

$a, b \in \mathbb{Z} \Rightarrow a + b + 1 \in \mathbb{Z}$ (sum of integers is always integer). Hence $a * b \in G$.

Therefore G is closed w.r.t to operation $*$.

G is a groupoid.

**Semi Group:** To prove G is Semigroup ,prove that $*$ is associative i.e., to prove $(a * b) * c = a * (b * c)$.

Let $a, b, c \in Z$.

L.H.S: $(a * b) * c = (a + b + 1) * c = a + b + 1 + c + 1 = a + b + c + 2$

R.H.S: $a * (b * c) = a * (b + c + 1) = a + 1 + b + c + 1 = a + b + c + 2$

Therefore $*$ is associative.

**Monoid:** To prove G is monoid, G must satisfies closure property, Associative property, identity property.

**Closure property:** Let $a, b \in \mathbb{Z} \Rightarrow a + b + 1 \in \mathbb{Z}$

( Sum of integers is always an integer)

So $a * b \in G$.

Therefore G is closed w.r.t. to operation $*$.

**Associative property:**

Let $a, b, c \in \mathbb{Z}$.

L.H.S: $(a * b) * c = (a + b + 1) * c = a + b + 1 + c + 1 = a + b + c + 2$

R.H.S: $a * (b * c) = a * (b + c + 1) = a + 1 + b + c + 1 = a + b + c + 2$

Therefore $*$ is associative.

**Existence of Identity:** Let $e \in G$ be the identity element of G.

$$a * e = e * a = a, \forall a \in G.$$

Now,

$$a * e = a$$
$$\Rightarrow a + e + 1 = a$$
$$\Rightarrow e = -1 \in G$$

Therefore $-1$ is the identity element. Also

$$e * a = a$$
$$\Rightarrow e + a + 1 = a$$
$$\Rightarrow e = -1 \in G$$

# ORDER OF GROUP AND ORDER OF ELEMENT

**Order of a group:** The order of the group is defined as the number of element in the group. It is denoted by $o(G)$.

**Order of an element:** Let G be a group with binary operation $*$ . By the order of an element $a \in G$ is meant the least positive integer n, if one exists , such that $a^n = e$ (the identity of G) . It is denoted by $o(a)$.

**Remarks: (i)** If there does not exist any positive integer $n$ such that $a^n = e$, then we say that $a$ is of infinite order.

**(ii) The order of the identity element is always 1.**

**Example : Find the order of each element of the multiplicative group { 1,-1,i,-i}.**

**Solution:** Since 1 is the identity element therefore $o(1) = 1$.

| | |
|---|---|
| -1 | $(-1)^1=-1$ |
| | $(-1)^2= 1$ (i.e., identity element)<br>$\therefore o(-1) = 2$ |
| i | $(i)^1=i$ |
| | $(i)^2= -1$ (i.e., identity element) |
| | $(i)^3=-i$ |
| | $(i)^4= 1$ (i.e., identity element)<br>$\therefore o(i) = 4$ |
| -i | $(-i)^1=-i$ |
| | $(-i)^2= -1$ (i.e., identity element) |
| | $(-i)^3=i$ |
| | $(i)^4= 1$ (i.e., identity element)<br>$\therefore o(-i) = 4$ |

**Example : Find the order of each element of the group { 0,1,2,3,4,5} ,the composition being addition modulo 6.**

**Solution:** Since 0 is the identity element therefore $o(0) = 1$.

| | |
|---|---|
| 1 | $(1)^1=1$ |
| | $(1)^2= 1+_6 1=2$ |
| | $(1)^3= 1+_6 1+_6 1=3$ |
| | $(1)^4= 1+_6 1+_6 1+_6 1=4$ |
| | $(1)^5= 1+_6 1+_6 1+_6 1+_6 1=5$ |
| | $(1)^6= 1+_6 1+_6 1+_6 1+_6 1+_6 1=0$(i.e., identity element) $\therefore o(1) = 6$ |
| 2 | $(2)^1=2$ |
| | $(2)^2=2+_6 2= 4$ |
| | $(2)^3=2+_6 2+_6 2$ =2 0(i.e., identity element) $\therefore o(2) = 3$ |

| | |
|---|---|
| 3 | $(3)^1=3$ |
| | $(3)^2= 3+_6 3=0$ (i.e., identity element)<br>$\therefore o(3) = 2$ |
| 4 | $(4)^1=4$ |
| | $(4)^2=4+_6 4= 8$ |
| | $(4)^3=4+_6 4+_6 4= 0$(i.e., identity element)<br>$\therefore o(4) = 3$ |
| 5 | $(5)^1=1$ |
| | $(5)^2= 5+_6 5=4$ |
| | $(5)^3= 5+_6 5+_6 5=3$ |
| | $(5)^4= 5+_6 5+_6 5+_6 5=2$ |
| | $(5)^2= 5+_6 5+_6 5+_6 5+_6 5=1$ |
| | $(5)^2= 5+_6 5+_6 5+_6 5+_6 5+_6 5=0$(i.e., identitiy element)<br>$\therefore o(5) = 6$ |

**Example**: Is multiplicative modulo 6 a group $(U_6 = \{0,1,2,3,4,5\}, *_6)$? If not, how to make it a group? Find the order of the all elements.

Solution:

| $*_6$ | [0] | [1] | [2] | [3] | [4] | [5] |
|---|---|---|---|---|---|---|
| [0] | 0 | 0 | 0 | 0 | 0 | 0 |
| [1] | 0 | 1 | 2 | 3 | 4 | 5 |
| [2] | 0 | 2 | 4 | 0 | 2 | 4 |
| [3] | 0 | 3 | 0 | 3 | 0 | 3 |
| [4] | 0 | 4 | 2 | 0 | 4 | 2 |
| [5] | 0 | 5 | 4 | 3 | 2 | 1 |

**Closure property**: Since all the elements of the table lie in the set $U_6 = \{0,1,2,3,4,5\}$, we can say that closure property is satisfied.

**Associativity property**: For all the elements in the table, it can be verified that $[a] *_6 ([b] *_6 [c]) = ([a] *_6 [b]) *_6 [c]$, for all $[a], [b], [c] \in U_6$ (H.W.)

**Existence of Identity**: From the table, it can be observed that 1 will the identity element as $[a] *_6 [1] = [a], for\ all\ [a] \in U_6$.

**Existence of inverse**: For $[0], [2], [3], [4]$ we don't get any of the element from $U_6$ so that $[a] *_6 [a^{-1}] = e = [1]$, for $[a] = [0], [2], [3], [4]$ is satisfied. Hence, inverse element do not exist for $[0], [2], [3], [4]$.

*Therefore, this property is not satisfied and hence we can say that this $U_6$ is not a group.*

Observe that if we remove $[0], [2], [3], [4]$ from $U_6$ then $S = \{[1], [5]\}$ will turns out the group(H.W.) and in this case, the order of the group $o(S) = 2$ and $o(1) = 1$ and $o(5) = 2$

**Examples: 1. In the infinite multiplicative group of non zero rational numbers. Find the order of each element.**

**2. Example : Find the order of each element in the additive group of integers.**

**Solution 1:** Since " 1" is the identity element therefore $o(1)=1$.

$(-1)^1=-1$; $(-1)^2=1$(identity element) therefore $o(-1)=2$

Now $(2)^1=2$; $(2)^2=4$; $(2)^3=8$; $(2)^4=16$ and so on.

Thus there exists no positive integer n such that $2^n=1$(identity element). Therefore $o(2)=$ infinite. Similarly order of the remaining element is infinite.

**Solution 2:** Since " 0" is the identity element therefore $o(0)=1$.

Now $(1)^1=1$; $(1)^2=1+1=2$; $(1)^3=1+1+1=3$; $(1)^4=1+1+1+1=4$ and so on.

Thus there exists no positive integer n such that $1^n=0$(identity element). Therefore $o(1)=$ infinite.

Similarly order of the remaining element is infinite.

## Remarks:

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

(2) The order of an element of a group is same as that of its inverse $a^{-1}$.

(3) In an infinite group element may be of finite as well as of infinite order.

# <u>SUBGROUP</u>

**SUBGROUP:** A non empty subset H of a group $G$ is called a subgroup of $G$ if H itself is a group under the same binary operation as of G.

Remark: For any group G, H={e} and H=G are always a subgroup of G. (Improper subgroups)

**Examples : $(\mathbb{Z}, +)$ of** $(\mathbb{Q}, +)$, **$(\mathbb{Q}, +)$ of** $(\mathbb{R}, +)$, **$(\mathbb{R}, +)$ of** $(\mathbb{C}, +)$, **$(\mathbb{Q}_+, +)$ of** $(\mathbb{R}_+, +)$,

(1) The multiplicative group { 1,-1} is a subgroup of the multiplicative group { 1,-1,i,-i}.

**(2)** The additive group of even integers is a subgroup of the additive group of all integers. (i.e. **$(2\mathbb{Z}, +)$ of $(\mathbb{Z}, +)$** )

(3) The multiplicative group of positive rational numbers is a subgroup of the multiplicative of all non zero rational numbers.

## Remarks:

(1) Every set is a subset of itself. Therefore if G is a group, then G itself is a group of G. Also if e is the identity of G, then the subset of G containing only one element i.e., e is also a subgroup of g. These two are subgroup of any group. They are called trivial or improper subgroup. A subgroup other than these two is called proper subgroup.

(2) The identity of a subgroup is same as that of the group.

(3) The inverse of any element of a subgroup is same as the inverse of the same regarded as an element of the group.

(4) The order of any element of subgroup is the same as the order of the element regarded as a member of the group.

.

**CRITERION FOR A NON EMPTY SET TO BE A SUBGROUP**

**Theorem 1:** A non empty subset H of a group G is a subgroup of G if and only if

(1) $a \in H, b \in H \Rightarrow ab \in H$

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

**Theorem 2:** A necessary and sufficient condition for a non empty subset H of a group to be a subgroup is that $a \in H, b \in H \Rightarrow ab^{-1} \in H$, where $b^{-1}$ is the inverse of b in G.

**INTERSECTION OF SUBGROUP**

**Theorem**: If $H_1$ and $H_2$ are two subgroup of a group G , then $H_1 \cap H_2$ is also a subgroup of G.

**Proof:** Since $H_1$ and $H_2$ are two subgroup of a group G, then $H_1 \cap H_2 \neq \emptyset$, since at lest the identity e is common to both $H_1$ and $H_2$.

In order to prove that $H_1 \cap H_2$ is a subgroup of G it is sufficient to prove that

$$a \in H_1 \cap H_2;\ \mathrm{b} \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$$

$$\text{Now, } a \in H_1 \cap H_2 \Rightarrow a \in H_1 \text{ and } a \in H_2$$

$$b \in H_1 \cap H_2 \Rightarrow b \in H_1 \text{ and b} \in H_2$$

But $H_1$ and $H_2$ subgroups. Therefore

$$a \in H_1; b \in H_1 \Rightarrow ab^{-1} \in H_1$$
$$a \in H_2; b \in H_2 \Rightarrow ab^{-1} \in H_2$$

Finally,

$$ab^{-1} \in H_1; ab^{-1} \in H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$$

Thus,

$$a \in H_1 \cap H_2; b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$$

Hence, $H_1 \cap H_2$ is a subgroup of G.

**Remark:** The union of two subgroup is not necessarily a subgroup.

**For example**, Let G be the additive group of integers.

Then $H_1$={……………….-6,-4,-2,0,2,4,6,…………},

$H_2$={……………….-12,-9,-6,-3,0,3,6,9,12…….} are two subgroups of G.

Also $H_1 \cup H_2$ ={………-12,-10,-9,-6,-4,-3,-2,,0,2,3,4,6,9,10,12……..}

Obviously $H_1 \cup H_2$ is not closed with respect to addition as

$2 \in H_1 \cup H_2; 3 \in H_1 \cup H_2 \Rightarrow 2+3 \notin H_1 \cup H_2$.

Therefore $H_1 \cup H_2$ is not a subgroup with respect to addition.

**Example: Let G be the additive group of integers. Then prove that the set of all multiples of integers by a fixed integer m is a subgroup of G.**

**Solution**: $G = \{\dots\dots\dots\dots\dots -3, -2, -1, 0, 1, 2, 3, \dots\dots\dots..\}$ is the additive group of integer.

Let $m$ be any fixed integer.

Let $H = \{\dots\dots\dots\dots\dots -3m, -2m, -1m, 0, 1m, 2m, 3m, \dots\dots\dots..\}$

Then $H \subseteq G$.

To prove that H is subgroup, we prove $a \in H; b \in H \Rightarrow ab^{-1} = a - b \in H$

Let $a = km$ and $b = nm$, for some $k, n \in \mathbb{Z}$ be any two element of H.

Then inverse of n$m$ in G is $(-n)m$ i.e., $-b = -nm$.

Now,

$$ab^{-1} = a - b = km + (-n)m = (k - n)m \in H,$$

since k $- n$ is also an integer.

Thus $a \in H; b \in H \Rightarrow ab^{-1} = a - b \in H$.

Therefore H is subgroup of G.

**Example: Let G be a set of all ordered pairs (a,b) of real numbers for which $\boldsymbol{a \neq 0}$. Let a binary operation × defined by $(\boldsymbol{a, b}) \times (\boldsymbol{c, d}) = (\boldsymbol{ac, bc + d})$. Show that (G, × ) is non abelian group. Does the subset H of all those elements of G which are of the form (1,b) form a subgroup of G?**

**Solution: Closure Property:** Let $(a, b)$ and $(c, d)$ be any two element of S. Then $a \neq 0$ and $c \neq 0$.

Now $(\boldsymbol{a}, \boldsymbol{b}) * (\boldsymbol{c}, \boldsymbol{d}) = (\boldsymbol{ac}, \boldsymbol{bc} + \boldsymbol{d}) \in \boldsymbol{S}$ (because $a \neq 0$ and $c \neq 0 \Rightarrow ac \neq 0$)

Hence S is closed with respect to the given composition( binary operation)

**Associativity:** Let $(a, b), (c, d), (e, f)$ be any three element of S.

L.H.S. $[(a, b) * (c, d)] * (e, f)$

$=(ac, bc + d) * (e, f) = (ace, (bc + d)e + f) = (ace, bce + de + f)$

R.H.S. $(a, b) * [(c, d) * (e, f)]$

$=(a, b) * (ce, de + f)$

$=(ace, b(ce) + de + f) = (ace, bce + de + f)$

Hence the given composition $*$ is associative.

**Existence of Identity:** Let $(x, y)$ be identity element of S such that

$$(x, y) * (a, b) = (a, b) = (a, b) * (x, y) \Rightarrow (xa, ya + b) = (a, b)$$
$$\Rightarrow xa = a; ya + b = b$$

We get $x = 1$ and $y = 0$.

Therefore (1,0) is the identity element.

**Existence of inverse:** Let $(c, d) \in S, c \neq 0$ be inverse of $(a, b) \in S$.
Now

$$(a, b) * (c, d) = (1,0) = (c, d) * (a, b)$$
$$\Rightarrow (ac, bc + d) = (1,0)$$
$$\Rightarrow ac = 1, bc + d = 0$$
$$\Rightarrow c = \frac{1}{a} \neq 0; d = -\frac{b}{a}$$

Hence $\left(\frac{1}{a}, -\frac{b}{a}\right)$ is an inverse of element (a,b).

**Hence the set S of all ordered pairs (a,b) of real numbers for which $\boldsymbol{a \neq 0}$ with respect to the operation $*$ defined by $(\boldsymbol{a}, \boldsymbol{b}) * (\boldsymbol{c}, \boldsymbol{d}) = (\boldsymbol{ac}, \boldsymbol{bc} + \boldsymbol{d})$ is a group.**

**To Prove H is a subgroup of G or not.**

**Observe that $\boldsymbol{H} = \{(\mathbf{1}, \boldsymbol{b})/\boldsymbol{b} \in \mathbb{R}\}$**

Obviously H is a non empty subset of G ((1,1)$\in H$).

Let (1,b) and (1,c) be any two elements of H then $b, c \in \mathbb{R}$. Then

$(1, b) \times (1, c)^{-1} = (1, b) \times (\frac{1}{1}, -\frac{c}{1}) = (1, b) \times (1, -c) = (1, b - c)$ (By definition of operation of G)

$(1, b - c)$ is definitely an element of H as $b - c \in \mathbb{R}$ . Thus

$$(1, b), (1, c) \in H \Rightarrow (1, b) \times (1, c)^{-1} \in H$$

Hence, H is subgroup of G.

**Example: Let H be the multiplicative group of all positive real numbers and R the additive group of all real numbers. Is H a subgroup of R?**

**Solution:** The set H of all positive real numbers is a subset of the set of R of all real numbers. But the group G is not a subgroup of the group R. The reason is that the composition/ binary operation in G is different from the composition/ binary operation in R.

**<u>LAGRANGE'S THEOREM:</u>**

**If H is a subgroup of finite group G, then**

$$\boldsymbol{o(H)/o(G).}$$

**In other words, "The order of each subgroup of a finite group is a divisor of the order of the group."**

**Note:** Lagrange's theorem has very important applications. Suppose G is a finite group of order n. If m is not a divisor of n , then there can be no subgroup of order m. Thus if G is a group of order 6, then there can be no group of order 5 or 4. Similarly if G is a group of prime order p then G can have no proper subgroup.

# CYCLIC GROUP

**CYCLIC GROUP:** A group $G$ is called cyclic group if for some $a \in G$, every element of $G$ is of the form $a^n$, for some integer n. The element $\boldsymbol{a}$ is then called a generator of $G$ and we write $G = < a >$

**Example:** The multiplicative group ={1,-1,i,-i} is cyclic .

We can write G={ $i, i^2, i^3, i^4$}.

Thus G is a cyclic group and i is a generator.

Also we can write G={ $-i, (-i^2), (-i^3), (-i^4)$}.

Thus –i is also the generator of G.

**Example:** The multiplicative group $\{1, w, w^2\}$ is cyclic. The generators are $w, w^2$.

**Example:** The group A=({0,1,2,3,4,5},$+_6$} is cyclic. This group is generated by 1 and another generator is 5.

## Remarks:

- Every cyclic group is an abelian.
- If a is a generator of a cyclic group G, then $a^{-1}$ is also generator of G.
- If "a" is a generator of an infinite cyclic group G, then the order of a must be infinite. If the order of a is finite ,then cyclic group generated by "a" is of finite order. Therefore the order of the cyclic group is equal to order of its generating element.
- If G is a cyclic group of order n then total number of generators of G will be equal to number of integer less than n and prime to n. i. e. $\varphi(n)$

  For example, if a is generator of a cyclic group G of order 8, then $a^3, a^5, a^7$ will be the only generators of G. Since 4 is not prime to 8 therefore $a^4$ cannot be generator of G. Similarly $a^2, a^6, a^8$ cannot be generators of G.
- If a finite group of order n contains an element of order n, then group must be cyclic.

**Example: Show that the group $(\{1,2,3,4,5,6\},x_7)$ is cyclic. How many generators are there?**

**Solution:** Let G={1,2,3,4,5,6}. If there exists an element $a \in G$ such that o(a)=6 i.e., the order of the group G then the group G will be cyclic group and a will be generator of G.

| | |
|---|---|
| 3 | $(3)^1=3$ |
| | $(3)^2= 3X_73=2$ |
| | $(3)^3= 3X_73X_73=3$ |
| | $(3)^4= 3X_73x_73x_73=4$ |
| | $(3)^5= 3X_73X_73X_73x_73=5$ |
| | $(3)^6= 3X_73x_73X_73X_73X_73=1$(i.e., identity element) $\therefore o(3) = 6$ |

Since o(3)=6= order of the group therefore G is a cyclic group and 3 is a generator of G.

Now If a is a generator of a cyclic group G, then $a^{-1}$ is also generator of G.

Therefore 5 is also generator of the group.

# PERMUTATION GROUP

**Definition:** Suppose S is a finite set having n distinct elements. Then a one-one mapping of S onto itself is called a permutation of degree n.

The number of elements in the finite set S is known as the degree of permutation.

**Total number of distinct permutations of degree n is n!**

**Equality of two permutation:** Two permutation f and g of degree n said to be equal if we have $f(a) = g(a), \forall a \in S$.

**Product or Composition of two Permutations:** The product or composition of two permutations f and g of degree n is denoted by $fog$, is obtained by first carrying out the operation defined by g and then by f. Similarly, $gof$.

**Example**: Let f=$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ , g=$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ be two permutations of degree 3. Then

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

and

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

Obviously $fog \neq gof$.