Index

Unit – 5.1 ⇝ Graph Theory – II

Method 1 ⇝ Euler Paths and Circuits

Euler Circuits

→ A circuit in a connected graph is an **Euler Circuit** if it contains every edge of the graph exactly once.

i.e., an Euler circuit in a connected graph G is a simple circuit containing every edge of G.

Euler Paths

→ A path in a connected graph is an **Euler Path** if it contains every edge of the graph exactly once.

i.e., an Euler path in a connected graph G is a simple path containing every edge of G.

Euler Graph

→ A connected graph which contains Euler circuit is called **Euler** or **Eulerian Graph**.

Some Results on Euler Paths and Circuits for Undirected Graph

(1) A connected undirected multigraph with at least two vertices has an Euler circuit if and only if each of its vertices has even degree.

(2) A connected undirected multigraph has an Euler path but not an Euler circuit if and only if it has two vertices of odd degree.

Steps to check whether the connected undirected graph has Euler Path or Circuit

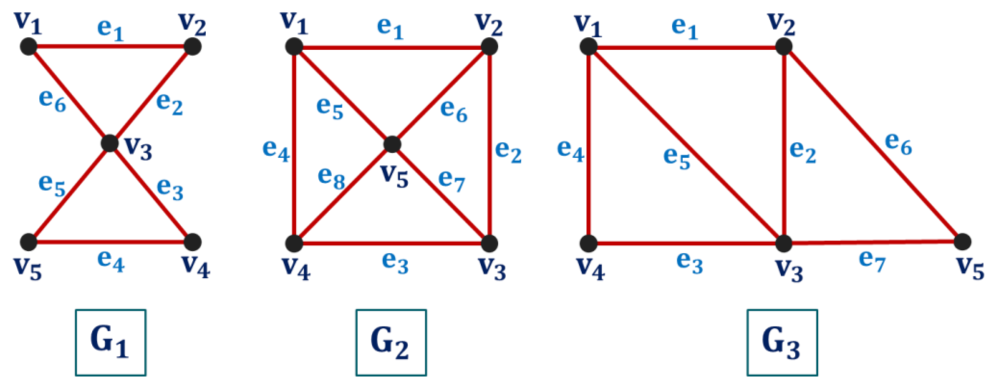
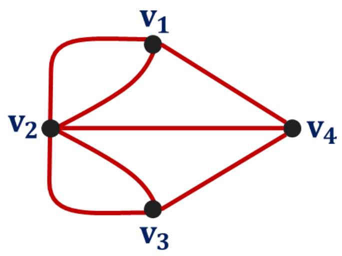
(1) List the degree of all vertices in the graph.

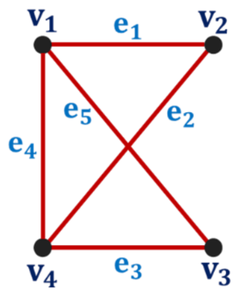
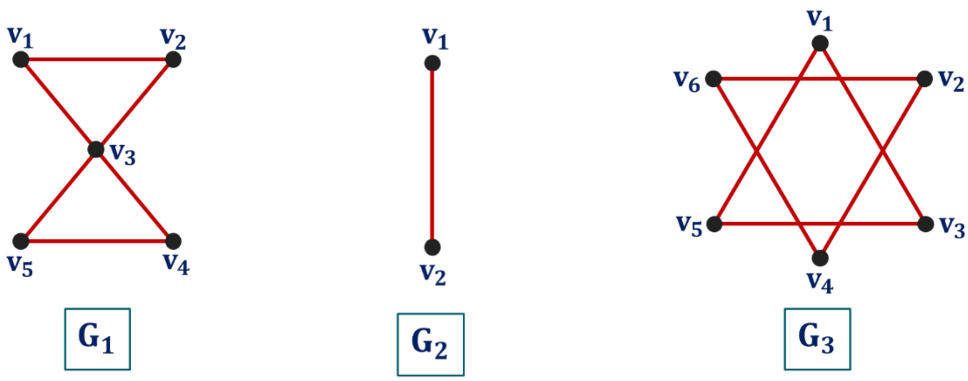
(2) If degree of any vertex is zero, then the graph is disconnected and hence it cannot have Euler path or circuit.

(3) If all the degrees are even, then the graph has both Euler path and Euler circuit.

(4) If exactly two vertices are of odd degree, then the graph has Euler path but no Euler circuit.

Examples of Method-1: Euler Paths and Circuits

C	1	Which of the following graphs have an Euler circuit? Of those that do not, which have an Euler path?  **Answer:** **G_1 has an Euler circuit $v_1e_1v_2e_2v_3e_3v_4e_4v_5e_5v_3e_6v_1$** **Neither G_2 nor G_3 has an Euler Circuit** **G_3 has an Euler path $v_1e_4v_4e_3v_3e_7v_5e_6v_2e_2v_3e_5v_1e_1v_2$** **$G_2$ does not have an Euler path.**
C	2	Check whether the following graph is Euler Graph or not.  **Answer:** **The given graph is not an Euler graph**

C	3	Check whether the following graph has Euler path or not.  **Answer**: **Euler path**: $v_4e_3v_3e_5v_1e_1v_2e_2v_4e_4v_1$
C	4	Check whether the following graphs has Euler path and circuit or not.  **Answer**: **G_1 has Euler path as well as Euler circuit** **G_2 has Euler path but it does not have an Euler circuit** **G_3 has neither Euler path nor Euler circuit**
C	5	For what values of n is the graph of K_n Eulerian? **Answer**: **K_n is Eulerian, when n is odd.**

Method 2 ⇝ Hamiltonian Paths and Circuits

Hamiltonian Circuit

→ A circuit which contains every vertex of the graph exactly once except end vertices is called **Hamiltonian circuit**.

Hamiltonian Path

→ A path in a graph is a **Hamiltonian Path** if it contains every vertex of the graph exactly once, where the end vertices may be distinct.

Hamiltonian Graph

→ A graph which contains Hamiltonian circuit is called **Hamiltonian Graph**.

Some Results on Hamiltonian Paths and Circuits

Result – 1 (Dirac's Theorem)

→ If G is a simple connected graph with n vertices $(n \geq 3)$ such that

$\deg(u) \geq \frac{n}{2}$, for every vertex $u \in G$, then G has a Hamiltonian circuit.

i.e., If G is a simple graph with n vertices with $n \geq 3$ such that the degree of every vertex in G is at least $\frac{n}{2}$, then G has a Hamiltonian circuit.

Result – 2

→ If G is a simple connected graph with n vertices $(n \geq 3)$ and m edges such that

$m \geq \left[\frac{(n-1)(n-2)}{2}\right] + 2$, then G has a Hamiltonian circuit.

Result – 3 (Ore's Theorem)

→ If G is a simple connected graph with n vertices with $n \geq 3$ such that $\deg(u) + \deg(v) \geq n$, for every pair of non – adjacent vertices u and v in G, then G has a Hamiltonian circuit.

Remark

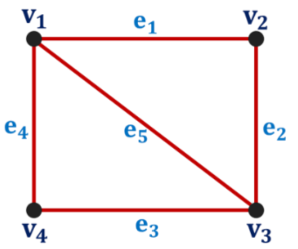
- The graph may be Hamiltonian even if, the conditions of above results does not hold.

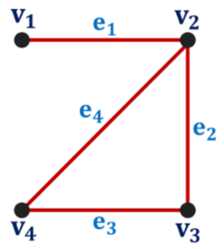
A Helpful Hints to Find a Hamiltonian Cycle

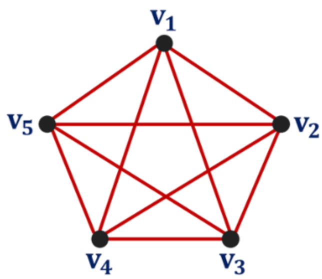
→ Let $G = (V, E)$ be a given graph.

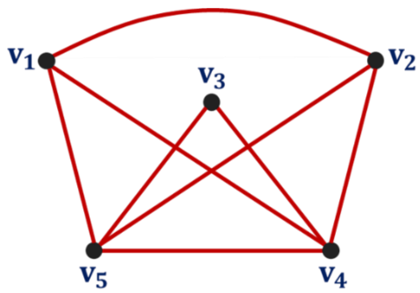
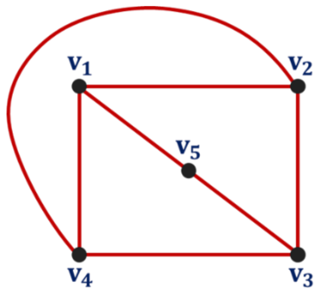
- If a graph has Hamiltonian cycle, then $\deg(u) \geq 2$, for all $u \in V$.
- If $u \in V$ and $\deg(u) = 2$, then the two edges incident with vertex u must appear in every Hamiltonian cycle for G.
- If $u \in V$ and $\deg(u) > 2$, then as we try to build a Hamiltonian cycle, once we pass through vertex u, any unused edges incident with u are deleted from further consideration.

Examples of Method-2: Hamiltonian Paths and Circuits

<table>
<tr>
<td>C</td>
<td>1</td>
<td>Which of the following graph has a Hamiltonian cycle? If yes, give a cycle. If not, does it contain a Hamiltonian path? If yes, give a path.


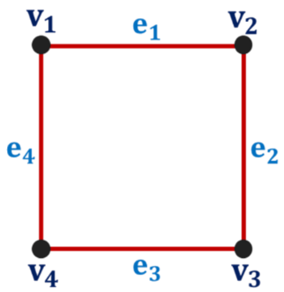
G_1


G_2
Answer: G_1 has a Hamiltonian cycle, $v_1e_1v_2e_2v_3e_3v_4e_4v_1$
G_2 has a Hamiltonian path, $v_1e_1v_2e_2v_3e_3v_4$</td>
</tr>
<tr>
<td>C</td>
<td>2</td>
<td>Using Dirac's Theorem show that the following graph is Hamiltonian graph.

</td>
</tr>
</table>

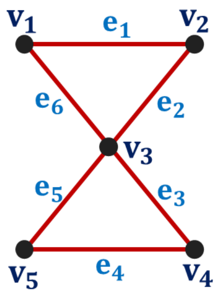
C	3	Show that the following graph is Hamiltonian graph. 
C	4	Show that the following graph is Hamiltonian graph. 

C	5	Give an example of a graph which contains **(1)** an Eulerian circuit that is also a Hamiltonian circuit **(2)** an Eulerian circuit but not Hamiltonian circuit **(3)** a Hamiltonian circuit but not an Eulerian circuit **(4)** a non – Eulerian and non – Hamiltonian circuit **(5)** an Eulerian circuit and a Hamiltonian circuit that are distinct.

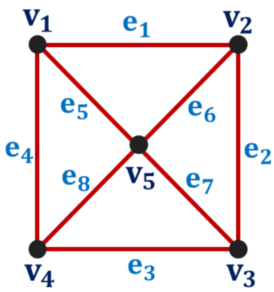
Answer:



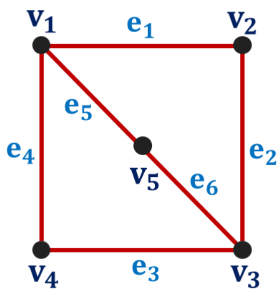
G_1



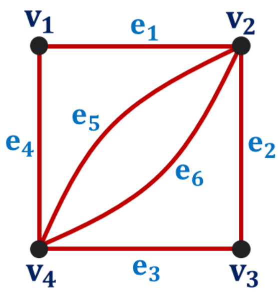
G_2



G_3



G_4



G_5

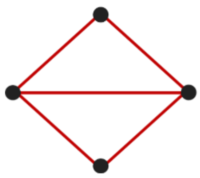
Method 3 ⇝ Introduction to Planar Graph

Planar Graph

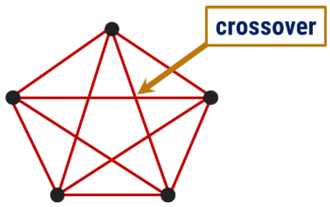
→ A graph G is said to be planar if G can be represented as a geometric picture on a plane such that there is no crossing over of edges of G.

→ A graph that cannot be drawn on a plane without a crossover between its edges is called non – planar graph.

→ Example:

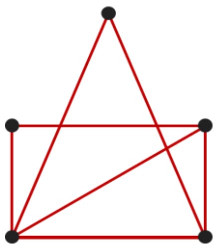


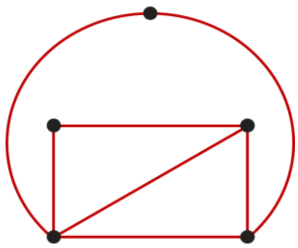
planar graph



non – planar graph

→ Note that if a graph G has been drawn with crossing edges, this does not mean that G is non – planar. There may be another way to draw the graph without crossovers.





Region of a Graph

→ A region of a planar graph is defined to be an area of the plane that is bounded by edges and is not further divided into sub – areas.

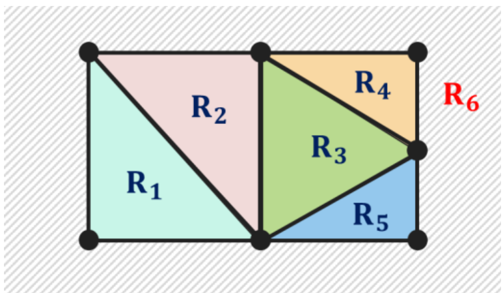
→ If the area of the region is finite, then the region is called finite region.

→ If the area of the region is infinite, then the region is called infinite, outer or unbounded region.

→ Example:

- Region $\mathbf{R_6}$ is an infinite region

  while all other are finite regions.



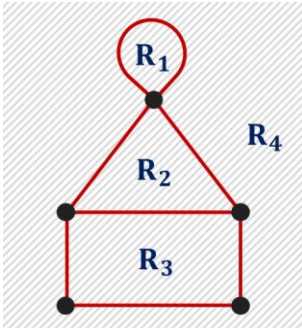
Euler's Formula

→ If a connected planar graph G has n vertices, e edges and r region, then

$$n + r = 2 + e.$$

→ Any connected planar graph with n vertices, e edges have $e - n + 2$ regions.

→ Example:



Here, no. of vertices $= n = 5$

no. of edges $= e = 7$

no. of regions $= r = 4$

L.H.S. $= n + r = 5 + 4 = 9 = 2 + e =$ R.H.S.

Results

(1) If G is a connected planar simple graph with e edges and n vertices, where $n \geq 3$, then $e \leq 3n - 6$.

i.e., If G is a connected simple graph with e edges and n vertices, where $n \geq 3$ and $e > 3n - 6$, then G is non – planar.

(2) If a connected planar simple graph has e edges and n vertices with $n \geq 3$ and no circuits of length three, then $e \leq 2n - 4$.

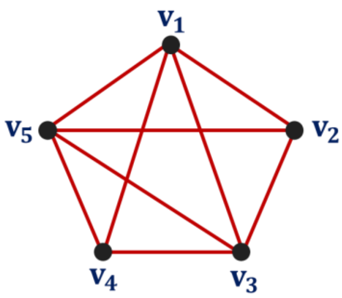
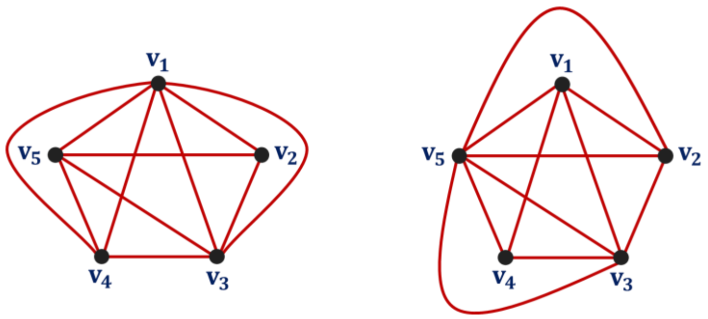
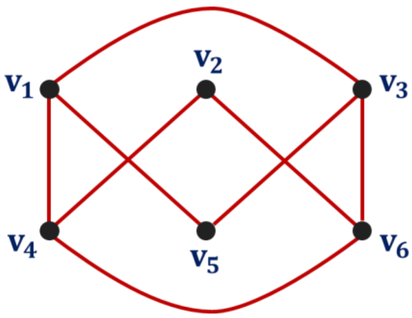
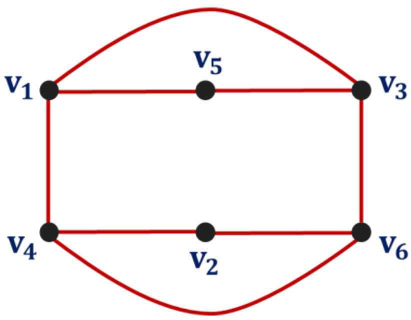
i.e., Let G be a connected simple graph with e edges and n vertices with $n \geq 3$ and no circuits of length three. If $e > 2n - 4$, then the graph G is non – planar.

Remark

→ For a connected simple graph G with e edges and n vertices, where $n \geq 3$, if $e \leq 3n - 6$ that does not mean the graph is planar.

→ For a connected simple graph G with e edges and n vertices, where $n \geq 3$, and no circuits of length three. If $e \leq 2n - 4$ that does not mean the graph is planar.

Examples of Method-3: Introduction to Planar Graph

C	1	Draw a planar graph representation of the following graph.  **Answer**: 
C	2	Draw a planar graph representation of the following graph.  **Answer**: 

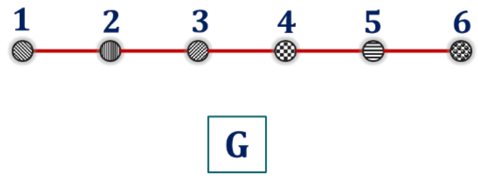
C	3	Suppose that a connected planar simple graph has 20 vertices, each of degree 3. Into how many regions does a representation of this planar graph split the plane? **Answer**: **12**
C	4	Is K_5 (Kuratowaski's First Graph) planar? **Answer**: **No**
C	5	Is $K_{3,\,3}$ (Kuratowaski's Second Graph) planar? **Answer**: **No**

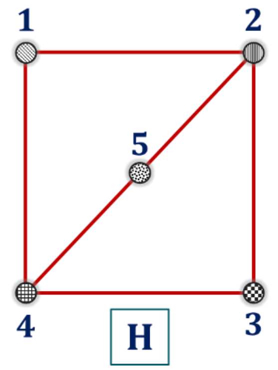
Method 4 ⇝ Introduction to Graph Coloring

Vertex Coloring

→ A **coloring** or vertex coloring of a simple graph is the assignment of a color to each vertex of the graph so that no two adjacent vertices are assigned the same color.

→ Example:





Chromatic Number

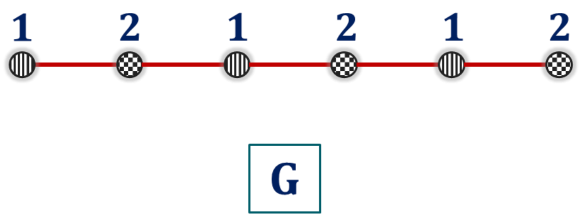
→ The least (minimum) number of colors needed for a coloring of the graph is called the chromatic number of a graph.

→ The chromatic number of a graph G is denoted by $\chi(G)$.

(Here χ is the Greek letter chi – read as **Kai**)

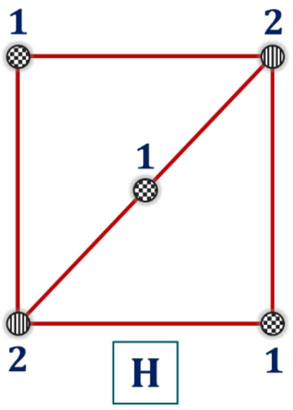
→ If $\chi(G) = k$, then G is known as k – chromatic.

→ Examples:



- Here, $\chi(G) = 2$

  $\therefore$ G is 2 $-$ chromatic.



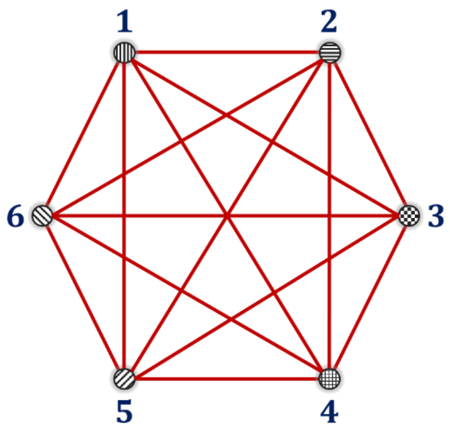
- Here, $\chi(H) = 2$

  $\therefore$ H is 2 $-$ chromatic.

Chromatic Number of a Complete Graph ($\mathbf{K_n}$)

$\rightarrow$ The chromatic number of a complete graph K_n with n vertices is **n**.

$\rightarrow$ Example:

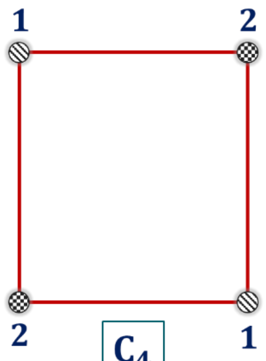


Chromatic Number of a Cycle Graph ($\mathbf{C_n}$)

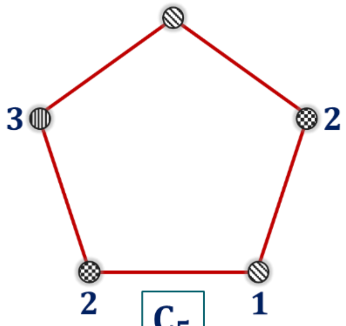
$\rightarrow$ The chromatic number of a cycle graph C_n with n vertices is

- 2 if **n** is even
- 3 if **n** is odd.

→ Example:



C_4



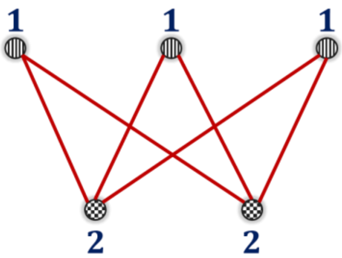
C_5

Chromatic Number of a Bipartite Graph ($K_{m,\ n}$)

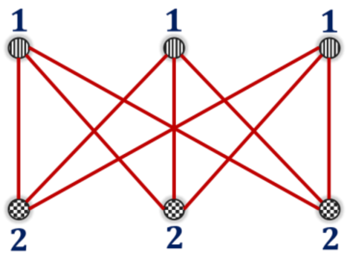
→ The chromatic number of a non – null graph is 2 if and only if the graph is bipartite.

→ The chromatic number of a complete bipartite graph is 2.

→ Example:



$K_{3,\ 2}$



$K_{3,\ 3}$

Remarks

→ A graph consisting of only isolated vertices is 1 – chromatic.

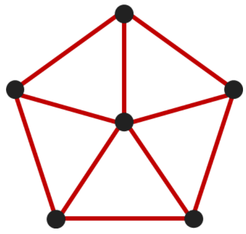
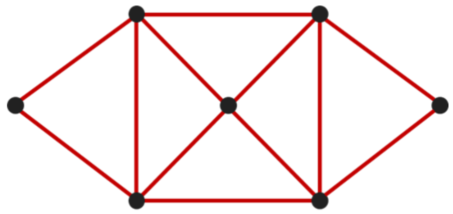
→ A chromatic number of a null graph is 1.

→ $\chi(G) \leq n$, where n is the number of vertices of graph G.

→ If $\deg(v) = d$ for a vertex v in graph G, then at most d colors are required for coloring of the vertices adjacent to v.

→ If H is a subgraph of G, then $\chi(H) \leq \chi(G)$.

Examples of Method-4: Introduction to Graph Coloring

C	1	Determine the chromatic number of following wheel graph W_6:  **Answer**: $\chi(W_6) = 4$
C	2	Find the chromatic number of the following graph:  G **Answer**: $\chi(G) = 4$
C	3	Show that K_5 is 5 – chromatic.

Unit 5.2 Group Theory

Method 1 ⇝ Binary Operation

Important Sets

The set of natural numbers	$\mathbb{N} = \{ 1,\ 2,\ 3, \dots \}$
The set of integers	$\mathbb{Z} = \{ \dots, -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3, \dots \}$
The set of rational numbers	$\mathbb{Q} = \left\{ \frac{p}{q} :\ p, q \in \mathbb{Z}\ \&\ q \neq 0 \right\}.$
The set of irrational numbers	$\mathbb{Q}^c = \{ \pi,\ e,\ \sqrt{2}, \dots \}$
The set of real numbers	$\mathbb{R} = \mathbb{Q} \cup \mathbb{Q}^c$
The set of positive real numbers	$\mathbb{R}^+$
The set of complex numbers	$\mathbb{C} = \{ z = x + iy : x, y \in \mathbb{R} \}.$
The set of all residue classes when elements of $\mathbb{Z}$ is divided by n	$\mathbb{Z}_n = \{ 0,\ 1,\ 2,\ 3, \dots,\ n-1 \}$ $\mathbb{Z}_n^* = \{ 1,\ 2,\ 3, \dots,\ n-1 \}$

Binary Operation

A function $*$: $\mathbf{A} \times \mathbf{A} \to \mathbf{A}$ is known as binary operation on A. i.e. if $(\mathbf{a},\mathbf{b}) \in \mathbf{A}\times\mathbf{A} \Rightarrow \mathbf{a}*\mathbf{b}\in\mathbf{A}$, $\forall \mathbf{a}, \mathbf{b}\in\mathbf{A}$ then $*$ is known as binary operation on A.

Properties of Binary Operation

(3) Algebraic Structures

A non-empty set Gequipped with one or more binary operations is known as algebraic structure.

The algebraic structure consisting of a set G and binary operations $*$, $\circ$ on G is denoted by $(G, *, \circ)$

Example

(1) $(\mathbb{N}, +)$

(2) $(\mathbb{Z}, +)$

(3) $(\mathbb{N}, -)$ Is not algebraic structure. Since, $-$ is not binary operation on $\mathbb{N}$.

(4) Closure Property

- A binary operation $*$ is define on a set G is known as closure, if $\mathbf{a*b\in G}$ forall $\mathbf{a,b \in G}$. If closure property is satisfied, then we say that G is **closed** under binary operation $*$.

- For Example:

Let, Addition and multiplication are closed in $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ and Subtraction is not closed in $\mathbb{N}$ also Division is not closed in $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$.

(5) Associative Property

→ Abinary operation $*$ is define on a set G is known as associative, if $(\mathbf{a} * \mathbf{b})*\mathbf{c}=\mathbf{a}*(\mathbf{b}*\mathbf{c})$ for all $\mathbf{a,b,c} \in \mathbf{G}$.For Example:

→ " $+$ " is associative in $\mathbb{N}$.

Reason: $\forall$ a, b, c $\in G \Rightarrow a + (b + c) = (a + b) + c$

→ ×(multiplication) is associative over $\mathbb{N}$.

Reason: a, b, c $(a \times b) \times c = a \times (b \times c)$.

(6) Commutative Property

- Let G be a non-empty set.

  Commutative property: $\mathbf{a * b = b * a}, \quad \forall\, a,\ b \in G$

- If commutative property is satisfied, then we say that binary operation $*$ is **commutative** in G.

- For Example:

Any two elements in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative under the binary operations addition and multiplication.

Additive Modulo n

→ For any $a, b \in \mathbb{Z}$, additive modulo n is defined as

$a +_n b = \mathbf{r}$, where $\mathbf{r}$ is remainder when $\mathbf{a + b}$ is divided by $\mathbf{n}$.

→ It is denoted by $+_n$ and read as "Additive modulo n".

→ For Example:

For additive modulo 5,

Let $2,\ 6 \in \mathbb{Z}, \quad 2 +_5 6 = 3$

Multiplicative Modulo n

→ For any $a, b \in \mathbb{Z}$, multiplication modulo n is defined as

$a \times_n b$ = remainder when $\mathbf{a \times b}$ is divided by **n**.

→ It is denoted by $\times_n$ and read as "multiplication modulo n".

→ For Example:

For multiplicative modulo 5,

Let $2,\ 6 \in \mathbb{Z},\quad 2\ \times_5 6 = 2$

Identity Element

→ Let G be a non-empty set and $*$ be binary operation on G.

If an element, $e \in G$ such that $a * e = a = e * a,\ \ \forall\, a \in G$, then **e** is known as Identity element of G.

→ For Example:

(1) For binary operation **addition**, identity element is $\mathbf{e = 0}$

Reason: $a + 0 = a = 0 + a$

(2) For binary operation **multiplication**, identity element is $\mathbf{e = 1}$

Reason: $a \times 1 = a = 1 \times a$

Inverse Element

→ Let G be a non-empty set and $*$ be binary operation on G.

If an element, $b \in G$ such that $a * b = e = b * a,\ \ \forall\, a \in G$, then **b** is inverse element of **a** in G, where **e** is identity element of G.

→ If element **b** is inverse element of **a**, then it is denoted by $\mathbf{b = a^{-1}}$.

→ For Example:

(6) For binary operation **addition**, $a^{-1} = -a$,

Reason: $a + (-a) = 0 = (-a) + a$

(7) For binary operation **multiplication**, $a^{-1} = \frac{1}{a}\ ; a \neq 0$

Reason: $a \times \frac{1}{a} = 1 = \frac{1}{a} \times a\ ; a \neq 0$

Table for Binary Operation or Composition Table

→ Let $*$ be the binary operation on set $G = \{\, a_1,\ a_2,\ \dots, a_n \,\}$.

→ Follow below steps to make table for binary operation "$*$":

(1) Give heading to rows and columns of table as $a_1, a_2, \ldots, a_n$ respectively.

(2) Entry of a_i^{th} raw and a_j^{th} column is $a_i * a_j$.

$*$	a_1	a_2	$\cdots$	a_j	$\cdots$	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$\cdots$	$a_1 * a_j$	$\cdots$	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$\cdots$	$a_2 * a_j$	$\cdots$	$a_2 * a_n$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
a_i	$a_i * a_1$	$a_i * a_2$	$\cdots$	$\vdots$	$\cdots$	$a_i * a_n$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
a_n	$a_n * a_1$	$a_n * a_2$	$\cdots$	$a_n * a_j$	$\cdots$	$a_n * a_n$

→ For Example:

Let $S = \{1, \omega, \omega^2\}$, where $\omega^3 = 1$ with binary operation $\times$.

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Example of Method-1: Binary Operation

C	1	On the set $\mathbb{Z}^+$, check whether $*$ is binary operation or not. $(\mathbf{1})$ $m * n = m + n - mn$ $(\mathbf{2})$ $m * n = m^n$ **Answer: (1) No, (2) Yes**
C	2	Let $*$ be a binary operation on $\mathbb{R}$ defined by $a * b = a - b$, Examine the identity element if exist. **Answer:$*$ has no identity element.**
C	3	On the set $\mathbb{N}$, check whether the binary operation $*$ is associative or not. $(\mathbf{1})$ $a * b = \dfrac{ab}{3}$ $(\mathbf{2})$ $a * b = a^b$ **Answer: (1) Yes, (2) No**
C	4	Let $*$ be a binary operation on $\mathbb{R}$ defined by $a * b = a+b+2ab$ then find an identity element in $\mathbb{R}$ with respect to $*$. **Answer: no identity element**
C	5	Let $*$ be a binary operation on $\mathbb{R}$ defined by $a * b = a+b+2ab$ then which elements has inverse and what are they **Answer: each element has inverse in $\mathbb{R}$ except $-\frac{1}{2}$.**
C	6	On the set $\mathbb{Q}$, check whether the binary operation $*$ is commutative or not. (1) $m * n = mn + 1$ (2) $m * n = \frac{m}{n}$ **Answer : (1)$*$ is commutative on the set $\mathbb{Q}$.** **Answer : (2)$*$ is not commutative on the set $\mathbb{Q}$.**

C | 7

Let $S = \{a, b, c, d\}$ and $*$ be a commutative binary operation on S. Find the missing entries in the following table.

$*$	a	b	c	d
a	b	b	a	d
b	?	c	c	c
c	?	?	d	b
d	?	?	?	a

Answer:

$*$	**a**	**b**	**c**	**d**
a	**b**	**b**	**a**	**d**
b	**b**	**c**	**c**	**c**
c	**a**	**c**	**d**	**b**
d	**d**	**c**	**b**	**a**

Method 2 ⇝ Group

Group

→ Let G be a non - empty set and $*$ be binary operation on G.

An algebraic structure $(G, *)$ is known as **group** if binary operation $*$ satisfies following conditions:

(1) Closure property

$a * b \in G, \quad \forall\, a,\ b \in G$

(2) Associative property

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

(2) Existence of identity element

There exists an element $e \in G$ such that $a * e = a = e * a, \quad \forall\, a \in G$

(3) Existence of inverse element

There exists an element $b \in G$ such that $a * b = e = b * a, \quad \forall\, a \in G$

→ For Example:

$(\mathbb{R}, +)$ is group.

Reason:

(1) Closure property

$\forall\, a,\ b \in \mathbb{R} \Rightarrow a + b \in \mathbb{R}$

⇒ Closure property satisfied.

(2) Associative property

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

⇒ Associative property satisfied.

(3) Existence of identity element

There exists $0 \in \mathbb{R}$ such that $a + 0 = a = 0 + a, \quad \forall\, a \in \mathbb{R}$

So, $e = 0$ is an identity element in $\mathbb{R}$.

(4) Existence of inverse element

Let $a \in \mathbb{R}$ then there exists $-a \in \mathbb{R}$ such that $a + (-a) = 0 = (-a) + a, \quad \forall\, a \in \mathbb{R}$

So, $a^{-1} = -a, \quad \forall\, a \in \mathbb{R}$

So, $(\mathbb{R}, +)$ is group.

Semigroup

→ Let G be a non-empty set together with a binary operation '$*$' on G, Then G, $*$ is known as a semigroup if the following conditions are satisfied.

1. Closure Property

2. Associative Property

One thing is clear that all group are semigroup.

→ For Example:

(1) $(\mathbb{N},+)$

(2) $(\mathbb{Z}^{+}, +)$

Monoid

→ Let G beanon-empty set together with a binary operation '$*$' on G, Then G, $*$ is known as a monoid if the following conditions are satisfied.

1. Closure Property

2. Associative Property

3. Existence of identity

One thing is clear that all group are monoid.

→ For Example:

(3)$(\mathbb{N},*)$

Example of Method-2: Group

C	1	Show that the set of cube root of unity forms a group under multiplication.
C	2	Show that $G = \left\{A\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} / \alpha \in \mathbb{R}\right\}$ is a group under matrix multiplication.
C	3	Check $(\mathbb{Z}_5^*, \times_5)$ is group or not? **Answer: Yes it is group.**
C	4	Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40. Find the identity element of this group? **Answer: 25**
C	5	Let $*$ be a binary operation on $\mathbb{R}$ defined by $a * b = a + b + 2ab$ is $\mathbb{R}, *$ semigroup? **Answer: $(\mathbb{R}, *)$ is a semigroup.**

Method 3 ⇝ Subgroup

Subgroup

→ Let $(G, *)$ be a group.

A non-empty subset H of a group G is known as subgroup of G if $(H, *)$ forms a **group**. it is denoted as $H \leq G$

→ For Example:

Let $G = (\mathbb{Q}, +)$ be a group and $\mathbb{Z}$ is a non-empty subset of $\mathbb{Q}$ then $H = (\mathbb{Z}, +)$ forms a group.

So, $(\mathbb{Z}, +)$ is subgroup of $(\mathbb{Q}, +)$.

→ For any group G, we have always two subgroups

(1)$(G,*)$

(2)$(\{ e \}, *)$, where "e" is the identity element of G.

Example of Method-3: Subgroup

C	1	Find all subgroups of $(\mathbb{Z}_{12}, +_{12})$. **Answer**: $\mathbb{Z}_{12} = \{ \mathbf{0},\ \mathbf{1},\ \mathbf{2},\ \mathbf{3} \dots \dots \mathbf{11} \}$ $\langle \mathbf{1} \rangle = \{ \mathbf{0},\ \mathbf{1},\ \mathbf{2},\ \mathbf{3}, \dots \dots\ \mathbf{11} \}$ $\langle \mathbf{2} \rangle = \{ \mathbf{0},\ \mathbf{2},\ \mathbf{4},\ \mathbf{6},\ \mathbf{8},\ \mathbf{10} \}$ $\langle \mathbf{3} \rangle = \{ \mathbf{0},\ \mathbf{3},\ \mathbf{6},\ \mathbf{9} \}$ $\langle \mathbf{4} \rangle = \{ \mathbf{0},\ \mathbf{4},\ \mathbf{8} \}$ $\langle \mathbf{6} \rangle = \{ \mathbf{0},\ \mathbf{6} \}$ $\langle \mathbf{12} \rangle = \{ \mathbf{0} \}$
C	2	Show that $(\{ 1,\ 4,\ 13,\ 16 \}, \times_{17})$ is a subgroup of $(\mathbb{Z}_{17}^*, \times_{17})$.

Method 4 ⇝ Abelian group

Abelian group or Commutative group

→ A group $(G, *)$ is known as abelian group if $a * b = b * a$; $\forall a, b \in G$.

→ For Example:

Group $(\mathbb{R}, +)$ is abelian group.

Reason: $\forall$ a, $b \in \mathbb{R} \Rightarrow a + b = b + a$

→ $(\mathbb{Z}_n, +_n)$ is abelian group for all - natural number n.

→ $(\mathbb{Z}_p^*, \times_p)$ is abelian group if p is prime number.

Example of Method-4: Abelian group

C	1	Show that $(\mathbb{Q}^+, *)$ forms an Abelian group. Where, $*$ defined by $a * b = \frac{ab}{2}$ $\forall a, b \in \mathbb{Q}^+$.
C	2	Show that $(\mathbb{Z}_6, +_6)$ is an abelian group.

Method 5 ⇝ Order of an Element of a Group

Order of Group

→ Let $(G, *)$ be a group.

The **total** number of elements in G is known as order of group.

→ Order of group is denoted by **O(G) or | G |** and read as "order of group".

→ If group G has infinite elements, then the order of group is not define.

→ For Example:

(3) If $G = (\mathbb{Z}_3^*, \times_3)$ then $O(\mathbb{Z}_3^*) = 2$

(4) If $G = (\mathbb{Z}_n, +_n)$ then $O(\mathbb{Z}_n) = n$

(5) If $G = (\mathbb{Z}, +)$ then $O(\mathbb{Z}) = \infty$

Order of an Element of a Group

→ Let $(G, *)$ be a group and $a \in G, e \in G$.

The order of an element **"a"** is the **smallest** positive integer **"n"** such that $\mathbf{a^n = e}$ then **"n"** is known as order of an element of group G.

→ Order of an element a is denoted by **O(a)** or **| a |** and read as "order of a".

→ If no such integer exists, we say that **"a"** has infinite order.

→ For Example:

Let $G = \{1, -1, i, -i\}$ then $(G, \times)$ is a group.

Identity element of group G is "1".

We find order of 1,

$(1)^{1} = 1 \Rightarrow O(1) = \mathbf{1}$

We find order of -1,

$(-1)^1 = -1, \ (-1)^{2} = 1 \Rightarrow O(-1) = \mathbf{2}$

We find order of i,

$(i)^1 = i, \ (i)^2 = -1, \ (i)^3 = -i, \ (i)^{4} = 1 \Rightarrow O(i) = \mathbf{4}$

We find order of $-i$,

$(-i)^1 = -i, \ (-i)^{2} = 1 \Rightarrow O(-i) = \mathbf{2}$

So, $O(1) = 1, \quad O(-1) = 2, \quad O(i) = 4, \quad O(-i) = 2.$

→ Results:

(6) Let "**e**" be an identity element of group G then $\mathbf{O(e) = 1}$.

(7) Identity element is the only element of order one.

(8) The order of every element of a finite group is finite.

(9) Let G be a group then for any $a \in G$ then $O(a) = O(a^{-1})$

Example of Method-5: Order of an Element of a Group

C	1	Find the order of each element of $(\mathbb{Z}_{10}, +_{10})$. **Answer :|1|=10, |2|=5,|3|=10,|4|=5,|5|=2,|6|=5,|7|=10,|8|=5,|9|=10**
C	2	Find the order of each element of $(\mathbb{Z}_7^*, \times_7)$. **Answer :|1|=1, |2|=3,|3|=6,|4|=1,|5|=6, |6|=2**
C	3	Find the order of each element of $(\mathbb{Z}, +)$. **Answer : Order of all nonzero element in $\mathbb{Z}$ are Infinite.**

Method 6⇝ Cyclic Group

Cyclic Group

→ A group G is known as cyclic group if there exists an element **$a \in G$** such that **every** element of G can be written as **power** of **"a"**.

i.e., $\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \} = G$

→ Here, **"a"** is a generator of the group G.

→ For Example:

Let $G = \{ 1, \ -1, \ i, \ -i \}$ be a group under multiplication then,

$\langle i \rangle = \{ i^1, \ i^2, \ i^3, \ i^4 \} = \{ i, \ -1, \ -i, \ 1 \} = G$

$\langle -i \rangle = \{ (-i)^1, \ (-i)^2, \ (-i)^3, \ (-i)^4 \} = \{ -i, \ 1, \ i, \ 1 \} = G$

So, generator of $G = \{ i, \ -i \}$

→ For $a \in (\mathbb{Z}_n, +_n)$ such that $(a, n) = 1$ then **"a"** is a generator of $(\mathbb{Z}_n, +_n)$

→ Note:

→ G= $(\mathbb{Z}_n, +_n)$ is always cyclic group.

→ The number of generators of $\mathbb{Z}_n$ are relatively prime to n.

→ If **G** is cyclic group then it is abelian. But, converse may not be true.

Example of Method-6: Cyclic Group

C	1	Prove that $(\mathbb{Z}_6, +_6)$ is cyclic group.
C	2	Prove that third root of unity is cyclic group.
C	3	Find all the generators of cyclic groups **(a)** $(\mathbb{Z}_5, +_5)$ **(b)** $(\mathbb{Z}_6, +_6)$. **(a) 1, 2, 3, 4 are the generators of $\mathbb{Z}_5$.** **(b) 1 and 5 are the generators of $\mathbb{Z}_{6,}$,**

* * * * * * * * * *