Pimpalner Education Society's

Karm. A. M. Patil Arts, Commerce and Kai. Annasaheb N. K. Patil Science Senior College Pimpalner, Tal.- Sakri, Dist.- Dhule.

CLASS NOTES

CLASS: S.Y.B.SC   SEM.-III

SUBJECT: MTH-302(A): GROUP THEORY

PREPARED BY: PROF. K. D. KADAM

MTH -302(A): GROUP THEORY

Unit-1: Groups **Marks-15**

1.1 Definition and Examples of a group.

1.2 Simple Properties of Group.

1.3 Abelian Group.

1.4 Finite and Infinite Groups.

1.5 Order of a Group.

1.6 Order of an Element and Its Properties.

Unit-2: Subgroups **Marks-15**

2.1 Definition and Examples of Subgroups.

2.2 Simple Properties of Subgroup.

2.3 Criteria for a Subset to be a Subgroup.

2.4 Cyclic Groups

2.5 Normal subgroups and Coset Decomposition.

2.6 Lagrange's Theorem for Finite Group.

2.7 Euler's Theorem and Fermat's Theorem.

Unit-3: Homomorphism and Isomorphism of Groups **Marks-15**

3.1 Definition and Examples of Group Homomorphism.

3.2 Properties of Group Homomorphism.

3.3 Kernel of a Group Homomorphism and it's Properties.

3.4 Definition and Examples of Isomorphism.

3.5 Definition and Examples of Automorphism of Groups.

3.6 Properties of Isomorphism of Groups.

Unit -4: Rings **Marks-15**

4.1 Definition and Simple Properties of a Ring.

4.2 Commutative Ring, Ring with unity, Boolean Ring.

4.3 Ring with zero divisors and without zero Divisors.

4.4 Integral Domain, Division Ring and Field. Simple Properties.

==

Recommended Book: -

1. University Algebra: N. S. Gopalakrishnan, New age international publishers, 2018. (Chapter 1: 1.3, 1.4, 1.5, 1.6,1.7, 1.8, 1.9)

Reference Books: -

1. Topics in Algebra: I. N. Herstein (John Wiley and Sons).
2. A first Course in Abstract Algebra: J. B. Fraleigh (Pearson).
3. A course in Abstract Algebra: Vijay K. Khanna and S. K. Bhambri, Vikas Publishing House Pvt. Ltd., Noida.

Learning Outcomes:

Upon successful completion of this course the student will be able to:

a) understand group and their types which is one of the building blocks of pure and applied mathematics.

b) understand Lagarnge, Euler and Fermat theorem

c) understand concept of automorphism of groups

d) understand concepts of homomorphism and isomorphism

e) understand basic properties of rings and their types such as integral domain and field.

==

UNIT-1: GROUPS

==

Binary Operation: Let G be a non-empty set. A function * : G x G → G given by * (a, b) = a * b, is called a binary operation on (or in) G.

Notation:

1) We use the notation a * b to denote * (a, b). If G is a non-empty set with a binary operations * then we denote this algebraic structure by (G, *)
2) Throughout this course we use the following notations:
   i) $\mathbb{N}$: The set of all natural numbers.
   ii) $\mathbb{Z}$: The set of all integers.
   iii) $\mathbb{Q}$: The set of all rational numbers.
   iv) $\mathbb{R}$: The set of all real numbers.
   v) $\mathbb{C}$: The set of all complex numbers.

Note: A non-empty set G is said to be closed for * if whenever a, b ∈ G implies a*b ∈ G.

e.g. 1) Usual addition and multiplication are binary operations in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

2) Usual subtraction of natural numbers is not a binary operation in $\mathbb{N}$, ∵ 2, 3 ∈ N but 2 - 3 = -1 ∉ $\mathbb{N}$.

3) Division of two integers is not a binary operation in $\mathbb{Z}$, ∵ 22, 5 ∈ $\mathbb{Z}$ but $\frac{22}{5} \notin \mathbb{Z}$.

Group: A non-empty set G with a binary operation * is said to be a group if

i) * is associative in G i.e. (a * b) * c = a * (b * c), ∀ a, b, c ∈ G.

ii) G has an identity element e ∈ G with a * e = a = e * a, ∀ a ∈ G.

iii) Every element of G has an inverse in G w.r.t. *.

i.e. for each a ∈ G, there exists b ∈ G such that a * b = e = b * a.

Note: A group G with a binary operation * is denoted by (G, *) or < G, * > or simply G.

Examples:

1) ($\mathbb{Z}$, +), ($\mathbb{Q}$, +), ($\mathbb{R}$, +), ($\mathbb{C}$, +) are groups w.r.t. usual addition with identity element 0 and inverse of any a is -a.

2) ($\mathbb{Q}'$ = $\mathbb{Q}$ -{0}, ×),($\mathbb{R}'$ = $\mathbb{R}$ - {0}, ×).($\mathbb{C}'$ = $\mathbb{C}$ - {0}, ×) are groups w.r.t. usual multiplication with identity element 1 and inverse of any element a is $\frac{1}{a}$.

Ex. Show that G = {1, -1} is a group w.r.t. usual multiplication.

Sol. Consider a table for the binary operation multiplication.

×	1	-1
1	1	-1
-1	-1	1

We observe that all entries in the table are elements of G. Therefore multiplication is a binary operation in G. We know that multiplication operation of numbers is associative.

Also 1 is an identity of G and from the table 1.1 = (-1).(-1) = 1 i.e. every element has multiplicative inverse in G. Hence (G, .) is a group.

Ex. Show that G = {1, -1, i, -i}, where i= $\sqrt{-1}$, is a group w.r.t. usual multiplication of complex numbers.

Sol. Consider a multiplication table for the binary operation multiplication

×	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
I	i	-i	-1	1
-i	-i	i	1	-1

We observe that all entries in the table are elements of G. Therefore multiplication is a binary operation in G. We know that multiplication operation of numbers is associative.
Also 1 is an identity of G and from the table elements 1, -1, i and -i has inverses 1, -1, -i and i in G i.e. every element has multiplicative inverse in G. Hence (G, .) is a group.

===

Ex. Let G be the set of all 2X 2 matrices over real numbers. Then G is a group w.r.t. addition of matrices but it is not a group w.r.t. multiplication of matrices.

Sol. 1) i) Clearly addition of matrices is a binary operation and is associative in G.

ii) $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the identity element of G.

iii) For any $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in$ G, ∃ $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in$ G such that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\therefore \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$$

Hence (G,+) is a group.

2) (G, .) is not group because $\begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix}$ has no multiplicative inverse in G as $\begin{vmatrix} 2 & 3 \\ 4 & 6 \end{vmatrix} = 0$

===

Ex. Let G = {A: A is non-singular matrix of order n over ℝ}. Show that G is a group w.r.t. usual multiplication of matrices.

Proof:

i) Let A, B ∈ G.

∴ A, B are non-singular matrices of order n.

∴ $|A| \neq 0, |B| \neq 0$.

∴ $|AB| = |A||B| \neq 0$.

∴ AB ∈ G.

Thus multiplication of matrices is a binary operation on G.

ii) We know that matrix multiplication is associative

i.e. (AB) C= A (BC), ∀ A, B, C ∈ G

i ii) For any A ∈ G, AI = A = IA, where I is the identity matrix of order n in G.

I is the identity element of G.

iv) Let A ∈ G.

∴ $|A| \neq 0$

Then ∃ $A^{-1} = B = \frac{1}{|A|}adj(A)$ such that AB = BA = I

Thus every element of G has inverse in G.

∴ (G, .) is a group is proved.

==

Ex. Let $\mathbb{Q}^+$ denote the set of all positive rationals. For a, b ∈ $\mathbb{Q}^+$, define $a * b = \frac{ab}{2}$

Show that ($\mathbb{Q}^+$, *) is a group.

Proof: i) Clearly a, b ∈ $\mathbb{Q}^+ \Longrightarrow a * b = \frac{ab}{2} \in \mathbb{Q}^+$.

i. e. * is closed in $\mathbb{Q}^+$.

ii) Let a, b, c ∈ $\mathbb{Q}^+$.

Consider $(a * b) * c = \frac{ab}{2} * c = \frac{\left(\frac{ab}{2}\right)c}{2} = \frac{abc}{4}$

and $a * (b * c) = a * \frac{bc}{2} = \frac{a\left(\frac{bc}{2}\right)}{2} = \frac{abc}{4}$

∴ (a * b) * c = a * (b * c).

i.e. * is associative in $\mathbb{Q}^+$.

iii) For a ∈ $\mathbb{Q}^+$, we have

$a * 2 = \frac{a2}{2} = a$ and $2 * a = \frac{2a}{2} = a$.

∴ 2 is the identity element in $\mathbb{Q}^+$.

iv) For a ∈ $\mathbb{Q}^+$ ∃ $\frac{4}{a} \in \mathbb{Q}^+$ with

$a * \frac{4}{a} = \frac{a\left(\frac{4}{a}\right)}{2} = 2$ and $\left(\frac{4}{a}\right) * a = \frac{\left(\frac{4}{a}\right)a}{2} = 2$

∴ $a^{-1} = \frac{4}{a}$ i.e. every element has inverse in $\mathbb{Q}^+$.

Hence ($\mathbb{Q}^+$, *) is a group.

==

Ex. Prove that $G = \left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} : x \text{ is a non-zero real number} \right\}$ is a group under matrix multiplication.

Proof: Let $G = \left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} : x \text{ is a non-zero real number} \right\}$ with operation multiplication

i) For $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$ & $B = \begin{bmatrix} y & y \\ y & y \end{bmatrix} \in G \Longrightarrow AB = \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \in G$ ……(1)

∵ x & y are non zero real numbers ⟹ 2xy is non zero real number.

∴ Multiplication is closed in G.

ii) For $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$, $B = \begin{bmatrix} y & y \\ y & y \end{bmatrix}$ & $C = \begin{bmatrix} z & z \\ z & z \end{bmatrix} \in G$ we have,

$$(AB)C = \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \begin{bmatrix} z & z \\ z & z \end{bmatrix} = \begin{bmatrix} 4xyz & 4xyz \\ 4xyz & 4xyz \end{bmatrix} \text{ by equation (1)}$$

$$\& \ A(BC) = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \begin{bmatrix} 2yz & 2yz \\ 2yz & 2yz \end{bmatrix} = \begin{bmatrix} 4xyz & 4xyz \\ 4xyz & 4xyz \end{bmatrix} \text{ by equation (1)}$$

∴ (AB)C = A(BC)

∴ Multiplication is associative in G.

iii) As $\frac{1}{2}$ is a non zero real number ⟹ $E = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \in G$ is an identity element

$$\because AE = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix} = A$$

$$\& \ EA = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} x & x \\ x & x \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix} = A \ \forall \ A = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \in G.$$

i. e. identity element is exist in G.

iv) For $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \in G$, suppose $B = \begin{bmatrix} y & y \\ y & y \end{bmatrix}$ is inverse of A.

$$\therefore AB = E = BA \text{ i. e. } \begin{bmatrix} x & x \\ x & x \end{bmatrix} \begin{bmatrix} y & y \\ y & y \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \Rightarrow \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

∴ $2xy = \frac{1}{2} \Rightarrow y = \frac{1}{4x}$ which is a non zero real number ⟹ $B = \begin{bmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{24x} \end{bmatrix} \in G.$

i. e. every element has inverse in G.

Hence G is a group under matrix multiplication is proved.

===

Properties of Groups:

Theorem: If G is a group, then i) Identity element of G is unique,

ii) Every element of G has unique inverse in G,

iii) $(a^{-1})^{-1} = a \ \forall \ a \in G$

iv) $(ab)^{-1} = b^{-1}a^{-1} \ \forall \ a, b \in G$ (Reversal law for the inverse of a product)

Proof: Let G be a group.

i)Let e and e' be identity elements of G.

∴ ee' = e ∵ e' is an identity element of G.

and ee' = e' ∵ e is an identity element of G.

∴ e = e'. Hence identity element of G is unique

ii) For a ∈ G. Suppose b and c are inverses of a in G.

∴ ab = e = ba and ac = e = ca

Now b = eb

$= (ca)\,b$

$= c(ab)$ by associative law

$= ce$

$= c$

Hence a has unique inverse in G

iii) Let $a \in G$

$\therefore aa^{-1} = e = a^{-1}a$

By definition of inverse of an element, a is the inverse of a^{-1}

$\therefore (a^{-1})^{-1} = a$

v) Let $a, b \in G$

Consider $(ab)(b^{-1}\, a^{-1}) = a(bb^{-1})\, a^{-1}$ by associative law.

$= aea^{-1}$ by associative law

$= aa^{-1}$

$= e$ ....(1)

Similarly, we have $(b^{-1}a^{-1})\,(ab) = e$ ....(2)

From (1) and (2),

$\therefore (ab)^{-1} = b^{-1}\, a^{-1}\ \forall\, a, b \in G$

===

Theorem: Let G be a group and a, b, c ∈ G. Then

i) Left cancellation law : $ab = ac \Longrightarrow b = c$,

ii) Right cancellation law: $ba = ca \Longrightarrow b = c$

Proof: Let G be a group and a, b, c ∈ G.

i) ab = ac

Pre-multiplying both the sides by a^{-1}, we get

$a^{-1}\,(ab) = a^{-1}\,(ac)$

$\therefore (a^{-1}\, a)\, b = (a^{-1}\, a))c$ by associative law

$\therefore eb = ec$

$\therefore b = c$

i) ba = ca

Post-multiplying both the sides by a^{-1}, we get

$(ba)a^{-1} = (ca)a^{-1}$

$\therefore b(aa^{-1}) = c(aa^{-1})$ by associative law

$\therefore be = ce$

$\therefore b = c.$

Hence proved.

Theorem: Let G be a group and a, b ∈ G. Then the equations

i) ax = b and i) ya = b have unique solutions in G.

Proof: Let G be a group and a, b ∈ G.

i) Consider the equation ax = b.

Pre-multiplying both the sides by a^{-1}, we get

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

$\therefore (a^{-1}a)x = a^{-1}b$ by associative law

$\therefore ex = a^{-1}b$

$\therefore x = a^{-1}b$

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

Uniqueness: Suppose x_1 and x_2 are solutions of ax = b.

$ax_1 = b$ and $ax_2 = b$

$\therefore ax_1 = ax_2$

$\therefore x_1 = x_2$ by left cancellation law.

Hence ax = b has unique solution in G.

ii) Similarly, we have $y = ba^{-1}$ is the unique solution of ya = b in G.

==

Abelian groups: A group G is said to be abelian group if ab = ba, $\forall$ a, b $\in$ G.

e.g. 1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are abelian groups.

2) Let $G = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad\text{-}bc \neq 0,\ a, b, c, d \in \mathbb{R}\}$. Then G is a group w.r.t. matrix multiplication. But it is not an abelian group.

$\because$ For $A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$ & $B = \begin{bmatrix} 1 & 4 \\ 1 & 3 \end{bmatrix}$ we have

$$AB = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 1 & 4 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 1+2 & 4+6 \\ 0+3 & 0+9 \end{bmatrix} = \begin{bmatrix} 3 & 10 \\ 3 & 9 \end{bmatrix}$$

$$BA = \begin{bmatrix} 1 & 4 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 1+0 & 2+12 \\ 1+0 & 2+9 \end{bmatrix} = \begin{bmatrix} 1 & 14 \\ 1 & 11 \end{bmatrix}$$

$\therefore AB \neq BA$

Finite and Infinite Group: A group G is said to be finite if the number of elements in G is finite otherwise it is called an infinite group.

Order of Group: If G is a finite group then the number of elements in G is called order of G and it is denoted by o(G).

Note: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are infinite abelian groups.

==

Ex.: Let $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots\ldots, \overline{n-1}\}$ the set of all residue classes of integers modulo n. Define a binary operation $+_n$ in $\mathbb{Z}_n$, as $\bar{a} +_n \bar{b} = \overline{a+b} = \bar{r}$ where r is the remainder obtained when a + b is divided by n. Show that $(\mathbb{Z}_n, +_n)$ is a finite abelian group.

Sol. i) Let a, b $\in \mathbb{Z}_n$, and r is the remainder obtained when a + b is divided by n.

$\therefore 0 \leq r < n$

Hence $\bar{a} +_n \bar{b} = \overline{a+b} = \bar{r} \in \mathbb{Z}_n$

$\therefore \mathbb{Z}_n$ is closed w.r.t. $+_n$

ii) Let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$,

$(\bar{a} +_n \bar{b}) +_n \bar{c} = (\overline{a + b}) +_n \bar{c}$

$= (\overline{a + b) + c}$

$= \overline{a + (b + c)}$

$= \bar{a} +_n (\overline{b + c})$

$= \bar{a} +_n (\bar{b} +_n \bar{c})$

$\therefore +_n$ is associative in $\mathbb{Z}_n$.

iii) For any $\bar{a} \in \mathbb{Z}_n$,

$\bar{a} +_n \bar{0} = \overline{a + 0} = \bar{a}$ and $\bar{0} +_n \bar{a} = \overline{0 + a} = \bar{a}$

$\therefore$ $\bar{0}$ is the identity of $\mathbb{Z}_n$

iv) For $\bar{a} \in \mathbb{Z}_n$, $\exists$ $\overline{n - a} \in \mathbb{Z}_n$, such that

$\bar{a} +_n \overline{n - a} = \overline{a + n - a} = \bar{n} = \bar{0}$ and $\overline{n - a} +_n \bar{a} = \overline{n - a + a} = \bar{n} = \bar{0}$

Hence every element of $\mathbb{Z}_n$ has inverse in $\mathbb{Z}_n$

v) For $\bar{a}, \bar{b} \in \mathbb{Z}_n$,

$\bar{a} +_n \bar{b} = \overline{a + b} = \overline{b + a} = \bar{b} +_n \bar{a}$

$\therefore +_n$ is commutative in $\mathbb{Z}_n$.

vi) $\mathbb{Z}_n$ contains n elements and n is finite.

$\mathbb{Z}_n$ is a finite set.

Thus $(\mathbb{Z}_n, +_n)$ is a finite abelian group.

==

Ex. Show that $G = \mathbb{Q} - \{-1\}$ is an abelian group under the binary operation $a * b = a + b + ab, \forall a, b \in G$.

Proof: Let * be a binary operation defined on $G = \mathbb{Q} - \{-1\}$ by

$a * b = a + b + ab, \forall a, b \in G$.

i) Let a, b, c ∈ G

Consider $(a * b) * c = (a + b + ab) * c$

$= (a + b + ab) + c + (a + b + ab) c$

$= a + b + ab + c + ac + bc + abc$

$= a + b + c + ab + ac + bc + abc$

$= a + b + c + bc + ab + ac + abc$

$= a + (b + c + bc) + a (b + c + bc)$

$= a * (b + c + bc)$

$= a * (b * c)$

$\therefore (a * b) * c = a * (b * c)$.

i.e. * is associative in G

ii) For a ∈ G, we have

$a * 0 = a + 0 + a0 = a$ and $0 * a = 0 + a + 0a = a$.

∴ 0 is the identity element of G.

iii) Let a ∈ G, suppose b is an inverse of a a * b = b * a = 0

∴ a + b + ab = 0

∴ b(1+ a) = -a

∴ b = $\frac{-a}{1+a}$ ∈ G ∵ $\frac{-a}{1+a}$ ≠ -1

i.e. every element has inverse in G.

Hence (G, *) is a group.

iv) As a * b = a + b + ab = b + a + ba = b * a ∀ a, b ∈ G.

∴ * is commutative in G.

Hence (G, *) is an abelian group is proved.

==

Ex. Show that G = ℝ – {1} is an abelian group under the binary operation a * b = a + b - ab, ∀ a, b ∈ G.

Proof: Let * be a binary operation defined on G = ℝ – {1} by

a * b = a + b - ab, ∀ a, b ∈ G.

i) Let a, b, c ∈ G

Consider (a * b) * c = (a + b - ab) * c

= (a + b - ab) + c - (a + b - ab) c

= a + b - ab + c - ac - bc + abc

= a + b + c - ab - ac - bc + abc

= a + b + c - bc - ab - ac + abc

= a + (b + c - bc) - a (b + c - bc)

= a * (b + c - bc)

= a * (b * c)

∴ (a * b) * c = a * (b * c).

i.e. * is associative in G

ii) For a ∈ G, we have

a * 0 = a + 0 - a0 = a and 0 * a = 0 + a - 0a = a.

∴ 0 is the identity element of G.

iii) Let a ∈ G, suppose b is an inverse of a

a * b = b * a = 0

∴ a + b - ab = 0

∴ b(1- a) = -a

∴ b = $\frac{-a}{1-a}$ ∈ G ∵ $\frac{-a}{1-a}$ ≠ 1

i.e. every element has inverse in G.

Hence (G, *) is a group.

iv) As a * b = a + b - ab = b + a - ba = b * a ∀ a, b ∈ G.

∴ * is commutative in G.

Hence (G, *) is an abelian group is proved.

Ex. Let $\mathbb{Q}^+$ denote the set of all positive rational numbers and for any a, b ∈ $\mathbb{Q}^+$, define $a * b = \frac{ab}{3}$. Show that ($\mathbb{Q}^+$, *) is an abelian group.

Proof: i) Clearly a, b ∈ $\mathbb{Q}^+ \Longrightarrow a * b = \frac{ab}{3} \in \mathbb{Q}^+$.

i. e. * is closed in $\mathbb{Q}^+$.

ii) For a, b, c ∈ $\mathbb{Q}^+$.

Consider $(a * b) * c = \left(\frac{ab}{3}\right) * c = \frac{\left(\frac{ab}{3}\right)c}{3} = \frac{abc}{9}$

and $a * (b * c) = a * \left(\frac{bc}{3}\right) = \frac{a\left(\frac{bc}{3}\right)}{3} = \frac{abc}{9}$

∴ (a * b) * c = a * (b * c).

i.e. * is associative in $\mathbb{Q}^+$.

iii) For a ∈ $\mathbb{Q}^+$, we have

$a * 3 = \frac{a3}{3} = a$ and $3 * a = \frac{3a}{3} = a$.

∴ 3 is the identity element of $\mathbb{Q}^+$.

iv) For a ∈ $\mathbb{Q}^+$. ∃ $\frac{9}{a} \in \mathbb{Q}^+$ with

$a * \frac{9}{a} = \frac{a\left(\frac{9}{a}\right)}{3} = 3$ and $\left(\frac{9}{a}\right) * a = \frac{\left(\frac{9}{a}\right)a}{3} = 3$

∴ $a^{-1} = \frac{9}{a}$ i.e. every element has inverse in $\mathbb{Q}^+$.

Hence ($\mathbb{Q}^+$, *) is a group.

v) As $a * b = \frac{ab}{3} = \frac{ba}{3} = b * a \ \forall\ a, b \in \mathbb{Q}^+$.

∴ * is commutative in $\mathbb{Q}^+$.

Hence ($\mathbb{Q}^+$, *) is an abelian group is proved.

Ex. Let $G = \{(a, b): a, b \in \mathbb{R}, a \neq 0\}$. Show that (G, ʘ) is a non-abelian group, where $(a, b)\ ʘ\ (c, d) = (ac, ad + b)$.

Sol. Let $G = \{(a, b): a, b \in \mathbb{R}, a \neq 0\}$ and operation ʘ is defined by

(a, b) ʘ (c, d) = (ac, ad + b) ∀ (a, b), (c, d) ∈ G

i) Let (a, b), (c, d) ∈ G

∴ a ≠ 0, c ≠ 0

∴ ac ≠ 0

∴ (a, b) ʘ (c, d) = (ac, ad + b) ∈ G

∴ ʘ is closed in G.

ii) Associativity: Let (a, b), (c, d), (e, f ∈ G.

[(a, b) ʘ (c, d)] ʘ (e, f) = (ac, ad +b) ʘ (e, f)

= (ace, acf +ad+b) ……..(1)

(a, b) ʘ [(c, d) ʘ (e, f)] = (a, b) ʘ (ce, cf+d)

= (ace, acf+ad+b) ……..(2)

From (1) and (2)

[(a, b) ʘ (e, d)] ʘ (e, f) = (a , b) ʘ [(c, d) ʘ (e, f)]

∴ ʘ is associative.

iii) Existence of identity element: As 1 & 0 ∈ R ⟹ (1, 0) ∈ G with

(a, b) ʘ (1, 0) = (a, b) = (1, 0) ʘ (a, b) = (a, b) ∀ (a, b) ∈ G

Thus (1, 0) is the identity of G.

iv) Existence of inverse:

For (a, b) ∈ G. Suppose (c, d) is inverse of (a, b).

∴ (a, b) ʘ (c, d) = (1, 0)

i.e. (ac, ad+b) = (1, 0)

i.e. ac = 1, ad+b = 0

∴ $c = \frac{1}{a}$ & $d = \frac{-b}{a}$

Hence $(a, b)^{-1} = (\frac{1}{a}, \frac{-b}{a}) \in G \quad \because \frac{1}{a} \neq 0$

∴ G is a group.

v) For (1, 2), (3,4) ∈ G.

(1, 2) ʘ (3, 4) = (3, 4+2) = (3, 6)

and (3, 4) ʘ (1, 2) = (3, 6+4) = (3, 10)

(1, 2) ʘ (3, 4) ≠ (3, 4) ʘ (1, 2)

∴ ʘ is not commutative in G.

Hence G is a non-abelian group is proved.

==

Ex. Let G be a group and for all a, b ∈ G, $(ab)^n = a^n b^n$, for three consecutive integers n. Show that G is an abelian group.

Proof: Let $(ab)^n = a^n b^n$ ……….(1)

$(ab)^{n+1} = a^{n+1} b^{n+1}$ ……...(2)

& $(ab)^{n+2} = a^{n+2} b^{n+2}$ ……...(3)

From (2), $a^{n+1} b^{n+1} = (ab)^{n+1}$

$(a^n a)(b^n b) = (ab)^n (ab) = (a^n b^n)(ab)$ by (1)

∴ $a^n (ab^n) b = a^n (b^n a) b$

∴ $ab^n = b^n a$ by cancellation laws. …..(4)

Similarly from (2) and (3), we have $ab^{n+1} = b^{n+1}a$

Now $ab^{n+1} = b^{n+1}a$

∴ $a(b^n b) = (b^n b) a$

∴ $(ab^n)b = b^n (ba)$

∴ $(b^n a)b = (b^n b) a$ by (4)

∴ $b^n (ab) = b^n (ba)$

∴ ab = ba by lett cancellation law.

Thus ab = ba, ∀ a, b ∈ G.

Hence G is abelian group is proved.

==

Ex. Show that a group G is abelian if and only if $(ab)^2 = a^2b^2$, ∀ a, b ∈ G.

Proof: Let G be an abelian group and a, b ∈ G.

∴ ab = ba .... (1)

Now $(ab)^2$ = (ab)(ab)

= a(ba)b)

= a(ab)b by (1)

= (aa)(bb)

= (aa)(bb)

= a^2b^2

Conversely, suppose that $(ab)^2 = a^2b^2$, ∀ a, b ∈ G.

For a, b ∈ G. we have $(ab)^2 = a^2b^2$

∴ (ab)(ab) = (aa)(bb)

∴ a(ba)b) = a(ab)b)

∴ (ba) = (ab) by cancellation laws

∴ ab = ba ∀ a, b ∈ G.

Hence G is an abelian group is poved.

==

Ex. If in a group G, every element is its own inverse then prove that G is abelian.

Proof: Let G be a group in which every element is its own inverse.

∴ For a, b ∈ G ⟹ a^{-1}= a and b^{-1} = b........ (1)

Now a, b ∈ G ⟹ ab ∈ G

⟹ $(ab)^{-1}$= ab

⟹ $b^{-1}a^{-1}$ = ab

⟹ ba= ab by (1)

Hence G is an abelian group is poved.

Ex. If G is a group such that $a^2 = e$, $\forall\ a \in G$, then show that G is abelian.

Proof: Let G be a group such that $a^2 = e$, $\forall\ a \in G$.

∴ For a, b ∈ G ⟹ a^2 = e and b^2 = e........ (1)

Now a, b ∈ G ⟹ ab ∈ G

⟹ $(ab)^2$ = e

⟹ $(ab)^2$ = ee ∵ e is identity in G

⟹ $(ab)^2 = a^2\ b^2$ by (1)

⟹ (ab)(ab) = (aa)(bb)

⟹ a(ba)b = a(ab)b

⟹ (ba) = (ab) by cancellation laws

⟹ ab = ba

Hence G is an abelian group is proved.

==

Euler's Totient Function: The function $\emptyset: \mathbb{N} \to \mathbb{N}$ defined by

$\emptyset(n)$ = The number of positive integers less than or equal to n and relatively prime to n, is called Euler's totient function.

e.g. 1) $\emptyset(8) = 4$ $\because$ 1, 3, 5, 7 are positive integers ≤ 8 and relatively prime to 8.

2) $\emptyset(1) = 1$

3) $\emptyset(5) = 4$

Note: If p is prime, then $\emptyset(p) = P - 1$

==

Ex. Let $\mathbb{Z}_n'$ denotes the set of all prime residue classes modulo n i.e. $\mathbb{Z}_n' = \{\bar{a} \in Z_n' : (a, n) = 1\}$. Show that $\mathbb{Z}_n'$ is an abelian group of order $\emptyset(n)$ w.r.t. $\times_n$.

Proof: i) Let $\bar{a}, \bar{b} \in \mathbb{Z}_n'$ and r is the remainder obtained when ab is divided by n.

Now $\bar{a}, \bar{b} \in \mathbb{Z}_n' \Rightarrow (a, n) = 1$ and $(b, n) = 1$

$\Rightarrow (ab, n) = 1$

$\Rightarrow (r, n) = 1$ $\because$ $ab \equiv r \pmod{n}$

$\Rightarrow \bar{r} \in \mathbb{Z}_n'$

Hence $\bar{a} \times_n \bar{b} = \overline{ab} = \bar{r} \in \mathbb{Z}_n'$

$\therefore$ x_n is closed in $\mathbb{Z}_n'$.

ii) Clearly $(\bar{a} \times_n \bar{b}) \times_n \bar{c} = \bar{a} \times_n (\bar{b} \times_n c)\ \forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n'$

iii) $(1, n) = l \Rightarrow \bar{1} \in \mathbb{Z}_n'$, Also $\bar{a} \times_n \bar{1} = \bar{a} = \bar{1} \times_n \bar{a},\ \forall\ \bar{a} \in \mathbb{Z}_n'$

$\therefore$ $\bar{1}$ is the identity of $\mathbb{Z}_n'$ w.r.t. $\times_n$

iv) Let $\bar{a} \in \mathbb{Z}_n'$,

$\therefore$ $(a, n) = 1$

$\therefore$ There exist $p, q \in Z$ such that $ap + nq = 1$.

$\therefore$ $ap - 1 = (-q)\, n$

$\therefore$ $ap - 1 \equiv 0 \pmod{n}$

$\therefore$ $ap \equiv 1 \pmod{n}$

$\therefore$ $\overline{ap} = \bar{1}$

$\therefore$ $\bar{a} \times_n \bar{p} = \bar{1}$

$\therefore$ $(\bar{a})^{-1} = \bar{p} \in \mathbb{Z}_n'$

Hence every element of $\mathbb{Z}_n'$ has inverse w.r.t. $\times_n$ in $\mathbb{Z}_n'$

v) As $\bar{a} \times_n \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \times_n \bar{a}\ \forall\ \bar{a}, \bar{b} \in \mathbb{Z}_n'$

vi) $\mathbb{Z}_n'$ contains exactly $\emptyset(n)$ elements.

From (i) to (vi), $\mathbb{Z}_n'$ is an abelian group of order $\emptyset(n)$.

==

Remark: In $Z_8' = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ i) $\bar{1}$ is the identity of $\mathbb{Z}_8'$.

ii) $(\bar{1})^{-1} = \bar{1}$, $(\bar{3})^{-1} = \bar{3}$, $(\bar{5})^{-1} = \bar{5}$, $(\bar{7})^{-1} = \bar{7}$ and iii) $o(\mathbb{Z}_8') = \emptyset(8) = 4$.

Integral power of an element in a group: Let G be a group and $a \in G$. For an integer n, we define a^n as follows: i) $a^n = aaa...a$ n-times if $n > 0$, ii) $a^n = e$ if $n = 0$ and

iii) $a^n = a^{-1}\, a^{-1}\, a^{-1} ...a^{-1}$ -n-times if $n < 0$

e.g. 1) In $(\mathbb{Z}, +)$ i) $2^4 = 2 + 2 + 2 + 2 = 8$, ii) $2^0 = 0$,

iii) $2^{-4} = 2^{-1} + 2^{-1} + 2^{-1} + 2^{-1} = (-2) + (-2) + (-2) + (-2) = -8$

2) In $(\mathbb{Z}_6, +_6)$ i) $(\bar{2})^4 = \bar{2} +_6 \bar{2} +_6 \bar{2} +_6 \bar{2} = \bar{8} = \bar{2}$, ii) $(\bar{2})^0 = \bar{0}$,

iii) $(\bar{2})^{-4} = (\bar{2})^{-1} +_6 (\bar{2})^{-1} +_6 (\bar{2})^{-1} +_6 (\bar{2})^{-1} = \bar{4} +_6 \bar{4} +_6 \bar{4} +_6 \bar{4} = \overline{16} = \bar{4}$

3) In $(\mathbb{Z}_8' = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}, \times_8)$ i) $(\bar{3})^4 = \bar{3} \times_8 \bar{3} \times_8 \bar{3} \times_8 \bar{3} = \overline{81} = \bar{1}$, ii) $(\bar{3})^0 = \bar{1}$,

iii) $(\bar{3})^{-4} = (\bar{3})^{-1} \times_8 (\bar{3})^{-1} \times_8 (3)^{-1} \times_8 (\bar{3})^{-1} = \bar{3} \times_8 \bar{3} \times_8 \bar{3} \times_8 \bar{3} = \overline{81} = \bar{1}$

==

Ex.: Let G be a group and $a \in G$, $n \in \mathbb{Z}$, Prove that $(a^n)^{-1} = (a^{-1})^n$

Proof: Case (i) $n > 0$

$\therefore$ $(a^n)^{-1} = (a\, a\, a ..... a)^{-1}$ n-times $= a^{-1}\, a^{-1}\, a^{-1} ...a^{-1}$ n-times $= (a^{-1})^n$

Case (ii) $n = 0$

$(a^0)^{-1} = e^{-1} = e = (a^{-1})^0$

Case (iii) $n < 0$

$(a^n)^{-1} = (a^{-1}\, a^{-1}\, a^{-1} ...a^{-1})^{-1}$ - n times $= (a^{-1})^{-1}(a^{-1})^{-1}.........(a^{-1})^{-1}$ - n times $= (a^{-1})^n$

Thus $(a^n)^{-1} = (a^{-1})^n$ $\forall\, n \in \mathbb{Z}$ is proved.

==

Ex.: Let $a \in G$ and $n \in \mathbb{Z}$, Prove that $a^{-n} = (a^{-1})^n$

Proof: Denote $-n = m < 0$

$\therefore$ $a^{-n} = a^m = a^{-1}\, a^{-1}\, a^{-1} ...a^{-1}$ -m-times $= a^{-1}\, a^{-1}\, a^{-1} ...a^{-1}$ n-times $= (a^{-1})^n$

Hence proved.

==

Ex.: Let G be a group and $a \in G$. For $m, n \in \mathbb{N}$, prove that

i) $a^m\, a^n = a^{m+n}$ and i) $(a^m)^n = a^{mn}$

Proof: Let $m, n \in \mathbb{N}$.

i) $a^m\, a^n = (a\, a\, ...\, a$ m-times$)\, (a\, a\, ...\, a$ n-times$)$

$= (a\, a\, ...\, a$ m+n-times$)$

$= a^{m+n}$

ii) $(a^m)^n = (a\, a\, ...\, a$ m-times$)^n$

$= (a\, a\, ...\, a$ m-times$)\, (a\, a\, ...\, a$ m-times$)......\, (a\, a\, ...\, a$ m-times$)$ n-times

$= a\, a\, ...\, a$ mn-times

$= a^{mn}$

Hence proved.

==

Ex.: Let G be a group and $a, b \in G$ be such that $ab = ba$. Prove that $(ab)^n = a^n\, b^n$, for all $n \in \mathbb{Z}$.

Proof: Let $n \in \mathbb{Z}$ and $a, b \in G$ be such that $ab = ba$.

Case (i) $n \in \mathbb{N}$

We first prove the result $ab^n = b^n a$ by induction on n.

For n= 1, $ab^1 = ab = ba = b^1 a$.

Suppose that $ab^k = b^k a$, for $k \in \mathbb{N}$

Now $ab^{k+1} = a(b^k b)$

$= (ab^k)b$

$= (b^k a)b$

$= b^k(ab)$

$= b^k(ba)$

$= (b^k b)a$

$= b^{k+1}a$

i. e. result is true for n = k $\Longrightarrow$ result is true for n = k+1

Hence by induction, $ab^n = b^n a, \forall n \in \mathbb{N}$ .. ….(i)

Now we claim $(ab)^n = a^n b^n, \forall n \in \mathbb{N}$.

For n = 1, $(ab)^1 = ab = a^1 b^1$

Suppose that $(ab)^k = a^k b^k$.

Now $(ab)^{k+1} = (ab)^k(ab)$

$= (a^k b^k)(ab)$

$= a^k (b^k a)b$

$= a^k (ab^k)b$ by (i)

$= (a^k a)(b^k b)$

$= a^{k+1} b^{k+1}$

Hence by induction $(ab)^n = a^n b^n, \forall n \in \mathbb{N}$.

case (ii) n = 0. Then $(ab)^0 = e = ee = a^0 b^0$.

case (iii) n < 0

Let n = -m, where $m \in \mathbb{N}$.

$(ab)^n = (ab)^{-m}$

$= ((ab)^{-1})^m$

$= ((ba)^{-1})^m$ $\because$ ab = ba

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

$= (a^{-1})^m (b^{-1})^m$ by case (i) as $m \in \mathbb{N}$

$= a^{-m} b^{-m}$

$= a^n b^n$.

Hence from case (i), (ii) and (iii), $(ab)^n = a^n b^n, \forall n \in \mathbb{Z}$ is proved.

==

Order of an Element in a Group: Let G be a group and $a \in G$. The smallest positive integer n (if it exists) such that $a^n = e$, is called order of a and it is denoted by o(a). If no such integer exists then a is said to be of infinite order.

Note: 1) The order of the identity element in any group is 1.

2) Let G be a group and $a \in G$. If $m \in \mathbb{N}$ is such that $a^m = e$ then $o(a) \leq m$

Examples:

1) Consider the group G = {1, -1, i, -i} under multiplication. Then

i) o(1) = 1 ∵ $1^1 = 1$.

ii) o(-1) = 2 ∵ $(-1)^1 = -1 \neq 1$, $(-1)^2 = 1$.

iii) o(i) = 4 ∵ $(i)^1 = i \neq 1$, $(i)^2 = -1 \neq 1$, $(i)^3 = -i \neq 1$, $(i)^4 = 1$.

iv) o(-i) = 4 ∵ $(-i)^1 = -i \neq 1$, $(-i)^2 = -1 \neq 1$, $(-i)^3 = i \neq 1$, $(-i)^4 = 1$.

2) Consider the group $(Z_{6,} +_6)$ with identity 0. Then

o (0) = 1, o (1) = 6, o (2) = 3, o (3) = 2, o (4) = 3, o (5) = 6.

3) In (Z, +), the order of 2 is infinite because there is no n ∈ ℕ such that $2^n = 0$.

==

Theorem: The order of every element in a finite group is finite.

Proof: Let G be a finite group of order n and a ∈ G.

Consider a set S = {a^m: m ∈ ℕ }. Then S ⊆ G.

Since G is finite, all the elements of S can not be distinct.

∴ $a^r = a^t$ for some r, t ∈ ℕ, r > t

∴ $a^{r-t} = e$ by cancellation law.

∴ o(a) ≤ r-t

∴ o (a) is finite

Hence order of every element of a finite group is finite is proved.

==

Ex.: Let G be a group and a, b ∈ G. Prove that 1) o (a^{-1}) = o (a) and 2) o (a) = o $(b^{-1}ab)$.

Proof:

1) Case (i) o(a) is finite say m.

∴ $a^m = e$

∴ $(a^m)^{-1} = e^{-1} = e$

∴ $(a^{-1})^m = e$

∴ $o(a^{-1}) \leq m$

ie. $o(a^{-1}) \leq o(a)$ .... (1)

Using (1), o $((a^{-1})^{-1}) \leq o(a^{-1})$

i.e. $o(a) \leq o(a^{-1})$ .... (2)

From (1) and (2) $o(a^{-1}) = o(a)$

Case (ii) o (a) is infinite.

Let if possible o (a^{-1}) is finite say r.

∴ $(a^{-1})^r = e$

∴ $(a^r)^{-1} = e$

∴ $a^r = e^{-1} = e$

∴ o(a) ≤ r

Impossible ∵ o(a) is infinite

Hence o (a^{-1}) is infinite.

$\therefore$ $o(a^{-1}) = o(a)$.

2) Claim: $(b^{-1}ab)^n = b^{-1}a^nb, \forall\ n \in \mathbb{N}$.

We prove it by induction on n.

For n = 1, $(b^{-1}ab)^1 = b^{-1}ab = b^{-1}a^1b$

Assume that $(b^{-1}ab)^k = b^{-1}a^kb$, where $k \in \mathbb{N}$

Now $(b^{-1}ab)^{k+1} = (b^{-1}ab)^k(b^{-1}ab)$

$= (b^{-1}a^kb)(b^{-1}ab)$

$= b^{-1}a^k(bb^{-1})ab$

$= b^{-1}a^keab$

$= b^{-1}a^kab$

$= b^{-1}a^{k+1}b$

Result is true for k + 1 also.

Hence by principle of finite induction

$(b^{-1}ab)^n = b^{-1}a^nb, \forall\ n \in \mathbb{N}$.

Case (i) o (a) is finite say m.

$\therefore$ $a^m = e$

Now $(b^{-1}ab)^m = b^{-1}a^mb$

$= b^{-1}eb$ $\quad \because a^m = e$

$= b^{-1}b$

$= e$

$\therefore$ $o(b^{-1}ab) \leq m$

$\therefore$ $o(b^{-1}ab) \leq o(a)$ ……(1)

Using (1), we have

$o((b^{-1})^{-1}(b^{-1}ab)(b^{-1})) \leq o(b^{-1}ab)$

$\therefore$ $o((b\,b^{-1})a(bb^{-1})) \leq o(b^{-1}ab)$

$\therefore$ $o(eae) \leq o(b^{-1}ab)$

$\therefore$ $o(a) \leq o(b^{-1}ab)$ …….(2)

from (1) and (2), $o(a) = o(b^{-1}ab)$.

Case (ii) o(a) is infinite.

Let if possible $o(b^{-1}ab)$ is finite say m.

$\therefore$ $(b^{-1}ab)^m = e$

$\therefore$ $b^{-1}a^mb = e$

$\therefore$ $a^m = beb^{-1}$

$\therefore$ $a^m = bb^{-1}$

$\therefore$ $a^m = e$

$\therefore$ $o(a) \leq m$

Impossible $\because$ o(a) is infinite.

Hence $o(b^{-1}ab)$ is infinite.

∴ $o(a) = o(b^{-1}ab)$.

==

Ex.: Let G be a group and a, b ∈ G. Prove that o(ab) = o(ba)

Proof: We have $ab = e(ab) = (b^{-1}b)(ab) = b^{-1}(ba)b$

∴ $o(ab) = o(b^{-1}(ba)b)$

∴ $o(ab) = o(ba)$ ∵ $o(b^{-1}ab) = o(a)$

Hence proved.

==

Ex. Let G be a group and a ∈ G, n ∈ ℕ. Show that $a^n = e$ if and only if o (a)|n.

Sol.: Let $a^n = e$ and o (a) = m.

By applying division algorithm on m and n, we get

$n = mq + r$, where $0 \le r < m$... (1)

Suppose that $r \neq 0$

∴ $r = n - mq$

∴ $a^r = a^{n-mq}$

∴ $a^r = a^n a^{-mq}$

∴ $a^r = a^n (a^m)^{-q}$

∴ $a^r = e (e)^{-q}$ ∵ $a^n = e$ & o(a) = m

∴ $a^r = e$

Thus $a^r = e$ and $r > 0$

∴ $o(a) \le r$

∴ $m \le r$

Impossible. ∵ o(a) = m

∴ r = 0

Hence by equation (1), n = mq. ∴ m |n i.e. o(a)|n

Conversely, Suppose that o(a)|n

∴ n = o (a)k, for some k ∈ ℕ

∴ $a^n = a^{o(a)k} = (a^{o(a)})^k = e^k = e$.

Hence proved.

==

Ex. In the group $(\mathbb{Z}'_7, \times_7)$, find (i) $(\bar{3})^2$ ii) $(\bar{4})^{-3}$ iii) $o(\bar{3})$ iv) $o(\bar{4})$

Sol. Let $\mathbb{Z}'_7 = \{\bar{1}, \bar{2}, \bar{3}, 4, \bar{5}, \bar{6}\}$ be a group under $\times_7$.

i) $(\bar{3})^2 = \bar{3} \times_7 \bar{3} = \bar{2}$.

ii) $(\bar{4})^{-3} = [(\bar{4})^{-1}]^3 = (\bar{2})^3 = \bar{2} \times_7 \bar{2} \times_7 \bar{2} = \bar{1}$. ∵ $(\bar{4})^{-1} = \bar{2}$

iii) Here $\bar{1} \in \mathbb{Z}'_7$ is an identity element.

Now $(\bar{3})^1 = \bar{3} \neq \bar{1}$, $(\bar{3})^2 = \bar{2} \neq \bar{1}$, $(\bar{3})^3 = \bar{6} \neq \bar{1}$, $(\bar{3})^4 = \bar{4} \neq \bar{1}$,

$(\bar{3})^5 = \bar{5} \neq \bar{1}$, $(\bar{3})^6 = \bar{1}$

∴ $o(\bar{3}) = 6$

iv) As $(\bar{4})^1 = \bar{4} \neq \bar{1}$, $(\bar{4})^2 = \bar{2} \neq \bar{1}$, $(\bar{4})^3 = \bar{1}$

$\therefore\ o(\bar{4}) = 3$

==

Ex. In the group $(\mathbb{Z}'_{11}, \times_{11})$, find (i) $(\bar{4})^3$ ii) $(\bar{5})^2$ iii) $o(\bar{9})$ iv) $o(\bar{7})$

Sol. Let $\mathbb{Z}'_{11} = \{\bar{1}, \bar{2}, \bar{3}, 4, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}\}$ be a group under $\times_{11}$

i) $(\bar{4})^3 = \bar{4} \times_{11} \bar{4} \times_{11} \bar{4} = \bar{9}$.

ii) $(\bar{5})^2 = \bar{5} \times_{11} \bar{5} = \bar{3}$.

iii) Here $\bar{1} \in \mathbb{Z}_{11}$ is an identity element.

Now $(\bar{9})^1 = \bar{9} \neq \bar{1}$, $(\bar{9})^2 = \bar{4} \neq \bar{1}$, $(\bar{9})^3 = \bar{3} \neq \bar{1}$,

$(\bar{9})^4 = \bar{5} \neq \bar{1}$, $(\bar{9})^5 = \bar{1}$.

$\therefore\ o(\bar{9}) = 5$

iv) As $(\bar{7})^1 = \bar{7} \neq \bar{1}$, $(\bar{7})^2 = \bar{5} \neq \bar{1}$, $(\bar{7})^3 = \bar{2} \neq \bar{1}$, $(\bar{7})^4 = \bar{3} \neq \bar{1}$, $(\bar{7})^5 = \overline{10} \neq \bar{1}$,

$(\bar{7})^6 = \bar{4} \neq \bar{1}$, $(\bar{7})^7 = \bar{6} \neq \bar{1}$, $(\bar{7})^8 = \bar{9} \neq \bar{1}$, $(\bar{7})^9 = \bar{8} \neq \bar{1}$, $(\bar{7})^{10} = \bar{1}$,

$\therefore\ o(\bar{7}) = 10$

==

Ex.: If in a group G, $a^5 = e$ and $aba^{-1} = b^2$, $\forall\ a, b \in G$, then find order of an element b.

Sol.: Let in a group G, $a^5 = e$ and $aba^{-1} = b^2$, $\forall\ a, b \in G$

As $b^2 = aba^{-1}$

$\therefore (b^2)^2 = (aba^{-1})(aba^{-1}) = ab(a^{-1}a)ba^{-1} = abeba^{-1} = ab^2a^{-1}$

$\therefore b^4 = a(aba^{-1})a^{-1} = a^2ba^{-2}$

$\therefore (b^4)^2 = (a^2ba^{-2})(a^2ba^{-2}) = a^2b^2a^{-2} = a^2(aba^{-1})a^{-2}$

$\therefore b^8 = a^3ba^{-3}$

$\therefore (b^8)^2 = (a^3ba^{-3})(a^3ba^{-3}) = a^3b^2a^{-3} = a^3(aba^{-1})a^{-3}$

$\therefore b^{16} = a^4ba^{-4}$

$\therefore (b^{16})^2 = (a^4ba^{-4})(a^4ba^{-4}) = a^4b^2a^{-4} = a^4(aba^{-1})a^{-4}$

$\therefore b^{32} = a^5ba^{-5} = ebe^{-1} = b$

$\therefore b^{31} = e$ by cancellation law.

$\therefore o(b) = 31$

==

UNIT-I-GROUP [MCQ'S]

==

1) Which of the following operations is not binary in $\mathbb{Z}$?

(A) addition (B) multiplication (C) subtraction (D)division

2) Let G be a non-empty set. If a*(b*c) = (a*b)*c for all a, b, c ∈ G, then a binary operation * on G is said to be ………..

(A) associative (B) closure (C) commutative (D) abelian.

3) What is the identity element in the group (Z, +)?

(A) 0 (B) 1 (C) -1 (D) 2

4) Consider the group ($\mathbb{Q}^+$, *) where a * b = $\frac{ab}{3}$ for all a, b ∈ $\mathbb{Q}^+$. What is the identity element in $\mathbb{Q}^+$?

(A) 0 (B) 1 (C) 2 (D) 3

5) Consider the group (Q^+, *) where a * b = $\frac{ab}{2}$ for all a, b ∈ Q^+. What is the inverse of an element a in Q^+ ?

(A) 2 (B) a (C) 4/a (D) a/2

6) Which of the following is not a group?

(A) ($\mathbb{Z}$, +) (B) ($\mathbb{N}$, +) (C) G = {1, -1, i, -i} under multiplication

(D) G = $\mathbb{R}$ – {1} under operation a*b = a + b - ab for all a, b ∈ G

7) Which of the following is incorrect?

(A) Identity element in a group is unique. (B) Every group is abelian.

(C) Inverse of every element in a group is unique. (D) None of the above.

8) In group G = {1, -1, i, -i} under usual multiplication i^{-1}=…..

(A) 1 (B) -1 (C) i (D) –i

9) In the group (Z_8', $\times_8$), $(\bar{3})^{-1}$= ……..

(A) $\bar{1}$ (B) $\bar{3}$ (C) $\bar{5}$ (D) $\bar{7}$

10) In a group G, for a ∈ G, $(a^{-1})^{-1}$= ……

(A) a (B) a^{-1} (C) e, identity in G (D) 1

11) Which of the following is an abelian group?

(A) G = $\mathbb{R}$ – {1} under operation a*b = a + b - ab for all a, b ∈ G

(B) G = {1, -1, i, -i, j, -j, k, -k} the group of quaternions under multiplication

(C) G = {A : A is a nonsingular matrix of order n over $\mathbb{R}$} under matrix mutl.

(D) G = {(a, b) : a, b ∈ $\mathbb{R}$, a ≠ 0 under operation (a, b)0(c, d) = (ac, bc+d) for all (a, b),(c, d) ∈ G

12) Which of the following is a non-abelian group?

(A) ($_2\mathbb{Z}$, +) (B) G = {1, -1, i, -i} under usual multiplication

(C) G = $\mathbb{Q}$ – {-1} under operation a*b = a + b + ab for all a, b ∈ G

(D) G = {(a, b) : a, b ∈ $\mathbb{R}$, a ≠ 0 under operation (a, b)0(c, d) = (ac, bc+d) for all (a, b),(c, d) ∈ G

13) Which of the following is a non-abelian group?

(A) ($\mathbb{R}$, +) (B) ($\mathbb{Z}_6$, $+_6$), (C) ($\mathbb{Z}_8'$, $+_8'$)

(D) G = { A : A is a nonsingular matrix of order n over $\mathbb{R}$} under matrix mult.

14) Which of the following groups is finite?

(A) $(\mathbb{Z}, +)$ (B) G = {1, -1, i, -i} under usual multiplication

(C) $G = \mathbb{Q} - \{-1\}$ under operation $a*b = a + b + ab$ for all $a, b \in G$

(D) $(\mathbb{Q}^+, *)$ under the operation $a * b = \frac{ab}{2}$ for all $a, b \in \mathbb{Q}^+$.

15) Which of the following groups is infinite?

(A) G = {1, -1, i, -i} under usual multiplication (B) $(\mathbb{Z}_6, +_6)$ (C) $(\mathbb{Z}_8', +_8')$

(D) $(\mathbb{Q}^+, *)$ under the operation $a * b = \frac{ab}{2}$ for all $a, b \in \mathbb{Q}^+$.

16) The number of elements present in a finite group G is …..

(A) order of group (B) order of element (C) index of group (D) None of above

17) The order of the group $(\mathbb{Z}_6, +_6)$ is……

(A) 2 (B) 3 (C) 5 (D) 6

18) In the group $(\mathbb{Z}, +)$, $(2)^4$ = …..

(A) 0 (B) 2 (C) 8 (D) 16

19) In the group $(\mathbb{Z}_6, +_6)$, $(\bar{3})^{-4}$ = …..

(A) $\bar{0}$ (B) $\bar{2}$ (C) $\bar{3}$ (D) $\bar{1}$

20) In the group $(\mathbb{Z}_8', +_8')$, $(\bar{5})^4$ = …..

(A) $\bar{1}$ (B) $\bar{3}$ (C) $\bar{5}$ (D) $\bar{7}$

21) In the group G = {1, -1, i, -i} under usual multiplication, order of i = …

(A) 1 (B) 2 (C) 3 (D) 4

22) Let G be a group and $a, b, c \in G$ Then $(abc)^{-1}$ =….

(A) $a^{-1}b^{-1}c^{-1}$ (B) $c^{-1}a^{-1}b^{-1}$ (C) $c^{-1}b^{-1}a^{-1}$ (D) $a^{-1}c^{-1}b^{-1}$

23) Let G be a group and $a, b \in G$ such that ab = ba. Which of the following is incorrect?

(A) $a^kb = ba^k$ for all $k \in \mathbb{N}$. (B) $(ab)^n = a^nb^n$ for all $n \in \mathbb{N}$.

(C) $(ab)^{-1} = a^{-1}b^{-1}$ (D) None of the above

24) A group G is called as … if the number of element in G is finite.

(A) abelian (B) finite (C) infinite (D) non-abelian

25) An abelian group is also known as …. group.

(A) finite (B) infinite (C) commutative (D) ordered

26) In any group G, $o(a^{-1})$ =……..

(A) o(a) (B) o(G) (C) 1/o(a) (D) 1/o(G)

27) In the group $(\mathbb{Z}, +)$, o(2) =…..

(A) 0 (B) 1 (C) 2 (D) infinite

28) How many elements in the group $(\mathbb{Z}, +)$ has finite order?

(A) 1 (B) 2 (C) 3 (D) infinite

29) If G is a group and $a \in G$, $m, n \in \mathbb{N}$ then $a^m a^n = \ldots.$

(A) a^{mn} (B) a^{m+n} (C) $a^{m/n}$ (D) $a^{(m, n)}$

30) Order of the identity element in any group is ….

(A) 0 (B) 1 (C) 2 (D) o(G)

31) Let G be a group and $a, b \in G$, $m \in \mathbb{N}$. Then $(b^{-1}ab)^m = \ldots..$

(A) $b^{-1}a^m b$ (B) $b^{-m}ab^m$ (C) $b^{-1}ab$ (D) e

==

UNIT-2: SUBGROUPS

==

Subgroup: Let (G, *) be a group. A non-empty subset H of G is said to be a subgroup of G if (H, *) itself forms a group. Denoted by $H \leq G$.

Note:

1) {e} is a subgroup of group G and is called a trivial subgroup G.
2) G is a subgroup of group G and is called an improper subgroup of G.
3) A subgroup H of group G is called a proper subgroup of G if $H \neq G$.
4) If H is a subgroup of group G and K is a subgroup of H then K is a subgroup of group G.
5) If a is an element of G, then $< a > = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of

e.g.1) $_3\mathbb{Z} = \{3n : n \in \mathbb{N}\}$ is a subgroup of $(\mathbb{Z}, +)$.

2) $(\mathbb{Q}^+, \times)$ is a subgroup of $(\mathbb{R} - \{0\}, \times)$

==

Theorem: A non-empty subset H of a group G is subgroup of G if and only if $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof: Suppose H is a subgroup of group G.

∴ H itself forms group.

∴ For $a, b \in H \Rightarrow a, b^{-1} \in H$ by existence of inverse

$\Rightarrow ab^{-1} \in H$ by closure property

Conversely, Suppose $a, b \in H \Rightarrow ab^{-1} \in H$.

We have to prove H itself forms a group.

i) Existence of Identity: As H is a non-empty subset H of G.

∴ $a \in H \Rightarrow a, a \in H \Rightarrow aa^{-1} = e \in H$

ii) Existence of Inverse: Let $a \in H \Rightarrow e, a \in H \Rightarrow ea^{-1} = a^{-1} \in H$

iii) Closure Property: Let $a, b \in H \Rightarrow a, b^{-1} \in H$

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

$\Rightarrow ab \in H$

iv) Associative law: Let $a, b, c \in H \Rightarrow a, b, c \in G$ ∵ $H \subseteq G$.

∴ $(ab)c = a(bc)$

From (i) to (iv), H itself forms a group.

∴ H is a subgroup of group G.

==

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

Proof: Suppose H is a subgroup of group G.

∴ H itself forms group.

∴ i) For $a, b \in H \Rightarrow ab \in H$ by closure property

ii) $a \in H \Rightarrow a^{-1} \in H$ by existence of inverse

Conversely, Suppose i) $a, b \in H \Rightarrow ab \in H$.

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

Now for $a \in H \Rightarrow a^{-1} \in H$ by (ii)

$\therefore$ $a, a^{-1} \in H \Rightarrow aa^{-1} \in H$ by (i)

$\Rightarrow e \in H$

i.e. identity element exist in H.

Again for $a, b, c \in H \Rightarrow a, b, c \in G \because H \subseteq G$.

$\therefore (ab)c = a(bc)$

i.e. associative law hold in H.

$\therefore$ H itself forms group.

$\therefore$ H is a subgroup of group G.

==

Theorem: A non-empty subset H of G is subgroup of a finite group (G, *) if and only if $a, b \in H \Rightarrow a*b \in H$

Proof: Suppose H is a subgroup of a finite group (G, *)

$\therefore$ (H, *) itself forms group.

$\therefore$ For $a, b \in H \Rightarrow a*b \in H$ by closure property

Conversely, Suppose $a, b \in H \Rightarrow a*b \in H$ …..(i)

Let G be a finite group say with n elements and $a \in H$

$\therefore$ There exists a positive integer m such that $a^m = e$, where $1 \le m \le n$

Now $a \in H \Rightarrow a^2 = a*a \in H$ by (i)

Again $a, a^2 \in H \Rightarrow a^3 = a*a^2 \in H$

In general $a^m \in H \Rightarrow e \in H$

i.e. identity element exist in H.

Now $e = a^m = a*a^{m-1} = a^{m-1}*a$.

$\therefore a^{-1} = a^{m-1} \in H$

i. e. every element has inverse in H.

Again for $a, b, c \in H \Rightarrow a, b, c \in G \because H \subseteq G$

$(a * b) * c = a * (b * c)$

i.e. associative law hold in H.

$\therefore$ (H, *) itself forms group.

$\therefore$ (H, *) is a subgroup of a finite group (G, *).

==

Theorem: Intersection of two subgroups of a group is a subgroup.

Proof: Suppose H and K be any two subgroups of a group G.

As $e \in H$ and $e \in K \Rightarrow e \in H \cap K$

$\therefore H \cap K \neq \emptyset$ i.e. $H \cap K$ is a non empty subset of G.

Now $a, b \in H \cap K \Rightarrow a, b \in H$ & $a, b \in K$

$\Rightarrow ab^{-1} \in H$ & $ab^{-1} \in K \because$ H & K are subgroups of G

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

Hence $H \cap K$ is a subgroup of a group G.

Remark: 1) Intersection of finite number of subgroups of a group is a subgroup.

2) Union of two subgroups may not be a subgroup.

e.g. Let $_2\mathbb{Z}$ & $_3\mathbb{Z}$ are subgroups of a group $(\mathbb{Z}, +)$ but $(_2\mathbb{Z} \cup {_3\mathbb{Z}}, +)$ is not a subgroup of a group $(\mathbb{Z}, +)$ $\because$ $2, 3 \in {_2\mathbb{Z}} \cup {_3\mathbb{Z}}$ but $2 + 3 = 5 \notin {_2\mathbb{Z}} \cup {_3\mathbb{Z}}$.

==

Theorem: Let H & K be any two subgroups of a group G. Then $H \cup K$ is a subgroup of group G if and only if either $H \subseteq K$ or $K \subseteq H$.

Proof: Suppose $H \cup K$ is a subgroup of group G. To prove either $H \subseteq K$ or $K \subseteq H$.

Let if possible $H \nsubseteq K$ and $K \nsubseteq H$.

$\therefore$ there exist some $b \in H$ but $b \notin K$ and $a \in K$ but $a \notin H$.

Now $b \in H \subseteq H \cup K$ and $a \in K \subseteq H \cup K$

$\Rightarrow a, b \in H \cup K$

$\Rightarrow ab^{-1} \in H \cup K$ $\because$ $H \cup K$ is a subgroup.

$\Rightarrow ab^{-1} \in H$ and/or $ab^{-1} \in K$

If $ab^{-1} \in H$ then $(ab^{-1})b \in H$ $\because$ $b \in H$ and H is a subgroup.

$\therefore a(b^{-1}b) \in H \Rightarrow ae \in H \Rightarrow a \in H$ which contradicts to $a \notin H$.

Similarly if $ab^{-1} \in K \Rightarrow b \in K$ which contradicts to $b \notin K$.

$\therefore$ Our supposition is wrong.

Hence either $H \subseteq K$ or $K \subseteq H$.

Conversely : Suppose either $H \subseteq K$ or $K \subseteq H$.

$\therefore H \cup K = K$ or $H \cup K = H$

$\therefore H \cup K$ is a subgroup of group G. $\because$ H and K are subgroups of a group G.

==

Ex. Determine whether $H_1=\{\bar{0}, \bar{4}, \bar{8}\}$ and $H_2=\{\bar{0}, \bar{5}, \overline{10}\}$ are subgroups is a group $(\mathbb{Z}_{12}, +_{12})$

Sol. We prepare composition table for $H_1=\{\bar{0}, \bar{4}, \bar{8}\}$ and $H_2=\{\bar{0}, \bar{5}, \overline{10}\}$ with operation $+_{12}$

$+_{12}$	$\bar{0}$	$\bar{4}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{4}$	$\bar{8}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{0}$
$\bar{8}$	$\bar{8}$	$\bar{0}$	$\bar{4}$

$+_{12}$	$\bar{0}$	$\bar{5}$	$\overline{10}$
$\bar{0}$	$\bar{0}$	$\bar{5}$	$\overline{10}$
$\bar{5}$	$\bar{5}$	$\overline{10}$	$\bar{3}$
$\overline{10}$	$\overline{10}$	$\bar{3}$	$\bar{8}$

As H_1 and H_2 are non-empty subsets of a finite group $(\mathbb{Z}_{12}, +_{12})$. We observe that $+_{12}$ is closed in H_1 but not in H_2.

$\therefore$ H_1 is a subgroup of a group $(\mathbb{Z}_{12}, +_{12})$ but H_2 is not a subgroup of a group $(\mathbb{Z}_{12}, +_{12})$.

==

Normalizer: Let G be a group and $a \in G$. Then $N(a) = \{x \in G : xa = ax\}$ is called a normalize of an element a of G.

Center of a Group: Let G be a group. Then $Z(G) = \{x \in G : xa = ax \ \forall \ a \in G\}$ is called a center of a group G.

==

Ex: Let G be a group and $a \in G$. Then show that $N(a) = \{x \in G : xa = ax\}$ is a subgroup of G.

Proof: Let $N(a) = \{x \in G : xa = ax\}$

For $e \in G$, $ea = ae \Rightarrow e \in N(a)$

$\therefore$ N(a) is a non empty subset of G.

For $x, y \in N(a) \Rightarrow xa = ax$ and $ya = ay$ where $x, y \in G$.

As G is a group. $\therefore x, y \in G \Rightarrow x, y^{-1} \in G \Rightarrow xy^{-1} \in G$

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

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

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

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

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

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

Hence N(a) is a subgroup of group G is proved

==

Ex: Let G be a group. Then show that $Z(G) = \{x \in G : xa = ax \ \forall \ a \in G\}$ is a subgroup of G.

Proof: Let $Z(G) = \{x \in G : xa = ax \ \forall \ a \in G\}$

For $e \in G$, $ea = ae \ \forall \ a \in G \Rightarrow e \in Z(G)$

$\therefore$ Z(G) is a non empty subset of G.

For $x, y \in Z(G) \Rightarrow xa = ax$ and $ya = ay \ \forall \ a \in G$ where $x, y \in G$.

As G is a group. $\therefore x, y \in G \Rightarrow x, y^{-1} \in G \Rightarrow xy^{-1} \in G$

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

$= x(ay^{-1}) \quad \because \ ya = ay \Rightarrow y^{-1}a = ay^{-1} \ \forall \ a \in G$

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

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

$= a(xy^{-1}) \quad \forall \ a \in G$

$\therefore xy^{-1} \in Z(G) \quad \forall \ a \in G$

Hence Z(G) is a subgroup of group G is proved

==

Ex: Let H be a subgroup of a group G and $a \in G$. Then show that $H_a = \{x \in G : xa^{-1} \in H\}$.

Proof: Let us denote $A = \{x \in G : xa^{-1} \in H\}$

Now $x \in A \Leftrightarrow xa^{-1} \in H$
$\Leftrightarrow xa^{-1} = h$, for some $h \in H$
$\Leftrightarrow x = ha$
$\Leftrightarrow x \in H_a$
$\therefore H_a = A$ i.e. $H_a = \{x \in G : xa^{-1} \in H\}$
Hence proved.

==

Ex: Let G be a group of all non-zero complex numbers under multiplication. Show that $H = \{a + ib : a^2 + b^2 = 1\}$ is a subgroup of G.

Proof: Let G be a group of all non-zero complex numbers under multiplication and $H = \{a + ib : a^2 + b^2 = 1\}$

As $1 = 1 + i0$ is non-zero complex number with $1^2 + 0^2 = 1$

$\therefore 1 \in H$ i.e. H is a non empty subset of G.

For $a + ib$ and $c + id \in H \Longrightarrow a^2 + b^2 = 1$ and $c^2 + d^2 = 1$ ………(1)

Consider $(a + ib)(c + id)^{-1} = \frac{a+ib}{c+id} \times \frac{c-id}{c-id}$

$= \frac{(ac+bd)+i(bc-ad)}{c^2+d^2}$

$= (ac + bd) + i(bc - ad)$ by (1)

Where $(ac+bd)^2 + (bc-ad)^2 = a^2c^2+2acbd+b^2d^2+b^2c^2-2bcad+a^2d^2$

$= a^2(c^2 + d^2) + b^2(c^2 + d^2)$

$= (c^2 + d^2)(a^2 + b^2)$

$= 1$ by (1).

$\therefore (a + ib)(c + id)^{-1} \in H$.

Hence H is a subgroup of group G is proved.

==

Cyclic Group: A group G is said to be cyclic group if there exists an element $a \in G$ such that every element of G is expressed in some integral powers of a.

Note: Here an element a is called generator of G and cyclic group G is denoted by

$G = \langle a \rangle$ or $(a) = \{a^n : n \in \mathbb{Z}\}$.

e. g. 1) $(\mathbb{Z}, +)$ is a cyclic group generated by 1.

2) $(n\mathbb{Z}, +)$ is a cyclic group generated by n.

3) $(\mathbb{Z}_n, +_n)$ is a cyclic group generated by $\overline{1}$.

4) A group $G = \{1, -1, i, -i\}$ under multiplication is a cyclic group generated by i.

==

Theorem: Every cyclic group is abelian.

Proof: Let G be any cyclic group G generated by 'a'.

$\therefore$ For $x, y \in G \Longrightarrow x = a^r$ and $y = a^t$ for some $r, t \in \mathbb{Z}$.

$\therefore xy = a^r a^t = a^{r+t} = a^{t+s} = a^t a^r = yx$

$\therefore$ G is an abelian group. Hence Proved.

Note : i) If $(m, n) = 1$ then $\overline{m}$ is generator of group $(\mathbb{Z}_n, +_n)$.

ii) If $G = \langle a \rangle$ with $o(G) = n$ and $(m, n) = 1$ then $G = \langle a^m \rangle$ for $0 < m < n$.

iii) Every abelian group may not be cyclic.

e.g. ($\mathbb{Z}'_8=\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}, \times_8$) is an abelian group but not cyclic because $(\bar{1})^n = \bar{1}\ \forall\ n \in \mathbb{Z}$, $(\bar{3})^n$ = either $\bar{3}$ *or* $\bar{1}\ \forall\ n \in \mathbb{Z}$, $(\bar{5})^n$ = either $\bar{5}$ *or* $\bar{1}\ \forall\ n \in \mathbb{Z}$ & $(\bar{7})^n$ = either $\bar{7}$ *or* $\bar{1}\ \forall\ n \in \mathbb{Z}$

$\therefore\ \bar{1}, \bar{3}, \bar{5}$ & $\bar{7}$ are not generators of $\mathbb{Z}'_8$

==

Theorem: If G is a cyclic group generated by a then a^{-1} is also generates G.

Proof: Let G be any cyclic group generated by 'a'.

Hence $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

As $a^{-1} \in \langle a^{-1} \rangle \Rightarrow a^{-1} \in G \Rightarrow \langle a^{-1} \rangle \subseteq G$ ……(1)

For $y \in G = \langle a \rangle \Rightarrow y = a^r$ for some $r \in \mathbb{Z}$.

$\therefore y = ((a^{-1})^{-1})^r = (a^{-1})^{-r} \in \langle a^{-1} \rangle$

$\therefore G \subseteq \langle a^{-1} \rangle$ ……(2)

From (1) and (2), $G = \langle a^{-1} \rangle$

$\therefore a^{-1}$ is also generates G is proved.

==

Ex: If G is be a group and $a \in G$. Then prove that $H = \{a^n : n \in \mathbb{Z}\}$ is the smallest subgroup of G containing a.

Proof: i) As $a = a^1 \in H\ \therefore H \neq \emptyset$.

$\therefore$ For $x, y \in H \Rightarrow x = a^r$ and $y = a^t$ for some $r, t \in \mathbb{Z}$.

$\therefore xy^{-1} = a^r (a^t)^{-1} = a^r a^{-t} = a^{r-t} \in H$

$\therefore$ H is a subgroup of group G.

ii) Let K be any subgroup of group G containing a.

We have to prove $H \subseteq K$.

Let $x \in H \Rightarrow x = a^r$ for some $r \in \mathbb{Z}$.

$\Rightarrow x = a^r \in K\ \because a \in K$ and K is a subgroup.

$\therefore\ H \subseteq K$. Hence H is the smallest subgroup of G containing a is proved.

==

Ex: Show that every subgroup of a cyclic group is cyclic.

Proof: Let G be any cyclic group generated by a.

$\therefore G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$

Let H be a subgroup of G.

If H = {e} then $H = \langle e \rangle$ and hence H is cyclic.

Suppose $H \neq \{e\}$.

Let $x \in H$ be such that $x \neq e$.

Now $x \in G \Rightarrow x = a^p$ for some $p \in \mathbb{Z}, p \neq 0$.

$\therefore x^{-1} = (a^p)^{-1} = a^{-p}$

Since either p or –p is positive $\Rightarrow$H contain at least one element a^n such that $n \in N$.

Let t be the least positive integer such that $a^t \in H$.

Claim $H = \langle a^t \rangle$

As $a^t \in \langle a^t \rangle \Rightarrow a^t \in H \Rightarrow \langle a^t \rangle \subseteq H$…..(1).

Let $y \in H \Rightarrow y \in G = \langle a \rangle$

$\therefore y = a^m$ for some $m \in \mathbb{Z}$.

By division algorithm, there exist integers q, r such that

$m = qt + r$, where $0 \le r < t$ ………(2)

If $r \neq 0$ then $a^r = a^{m-qt} = a^m a^{-qt} = a^m (a^t)^{-q} \in H \because y = a^m \in H$ and $a^t \in H$

$\therefore t \le r$ by choice of t. Which contradicts to $r < t$.

Hence r = 0.

$\therefore$ by (2) m = qt

$\therefore y = a^m = a^{qt} = (a^t)^q \in \langle a^t \rangle$

Hence $H \subseteq \langle a^t \rangle$……(3)

From (1) and (3) $H = \langle a^t \rangle$.

Hence H is a cyclic is proved.

==

Dihedral Group: Let $G = \{x^i y^j : i = 0,1; j = 0, 1, 2, \ldots, n-1, x^2 = e = y^n, xy = y^{-1}x\}$, then group G is called dihedral group for $n \ge 3$.

Note:i) Dihedral group G is also written as

$G = \{y, y^2, y^3, \ldots, y^{n-1}, y^n = e = x^2, x, xy, xy^2, \ldots, xy^{n-1}, xy = y^{-1}x\}$

ii) We write $G = D_{2n}$ since $o(G) = 2n$.

==

Ex. Find composition table for n = 3 i.e. $G = D_6 = \{e = x^2 = y^3, x, y, y^2, xy, xy^2\}$.

Sol.: Let for n = 3, $G = \{e = x^2 = y^n, x, y, y^2, xy, xy^2\} = D_6$

As in dihedral group $xy = y^{-1}x$.

$\therefore$ i) $y(xy) = y(y^{-1}x) = (yy^{-1})x = x$.

ii) $yx = (yx)e = (yx)y^3 = (yxy)y^2 = xy^2$

iii) $y(xy^2) = (yx)y^2 = (xy^2)y^2 = (xy)y^3 = xy$

iv) $y^2x = y(yx) = y(xy^2) = (yxy)y = xy$, etc.

Using this we get, composition table for the elements of G is

.	e	x	Y	y^2	xy	xy^2
E	e	x	Y	y^2	xy	xy^2
X	x	e	Xy	xy^2	y	y^2
Y	y	xy^2	y^2	e	x	Xy
y^2	y^2	xy	E	y	xy^2	X
xy	xy	y^2	xy^2	x	e	Y
xy^2	xy^2	y	X	xy	y^2	E

We observe that G is finite non-abelian group with $o(G) = o(D_6) = 6$.

==

Right coset: Let H be a subgroup of a group G and $a \in G$. Then the set $H_a = \{ha : h \in H\}$ is called right coset of H by a in G.

Left coset: Let H be a subgroup of a group G and $a \in G$. Then the set ${}_aH = \{ah : h \in H\}$ is called left coset of H by a in G.

Note: Let H be a subgroup of a group G and a, b ∈ G. Then $(H_a)_b$= {(ha)b: h ∈ H}, & $_a(_bH)$= {a(bh): h ∈ H}.

==

Ex. Let G = {1, -1, i, -i} be a group under multiplication and H = {1, -1} be its subgroup. Then find all right and left cosets of H in G.

Sol.: Let G = {1, -1, i, -i} be a group under multiplication and H = {1, -1} be its subgroup.

i) All right cosets of H in G are as follows

H_1= {h1: h ∈ H}= {1.1, (-1).1} = {1, -1} = H

H_{-1}= {h(-1): h ∈ H}= {1.(-1), (-1).(-1)} = {-1, 1} = H

H_i= {hi: h ∈ H}= {1.i, (-1).i} = {i, -i}

H_{-i}= {h(-i): h ∈ H}= {1.(-i), (-1).(-i)} = {-i, i}

i.e. {1, -1} & {i, -i} are the right cosets of H in G.

ii) All left cosets of H in G are as follows

$_1H$= {1h: h ∈ H}= {1.1, 1.(-1)} = {1, -1} = H

$_{-1}H$= {(-1)h: h ∈ H}= {(-1).1, (-1).(-1)} = {-1, 1} = H

$_iH$= {ih: h ∈ H}= {i.1, i.(-1)} = {i, -i}

$_{-i}H$= {(-i)h: h ∈ H}= {(-i).1, (-i).(-1)} = {-i, i}

i.e. {1, -1} & {i, -i} are the leftt cosets of H in G.

==

Ex. Let G = {1, -1, i, -i, j, -j, k, -k} be a group under multiplication and H = {1, -1, i, -i} be its subgroup. Find all the left and right cosets of H in G.

Sol.: Let G = {1, -1, i, -i, j, -j, k, -k} be a group under multiplication and H = {1, -1, i, -i} be its subgroup. Here we use i.j = k, j.k = i and k.i = j

i) All the left cosets of H in G are as follows

$_1H$= {1h: h ∈ H}= {1.1, 1.(-1), 1.i, 1.(-i)} = {1, -1, i, -i} = H

$_{-1}H$= {(-1)h: h ∈ H}= {(-1).1, (-1).(-1), (-1).i, (-1).(-i)} = {-1, 1, -i, i} = H

$_iH$= {ih: h ∈ H}= {i.1, i.(-1), i.i, i.(-i)} = {i, -i, -1, 1} = H

$_{-i}H$= {(-i)h: h ∈ H}= {(-i).1, (-i).(-1), (-i).i, (-i).(-i)} = {-i, i, 1, -1} = H

$_jH$= {jh: h ∈ H}= {j.1, j.(-1), j.i, j.(-i)} = {j, -j, -k, k}

$_{-j}H$= {(-j)h: h ∈ H}= {(-j).1, (-j).(-1), (-j).i, (-j).(-i)} = {-j, j, k, -k}

$_kH$= {kh: h ∈ H}= {k.1, k.(-1), k.i, k.(-i)} = {k, -k, j, -j}

$_{-k}H$= {(-k)h: h ∈ H}= {(-k).1, (-k).(-1), (-k).i, (-k).(-i)} = {-k, k, -j, j}

i.e. {1, -1, i, -i} & {j, -j, k, -k} are the leftt cosets of H in G.

Similarly all the right cosets of H in G are {1, -1, i, -i} & {j, -j, k, -k}.

==

Theorem: Let G be a group and H a subgroup of G. Then

i) $H_e = H = {}_eH$

ii) $(H_a)_b = H_{(ab)}$ and $_a(_bH) = {}_{(ab)}H$

iii) If G is abelian then $H_a = {}_aH$, ∀ a ∈ G

Proof : i) $H_e = \{he: h \in H\} = \{h: h \in H\} = H$

and $_eH = \{eh: h \in H\} = \{h: h \in H\} = H$

$\therefore H_e = H = {}_eH$

ii) $(H_a)_b = \{(ha)b: h \in H\}$

$= \{h(ab): h \in H\}$ by associative law.

$= H_{(ab)}$

Similarly $_a(_bH) = {}_{(ab)}H$

iii) Let G be an abelian group and $a \in G$

$\therefore H_a = \{ha: h \in H\}$

$= \{ah: h \in H\}$ $\because$ G is abelian.

$= {}_aH$

Hence proved.

==

Theorem: Let H be a subgroup of a group G. Then

i) $a \in H \Leftrightarrow H_a = H$

ii) $H_a = H_b \Leftrightarrow$ and $ab^{-1} \in H$

Proof : i) Suppose $a \in H$. Let $x \in H_a$

$\therefore x = ha$, for some $h \in H$

As $h, a \in H \Rightarrow ha \in H \Rightarrow x \in H$

$\therefore H_a \subseteq H$ ....(1)

Let $y \in H$

$\therefore y = ye = y(a^{-1}a) = (ya^{-1})a \in H_a$ $\because$ y, a $\in$ H and H is a subgroup.

$\therefore H \subseteq H_a$ ....(2)

From (1) and (2) $H = H_a$

Conversely, suppose $H = H_a$

Now $a = ea \in H_a = H$ i.e. $a \in H$.

Hence proved.

ii) $H_a = H_b \Leftrightarrow (H_a)_{b^{-1}} = (H_b)_{b^{-1}}$

$\Leftrightarrow H_{(ab^{-1})} = H_{(bb^{-1})}$

$\Leftrightarrow H_{(ab^{-1})} = H_e$

$\Leftrightarrow H_{(ab^{-1})} = H$

$\Leftrightarrow ab^{-1} \in H$ by (i)

Hence proved.

==

Theorem: Let H be a subgroup of a group G. Then

i) $a \in H \Leftrightarrow {}_aH = H$

ii) $_aH = {}_bH \Leftrightarrow$ and $b^{-1}a \in H$

Proof : i) Suppose $a \in H$. Let $x \in {}_aH$

$\therefore x = ah$, for some $h \in H$

As $a, h \in H \Rightarrow ah \in H \Rightarrow x \in H$

$\therefore {}_aH \subseteq H$ ....(1)

Let $y \in H$

$\therefore y = ey = (aa^{-1})y = a(a^{-1}y) \in {}_aH$ $\quad \because a, y \in H$ and H is a subgroup.

$\therefore H \subseteq {}_aH$ ....(2)

From (1) and (2) $H = {}_aH$

Conversely, suppose $H = {}_aH$

Now $a = ae \in {}_aH = H$ i.e. $a \in H$.

Hence proved.

ii) ${}_aH = {}_bH \Leftrightarrow {}_{b^{-1}}({}_aH) = {}_{b^{-1}}({}_bH)$

$\Leftrightarrow {}_{(b^{-1}a)}H = {}_{(b^{-1}b)}H$

$\Leftrightarrow {}_{(b^{-1}a)}H = {}_eH$

$\Leftrightarrow {}_{(b^{-1}a)}H = H$

$\Leftrightarrow b^{-1}a \in H$ by (i)

Hence proved.

==

Theorem: Let H be a subgroup of a group G. Then

i) Any two right cosets of H are either disjoint or identical.

ii) Any two left cosets of H are either disjoint or identical.

Proof : i) Let H_a and H_b be any two right cosets of H in G.

We have to prove either $H_a \cap H_b = \emptyset$ or $H_a = H_b$.

If $H_a \cap H_b = \emptyset$ then we are trough.

But if $H_a \cap H_b \neq \emptyset$ then there exist some $x \in H_a \cap H_b$

$\therefore x \in H_a$ and $x \in H_b$

$\therefore x = ha$ and $x = kb$ for some $h, k \in H$

$\therefore ha = kb$ for some $h, k \in H$

$\therefore a = h^{-1}kb$ for some $h, k \in H$ ....(1)

$\therefore H_a = H_{(h^{-1}kb)}$ by (1)

$\therefore Ha = (H_{(h^{-1}k)})_b$

$\therefore Ha = H_b$ $\quad \because h, k \in H$ and H is a subgroup $\Rightarrow h^{-1}k \in H \Rightarrow H_{(h^{-1}k)} = H$

Hence any two right cosets of H are either disjoint or identical is proved.

i) Let ${}_aH$ and ${}_bH$ be any two left cosets of H in G.

We have to prove either ${}_aH \cap {}_bH = \emptyset$ or ${}_aH = {}_bH$.

If ${}_aH \cap {}_bH = \emptyset$ then we are trough.

But if ${}_aH \cap {}_bH \neq \emptyset$ then there exist some $x \in {}_aH \cap {}_bH$

$\therefore x \in {}_aH$ and $x \in {}_bH$

$\therefore x = ah$ and $x = bk$ for some $h, k \in H$

$\therefore ah = bk$ for some $h, k \in H$

$\therefore a = bkh^{-1}$ for some $h, k \in H$ ....(1)

∴ ${}_aH = {}_{(bkh^{-1})}H$ by (1)

∴ ${}_aH = {}_b({}_{(kh^{-1})}H)$

∴ ${}_aH = {}_bH$ ∵ h, k ∈ H and H is a subgroup ⟹ $kh^{-1} \in H$ ⟹ ${}_{(kh^{-1})}H = H$

Hence any two left cosets of H are either disjoint or identical is proved.

==

Lagranges Theorem: If H is a subgroup of a finite group G then o(H) | o(G).

Proof : Let H be a subgroup of a finite group G.

If H = {e} or H = G then o(H) | o(G).

So suppose $\{e\} \subset H \subset G$ i.e. 1 < o(H) < o(G).

Let $a_1 \in G$ be such that $a_1 \notin H$.

∴ $a_1 \neq e$ ∵ $e \in H$.

Let o(H) = m and H = $\{e, h_2, h_3, \ldots\ldots\ldots h_m\}$

Consider the right coset $Ha_1 = \{a_1, h_2a_1, h_3a_1, \ldots\ldots\ldots h_ma_1\}$

∴ $a_1 \in Ha_1$ but $a_1 \notin H = He$

∴ $Ha_1 \neq H$

∴ $H \cap Ha_1 = \emptyset$

We observe that Ha_1 contain m distinct elements ∵ $h_i \neq h_j \Longrightarrow h_ia_1 \neq h_ja_1$ for all i, j.

∴ $H \cup Ha_1$ contain exactly 2m elements.

If $H \cup Ha_1 = G$ then o(G) = 2m = 2.o(H).

∴ o(H) | o(G)

If $H \cup Ha_1 \neq G$ then there exists $a_2 \in G$ be such that $a_2 \notin H \cup Ha_1$.

∴ $a_2 \neq e$ ∵ $e \in H \cup Ha_1$

Consider the right coset $Ha_2 = \{a_2, h_2a_2, h_3a_2, \ldots\ldots\ldots h_ma_2\}$

∴ $a_2 \in Ha_2$ but $a_2 \notin H \cup Ha_1$ i.e. $a_2 \notin H = He$ and $a_2 \notin Ha_1$

∴ He, Ha_1 and Ha_2 are pair wise disjoint.

Also Ha_2 contain m distinct elements.

∴ $H \cup Ha_1 \cup Ha_2$ contain exactly 3m elements.

If $H \cup Ha_1 \cup Ha_2 = G$ then o(G) = 3m = 3.o(H).

∴ o(H) | o(G)

Otherwise we continue the above process. As G is finite, process must stop after a finite number of steps. Suppose that we have k pair-wise disjoint right cosets say

$H, Ha_1, Ha_2, \ldots\ldots\ldots\ldots Ha_{k-1}$ such that $H \cup Ha_1 \cup Ha_2 \cup \ldots\ldots\ldots \cup Ha_{k-1} = G$

∴ o(G) = km = k.o(H)

∴ o(H) | o(G)

==

Ex. Show that every group of prime order is cyclic and hence abelian.

Proof: Let G be a group of prime order p.

∴ There exist $a \in G$ such that $a \neq e$ ∵ p is prime.

Consider a cyclic subgroup H = < a >.

∴ o(H) > 1 ∵ $a \in H$ and $a \neq e$.

By Lagrange's theorem, o(H) | o(G).

∴ o(H) | p

∴ o(H) = 1 or p ∵ p is prime

∴ o(H) = p ∵ o(H) > 1.

∴ o(H) = o(G)

∴ G = H = < a >

Hence G is a cyclic group.

As every cyclic group is abelian.

∴ G is an abelian group is proved.

==

Ex. Show that order of every element of a finite group is a divisor of order of a group.

Proof: Let G be a finite group and a ∈ G.

∴ o(a) is finite say m. ∵ order of an element of a finite group is finite.

∴ $a^m = e$

∴ < a > = { e, a, a^2, ……. a^{m-1} } i.e. o(< a >) = m

By Lagrange's theorem, o(< a >) | o(G).

∴ m | o(G)

∴ o(a) | o(G)

Hence proved.

==

Ex. If a is an element of a finite group G, then show that $a^{o(G)} = e$

Proof: Let G be a finite group and a ∈ G.

∴ o(a) | o(G)

∴ o(G) = o(a).r, for some r ∈ N.

∴ $a^{o(G)} = a^{o(a).r} = (a^{o(a)})^r = e^r = e$

Hence proved.

==

Euler's Theorem: If an integer a is relatively prime to a natural number n then $a^{\emptyset(n)} \equiv 1 \pmod{n}$, where ∅(n) being the Euler's totient function.

Proof: Consider $\mathbb{Z}_n' = \{\bar{a} : (a, n) = 1\}$, the group of prime residue classes modulo n.

Let (a, n) = 1

∴ $\bar{a} \in \mathbb{Z}_n'$

∴ $\bar{a}^{\emptyset(n)} = \bar{1}$ ∵ $o(\mathbb{Z}_n') = \emptyset(n)$ and $\bar{1} \in \mathbb{Z}_n'$ is an identity element.

∴ $\overline{a^{\emptyset(n)}} = \bar{1}$

∴ $a^{\emptyset(n)} \equiv 1 \pmod{n}$

Hence proved.

==

Fermat's Theorem: If p is prime number and a is an integer such that p ∤ a then $a^{p-1} \equiv 1 \pmod{n}$.

Proof: Let p is a prime number and a ∈ ℤ such that p ∤ a.

Let (a, p) = 1

∴ By Euler's theorem

$\therefore a^{\phi(p)} \equiv 1 (\text{mod } p)$

$\therefore a^{p-1} \equiv 1 (\text{mod } p)$ $\quad \because \phi(p) = p - 1$ if p is prime.

Hence proved.

===

Ex. Find all subgroups of $(\mathbb{Z}_{12}, +_{12})$.

Sol. : We know that for any group G, if $a \in G$ then $< a > = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

Let $\mathbb{Z}_{12} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11} \}$

i) $< \bar{0} > = \{\bar{0}^n : n \in \mathbb{Z}\} = \{ \bar{0} \}$

ii) $< \bar{1} > = \{\bar{1}^n : n \in \mathbb{Z}\} = \{n\bar{1} : n \in \mathbb{Z}\}$

$= \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11} \}$

$< \bar{1} > = < \bar{5} > = < \bar{7} > = < \overline{11} > = \mathbb{Z}_{12}$ $\because (1, 12)=(5, 12)=(7, 12)=(11, 12)= 1$

iii) $< \bar{2} > = \{\bar{2}^n : n \in \mathbb{Z}\} = \{ \bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\} = < \overline{10} >$ $\quad \because \bar{2}^{-1} = \overline{10}$

iv) $< \bar{3} > = \{\bar{3}^n : n \in \mathbb{Z}\} = \{ \bar{0}, \bar{3}, \bar{6}, \bar{9}\} = < \bar{9} >$ $\quad \because \bar{3}^{-1} = \bar{9}$

v) $< \bar{4} > = \{\bar{4}^n : n \in \mathbb{Z}\} = \{ \bar{0}, \bar{4}, \bar{8}\} = < \bar{8} >$ $\because \bar{4}^{-1} = \bar{8}$

vi) $< \bar{6} > = \{\bar{6}^n : n \in \mathbb{Z}\} = \{ \bar{0}, \bar{6}\}$

Thus $\{ \bar{0} \}, \{ \bar{0}, \bar{6}\}, \{ \bar{0}, \bar{4}, \bar{8}\}, \{ \bar{0}, \bar{3}, \bar{6}, \bar{9}\}, \{ \bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$ & $\mathbb{Z}_{12}$ are the subgroups of $\mathbb{Z}_{12}$.

===

Ex. Show that $(\mathbb{Z}_7', \times_7)$ is a cyclic group. Find all its generators, all its proper subgroups and the order of every element.

Proof. : Let $(\mathbb{Z}_7' = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}, \times_7)$ is a group of order 6.

We know that for any group G, if $a \in G$ then $< a > = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

i) $< \bar{1} > = \{\bar{1}^n : n \in \mathbb{Z}\} = \{ \bar{1} \}$

ii) $< \bar{2} > = \{\bar{2}^n : n \in \mathbb{Z}\} = \{\bar{2}^1, \bar{2}^2, \bar{2}^3 = \bar{1} \}$

$= \{ \bar{2}, \bar{4}, \bar{1}\} = < \bar{4} >$ $\quad \because \bar{2}^{-1} = \bar{4}$

iii) $< \bar{3} > = \{\bar{3}^n : n \in \mathbb{Z}\} = \{\bar{3}^1, \bar{3}^2, \bar{3}^3, \bar{3}^4, \bar{3}^5, \bar{3}^6 = \bar{1} \}$

$= \{ \bar{3}, \bar{2}, \bar{6}, \bar{4}, \bar{5}, \bar{1}\} = \mathbb{Z}_7'$

$< \bar{3} > = < \bar{3}^5 > = \mathbb{Z}_7'$ $\because (5, 6) = 1$

i.e. $< \bar{3} > = < \bar{5} > = \mathbb{Z}_7'$

$\therefore \mathbb{Z}_7'$ is a cyclic group with generators $\bar{3}$ & $\bar{5}$.

iv) $< \bar{6} > = \{\bar{6}^n : n \in \mathbb{Z}\} = \{ \bar{6}, \bar{1}\}$

$\therefore \{ \bar{1}, \bar{6}\}, \{ \bar{1}, \bar{2}, \bar{4}\}$ are the proper subgroups of $\mathbb{Z}_7'$.

The order of every element $\mathbb{Z}_7'$ are

$o(\bar{1}) = 1$, $\quad \because$ 1 is the least positive integer such that $\bar{1}^1 = \bar{1}$

$o(\bar{6}) = 2$, $\quad \because$ 2 is the least positive integer such that $\bar{6}^2 = \bar{1}$

$o(\bar{2}) = o(\bar{4}) = 3$ $\quad \because$ 3 is the least positive integer such that $\bar{2}^3 = \bar{4}^3 = \bar{1}$

and $o(\bar{3}) = o(\bar{5}) = 6$ $\quad \because$ 6 is the least positive integer such that $\bar{3}^6 = \bar{5}^6 = \bar{1}$

===

Ex. Show that ($\mathbb{Z}_{11}' = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}\}, \times_{11}$) is a cyclic group. Find all its generators, all its proper subgroups and the order of every element.

Proof. : We know that for any group G, if a ∈ G then

$< a > = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

i) $< \bar{1} > = \{\bar{1}^n : n \in \mathbb{Z}\} = \{ \bar{1} \}$

ii) $< \bar{2} > = \{\bar{2}^n : n \in \mathbb{Z}\} = \{\bar{2}^1, \bar{2}^2, \bar{2}^3, \bar{2}^4, \bar{2}^5, \bar{2}^6, \bar{2}^7, \bar{2}^8, \bar{2}^9, \bar{2}^{10} = \bar{1} \}$

$= \{ \bar{2}, \bar{4}, \bar{8}, \bar{5}, \overline{10}, \bar{9}, \bar{7}, \bar{3}, \bar{6}, \bar{1}\} = \mathbb{Z}_{11}'$

$< \bar{2} > = < \bar{2}^3 > = < \bar{2}^7 > = < \bar{2}^9 > = \mathbb{Z}_{11}'$ $\because (3, 10)=(7, 10)=(9, 10)= 1$

i.e. $< \bar{2} > = < \bar{8} > = < \bar{7} > = < \bar{6} > = \mathbb{Z}_{11}'$

$\therefore \mathbb{Z}_{11}'$ is a cyclic group with generators $\bar{2}, \bar{8}, \bar{7}$ & $\bar{6}$.

iii) $< \bar{3} > = \{\bar{3}^n : n \in \mathbb{Z}\} = \{ \bar{3}, \bar{9}, \bar{5}, \bar{4}, \bar{1}\} = < \bar{4} >$ $\because \bar{3}^{-1} = \bar{4}$

iv) $< \bar{5} > = \{\bar{5}^n : n \in \mathbb{Z}\} = \{ \bar{5}, \bar{3}, \bar{4}, \bar{9}, \bar{1}\} = < \bar{9} >$ $\because \bar{5}^{-1} = \bar{9}$

v) $< \overline{10} > = \{\overline{10}^n : n \in \mathbb{Z}\} = \{ \overline{10}, \bar{1}\}$

$\therefore \{ \bar{1}, \overline{10}\}, \{ \bar{1}, \bar{3}, \bar{4}, \bar{5}, \bar{9}\}$, are the proper subgroups of $\mathbb{Z}_{11}'$.

The order of every element of $\mathbb{Z}_{11}'$ are

$o(\bar{1})= 1$, $\because$ 1 is the least positive integer such that $\bar{1}^1 = \bar{1}$

$o(\overline{10}) = 2$, $\because$ 2 is the least positive integer such that $\overline{10}^2 = \bar{1}$

$o(\bar{3})= o(\bar{4})= o(\bar{5})= o(\bar{9})= 5$

$\because$ 5 is the least positive integer such that $\bar{3}^5 = \bar{4}^5 = \bar{5}^5 = \bar{9}^5 = \bar{1}$

and $o(\bar{2})= o(\bar{6})= o(\bar{7})= o(\bar{8})= 10$

$\because$ 10 is the least positive integer such that $\bar{2}^{10} = \bar{6}^{10} = \bar{7}^{10} = \bar{8}^{10} = \bar{1}$

==

Ex. Let A, B be subgroups of a finite group G, whose orders are relatively prime. Show that A ∩ B = { e }

Proof: We have (o(A), o(B)) = 1.

∴ There exist integers m, n such that

m.o(A) + n.o(B) = 1……….(1)

Let x ∈ A ∩ B

∴ x ∈ A and x ∈ B

∴ o(x) | o(A) and o(x) | o(B)

∴ o(x) | m.o(A) + n.o(B)

∴ o(x) | 1 by (1)

∴ $x^1 = e$

∴ x = e

Hence A ∩ B = { e } is proved.

==

Ex. Let G be a groups of prime order p, then prove that G has no proper subgroup.

Proof: Let G be a groups of prime order p.

$\therefore$ o(G) = p.

Let H be a subgroup of a group G.

By Lagrange's theorem o(H) | o(G)

$\Longrightarrow$ o(H) | p

$\Longrightarrow$ o(H) = 1 or p $\because$ p is prime number.

If o(H) = 1, then H = {e} is not a proper subgroup.

If o(H) = p, then o(H) = o(G) $\Longrightarrow$ H = G is not a proper subgroup.

Hence G has no proper subgroup is proved.

==

Ex. Show that every proper subgroup of a group of order 35 is cyclic.

Proof. : Let G be a groups of order 35 and H be a proper subgroup G.

By Lagrange's theorem o(H) | 35

$\therefore$ o(H) = 5 or 7 $\because$ H is a proper subgroup G.

i.e. o(H) is prime and every group of prime order is cyclic.

$\therefore$ H is cyclic.

Hence every proper subgroup of a group of order 35 cyclic is proved.

==

Ex. Show that every proper subgroup of a group of order 77 is cyclic.

Proof. : Let G be a groups of order 77 and H be a proper subgroup G.

By Lagrange's theorem o(H) | 77

$\therefore$ o(H) = 7 or 11 $\because$ H is a proper subgroup G.

i.e. o(H) is prime and every group of prime order is cyclic.

$\therefore$ H is cyclic.

Hence every proper subgroup of a group of order 77 cyclic is proved.

==

Ex. Find the remainder obtained when 15^{27} is divided by 8.

Sol.: By taking a = 15 and n = 8, we have (a, n) = (15, 8) = 1 and $\emptyset(n) = \emptyset(8) = 4$

$\therefore$ By Euler's theorem, $a^{\emptyset(n)} \equiv 1(\text{mod}n)$, we get,

$15^{\emptyset(8)} \equiv 1(\text{mod}8)$

i.e. $15^4 \equiv 1(\text{mod}8)$

$\therefore (15^4)^6 \equiv 1^6\ (\text{mod}8)$

$\therefore 15^{24} \equiv 1\ (\text{mod}8)$………(1)

As $15 \equiv 7\ (\text{mod}8)$

$\therefore 15^2 \equiv 7^2\ (\text{mod}8)$

$\therefore 15^2 \equiv 1\ (\text{mod}8)$

$\therefore\ 15^3 \equiv 7x1\ (\text{mod}8)$

$\therefore 15^3 \equiv 7\ (\text{mod}8)$ ………(2)

From (1) and (2), we get,

$15^{24} \times 15^{3} \equiv 1 \times 7 \pmod{8}$

$\therefore 15^{27} \equiv 7 \pmod{8}$

$\therefore$ 7 is the remainder when 15^{27} is divided by 8.

==

Ex. Find the remainder obtained when 33^{19} is divided by 7.

Sol.: By taking a = 33 and p = 7 i.e. p = 7 is prime and $p \nmid a$.

$\therefore$ By Fermat's theorem, $a^{p-1} \equiv 1 \pmod{p}$, we get,

$33^{6} \equiv 1 \pmod{7}$

$\therefore (33^{6})^{3} \equiv 1^{3} \pmod{7}$

$\therefore 33^{18} \equiv 1 \pmod{7}$

and $33 \equiv 5 \pmod{7}$

$\therefore 33^{18} \times 33 \equiv 1 \times 5 \pmod{7}$

$\therefore 33^{19} \equiv 5 \pmod{7}$

$\therefore$ 5 is the remainder when 33^{19} is divided by 7.

==

Ex. Find the remainder obtained when 3^{54} is divided by 11.

Sol.: By taking a = 3 and p = 11 i.e. p = 11 is prime and $p \nmid a$.

$\therefore$ By Fermat's theorem, $a^{p-1} \equiv 1 \pmod{p}$, we get,

$3^{10} \equiv 1 \pmod{11}$

$\therefore (3^{10})^{5} \equiv 1^{5} \pmod{11}$

$\therefore 3^{50} \equiv 1 \pmod{11}$

and $3^{4} = 81 \equiv 4 \pmod{11}$

$\therefore 3^{50} \times 3^{4} \equiv 1 \times 4 \pmod{11}$

$\therefore 3^{54} \equiv 4 \pmod{11}$

$\therefore$ 4 is the remainder when 3^{54} is divided by 11.

==

Normal Subgroup: A subgroup H of a group G is called normal subgroup of G if $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$.

==

Ex. Prove that every subgroup of an abelian group is normal.

Proof: Let G be an abelian group and H be any subgroup of G.

$\therefore gh = hg \quad \forall \quad h, g \in G$ ………..(1)

For any $h \in H \subseteq G$ and for any $g \in G$,

$ghg^{-1} = hgg^{-1} = he = h \in H$ by (1)

$\therefore$ H is a normal subgroup of G is proved.

==

Ex. Prove that every subgroup of a cyclic group is normal.

Proof: Let G be a cyclic group and H be any subgroup of G.

As every cyclic group is an abelian group.

$\therefore gh = hg \quad \forall\ h, g \in G$ ....(1)

For any $h \in H \subseteq G$ and for any $g \in G$,

$ghg^{-1} = hgg^{-1} = he = h \in H$ by (1)

$\therefore$ H is a normal subgroup of G is proved.

==

Ex. If H is a subgroup of a group G and if the normalize of H, $N(H) = \{g \in G : gHg^{-1} = H\}$, then prove that a) N(H) is subgroup of G and b) H is a normal subgroup of N(H).

Proof: Let H is a subgroup of a group G and $N(H) = \{g \in G: gHg^{-1} = H\}$is the normalize of H.

a) As $aHa^{-1} = H\ \forall\ a \in H$

$\therefore a \in H \Rightarrow a \in N(H) \Rightarrow H \subseteq N(H) \subseteq G$.

For $a, b \in N(H) \Rightarrow a, b \in G$ with $aHa^{-1} = H$ and $bHb^{-1} = H$ ....(1)

Now $a, b \in G \Rightarrow ab^{-1} \in G$

Consider $(ab^{-1})H(ab^{-1})^{-1} = (ab^{-1})H(ba^{-1})$

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

$= aHa^{-1} \qquad \because bHb^{-1} = H \Rightarrow b^{-1}Hb = H$

$= H$

Hence $ab^{-1} \in N(H)$.

$\therefore$ N(H) is a subgroup of G is proved.

b) For any $a \in N(H) \Rightarrow aHa^{-1} = H$.

$\therefore$ H is a normal subgroup of N(H).

Hence proved.

==

Index: If H is a subgroup of a finite group G, then the number of distinct right (or left) cosets of H in G is called index of H in G. Denoted by (G:H) or $i_G(H) = \frac{O(G)}{O(H)}$

Ex. If G is a group and H is a subgroup of index 2 in G, then prove that H is a normal subgroup of G.

Proof: Let H be a subgroup of index 2 in G. Then number of distinct right (or left) cosets of H in G is 2. Let $g \in G \Rightarrow g \in H$ or $g \notin H$.

If $g \in H$ then $gHg^{-1} = H$.

And if $g \notin H$ then $gH \neq H$ and $H \neq Hg$ i.e. $gH \cap H = \emptyset$ and $H \cap Hg = \emptyset$

As there are only two distinct right (or left) cosets of H in G

$\Rightarrow G = He \cup Hg$ and $G = eH \cup gH$

$\Rightarrow G = H \cup Hg = H \cup gH$

$\Rightarrow Hg = gH$

$\Rightarrow H = gHg^{-1}$

Thus either case $gHg^{-1} = H \ \forall g \in G$.

Hence H is a normal subgroup of G is proved.

==

UNIT-2-SUBGROUP

==

1) Which of the following is a improper subgroup of a group G?

(A) {e} (B) G (C) every subgroup of G (D) None of the above

2) Which of the following is a trivial subgroup of a group G?

(A) {e} (B) G (C) every subgroup of G (D) None of the above

3) A subgroup H of a group G is called …. if $H \neq G$

(A) trivial (B) improper (C) proper (D) None of the above

4) Which of the following is a subgroup of a group G = {1, -1, i, -i} under usual multiplication?

(A) {1, i} (B) {-1, -i} (C) {i, -i} (D) {1, -1}

5) Which of the following is a subgroup of the group $(Z_8, +_8)$?

(A) $\{\bar{0}, \bar{3}, \bar{5}\}$ (B) $(Z_4, +_4)$? (C) $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ (D) $\{\bar{0}, \bar{4}, \bar{6}\}$

6) Which of the following is a not subgroup of (Z, +)?

(A) The set of all even integers (B) nZ for any $n \in N$

(C) The set of all odd integers (D) {0}

7) Which of the following is a not subgroup of thegroup (R, +)?

(A) (R, +) (B) (Q, +) (C) (Z, +) D) None of these

8) Let H, K be subgroups of a group G. Then $H \cup K$ is a subgroup of G if and only if ……

(A) $H \subseteq K$ (B) $K \subseteq H$ (C) $H \subseteq K$ or $K \subseteq H$ (D) $H \subseteq K$ and $K \subseteq H$

9) The number of generators for the group G = {1, -1, i, -i} under usual multiplication are …

(A) 1 (B) 2 (C) 3 (D) 0

10) Which of the following group is not cyclic?

(A) G = {1, -1, i, -i} (B) $(Z_6, +_6)$ (C) (Z'_8, X_8) (D) (Z, +)

11) Which of the following group is abelian but not cyclic?

(A) G = {1, -1, i, -i} (B) $(Z_6, +_6)$ (C) (Q, +) (D) (Z, +)

12) If A and B are two subgroups of a group G, then which of the following is certainly a subgroup of G?

(A) $A \cap B$ (B) $A \cup B$ (C) AB (D) None of these

13) The number of proper subgroups of the group (Z, +) are …

(A) 1 (B) 2 (C) 5 (D) infinite

14) Cyclic group of order 10 has … number of subgroups.

(A) 1 (B) 2 (C) 4 (D) 10

15) Cyclic group of order 15 has … number of subgroups.

(A) 1 (B) 2 (C) 4 (D) 10

==

16) Every cyclic group has at least ….. generators.
(A) 1 (B) 2 (C) 3 (D) infinite

17) The number of distinct left cosets of a subgroup H = {1, -1} in the group G = {1, -1, i, -i} under usual multiplication are
(A) 1 (B) 2 (C) 3 (D) 4

18) If H is a subgroup of a finite group G, then o(H)|o(G). This is the statement of …… theorem.
(A) Euler’s (B) Fermat’s (C) Lagrange’s (D) Cauchy’s

19) If n ∈ N and a ∈ Z such that (a, n) = 1, then $a^{\emptyset(n)} \equiv 1 \pmod{n}$. This is the statement of …… theorem.
(A) Euler’s (B) Fermat’s (C) Lagrange’s (D) Cauchy’s

20) If p is prime and a ∈ Z, such that p ∤ a, then $a^{p-1} \equiv 1 \pmod{n}$. This is the statement of …… theorem.
(A) Euler’s (B) Fermat’s (C) Lagrange’s (D) Cauchy’s

21) Let G be a finite group and a ∈ G. Then $a^{o(G)}$ = ….
(A) e (B) a (C) a^2 (D) o(G)

22) Let Ø(n) be an Euler’s totient function. Then Ø(10)= …..
(A) 1 (B) 2 (C) 4 (D) 9

23) Let Ø(n) be an Euler’s totient function. Then Ø(17)= …..
(A) 1 (B) 2 (C) 16 (D) 7

24) The remainder obtained when 3^{54} divided by 11 is …..
(A) 5 (B) 3 (C) 4 (D) 7

25) The number of subgroups of a group of order 41 = …..
(A) 0 (B) 1 (C) 2 (D) 41

==

UNIT-3: HOMOMORPHISM AND ISOMORPHISM OF GROUPS

- Homomorphism (or Group homomorphism): Let $(G, *)$ and $(G', *')$ be any two groups, then the mapping $f: G \to G'$ is said to be homomorphism (or Group homomorphism) if $f(a * b) = f(a) *' f(b)\ \forall\, a, b \in G$.
- Trivial Homomorphism: Let $(G, *)$ and $(G', *')$ be any two groups, then the mapping $f: G \to G'$ defined by $f(a) = e'\ \forall\, a \in G$ is called trivial homomorphism where e' is an identity element in G'.
- Remark: A homomorphism $f: G \to G$ is called an <u>Endomorphism.</u>
- One-One Function: A function $f: G \to G'$ is said to be one-one function (or injective function) if $f(a) = f(b) \Rightarrow a = b$.
- Onto Function: A function $f: G \to G'$ is said to be onto function (or surjective function) if for $y \in G' \Rightarrow \exists\, x \in G$ with $f(x) = y$.
- Bijective Map: A one-one and onto map is called the bijective map.
- Kernel of homomorphism: Let $f: (G, *) \to (G', *')$ be homomorphism, then the set $Ker(f) = \{x \in G: f(x) = e',$ indentity element in $G'\}$ is called kernel of homomorphism.

<u>Ex.</u> Let $(\mathbb{Z}, +)$ be the group of integers under addition and $G = \{2^n : n \in \mathbb{Z}\}$ group under multiplication. Show that $f: \mathbb{Z} \to G$ defined by $f(n) = 2^n, \forall\, n \in \mathbb{Z}$ is onto group homomorphism.

Proof: For $m, n \in \mathbb{Z} \Rightarrow f(m) = 2^m$ and $f(n) = 2^n$

Consider, $f(m + n) = 2^{m+n}$

$= 2^m . 2^n$

$= f(m). f(n)$

$\therefore$ f is group homomorphism.

For $2^n \in G \Rightarrow \exists\, n \in \mathbb{Z}$ with $f(n) = 2^n$

$\therefore$ f is onto.

Hence, f is onto group homomorphism is proved.

Ex. Prove that the mapping $f: C \to C_0$ such that $(z) = e^z$ is a homomorphism of the additive group of complex numbers onto the multiplicative group of non-zero complex numbers. What is the kernel of f?

Proof: Let the mapping $f: C \to C_0$ defined by $(z) = e^z$

For $z_1, z_2 \in C \Longrightarrow f(z_1) = e^{z_1}$ and $f(z_2) = e^{z_2}$

Now $f(z_1 + z_2) = e^{z_1 + z_2} = e^{z_1}\, e^{z_2} = f(z_1)\, f(z_2)$

$\therefore$ f is a homomorphism.

For any non zero complex number z in $C_0 \Longrightarrow \exists\, \log z \in C$ with $f(\log z) = e^{\log z} = z$

$\therefore$ f is onto.

Hence f is onto group homomorphism.

$1 \in C_0$ is a multiplicative identity.

$\therefore$ Ker f = { z ∈ C : f(z) = 1}

= { z ∈ C : e^z = 1}

= { 0 }

==

Ex. Consider $(\mathbb{Z},+)$ the additive group of integers and $G = \{1,-1,i,-i\}$ the group under multiplication. Show that $f : \mathbb{Z} \to G$, defined by $f(n) = i^n \; \forall \, n \in \mathbb{Z}$ is group homomorphism. Find its Kernel.

Proof: Let $m,n \in \mathbb{Z} \Rightarrow f(m) = i^m$ and $f(n) = i^n$

Consider, $f(m+n) = i^{m+n}$

$= i^m . i^n$

$= f(m).f(n)$

$\therefore f$ is group homomorphism. $1 \in G$ is an identity element.

$\therefore Ker(f) = \{n \in \mathbb{Z} : f(n) = 1\}$

$= \{n \in \mathbb{Z} : i^n = 1\}$

$= 4\mathbb{Z}$

==

Ex. Let $\mathbb{C}^* = \mathbb{C} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$ be the groups under multiplication. Show that $f: \mathbb{C}^* \to \mathbb{R}^*$ defined by $f(z) = |z|, \;\; \forall \, z \in \mathbb{C}^*$ is a group homomorphism. Find its kernel.

Proof: For $z_1, z_2 \in \mathbb{C}^*$

$\Rightarrow f(z_1) = |z_1|$ and $f(z_2) = |z_2|$

Consider $f(z_1.z_2) = |z_1 z_2|$

$= |z_1|.|z_2|$

$= f(z_1).f(z_2)$

$\therefore f$ is group homomorphism.

$1 \in \mathbb{R}^*$ is an identity element.

$\therefore Ker(f) = \{ z \in \mathbb{C}^* : f(z) = 1\}$

$= \{ z \in \mathbb{C}^* : |z| = 1\}$

$\therefore Ker(f) =$ Set of all complex numbers whose modulus is 1.

==

Ex. Let $G = \{ a, a^2, a^3, \dots ,, a^{12}(= e)\}$ be a cyclic group of order 12 generated by a. Show that $f: G \to G$ defined by $f(x) = x^4 \; \forall \, x \in G$ is a group homomorphism. Find its Kernel.

Proof: Let G be a cyclic group of order 12 generated by a.

$\therefore G$ is abelian.

$\therefore (xy)^n = x^n y^n \; \forall \, x, y \in G$ ----------- (1)

For $x, y \in G \Rightarrow f(x) = x^4$ and $f(y) = y^4$

Consider $f(xy) = (xy)^4$

$= x^4 . y^4$ by (1)

$= f(x).f(y)$

$\therefore f$ is group homomorphism.

As $a^{12} = e$ is an identity element in G

$\therefore Ker(f) = \{x \in G : f(x) = e\}$

$= \{x \in G : x^4 = e\}$

$= \{e, a^3, a^6, a^9\}$

==

Ex. Consider $(\mathbb{R}, +)$ a group of reals under usual addition . Show that

1) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x \ \forall \ x \in \mathbb{R}$ is a group homomorphism. Find its Kernel.

2) $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x + 1 \ \forall \ x \in \mathbb{R}$ is not a group homomorphism.

Proof: 1) Let $x, y \in \mathbb{R} \Rightarrow f(x) = 2x$ and $f(y) = 2y$

Consider, $f(x + y) = 2(x + y)$

$= 2x + 2y$

$= f(x) + f(y)$

$\therefore f$ is group homomorphism. $0 \in \mathbb{R}$ is an identity element.

$\therefore Ker(f) = \{x \in \mathbb{R} : f(x) = 0\}$

$= \{x \in \mathbb{R} : 2x = 0\}$

$= \{0\}$

2) Let,$x, y \in \mathbb{R} \Rightarrow g(x) = x + 1$ and $g(y) = y + 1$

Consider, $g(x) + g(y) = x + 1 + y + 1$

$= x+y+2$ ---------- (1)

And $g(x + y) = x + y + 1$ ---------- (2)

$\therefore$ By (1) & (2) $\Rightarrow g(x + y) \neq g(x) + g(y)$

$\therefore g$ is not a group homomorphism is proved.

==

Ex. Let, $G = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0\right\}$ the group of all non-singular matrices of order 2 over $\mathbb{R}$ under matrix multiplication and let $\mathbb{R}^* = \mathbb{R} - \{0\}$ the group of non-zero real numbers under multiplication.Define $f : G \to \mathbb{R}^*$ by $f(A) = |A|$ for all $A \in G$. Show that f is onto group homomorphism and find it's Kernel.

Proof: For $A, B \in G \Rightarrow f(A) = |A|$ & $f(B) = |B|$

Consider $f(AB) = |AB|$

$= |A||B|$

$= f(A).f(B)$

$\therefore f$ is group homomorphism.

For $x \in \mathbb{R}^* \Rightarrow \exists \ A = \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} \in G$ with $|A| = x \neq 0$

Such that $f(A) = \begin{vmatrix} x & 0 \\ 0 & 1 \end{vmatrix} = x$

$\therefore f$ is ontogroup homomorphism. $1 \in \mathbb{R}^*$ is an identity element.

$\therefore Ker(f) = \{A \in G : f(A) = 1\}$

$= \{A \in G : |A| = 1\}$

= set of all 2×2 matrices whose determinant is 1.

==

Ex. Let $G = \{ A: A \text{ is } n \times n \text{ matrix over } \mathbb{R} \text{ and } |A| \neq 0\}$ the group under non-singular matrices of order n over $\mathbb{R}$ under multiplication and $\mathbb{R}^* = \mathbb{R} - \{0\}$, the group of non-zero real numbers under multiplication. Show that $f: G \to \mathbb{R}^*$ defined by $f(A) = |A| \ \forall A \in G$ is onto group homomorphism.

Proof: For $A, B \in G \Rightarrow f(A) = |A|$ and $f(B) = |B|$

Consider, $f(AB) = |AB|$

$= |A||B|$

$= f(A).f(B)$

$\therefore$ f is group homomorphism.

For $x \in \mathbb{R}^* \Rightarrow x$ is non-zero real number

$$\Rightarrow \exists \text{ matrix } A = \begin{bmatrix} x & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & . & . & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \in G \text{ with } f(A) = |A| = x \neq 0$$

$\therefore$ f is onto.

Hence, f is an onto group homomorphism is proved.

==

Ex. Let $G = (\mathbb{Z}, +)$ the additive group of integers and $G' = \{ 1, -1\}$ a group under multiplication. Show that $f: G \to G'$ defined by

$$f(n) = \begin{cases} 1, & \text{if n is even} \\ -1, & \text{if n is odd} \end{cases}$$

is onto group homomorphism.

Proof: For $m, n \in \mathbb{Z}$

Case i) If m and n both are even, then $(m + n)$ is even.

$\therefore f(m) = 1, f(n) = 1$ and $f(m + n) = 1$

Now $f(m + n) = 1 = 1 \times 1 = f(m).f(n)$

Case ii) If m and n both are odd, then $(m + n)$ is even.

$\therefore f(m) = -1, f(n) = -1$ and $f(m + n) = 1$

Now $f(m + n) = 1 = (-1) \times (-1) = f(m).f(n)$

Case iii) If one is even and other is odd.

Say m is even and n is odd, then $(m + n)$ is odd.

$\therefore f(m) = 1, f(n) = -1$ and $f(m + n) = -1$

Now $f(m + n) = -1 = (1) \times (-1) = f(m).f(n)$

$\therefore$ By cases (i), (ii), (iii) we have,

$f(m + n) = f(m).f(n) \quad \forall\ m, n \in \mathbb{Z}$

$\therefore$f is a group homomorphism.

For $1 \in G' \Rightarrow 2 \in G$ with $f(2) = 1$

And $-1 \in G' \Rightarrow 3 \in G$ with $f(3) = -1$

$\therefore$ f is onto.

Hence, f is onto group homomorphism is proved.

==

Ex. Let $f: G \to G'$ be a group homomorphism. Prove that

i) If e is an identity element of G then f(e) is the identity element of G′.

ii) $f(a^{-1}) = [f(a)]^{-1}, \quad \forall\ a \in G.$

iii) $f(a^m) = [f(a)]^m, \quad \forall\ a \in G$ and $m \in \mathbb{Z}$.

Proof: Let, $f: G \to G'$ be a group homomorphism.

i) Let e is an identity element of G and e′ be an identity element of G′.

For $a \in G \Rightarrow f(a) \in G'$

$\therefore f(a)e' = f(a)$

$= f(ae)$

$= f(a).f(e) \quad \because$ f is homomorphism.

$\therefore\ e' = f(e)$ by left cancellation law

i.e. f(e) is an identity element of G′.

ii) For $a \in G \Rightarrow a^{-1} \in G$ with $aa^{-1} = e$

$\therefore f(aa^{-1}) = f(e)$

$\therefore f(a).f(a^{-1}) = e'$

$\therefore f(a^{-1}) = f(a)^{-1}.e'$

$\therefore\ f(a^{-1}) = [f(a)]^{-1} \qquad \forall\ a \in G.$

iii) Case i) If m is positive integer then

$$f(a^m) = \underbrace{f(a.a.a \ldots .a)}_{m \text{ times}}$$

$$= \underbrace{f(a).f(a).f(a) \ldots .f(a)}_{m \text{ times}} \quad \because \text{f is homomorphism}$$

$\therefore\ f(a^m) = [f(a)]^m$

Case ii) If $m = 0$, then $f(a^0) = f(e) = e' = [f(a)]^0$

Case iii) If m is negative integer, then $m = -n$, where n is positive integer,

$\therefore\quad f(a^m) = f(a^{-n})$

$= f[(a^{-1})^n]$

$= f[(a^{-1})]^n$

$= [f(a)^{-1}]^n$

$= f(a)^{-n}$

$= [f(a)]^m\ \forall\ a \in G.$

$\therefore$ By cases (i), (ii) & (iii) $f(a^m) = [f(a)]^m, \quad \forall\ a \in G$ and $m \in \mathbb{Z}$.

Hence proved.

==

Ex. Prove that homomorphic image of an abelian group is abelian.

Proof: Let $f: G \rightarrow G'$ be a group homomorphism, then

$f(G) = \{ f(x): x \in G\}$ is homomorphic image of G and G is abelian.

For $a', b' \in f(G) \Rightarrow \exists\ a, b \in G$ with $f(a) = a'$ & $f(b) = b'$.

Consider, $a'b' = f(a) . f(b)$

$= f(ab)$ $\because f$ is homomorphism.

$= f(ba)$ $\because G$ is abelian

$= f(b). f(a)$ $\because f$ is homomorphism.

$\therefore a'b' = b'a'$

Hence, homomorphic image of an abelian group is abelian is proved.

==

- NOTE: Converse of above is not true.

==

Ex. Prove that homomorphic image of cyclic group is cyclic.

Proof: Let, $f: G \rightarrow G'$ be a group homomorphism, then

$f(G) = \{ f(x): x \in G\}$ is homomorphic image of G and G is a cyclic group say $G = < a >$

Claim: $f(G) = < f(a) >$

As $a \in G \Rightarrow f(a) \in f(G)$

$\Rightarrow < f(a) > \subseteq f(G)$……….(1)

Let $y \in f(G) \Rightarrow \exists\ x \in G$ with $f(x) = y$

Now, $x \in G \Rightarrow \exists\ m \in \mathbb{Z}$ with $x = a^m$

$\therefore y = f(x) = f(a^m) = [f(a)]^m \in < f(a) >$

$\therefore f(G) \subseteq < f(a) >$ …………(2)

$\therefore$ By (1) and (2) $f(G) = < f(a) >$

Hence, homomorphic image of cyclic group is cyclic.

==

Ex. Prove that homomorphic image of finite group is finite.

Proof: Let, $f: G \rightarrow G'$ be a group homomorphism, then

$f(G) = \{ f(x): x \in G\}$ is homomorphic image of G and G is a finite say $G = \{x_1, x_2, x_3, \ldots, x_n\}$

$\therefore f(G) = \{f(x_1), f(x_2), f(x_3), \ldots, f(x_n)\}$ which is finite.

Hence, homomorphic image of a finite group is finite is proved.

==

- NOTE : Converse of above is not is true.

==

Ex. Let, $f: G \rightarrow G'$ be a group homomorphism, then prove that

i) $Ker(f)$ is a subgroup of G.

ii) f is one-one iff $Ker(f) = \{e\}$ where e is an identity element in G.

iii) If H' is a subgroup of G' then $Ker(f) \subseteq f^{-1}(H')$.

Proof: Let, $f: G \to G'$ be a group homomorphism, then

i) $Ker(f) = \{x \in G : f(x) = e',$ identity element in $G'.\}$

As $e \in G \Rightarrow f(e) = e' \Rightarrow e \in Ker(f)$

$\therefore Ker(f)$ is a non-empty subset of G.

For $x, y \in Ker(f)$

$\Rightarrow x, y \in G$ with $f(x) = e'$ & $f(y) = e'$

$\Rightarrow xy^{-1} \in G$ with

$$f(xy^{-1}) = f(x).f(y^{-1})$$
$$= f(x).f(y)^{-1}$$
$$= e'.(e')^{-1}$$
$$= e'$$

$\therefore xy^{-1} \in Ker(f)$

Hence, $Ker(f)$ is a subgroup of group G.

i) Suppose, f is one-one.

Let $x \in Ker(f) \Leftrightarrow f(x) = e'$

$\Leftrightarrow f(x) = f(e)$

$\Leftrightarrow x = e \because f$ is one-one.

$\Leftrightarrow Ker(f) = \{e\}$

Conversely, Suppose $Ker(f) = \{e\}$

For $x, y \in G$

Let $f(x) = f(y)$

$\therefore f(x).f(y)^{-1} = e'$

$\therefore f(x).f(y^{-1}) = e'$

$\therefore f(xy^{-1}) = e'$

$\therefore (xy^{-1}) \in Ker(f) = \{e\}$

$\therefore xy^{-1} = e$

$\therefore x = y$

$\therefore f$ is one-one.

iii) Let H' be a subgroup of group G'.

For $x \in Ker(f) \Rightarrow f(x) = e' \in H'$

$\Rightarrow x \in f^{-1}(H')$

$\therefore Ker(f) \subseteq f^{-1}(H')$

Hence proved.

==

Ex. Let, f and g be group homomorphism from $G \to G$. Show that $H = \{x \in G : f(x) = g(x)\}$ is a subgroup of G.

Proof: Let f and g be group homomorphisms from $G \to G$ with

$H = \{x \in G : f(x) = g(x)\}$

We observe that $f(e) = e$ and $g(e) = e$ for $e \in G \therefore e \in H$

$\therefore H$ is non-empty subset of G.

For $x, y \in H \Rightarrow x, y \in G$ with $f(x) = g(x)$ & $f(y) = g(y)$

$\Rightarrow xy^{-1} \in G$ with $f(xy^{-1}) = f(x).f(y^{-1})$

$\because f$ is homomorphism.

$\therefore f(xy^{-1}) = f(x).f(y)^{-1}$

$= g(x).g(y)^{-1}$

$= g(x).g(y^{-1})$

$\therefore f(xy^{-1}) = g(xy^{-1}) \because g$ is homomorphic.

$\Rightarrow xy^{-1} \in H$

$\therefore H$ is a subgroup of G is proved.

==

❖ Isomorphism : Let, $(G, *)$ and $(G', *')$ be any two groups then the mapping $f : G \to G'$ is said to be an isomorphism if 1) f is group homomorphism, 2) f is one-one & 3) f is onto.

❖ Remark: An isomorphism $f : G \to G$ is called an automorphism.

==

Ex. Let G be a group of all matrices of the type $\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in G$ and $a^2 + b^2 = 1\}$ under matrix multiplication and G' be a group of non-zero complex numbers under multiplication. Show that $f : G \to G'$ defined by $(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}) = a + ib$, is an isomorphism.

Proof: Let $f : G \to G'$ defined by $(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}) = a + ib$.

i) For $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \in G \Longrightarrow f(A) = a + ib$ and $f(B) = c + id$

Now $AB = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac \end{bmatrix}$

i.e. $AB = \begin{bmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{bmatrix}$

$\therefore f(AB) = (ac - bd) + i(ad + bc) = (a + ib)(c + id) = f(A).f(B)$

$\therefore$ f is a homomorphism.

ii) Suppose $f(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}) = f(\begin{bmatrix} c & d \\ -d & c \end{bmatrix})$

$\Longrightarrow a + ib = c + id$

$\Longrightarrow a = c$ and $b = d$

$\Longrightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$

$\therefore$ f is one one.

iii) For $a + ib \in G' \Longrightarrow \exists \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in G$ with $(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}) = a + ib$.

By (i), (ii), (iii) f is an isomorphism is proved.

==

Ex. Let, $(\mathbb{R}, +)$ be a group of reals under addition and $(\mathbb{R}^+, \times)$ the group of positive reals under multiplication. Show that $f : \mathbb{R} \to \mathbb{R}^+$ defined by $f(x) = 2^x \ \forall \ x \in \mathbb{R}$ is an isomorphism.

Proof: 1) For $x, y \in \mathbb{R}$ $\Rightarrow$ $f(x) = 2^x$ and $f(y) = 2^y$

Consider $f(x+y) = 2^{x+y}$

$= 2^x \times 2^y$

$\therefore f(x+y) = f(x) \times f(y)$

$\therefore$ f is group homomorphism.

2) For $x, y \in \mathbb{R}$

Let $f(x) = \text{f}(y)$

$\therefore 2^x = 2^y$

$\therefore log_2 2^x = log_2 2^y$

$\therefore x = y$

$\therefore f$ is one-one.

3) For $x \in \mathbb{R}^+ \Rightarrow x$ is a positive real number $\exists\, log_2 x \in \mathbb{R}$

Such that $f(log_2 x) = 2^{\,log_2 x} = x$

$\therefore$ f is onto.

$\therefore$ By (1), (2) and (3) f is an isomorphism is proved.

==

Ex. Consider the group $(\mathbb{Z}_5, +_5)$ and $G = \{a, a^2, a^3, a^4, a^5(= e)\}$ be a cyclic group generated by a.Show that $f: \mathbb{Z}_5 \to G$ defined by $f(\bar{n}) = a^n$ $\forall\, \bar{n} \in \mathbb{Z}$ is an isomorphism.

Proof: 1) For $\bar{m}, \bar{n} \in \mathbb{Z}_5 \Rightarrow f(\bar{m}) = a^m$and $f(\bar{n}) = a^n$

Consider $f(\bar{m} +_5 \bar{n}) = f(\overline{m+n})$

$= a^{m+n}$

$= a^m . a^n$

$\therefore f(\bar{m} +_5 \bar{n}) = f(\bar{m}).f(\bar{n})$

$\therefore f$ is a group homomorphism.

2) For $\bar{m}$, $\bar{n} \in \mathbb{Z}_5$

Suppose $f(\bar{m}) = f(\bar{n})$

$\therefore a^m = a^n$

$\therefore m = n$

$\therefore \overline{m} = \overline{n}$

$\therefore$ f is one-one.

3) For $a^n \in G \Rightarrow \exists\, \bar{n} \in \mathbb{Z}_5$ with $f(\bar{n}) = a^n$ $\therefore$ f is onto.

$\therefore$ By (1), (2) and (3) f is an isomorphism is proved.

==

Ex. Let G be a group and $a \in G$. Show that $f_a : G \to G$ defined by $f_a(x) = axa^{-1}$, for all $x \in G$ is an automorphism.

Proof: 1) f_a is a group homomorphism:

For $x, y \in G$, we have $f_a(x) = axa^{-1}$ and $f_a(y) = aya^{-1}$

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

$= (ax)\, e\, (ya^{-1})$

$= (ax)\, (a^{-1}a)\, (ya^{-1})$

$= (axa^{-1})(aya^{-1})$

$= f_a(x) . f_a(y)$

$\therefore$ f_a is group homomorphism.

2) f_a is one-one :

Let, $f_a(x) = f_a(y)$ for $x, y \in G$

$\therefore$ $axa^{-1} = aya^{-1}$

$x = y$ by cancellation laws

$\therefore$ f_a is one-one.

3) f_a is onto :

For $x \in G \Rightarrow \exists\ a^{-1}xa \in G \because a \in G$ with

$f_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x$

$\therefore f_a$ is onto.

$\therefore$ By (1), (2) and (3) f_a is an automorphism is proved.

===

Ex. Let G be a group and $f : G \to G$ be a map defined by $f(x) = x^{-1}$For all $x \in G$.
Prove that a) If G is abelian then f is an isomorphism.
b) If f is group homomorphism then G is abelian.

Proof: a) Let G is abelian.

$\therefore$ $xy = yx\ \forall\ x, y \in G$ --------- (1)

1) For $x, y \in G \Rightarrow f(x) = x^{-1}$ and $f(y) = y^{-1}$

Consider $f(xy) = f(yx)$ By (1)

$f(xy) = (yx)^{-1}$

$= x^{-1}y^{-1}$

$\therefore$ $f(xy) = f(x).f(y)$

$\therefore$ f is a group homo-morphism.

2) For $x, y \in G$

Suppose $f(x) = f(y)$

$\therefore$ $x^{-1} = y^{-1}$

$\therefore$ $(x^{-1})^{-1} = (y^{-1})^{-1}$

$\therefore$ $x = y$

$\therefore$ f is one-one.

3] For $x \in G \Rightarrow \exists\, x^{-1} \in G$ with $f(x^{-1}) = (x^{-1})^{-1} = x$

$\therefore$ f is onto.

By (1), (2) and (3), f is an isomorphism.

b) Suppose f is a group homomorphism.

For $x, y \in G$

Consider $xy = [(xy)^{-1}]^{-1}$

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

$= f(y^{-1}x^{-1})$

$= f(y^{-1})f(x^{-1}) \because f$ is homomorphic

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

$\therefore xy = yx$

Hence G is abelian is proved.

===

Ex. Let G be a group and $f : G \to G$ be a map defined by $f(x) = x^{-1}$ For all $x \in G$. Prove that G is abelian iff f is an automorphism.

Proof: Let G is abelian.

$\therefore \quad xy = yx \qquad \forall\ x, y \in G$ --------- (1)

1) For $x, y \in G \Rightarrow f(x) = x^{-1}$ and $f(y) = y^{-1}$

Consider $f(xy) = f(yx)$ By (1)

$f(xy) = (yx)^{-1}$

$= x^{-1}y^{-1}$

$\therefore f(xy) = f(x).f(y)$

$\therefore f$ is a group homo-morphism.

2) For $x, y \in G$

Suppose $f(x) = f(y)$

$\therefore x^{-1} = y^{-1}$

$\therefore (x^{-1})^{-1} = (y^{-1})^{-1}$

$\therefore x = y$

$\therefore f$ is one-one.

3) For $x \in G \Rightarrow \exists\ x^{-1} \in G$ with $f(x^{-1}) = (x^{-1})^{-1} = x$

$\therefore f$ is onto.

By (1), (2) and (3) f is an isomorphism.

Conversely: Suppose f is an automorphism hence f is a group homomorphism.

For $x, y \in G$

Consider $xy = [(xy)^{-1}]^{-1}$

$= f[(xy)^{-1}]$

$= f(y^{-1}x^{-1})$

$= f(y^{-1})f(x^{-1}) \because f$ is homomorphic

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

$\therefore xy = yx$

Hence G is abelian is proved.

===

Ex. Prove that every finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +_n)$.

Proof: Let, G be a finite cyclic group of order n.

$\therefore G = \{e, a, a^2, \dots, a^{n-1}\} = \langle a \rangle$

Define $f : G \to \mathbb{Z}_n$ by $f(a^k) = \bar{k}\ \forall\ a^k \in G$

For a^k & $a^s \in G$, we have $f(a^k) = \bar{k}$ and $f(a^s) = \bar{S}$.

By division algorithm $k + s = nq + r$ where $0 \le r < n$

$\therefore \overline{k+s} = \bar{r}$

Consider $f(a^k . a^s) = f(a^{k+s})$

$= f(a^{nq+r})$

$= f[(a^n)^q . a^r]$

$= f[e^q . a^r]$

$= f(a^r)$

$= \bar{r}$

$= \overline{k+s}$

$= \bar{k} +_n \bar{s}$

$\therefore f(a^k . a^s) = f(a^k) +_n f(a^s)$

$\therefore f$ is a group homomorphism.

Also for a^k & $a^s \in G$

Let $f(a^k) = f(a^s)$

$\therefore \bar{k} = \bar{s}$

$k = s \quad \because 0 \le k, \quad s \le n$

$\therefore a^k = a^s$

$\therefore f$ is one-one.

For $\bar{k} \in \mathbb{Z}_n \Rightarrow \exists\ a^k \in G$ with $f(a^k) = \bar{k}$. $\therefore f$ is onto.

Hence f is an isomorphism is proved.

==

Ex. Prove that every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.

Proof: Let G be a infinite cyclic group generated by a.

$i.e.\ G = \{a^n : n \in \mathbb{Z}\}$

Define $f : G \to \mathbb{Z}$ by $f(a^n) = n \ \forall\ a^n \in G$

1) For a^m and $a^n \in G$, we have $f(a^m) = m$ and $f(a^n) = n$

Consider, $f(a^m . a^n) = f(a^{m+n})$

$= m + n$

$= f(a^m) + f(a^n)$

$\therefore f$ is group homomorphism.

2) Let $f(a^m) = f(a^n) \quad \forall\ m, n \in G$

$\Rightarrow \quad m = n$

$\Rightarrow \quad a^m = a^n$

$\therefore f$ is one-one.

3) For $n \in \mathbb{Z} \Rightarrow \exists\ a^n \in G$ with $f(a^n) = n$.

$\therefore f$ is onto.

$\therefore$ By (1), (2) and (3), f is an isomorphism.

$i.e.\ \ G \cong \mathbb{Z}$ is proved.

===

Ex. Let $f : G \to G'$ be a group homomorphism. If $a \in G$ and $o(a)$ is finite then show that $o(f(a)) | o(a)$.

Proof: Let $f : G \to G'$ be a group homomorphism and $a \in G$ with $o(a)$ is finite say $o(a) = n$.

$\therefore a^n = e$

$\therefore f(a^n) = f(e)$

$\therefore f(a)^n = e'$ $\quad\because$ f is homomorphic.

$\therefore o(f(a)) | n$

$\therefore o(f(a)) | o(a)$. Hence proved.

===

Ex. If $f : G \to G'$ be an isomorphism then show that $o(a) = o(f(a))\ \forall\ a \in G$.

Proof: Let, $f : G \to G'$ is an isomorphism.

Case i) If $o(a)$ is finite say $o(a) = n$

$\therefore a^n = e$

$\therefore f(a^n) = f(e)$

$\therefore f(a)^n = e'$ $\quad\because$ f is homomorphism.

$\therefore o(f(a)) \leq n$

$\therefore o(f(a)) \leq o(a)$ --------- (1)

If $o(f(a)) = m$ then

$f(a)^m = e'$

$f(a^m) = f(e)$ $\quad\because$ f is homomorphism.

$\therefore a^m = e$ $\quad\because$ f is one-one.

$o(a) \leq m$

$o(a) \leq o(f(a))$ ---------- (2)

$\therefore$ By (1) and (2) $o(a) = o(f(a))$

Case ii) If $o(a)$ is infinite then we have to prove $o(f(a))$ is infinite.

If $o(f(a))$ is finite say m.

$\therefore f(a)^m = e'$

$\therefore f(a^m) = f(e)$ $\quad\because$ f is homomorphism.

$\therefore a^m = e \because f$ is one-one.

$\therefore o(a) \leq m$, which contradicts to $o(a)$ is infinite.

$\therefore o(f(a))$ is infinite.

$\therefore$ By cases (i) and (ii) $o(a) = o(f(a))$ is proved.

===

Ex. If $G = \{1, -1, i, -i\}$ is the group under multiplication and $\bar{G} = \{\bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ is a group under multiplication modulo 10 then Show that G and $\bar{G}$ isomorphic.

Proof: Let $G = \{1, -1, i, -i\}$ is a group under multiplication with identity element 1.

We observe that $o(1) = 1, o(-1) = 2, o(i) = o(-i) = 4$

Let $\bar{G} = \{\bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ is a group with identity element $\bar{6}$.

$\therefore o(\bar{6}) = 1$, $o(\bar{2}) = 4 = o(\bar{8})$ $\because$ $\bar{2}^{-1} = \bar{8}$ and $o(\bar{4}) = 2$

$\therefore$We define $f : G \to \bar{G}$ as $f(1) = \bar{6}$, $f(-1) = \bar{4}$, $f(i) = \bar{2}$, $f(-i) = \bar{8}$

Which is one-one and onto.

For -1 ,$-i \in G$, We have $f\big((-1)(-i)\big) = f(i) = \bar{2}$ and

$$f(-1) \times_{10} f(-i) = \bar{4} \times_{10} \bar{8} = \bar{2}$$

$\therefore$ $f\big((-1)(-i)\big) = f(-1) \times_{10} f(-i)$ which is true for all element in G.

$\therefore$ f is group homomorphism. $\therefore$ f is group isomorphism.

$i.e.$ $G \cong \bar{G}$is proved.

==

Ex. Show that the groups $G = \{1, -1, i, -i\}$ is the group under usual multiplication and $\mathbb{Z}'_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ is a group under multiplication modulo 8 are not isomorphic.

Proof: Suppose G is isomorphic to $\mathbb{Z}'_8$. $i.e.\ G \cong \mathbb{Z}'_8$

$i.e.$ $f : G \to \mathbb{Z}'_8$ is an isomorphism.

$\therefore$ $o(a) = o\big(f(a)\big)\ \forall\ a \in G$ ---------- (1)

We observe that $1 \in G$ is an identity element.

$\therefore$ $o(1) = 1, o(-1) = 2, o(i) = o(-i) = 4$ and

$\bar{1} \in \mathbb{Z}'_8$ is an identity element under $\times_8$.

$\therefore$ $o\ (\bar{1}) = 1, o(\bar{3}) = 2, o\big(\bar{5}\big) = 2, o(\bar{7}) = 2$.

As $i \in G$ with $o(i) = 4$ $\therefore$ $o\big(\mathrm{f}(i)\big) = 1\ or\ 2$

which contradicts to equation (1).

$\therefore$ G and $\mathbb{Z}'_8$ are not isomorphic is proved.

Ex. Show that the set of all automorphisms of a group G forms a group under composition of mappings.

Proof: Let, A be the set of all automorphisms of a group G.

$i.e.$ $A = \{f \mid f : G \to G$ is an automorphism.$\}$

1) For $f,\ g \in A$

$\Rightarrow$ $f : G \to G$ & $g : G \to G$ is an automorphism.

$\Rightarrow$ $fog : G \to G$ is an automorphism.

$\Rightarrow$ $fog \in A$

$i.e.$ Composition of mappings is a binary operation in A.

2) For $f,\ g$ & $h \in A$, we have

$$[(fog)oh](x) = (fog)\ (h(x))$$
$$= f\ [g\big(h(x)\big)]$$
$$= fo\ [g\big(h(x)\big)]$$

$\therefore$ $[(fog)oh](x) = [fo(goh)](x)$ $\forall$ $x \in G$

$\therefore\ (fog)oh = fo(goh)$

$\therefore$ Composition of mappings is associate in A.

3) Let $I : G \to G$ defined by $I(x) = x$ is an automorphism with

$(foI)(x) = f\big(I(x)\big) = f(x)$

$= I\,[f(x)]$

$= (Iof)(x) \quad \forall \ x \in G$

$\therefore foI = Iof$

$\therefore\ I \in A$ is an identity element.

4) For $f \in A$

$\Rightarrow$ f : G → G is an automorphism.

$\Rightarrow f^{-1} : G \to G$ is an automorphism with

$(fof^{-1})(x) = f[f^{-1}(x)] = x = I(x)$

& $(f^{-1}of)(x) = f^{-1}[f(x)] = x = I(x)$

$\therefore\ f^{-1} \in A$ i.e. every mapping has inverse in A.

By (1), (2), (3) and (4) set of automorphisms A forms a group under composition of mappings is proved.

==

HOMOMORPHISM AND ISOMORPHISM OF GROUPS

==

1) Let $(G, *)$ and $(G', *')$ be any two groups, then the mapping $f: G \to G'$ is said to be homomorphism (or Group homomorphism) if $f(a * b) = \cdots ... \ \forall\ a, b \in G$.

[A] $f(a) * f(b)$ [B] $f(a) *' f(b)$ [C] $f(a *' b)$ [D] $f(ab)$

2) Let $(G, *)$ and $(G', *')$ be any two groups, then the mapping $f: G \to G'$ defined by $f(a) = e'\ \forall\ a \in G$ is called trivial homomorphism where e' is an identity element in G'.

[A] e [B] 0 [C] e' [D] 1

3) A homomorphism $f: G \to G$ is called an ……

[A] Endomorphism [B] Isomorphism [C] Automorphism [D]None of these

4) A function $f: G \to G'$ is said to be one-one function if $f(a) = f(b) \Rightarrow$ ……

[A] a = b [B] a ≠ b [C] a < b [D] a > b

5) A function $f: G \to G'$ is said to be …… function if for $y \in G' \Rightarrow \exists\ x \in G$ with $f(x) = y$.

[A] many-one [B] one-one [C] onto [D] inverse

6) A one-one and onto map is called the …… map.

[A] injective [B] bijective [C] surjective [D] many-one

7) If $f: G \to G'$ is a group homomorphism and f is one-one then $Ker(f) =$ …….

[A] $\{e\}$ [B] $\{e'\}$ [C] $\{0\}$ [D] $\{1\}$

8) Homomorphic image of an abelian group is ……

[A] cyclic [B] abelian [C] finite [D] infinite

9) Homomorphic image of a cyclic group is ……

[A] cyclic [B] abelian [C] finite [D] infinite

10) Homomorphic image of a finite group is ……

[A] cyclic [B] abelian [C] finite [D] infinite

11) Let $G = \{ a, a^2, a^3, \dots ,, a^{12}(= e)\}$ be a cyclic group of order 12 generated by a.
If $f: G \to G$ defined by $f(x) = x^4 \; \forall \; x \in G$ is a group homomorphism,
then $Ker(f) =$ ……

[A] $\{e\}$ [B] $\{e , a^3, a^6, a^9\}$ [C] $\{e , a^4, a^8\}$ [D] $\{1, -1\}$

12) Let $(\mathbb{Z}, +)$ the additive group of integers and $G = \{1, -1, i, -i\}$ the group under multiplication. If $f : \mathbb{Z} \to G$, defined by $f(n) = i^n \; \forall \, n \in \mathbb{Z}$ is homomorphism,
then $Ker(f) =$ ……

[A] $\{e\}$ [B] $\mathbb{Z}$ [C] ${}_4\mathbb{Z}$ [D] $\{1, -1\}$

13) An isomorphism f: G → G is called an …….

[A] Endomorphism [B] Homomorphism [C] Automorphism [D] None of these

14) Let, $(G ,*)$ and $(G',*')$ be any two groups then the mapping $f : G \to G'$ is said to be an isomorphism if ……

[A] f is group homomorphism [B] f is one-one
[C] f is onto [D] All of these

15) Let G be a group and $f : G \to G$ be a map defined by $f(x) = x^{-1}$ for all $x \in G$, is group homomorphism then group G is ……

[A] cyclic [B] abelian [C] finite [D] infinite

16) Every finite cyclic group of order n is isomorphic to ……

[A] $(\mathbb{Z}_n , +_n)$ [B] $(\mathbb{Z} , +)$ [C] (Q, +) [D] (R , +)

17) Every infinite cyclic group of order n is isomorphic to ……

[A] $(\mathbb{Z}_n , +_n)$ [B] $(\mathbb{Z} , +)$ [C] (Q, +) [D] (R , +)

UNIT 4: RINGS

==

Ring: A non-empty set R with two binary operations $+$ (addition) and $\cdot$ (multiplication)

$i.e.$ $(R, +, \cdot)$ is called a ring if:

I) $(R, +)$ is an abelian group.

II) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for $a, b \in R$.

III) $a(b + c) = ab + ac$ (left distributive law) and

$(a + b)c = ac + bc$ (right distributive law) $\forall\, a, b, c \in R$

Commutative Ring: A ring $(R, +, .)$ is said to be a commutative ring if

$a \cdot b = b \cdot a \;\; \forall\, a, b \in R$

Ring with unity (or ring with identity): A ring $(R, +, .)$ is said to be a ring with unity (or ring with identity) if there exists an element $1 \in R$ with $a \cdot 1 = 1 \cdot a = a, \forall\, a \in R$.

Ring with zero divisors: A ring $(R, +, .)$ is said to be a ring with zero divisors if $\exists\, a, b \in R$ with $a \neq 0, b \neq 0$ but $ab = 0$.

Ring without zero divisors: A ring $(R, +, .)$ is said to be a ring without zero divisors if $ab = 0 \;\Rightarrow either\; a = 0 \; or\; b = 0$.

$e.g.$ 1) $(\mathbb{Z}, +, .), (\mathbb{Q}, +, .), (\mathbb{R}, +, .), (\mathbb{C}, +, .)$ are commutative rings with unity and without zero divisors.

2) Let $\mathbb{R}$ be the set of all 2×2 matrices over reals then $(\mathbb{R}, +, .)$ is a non-commutative ring with unity.

3) $({}_2\mathbb{Z}, +, .)$ is a commutative ring without unity.

4) $(\mathbb{Z}_8, +_8, \times_8)$ is a commutative ring with unity and with zero divisors.

$\because\; \bar{2} \neq \bar{0}, \bar{4} \neq \bar{0}$ but $\bar{2} \times_8 \bar{4} = \bar{0}$.

Multiplicative Inverse: An element $b \in R$ is said to be multiplicative inverse of an element $a \in R$ if $a \cdot b = b \cdot a = 1$ where 1 is an identity/unity in R.

Remark:

1. Additive identity is called zero element.
2. Multiplicative identity is called unity.
3. Those elements have multiplicative inverse are called units.

==

Theorem: Let $(R, +, .)$ be a ring and $a, b, c \in R$ then

1) $a \cdot 0 = 0 \cdot a = 0$
2) $a(-b) = -(ab) = (-a)b$
3) $(-a)(-b) = ab$
4) $a(b - c) = ab - ac$
5) $(a - b)c = ac - bc$

Proof: Let, $(R,+,\ .)$ be a ring.

I) $0 \in R$ is an additive identity.

$\therefore 0+0=0$

$\therefore a(0+0)=a0$

$\therefore a0+a0=a0$ by left distributive law

$\therefore a0+a0=a0+0$

$\therefore a0=0$ by left cancellation law

Similarly $0a=0$

$\boxed{\therefore a0=0=0a}$

II) As $(-b)+b=0$

$\therefore a[(-b)+b]=a0$

$\therefore a(-b)+ab=0$ by (1)

$\therefore a(-b)=-(ab)$

Similarly $(-a)b=-(ab)$

$\boxed{\therefore a(-b)=-(ab)=(-a)b}$

III) Consider $(-a)(-b)=-[a(-b)]=-[-(ab)]$

$\boxed{\therefore (-a)(-b)=ab}$

IV) Consider $a(b-c)=a[b+(-c)]=ab+a(-c)$ by left distributive law

$\boxed{\therefore a(b-c)=ab-ac}$ by (2)

V) Consider $(a-b)c=[a+(-b)]c=ac+(-b)c$ by right distributive law

$\boxed{\therefore (a-b)c=ac-bc}$ by (2)

Hence proved.

==

Theorem: Let $(R,+,\ .)$ be a ring with identity element 1 and $a \in R$, then

1) $(-1)a=-a$ 2) $(-1)(-1)=1$.

Proof: Let, $(R,+,\ .)$ be a ring with identity element 1 and $a \in R$

1) Consider $(-1)a=-(1\cdot a)$

$\therefore (-1)a=-a$ $\because$ 1 is an identity element.

2) Consider $(-1)(-1)=(1\cdot 1)$

$\therefore (-1)(-1)=1$ Hence proved.

==

Ex: Show that a ring R is commutative if and only if

$(a+b)^2=a^2+b^2+2ab \quad \forall\ a,b \in R.$

Proof: Suppose a ring R is commutative.

$\therefore ab=ba \quad \forall\ a,b \in R$ ------ (1)

Consider,

$(a+b)^2 = (a+b)(a+b)$

$= (a+b)a + (a+b)b$ by left distributive law

$= a^2 + ba + ab + b^2$ by right distributive law

$= a^2 + ab + ab + b^2$ by (1)

$= a^2 + 2ab + b^2$

$\therefore\ (a+b)^2 = a^2 + b^2 + 2ab \ \ \forall\ a, b \in R$

Conversly: Suppose $(a+b)^2 = a^2 + b^2 + 2ab \ \ \forall\ a, b \in R$

$\therefore (a+b)(a+b) = a^2 + 2ab + b^2$

$\therefore (a+b)a + (a+b)b = a^2 + 2ab + b^2$

$\therefore\ a^2 + ba + ab + b^2 = a^2 + ab + ab + b^2$

$\therefore\ ba = ab$ by cancellation laws

$\therefore$ Ring R is commutative ring is proved.

===

Ex: Let R be a ring with identity element 1 and $(ab)^2 = a^2b^2\ \ \forall\ a, b \in R$. Show that R is commutative.

Proof: Let R be a ring with identity element 1 and

$(ab)^2 = a^2b^2\ \ \forall\ a, b\ \in R$ ------- (1)

For $a, b+1 \in R, we$ have

$[a(b+1)]^2 = a^2(b+1)^2$

$\therefore a(b+1)\cdot a(b+1) = a^2(b+1)(b+1)$

$\therefore (ab+a)(ab+a) = a^2(b^2+b+b+1)$

$\therefore (ab)^2 + aba + a^2b + a^2 = a^2b^2 + a^2b + a^2b + a^2$

$\therefore a^2b^2 + aba + a^2b + a^2 = a^2b^2 + a^2b + a^2b + a^2$

$\therefore\ \ aba = \ a^2b\ \ \forall\ a, b\ \in R$ ----- (2)

For $a+1, b\ \in R$, from (2), we have

$(a+1)b(a+1) = (a+1)^2 b$

$\therefore\ (ab+b)(a+1) = (a+1)(a+1)b$

$\therefore aba + ab + ba + b = (a+1)(ab+b)$

$\therefore\ a^2b + ab + ba + b = a^2b + ab + ab + b$ by (2)

$\therefore\ ba = ab\ \forall\, a, b \in R$

Hence R is a commutative ring is proved.

===

Ex: Show that $(\mathbb{Z}_6, +_6, \times_6)$ is a commutative ring with unity and with zero divisors.

Proof: Let, $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

We prepare composition tables of $+_6$ & $\times_6$ for $\mathbb{Z}_6$ as follows

$+_6$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$\times_6$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

We observe that $+_6$ and $\times_6$ are binary operations in $\mathbb{Z}_6$ are also commutative and associative in $\mathbb{Z}_6$. Additive inverse of $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$ are $\bar{0}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}$ resp. in $\mathbb{Z}_6$. $\bar{0} \in \mathbb{Z}_6$ is an additive identity and $\bar{1} \in \mathbb{Z}_6$ is a multiplicative identity in $\mathbb{Z}_6$.
As $\mathbb{Z}_6 \subseteq \mathbb{Z}$ $\therefore$ distributive laws hold in $\mathbb{Z}_6$.

$\therefore$ $(\mathbb{Z}_6, +_6, \times_6)$ is a commutative ring with unity and with zero divisors.

$\because$ $\bar{2} \neq 0, \bar{3} \neq 0$ and $\bar{4} \neq \bar{0}$ but $\bar{2} \times_6 \bar{3} = \bar{0}$ and $\bar{3} \times_6 \bar{4} = \bar{0}$.

==

Ex: Show that the set $R = \{0, 2, 4, 6\}$ is a commutative ring under addition and multiplication modulo 8.

Proof: Let $R = \{0,2,4,6\}$

We prepare composition tables of $+_8$ and $\times_8$ for R as follows

$+_8$	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

$\times_8$	0	2	4	6
0	0	0	0	0
2	0	4	0	4
4	0	0	0	0
6	0	4	0	4

We observe that $+_8$ and $\times_8$ are binary operations in R, are also commutative and associative in R. $\because$ $R \subseteq \mathbb{Z}$.

Additive inverse of 0,2,4 & 6 are 0,6,4 & 2 in R.

$0 \in R$ is an additive identity. As $R \subseteq \mathbb{Z}$.

$\therefore$ Distributive laws hold in R.

$\therefore$ $(R, +_8, \times_8)$ is a commutative ring is proved.

Ex: Show that $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ forms a ring under addition and multiplication modulo 7.

Proof: Let $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

We prepare composition tables of $+_7$ & $\times_7$ for $\mathbb{Z}_7$ as follows

$+_7$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

$\times_7$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

We observe that $+_7$ and $\times_7$ are binary operations in $\mathbb{Z}_7$, are also commutative and associative in $\mathbb{Z}_7$. $\because$ $\mathbb{Z}_7 \subseteq \mathbb{Z}$.

Additive inverse of $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$ are $\bar{0}, \bar{6}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}$ respectively in $\mathbb{Z}_7$. $0 \in \mathbb{Z}_7$ is an additive identity and $\bar{1} \in \mathbb{Z}_7$ is a multiplicative identity in $\mathbb{Z}_7$.

As $\mathbb{Z}_7 \subseteq \mathbb{Z}$ $\therefore$ distributive laws hold in $\mathbb{Z}_7$.

Hence, $\mathbb{Z}_7$ forms a commutative ring under $+_7$ and $\times_7$ is proved.

Ex: In the ring $(\mathbb{Z}_{10}, +_{10}, \times_{10})$, find all divisors of zero.

Solution: Let, $(\mathbb{Z}_{10}, +_{10}, \times_{10})$ be a ring with zero element $\bar{0}$.

We prepare table for $\times_{10}$ of $\mathbb{Z}_{10}$ as follows

$\times_{10}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\bar{2}$	$\bar{5}$	$\bar{8}$	$\bar{1}$	$\bar{4}$	$\bar{7}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{2}$	$\bar{6}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{2}$	$\bar{6}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$

$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{8}$	$\bar{5}$	$\bar{2}$	$\bar{9}$	$\bar{6}$	$\bar{3}$
$\bar{8}$	$\bar{0}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{9}$	$\bar{0}$	$\bar{9}$	$\bar{8}$	$\bar{3}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

From the table, we observe that $\bar{2} \neq \bar{0}, \bar{4} \neq \bar{0}, \bar{5} \neq \bar{0}$,

$\bar{6} \neq \bar{0}, \bar{8} \neq \bar{0}$ but $\bar{2} \times_{10} \bar{5} = \bar{0}, \bar{4} \times_{10} \bar{5} = \bar{0}, \bar{5} \times_{10} \bar{6} = \bar{0}$ and $\bar{5} \times_{10} \bar{8} = \bar{0}$.

$\therefore \bar{2}, \bar{4}, \bar{5}, \bar{6}$ & $\bar{8}$ are the zero divisors in a given ring.

==

Ex: On the set $\mathbb{Z}$ of integers, define binary operations $\oplus$ and $\odot$ as

$a \oplus b = a + b - 1$ and $a \odot b = a + b - ab \ \forall \ a, b \in \mathbb{Z}$.

Show that $(\mathbb{Z}, \oplus, \odot)$ is a commutative ring with identity element 0.

Proof: I) $(\mathbb{Z}, \oplus)$ is an abelian group:-

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

1) $a \oplus b = a + b - 1 \in \mathbb{Z} \ \forall \ a, b \in \mathbb{Z}$.

$\therefore \oplus$ is a binary operation in $\mathbb{Z}$.

2) Consider, $a \oplus (b \oplus c) = a \oplus (b + c - 1)$

$= a + b + c - 1 - 1$

$= (a + b - 1) + c - 1$

$= (a + b - 1) \oplus c$

$a \oplus (b \oplus c) = (a \oplus b) \oplus c$

$\therefore \oplus$ is associative in $\mathbb{Z}$.

3) As $a \oplus 1 = a + 1 - 1 = a = 1 \oplus a \ \forall \ a \in \mathbb{Z}$

$\therefore 1 \in \mathbb{Z}$ is an identity element under $\oplus$

4) As $a \in \mathbb{Z} \Rightarrow \exists \ 2 - a \in \mathbb{Z}$ with

$a \oplus (2 - a) = a + 2 - a - 1 = 1 = (2 - a) \oplus a$

$\therefore 2 - a$ is an inverse of a in $\mathbb{Z}$.

5) As $a \oplus b = a + b - 1 = b + a - 1 = b \oplus a \ \forall a, b \in \mathbb{Z}$.

$\therefore \oplus$ is commutative in $\mathbb{Z}$.

$\therefore (\mathbb{Z}, \oplus)$ is an abelian group.

II) $a \odot b = a + b - ab \in \mathbb{Z} \ \forall a, b \in \mathbb{Z}$

Consider, $a \odot (b \odot c) = a \odot (b + c - bc)$

$= a + b + c - bc - a(b + c - bc)$

$= a + b + c - bc - ab - ac + abc$ --- (1)

& $(a \odot b) \odot c = (a + b - ab) \odot c$

$= a + b - ab + c - (a + b - ab)c$

$= a + b - ab + c - ac - bc + abc$ ---- (2)

By (1) and (2) $a \odot (b \odot c) = (a \odot b) \odot c$

$\therefore \odot$ is associative in $\mathbb{Z}$.

3) Consider, $a \odot (b \oplus c) = a \odot (b + c - 1)$

$$= a + b + c - 1 - a(b + c - 1)$$
$$= a + b + c - 1 - ab - ac + a$$
$$= 2a + b + c - ab - ac - 1 \quad \text{----} \ [3]$$

& $(a \odot b) \oplus (a \odot c) = (a + b - ab) \oplus (a + c - ac)$

$$= a + b - ab + a + c - ac - 1$$
$$= 2a + b + c - ab - ac - 1 \quad \text{-----} \quad [4]$$

By [3] and [4] $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$

Similarly $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c) \quad \forall\ a, b, c \in \mathbb{Z}$

$i.e.$ distributive laws hold in $\mathbb{Z}$. $\therefore$ $(\mathbb{Z}, \oplus, \odot)$ is a ring.

4) As $a \odot b = a + b - ab = b + a - ba = b \odot a \quad \forall\ a, b \in \mathbb{Z}$.

$\therefore$ $\odot$ is commutative in $\mathbb{Z}$.

5) As $0 \in \mathbb{Z}$ with $a \odot 0 = a + 0 - a \cdot 0 = a = 0 \odot a\ \forall\ a \in \mathbb{Z}$

$\therefore$ $\bar{0} \in \mathbb{Z}$ is an identity element in $\mathbb{Z}$.

Hence, $(\mathbb{Z}, \oplus, \odot)$ is a commutative ring with identity element 0 is proved.

==

Ex: Prove that a non-zero element $\bar{m}$ in $(\mathbb{Z}_n, +_n, \times_n)$ is a zero divisor if and only if m is not relatively prime to n, where $n > 1$.

Proof: Suppose a non-zero element m is a zero divisor.

We have to prove $(m, n) \neq 1$.

If $(m, n) = 1$ --------- (1)

As $\bar{m}$ is a zero divisor $\therefore\ \exists\ \bar{t} \in (\mathbb{Z}_n, +_n, \times_n)$ with $\bar{t} \neq 0$ where $0 < t < n$ with $\bar{m} \times_n \bar{t} = \bar{0}$

$\therefore\ \overline{mt} = \bar{0} \quad \therefore\ n \mid mt \quad \therefore\ n \mid t$

Which contradicts to $0 < t < n$. $\therefore$ $(m, n) \neq 1$

$i.e.$ m is not relatively prime to n.

Conversely, Suppose m is not relatively prime to n.

$\therefore (m, n) = d > 1 \quad \therefore\ d \mid m$ and $d \mid n$.

$\therefore\ m = dr$ and $n = dk$ for some $0 < r, t < n$.

$\therefore\ mk = drk = (dk)r = nr \quad \therefore\ \overline{mk} = \overline{nr} = \bar{0}$

$\therefore\ \bar{m} \times_n \bar{k} = \bar{0}$ with $\bar{m} \neq \bar{0}$ & $\bar{k} \neq \bar{0}$

$\therefore\ \bar{m}$ is a zero divisor.

==

Ex: Show that $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \overline{(n-1)}\}$ the set of residue classes of integers modulo n, forms a commutative ring with identity element underaddition modulo $n(+_n)$ and multiplication modulo $n(\times_n)$ operations.

Proof : I) $(\mathbb{Z}_n, +_n)$ is an abelian group:-

1) As $\bar{a} +_n \bar{b} = \overline{a+b} \in \mathbb{Z}_n \quad \forall\, \bar{a}, \bar{b} \in \mathbb{Z}_n$

$\therefore$ $+_n$ is a binary operation in $\mathbb{Z}_n$.

2) As $\bar{a} +_n (\bar{b} +_n \bar{c}) = \bar{a} +_n (\overline{b+c})$

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

$\therefore$ $+_n$ is associative in $\mathbb{Z}_n$.

3) As $\bar{a} +_n \bar{0} = \overline{a+0} = \bar{a} = \bar{0} +_n \bar{a} \quad \forall\, \bar{a} \in \mathbb{Z}_n$

$\therefore$ $\bar{0}$ is an additive identity in $\mathbb{Z}_n$.

4) For $\bar{a} \in \mathbb{Z}_n \;\Rightarrow\; \exists\; \overline{(n-a)} \in \mathbb{Z}_n$ with

$\bar{a} +_n \overline{(n-a)} = \overline{a + (n-a)} = \bar{0} = \overline{(n-a)} +_n \bar{a}$

$\therefore$ $\overline{n-a}$ is an additive inverse in $\mathbb{Z}_n$.

5) As $\bar{a} +_n \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} +_n \bar{a} \qquad \forall\, \bar{a}, \bar{b} \in \mathbb{Z}_n$

$\therefore$ $+_n$ is commutative in $\mathbb{Z}_n$.

II) As $\bar{a} \times_n \bar{b} = \overline{ab} \in \mathbb{Z}_n \quad \forall\, \bar{a}, \bar{b} \in \mathbb{Z}_n$

$\therefore$ $\times_n$ is a binary operation in $\mathbb{Z}_n$.

Consider, $\bar{a} \times_n (\bar{b} \times_n \bar{c}) = \bar{a} \times_n \overline{bc} = \overline{a(bc)} = \overline{(ab)c}$

$$= \overline{ab} \times_n \bar{c} = (\bar{a} \times_n \bar{b}) \times_n \bar{c}$$
$$\forall\, \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$$

$\therefore$ $\times_n$ is associative in $\mathbb{Z}_n$.

III) For $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$

Consider, $\bar{a} \times_n (\bar{b} +_n \bar{c}) = \bar{a} \times_n (\overline{b+c})$

$$= \overline{a(b+c)}$$
$$= \overline{ab + ac}$$
$$= \overline{ab} +_n \overline{ac}$$
$$= (\bar{a} \times_n \bar{b}) +_n (\bar{a} \times_n \bar{c})$$

Similarly, $(\bar{a} +_n \bar{b}) \times_n \bar{c} = (\bar{a} \times_n \bar{c}) +_n (\bar{b} \times_n \bar{c})$

$\therefore$ distributive laws holds in $\mathbb{Z}_n$.

IV) As $\bar{a} \times_n \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \times_n \bar{a} \quad \forall\ \bar{a}, \bar{b} \in \mathbb{Z}_n$

$\therefore \times_n$ is commutative in $\mathbb{Z}_n$.

V) As $\bar{a} \times_n \bar{1} = \overline{a \cdot 1} = \bar{a} = \bar{1} \times_n \bar{a} \quad \forall\ \bar{a} \in \mathbb{Z}_n$

$\therefore\ \bar{1}$ is the multiplicative identity in $\mathbb{Z}_n$.

Hence, $(\mathbb{Z}_n, +_n, \times_n)$ is a commutative ring with identity element is proved.

==

Ex: Denote $R = {}_2\mathbb{Z}$ = the set of even integers**.** For $a, b \in R$ we define $a + b$ = usual addition of a and b and $a \odot b = \frac{ab}{2}$ where a, b is the usual product of a and b. Show that $(R, +, \odot)$ is a commutative ring with identity element 2.

Proof: I) <u>$(R, +)$ is an abelian group:-</u>

1) As sum of two even integers is even.
   $\therefore +$ is a binary operation in R.
2) As $a + (b + c) = (a + b) + c \quad \forall\, a, b \in R$
   $\therefore +$ is associative in R.
3) As $a + 0 = a = 0 + a \quad \forall\ a \in R$
   $\therefore$ 0 is an identity element in R.
4) For $a \in R \Rightarrow \exists\ -a \in R$ with $a + (-a) = 0 = (-a) + a$
   $\therefore -a$ is an additive inverse of a in R.
5) As $a + b = b + a \quad \forall\ a, b \in R$

II) For $a, b \in R \Rightarrow a\ \&\ b$ are even integers

$\Rightarrow ab$ is multiple of 4

$\Rightarrow \frac{ab}{2}$ is even integer

$\Rightarrow a \odot b \in R$

$i.e.$ $\odot$ is a binary operation in R.

Consider $a \odot (b \odot c) = a \odot (\frac{bc}{2})$

$$= \frac{a(\frac{bc}{2})}{2} = \frac{(\frac{ab}{2})c}{2}$$

$$= \left(\frac{ab}{2}\right) \odot c$$

$$= (a \odot b) \odot c \quad \forall\, a, b, c \in R$$

$\therefore\ \odot$ is associative in R.

III) For $a, b, c \in R$

Consider, $a \odot (b + c) = \frac{a(b+c)}{2} = \frac{ab}{2} + \frac{ac}{2} = (a \odot b) + (a \odot c)$

Similarly, $(a + b) \odot c = (a \odot c) + (b \odot c)$

$i.e.$ distributive laws holds in R.

IV) As $a \odot b = \frac{ab}{2} = \frac{ba}{2} = b \odot a \quad \forall\, a, b \in R$

$\therefore$ $\odot$ is commutative in R.

V) As $a \odot 2 = \frac{a(2)}{2} = a = 2 \odot a \quad \forall\ a \in R$

$\therefore$ 2 is an identity element in R.

Hence $(R, +, \odot)$ is commutative ring with identity element 2 is proved.

==

Integral Domain: A commutative ring without zero divisors is called an Integral domain.

Field: A commutative ring with identity element and having inverse to all non-zero elements is called a Field.

Division Ring (or Skew field): A ring with identity element is called a Division ring or skew field.

==

Ex. Show that $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ the set of Gaussian integers, forms an integral domain under usual addition and multiplication of complex numbers.

Proof: I) $(\mathbb{Z}[i], +)$ is an abelian group:

1) As $(a + ib) + (c + id) = (a + c) + i(b + d) \in \mathbb{Z}[i]$
$\forall\, a + ib, c + id \in \mathbb{Z}[i]$ $\therefore$ $+$ is a binary operation in $\mathbb{Z}[i]$.

2) As $(a + ib) + [(c + id) + (e + if)]$
$= (a + ib) + (c + e) + i(d + f)$
$= [a + (c + e)] + i[b + (d + f)]$
$= [(a + c) + e] + i[(b + d) + f]$
$= (a + c) + i(b + d) + (e + if)$
$= [(a + ib) + (c + id)] + (e + if)\ \forall\, a + ib, c + id, e + if \in \mathbb{Z}[i]$

$i.e.$ $+$ is associative in $\mathbb{Z}[i]$.

3) As $(a + ib) + (0 + i0) = a + ib = (0 + 0i) + (a + ib)$
$\forall\ a + ib \in \mathbb{Z}[i]$

$\therefore$ $0 + i0$ is an identity element in $\mathbb{Z}[i]$.

4) As $(a + ib) + (-a - ib) = 0 + i0 = (-a - ib) + (a + ib)$
$\therefore$ $-a - ib$ is an inverse of $a + ib$ in $\mathbb{Z}[i]$.

5) As $(a + ib) + (c + id) = (a + c) + i(b + d)$
$= (c + a) + i(d + b)$
$= (c + id) + (a + ib) \forall\, a + ib, c + id \in \mathbb{Z}[i]$

$\therefore$ $+$ is commutative in $\mathbb{Z}[i]$.

II) 1) As $(a+ib)(c+id)=(ac-bd)+i(ad+bc)\in\mathbb{Z}[i]\ \forall\ a+ib, c+id\in\mathbb{Z}[i]$

$\therefore\ \cdot$ is a binary operation in $\mathbb{Z}[i]$.

2) For $(a+ib),(c+id),(e+if)\in\mathbb{Z}[i]$

Consider $(a+ib)[(c+id)(e+if)]$

$=(a+ib)[(ce-df)+i(cf+de)]$

$=(ace-adf-bcf-bde)+i(acf+ade+bce-bdf)$

$=[(ac-bd)+i(ad+bc)](e+if)$

$=[(a+ib)(c+id)](e+if)$

$\therefore\ \cdot$ is a associative operation in $\mathbb{Z}[i]$.

III) For $a+ib, c+id\ \&\ e+if\ \in\mathbb{Z}[i]$

Consider, $(a+ib)[(c+id)+(e+if)]$

$=(a+ib)[(c+e)+i(d+f)]$

$=(ac+ae-bd-bf)+i(ad+af+bc+be)$

$=(ac-bd)+i(ad+bc)+(ae-bf)+i(af+be)$

$=(a+ib)(c+id)+(a+ib)(e+if)$

Similarly $[(a+ib)+(c+id)](e+if)=(a+ib)(e+if)+(c+id)(e+if)$

$i.e.$ distributive laws holds in $\mathbb{Z}[i]$.

IV) As $(a+ib)(c+id)=(ac-bd)+i(ad+bc)$

$=(ca-db)+i(da+cb)$

$=(c+id)(a+ib)\ \ \forall\ a+ib, c+id\ \in\mathbb{Z}[i]$

$\therefore\ \cdot$ is commutative in $\mathbb{Z}[i]$.

V) If $(a+ib)(c+id)=0+i0$

$\Rightarrow either\ a+ib=0+i0\ \ or\ \ c+id=0+i0$

$\therefore(\mathbb{Z}[i],+,\cdot)$ is an integral domain is proved.

==

Ex. Show that $R=\{a+b\sqrt{2} : a,b\ \in\ \mathbb{Z}\}$ is an integral domain under usual addition and multiplication of complex numbers.

Proof: I) <u>$(R,+)$ is an abelian group:</u>

1) As $\left(a+b\sqrt{2}\right)+\left(c+d\sqrt{2}\right)=(a+c)+(b+d)\sqrt{2}\ \in\ R$

$\forall\ a+b\sqrt{2}, c+d\sqrt{2}\ \in\ R\ \therefore\ +$ is a binary operation in R.

2) As $\left(a+b\sqrt{2}\right)+\left[\left(c+d\sqrt{2}\right)+\left(e+f\sqrt{2}\right)\right]$

$=\left(a+b\sqrt{2}\right)+(c+e)+(d+f)\sqrt{2}$

$=[a+(c+e)]+[b+(d+f)]\sqrt{2}$

$=[(a+c)+e]+[(b+d)+f]\sqrt{2}$

$=(a+c)+(b+d)\sqrt{2}+\left(e+f\sqrt{2}\right)$

$= [(a+b\sqrt{2})+(c+d\sqrt{2})]+(e+f\sqrt{2})$

$\forall\ a+b\sqrt{2}, c+d\sqrt{2}, e+f\sqrt{2}\ \in\ R$

$i.e. +$ is associative in R.

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

$\forall\ a+b\sqrt{2}\ \in\ R$

$\therefore\ 0+0\sqrt{2}$ is an identity element in R.

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

$\therefore\ -a-b\sqrt{2}$ is an inverse of $a+b\sqrt{2}$ in R.

5) As $(a+b\sqrt{2})+(c+d\sqrt{2})$

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

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

$= (c+d\sqrt{2})+(a+b\sqrt{2}) \forall\ a+b\sqrt{2}, c+d\sqrt{2} \in\ R$

$\therefore\ +$ is commutative in R.

II) 1) As $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac-bd)+(ad+bc)\sqrt{2} \in R$

$\forall\ a+b\sqrt{2}, c+d\sqrt{2}\ \in\ R$

$\therefore\ \cdot$ is a binary operation in R.

2) For $(a+b\sqrt{2}), (c+d\sqrt{2}), (e+f\sqrt{2}) \in \mathbb{R}$

Consider $(a+b\sqrt{2})[(c+d\sqrt{2})(e+f\sqrt{2})]$

$= (a+b\sqrt{2})[(ce+2df)+(cf+de)\sqrt{2}]$

$= (ace+2adf+2bcf+2bde)+(acf+ade+bce+2bdf)\sqrt{2}$

$= [(ac+2bd)+(ad+bc)\sqrt{2}](e+f\sqrt{2})$

$= [(a+b\sqrt{2})(c+d\sqrt{2})](e+f\sqrt{2})$

$\therefore\ \cdot$ is a associative operation in $\mathbb{R}$.

III) For $a+b\sqrt{2}, c+d\sqrt{2}\ \&\ e+f\sqrt{2}\ \in\ R$

Consider $(a+b\sqrt{2})[(c+d\sqrt{2})+(e+f\sqrt{2})]$

$= (a+b\sqrt{2})[(c+e)+(d+f)]\sqrt{2}$

$= (ac+ae-bd-bf)+(ad+af+bc+be)\sqrt{2}$

$= (ac-bd)+(ad+bc)\sqrt{2}+(ae-bf)+(af+be)\sqrt{2}$

$= (a+b\sqrt{2})(c+d\sqrt{2})+(a+b\sqrt{2})(e+f\sqrt{2})$

Similarly $[(a+b\sqrt{2})+(c+d\sqrt{2})](e+f\sqrt{2})$

$= (a+b\sqrt{2})(e+f\sqrt{2})+(c+d\sqrt{2})(e+f\sqrt{2})$

$i.e.$ distributive laws holds in R.

IV) As $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac-bd)+(ad+bc)\sqrt{2}$

$= (ca-db)+(da+cb)\sqrt{2}$

$= (c+d\sqrt{2})(a+b\sqrt{2}) \quad \forall\, a+b\sqrt{2}, c+d\sqrt{2} \in R$

$\therefore\ \cdot$ is commutative in R.

V) If $(a+b\sqrt{2})(c+d\sqrt{2}) = 0+0\sqrt{2}$

$\Rightarrow either\ a+b\sqrt{2} = 0+0\sqrt{2} \quad or \quad c+d\sqrt{2} = 0+0\sqrt{2}$

$i.e.$ $(R,+,\ \cdot)$ is a commutative ring without zero divisors.

$\therefore$ $(R,+,\ \cdot)$ is an integral domain is proved.

==

Ex: Show that $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} : a,b \in \mathbb{Z}\}$ is an integral domain under usual addition and multiplication of complex numbers.

Proof: I) $(\mathbb{Z}[\sqrt{-5}],+)$ is an abelian group:

1) As $(a+b\sqrt{-5})+(c+d\sqrt{-5}) = (a+c)+(b+d)\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$

$\forall\, a+b\sqrt{-5}, c+d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$

$\therefore$ $+$ is a binary operation in $\mathbb{Z}[\sqrt{-5}]$.

2) As $(a+b\sqrt{-5})+[(c+d\sqrt{-5})+(e+f\sqrt{-5})]$

$= (a+b\sqrt{-5})+(c+e)+(d+f)\sqrt{-5}$

$= [a+(c+e)]+[b+(d+f)]\sqrt{-5}$

$= [(a+c)+e]+[(b+d)+f]\sqrt{-5}$

$= (a+c)+(b+d)\sqrt{-5}+(e+f\sqrt{-5})$

$= [(a+b\sqrt{-5})+(c+d\sqrt{-5})]+(e+f\sqrt{-5})$

$\forall\, a+b\sqrt{-5}, c+d\sqrt{-5}, e+f\sqrt{-5} \in \sqrt{-5}]$

$i.e.$ $+$ is associative in $\mathbb{Z}[\sqrt{-5}]$.

2) As $(a+b\sqrt{-5})+(0+0\sqrt{-5})$

$= a+b\sqrt{-5} = (0+0\sqrt{-5})+(a+b\sqrt{-5})$

$\forall\ a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$

$\therefore$ $0+0\sqrt{-5}$ is an identity element in $\mathbb{Z}[\sqrt{-5}]$.

3) As $(a+b\sqrt{-5})+(-a-b\sqrt{-5}) = 0+0\sqrt{-5} = (-a-b\sqrt{-5})+(a+b\sqrt{-5})$

$\therefore$ $-a-b\sqrt{-5}$ is an inverse of $a+b\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$.

4) As $(a+b\sqrt{-5})+(c+d\sqrt{-5}) = (a+c)+(b+d)\sqrt{-5}$

$= (c+a)+(d+b)\sqrt{-5}$

$= (c+d\sqrt{-5})+(a+b\sqrt{-5})$

$\forall\ a+b\sqrt{-5}, c+d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$

$\therefore$ $+$ is commutative in $\mathbb{Z}[\sqrt{-5}]$.

II) 1) As $(a+b\sqrt{-5})(c+d\sqrt{-5}) = (ac-bd)+(ad+bc)\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$

$\forall\ a+b\sqrt{-5}, c+d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$

$\therefore$ $\cdot$ is a binary operation in $\mathbb{Z}[\sqrt{-5}]$.

2) For $(a+b\sqrt{-5}), (c+d-5), (e+f\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$.

Consider $(a+b\sqrt{-5})[(c+d\sqrt{-5})(e+f\sqrt{-5})]$

$= (a+b\sqrt{-5})[(ce-5df)+(cf+de)\sqrt{-5}]$

$= (ace-5adf-5bcf-5bde)+(\ acf+ade+bce-5bdf)\sqrt{-5}$

$= [(ac-5bd)+(\ ad+bc)\sqrt{-5}](e+f\sqrt{-5})$

$= [(a+b\sqrt{-5})(c+d\sqrt{-5})](e+f\sqrt{-5})$

$\therefore$ $\cdot$ is a associative operation in $\mathbb{Z}[\sqrt{-5}]$..

III) For $a+b\sqrt{-5}, c+d\sqrt{-5}$ & $e+f\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$

Consider, $(a+b\sqrt{-5})[(c+d\sqrt{-5})+(e+f\sqrt{-5})]$

$= (a+b\sqrt{-5})[(c+e)+(d+f)]\sqrt{-5}$

$= (ac+ae-bd-bf)+(ad+af+bc+be)\sqrt{-5}$

$= (ac-bd)+(ad+bc)\sqrt{-5}+(ae-bf)+(af+be)\sqrt{-5}$

$= (a+b\sqrt{-5})(c+d\sqrt{-5})+(a+b\sqrt{-5})(e+f\sqrt{-5})$

Similarly $[(a+b\sqrt{-5})+(c+d\sqrt{-5})](e+f\sqrt{-5})$

$= (a+b\sqrt{-5})(e+f\sqrt{-5})+(c+d\sqrt{-5})(e+f\sqrt{-5})$

$i.e.$ distributive laws holds in $\mathbb{Z}[\sqrt{-5}]$.

IV) As $(a+b\sqrt{-5})(c+d\sqrt{-5}) = (ac-bd)+(ad+bc)\sqrt{-5}$

$= (ca-db)+(da+cb)\sqrt{-5}$

$= (c+d\sqrt{-5})(a+b\sqrt{-5})$

$\forall\ a+b\sqrt{-5}, c+d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$

$\therefore$ $\cdot$ is commutative in $\mathbb{Z}[\sqrt{-5}]$.

V) If $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 0+0\sqrt{-5}$

$\Rightarrow either\ a+b\sqrt{-5} = 0+0\sqrt{-5}\ \ or\ \ c+d\sqrt{-5} = 0+0\sqrt{-5}$

$i.e.$ $(\mathbb{Z}[\sqrt{-5}], +, \cdot)$ is a commutative ring without zero divisors.

$\therefore$ $(\mathbb{Z}[\sqrt{-5}], +, \cdot)$ is an integral domain is proved.

==

Ex. Let $\mathbb{R}$ be the set of all real numbers. Show that $\mathbb{R} \times \mathbb{R}$ forms a field under addition and multiplication defined by $(a, b) + (c, d) = (a + c, b + d)$ & $(a, b) . (c, d) = (ac - bd, ad + bc)$.

Proof: I) $(\mathbb{R} \times \mathbb{R}, +)$ is an abelian group:

1) As $(a,b) + (c,d) = (a + c, b + d) \in \mathbb{R} \times \mathbb{R} \quad \forall (a,b),(c,d) \in \mathbb{R} \times \mathbb{R}$

$\therefore$ $+$ is a binary operation in $\mathbb{R} \times \mathbb{R}$.

2) As $(a,b) + [(c,d) + (e,f)]$

$= (a,b) + [(c,d) + (e,f)$

$= (a,b) + (c + e, d + f)$

$= (a + c + e, b + d + f)$

$= (a + c, b + d) + (e,f)$

$= [(a,b) + (c,d)] + (e,f) \quad \forall (a,b),(c,d),(e,f) \in \mathbb{R} \times \mathbb{R}$

$i.e. +$ is associative in $\mathbb{R} \times \mathbb{R}$.

3) As $(a,b) + (0,0) = (a,b) = (0,0) + (a,b) \quad \forall (a,b) \in \mathbb{R} \times \mathbb{R}$

$\therefore$ $(0,0)$ is an identity element in $\mathbb{R} \times \mathbb{R}$.

4) As $(a,b) + (-a,-b) = (0,0) = (-a,-b) + (a,b)$

$\therefore$ $(-a,-b)$ is an inverse of (a,b) in $\mathbb{R} \times \mathbb{R}$.

5) As $(a,b) + (c,d) = (a + c, \ b + d)$

$= (c + a, \ d + b)$

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

$\therefore$ $+$ is commutative in $\mathbb{R} \times \mathbb{R}$.

II) 1) As $(a,b).(c,d) = (ac - bd, ad + bc) \in \mathbb{R} \times \mathbb{R} \ \forall (a,b),(c,d) \in \mathbb{R} \times \mathbb{R}$

$\therefore$ $\cdot$ is a binary operation in $\mathbb{R} \times \mathbb{R}$.

2) For $(a,b),(c,d)$ & $(e,f) \in \mathbb{R} \times \mathbb{R}$

Consider $(a,b).[(c,d).(e,f)]$

$= (a,b).[(ce - df, cf + de)]$

$= (ace - adf - bcf - bde, acf + ade + bce - bde)$

$= (ac - bd, ad + bc).(e,f)$

$= [(a,b).(c,d)].(e,f)$

$\therefore$ $\cdot$ is a associative operation in $\mathbb{R} \times \mathbb{R}$.

III) For $(a,b),(c,d)$ & $(e,f) \in \mathbb{R} \times \mathbb{R}$

Consider $(a,b).[(c,d) + (e,f)]$

$= (a,b).(c + e, d + f)$

$= (ac + ae - bd - bf, ad + af + bc + be)$

$= (ac - bd, ad + bc) + (ae - bf, af + be)$

$= (a,b).(c,d) + (a,b).(e,f)$

Similarly $[(a,b)+(c,d)].(e,f)=(a,b)(e,f)+(c,d)(e,f)$

$i.e.$ distributive laws holds in $\mathbb{R}\times\mathbb{R}$.

IV) As $(a,b).(c,d)=(ac-bd,ad+bc)$

$$=(ca-db,da+cb)$$

$$=(c,d).(a,b)\ \ \forall\,(a,b),(c,d)\in\mathbb{R}\times\mathbb{R}$$

$\therefore\ \cdot$ is commutative in $\mathbb{R}\times\mathbb{R}$.

V) As $(a,b).(1,0)=(a,b)=(1,0).(a,b)\ \ \forall\,(a,b)\in\mathbb{R}\times\mathbb{R}$

$\therefore\ (1,0)$ is a multiplicative identity element in $\mathbb{R}\times\mathbb{R}$.

VI) If $(a,b)\neq(0,0)$ then $(a,b)^{-1}=(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2})$

$\because\ (a,b).\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)=\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right).(a,b)=(1,0)$

i.e. every non-zero element has inverse in $\mathbb{R}\times\mathbb{R}$

$\therefore\ (\mathbb{R}\times\mathbb{R},+,\ \cdot)$ is a commutative ring with unity and every non-zero element has inverse in it.

$\therefore\ (\mathbb{R}\times\mathbb{R},+,\ \cdot)$ is a field.

==

Ex: For $n>1$, Prove that $\mathbb{Z}_n$ is an integral domain iff n is prime.

Proof: Suppose $\mathbb{Z}_n$ is an integral domain.We have to prove n is prime.

If n is not prime then $n=mt$ for $1<m<n\ \&\ 1<t<n$.

$$\therefore\ \bar{n}=\overline{mt}$$

$$\therefore\ \bar{0}=\bar{m}\times_n\bar{t}$$

$\therefore\ \bar{m}=\bar{0}\ \ or\ \ \bar{t}=\bar{0}$ $\quad\because\ \mathbb{Z}_n$ is an integral domain

$\therefore\ \ n\,|\,m$ and $n\,|\,t$ which contradicts to $1<m<n\ \&\ 1<t<n$.

Hence, n is prime.

Conversely, Suppose n is prime.

For $\bar{a}\ \&\ \bar{b}\ \in\ \mathbb{Z}_n$ with $\bar{a}\times_n\bar{b}=\bar{0}$ $\quad\therefore\ \overline{ab}=\bar{0}$

$\therefore\ n\,|\,a\ \ or\ \ n\,|\,b$ $\quad\because\ \ n$ is prime.

$$\therefore\ \bar{a}=\bar{0}\ \ or\ \ \bar{b}=\bar{0}$$

$i.e.\,\mathbb{Z}_n$ has no zero divisors.

Hence, $\mathbb{Z}_n$ is an integral domain is proved.

==

Ex: Prove that commutative ring $(R,+,\cdot)$ is an integral domain iff cancellation laws holds in R.

Proof: Suppose, a commutative ring $(R,+,\cdot)$ is an integral domain.

For $a,b,c\ \in R$

Let $ab=ac$ with $a\neq0\ \therefore a(b-c)=0$

$\therefore\ \ b-c=0$ $\quad\because\ \ R$ is an I.D

$$\therefore b = c$$

$i.e.$ cancellation laws holds in R.

Conversely, Suppose cancellation laws hold in R.

Let $ab = 0$ for $a, b \in R$

If $a = 0$, then we are through.

If $a \neq 0$, then $ab = a0$ $\therefore$ $b = 0$ by cancellation law

$$i.e.\ ab = 0 \Rightarrow either\ a = 0\ or\ b = 0$$

$\therefore$ $(R, +, \cdot)$ is an integral domain is proved.

==

Ex: Prove that a commutative ring $(R, +, \cdot)$ is an integral domain if and only if $a, b \in R, ab = 0 \Rightarrow either\ a = 0\ or\ b = 0.$

Proof: Suppose, a commutative ring $(R, +, \cdot)$ is an integral domain.

$\therefore$ cancellation laws holds in R.

For $a, b \in R$ Suppose, $ab = 0$

If $a = 0$, then we are through. But if $a \neq 0$ then

$ab = 0 \Rightarrow ab = a0 \Rightarrow b = 0$ by cancellation law

$\therefore$ $ab = 0 \Rightarrow either\ a = 0\ or\ b = 0$

Conversely, Suppose For $a, b \in R$

$\therefore ab = 0 \Rightarrow either\ a = 0\ or\ b = 0$

$i.e.$ R has no zero divisors.

$\therefore$ $(R, +, \cdot)$ is an integral domain is proved.

==

Ex: Prove that every field is an integral domain but converse may not be true.

Proof: Let, $(F, +, \cdot)$ be any field.

$i.e.$ $(F, +, \cdot)$ is a commutative ring with identity element 1 and every non-zero element has inverse in it.

For $a, b \in F$ Suppose $ab = 0$ -------- (1)

If $a \neq 0$ then a^{-1} is exists. $\because$ F is field.

Pre-multiplying by a^{-1} to equation (1), we get

$$a^{-1}(ab) = a^{-1}0$$

$$\Rightarrow (a^{-1}a)b = 0$$

$$\Rightarrow 1 \cdot b = 0$$

$$\Rightarrow b = 0$$

$\therefore$ $(F, +, \cdot)$ has no zero divisors.

Hence, $(F, +, \cdot)$ is an integral domain.

Hence every field is an integral domain is proved. But converse may not be true.$e.g.$ $(\mathbb{Z},+,\cdot)$ is an integral domain but not a field.

$\because\ 2^{-1} = \frac{1}{2} \notin \mathbb{Z}$.

==

Ex: Prove that every finite integral domain is a field.

Proof: Let $(R,+,\cdot)$ be any finite integral domain.

$i.e.$ $(R,+,\cdot)$ is a commutative ring without zero divisors.

As R is a finite say $R = \{a_1, a_2, \dots, a_n\}$ where $a_1, a_2, \dots, a_n$ are distinct elements of R.

For $a \in R$ with $a \neq 0$

$\therefore\ aa_1, aa_2, aa_3, \dots, aa_n$ are the distinct elements of R.

$$\because\ R = \{aa_1, aa_2, aa_3, \dots, aa_n\}$$

As $a \in R$ $\therefore$ $a = aa_k$ for some k.

<u>Claim</u>: a_k is an identity element.

For $a_j \in R \Rightarrow a_j = a \cdot a_r$ for some r.

$$= (a \cdot a_k)a_r$$
$$= (a_k a)a_r$$
$$= a_k(aa_r)$$
$$\therefore\ a_j = a_k \cdot a_j$$

$\therefore$ a_k is an identity element. Denoted by $a_k = 1$

$\therefore$ $a_k = 1 \in R$. $\Rightarrow 1 = a \cdot a_s$ for some S.

$\therefore$ Every non-zero element has inverse in R.

$\therefore$ $(R,+,\cdot)$ is a field.

Hence every finite integral domain is a field is proved.

==

Ex: Prove that $(\mathbb{Z},+,\cdot)$ is an integral domain but not field.

Proof: Let $(\mathbb{Z},+,\cdot)$ is a commutative ring with identity element 1.

For $a, b \in \mathbb{Z}$ with $ab = 0 \Rightarrow$ $either\ a = 0\ or\ b = 0$

$i.e.$ $\mathbb{Z}$ has no zero divisors. $\therefore$ $(\mathbb{Z},+,\cdot)$ is an integral domain.

But for any non-zero integer n has multiplicative inverse $\frac{1}{n} \notin \mathbb{Z}$

$\therefore$ $(\mathbb{Z},+,\cdot)$ is not a field.

==

Ex. If p is prime number, then show that $\mathbb{Z}_p$ is an integral domain.

Proof: Let p is prime.

For $\bar{a}$ & $\bar{b} \in \mathbb{Z}_p$ with $\bar{a} \times_p \bar{b} = \bar{0}$ $\therefore$ $\overline{ab} = \bar{0}$

$\therefore\ p \mid a \ \ or \ \ p \mid b \qquad \because\ p$ is prime.

$\therefore\ \bar{a} = \bar{0} \ \ or \ \ \bar{b} = \bar{0}$

$i.e.\ \mathbb{Z}_p$ has no zero divisors.

Hence $\mathbb{Z}_p$ is an integral domain is proved.

==

Ex. In the ring $(\mathbb{Z}_7, +_7, \times_7)$, find

i) - $(\bar{4} \times_7 \bar{6})$, ii) $\bar{3} \times_7 (\overline{-6})$, iii) $(\overline{-5}) \times_7 (\overline{-5})$,

iv) Units in $\mathbb{Z}_7$, v) additive inverse of $\bar{6}$, vi) zero divisors.

Is $\mathbb{Z}_7$ a field or an integral domain? Justify.

Proof: Let $(\mathbb{Z}_7, +_7, \times_7)$ be a ring

We prepare composition tables of $+_7$ & $\times_7$ for $\mathbb{Z}_7$ as follows

$+_7$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

$\times_7$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

In $\mathbb{Z}_7$. $\bar{0} \in \mathbb{Z}_7$ is an additive identity and $\bar{1} \in \mathbb{Z}_7$ is a multiplicative identity in $\mathbb{Z}_7$.

Additive inverse of $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$ are $\bar{0}, \bar{6}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}$ respectively.

i) - $(\bar{4} \times_7 \bar{6})$ = - $(\bar{3})$ = $\bar{4}$

ii) $\bar{3} \times_7 (\overline{-6}) = \bar{3} \times_7 \bar{1} = \bar{3}$

iii) $(\overline{-5}) \times_7 (\overline{-5}) = \bar{2} \times_7 \bar{2} = \bar{4}$

iv) As $\bar{2} \times_7 \bar{4} = \bar{1}$, $\bar{3} \times_7 \bar{5} = \bar{1}$ & $\bar{6} \times_7 \bar{6} = \bar{1}$

$\therefore\ \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$ are the units in $\mathbb{Z}_7$.

v) Additive inverse of $\bar{6}$ = -$\bar{6}$ = $\bar{1}$. $\qquad \because\ \bar{6} +_7 \bar{1} = \bar{0}$

vi) From second table we observe that product of two non-zero elements is not zero. $\therefore$ No zero divisors in $\mathbb{Z}_7$.

We observe that $(\mathbb{Z}_7, +_7, \times_7)$ is a commutative ring with unity and every non-zero element has inverse in it.

$\therefore\ (\mathbb{Z}_7, +_7, \times_7)$ is a field and hence an integral domain.

==

Ex. Which of the following rings are integral domains?

(i) $\mathbb{Z}_{187}$, (ii) $\mathbb{Z}_{61}$, (iii) $\mathbb{Z}_{22}$, (iv) $(\mathbb{Z}, +, \cdot)$.

Solution: By using the result that if p is prime, then $\mathbb{Z}_p$ is an integral domain, we have,

i) $187 = 11 \times 17$ is not prime. $\therefore \mathbb{Z}_{187}$ is not an integral domain.

ii) 61 is prime. $\therefore \mathbb{Z}_{61}$ is an integral domain.

iii) $22 = 2 \times 11$ is not prime. $\therefore \mathbb{Z}_{22}$ is not an integral domain.

iv) $(\mathbb{Z}, +, \cdot)$ is a commutative ring with unity but has no zero divisors

$\therefore (\mathbb{Z}, +, \cdot)$ is not an integral domain.

==

Boolean ring: A ring $(R, +,\cdot)$ is said to be a Boolean ring if $a^2 = a \ \forall\, a \in R$.

$e.g.$ $(\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}, +_2, \times_2)$ is a Boolean ring. $\because\ \bar{0}^2 = \bar{0} \times_2 \bar{0} = \bar{0}$ and $\bar{1}^2 = \bar{1} \times_2 \bar{1} = \bar{1}$.

==

Ex: Prove that every Boolean ring is a commutative ring.

Proof: Let, $(R, +,\cdot)$ be any Boolean ring.

$\therefore\ a^2 = a \quad \forall\ a \in R.$

For $a \in R \ \Rightarrow\ -a \in R.$

$\Rightarrow (-a)^2 = -a$

$\Rightarrow a^2 = -a$

$\Rightarrow a = -a \quad \forall\ a \in R$ -------- (1)

For $a, b \in R \ \Rightarrow\ a + b \in R$

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

$\Rightarrow\ (a + b)(a + b) = (a + b)$

$\Rightarrow a(a + b) + b(a + b) = (a + b)$

$\Rightarrow\ a^2 + ab + ba + b^2 = a + b$

$\Rightarrow\ a + ab + ba + b = a + b$

$\Rightarrow ab = -ba$

$\Rightarrow ab = ba$ by (1)

$i.e.$ $(R, +,\cdot)$ is a commutative ring.

Hence every Boolean ring is a commutative ring.

==

Ex: In a Boolean ring R. Show that $i)\ 2x = 0\ \forall\ x \in R,\ ii)\ xy = yx \ \forall\ x, y \in R.$

Proof: Let $(R, +,\cdot)$ be any Boolean ring.

$\therefore\ x^2 = x \quad \forall\ x \in R$

1) For $x \in R \Rightarrow -x \in R$

$\Rightarrow\ (-x)^2 = -x$

$\Rightarrow\ x^2 = -x$

$\Rightarrow\ x = -x$ ------ (1)

$\Rightarrow\ x + x = 0$

$\Rightarrow\ 2x = 0 \quad \forall\ x\ \in R.$

2) For $x, y \in R \Rightarrow x + y \in R$

$\Rightarrow (x+y)^2 = (x+y)$

$\Rightarrow (x+y)(x+y) = (x+y)$

$\Rightarrow x(x+y) + y(x+y) = (x+y)$

$\Rightarrow x^2 + xy + yx + y^2 = x + y$

$\Rightarrow x + xy + yx + y = x + y$

$\Rightarrow xy = -yx$

$\Rightarrow xy = yx \quad \forall\ x, y \in R$ by (1)

Hence proved.

===

UNIT 4: RINGS [MCQ'S]

===

1) If (R, +, .) is a ring with zero element 0 then for all a∈ R with a.0 = 0.a = ……

A) a B) 0 C) 1 D) None of these

2) If Z_p is finite field then p is ……

A) composite B) even C) prime D) odd

3) Ring $(Z_n, +_n, \times_n)$ is an integral domain and a field if and only if n is ……

A) composite B) even C) prime D) odd

4) Ring $(Z_n, +_n, \times_n)$ is not a field if and only if n is ……

A) composite B) even C) prime D) odd

5) Ring $(Z_n, +_n, \times_n)$ is a ring with zero divisors if and only if n is ……

A) composite B) even C) prime D) odd

6) Ring $(Z_n, +_n, \times_n)$ is a ring without zero divisors if and only if n is ……

A) composite B) even C) prime D) odd

7) A non-zero element m in ring $(Z_n, +_n, \times_n)$ is invertible if and only if ……

A) m and n are even B) m and n are odd

C) m and n are relatively prime D) None of these

8) If p is prime then Z_p is …..

A) Not Ring B) Boolean Ring C) Finite Field D) None of these

9) Every field is ……

A) a Boolean ring B) an Integral domain

C) Not a ring D) Not Integral domain

10) Every Integral domain is ……

A) Not a ring B) a field C) May not be a field D) a Boolean ring

11) Every finite Integral domain is ……

A) Not a ring B) a field C) not a field D) Boolean ring

12) Which of the following is a field ?

A) (Z, +, .) B) (Q, +, .) C) (2Z, +, .) D) None of these

13) Which of the following is a field ?

A) Z_{18} B) Z_{19} C) Z_{48} D) Z_{187}

14) Which of the following is not a field ?

A) Z_{19} B) Z_{29} C) Z_{41} D) Z_{187}

15) (Z, +, .) is an integral domain and ……

A) a field B) not a field C) a Boolean ring D) None of these

16) (Z, +, .) is ……

A) an integral domain but not a field B) both an integral domain and a field

C) a field but not an integral domain D) neither an integral domain nor a field

17) (2Z, +, .) the ring of even integers is Integral domain ……

A) with unity B) without unity

C) with zero divisors D) None of these

18) If R is a commutative ring and a, b ∈ R then $(a+b)^2$ = ……

A) a+b B) a^2+b^2+2ab C) $a^2+b^2+ab+ba$ D) None of these

19) If R is a ring and a, b ∈ R such that $(a+b)^2 = a^2+b^2+2ab$ then R is ……

A) Ring with zero divisors B) Field

C) Commutative D) None of these

20) Zero divisors in a ring $(Z_6, +_6, x_6)$ are

A) $\bar{2}, \bar{3}$ B) $\bar{1}, \bar{5}$ C) $\bar{0}, \bar{5}$ D) None of these

21) If R is a Boolean ring then a^2 = … for all a∈ R.

A) 0 B) 1 C) a D) None of these

22) If R is a Boolean ring then R is ……

A) ring with zero divisors B) a field

C) a commutative ring D) an integral domain

23) If R is a Boolean ring then a + a = …… for all a∈ R.

A) a B) 0 C) 1 D) -a

24) If R is a Boolean ring then for a, b ∈ R with a + b = 0 ⟹ ……

A) a B) b C) a = b D) None of these

==

॥ अंतरी पेटवू ज्ञानज्योत ॥

विद्यापीठ गीत

मंत्र असो हा एकच ह्रदयी 'जीवन म्हणजे ज्ञान'
ज्ञानामधूनी मिळो मुक्ती अन मुक्तीमधूनी ज्ञान ॥धृ ॥
कला, ज्ञान, विज्ञान, संस्कृती साधू पुरूषार्थ
साफल्यास्तव सदा 'अंतरी पेटवू ज्ञानज्योत'
मंगल पावन चराचरातून स्त्रवते अक्षय ज्ञान ॥१ ॥
उत्तम विद्या, परम शक्ति ही आमुची ध्येयासक्ती
शील, एकता, चारित्र्यावर सदैव आमुची भक्ती
सत्य शिवाचे मंदिर सुंदर, विद्यापीठ महान ॥२ ॥
समता, ममता, स्वातंत्र्याचे नांदो जगी नाते,
आत्मबलाने होऊ आम्ही आमुचे भाग्यविधाते,
ज्ञानप्रभुची लाभो करूणा आणि पायसदान ॥३ ॥

— कै.प्रा. राजा महाजन

THE NATIONAL INTERGRATION PLEDGE

"I solemnly pledge to work with dedication to preserve and strengthen the freedom and integrity of the nation.

I further affirm that I shall never resort to violence and that all differences and disputes relating to religion, language, region or other political or economic grievance should be settled by peaceful and constitutional means."