Group Theory

Binary Composition or Binary Operation :-

A binary composition $*$ on a non-empty set G is a function from $G \times G$ to G i.e $* : G \times G \to G$ such that $\forall\ a, b \in G$ we have $a * b \in G$

→ If $*$ is a binary operation on a set G, we say that the set G is closed under the operation $*$

Example :-1 Let $G = Z$ set of integers

$*$ is (a) addition '+'. Since $\forall\ a, b \in Z$ we have $a+b \in Z$, ∴ '+' is a binary composition.

(b) Subtraction: '−' Since $\forall\ a, b \in Z$ we have $a-b \in Z$, ∴ '−' is a binary composition.

(c) Multiplication: '.' Since $\forall\ a, b \in Z$ we have $a.b \in Z$ ∴ '.' is a binary composition.

(d) Division: '÷' Since $\forall\ a, b \in Z$ we have $a \div b = \frac{a}{b}$ may not belong to Z.

∴ ÷ is not a binary composition.

Example :- 2 Define $*$ on Z by $a * b = a + b$ $\forall\ a, b \in Z$

E → even integers $*$ is a B.C

O → odd integers $*$ is not a B.C

Group :- A non-empty set G with a Binary operation '$*$' is said to form a group if it satisfies the following axioms.

(1) Associativity :- $a * (b * c) = (a * b) * c$, $\forall\ a, b, c \in G$

(2) Existence of Identity : $\forall\ a \in G$, $\exists$ an element $e \in G$ $\exists$ such that $a * e = a = e * a$

'e' is the identity element.

(iii) Existence of inverse :- $\forall\ a \in G$ $\exists$ an element $a' \in G$

$\ni$ such that $\boxed{a * a' = e = a' * a}$ ← identity element

$a' \in G$ is called inverse of element $a \in G$

$\rightarrow (G, *)$ is a group.

Abelian Group :- A group $(G, *)$ is said to be an abelian group or a commutative group if

$$\boxed{a * b = b * a \quad \forall\ a, b \in G}$$

(Famous mathematician who discover this property.)

Finite Group :- A group G is said to be finite if the set G is finite, else it is infinite

Example-(1) $G = Z$, the set of integers

'$*$' is addition '$+$'

(i) closure : $\forall\ a, b \in G$, $a * b = a + b \in G$

$\therefore$ G is closed under the operation $*$ i.e. $+$

(2) Associativity : Since integers are associative under addition

$\therefore$ Associativity holds.

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

(3) Identity :- $\forall\ a \in G$ $\exists\ 0 \in G \rightarrow a + 0 = a = 0 + a$

$\therefore$ $0 \in G$ is the identity element.

(4) Inverse :- $\forall\ a \in G$ $\exists\ -a \in G$ $\ni$ $a + (-a) = 0 = (-a) + a$

$\therefore$ $(-a) \in G$ is the inverse of $a \in G$.

$\therefore$ $(G, +)$ is a group.

Since integers are commutative under addition.

i.e. $a+b = b+a \quad \forall\ a,b \in G$ ∎

$\therefore (G,+)$ is a Abelian Group.

$\therefore (G,+)$ is a Infinite Abelian Group.

Examples

(2) The set of rationals $\mathbb{Q}$ under addition.

⇒ Similiar to example-(1)

(3) The set of ~~ration~~ real numbers ($\mathbb{R}$) under addition.

(4) Set of integers under subtraction

Sol:- (i) Closure :- Since $\forall\ a,b \in G$

$a-b \in G$, $\therefore$ closure property holds.

(ii) Associativity :- It is not true.

As for $2,3,4 \in G\ (=\mathbb{Z})$

$(2-3)-4 \neq 2-(3-4)$

Therefore, integers under subtraction do not form a group.

Ex (5) Let $G=\mathbb{Z}$, the set of integers.

Define the composition $*$ on G by

$a * b = a \cdot b$, $\forall\ a,b \in G$

(i) Closure :- Since $\forall\ a,b \in G$

$a \cdot b \in G$ $\therefore$ closure property holds.

(ii) Associative :- Since integers are associative under multiplication,

Therefore associativity holds.

i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall\ a,b,c \in G$

(iii) Identity :- $\forall\ a \in G\ \exists\ 1 \in G \ni a \cdot 1 = a = 1 \cdot a$

$\therefore 1 \in G$ is the identity.

(iv) Inverse :- $\forall\ a \in G$, $a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$

But $\frac{1}{a}$ may not belong to G

Therefore, G is not a group under ~~integers~~ multiplication.

Ex-6 $G = Q - \{0\}$ under multiplication.

(iv) Inverse : $\forall\ a \in G\ \exists\ \frac{1}{a} \in G \Rightarrow a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$

$\therefore \frac{1}{a} \in G$ is the Inverse of $a \in G$.

Note:

~~Under multiplication in~~

Any set containing '0' is not a group under multiplication.

Ex-7 $G = Q^+$, set of positive rational numbers under multiplication

Ex-8 The set of natural number under addition

① closure :- $\forall\ a, b \in G$, $a+b \in G$.

$\therefore$ closure property holds.

② Associativity :- Since natural number are associative under addition. $\therefore$ associativity holds.

i.e $\forall\ a, b, c \in G$

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

③ Identity :- Since $\forall\ a \in G$ $\nexists$ any element $b \in G \Rightarrow$

$a+b = a = b+a.$

$\therefore$ Identity element does not exist.

Hence $(G, +)$ does not form a group.

Example: The set S of positive irrational numbers together with 1 under multiplication

Since $\sqrt{2} \cdot \sqrt{2} = 2 \in S$ $\therefore$ closure property fails.

Example :- The set of all rational numbers of the form $3^m \cdot 6^n$, where m and n are integers under multiplication.

$G = \{ 3^m \cdot 6^n \mid m, n \in Z \}$

Closure :- Let $3^m \cdot 6^n \in G$ and $3^{m_1} \cdot 6^{n_1} \in G$; $m, m_1, n, n_1 \in$

Then $(3^m \cdot 6^n) \cdot (3^{m_1} \cdot 6^{n_1}) \Rightarrow 3^{m+m_1} \cdot 6^{n+n_1} \in G$

as $m+m_1$ & $n+n_1 \in G$

(2) Associativity :- Since the set of rational number is associative under multiplication.

∴ Associativity Holds.

(3) Identity :- $\forall\ 3^m \cdot 6^n \in G\ \exists\ 3^0 \cdot 6^0 = 1 \in G$

$\Rightarrow (3^m \cdot 6^n) \cdot (3^0 \cdot 6^0) = (3^m \cdot 6^n) = (3^0 \cdot 6^0) \cdot (3^m \cdot 6^n)$

∴ $3^0 \cdot 6^0 = 1 \in G$ is the identity element.

(4) Inverse :- $\forall\ 3^m \cdot 6^n \in G\ \exists\ 3^{-m} \cdot 6^{-n} \in G \Rightarrow$

$(3^m \cdot 6^n) \cdot (3^{-m} \cdot 6^{-n}) = 1 = (3^{-m} \cdot 6^{-n}) \cdot (3^m \cdot 6^n)$

∴ $(3^{-m} \cdot 6^{-n}) \in G$ is the inverse of $3^m \cdot 6^n \in G$.

∴ G form a group under multiplication.

Example :- The set $R^n = \{(a_1, a_2 \dots a_n) \mid a_i \in R\}$ under the operation of component wise addition.

Closure :- $\forall\ (a_1, a_2, \dots a_n) \in R^n$ and $(b_1, b_2, \dots b_n) \in R^n$,

we have $(a_1, a_2 \dots a_n) + (b_1, b_2 \dots b_n)$

$= (a_1+b_1, a_2+b_2, \dots a_n+b_n) \in R^n$

∴ Closure property holds.

Associativity : $\forall\ (a_1, a_2 \dots a_n), (b_1, b_2 \dots b_n)$ and $(c_1, c_2 \dots c_n) \in R^n$

$(a_1, a_2, \dots a_n) + (b_1, b_2 \dots b_n) + (c_1, c_2 \dots c_n)$

$= (a_1+b_1)+c_1, (a_2+b_2)+c_2 \dots (a_n+b_n)+c_n)$

$= a_1+(b_1+c_1), a_2+(b_2+c_2) \dots, a_n+(b_n+c_n)$

Example :- 11

The subset $G = \{1, -1, i, -i\}$ of the set of complex no. is a group under multiplication.

Sol :- (i) Closure :-

	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Clearly, from the Cayley table, closure property holds.

(ii) Associativity :- Since, complex numbers are associative under multiplication.

$\therefore$ Associativity holds

(iii) Identity :- Since $1 \cdot 1 = 1$, $-1 \cdot 1 = -1$, $i \cdot 1 = i$, $-i \cdot 1 = -i$

$\therefore$ $1 \in G$ is the identity elements.

(iv) Inverse :- Since $1 \cdot 1 = 1 \Rightarrow$ inverse of 1 is 1

$-1 \cdot -1 = 1 \Rightarrow$ inverse of -1 is -1

$i \cdot -i = 1 \Rightarrow$ inverse of i is $-i$

$-i \cdot i = 1 \Rightarrow$ inverse of $-i$ is i

$\therefore$ G is a group under multiplication.

Since $\forall\ a, b \in G$ we have $a \cdot b = b \cdot a$

$\therefore$ G is an abelian finite group.

Note :- The numbers $1, -1, i, -i$ are the four forth roots of unity.

Thus we have shown that the four forth roots of unity form a finite Abelian group under multiplication

Example:- **Quaternion Group (Q_8)**

Let $G = \{1, -1, i, -i, j, -j, k, -k\}$ Define composition on G using multiplication as $i^2 = j^2 = k^2 = -1$

$ij = -ji = k$, $jk = -kj = i$ $ki = -ik = j$

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

Clearly, from cayley Table, closure property holds.

Since $\forall\ a, b, c \in G$, we have $(ab)c = a(bc)$

$\therefore$ Associativity Holds. (Complex Number)

Identity:- Since $1 \cdot 1 = 1$, $1 \cdot (-1) = -1$, $1 \cdot i = i$, $1 \cdot -i = -i$

$1 \cdot j = j$, $1 \cdot (-j) = j$, $1 \cdot k = k$, $1 \cdot (-k) = -k$

$\therefore$ $1 \in G$ is the identity.

Since, $1 \cdot 1 = 1 \Rightarrow$ Inverse of 1 is 1

$-1 \cdot -1 = 1 \Rightarrow$ inverse of -1 is -1

$i \cdot -i = 1 \Rightarrow$ inverse of i is -i

$-i \cdot i = 1 \Rightarrow$ inverse of -i is i

$j \cdot -j = 1 =$ inverse of j is -j

$-j \cdot j = 1 \Rightarrow$ inverse of -j is j

$k \cdot -k = 1 \Rightarrow$ inverse of k is -k

$-k \cdot k = 1 =$ ——— -k — k

∴ G is a group under the given composition.

Clearly, G is non-abelian as

$ij \neq ji$

Example:-

Let $G = \{1, \omega, \omega^2\}$ where ω is cube root of unity under multiplication.

Sol:- (1) Closure:-

	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Clearly, from the Cayley Table, closure property holds.

2) Associativity:-

Since, complex numbers are associative under multiplication. Therefore associativity holds.

i.e $(a.b).c = a.(b.c)$ $\forall$ $a, b, c \in G$

3) Identity:- Since $1.1 = 1$, $1.\omega = \omega$, $1.\omega^2 = \omega^2$

Therefore $1 \in G$ is the identity element.

4) Inverse:- $1.1 = 1 \Rightarrow 1$ is inverse of 1

$\omega.\omega^2 = 1 \Rightarrow \omega^2$ is inverse of ω

$\omega^2.\omega = 1 \Rightarrow \omega$ is inverse of ω^2

∴ G is a group under multiplication.

Since, $a.b = b.a$, $\forall$ $a, b \in G$, Therefore G is an abelian Group

Example:- Show that the set $G = \{x + y\sqrt{5} \mid x, y \in \mathbb{Q}\}$ forms a group under addition.

Sol:- Closure: Let $a = x_1 + y_1\sqrt{5} \in G$ & $b = x_2 + y_2\sqrt{5}$

$a+b = (x_1+y_1\sqrt{5}) + (x_2+y_2\sqrt{5})$

$= (x_1+x_2) + (y_1+y_2\sqrt{5}) \in G$

As, $(x_1+x_2),\ (y_1+y_2) \in Q$

2) Associativity :-

$a = x_1+y_1\sqrt{5} \in G \qquad b = x_2+y_2\sqrt{5} \in G \qquad c = x_3+y_3\sqrt{5} \in G$

$(a+b)+c \Rightarrow ((x_1+y_1\sqrt{5}) + (x_2+y_2\sqrt{5})) + (x_3+y_3\sqrt{5})$

$\Rightarrow ((x_1+x_2) + (y_1+y_2)\sqrt{5}) + (x_3+y_3\sqrt{5})$

$\Rightarrow (x_1+x_2)+x_3 + ((y_1+y_2)+y_3)\sqrt{5}$

$\Rightarrow x_1+(x_2+x_3) + (y_1+(y_2+y_3))\sqrt{5}$

$\Rightarrow (x_1+y_1\sqrt{5}) + ((x_2+y_2\sqrt{5}) + (x_3+y_3\sqrt{5}))$

$\Rightarrow a+(b+c)$

$\therefore$ Associativity Holds.

3) Identity :- $0+0\sqrt{5} \in G$ is the identity element as

$(x+y\sqrt{5}) + (0+0\sqrt{5}) = x+y\sqrt{5} = 0+0\sqrt{5}+x+y\sqrt{5}$

$\forall\ x+y\sqrt{5} \in G$

4) Inverse :- for every $x+y\sqrt{5} \in G\ \exists\ (-x-y\sqrt{5} \in G) \ni$

$(x+y\sqrt{5}) + (-x-y\sqrt{5}) = 0+0\sqrt{5} = (-x-y\sqrt{5}) + (x+y\sqrt{5})$

$\therefore\ (-x-y\sqrt{5}) \in G$ is the inverse of $(x+y\sqrt{5}) \in G$

$\therefore$ G forms a group under addition.

Example :- Let $G = \{A \mid A$ is a 2x2 matrix over R$\}$ under matrix addition.

Sol :- Closure Property :- Let $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in G$, $\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in G$

Then $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix} \in G$

Therefore, closure property Holds.

→ Since, matrix addition is associative. Therefore associativity holds.

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

∴ Associativity Holds.

→ Identity :- $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in G$ is the identity element.

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

$\forall$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$

→ Inverse :- $\forall$ $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ $\exists$ $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in G \ni$

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

∴ $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in G$ is the Inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$

Therefore, G forms a group under addition.
G is an abelian group.

Example :- $G = GL(2,R)$

General Linear Group of 2×2 matrix with real enteries $\ni |A| \neq 0$

Let $G = \{A \mid A$ is 2×2 matrix over R with $|A| \neq 0\}$ under multiplication.

Sol:-

Closure:- Let $A, B \in G \Rightarrow |A| \neq 0, \ |B| \neq 0$

Then $|AB| = |A||B| \neq 0$

$\therefore$ Closure property holds.

Associativity:- Since matrix multiplication is associative

Therefore associativity Holds.

Identity:- $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ is the identity element.

as $AI = I = IA \ , \ \forall \ A \in G$

Inverse:- Let $A \in G$

$\Rightarrow A \cdot \text{adj } A = |A| \cdot I = \text{Adj } A \cdot A$

$\Rightarrow A \cdot \left[\frac{\text{Adj } A}{|A|}\right] = I = \left[\frac{\text{Adj } A}{|A|}\right] A$

$\Rightarrow A^{-1} = \frac{\text{Adj } A}{|A|} \in G$

Therefore, G forms a group under multiplication.

Since, matrix multiplication is not commutative in general.

Therefore, the group G is non-abelian

Example:-

$G = SL(2, R) = \{A \mid A \text{ is } 2 \times 2 \text{ matrix over } R \text{ with } |A| = 1\}$

= Special linear group of 2×2 matrixes A over R with $|A| = 1$

Problem:- The set of all 2×2 matrices with real entries under matrix multiplication is not a group as inverse of matrix A does not exist i.e when $|A|=0$

Example:- Let $G=\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} \mid a\in R, a\neq 0\right\}$ under matrix multiplication.

Sol:- 1) **Closure:-** Let $\begin{bmatrix} a & a \\ a & a \end{bmatrix}, \begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G$; $a,b\in R$, $a,b\neq 0$

Then $\begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} \in G$ as $2ab\neq 0$, $ab\in R$

$\therefore$ Closure Property Holds.

2) Associativity :- Since matrix multiplication is associative, Therefore associativity holds.

3) **Identity:-** Let $\begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G$ be the identity element

then $\begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$, $\forall \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G$

$\Rightarrow \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \Rightarrow 2ab = a \Rightarrow b = \frac{1}{2}$

$\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \in G$ is the identity element.

4) **Inverse:-** Let $\begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G$ and Let $\begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G$ be the inverse of $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$

$\begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$

$\begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ $\quad b = \frac{1}{4a}$.

Therefore, $\begin{bmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{bmatrix} \in G_1$ is inverse of $\begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G_1$.

Therefore G_1 is a group under multiplication.

Note :-

If $|A| = 0$, then also it can be invertable with respect to some identity element. Note that this is so, in this case the identity element is not the usual unit matrix I_2.

Remark :- Though matrix multiplication is not commutative, their may be a subset of set of matrix which is abelian.

Problem :-

Let $G = \left\{ \begin{bmatrix} a & 0 \\ 2a & 0 \end{bmatrix} \mid a \in \mathbb{Q}, a \neq 0 \right\}$ Show that G is a group w.r.t matrix multiplication.

Problem :- Show that the set of all 3×3 matrices of the form $\left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbb{R} \right\}$ is an group w.r.t matrix multiplication [Heisenberg Group]

Problem :- Show that the set of matrices $G_1 = \left\{ \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \mid \alpha \in \mathbb{R} \right\}$ forms a group under matrix multiplication.

Ques :- Show that the set G of all the rational number is an abelian Group under binary operation '$*$' defined by $a * b = \frac{ab}{2}$, $\forall\ a, b \in G_1$.

Sol:- Closure:- $a, b \in G$, $a * b = \frac{ab}{2} \in G$

$\therefore$ Closure property Holds.

Associativity:- $\forall$ $a, b, c \in G$ $(a * b) * c = \left(\frac{ab}{2} * c\right)$

$= \frac{abc}{4} = a * (b * c)$

$\therefore$ Associativity Holds.

Identity:- $2 \in G$ is the Identity as

$a * 2 = a = 2 * a$, $\forall$ $a \in G$

Inverse:- Let $b \in G$ be inverse of $A \in G$

$a * b = 2$

$\Rightarrow \frac{ab}{2} = 2$

$\Rightarrow b = \frac{4}{a} \in G$ is the inverse of $a \in G$

Therefore G forms an abelian Group under the binary operation '*'.

Some Useful Results:-

① Divison Algorithm; Let a and b be two Integers with $b > 0$, Then, $\exists$ unique integers q and r $\ni$

$\boxed{a = bq + r}$; $0 \leq r < b$

② We say that b divides a. if and only if $r = 0$ and $\underline{a = bq}$

③ Greatest common divisor $(a, b) = d$ iff (a) $\frac{d}{a}$ and $\frac{d}{b}$

(b) If $\frac{k}{a}$ and $\frac{k}{b}$, then $k \leq d$

④ If greatest common divisor (gcd) $(a,b)=1 \Rightarrow \exists$ integers x and y ∋ $ax+by=1$

$gcd(a,b)=1 \Rightarrow a$ and b are relatively prime

Example-19

Let n be a positive integer. Let $Z_n=\{0,1,2,3,\ldots,(n-1)\}$ For $a,b \in Z_n$, define the operation, $a \oplus b = c$, where 'c' is the remainder when $a+b$ is divided by n.

It is called group of integers under addition modulo n

Sol:- Let $n=5$ $Z_5=\{0,1,2,3,4\}$

⊕	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

1) By Cayley Table, closure property holds.

2) Associativity:- $\forall (a,b,c) \in Z_n$, we get $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

3) Identity:- $0 \in Z_n$ is the identity as,

$a \oplus 0 = a \quad \forall \quad a \in Z_n$

④ Inverse:-

$0 \oplus 0 = 0 \Rightarrow$ Inverse of '0' is '0'

$1 \oplus 4 = 0 \Rightarrow$ Inverse of '1' is '4'

$2 \oplus 3 = 0 \Rightarrow$ Inverse of '2' is '3'

$3 \oplus 2 = 0 \Rightarrow$ Inverse of '3' is '2'

$4 \oplus 1 = 0 \Rightarrow$ Inverse of '4' is '1'

$(Z_5, \oplus)$ is a group.

This is group under 'addition modulo ⊕'.

1) Closure:- $\forall\ a,b \in Z_n$, we have

$a+b = n\cdot q + c \quad ; \quad 0 \le c < n$

$\Rightarrow a \oplus b = c \quad , \quad c \in Z_n$

$\therefore$ Closure property holds.

2) Associativity:- Clearly, $\forall\ a,b,c \in Z_n$

$(a \oplus b) \oplus c = a \oplus (b \oplus c)$

3) Identity:- $0 \in Z_n$ is the identity as,

$a \oplus 0 = a = 0 \oplus a \quad \forall\ a \in Z_n$

④ Inverse:- $\forall\ a \in Z_n \ (a \neq 0) \quad \exists\ (n-a) \in Z_n$ s.t.

$a \oplus (n-a) = 0 = (n-a) \oplus a$,

$\therefore (n-a) \in Z_n$ is the inverse of $a \in Z_n$

→ Also inverse of $0 \in Z_n$ is zero

$\therefore Z_n$ forms a group under addition modulo n.

Note:- If we exclude 0 from above set, it will not form a group.

Example-20

Let $U_n = \{x \in Z \mid 1 \le x < n \ , \ \gcd(x,n) = 1\}$

ie $U(4) = \{1,3\}$ $\qquad U_8 = \{1,3,5,7\}$

$U(5) = \{1,2,3,4\}$

$U(6) = \{1,5\}$

Define ⊗ on U(n) by $a \otimes b = c$, where c is the remainder obtained when ab is divided by n.

① Closure:-

⊗	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Clearly, from Cayley-table closure property holds.

2) Associativity :- $\forall\ a,b,c \in U(8)$ we have

$$(a \otimes b) \otimes c = a \otimes (b \otimes c)$$

$\therefore$ Associativity Holds.

③ Identity :- $\forall\ a \in U(8)$

$$1 \otimes a = a = a \otimes 1$$

$\therefore$ $1 \in U(8)$ is the identity.

④ Inverse :-

$1 \otimes 1 = 1 \Rightarrow 1 \in U(8)$ is inverse of 1

$3 \otimes 3 = 1 \Rightarrow 3 \in U(8)$ ——— 3

$5 \otimes 5 = 1 \Rightarrow 5 \in U(8)$ ——— 5

$7 \otimes 7 = 1 \Rightarrow 7 \in U(8)$ ——— 7

$(U(8), \otimes)$ is a group.

We now show that $(U(n), \otimes)$ forms a group.

① Closure :- for $a,b \in U(n)$ let $a \otimes b = c$

To show : $c \in U(n)$

i.e. to show $1 \leq c < n$ and $\gcd(c,n) = 1$

we have, $ab = nq + c$, $0 \leq c < n$

If $c = 0$ then $ab = nq$

$\Rightarrow n \mid ab$

If $c = 0$ then $ab = nq$

$\Rightarrow n \mid a$ as $n \nmid b$ as $\gcd(n,b) = 1$ as $b \in U(n)$

But $n \nmid a$ as $\gcd(a,n) = 1$ as $a \in U(n)$

$\therefore$ $c \neq 0$

$\therefore$ $1 \leq c < n$

$\therefore$

Now, to show $\gcd(c,n) = 1$

i.e. c and n are co-prime.

i.e. there is no prime p which is dividing both c and n.

Let if possible, there is a prime p.

$\Rightarrow p \mid c$ and $p \mid n$

We have, $ab = nq + c$

$\Rightarrow p \mid ab$ [$\because p \mid n \Rightarrow p \mid nq$, $p \mid c$
$\Rightarrow p \mid nq + c \Rightarrow p \mid ab$]

$\Rightarrow p \mid a$ or $p \mid b$

If $p \mid a$ then as $p \mid n$ and $\gcd(a,n) = 1$

So, this is not possible

Also, If $p \mid b$ then as $p \mid n$ and $\gcd(b,n) = 1$

So, it is not possible.

$\Rightarrow$ So, $\gcd(c,n) = 1$

$\therefore c \in U(n)$

$\Rightarrow a \otimes b \in U(n)$

$\therefore$ closure property Holds.

2) Associativity :- $\forall a, b, c \in U(n)$ we have

$(a \otimes b) \otimes c = a \otimes (b \otimes c)$

i.e. Associativity Holds.

Identity :- $1 \in U(n)$ is the identity as,

$$a \otimes 1 = a = 1 \otimes a \quad \forall \quad a \in U(n)$$

Inverse :- Let $a \in U(n)$ [To find a^{-1}]

$\Rightarrow \gcd(a,n) = 1 \quad \exists$ integers x and $y \ni ax + ny = 1$ — ①

By division algorithm,

$$x = nq + r, \quad 0 \leq r < n$$

If $r = 0$ then $x = nq$

So from ① $anq + ny = 1$

$\Rightarrow n(aq + y) = 1$

This is not possible $n > 1$ and $aq + y \in \mathbb{Z}$

Therefore $r \neq 0 \quad \therefore \quad 1 \leq r < n$

Also r and n are co-prime

If r, n are not co-prime

$\Rightarrow \exists$ a prime $p \Rightarrow p/r$ and p/n

$\Rightarrow \frac{p}{nq} \Rightarrow \frac{p}{nq + r} \Rightarrow \frac{p}{x} \Rightarrow \frac{p}{ax}$ also $\frac{p}{n} \Rightarrow \frac{p}{ny}$

$\Rightarrow \frac{p}{ax + ny} \geq 1$

It is not possible.

Therefore r and n are co-prime and $1 \leq r < n$

$\Rightarrow r \in U(n)$

We have $x = nq + r$

$\Rightarrow ax + ny = anq + ar + ny = 1$

$\Rightarrow ar = 1 + (-aq - y)n$

$\Rightarrow a \otimes r = 1$

$\Rightarrow a^{-1} = r \in U(n)$

Problem:- Show that the set $G = \{1, 2, \ldots (n-1)\}$ forms a group w.r.t multiplication modulo n. iff 'n' is prime

Solution:- Let 'n' be prime say p.

Then, $G = \{1, 2, \ldots, (p-1)\} = U(p)$ which is a group.

Conversely, $G = \{1, 2, 3, \ldots, (n-1)\}$ forms a group under multiplication modulo n.

To show:- n is prime.

Let n be composite, say $n = rs$, $1 < r, s < n$

Now $1 < r < n \Rightarrow r \in G$ and G is group.

$\Rightarrow \exists\ t \in G \ni r \otimes t = 1$ [∵ Inverse of r is t]

$\Rightarrow rt = nq + 1$

$\Rightarrow rt = rsq + 1$

$\Rightarrow r(t - sq) = 1$

a ⊗ as $r > 1$ and $(t - sq)$ is an integer.

∴ our assumption is wrong and hence n is prime.

Problem:- Let $G = \{2^n \mid n \in \mathbb{Z}\}$. Prove that G forms an abelian group under multiplication.

Sol:-

1) **Closure:-** Let $2^n, 2^m \in G$. Then $2^n \cdot 2^m = 2^{n+m} \in G$

∴ closure property Holds

2) **Associativity:-** Since set of rational numbers always associative under multiplication. therefore associativity holds.

(3) Identity :- $2^0 \in G$ is the identity as,

$$2^n \cdot 2^0 = 2^n = 2^0 \cdot 2^n \quad \forall\, n \in \mathbb{Z}$$

4) Inverse :- for $2^n \in G$, $\exists\ 2^{-n} \in G$ $\ni$

$$2^n \cdot 2^{-n} = 2^0 = 2^{-n} \cdot 2^0$$

$\therefore$ $2^{-n} \in G$ is the inverse of $2^n \in G$.

Since, rationals are commutative under multiplication.

Therefore, G is an abelian group under multiplication.

Problem :- Prove that the set $R^n = \{(a_1, a_2, \ldots a_n) \mid a_i \in R\}$ forms a group under component-wise addition., i.e

$(a_1, a_2, \ldots a_n) + (b_1, b_2, \ldots b_n) = (a_1+b_1, a_2+b_2, \ldots a_n+b_n)$

Solution :-

1) Closure :- $\forall (a_1, a_2, \ldots a_n), (b_1, b_2, \ldots b_n) \in R^n$

$(a_1, a_2, \ldots a_n) + (b_1, b_2, \ldots b_n) = (a_1+b_1, b_2+a_2, \ldots a_n+b_n) \in R^n$

$\therefore$ Closure property holds.

2) Associativity :- $\forall (a_1, a_2, \ldots a_n), (b_1, b_2 \ldots b_n), (c_1, c_2, \ldots c_n) \in R^n$.

$$\big((a_1, a_2 \ldots a_n) + (b_1, b_2 \ldots b_n)\big) + (c_1, c_2, \ldots c_n) = (a_1+b_1, a_2+b_2 \ldots a_n+b_n) + (c_1, c_2, \ldots c_n)$$

$$= \big((a_1+b_1)+c_1, (a_2+b_2)+c_2, \ldots (a_n+b_n)+c_n\big)$$

$$= \big(a_1+(b_1+c_1), a_2+(b_2+c_2), \ldots a_n+(b_n+c_n)\big)$$

$$= (a_1, a_2, \ldots a_n) + [(b_1+c_1, b_2+c_2, \ldots b_n+c_n]$$

$$= [a_1, a_2, \ldots a_n] + [[b_1, b_2 \ldots b_n] + [c_1, c_2, \ldots c_n]]$$

$\therefore$ Associativity Holds.

Identity :- $[0,0,\ldots 0] \in R^n$ is the identity as.

$\forall\ (a_1, a_2, \ldots a_n) \in R^n$

$(a_1, a_2, \ldots a_n) + (0,0,\ldots 0) = [a_1, a_2 \ldots a_n]$

Inverse :- $\forall\ (a_1, a_2 \ldots a_n) \in R^n\ \exists\ (-a_1, -a_2, \ldots -a_n) \in R^n$

$\Rightarrow\ (a_1, a_2 \ldots a_n) + (-a_1, -a_2 \ldots -a_n) = (0,0,\ldots 0)$

$\therefore$ R^n forms a group under component wise addition.

Elementary Properties of Groups :-

Theorem :- In a group G, prove that

1) Identity element is unique

Let $e \in G$ and $e' \in G$ be the two identities.

To show. : $e = e'$

Now $e \in G$ and e' is the identity, therefore

$$ee' = e = e'e \quad - (1)$$

Also, $e' \in G$ and e is the identity, therefore,

$$e'e = e' = ee' \quad - (2)$$

From (1) & (2) we get,

$$e = e'$$

Thus, Identity element is unique

2) Inverse of each element $a \in G$ is unique.

Proof:- Let $a' \in G$ and $a'' \in G$ be the two inverse of $a \in G$

$\Rightarrow$ $aa' = e = a'a$ and $aa'' = e = a''a$ [To show $a' = a''$]

$a' = a'e = a'(aa'') = (a'a)a'' = e(a'') = a''$

$\therefore$ $\boxed{a' = a''}$

$\therefore$ Inverse of $a \in G$ is unique.

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

We know that $aa^{-1} = e = a^{-1}a \quad \forall \; a \in G$ And, $a \cdot b = e$
$\Rightarrow a^{-1} = b$

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

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

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

To prove,

$(ab)(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})(ab) \Rightarrow a(bb^{-1})a^{-1} =$

$= (ae)a^{-1} = aa^{-1} = e$

Also, $(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b$ by associativity

$(b^{-1}e)b = b^{-1}b = e$

$ab^{-1} = b^{-1}a^{-1} \quad \forall \; a, b \in G$

(5) $(a_1, a_2, \cdots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1} \cdots a_2^{-1}a_1^{-1} \quad \forall \; a_1, a_2, \cdots, a_n \in G$

We shall prove the result by induction on 'n'.

for $n = 2$, the result holds.

Let the result be true for $n = k$

i.e, $(a_1, a_2, \cdots a_k)^{-1} = a_k^{-1}a_{k-1}^{-1}, \cdots a_2^{-1}a_1^{-1}$ — (1)

To prove the result for $n = k+1$, i.e.

$(a_1, a_2 \cdots a_k, a_{k+1})^{-1} = a_{k+1}^{-1}a_k^{-1} \cdots a_2^{-1}a_1^{-1}$

L.H.S $= (a_1 a_2 \cdots a_k a_{k+1})^{-1} = ((a_1 a_2 \cdots a_k) a_{k+1})^{-1}$

$= a_{k+1}^{-1} (a_1 a_2 \cdots a_k)^{-1}$

$= a_{k+1}^{-1} a_k^{-1} \cdots a_2^{-1} a_1^{-1}$ using ①

$=$ R.H.S

⑥ $ab = ac \Rightarrow b = c$ (Left Cancellation Law)

and $ba = ca \Rightarrow b = c$ $\forall$ $a, b, c \in G$ (Right Cancellation Law)

Let $ab = ac$ $\forall$ $a, b, c \in G$

To show $b = c$

$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c$

$b = ec = c$

$b = c$

Now let $ba = ca$ $\forall$ $a, b, c \in G$

To show $b = c$

$b = be = b(aa^{-1}) = (ba)a^{-1} = (ca)(a^{-1}) = c(aa^{-1}) = ce = c$

Let G be a group and a be any element of G.

Then i) $a^0 = e$

(ii) $a^m = a \cdot a \cdot a \cdots a$ } m times $\forall$ $m \in N$

(iii) $a^{-m} = (a^{-1})^m$ $m \in N$

(iv) $a^{n+m} = a^n . a^m$, $m, n \in N$

v) $(a^n)^m = a^{nm}$ $\forall$ integers m and n.

Problem:- If in a group G, $a^2 = e$ $\forall$ $a \in G$ then show that the group G is abelian.

To show $ab = ba$, $\forall$ $a, b \in G$.

Sol:- We have $\forall$ $a \in G$, $a^2 = e \Rightarrow a^{-1}a^2 = a^{-1}e = a^{-1}$

$\Rightarrow (a^{-1}a)a = a^{-1} \Rightarrow e \cdot a = a^{-1} \Rightarrow a = a^{-1}$ ① $\forall$ $a \in G$

Since $a, b \in G \Rightarrow ab \in G$ (By closure property)

Then by ①, $(ab)^{-1} = ab \Rightarrow b^{-1}a^{-1} = ab$

$\Rightarrow ba = ab$ (Using ① $b^{-1} = b$, $a^{-1} = a$)

$\Rightarrow$ The group G is abelian.

Problem:- If in a group G, $(ab)^2 = a^2b^2$ $\forall$ $a, b \in G$. Show that the group G is abelian. and conversely.

Proof:- To show $ab = ba$, $\forall$ $a, b \in G$

Given: $(ab)^2 = a^2b^2$ $\forall$ $a, b \in G$

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

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

$\Rightarrow ba = ab$ (Using LCL and RCL)

Therefore, the group G is abelian.

Conversely, Given $ab = ba$, $\forall$ $a, b \in G$

To prove: $(ab)^2 = a^2b^2$ $\forall$ $a, b \in G$

L.H.S $(ab)^2 = (ab)(ab)$

$= a(ba)b$ (Using associative)

$= a(ab)b$ as G is abelian.

$= (aa)(bb)$ using associativity

$= a^2b^2$ = RHS

Problem:- If the group G is abelian.

Show that $(ab)^n = a^n.b^n$, $n \in \mathbb{Z}$

Solution:- Given : $ab = ba \quad \forall \; a,b \in G$

Case-1 : $n=0$

L.H.S $(ab)^0 = e$

R.H.S $a^0 b^0 = e.e = e$

L.H.S = R.H.S for $n=0$

Case-2 When n is a positive integers.

To show:- $(ab)^n = a^n.b^n$.

for $n=1$, LHS $= (ab)^1 = ab$

R.H.S $\Rightarrow a^1 b^1 = ab =$ R.H.S

Therefore result is true for $n=1$

Let the result be true for $n=k$

i.e. $(ab)^k = a^k b^k \quad -(A)$

To prove the result for $n = k+1$ i.e.

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

L.H.S $(ab)^{k+1} = (ab)^k.(ab)$

$\Rightarrow (a^k b^k)(ab)$ - Using (A)

$= a^k(b^k a)b$ using associativity.

$= a^k(ab^k)b$ as G is a abelian.

$= (a^k a)(b^k b) = a^{k+1} b^{k+1} =$ R.H.S

Therefore, by induction, $(ab)^n = a^n b^n$, $\forall \; n \in Z^+$

Case-3 : 'n' is a -ve integer.

Let $n = -m$, where $m \in Z^+$

L.H.S $= (ab)^n = (ab)^{-m} = [(ab)^m]^{-1}$

$\Rightarrow (a^m b^m)^{-1}$ as m is a +ve integer

$\Rightarrow [b^m]^{-1} \cdot [a^m]^{-1}$ as $(ab)^{-1} = b^{-1}a^{-1}$ $\forall$ $a, b \in G$

$\Rightarrow b^{-m} \cdot a^{-m} = b^n \cdot a^n = a^n \cdot b^n$ = RHS as G is abelian.

$\therefore$ $\boxed{(ab)^n = a^n b^n \quad \forall \quad n \in Z}$

Problem :- If a and b be any two elements of a group G, then prove that

$(bab^{-1})^n = ba^n b^{-1}$ $\forall$ $a, b \in G$ and $n \in Z$

Sol :- Case-1 :- $n = 0$

L.H.S $(bab^{-1})^0 = e$ R.H.S $ba^0 b^{-1} = beb^{-1} = bb^{-1} = e$

L.H.S = R.H.S for $n = 0$

Case-2 When n is +ve integer., $n \in Z^+$

For $n = 1$

LH.S $= (bab^{-1})^1 = bab^{-1} = ba^1 b^{-1} =$ R.H.S

Let the result be true for $n = k$.

i.e $(bab^{-1})^k = ba^k b^{-1}$ $\forall$ $a, b \in G$ - (A)

To prove, the result for $n = k+1$, i.e

$(bab^{-1})^{k+1} = ba^{k+1} b^{-1}$ $\forall$ $a, b \in G$

L.H.S $(bab^{-1})^{k+1} = (ba^1 b^{-1})^k (bab^{-1})$

$= [ba^k b^{-1}][bab^{-1}]$ Using A

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

$= ba^{k+1} b^{-1} =$ R.H.S.

Therefore, the result is true for $n=k+1$ and hence by induction, $(bab^{-1})^n = ba^n b^{-1}$ where $n \in Z^+$.

Case-3 : n is a -ve integer, say $n=-m$ where $m \in Z^+$.

L.H.S $= (bab^{-1})^n = (bab^{-1})^{-m} = [(bab^{-1})^m]^{-1} = [ba^m b^{-1}]^{-1}$ Using Case-2.

$\Rightarrow (b^{-1})^{-1} \cdot (a^m)^{-1} (b)^{-1} = ba^{-m} b^{-1} = ba^n b^{-1}$ = R.H.S.

Problem:- Let G be a group such that $ab = ca \ \forall \ a,b, \in G \Rightarrow b=c$

Show that the group G is abelian.

Solution:- To show :- $ab = ba \ \forall \ a,b \in G$.

$\forall \ a \in G \Rightarrow a^{-1}a = e = aa^{-1}$

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

$\Rightarrow a^{-1}(ab) = (ba)a^{-1}$ using associativity.

$\Rightarrow ab = ba$ using given hypothesis.

$\therefore$ The group G is abelian.

Problem:- Prove that a group G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1} \ \forall \ a,b \in G$

Let the group G be abelian.

i.e. $ab = ba \ \forall \ a,b \in G$

To show : $(ab)^{-1} = a^{-1}b^{-1}$

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

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

$= a(a^{-1}b)b^{-1}$ [As G is abelian]

$= (aa^{-1})(bb^{-1}) = ee = e$

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

Conversely, Given: $(ab)^{-1} = a^{-1}b^{-1} \quad \forall \quad a, b \in G$

To show: G is abelian. i.e. $ab = ba \quad \forall \quad a, b \in G$

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

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

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

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

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

$\Rightarrow a^{-1} = ba^{-1}b^{-1}$

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

$\Rightarrow a^{-1}b = ba^{-1}$

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

$\Rightarrow b = aba^{-1}$

$\Rightarrow eb = (ab)a^{-1}$

$\Rightarrow ba = (ab)a^{-1}a$

$\Rightarrow ba = ab \quad \forall \quad ab \in G$

$\Rightarrow$ Group G is abelian.

Problem:- If $a_1, a_2, \ldots a_n$ belonging to a group G, what is the inverse of $a_1 a_2 \ldots a_n$?

To show:- $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$

$(a_1 a_2 \ldots a_n)(a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1})$

$\Rightarrow a_1 a_2 \ldots a_{n-1}(a_n a_n^{-1}) a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$

$\Rightarrow a_1 a_2 \ldots a_{n-2}(a_{n-1} a_{n-1}^{-1}) a_{n-2}^{-1} \ldots a_2^{-1} a_1^{-1}$

$\Rightarrow a_1(a_2 a_2^{-1}) a_1^{-1} = a_1 a_1^{-1} = e$

$\Rightarrow (a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}$

Problem:- Let $n > 2$. Show that $U(n)$ has atleast two elements such that $x^2 = e$, where $e = 1$

Solution:- $U(n) = \{x \mid 1 \leq x < n, \gcd(x, n) = 1\}$

$\Rightarrow 1 \in U(n)$ and $1^2 = 1$

Let $\gcd(n, n-1) = d$

$\Rightarrow d/n-1$ and $d/n \Rightarrow d/n-(n-1) \Rightarrow d/1 = d = 1$

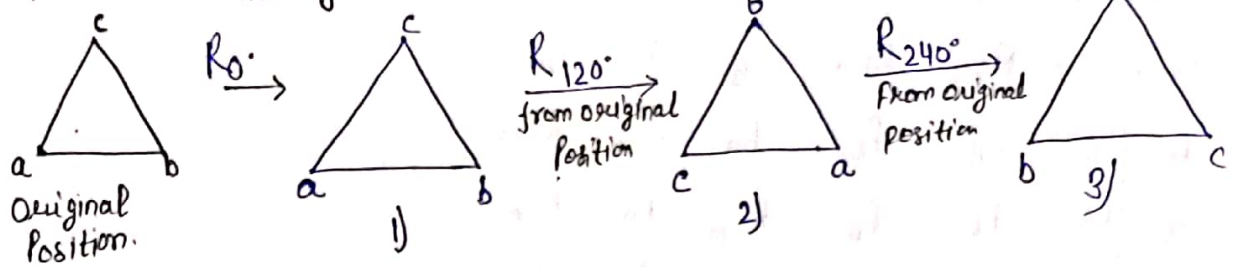
$\therefore \gcd(d, n-1) = 1$, $(n-1) \in U(n)$

$(n-1)^2 = n^2 + 1 - 2n = n(n-2) + 1 = 1$

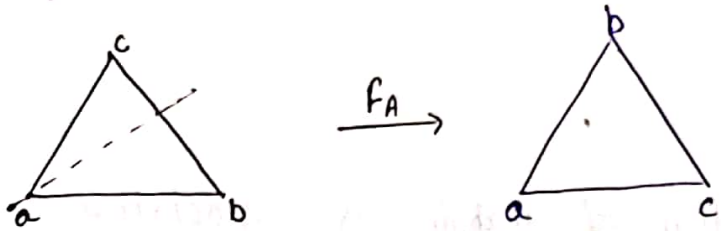
1 and $(n-1)$ in $U(n)$ $\ni 1^2 = 1$, $(n-1)^2 = 1$

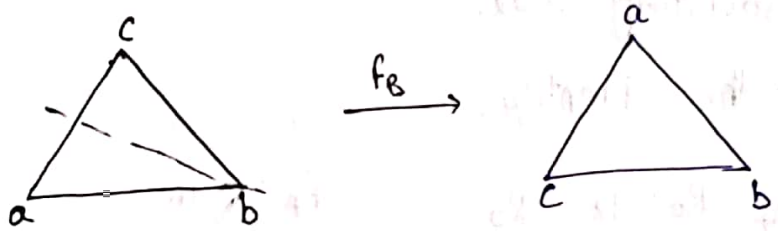
Symmetry

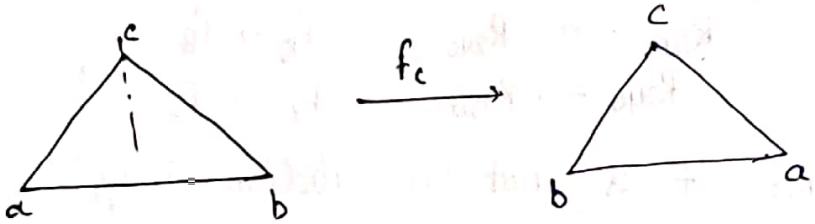
1) Rotation through 0°



Reflection about axis through vertex





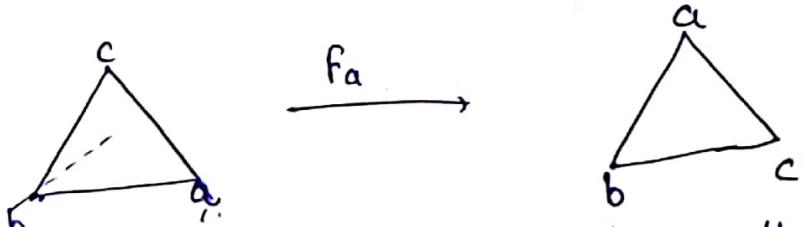


Their are 6 position.

$$S = \{R_0, R_{120}, R_{240}, f_A, f_B, f_C\}$$

$R_{120} f_A = f_C$ $\quad R_{240} R_{120} = R_0$ $\quad f_A f_C = R_{240}$ $\quad f_B R_{240} = f_A$

i.e. $fog = x$



In f_x type symmetry position matter not position of (a, b, c)

	R_0	R_{120}	R_{240}	f_A	f_B	f_C
R_0	R_0	R_{120}	R_{240}	f_A	f_B	f_C
R_{120}	R_{120}	R_{240}	R_0	f_C	f_A	f_B
R_{240}	R_{240}	R_0	R_{120}	f_B	f_C	f_A
f_A	f_A	f_B	f_C	R_0	R_{120}	R_{240}
f_B	f_B	f_C	f_A	R_{240}	R_0	R_{120}
f_C	f_C	f_A	f_B	R_{120}	R_{240}	R_0

Clearly, from cayley table,

Closure property Holds.

Associativity :- Since composition of mapping is associative, therefore associativity Holds.

Identity :- $R_0 \in G$ is the identity.

Inverse :- Inverse of R_0 is R_0

$R_{120} \longrightarrow R_{240}$

$R_{240} \longrightarrow R_{120}$

$f_A \rightarrow f_A$

$f_B \rightarrow f_B$

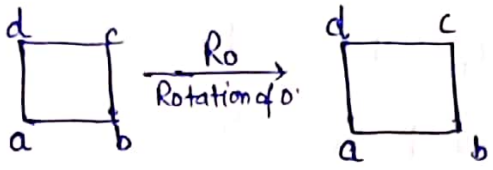
$f_C \rightarrow f_C$

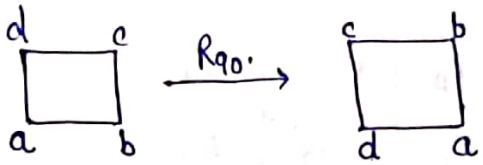
Since, $f_A f_B \neq f_B f_A$. Since it is not a abelian Group

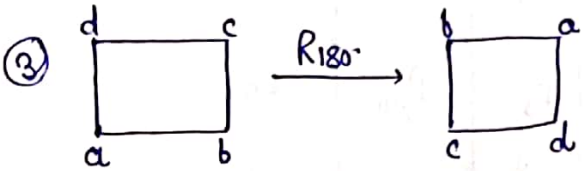
This Group is called Dihedral group.

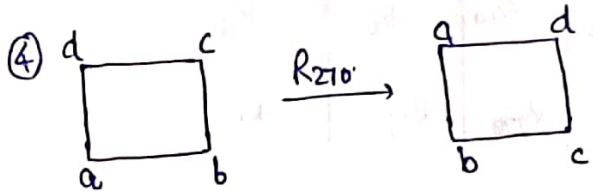
Dihedral group :- Group of symmetries of a regular n-sided polygon.

Symmetries of a Square :-

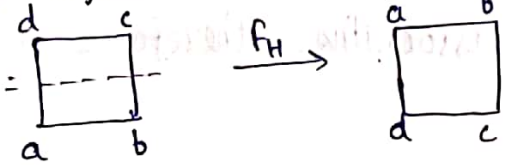
① 

② 

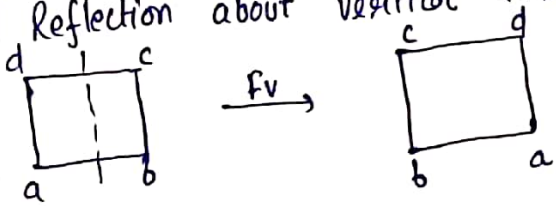
③ 

④ 

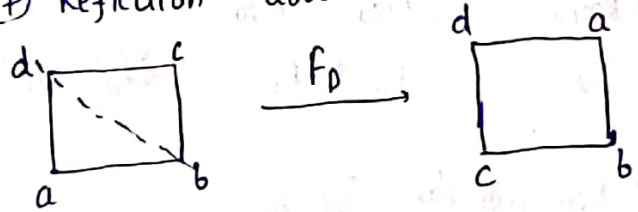
⑤ Reflection about horizontal axis



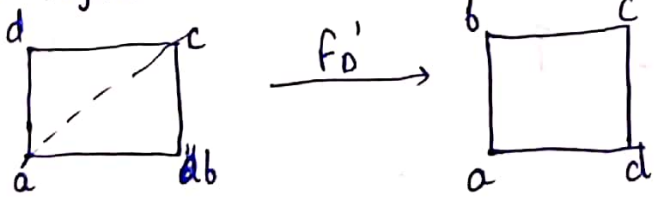
⑥ Reflection about vertical axis.



⑦ Reflection about main diagonal.



⑧ Reflection about other diagonal.



$$G_{12} = \{ R_0, R_{90}, R_{270}, R_{180}, f_H, f_V, f_D, f_D' \}$$

	R_0	R_{90}	R_{180}	R_{270}	f_H	f_V	f_D	f_D'
R_0	R_0	R_{90}	R_{180}	R_{270}	f_H	f_V	f_D	f_D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	f_D'	f_D	f_H	f_V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	f_V	f_H	f_D	f_D'
R_{270}	R_{270}	R_0	R_{90}	R_{180}	f_D	f_D'	f_V	f_H
f_H	f_H	f_D	f_V	f_D'	R_0	R_{180}	R_{90}	R_{270}
f_V	f_V	f_D'	f_H	f_D	R_{180}	R_0	R_{270}	R_{90}
f_D	f_D	f_V	f_D'	f_H	R_{270}	R_{90}	R_0	R_{180}
F_D'	F_D'	f_H	f_D	f_V	R_{90}	R_{270}	R_{180}	R_0

Clearly, from Cayley Table G is closed.

→ Since composition of mapping is associative, therefore associativity Holds.

$(f_V f_H) R_{90} = R_{180} R_{90} = R_{270}$

$f_V (f_H R_{90}) = f_V f_D' = R_{270}$

→ R_0 is the identity

→ Inverse :- $R_0 \to R_0$, $R_{90} \to R_{270}$, $R_{180} \leftrightarrow R_{180}$, $R_{270} \to R_{270}$

$f_H \to f_H$ $f_V \to f_V$ $f_D \to f_D$ & $f_D' \to f_D'$

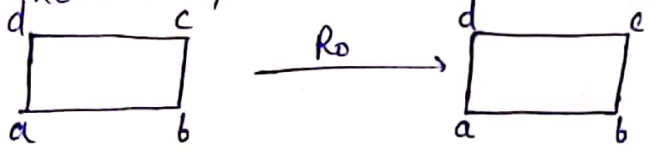
∴ G forms a group. * Non-abelian Group.

→ Dihedral group of order 8.

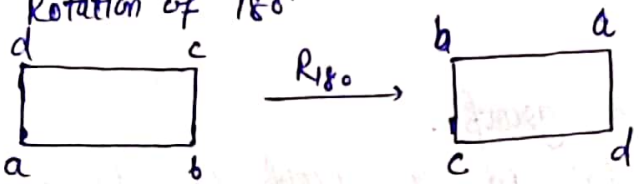
Represented by $D_4 = G = \{ \dots ? \}$

Problem:- Describe the symmetries of a non-square rectangle and construct cayley Table. Is this group Abelian.

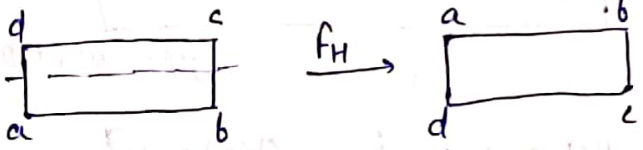
1) Rotation of 0°



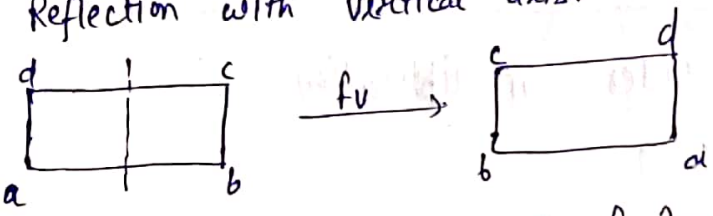
2) Rotation of 180°



3) Reflection with Horizontal axis's.



4) Reflection with vertical axis.



$G = \{ R_0, R_{180}, F_H, F_V \}$

	R_0	R_{180}	F_H	F_V
R_0	R_0	R_{180}	F_H	F_V
R_{180}	R_{180}	R_0	F_V	F_H
F_H	F_H	F_V	R_0	R_{180}
F_V	F_V	F_H	R_{180}	R_0

Chapter-2 Finite Groups and subgroups.

Order of the group :- The number of elements in a group denoted as $O(G)$ or $|G|$

$U(12) = \{1,5,7,11\}$

$O(U(12)) = 4$

Order of an element in a group.

The order of an element 'a' in a group G is the least positive integers $n \Rightarrow \boxed{a^n = e \quad \text{i.e.} \quad O(a) = n}$ for multiplicatio

for addition, $\boxed{n \Rightarrow na = e \quad \text{i.e.} \quad O(a) = n}$

(1) $G = \{1, -1, i, -i\}$ under multiplication.

$\therefore \quad O(1) = 1$ as $1^1 = 1$

$O(-1) = 2$ as $(-1)^2 = 1$

$O(i) = 4$ as $(+i)^4 = 1$

$O(-i) = 4$ as $(-i)^4 = 1$

Remark :- Order of $a = n$ if and only if,

1) $a^n = e$
2) If $a^k = e$, then $k \geq n$

→ If the element 'a' has infinite order and $a^\alpha = e$ then α must be 0.

Some Useful Results :-

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

Let $o(a)$ be 'n' [To show $o(a^{-1}) = n$]

$\Rightarrow a^n = e$ and n is the least +ve integer.

$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e.$

Let $(a^{-1})^k = e$ [To show: $k \geq n$]

$\Rightarrow a^{-k} = e \Rightarrow a^k = e^{-1} = e \Rightarrow \underline{k \geq n}$

[$\because o(a) = n$, so n is the least +ve integer $\Rightarrow a^n = e$]

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

(2) $o(x^{-1}ax) = o(a) \quad \forall \; a \in G$

Let $o(a) = n$ [To show $o(x^{-1}ax) = n$]

$\Rightarrow a^n = e$ & n is the least +ve integer.

$(x^{-1}ax)^n = xa^n x^{-1} = x^{-1}a^n x^{-1} = x^{-1}ex = x^{-1}x = e$

Now, let $(x^{-1}ax)^k = e$ [To show $k \geq n$]

$\Rightarrow x^{-1}a^k x = e \Rightarrow xx^{-1}a^k xx^{-1} = xex^{-1}$

$\Rightarrow a^k = xx^{-1} \Rightarrow a^k = e \Rightarrow k \geq n$

As order of a is 'n'.

$\therefore o(x^{-1}ax) = n = o(a)$

(3) $o(ab) = o(ba) \quad \forall \quad a, b \in G$

$ab = (b^{-1}b)ab = b^{-1}(ba)b$

Then $o(ab) = o(b^{-1}(b \cdot a)b) = o(ba)$ - [using 2]

④ Let $a^m = e$, $m \in Z^+$, then show that $o(a)$ divides m.

Let $o(a) = n$ [To show: n divides m]

By divison algorithm, $m = nq + r$, $0 \le r < n$ [To show, $r = 0$]

$\Rightarrow e = a^m = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e^q a^r = a^r$

$\Rightarrow a^r = e$ where $0 \le r < n$

Suppose $r \neq 0$ then $0 < r < n$ and $a^r = e$

So, theire is a contradiction, $o(a) = n$, so n is the least +ve integer $\ni$ $a^n = e$.

∴ Our assumption is wrong. Hence $r = 0$

∴ $m = nq = n$ divides m.

⑤ Prove that $o(a)^k = \dfrac{o(a)}{\gcd(o(a), k)}$

Let $o(a) = n \Rightarrow \gcd(o(a), k) = \gcd(n, k)$

To show :- $o(a^k) = \dfrac{n}{\gcd(n,k)}$

Let $\gcd(n,k) = d$

To show, $o(a^k) = \dfrac{n}{d}$

$(a^k)^{\frac{n}{d}} = (a^n)^{k/d} = (e)^{k/d} = e$ [As, $o(a) = n \Rightarrow a^n = e$]

Let $(a^k)^m = e$ [To show $m \ge \frac{n}{d}$]

$\Rightarrow a^{km} = e$

$\Rightarrow n / km \Rightarrow \frac{n}{d} \mid \frac{k}{d} m$

$\gcd(n,k) = d \Rightarrow \gcd\left(\frac{n}{d}, \frac{k}{d}\right) = 1$

Now, $\frac{n}{d} \mid \frac{k}{d} m$ and $\gcd\left(\frac{n}{d}, \frac{k}{d}\right) = 1$

$\Rightarrow \frac{n}{d} \mid m \Rightarrow m \geq \frac{n}{d}$

$\therefore o(a^k) = \frac{n}{d} = \frac{o(a)}{\gcd(o(a), k)}$

⑥ Prove that $o(ab) = o(a) \cdot o(b)$. If $\gcd(o(a), o(b)) = 1$ and $ab = ba$

Let $o(a) = m$ and $o(b) = n$

To show $o(ab) = mn$

$(ab)^{mn} = a^{mn} \cdot b^{mn} \Rightarrow (a^m)^n \cdot (b^n)^m \Rightarrow e^n \cdot e^m = e \cdot e = e.$

Let $(ab)^k = e$ [To show $k \geq mn$]

$a^k \cdot b^k = e$ [As G is abelian]

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

$a^{kn} = b^{kn} = (b^n)^{-k} = e^{-k} = e$

$\Rightarrow o(a) \mid kn$ by ④

$\Rightarrow m \mid kn$

$\Rightarrow m \mid k$ as $\gcd(m,n) = 1$

$a^k \cdot b^k = e \Rightarrow b^k = a^{-k} \Rightarrow b^{km} = a^{-km} = (a^m)^{-k} = e$

Now $m \mid k$, $n \mid k = \text{lcm}(m,n) \mid k$

$= mn \mid k$ [$\text{lcm}(m,n) \cdot \gcd(m,n) = mn$]

$\gcd(m,n) = 1$

$\boxed{k \geq mn}$

Problem:- If a group contains a and b such that $o(a) = 4$ $o(b) = 2$ and $a^3b = ba$. Find $o(ab)$.

$(ab)^2 = (ab)(ab) = a(ba)b = a(a^3b)b$ as $a^3b = ba$

$= a^4b^2 = e \cdot e$ as $o(a) = 4$

$o(b) = 2.$

$\Rightarrow (ab)^2 = e \quad \Rightarrow o(ab) \mid 2$, using properties (4)

$\Rightarrow o(ab) = 1$ or $o(ab) = 2$

If $o(ab) = 1 \Rightarrow ab = e$

$\Rightarrow abb^{-1} = eb^{-1}$

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

$\Rightarrow o(a) = o(b^{-1}) = o(b)$ using property (1)

$\Rightarrow o(a) \neq o(b)$

$\therefore o(ab) \neq 2$

Problem:- a) For the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ forms the special linear group $SL(2,R)$ [$SL(2,R) = \{A \mid A$ is a 2×2 matrix, $|A| = 1\}$]

Find $o(A)$, $o(B)$ and $o(AB)$

Sol:- $A^2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

$A^4 = A^2 \cdot A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

$\Rightarrow A^4 = I = o(A) = 4.$

$B^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$

$B^3 = B^2 \cdot B = B \cdot B^2 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

$\Rightarrow B^3 = I = o(B) = 3.$

$AB = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$(AB)^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$

$(AB)^3 = (AB)^2 \cdot (AB) = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$

$(AB)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$

$\Rightarrow o(AB)$ is not finite although $o(A)$ and $o(B)$ are finite.

b) For the element $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in the special linear group $SL(2,R)$. Find the order of A. If we knew 'A' as a member of $SL(2,Z_p)$ where 'p' is a prime, what is the order A?

Z_p = Modulo under p.

$= 0, 1, 2, 3, \ldots, (p-1)$

$A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \Rightarrow o(A)$ is not finite.

$A^p = \begin{bmatrix} 1 & p \\ 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$\Rightarrow o(A) = p.$

Problem:- If $o(a) = n$ and k/n Prove that :-

$o(a^{n/k}) = k$

$$o(a^{n/k}) = \frac{o(a)}{gcd(o(a), n/k)} = \frac{n}{gcd(n, n/k)} = \frac{n}{n/k} = k$$

$\boxed{o(a^{n/k}) = k}$

Problem:- If a group contains an element x such that $o(x) = 6$ Find $o(x^2)$, $o(x^3)$, $o(x^4)$, $o(x^5)$

Using :- $o(x^k) = \frac{o(x)}{gcd(o(x), k)}$

$$o(x^2) = \frac{o(x)}{gcd(o(x), 2)} = \frac{6}{gcd(6,2)} = \frac{6}{2} = 3$$

$$o(x^5) = \frac{6}{gcd(6,5)} = \frac{6}{1} = 6.$$

$$o(x^3) = \frac{6}{2} = 2$$

$$o(x^4) = \frac{6}{2} = 3$$

Let y be any other element of the group such that ~~only~~ $o(y) = 9$. Find $o(y^j) =$ for $j = 2, 3, \ldots, 8$.

$o(y^2) = \frac{9}{\gcd(9,2)} = \frac{9}{1} = 9$ $\quad$ $o(y^3) = \frac{9}{\gcd(9,3)} = \frac{9}{3} = 3$

$o(y^4) = \frac{9}{\gcd(9,4)} = 9$ $\quad$ $o(y^5) = \frac{9}{\gcd(9,5)} = \frac{9}{1} = 9$

$o(y^6) = \frac{9}{\gcd(9,6)} = \frac{9}{3} = 3$ $\quad$ $o(y^7) = \frac{9}{\gcd(9,7)} = 9$

$o(y^8) = \frac{9}{\gcd(9,8)} = \frac{9}{1} = 9$.

Note :- $SL(2,R) \leq GL(2,R)$

Subgroup :-

A non-empty subset H of a group G is said to be a subgroup of G if H is a group under the operation of G.

We denote it as $H \leq G$

→ If H is a subgroup of G, but not equal to G itself, then H is called a proper subgroup of G.

Ex :- $Z_n = \{0, 1, 2, 3, \ldots (n-1)$ is a group under $\oplus\}$

$Z = \{$ The set of integers is a group under addition. $\}$

From both the group values it looks $Z_n \leq Z$ but $Z_n \not\leq Z$ as their operation are different.

→ The group G and the singleton set $\{e\}$ are both subgroups of G, called **trivial subgroups.**

All other subgroups will be called non-trivial subgroups.

Example:- Let $G = \{1, -1, i, -i\}$, G is a group under multiplication

Let us take i) $H = \{1, -1\}$, $H \leq G$

ii) $K = \{1, -1, i\}$, K is not a group under multiplication as $-1 \times i = -i \notin K$.

and Hence, $K \not\leq G$

Subgroup Tests:-

Theorem 1:- (Two step subgroup Test)

A non-empty subset H of a group G is a subgroup of G iff (i) $a, b \in H \Rightarrow ab \in H$

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

Proof:- Let $H \leq G$, Then H is itself a group.

$\therefore$ $a, b \in H \Rightarrow ab \in H$ (closure)

Also, $a \in H \Rightarrow a^{-1} \in H$

$\therefore$ (i) & (ii) holds.

Conversely, Let (i) and (ii) holds.

To prove, H is subgroup of G. ie $H \leq G$

Clearly by (i) closure property holds.

Let $a, b, c \in H \Rightarrow a, b, c \in G$ as $H \subseteq G$

Since G is associative, therefore $(ab)c = a.(bc)$

$\therefore$ Associativity Holds.

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

Therefore $aa^{-1} \in H \Rightarrow e \in H$

Therefore H has identity.

Clearly, by (ii) $\forall$ $a \in H$, we have $a^{-1} \in H$
Therefore, H is a group and hence a subgroup of G.

Note:- Subgroups of an abelian group is also an abelian.

Theorem -2 One-step subgroup Test :-
A non-empty subset H of a group G is a subgroup of G iff $\boxed{a,b \in H \Rightarrow ab^{-1} \in H}$

Proof :- Let H be a subgroup of G.

To show :- $\forall$ $a,b \in H \Rightarrow ab^{-1} \in H$

$\Rightarrow$ H is itself a group.

Since $b \in H$ and H is a group, therefore $b^{-1} \in H$

Now, $a,b^{-1} \in H$ and H is a group, therefore by closure $ab^{-1} \in H$

Conversely, given : $\forall$ $a,b \in H \Rightarrow ab^{-1} \in H$

To show :- $H \leq G$

Associativity : Let $a,b,c \in H \Rightarrow a,b,c \in G$

And G is associative, therefore $(ab)c = a(bc)$

$\therefore$ H is a associative

Existence of identity :- Let $a \in H$

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

Existence of inverse :- Let $a \in H$, Now $a,e \in H \Rightarrow ea^{-1} \in H$

$\Rightarrow \boxed{a^{-1} \in H}$

Closure :- Let $a,b \in H$ [To show $ab \in H$]

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

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

Therefore H forms a group. and hence a subgroup of G.

Theorem 3:- (Finite Subgroup Test) :-
A non-empty finite subset H of a group G is a subgroup of G if and only if $\forall\ a,b \in H \Rightarrow ab \in H$, i.e. H is closed under the operation of G.

Proof:- Let H be a subgroup of G.
Then H is itself a group.
$\therefore \forall\ a,b \in H \Rightarrow ab \in H$ (by closure)

Converse:- Given : $\forall\ a,b \in H \Rightarrow ab \in H$
To prove :- $H \leq G$.
By Two step subgroup test, it is enough to show that :-
$a \in H \Rightarrow a^{-1} \in H$

If $a=e$, then $a^{-1} = e^{-1} = e = a \in H$
Now, let $a \neq e$ [To show $a^{-1} \in H$]
Consider, $a, a^2, a^3, a^4, \ldots \in H$, by closure
But H is finite, so $a^i = a^j$ for some $i \neq j$.
Without loss of generality $i > j$
$\Rightarrow i-j > 0 \Rightarrow i-j \geq 1$

Suppose $i-j = 1$
Then $a^i = a^j \Rightarrow a^{i-j} = e \Rightarrow a = e$
Their is a contradiction, as $a \neq e$
$\therefore i-j \neq 1$, $\therefore i-j > 1$
Now, $a^{i-j} = e \Rightarrow a^{i-j}a^{-1} = ea^{-1}$
$\Rightarrow a^{i-j-1} = a^{-1}$ where $i-j-1 \geq 1$
Since $a^{i-j-1} \in H \Rightarrow a^{-1} \in H$ $\therefore$ by two step subgroup test.

$\boxed{H \leq G}$

Problem:- Let G be an abelian group with identity e. Let $H = \{x \in G \mid x^2 = e\}$ show that $H \leq G$.

As, $e^2 = e$, so $e \in H$. Therefore H is non-empty.

Let $a, b \in H$ [To show: $ab^{-1} \in H$]

$\Rightarrow a^2 = e$, $b^2 = e$ [To show $(ab^{-1})^2 = e$]

$(ab^{-1})^2 = (ab^{-1})(ab^{-1}) = a(b^{-1}a)b^{-1}$ (using associativity.)

$= a(ab^{-1})b^{-1}$ [as G is abelian]

$= aa(b^{-1}b^{-1})$

$= a^2(b^{-1})^2 \Rightarrow e(b^2)^{-1} = ee^{-1} = e$

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

Therefore, by one step subgroup test $H \leq G$.

Problem:- Let G be an abelian group under multiplication with identity e. Let $H = \{x^2 \mid x \in G\}$ show that $H \leq G$.

For $e \in G$, $e^2 \in H$, $\therefore H \neq \phi$.

Let $a^2, b^2 \in H$ [To show: $a^2(b^2)^{-1} \in H$]

$a^2(b^2)^{-1} = a^2(b^{-1})^2 = (aa)(b^{-1}b^{-1}) = a(ab^{-1})b^{-1} = a(b^{-1}a)b^{-1}$

$= (ab^{-1})(ab^{-1}) = (ab^{-1})^2 \in H$

$\therefore$ By one-step subgroup Test $\boxed{H \leq G}$

Problem:- Let G be a group of non-zero real numbers under multiplication.

$H = \{x \in G \mid x = 1$ or x is irrational$\}$ and

$K = \{x \in G \mid x \geq 1\}$

Show that H and K are not subgroup of G.

For $\sqrt{2}, \sqrt{2} \in H$, we have $\sqrt{2}.\sqrt{2} = 2 \notin H$

$\therefore H \not\leq G$

For $2, 3 \in K$, $2.3^{-1} = 2.\left(\frac{1}{3}\right) = \frac{2}{3} \notin K$

$\therefore K \not\leq G$

Problem:- Show that a group of order 6 cannot have a subgroup of order 4.

Let G be a group $\ni o(G) = 6$

Let $H \leq G \ni o(H) = 4$

Let $x \in G \ni x \notin H$

Let $H = \{h_1, h_2, h_3, h_4\}$

Then $xH = \{xh_1, xh_2, xh_3, xh_4\}$

Now H and xH have no common element because if $h_i = xh_j$ for some i & j

$= h_i h_j^{-1} = xh_j h_j^{-1} \Rightarrow h_i h_j^{-1} = x$

$\Rightarrow x = h_i h_j^{-1} \in H$

But $x \notin H$. Therefore our assumption is wrong. Hence a group of order 6 cannot have a subgroup of order 4.

Problem:- Show that $H = \{(1,b) \mid b \in \mathbb{R}\}$ is a subgroup of the group $G = \{(a,b) \mid a \neq 0, b \in \mathbb{R}\}$ under the composition $*$ given by, $(a,b) * (c,d) = (ac, bc+d) \ \forall \ (a,b), (c,d) \in G$.

Sol:- Clearly $\in H$ is non-empty as $(1,0) \in H$

Identity in G: $(1,0) \in H$

Inverse of $(1,b) \in G$ is $(1,-b) \in G$

Let $(1,b), (1,c) \in H$ [To show: $(1,b) * (1,c)^{-1} \in H$

Problem:- Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{Z} \right\}$ ~~$= GL(2,\mathbb{Z})$~~ under addition. Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a+b+c+d=0 \right\}$

Prove that $H \leq G$. If 0 is replaced by 1, what happens?

Since $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in H$, $\therefore H \neq \phi$.

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in H$

To show :- $\begin{bmatrix} a & b \\ c & d \end{bmatrix} - \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in H$

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

$$(a-a') + (b-b') + (c-c') + (d-d') = (a+b+c+d) - (a'+b'+c'+d')$$
$$= 0 - 0 = 0$$

By one step subgroup test $H \leq G$.

→ When 0 is replaced by 1. Then $H \not\leq G$ since it does not contain identity $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Problem:- Let $G = GL(2,\mathbb{R})$. Let $H = \{A \in G \mid |A| \text{ is a power of } 2\}$. Show that $H \leq G$.

Since $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$ having determinant $4 = 2^2$

$\therefore \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \in H \quad \therefore H \neq \phi$

Let $A, B \in H$ [To show: $AB \in H$ and $A^{-1} \in H$]

$|A| = 2^n$, $|B| = 2^m$ for some integer m and n.

$|A \cdot B| = |A| \cdot |B| = 2^n \cdot 2^m = 2^{n+m} \Rightarrow AB \in H$

Also $|A^{-1}| = |A|^{-1} = 2^{-n} \Rightarrow A^{-1} \in H \quad \therefore H \leq G.$

Problem:- Let H be a subgroup of R under addition. Let $K = \{2^a \mid a \in H\}$. Prove that K is a subgroup of $R^* = R - \{0\}$ under multiplication.

Problem:- Let $H = \{a+bi \mid a,b \in R, a^2+b^2 = 1\}$ Prove or disprove that H is a subgroup of C^*. Describe the elements of H geometrically.

Since $1+0i \in H \quad \therefore H \neq \phi$

Let $(a+bi), (c+di) \in H \Rightarrow a^2+b^2 = 1 \; ; \; c^2+d^2 = 1$

To show:- $(a+bi)(c+di)^{-1} \in H$ and $(a+bi)^{-1} \in H$

$$(a+bi)(c+di) = (ac-bd) + i(ad+bc)$$

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

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

$$= a^2+b^2 = 1$$

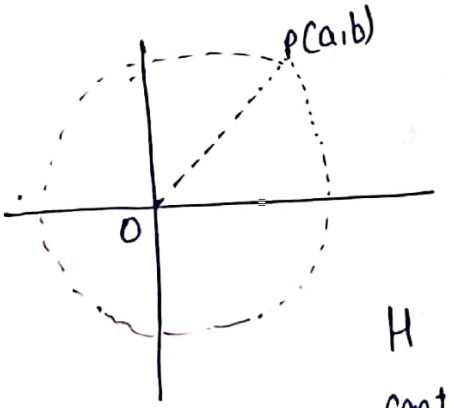
$\therefore (a+bi)(c+di) \in H$

Also, $(a+bi)^{-1} = \frac{1}{a+bi}\left[\frac{a-bi}{a-bi}\right] = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{(a^2+b^2)}i$

$= a-bi \in H$ as $a^2+b^2 = 1$

$\frac{a}{a^2+b^2}$

$\therefore H \leq C^*$



$OP = \sqrt{a^2+b^2} = 1$

Let $z = a+ib \in H$. Then

$|z|$ = Distance of the point P(z) from origin $= \sqrt{a^2+b^2} = 1$

H represents all points on the circle of radius 1, centred at the origin.

Def : Centre of a group :-

The center of a group G, i.e. $Z(G) = \{a \in G \mid ax = xa \ \forall x \in G\}$ i.e the set of all those elements 'a' in G which commute with every element of G.

Note :- G is abelian if and only if $Z(G) = G$.

Theorem :- The center of a group G is a subgroup of G.

Proof :- We have $Z(G) = \{a \in G \mid ax = xa \ \forall x \in G\}$

Since $ex = xe \ \forall \ x \in G \ \therefore e \in Z(G)$ and thus $Z(G) \neq \emptyset$

Let $(a,b) \in Z(G)$ [To show: $ab \in Z(G)$]

$\Rightarrow ax = xa \ \forall x \in G$ -①

$\Rightarrow bx = xb \ \forall x \in G$ -②

i.e. to show $(ab)x = x(ab) \ \forall x \in G$.

Consider $(ab)x = a(bx)$

$= a(xb)$ (Using -2)

$= (ax)b = (xa)b$ (using -1)

$= x(ab)$

$\therefore (ab)x = x(ab) \ \forall x \in G$

$\therefore ab \in Z(G)$

Let $a \in Z(G)$ [To show $a^{-1} \in Z(G)$ i.e $a^{-1}x = xa^{-1} \ \forall x \in G$]

$\Rightarrow ax = xa$

$\Rightarrow a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$

$\Rightarrow (a^{-1}a)(xa^{-1}) = (a^{-1}x)(aa^{-1})$

$\Rightarrow xa^{-1} = a^{-1}x$ as $a^{-1}a = aa^{-1} = e$

$\Rightarrow a^{-1} \in Z(G)$

$\therefore$ By two step subgroup test

$Z(G) \leq G$.

Def:- Centralizer of an element in a group.

Let 'a' be a fixed element of a group. The centralizer of the element 'a' in the group G is,

$$C_G(a) = \{ g \in G \mid ga = ag \}$$

Theorem:-

For each 'a' in a group G, the centralizer of 'a' is a subgroup of G.

Proof:-

We have $C_G(a) = \{x \in G \mid xa = ax\}$

Since $ea = ae \Rightarrow e \in C_G(a)$, $\therefore C_G(a) \neq 0$

Let $x, y \in C_G(a)$ [To show: $xy^{-1} \in C_G(a)$]

$\Rightarrow xa = ax$ -① i.e $(xy^{-1})a = a(xy^{-1})$

$\Rightarrow ay = ya$ -②

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

$= x(ay^{-1}) = (xa)y^{-1} = (ax)y^{-1}$ (using ①)

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

[We have $ya = ay$ (using 2)
$\Rightarrow y^{-1}(ya)y^{-1} = y^{-1}(ay)y^{-1}$
$\Rightarrow y^{-1}y(ay) = (y^{-1}a)(yy^{-1})$
$ay^{-1} = y^{-1}a$]

$\therefore (xy^{-1})a = a(xy^{-1}) \Rightarrow xy^{-1} \in C_G(a)$

$\therefore C_G(a) \leq G.$

Ques:- Let G be a group and $a \in G$ Prove that,

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

Def:- Let G be a group. Let $H \leq G$ and $x \in G$. Then,

$xHx^{-1} = \{xhx^{-1} \mid h \in H\}$ is called a conjugate of the subgroup H.

Theorem:- Let G be a group, Let $H \leq G$ and $x \in G$. Then xHx^{-1} is a subgroup of G.

Proof:- Let $a, b \in xHx^{-1}$

$\Rightarrow a = xh_1x^{-1}$, $h_1 \in H$

$b = xh_2x^{-1}$, $h_2 \in H$

Then $(ab) = (xh_1x^{-1})(xh_2x^{-1})$

$= xh_1(x^{-1}x)h_2x^{-1}$

$= xh_1h_2x^{-1} \in xHx^{-1}$ as $h_1h_2 \in H$

Now, $a = xh_1x^{-1} \in xHx^{-1}$

$a^{-1} = (xh_1x^{-1})^{-1} = (x^{-1})^{-1}h_1^{-1}x^{-1}$

$= xh_1^{-1}x^{-1} \in xHx^{-1}$ (as $h_1^{-1} \in H$)

[Also, $xex^{-1} \in xHx^{-1} \Rightarrow e \in xHx^{-1}$

$\therefore xHx^{-1} \neq \phi$.]

Therefore by two-step subgroup test $xHx^{-1} \leq G$.

Def:- Let G be a group. Let $H \leq G$, Then normalizer of subgroup H in G is defined as,

$N_G(H) = \{x \in G \mid xHx^{-1} = H\}$

Theorem:- For any subgroup H of a group G, $N_G(H)$ is a subgroup of G.

Proof:- Since $eHe^{-1} = H \Rightarrow e \in N_G(H)$.

$\therefore N_G(H)$ is non-empty.

Let $x, y \in N_G(H)$

To show: $xy \in N_G(H)$

$\Rightarrow xHx^{-1} = H$ and $yHy^{-1} = H$

To show: $(xy)H(xy)^{-1} = H$

$$(xy)H(xy)^{-1} = (xy)H(y^{-1}x^{-1})$$
$$= x(yHy^{-1})x^{-1} = xHx^{-1} = H$$

$\therefore (xy)H(xy)^{-1} = H$

$\therefore xy \in N_G(H)$

Let $x \in N_G(H)$ [To show: $x^{-1} \in N_G(H)$]

$\Rightarrow xHx^{-1} = H$

To show: $x^{-1}H(x^{-1})^{-1} = H$

$\Rightarrow x^{-1}(xHx^{-1})x = x^{-1}Hx$

$H = x^{-1}Hx$

$H = x^{-1}H(x^{-1})^{-1}$

$\therefore N_G(H) \leq G$.

Def:- Let G be a group. Let $H \leq G$, then centralizer of subgroup H is defined as,

$$C_G(H) = \{x \in G \mid xh = hx \ \forall \ h \in H\}$$

i.e. the set of all those element of G which commute with every element of H.

Theorem:- For any sub-group H of a group G, $C_G(H)$ is a subgroup of G.

Proof:- $C_G(H) = \{x \in G \mid xh = hx \ \forall \ h \in H\}$

Since $eh = he \ \forall \ h \in H \Rightarrow e \in C_G(H)$

$\therefore \ C_G(H) \neq \phi$.

Let $x_1, x_2 \in C_G(H)$ [To show: $(x_1 x_2^{-1})h = h(x_1 x_2^{-1}) \ \forall \ h \in H$]

$(x_1 x_2^{-1})h = x_1(x_2^{-1}h) = x_1(hx_2^{-1})$

[As $x_2 \in C_G(H) \Rightarrow x_2 h = hx_2 \Rightarrow x_2^{-1}x_2 h x_2^{-1} = x_2^{-1} h x_2 x_2^{-1}$

$\Rightarrow h x_2^{-1} = x_2^{-1} h$]

$= (x_1 h)x_2^{-1} = (h x_1)x_2^{-1}$. [As $x_1 \in C_G(H) \Rightarrow x_2 h = h x_1$]

$= h(x_1 x_2^{-1})$

$\Rightarrow x_1 x_2^{-1} \in C_G(H)$

$\therefore \ C_G(H) \leq G$

Def:-

Let G be a group and let $a \in G$.

Let $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

$\langle a \rangle$ is called the cyclic subgroup of the group G generated by 'a'.

Cyclic Groups.

Def:- Let G be a group and let $a \in G$

let $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{a^1, a^2, a^3, \ldots a^0, a^{-1}, a^{-2} \ldots\}$

$\langle a \rangle$ is called cyclic subgroup of the Group G generated by 'a'.

→ A group G is called a cyclic group if $\exists$ an element 'a' in G such that every element of G is an integral power of a.

Then G is said to be generated by a, and a is called generator of G.

We write $G = \langle a \rangle$

So, if G is a cyclic group generated by a, then

$$G = \{a^n \mid n \in \mathbb{Z}\}$$

If G is a cyclic group under addition, then

$$G = \{na \mid n \in \mathbb{Z}\}$$

$$na = \underbrace{a + a + a + \cdots + a}_{n \text{ times}}$$

1) Let $G = \mathbb{Z}$ under addition.
Then $\mathbb{Z} = \langle 1 \rangle$ and $\mathbb{Z} = \langle -1 \rangle$

2) $(\mathbb{Z}_8, \oplus) = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$\mathbb{Z}_8 = \langle 1 \rangle$

3) $U_8 = \{1, 3, 5, 7\}$ is not a cyclic as there doesnot exist any $R \in U(8)$ such that U_8

④ $(m\mathbb{Z}, +)$

$(2\mathbb{Z}, +) = \{2k \mid k \in \mathbb{Z}\}$

$= \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$

Generated by: $\langle 2 \rangle$ and $\langle -2 \rangle$ is a cyclic group.

⑤ $U(20) = \{1, 3, 6, 7, 9, 11, 13, 17, 19, \otimes_{20}\}$

$\langle 3 \rangle = \{3, 9, 7, 1\} \neq U(20)$

$\langle 7 \rangle \neq U(20)$

$\langle 9 \rangle = \{9, 1\} \neq U(20)$

$\langle 11 \rangle = \{11, 1\} \neq U(20)$

$\langle 13 \rangle = \{13, 1, 9, 7\} \neq U(20)$

$\langle 17 \rangle \neq U(20)$

$\langle 19 \rangle \neq \{19, 1\} \neq U(20)$

⑥ $U(14) = \{1, 3, 5, 9, 11, 13\}$

$\langle 3 \rangle = \{1, 3, 9, 13, 11, 15\} = U(14)$

Theorem :-

Every cyclic group is abelian, but not conversely.

Proof :- Let G_1 be a cyclic group.

Let $G_1 = \langle a \rangle$

Let $x, y \in G_1$

$\Rightarrow x = a^s, \quad y = a^r \quad ; \quad r, s \in \mathbb{Z}$

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

$xy = yx$

$U(8)$ is an abelian group but not cyclic.

Theorem :- Let G be a group and let $a \in G$

1) If a has infinite order, then all distinct powers of 'a' are distinct powers of a are distinct group elements.

2) If a has finite order n, then

$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ iff $n/i-j$

for example $U(8) = \{1, 3, 5, 7, \otimes_8\}$

$O(3) = 2$

$\langle 3 \rangle = \{3^0, 3^1, 3^2, \ldots\}$

$= \{1, 3\}$ a finite groups.

Proof :- 1) Let a has infinite order then, there is no non-zero 'n' such that $a^n = e$

Let $a^i = a^j$ for $i \neq j$

$\Rightarrow$ ~~$a^i = a^j$~~ if $a^{i-j} = e$

$\Rightarrow$ $i - j = 0$ as a infinite order.

$\Rightarrow$ $i = j$ a contradiction,

This implies that all distinct power of a, distinct group elements.

2) Let $o(a) = n \Rightarrow$ n is least +ve integers such that,

$a^n = e$

We first show that $e, a, a^2, \ldots, a^{n-1}$ are all distinct.

Let $a^i = a^j$; $i, j \in \{0, 1, 2, \ldots, (n-1)\}$

$i \neq j$

Let $i > j$ then $i - j \in \{0, 1, 2, \ldots (n-1)\}$

$a^i = a^j \Rightarrow a^{i-j} = e$

and $i - j < n$

A contradiction as $o(a) = n$, the least positive integer.

$\Rightarrow$ $a^i \neq a^j$ for $i \neq j$

Let $a^k \in \langle a \rangle$

Applying division algorithm, to k and n, $\exists\ q, r \in \mathbb{Z}$ such that, $R = nq + r$

$$a^k = a^{nq+r}$$
$$a^k = a^{nq} \cdot a^r$$
$$a^k = (a^n)^q \cdot a^r$$
$$a^k = a^r \cdot e^q$$
$$a^k = a^r \quad \text{with} \quad 0 \leq r < n$$

a^k is of the form $a^0, a^1, a^2, \ldots a^{n-1}$

$\Rightarrow$ $a^k \in \{e, a, a^2, \ldots, a^{n-1}\}$

$\langle a \rangle \subseteq \{e, a, a^2, \ldots, a^{n-1}\}$

Also, i-e $\{e, a, \ldots, a^{n-1}\} \subseteq \langle a \rangle$

$\Rightarrow$ $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$

To show, $a^i = a^j \Rightarrow a^{i-j} = e$

Applying division algorithm to, $(i-j)$ and n $\exists\ q, r \in \mathbb{Z}$ such that,

$$i - j = nq + r, \quad 0 \leq r \leq n$$
$$a^{i-j} = a^{nq+r}$$
$$e = (a^n)^q a^r$$
$$e = e^q a^r$$
$$e = a^r$$
$$a^r = e$$

Since n is the least positive integer such that $a^n = e$

$\therefore$ we must have $r = 0$

$\Rightarrow \quad i - j = nq$

$\underline{n \mid i-j}$ $\square$

Conversely, let $n \mid i-j$

$i - j = nq \quad , q \in \mathbb{Z}$

$a^{i-j} = a^{nq} = (a^n)^q = (e)^q = e$

$a^{i-j} = e$

$a^i = aj$

Corollary:- Let G be a group. Let $a \in G$ such that $o(a) = n$

If $a^k = e$, then $n \mid k$.

Lemma:- If $a \in \langle a^k \rangle$, then $\langle a \rangle \subseteq \langle a^k \rangle$

Example:- $(Z_8, \oplus)$

$\langle 3 \rangle = \{0, 3, 6, 1, 4, 7, 2, 5\}$

$2 \in \langle 3 \rangle$

$\langle 2 \rangle = \{0, 2, 4, 6\} \subseteq \langle 3 \rangle$

$\langle 4 \rangle = \{0, 4\} \quad \subseteq \langle 2 \rangle$

Proof:- Let $x \in \langle a \rangle \Rightarrow x = a^m$, $m \in \mathbb{Z}$

Now $a \in \langle a^k \rangle \Rightarrow a = (a^k)^p$, $p \in \mathbb{Z}$

$x = a^m = (a^{kp})^m = (a^k)^{mp}$

$\in \langle a^k \rangle$

$\langle a \rangle \subseteq \langle a^k \rangle$

Theorem:- Let $G_1 = \langle a \rangle$ be a cyclic group of order n. Then $G_1 = \langle a^k \rangle$ iff $\gcd(k,n) = 1$

Proof:- Let $G_1 = \langle a \rangle$ be a cyclic group of order n.

i.e. $O(G_1) = o(\langle a \rangle) = o(a) = n$

As, $o(a) = n \Rightarrow a^n = e$

Let $G_1 = \langle a^k \rangle \Rightarrow o(a^n) = o(a^k) = n$

To Show, $\gcd(k,n) = 1$

$\gcd(k,n) = d > 1$

$\Rightarrow d|k, \; d|n$

$\Rightarrow k = sd \quad n = td$, $t, s \in \mathbb{Z}$

Now, $(a^k)^t = (a^{sd})^t$

$= (a^{td})^s = (a^n)^s = e^s = e$

Now, $o(a^k) = n$ and $t < n$

A contradiction, $\gcd(k,n) = 1$

Converse:-

Let $\gcd(k,n) = 1$

$\exists \; u, v \in \mathbb{Z}$ such that

$uk + vn = 1$

$a = a^1 = a^{uk+vn}$

$a = a^{uk} a^{vn}$

$a = (a^{uk})(a^n)^v = (a^{uk}) e^v = a^{uk}$

$\Rightarrow a = a^{ku} = (a^k)^u$

$a \in \langle a^k \rangle$

By lemma, $\langle a \rangle \subseteq \langle a^k \rangle$

$\Rightarrow G_1 \subseteq \langle a^k \rangle$

Also, $\langle a^k \rangle \subseteq G_1 \Rightarrow G_1 = \langle a^k \rangle$

Example:- $U(14) = \{1, 3, 5, 9, 11, 13\}$

$U(14) = \langle 3 \rangle$

$n = 6$, $k = 1, 5$

$\langle 3^1 \rangle$ $\langle 3^5 \rangle$

$\{3\}$ $\{5\}$

Corollary:- An integer $k \in Z_n$ is a generator of Z/n iff $\gcd(k, n) = 1$

$Z_8 = \{6, 1, 2, \ldots 7\}$

$= \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

$Z_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$