GROUP THEORY:

Groupoid or Binary Algebra: Definition
A non empty set 'G' equipped with one binary operation '*' is called 'groupoid'.
i.e G is a groupoid if G is closed for *
It is denoted by $(G, *)$

→ Close means like in natural numbers →
$N = \{1, 2, 3 - - -\}$
If we take any two numbers and add them or multiply them, the output will also belong to natural numbers.
Eg: $3 + 4 = 7 \in N$
$3 * 4 \in 12 \in N$
(So these two numbers are closed in addition or multiplication operations. This is true for any number in the natural numbers.

Now, $3 - 4 = -1 \notin N$
So, it is not closed in subtraction or division
$3 \div 4 = 0.7 \notin N$

→ The integers → $Z = \{-- 2, -1, 0, 1, 2 --\}$
Its closed for addition, subtraction, multiplication but not division

For Eg: $(N, +)$, $(Z, -)$, $(Q, \times)$ etc.
Note: Groupoid is also called quasi group

Semi Group: Definition

An algebraic structure $(G, *)$ is called semi group if the binary operation $*$ satisfies associative property. i.e

[G_1] $(a*b)*c = a*(b*c)$, $\forall\ a \in G$

Eg: The algebraic structures $(N, +)$, $(Z, +)$, $(Z, \times)$, $(Q, \times)$ are semi groups but the structure $(Z, -)$ is not so because Subtraction $(-)$ is not associative.

Eg: The structures $(P(S), \cup)$ and $(P(S), \cap)$ where $P(S)$ is the power set of a set S are semi groups as both the operations union $(\cup)$ and intersection $(\cap)$ are associative.

Monoid: Definition:

A semi group is called <u>monoid</u> if there exists any identity element 'e' in G such that:

$$e*a = a*e = a \quad \forall\ a \in G$$

Eg: $N = \{1, 2, 3, 4 - -\}$
Generally, additive identity is 0 as 0 + any number is that number. But natural numbers do not have additive identity because $0 \notin N$.

Eg 1: The semi group $(N, *)$ is a monoid because 1 is the identity for multiplication

But semi group $(N, +)$ is not because 0 is identity for addition but is not present in N.

Eg 2: The semigroups $(P(S), \cup)$ and $(P(S), \cap)$ are monoid because ϕ and S are the identities respectively for union ($\cup$) and intersection ($\cap$) is $P(S)$

$$\boxed{N \subset Z \subset Q \subset R \subset C}$$

Group: Definition
An algebraic structure of set G and a binary operation * defined in G i.e. $(G, *)$ is called a group if * satisfies the following postulate.

[G_1] Closure: $a \in G, b \in G \Rightarrow a * b \in G \ \forall a, b \in G$

[G_2] Associatively: The composition * is associative in G i.e.
$(a * b) * c = a * (b * c) \ \forall \ a, b, c \in G$

[G_3] Existence of identity: There exist an identity element e in G such that,
$e * a = a * e = a \ \forall \ a \in G$

[G_4] Existence of inverse: Each of element of G is invertible, i.e for every $a \in G$, there exists a^{-1} in G such that

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

Eg: $-2 + 2 = 0$

Inverse element for addition

$2 \times \frac{1}{2} = \underbrace{1}_{\text{multiplicative identity}}$

- $(N, +)$ → ✗ Not a group
  [0 is not an identity
- $(N, \times)$ → ✗ Not a group
  as Eg: $\underbrace{\frac{1}{2}}_{\notin N} \times 2 = 1$

  $\frac{1}{2} \notin N$

In natural numbers multiplicative inverse does not exist.

- $(Z, +)$ → ✓ Is a group
  Eg: $-3 + 3 = 0$
  [Additive inverse exists. Rest all conditions also fulfilled]
- $(Z, \times)$ → ✗ Not a group
  Eg: $3 \in Z$

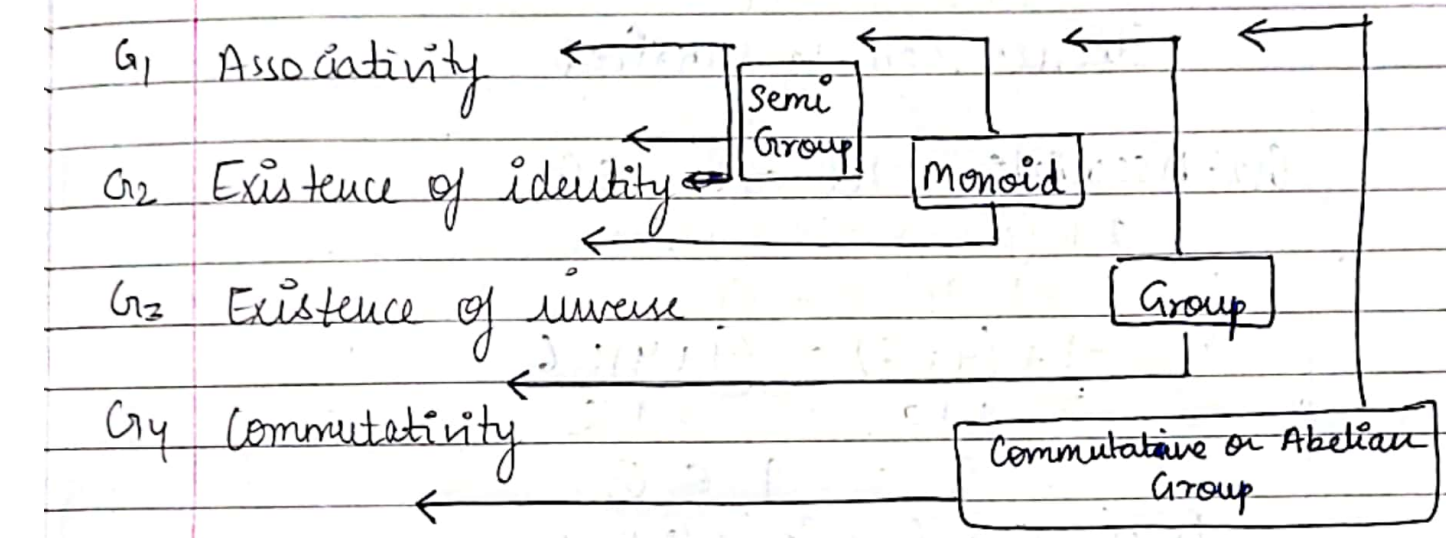
  $3 \times \frac{1}{3} \in Z$, $\frac{1}{3} \notin Z$

Thus a group $(G, *)$ is a monoid in which each of its element has its inverse present in it.

Abelian Group or Commutative group: Definition

A group $(G, *)$ is said to be abelian or commutative if $*$ is commutative also A group $(G, *)$ is an abelian group if:
(Always closed group)

$[G_4]$ Commutativity: $a * b = b * a, \forall a, b \in G$



Finite and Infinite Groups:

A group $(G, *)$ is said to be finite if its underlying set G is a finite set and a group which is not finite is called infinite group

Order of a group: Definition

The number of elements in a finite group is called the order of the group.
It is denoted by $O(G)$
If $(G, *)$ is an infinite group, then it is said to be of infinite order.

Q1) Show that the set of integers form an abelian group under addition.

$Z = \{ \cdots -2, -1, 0, 1, 2, \cdots \}$

Let $G = \{ \cdots -2, -1, 0, 1, 2 \cdots \}$

G_1: Closure: Let $a, b \in G \Rightarrow a+b \in G$

Eg: $1, 2, \in G$

$1+2 = 3 \in G$

Closure law is satisfied

G_2: Associative: Let $a, b, c \in G$

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

Eg: $-1, 4, 6 \in G$

$-1 + (4+6) = (-1+4) + 6$

$-1 + 10 = 3 + 6$

$9 = 9 \in G$

Associative law is satisfied

G_3: Identity: Let $a \in G$ and 0 be the identity

$a + 0 = 0 + a = a$

Eg: $3, 0 \in G$

$3 + 0 = 0 + 3 = 3 \in G$

G_4: Inverse: $-a$ is the inverse of a, $a, -a \in G$

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

Eg: $2, -2, 0 \in G$

$2 + (-2) = (-2) + 2 = 0$

G_5: Commutative: Let $a, b \in G$

$a + b = b + a$

$\therefore (G, +)$ is a abelian group under addition

(Q2) G is the set of rationals except -1 binary operation * is defined by $a*b = a+b+ab$.
Show that it is a group.
$G = Q - \{-1\}$

G_1: Let $a, b \in G \Rightarrow a*b = ab+a+b \in G$
Closure is satisfied.

G_2: Let $a, b, c \in G$
$a*(b*c) = a*(b+c+bc)$
$= a + b + c + bc + a(b+c+bc)$
$= a + b + c + bc + ab + ac + abc$ — ②

$(a*b)*c = (a+b+ab)*c$
$= a + b + ab + c + c(a+b+ab)$
$= a + b + c + ab + ac + bc + abc$ — ①
from ① and ②
$a*(b*c) = (a*b)*c$
Associative law is satisfied.

G_3: Let $a \in G$ and e be the identity
$a*e = e*a = a$
$a + e + ae = e + a + ea = a$
$a + e + ae = e + a + ae$
Identity is satisfied
$a + e + ae = a$
$e(a+1) = 0$
$e = 0 \quad (a \neq -1)$

G_4: Let $a \in G$ and a^{-1} be inverse of a.

$a * a^{-1} = a^{-1} * a = e$

$a + a^{-1} + a a^{-1} = a + a^{-1} + a a^{-1} = 0$

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

Inverse is satisfied

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

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

$a^{-1} = \frac{-a}{1+a}$ ($a \neq -1$, and anyways is given in Q, but write in other Q's)

$\therefore (G, *)$ is a group

Q3) In Z we define $a * b = a + b + 1$ Show that $(Z, *)$ is an abelian group

G_1: $a, b \in Z \Rightarrow a * b = a + b + 1 \in Z$

Closure is satisfied

G_2: Let $a, b, c \in Z$

$(a * b) * c = (a + b + 1) * c$

$= a + b + 1 + c + 1$

$= a + b + c + 2$ — ①

$a * (b * c) = a * (b + c + 1)$

$= a + b + c + 1 + 1$

$= a + b + c + 2$ — ②

From ① and ②

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

Associative law is satisfied

G_3: Identity: Let $a \in Z$ and e be identity

$a * e = e * a = a$

$a + e + 1 = e + a + 1 = a$

Identity is satisfied

$a+e+1 = a$

$e = -1 \in Z$

$a+e+1 = e+a+1 \Rightarrow$

Identity is satisfied

G_4: Let $a \in Z$ and a^{-1} be inverse of a

$a * a^{-1} = a^{-1} * a = e$

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

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

$a^{-1} = -2 - a$

$a^{-1} = -(2+a) \in Z$

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

Inverse is satisfied

G_5: Let $a, b \in Z$

$a * b = b * a$

$a + b + 1 = b + a + 1$

∴ Commutative is satisfied

$(Z, *)$ is an abelian group

Q4) Let G be the set of all positive rational numbers and $*$ be the binary operation on G defined by $a * b = \frac{ab}{7} \forall a, b \in G$. Prove that G is abelian group. Solve $3 * x = 2^{-1}$ in G.

G_1: let $a, b \in G \Rightarrow a * b = \frac{ab}{7} \in G$

Closure is satisfied.

G_2: Let $a, b, c \in G$

$a * (b * c) = a * \frac{bc}{7} = \frac{abc}{49}$

$(a * b) * c = \frac{ab}{7} * c = \frac{abc}{49}$

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

Associative law satisfied

G_3: Identity: Let $a \in G$ and e be identity

$a * e = e * a = a$

$\frac{ae}{7} = \frac{ea}{7} = a$

$\frac{ae}{7} = \frac{ea}{7}$

Identity is satisfied.

$\frac{ae}{7} = a$

$\boxed{e = 7}$

G_4: Let $a \in G$ such that a^{-1} is inverse of a

$a * a^{-1} = a^{-1} * a = e$

$\frac{aa^{-1}}{7} = \frac{a^{-1}a}{7} = 7$

$\frac{a^{-1}a}{7} = \frac{aa^{-1}}{7}$

Inverse is satisfied.

$\frac{aa^{-1}}{7} = 7$

$a^{-1} = \frac{49}{a}$

Q5: Let $a, b \in Q$

$$a * b = b * a$$

$$\frac{ab}{7} = \frac{ba}{7}$$

Commutative is satisfied.

Now $3 * x = 2^{-1}$

$$a = \frac{a}{49} \Rightarrow 2^{-1} = \frac{2}{49}$$

$$3 * x = 3x/7$$

$$\therefore \frac{3x}{7} = \frac{2}{49}\ 7$$

$$x = \frac{2}{21}$$

Now $3 * x = 2^{-1}$

$$a^{-1} = \frac{49}{a} \Rightarrow 2^{-1} = \frac{49}{2}$$

$$3 * x = 3x/7$$

$$\therefore \frac{3x}{7} = \frac{49}{2}$$

$$\boxed{x = \frac{343}{6}}$$

Q5) Show that cube root of unity is an abelian group under multiplication.

$$x = \sqrt[3]{1}$$

$$x = 1^{1/3}$$

$$x^3 = 1$$

$$x^3 - 1 = 0$$

$$(x-1)(x^2 + x + 1) = 0$$

$$x = 1, \frac{-1 \pm \sqrt{3}i}{2}$$

$$x = 1, \omega, \omega^2$$

$(\omega^3 = \omega \cdot \omega^2 = 1, \ 1 + \omega + \omega^2 = 0)$

Cayley's table →

X (multiplication)	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

The above entries in the table is satisfying all axioms.

G_1: Let $a, b \in G$, $a \cdot b \in G$.
Closure is satisfied

G_2: Let $a, b, c \in G$
$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
$abc = abc$
Associative is satisfied.

G_3: 1 in the top row indicates the identity element
Let $a \in G$,
$a \cdot 1 = 1 \cdot a = a \quad (e = 1)$
Identity is satisfied.

G4: Let $(1)^{-1} = 1$

$\omega^{-1} = \omega^2$

$(\omega^2)^{-1} = \omega$

Inverse of all elements is present

$\therefore$ Inverse is satisfied.

G5: Let $a, b \in G$

As the Cayley matrix is symmetric,

$a \cdot b = b \cdot a$

$\therefore$ Commutative is satisfied

$(G, *)$ is an abelian group under multiplication.

(Q6) If $G = \{f_1, f_2, f_3, f_4\}$ of four functions defined by $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = \frac{1}{x}$, $f_4(x) = -\frac{1}{x}$ $\forall x \in R - \{0\}$ is an abelian group

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Let $x \in R - \{0\}$

$f_1 \circ f_1 = f_1(f_1(x)) = f_1(x) = x = f_1$

$f_1 \circ f_2 = f_1(f_2(x)) = f_1(-x) = -x = f_2$

$f_1 \circ f_3(x) = f_1(f_3(x)) = f_1\left(\frac{1}{x}\right) = \frac{1}{x} = f_3$

$f_1 \circ f_4(x) = f_1(f_4(x)) = f_1\left(-\frac{1}{x}\right) = -\frac{1}{x} = f_4$

$f_2 \circ f_1 = f_2(f_1(x)) = f_2(x) = -x = f_2$

$f_2 \circ f_2 = f_2(f_2 x) = f_2(-x) \Rightarrow x = f_1$

$f_3 \circ f_2 = f_3(f_2(x)) = f_3(-x) \Rightarrow -\frac{1}{x} = f_4$

(Like this check all and add to the table)

→ The above entries in the composition table satisfy all the axioms.

G_1: Let $a, b \in G$, $a \circ b \in G$

Closure is satisfied

G_2: Let $a \circ (b \circ c) = (a \circ b) \circ c$

Eg: $(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$

$f_2 \circ f_3 = f_1 \circ f_4$

$f_4 = f_4$

Associative is satisfied.

G_3: f_1 is the top row indicates the identity $(e = f_1)$

$a \circ f_1 = f_1 \circ a = a \quad (a \in G)$

Identity is satisfied.

G_4: Let $(f_1)^{-1} = f_1$, $(f_2)^{-1} = f_2$

$(f_3)^{-1} = f_3$, $(f_4)^{-1} = f_4$

Inverse of all elements is present

∴ Inverse is satisfied

G_5: Let $a, b \in G$

$a \circ b = b \circ a \in G$ (As the comparison matrix is symmetric)

∴ Commutative is satisfied

$(G, \circ)$ is an abelian group under composition

Q7) Show that the fourth roots of unity is an abelian group under multiplication

$x = \sqrt[4]{1}$

$x = 1^{1/4}$

$x^4 = 1$

$(x^4 - 1) = 0 \Rightarrow (x^2 - 1)(x^2 + 1)$

$x^2 - 1 = 0$, $x^2 + 1 = 0$

$x = \pm 1$, $x = \pm i$

$G_1 = 1, -1, i, -i$

X	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

The above entries in the composition table satisfy all the axioms

G_1: Let $a, b \in G \Rightarrow a \cdot b \in G$

Closure is satisfied

G2: Let $a, b, c \in G$

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

$abc = abc$

Associative is satisfied

G3: 1 in the top row indicates the identity

$a \cdot 1 = 1 \cdot a = a \quad (a \in G)$

Identity is satisfied.

G4: Let $(1)^{-1} = 1$, $(-1)^{-1} = -1$, $(i)^{-1} = (-i)$, $(-i)^{-1} = i$

Inverse is satisfied.

G5: Let $a, b \in G$, $a \cdot b = b \cdot a \in G$

Commutative is satisfied

$(G, *)$ is abelian group under multiplication

Addition and Multiplication modulo m:

There are two special types of operations addition modulo m, written as $+ \bmod m$ or $\oplus_m$ or $+_m$ and multiplication modulo m written as $\times \bmod m$ or $\otimes_m$ or $\times_m$ on the set of integers Z.

Let a and b be any two integers and m be positive integer greater than 1

The addition modulo m of a and b is defined as least non negative remainder r obtained

when $a+b$ is divided by m.
It is written as $a +_m b = r$, where $0 \leq r < m$

Eg: $5 +_4 5 = 2$
as $5+5 = 10$ and when 10 is divided by 4, the remainder is 2

$3 +_5 8$ ($\because 3+8 = 11$ and when 11 is divided by 5, the remainder is 1)
$3 +_5 8 = 1$

$23 +_7 10 = 5$

The multiplication modulo m of a and b is defined as the least non-negative remainder r obtained when product ab is divided by m.
It is written as $a \times_m b = r$, where $0 \leq r < m$

Eg: $5 \times_4 5 = 1$
as $5 \times 5 = 25$ and when 25 is divided by 4, the remainder is 1.

$3 \times_5 8 = 4$ ($\because 3 \times 8 = 24$ and when 24 is divided by 5, remainder is 4.

$23 \times_7 10 = 6$

Q) Prove that $Z_4 = \{0, 1, 2, 3\}$ is an abelian group w.r.t addition modulo 4.
$Z_4 = \{0, 1, 2, 3\}$

Composition table of Cayley's table:

$+_m$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

i) Closure axiom: All the entries in the table are elements of Z_4
∴ Closure axiom is satisfied

ii) Associative axiom:
Consider, $(1 +_4 2) +_4 3 = 3 +_4 3 = 2$
$1 +_4 (2 +_4 3) = 1 +_4 1 = 2$
∴ Associative axiom is satisfied

iii) Identity axiom: The row leaded by the element 0 is identical to the top row
∴ 0 is the identity element & $0 \in Z_4$
$e = 0$
∴ $a * e = a$ (for $a \in Z_4$)

iv) Inverse axiom: From the table it is clear $0^{-1} = 0$, $1^{-1} = 3$, $2^{-1} = 2$, $3^{-1} = 1$. So every element has its inverse in set Z_4
∴ For $a \in Z_4$, there exits $a^{-1} \in Z_4$ such that $a * a^{-1} = e = 0$

From i, ii, iii, iv, Z_4 is a group.

v) Commutative axiom: From the table it is clear that about the principal diagonal, the table is symmetrical. Therefore commutative axiom is satisfied.
By (i), (ii), (iii), (iv), (v), $(Z_4, +_4)$ is an abelian group.

Q9) Prove that $Z_{10} = \{1, 3, 7, 9\}$ is an abelian group w.r.t multiplication modulo 10.
$Z_{10} = \{1, 3, 7, 9\}$
Cayley's table or Composition table,

X_{10}	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

i) Closure axiom: All the entries in table are the elements of Z_{10}
∴ Closure axiom is satified

ii) Associative axiom:
Consider, $(1 \times_{10} 3) \times_{10} 7 = 3 \times_{10} 7 = 1$
$1 \times_{10} (3 \times_{10} 7) = 1 \times_{10} 1 = 1$
∴ Associative axiom is satisfied. $(Z_4, \times_{10})$ is ~~monoid~~ semi-group

iii) Identity axiom:
The row leaded by 1 is identical to the top row. So 1 is the identity element,
$1 \in Z_{10}$. So $e = 1$

∴ Identity axiom is satisfied.

iv) Inverse axiom:
From the table it is clear that, $1^{-1}=1$, $3^{-1}=7$, $7^{-1}=3$, $9^{-1}=9$. Every element has inverse in Z_{10}
By i, ii, iii, iv. $(Z_{10}, \times_{10})$ is a group.

v) Commutative axiom: From the table it is clear that about the principal diagonal it is symmetrical.
∴ Commutative law is satisfied.
By i, ii, iii, iv. → $(Z_{10}, \times_m)$ is abelian group

PROPERTIES OF GROUP

1) Theorem: (Uniqueness of Identity)
The identity element in a group is unique
Let $(G, *)$ be a group having two identities e and e' then.
as e identity of $G \Rightarrow e'e = e'$ —①
as e' is identity of $G \Rightarrow ee' = e$. —②
From ① and ②
ee' is a unique element of G,
∴ $e = e'$
Hence, the identity element of a group is unique

2) Theorem: (Uniqueness of inverse)
The inverse of an element in a group is unique
Let a be any element of the group $(G, *)$ which has two inverse b and c in the group.

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

& $a^{-1} = c \Rightarrow a * c = e = c * a$

Now, $b * a = e$

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

$b * (a * c) = e * c$ (By associativity axiom and identity axioms of group)

$b * e = c$

$\boxed{b = c}$

Therefore, the inverse of every element of a group is unique.

Remark: the inverse of the identity of a group is itself.

3) Theorem:
If G is a group the for $a, b \in G$

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

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

i.e. the inverse of the product (binary operation) of two elements is the product (binary operation) of their inverse in the reverse order

a) Let $a \in G$ and a^{-1} is inverse of a. $\forall\ a^{-1} \in G$

b) since a^{-1} is the inverse of a,

$a * a^{-1} = e = a^{-1} * a$

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

Inverse of $a^{-1} = a$

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

Remark, for additive operation $-(-a) = a$

b)

Let $a, b, ab, a^{-1}, b^{-1}, b^{-1}a^{-1} \in G$

Now, $(ab) * (b^{-1}a^{-1})$

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

$\Rightarrow a e a^{-1}$

$\Rightarrow$

Let $a, b, a^{-1}, b^{-1} \in G$ such that a^{-1} is inverse of a, b^{-1} is inverse of b

taking, $(a * b) * (b^{-1} * a^{-1})$

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

$\Rightarrow a * e * a^{-1}$

$\Rightarrow a * a^{-1}$

$\Rightarrow e$ — (1)

Similarly, $(b^{-1} * a^{-1}) * (a * b)$

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

$\Rightarrow b^{-1} * e * b$

$\Rightarrow b^{-1} * b$

$= e$ — (2)

So, if $(a * b) = x$ & $(b^{-1} * a^{-1}) = y$

from (1) and (2)

$x * y = e$

$y * x = e$

So, $x = y^{-1}$ and $y = x^{-1}$

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

Generalised Reversal law:

By principle of induction, the above theorem can be generalised as:

$(a * b * c * \cdots * p)^{-1} = p^{-1} * \cdots c^{-1} * b^{-1} * a^{-1}$

Remarks:

1. If the composition is addition (+) then this can be written as: $-(a+b) = (-b) + (-a)$
2. If G is commutative group, then for $a, b \in G$

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

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

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

If G is commutative, $a * b = b * a$

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

4) Theorem: If $a, b \in (G, *)$, then the equation $a * x = b$ has a unique solution which is, $x = a^{-1} * b$

Suppose we assume $a * x = b$ has two solutions p and q

$x = p$ and $x = q$

So, $a * p = b$ and $a * q = b$

$$a * p = a * q$$

$$a^{-1} * a * p = a^{-1} * a * q$$

$$e * p = e * q$$

$$p = q$$

Now if $a, b \in G$ then, $a^{-1} b \in G$ by closure property.

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

$$= e * b$$

$$= b$$

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

as, $a * x = b$

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

5) If $a, b, c \in G$

i) If $a * b = a * c$, then $b = c$

Now, taking $a, b, c \in G$ and a^{-1} also $\in G$

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

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

$e * b = e * c$

$\therefore b = c$

Hence proved

ii) If $b * a = c * a$, $b = c$

Given, $b * a = c * a$

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

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

$b * e = c * e$

$\therefore b = c$

Hence proved

6) Theorem: Alternate definition of group

If for all elements a, b of a semi-group G, equations $ax = b$ and $ya = b$ have unique solutions in G, then G is group.

G being a semi-group, is a non-empty set. Therefore let $a \in G$, then the equations $ax = a$ and $ya = a$ will have unique solutions in G. Let these solutions be denoted by e_1 and e_2 respectively, then

$ae_1 = a$ and $e_2 a = a$ — (1)

Again if b be any other element of G, then by the given property

$x, y \in G$ so that $ax = b$ and $ya = b$ — (ii)

Now, $ya = b \Rightarrow ya e_1 = be_1$

$ya = be_1$ by (i)

$b = be_1$ by (ii)

e_1 is right identity in G

Again $ax = b \Rightarrow e_2 ax = e_2 b$

$ax = e_2 b$ by (i)

$b = e_2 b$ by (ii)

e_2 is the left identity in G

Since e_1 is right identity in G and $e_2 \in G$,

$e_2 e_1 = e_2$ — (3)

Since e_2 is left identity G and $e_1 \in G$,

$e_2 e_1 = e_1$ — (4)

$\therefore e_2 = e_1$ (From (3), (4))

Hence there exists an identity $e_1 = e_2 = e$ in G.

Again using the property for the elements $a, e \in G$ we find that equations $ax = e$ and $ya = e$ have unique solutions in G

Let these solutions be x_a & y_a, so

$ax_a = e$ and $y_a a = e$

x_a and y_a are right & left inverses of a in G.

Now, $ax_a = e \Rightarrow y_a(ax_a) = y_a e$

$(y_a a)x_a = e_a e$

$e x_a = y_a e$

$\boxed{x_a = y_a}$

∴ There exists inverse of a in G
Since the identity exists and every element of G is invertible in semi-group G, therefore G is a group.

Remark: If G is a semi-group such that $a, b \in G$, only the equation $ax = b$ (or $ya = b$) has a unique solution in G, then G may not be a group.
This can be observed by following example:

Ex: Let G be any non-empty set having atleast two elements.
Define a binary operation * as follows:

NOTE: An element $a \in G$ is called idempotent if $a * a = a$.

7. Theorem: A group $\{G, *\}$ can't have an idempotent element except identity element.
Suppose a is idempotent element such that $a * a = a$ and e is identity element
$\forall\ a, e \in G$

Given, $a * a = a$

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

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

$a * e = e$

$a = e$

∴ Proved

Eg: If $\{G, *\}$ is an abelian group show that $(a*b)^n = a^n * b^n \Rightarrow a, b \in G$ where n is a positive integer.

We will prove this by mathematical induction.

i) for $n = 1$, $(a*b)^1 = a^1 * b^1$

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

so for $n=1$, it is proved

ii) For $n=2$, $(a*b)^2 = a^2 * b^2$

L.H.S $\Rightarrow (a*b) * (a*b)$

$\Rightarrow a*(b*a)*b$

$\Rightarrow a*(a*b)*b$ (Commutative law)

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

$= a^2 * b^2$

iii) Now assuming that, $(a*b)^k = a^k * b^k$

So for $n = k+1$,

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

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

~~$= a^k * (b^k$~~

$= (b^k * a^k) * (a*b)$ (commutative law)

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

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

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

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

$\Rightarrow (b^k * b) * a^{k+1}$

$\Rightarrow b^{k+1} * a^{k+1}$

So prove for $n = k+1$,

Now we can say that, $(a*b)^n = b^n * a^n$

SUB-GROUP : Definition →

A non-empty subset H of a group G is called a subgroup of G if

i) H is stable (closed) for the composition defined in G i.e

$a \in H, b \in H, \quad a * b \in H$

and

ii) H itself is a group for the composition induced by that of G.

Proper & Improper Subgroup:

Every group G of order greater than 1 has atleast two subgroups which are,

i) G (itself)

ii) $\{e\}$ i.e the group of identity alone

The above two subgroups are known as improper or trivial sub-groups

A subgroup other than these two is known as proper sub-group

Remark: If any subset of the Group G is a group for any operation other than the composition of G, then it is not called a subgroup of G.

Eg: The group $\{1, -1\}$ is a part of $(\mathbb{C}, +)$ which is a group of multiplication but not for the composition $(+)$ of the basic group. Therefore it is not a subgroup of $(\mathbb{C}, +)$.

Examples of Sub-Group:

i) Additive Groups:

1) $(Z, +)$ is a subgroup of $(Q, +)$
2) $(Q, +)$ is a sub-group of $(R, +)$
3) The set E of even integers is proper subgroup of additive group $(E, +)$, whereas the set O of odd integers is not a subgroup of the additive groups $(Q, +)$ $(Z, +)$
4) The set nZ of multiples of some given integer m is a sub-group of $(Z, +)$
5) The group $\{0, 4\}$ is subgroup of $(Z_8, +_8)$

ii) Multiplicative Groups:

1) $(Q, \times)$ is subgroup of $(R, \times)$
2) $\{1, -1\}$, $\{1, \omega, \omega^2\}$, $\{1, -1, i, -i\}$ are subgroup of $(C, \times)$ the group of non-zero complex numbers
3) The multiplication operation $(\{1, -1\}, \times)$ is a subgroup of $\{1, -1, i, -i\}$

Ex: $G = \{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}$

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

Here $(H, *)$ is a sub-group w.r.t + operation of $(G, *)$

But $I = \{\ldots -3, -1, 0, 1, 3, 5 \ldots\}$ is not a subgroup as for all elements of I for '+' operation, $a + b \notin I$. This violates the closure property.

THEOREMS OF SUBGROUP:

1) If H is sub-group of G, then:
(a) The identity of H is same as that of G
(b) The inverse of any element of H is same as that of the inverse as an element of G.
(c) The order of any element a of H is the same as the order of a in G

(a) Let e and e' be identities of G & H resp.
If $a \in H$, $a*e' = e'*a = a$ — (1)
Now, $a \in H \Rightarrow a \in G$
$\therefore a*e = e*a = a$ — (2)
From (1) and (2)
$a*e' = a*e$
$a^{-1}*(a*e') = a^{-1}*(a*e)$
$(a^{-1}*a)*e' = (a^{-1}*a)*e$
$\boxed{e' = e}$

(b) Let $a \in H$ and b & c are inverse of a and e is identity of G and H
$a*b = b*a = e$ — (1)
$a*c = c*a = e$ — (2)
From (1) & (2)
$a*b = a*c$
$\boxed{b = c}$

(c) Let order of $a \in H$ be m and n in H & G resp.
If e be the identity by the definition of order
$a^m = e$ and $a^n = e$
$a^m = a^n$
$a^m * a^{-n} = a^n * a^{-n}$
$a^{m-n} = a^0$

$m - n = 0$

$\boxed{m = n}$

Thus the order of an element of subgroup is the same as that of the sub-group & original group

Imp

Subset H of a subgroup G is a subgroup iff:

i) $a \in H, b \in H \Rightarrow a * b \in H$

ii) $e \in H$ where e is identity of G.

iii) $a \in H \Rightarrow a^{-1} \in H$, where a^{-1} is inverse of a in G.

2) A non void subset H of group G is a sub-group iff, $a \in H, b \in H, \Rightarrow a * b^{-1} \in H$.

Let H is a subgroup of group G and $b \in H$

So, $b \in H \Rightarrow b^{-1} \in H$ (as H is subgroup of G)

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

$a * b^{-1} \in H$ (by closure property in H)

∴ If H is a subgroup of G, then the condition is necessary.

Converse: If the condition is true then H will be subgroup of G.

Now $H \neq \phi$ (non-empty set)

Let $a \in H$

∴ Identity exists in H

Again by same condition, $e \in H, a^{-1} \in G$ ~~$\Rightarrow e * a \in a^{-1} \in H$~~

$\Rightarrow e * a^{-1} \Rightarrow a^{-1} \in H$

Inverse of every element exist in H

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

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

H is closed for the operation of G.

Therefore H is a subgroup of G which proves that the given condition is sufficient for H to be subgroup.

3) A nonvoid finite subset H of group G is a subgroup iff:

$a \in H, b \in H, a * b \in H$

Let H be a finite sub-group of G, then H will be closed for the operation of G

$\therefore a \in H, b \in H \Rightarrow a * b \in H$

Conversely :- If $a \in H, b \in H \Rightarrow a * b \in H$

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

Thus we will see that, $a^{n-1} \in H, a \in H$

$\Rightarrow a^n \in H \quad \forall \; n \in N$

$\therefore a, a^2, a^3 \ldots a^n \ldots$ are element of H.

But H is finite subset of G, so all the powers of a cannot be distinct.

So let $a^i = a^j, \; i > j$

$a^{i} * a^{-j} = a^{i-j} = a^0 = e \quad [\because a^i \in G \Rightarrow (a^j)^{-1} = a^{-j} \in G]$

$a^{i-j} = e$ where e is identity of G

$a^r = e \in H \quad [\because i - j = r \in N, r > 0]$

$\therefore$ Identity element exists in H

Again, $a^{r-1} \in H \Rightarrow a^r * a^{-1} \in H$

$e * a^{-1} = a^{-1} \in H$

Thus each element of H has its inverse in H

Hence H is subgroup of G.

4) The intersection of any 2 subgroups of a group G is again a subgroup of G.

Let H_1 & H_2 be two subgroups of G

$\because e \in H_1, e \in H_2 \Rightarrow e \in H_1 \cap H_2$

$\therefore H_1 \cap H_2 \neq \phi$

Now let $a, b \in H_1 \cap H_2$ then

$a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1$ and $a, b \in H_2$

$\Rightarrow a * b^{-1} \in H_1$ and $a * b^{-1} \in H_2$ [$\because H_1$ & H_2 are subgroups]

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

$\therefore H_1 \cap H_2$ is a subgroup of G

Generalisation:

If $H_1, H_2 - - - H_n$ be a finite family of subgroups of G, then $H_1 \cap H_2 \cap H_3 - - \cap H_n$ is also a subgroup of G.

Remark:

The union of two subgroups is not necessarily a subgroup.

Eg: The group $G = (Z, +)$ has 2 subgroups $H = \{2n : n \in Z\}$ and $K = \{3n; n \in Z\}$.

And their union $H \cup K = \{ - - -6, -4, -3, -2, 0, 2, 3, 4, 6 - - - \}$ is not a subgroup because it is not closed for +

Eg: $2 \in H \cup K$, $3 \in H \cup K$

But the sum $2 + 3 = 5 \notin H \cup K$

This shows its not closed for addition.

→ If H & K are two sub-groups of any group G, then their product HK or KH need not be a subgroup.

5) If H & K are two sub-group of group G, then HK is a subgroup of G iff ($\Leftrightarrow$) HK = KH.

Let HK = KH, the we shall prove that HK is a subgroup of G

$(HK)(HK)^{-1} = (HK)(K^{-1}H^{-1})$

$= H(KK^{-1})H^{-1}$ ($\because$ associativity)

$= (HK)H^{-1}$ ($\because$ K is subgroup, $KK^{-1} = K$)

$= KHH^{-1}$ ($\because HK = KH$)

$= KH$

$= HK$

$\therefore$ HK is subgroup of G.

Conversely $\Rightarrow$ Now let HK be subgroup of G, then,

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

$K^{-1}H^{-1} = HK$

$KH = HK$

[$\because$ H, K are subgroups, $H^{-1} = H$, $K^{-1} = K$]

$\therefore$ If HK is subgroup $\Rightarrow$ KH = HK

{# If H & K are subgroups of Commutative group G then HK is a subgroup of G.
[$\because$ G is abelian $\Rightarrow$ HK = KH $\Rightarrow$ HK is subgroup]}

(Q1) Show that $H = \{0, 2, 4\}$ is a subgroup of the group that $G = \{0, 1, 2, 3, 4, 5\}$ under addition modulo 6.

Clearly $H = \{0, 2, 4\} \subset G$ — ①

Cayley's table or Composition table :

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

i) Closure axiom: All the entries in table are the elements of H.
∴ Closure is satisfied

ii) Associative axiom:
Consider $(0 +_6 2) +_6 4 \Rightarrow 2 +_6 4 = 0$
$0 +_6 (2 +_6 4) \Rightarrow 0 +_6 0 = 0$
∴ Associative axiom is satisfied

iii) Identity axiom: The row leaded by 0 is identical to top row, 0 is identity element and $0 \in H$.
∴ $e = 0$
∴ Identity axiom is satisfied

iv) Inverse axiom: From the table it is clear that $0^{-1} = 0, 2^{-1} = 4, 4^{-1} = 2$, so every element has inverse in the set H
∴ Inverse is satisfied

From i, ii, iii, iv, $(H, +_6)$ is a group ——— ②
From ① and ②, H is a subgroup of G.

Q.2) Prove that $H = \{a + ib \mid a, b \in \mathbb{Q}\}$ is a subgroup of $(C, +)$

Clearly H is a non-empty subset of $\mathbb{C}$
Let $x, y \in H$ where $x = a_1 + ib_1$, $y = a_2 + ib_2$
Then $x - y = (a_1 + ib_1) - (a_2 + ib_2)$
$= (a_1 - a_2) + i(b_1 - b_2) \in H$
(as $a_1 - a_2 \in \mathbb{Q}$ & $b_1 - b_2 \in \mathbb{Q}$)
$\therefore x \in H, y \in H, x - y \in H$
$\therefore H$ is a subgroup of $(\mathbb{C}, +)$

(Q3) Prove that H is a sub-group of group $(\mathbb{C}_0, \times)$ where $H = \{a + \sqrt{2}b \mid a \in \mathbb{Q}, b \in \mathbb{Q}, a^2 + b^2 \neq 0\}$.
Clearly H is an non-empty subset of $\mathbb{C}_0$
Let $x, y \in H$, where $x = a_1 + b_1\sqrt{2}$ and $y = a_2 + b_2\sqrt{2}$
$a_1, a_2, b_1, b_2 \in \mathbb{Q}$, $a_1^2 + b_1^2 \neq 0$, $a_2^2 + b_2^2 \neq 0$

$$xy^{-1} = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})^{-1}$$
$$= \frac{a_1 + b_1\sqrt{2}}{a_2 + b_2\sqrt{2}} \Rightarrow \frac{a_1 + b_1\sqrt{2}}{a_2 + b_2\sqrt{2}} \cdot \frac{a_2 - b_2\sqrt{2}}{a_2 - b_2\sqrt{2}}$$
$$= \frac{(a_1 + b_1\sqrt{2})(a_2 - b_2\sqrt{2})}{a_2^2 - 2b_2^2}$$
$$= \frac{a_1a_2 - 2b_1b_2}{a_2^2 - 2b_2^2} + \frac{(a_2b_1 - a_1b_2)\sqrt{2}}{a_2^2 - 2b_2^2}$$

Now if $a_2^2 - 2b_2^2 = 0$
$a_2 = \sqrt{2}b$, $a_2 \notin \mathbb{Q}$
which is false
$\therefore a_2^2 - 2b_2^2 \neq 0$
Consequently $\left(\frac{a_1a_2 - 2b_1b_2}{a_2^2 - 2b_2^2}\right)$ and $\left(\frac{a_2b_1 - a_1b_2}{a_2^2 - 2b_2^2}\right)$ are rational.
Therefore, $xy^{-1} \in H$
Hence H is a subgroup of $(\mathbb{C}_0, \times)$

Q4) If an element of a group G, then prove that its normalizer $N(a) = \{x \in G \mid ax = xa\}$ is a subgroup of G.

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

$\therefore N(a) \neq \phi$

Let $x_1, x_2 \in N(a)$, then by definition of $N(a)$

$ax_1 = x_1a$ and $ax_2 = x_2a$

Now, $ax_2 = x_2a$

$x_2^{-1}(ax_2)x_2^{-1} = x_2^{-1}(x_2a)x_2^{-1}$

$(x_2^{-1}a)(x_2x_2^{-1}) = (x_2^{-1}x_2)(ax_2^{-1})$

$x_2^{-1}ae = eax_2^{-1}$

$x_2^{-1}a = ax_2^{-1}$

$\therefore x_2^{-1} \in N(a)$

So, $x_2 \in N(a) \Rightarrow x_2^{-1} \in N(a)$

Again, $a(x_1x_2^{-1}) = (ax_1)x_2^{-1}$ [$\because$ by associativity]

$= (x_1a)x_2^{-1}$ [$x_1 \in N(a)$]

$= x_1(ax_2^{-1})$ [$\because$ by associativity]

$= (x_1x_2^{-1})a$

$\therefore x_1x_2^{-1} \in N(a)$

Thus we see that

$x_1 \in N(a), x_2 \in N(a) \Rightarrow x_1x_2^{-1} \in N(a)$

$\therefore N(a)$ is a subgroup of G.

CYCLIC GROUP

A group G is a cyclic group if there exists an element $a \in G$ such that $G = [a]$ i.e every element of G can be expressed in integral power of a.

a is called generator of G.

Eg: $G = \{ \cdots a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2 \cdots \}$

If the operation of the group G is addition (+) then,

$G = [a] = \{ \cdots -3a, -2a, -a, 0, a, 2a, 3a \cdots \}$

Q1) Prove that the set $G = \{x \mid x^n = 1\}$ of n^{th} roots of unity is finite multiplicative cyclic group of order n.

Let $x_1, x_2 \in G$, then $x_1^n = 1$ and $x_2^n = 1$

But $x_1^n = 1$, $x_2^n = 1 \Rightarrow x_1^n x_2^n = 1 \cdot 1 = 1$

$$(x_1 x_2)^n = 1$$

$$\Rightarrow x_1 x_2 \in G$$

So G is closed for multiplication

Also $1^n = 1 \Rightarrow 1 \in G$ which is the identity element for multiplication.

Further for each $x \in G$,

$$x \in G \Rightarrow x^n = 1$$

$$\frac{1}{x^n} = 1$$

$$\left(\frac{1}{x}\right)^n = 1$$

$$\Rightarrow \frac{1}{x} \in G$$

which is the inverse of each element, so each element is invertible. Lastly multiplication of numbers is associative, so it is also associative in G. Hence G is a group for multiplication.

$\therefore x^n = 1$ has n roots, $O(G) = n$

G is cyclic group: $1 = \cos 2m\pi + \sin 2m\pi$, $m \in Z$

$1^{1/n} = \cos\frac{2m\pi}{n} + \sin\frac{2m\pi}{n}$, $m = 0, 1, 2 \cdots (n-1)$

[By Demoivre's theorem]

$= e^{\frac{2\pi i m}{n}}$, $m = 0, 1, 2, 3 \cdots (n-1)$

(By Euler's theorem)

$\therefore G_1 = \{ e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, e^{\frac{6\pi i}{n}} \cdots e^{2n\pi i/n} \}$

$= [e^{2\pi i/n}]$, $m = 0, 1, 2 \cdots (n-1)$

$\therefore G$ is a cyclic group of the order n generated by $e^{2\pi i/n}$.

Q2) Find all generators of the cyclic group: $(G = \{0, 1, 2, 3, 4, 5\}, +_6)$

We find that,

$1(0) = 0 \Rightarrow \phi(0) = 1$

$1(1) = 1, 2(1) = 2, 3(1) = 3, 4(1) = 4, 5(1) = 5, 6(1) = 0 \Rightarrow \phi(1) = 6$

$1(3) = 3, 2(3) = 0 \Rightarrow \phi(3) = 2$

$1(2) = 2, 2(2) = 4, 3(2) = 0 \Rightarrow \phi(2) = 3$

$1(4) = 4, 2(4) = 2, 3(4) = 0 \Rightarrow \phi(4) = 3$

$1(5) = 5, 2(5) = 4, 3(5) = 3, 4(5) = 2, 5(5) = 1, 6(5) = 0$

$\Rightarrow O(5) = 6$

Observing the order of all elements of G, we find that,

$O(1) = O(5) = O(G)$

$\therefore G = [1] = [5]$ are two generators of G.

$O(G) = p^n$

No. of generators $\Rightarrow p^n - p^{n-1}$

Eg: $O(G) = 6 = 3.2$

No. of generators, $(3^1-3^0)(2^1-2^0)$

$= 2 \times 1 = 2$

Q3) Find all generators of cyclic group $(G = \{1,2,3,4\}, \times_5)$

We have $O(G) = 4$.

Generator is that element, whose order is 4 of G

$1^2 = 1 \Rightarrow O(1) = 1$

$2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1 \Rightarrow O(2) = 4$

$3^1 = 3, 3^2 = 4, 3^3 = 2, 3^4 = 1 \Rightarrow O(3) = 4$

$4^1 = 4, 4^2 = 1 \Rightarrow O(4) = 2$

So, $2, 3 \in G$ such that

$O(2) = 4 = O(G)$ and $O(3) = 4 = O(G)$

2, 3 are two generators of cyclic group G.

PROPERTIES:

1) Theorem: Every cyclic group is abelian.

Let $G = [a]$ be a cyclic group and $x, y \in G$, Where $x = a^m$, $y = a^n$

Then, $x * y = a^m a^n = a^{m+n}$

$= a^{n+m} = y * x$

Now $x * y = a^m * a^n$

$= (a * a * a \cdots * a)_{m \text{ times}} * (a * a * \cdots a)_{n \text{ times}}$

$= a^{m+n}$

$= a^{n+m}$

$= y * x$

$\therefore$ G is abelian group

Every abelian group need not be cyclic.
Eg: $(\mathbb{R}, +)$ is abelian but not cyclic

2) Theorem: If a is generator of cyclic group G, then a^{-1} is also its generator.
Let $G = [a]$ be a cyclic group and $x \in G$.
Since G is a cyclic group, so there exists an integer m such that
$$x = a^m$$
$$\Rightarrow x = (a^{-1})^{-m} \quad [-m \in \mathbb{Z}]$$
x can also be expressed as some integral pow of a^{-1}
$\therefore$ a^{-1} is also a generator
$\therefore$ $G = [a] \Rightarrow G = [a^{-1}]$

3) The order of a finite cyclic group is equal to the order of its generator. i.e
O(Finite cyclic group) = O(generator of group)
Let $G = [a]$ be a finite cyclic group and $O(a) = n$
Let $H = \{a, a^2, a^3 \dots a^n = e\}$
Clearly H is a subgroup of G whose order is n

Case1) When $m \leq n$: If $a^m \in G$ then $a^m \in H$
$\therefore H \subset G$ —— (1)

Case2) When $m > n$: $m = qn + r$, $0 \leq r < n$, $q, r \in \mathbb{Z}$
$$a^m = a^{qn+r}$$
$$= (a^n)^q a^r$$
$$= e a^r$$
$\therefore G \subset H$ —— (2)

From (1) & (2)

$H = G$

But, $O(H) = n$

$O(G) = n = O(a)$

Corollary:

A finite group of order n is cyclic iff it has an element of order n.

Proof: Let $G = [a]$ be a finite cyclic group of order n. Then by above theorem, an element exists in G such that

$O(a) = O(G) = n$

Conversely ($\Leftarrow$): Let G be a finite ~~gro~~ cyclic group of order n in which an element a exists such that, $O(a) = n$

Now if $H = [a]$, then $H \subset G$ and by the above theorem,

$O(a) = n \Rightarrow O(H) = n$

$\Rightarrow O(H) = O(G)$

Similarly G is a finite group such that

$H \subset G$ and $O(G) = O(H)$

$G = H = [a]$

$\Rightarrow$ G is a cyclic group generated by a.

4) Theorem: Every infinite cyclic group has two & only two generators.

Let $G = [a]$ be a cyclic group.

a is a generator $\Rightarrow a^{-1}$ is also generator

To show: $a \neq a^{-1}$

Assume $a = a^{-1}$,

$$a = a^{-1}$$
$$a * a = a^{-1} * a$$
$$a^2 = e$$
$$\Rightarrow O(a) = 2 \Rightarrow O(G) = 2$$

Which is not possible as G is infinite group

$\therefore a \neq a^{-1}$

To show that G does not have any generator other than these 2:

Let if possible, a^m, $m \neq \pm 1$ be also a generator

For $a \in G$, there exists an integer n such that:

$$a = (a^m)^n = a^{mn}$$
$$a * a^{-1} = a^{mn} * a^{-1}$$
$$e = a^{mn-1}$$
$$O(a) = mn - 1 \Rightarrow \text{finite}$$

$O(a)$ is finite

Which contradicts G is infinite

Hence a^m cannot be generator of G unless $m = 1$ or -1. Consequently G has exactly 2 generators a & a^{-1}.

5) Theorem: Every sub-group of a cyclic group is also cyclic.

Let $G = [a]$ be cyclic group and H be sub-group of G.

If $H = G$ or $H = \{e\}$, then clearly H is also cyclic

If H is a proper sub-group of G, then H contains

atleast one element a^m $(m \in Z, m \neq 0)$ other than the identity.

$a^m \in H \Rightarrow a^{-m} \in H$ [$\because H$ is sub-group]

Since $m \neq 0$, therefore $m > 0$ or $-m > 0$

$\Rightarrow$ There exists positive integral powers of a in H

Let m be the least +ve integer $\forall$ $a^m \in H$,

To prove, $H = [a^m]$

Let $a^n \in H$, then by division algorithm, there exists two integers q & r such that

$n = mq + r \qquad 0 \leq r < m$

or $n - mq = r$

Now since, $a^m \in H \Rightarrow (a^m)^q = a^{mq} \in H$

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

Now, $a^n \in H$, $a^{-mq} \in H \Rightarrow a^n * a^{-mq} = a^{n-mq} \in H$

$\Rightarrow a^r \in H$ - [$\because n - mq = r$]

But m is the least positive integer such that $a^m \in H$ and $0 \leq r < m$ (But r cannot be smaller than m as we have assumed m as least positive)

Therefore $r = 0$, and $n = mq$

so, $a^n = a^{mq} = (a^m)^q$

$\Rightarrow H = [a^m]$

$\therefore$ Every subgroup of G is cyclic.

Corollary:

Every proper subgroup of an infinite cyclic group is infinite.

Proof: Let $G = [a]$ be an infinite cyclic group

And H be a proper subgroup of G. Then by the above theorem H is cyclic and $H = [a^m]$ where m is the least positive integer such that $a^m \in H$.

Let if possible, $O(H) = p \Rightarrow O(a^m) = p$

$$(a^m)^p = e$$

$$a^{mp} = e$$

$\Rightarrow O(a)$ is finite

$\Rightarrow O(G)$ is finite

which is contrary to the hypothesis. Therefore the order of H cannot be finite. Consequently, every proper sub-group of G is infinite