Cyclic Group

A Group $(G, *)$ is called Cyclic Group if there exist an element $a \in G$ such that every element of G can be written as a^n, for some integer n

i.e $G = \langle a \rangle = \{ a^n / n \in Z \}$ we say that G is generated by a or a is generated of G

If binary operation is addition then

$a^n = \underbrace{(a+a+a \text{ ---------- } +a}_{n \text{ times}} = nxa$

If binary operation is multiplication

$a^n = \underbrace{axaxa \text{ ---- } a}_{n \text{ times}}$

Example $G = \{1, -1, i, -i\}$ Show that

1) G is Group under multiplication
2) G is abelian Group
3) G is cyclic Group, if it is cyclic find its generator

Solution: (1) (G, x)

P-1) $1 \times -1 = -1 \times 1$

P-2) $e = 1 \in G$

P-3) $a.a^{-1} = e = 1$ (Check For all elements in G)

Composition Table (Only done wh. for finite sets)

X	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	$i^2 = -1$	$1 = -i^2$
-i	-i	i	$-i^2 = 1$	$-1 = i^2$

(1) Check for existence of identity $e = 1$

(2) Check for inverse.

All properties exist for G to be a Group.

$\therefore$ G is a Group.

(2) From table $a.b = b.a$ for all $a, b \in G$

$\therefore (G, \times)$ is a abelian Group.

(3) To check cyclic

Take any element from G., Suppose $a = 1$

$\therefore a^n = (1)^n$ For $G = n = (0, 1, 2, 3 \cdots -1, -10)$

$(1)^n$ for all $n \in Z = \{1\} \neq G$

$\therefore a = 1$ is not generator

NOTE

for any element in a set if we get a single element as generator then the whole set is cyclic group.

for $a = -1$ $(a)^n = (-1)^n$ for all $n (-1, -2, 0, 1, \cdots m)$

$= \{1, -1\} \neq G.$

$\therefore a = -1$ isnot generator of G

for $a = i$ $(a)^n = (i)^n$ for all $n (-1, -2, -0, 1, 2 \cdots)$

$= \{i, i^2, i^3, i^{-1}, i^{-2} \cdots\} = \{1, i, -i, 1\} = G$

$\therefore a = i$ is the generator of G

$\therefore (G, \times)$ is cyclic Group.

Similarly for $a = -i$

NOTE : If (a) = generator of cyclic group then inverse of (a) for any binary operation is also a generator.

Example : $a = 1$ is generator for $(z, +)$

then $a = -1$ is also generator for $(z, +)$

And hence we get two generator for $(z, +)$

Example $(Z, +)$ determine wether it is cyclic group or not.

Soln $Z = \{ \ldots\ldots -2, -1, 0, 1, 2 \ldots\ldots \}$

For $a = 0$ $\quad a^n = (0)^n = n.a = n.(0) = \{0\}$

$\therefore a = 0$ in not generator of $(Z, +)$

for any value of $n = -1, -2, 0, 1, 2$ we will get set of Z

For $a = 1$ $\quad a^n = (1)^n = 1.n = n = \{ \ldots -2, -1, 0, 1, 2 \ldots \}$

$\therefore a = 1$ is generator of $(Z, +)$

$\therefore (Z, +)$ under $a = 1$ is a cyclic group.

For $a = -1$ $\quad a^n = (-1)^n = (-1.n) = -n = \{ \ldots -2, -1, 0, 1, 2 \ldots \}$

$\therefore a = -1$ is generator of $(Z, +)$

$\therefore (Z, +)$ under $a = -1$ is a cyclic group.

By inverse of generation

For $a = 2$ $\quad a^n = (2)^n = 2.n = n = \{ \ldots -2, 0, 2 \ldots \}$

$\therefore a = 2$ is not a generator of $(Z, +)$

$\therefore a = -2$ is also not a generator of $(Z, +)$

$\therefore (Z, +)$ under $a = 2, -2$ is not a cyclic group.

$\therefore (Z, +)$ is cyclic group

* Every cyclic have 2 generator (atleast) Because it will contain it's inverse.

3) Is $(\mathbb{Q}, +)$ is cyclic group.

Soln $\mathbb{Q} = \{ p/q \mid p, q \in Z \quad q \neq 0 \}$

For $a = 0 \in \mathbb{Q}$.

$a^n = n.a = n.0 = \{0\}$

$\therefore a = 0$ is not the generator & $\mathbb{Q}$ is not cyclic group.

for $a = 1$

$a^n = n.a = n.1 = \{ \cdots -2, -1, 0, 1, 2 \cdots \} = Z$

but $\neq \mathbb{Q}$

$\therefore a = 1, -1$ is not generator of Group $(\mathbb{Q}, +)$

for $a = 3/5$

$a^n = \frac{3}{5} \times n = \{ \cdots \frac{-6}{5}, \frac{-3}{5}, 0, 3/5, \frac{6}{5} \cdots \}$

This set is rational but all elements in $\mathbb{Q}$ are not present $\therefore a = 3/5$ & $-3/5$ is not generator of $(\mathbb{Q}, +)$

Every element $a \in \mathbb{Q}$. $\langle a \rangle$

$\langle a \rangle = \{ n.a \mid n \in Z \} \neq \mathbb{Q}$

$\therefore \mathbb{Q}$ has no generator.

$\therefore (\mathbb{Q}, +)$ is not cyclic group.

Example Check for $(R, +)$ (H.W)

* Divides

If $a, b \in z$ and a/b (a divides b) b = integer multiple of a.

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

Notation : a/b (a divides b)

$a \nmid b$ (a dosenot divides b)

Example · does 2 divide 4 ?

Suppose $a = 2$, $b = 4$

∴ is it possible to express $(b = c \times a)$

∴ $(\overset{b}{4} = \overset{c}{2} \times \overset{a}{2}) = (b = c \cdot a)$.

∴ $2/4$

Example does 4 divide 2 ?

$a = 4$ $b = 2$ $\longrightarrow$ $\overset{b}{2} = \overset{c}{\frac{1}{2}} \times \overset{a}{4}$ ∴ $(\frac{1}{2} \notin z)$

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

∴ $4 \nmid 2$

* Division Algorithm

$a, b \in z$, $a = bq + r$ (divisor)

quotient → always an integer

remainder → never negative → $0 \leq r$

Example $a = 5$, $b = 2$

∴ $5 = 2(2) + 1 = a = bq + r$

∴ $q = 2$, $r = 1$

Example ① $a = -5$, $b = 2$

$-5 \neq 2(-2) + 1 = -3$ ✗ $\quad a = bq + r$

$\therefore q = -2 \quad r = 1$

Here L.H.S & R.H.S is not equal & always $r \geq 0$ $\therefore (-2, 1)$ not possible

② $\therefore a = -5, \; b = 2$

$\overset{a}{-5} = \overset{b}{2}(-3) + \overset{r}{1} = -6 + 1$ ✗

$\therefore q = -3 \quad r = 1$

③ To calculate time $\quad 11 + 5^{00} = 511$

$511 = 24(\;\;)$

* Modular Arithmetic

If a and b are integer and $m \in Z^+$ then integers a is congurent to b modulo m if m divides $a-b$ i.e $\frac{a-b}{m}$ = integer

Notations

$a \equiv b \pmod m$ — a is congruent to b at mod m

$a \not\equiv b \pmod m$ — a is not congruent to b at mod m

Exg: $a = 17 \quad b = 5 \quad m = 6$

Sol: $\frac{a-b}{m} = \frac{17-5}{6} = \frac{12}{6} = (2 = \text{Integer}) \; (2 \in Z)$

$\therefore$ m divides $a-b$ $\leftrightarrow$ 6 divides $a-b$

i.e $17 \equiv 5 \pmod 6$

if we divide 17/6 Remainder is 5.

Example 2 $a = 50^\circ$ $m = 24$ hr clock.

$50 \equiv ? \pmod{24}$.

Soln $\frac{50}{24} =$ ∴ Remainder = 2.

$\therefore 50 \equiv 2 \pmod{24}$

Example 3 24 hr clock 12 hr clock.

Suppose 21 → To get time in 12hr we divide by 12 in 24hr clock.

$21 \equiv 9 \pmod{12}$ (9 → remainder, 12 → divisor)

12 $12 \equiv 0 \pmod{12}$ (0 → remainder)

Example 4 $a = 24$ $b = 14$ $m = 6$

$\frac{a-b}{m} = \frac{24-14}{6} = \frac{10}{6} = \frac{5}{3} \notin Z$

∴ m does not divide a-b

$a \not\equiv b \pmod{m}$

$24 \not\equiv 14 \pmod{6}$

Example 5 $a \equiv b \pmod{m}$ $c \equiv d \pmod{m}$

Do addition of modulo.

$\therefore a + c \equiv b + d \pmod{m}$ (Addition)

$ac \equiv bd \pmod{m}$ Multiplication.

$a \equiv b \pmod{m}$

$c \equiv d \pmod{m}$

→ 0 is congruent to 0 itself $q = 0$ also

Calculating modulo for certain term :-

→ $0 \equiv 0 \pmod 5$, $1 \equiv 1 \pmod 5$, $2 \equiv 2 \pmod 5$, $3 \equiv 3 \pmod 5$

$5 \equiv 0 \pmod 5$, $6 \equiv 1 \pmod 5$, $7 \equiv 2 \pmod 5$, $8 \equiv 3 \pmod 5$

$9 \equiv 4 \pmod 5$, $10 \equiv 0 \pmod 5$, $11 \equiv 1 \pmod 5$

$(-1) \equiv 4 \pmod 5$ ↳ remainder 5/10 for all.

↳ $(-1) = (-1)(5) + 4$

quotient ↳ ↓ ↳ remainder

modulo.

$(-2) \equiv ? \pmod 5$ $\quad (-2) = (-1)(5) + 3$

$(-2) \equiv 3 \pmod 5$

$\therefore Z_5 = \{0, 1, 2, 3, 4\}$

Z = Infinite set

Z_m = Set of Integer under modulo m

Q Find elements of $Z_{10} = ?$

$Z_{10} = \{0, 1, 2, \text{----} 9\}$

$\therefore Z_m = \{0, 1, 2 \text{ - - - - } (m-1)\}$ elements in Z_m

Operations on Modulo :-

$+_m$ → addition modulo m

X_m → multiplication modulo m

Example $Z_5 = \{\overset{0}{0}, \overset{1}{1}, \overset{2}{2}, \overset{3}{3}, \overset{4}{4}, \overset{5}{5}, \overset{6}{6}, \overset{7}{7}, \overset{8}{8}, \overset{9}{9}\}$

$2, 3 \in Z_5$ Do addition for modulo 5

addition for modu

$2 (+_5) 3 \Rightarrow 5 = 0$

$2 (+_5) 4 = 6 = 1$

↳ count position in set of Z_m

$2 (X_5) 4 = 8 = 3$

↳ multiplication.

Composition M Table

$Z_5 = \{0, 1, 2, 3, 4\}$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	2	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(1) Find is it a Group ? Yes
(2) Is it Abelian Group? (Commutative property)
(3) If it cyclic group?

1- prop
Associative

(1) For all $a, b, c \in Z_5$

$$a +_5 (b +_5 c) = (a +_5 b) +_5 c$$

$\because$ addition is associative

$\therefore Z_5$ is Associative under addition module 5

2- prop
Identity

For element $e = 0 \in Z_5$, There exist $e = 0 \in Z_5$

$a + e = a$ for all $a \in Z_5$

3- prop
Inverse

Here we need to find inverse as $+_5$

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

$Z_5, +_5$ is a Group

Suppose $Z_5 = \{0, 1, 2, 3, 4\}$

For $a = 0$, $0 +_5 0 = 0$

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

ingeneral $a^{-1} = -1$. but it -1 doesnot belong in Z_5

$\therefore$ We are finding for addition modulor 5 $+_5$

1 ke sath kuna no. add karenge ke usa 5 modulo = 0 hai

For this check composition Table

$\therefore$ For $a = 1$ $\quad 1 +_5 a^{-1} = 0 \quad a^{-1} = 4$

Similarly $a = 2$ $\quad 2 +_5 a^{-1} = 0 \quad a^{-1} = 3$

$a = 3$ $\quad 3 +_5 a^{-1} = 0 \quad a^{-1} = 2$

$a = 4$ $\quad 4 +_5 a^{-1} = 0 \quad a^{-1} = 1$

$\therefore$ All inverse exist in Z_5 $\therefore$ property verified.

(2) For Z_5 to be abelian it should be commutative.

$$(a) +_5 (b) = (b_a) +_5 (a)$$

This is true for Z_5 ∴ It is abelian.

(3) Z_5 to be cyclic group it should have generator

For element $a = 0 \in Z_n$

$$a^n = n.a = n.0 = \{0\} \neq Z_5$$

∴ $a = 0$ is not generator of $(Z_5, +_5)$

For $a = 1$

$$a^n = n.a = n.1 = \{0, 1, 2, 3, 4\}$$

for $n = -1$

$$(-1) = (-1)(5) + (4) \rightarrow \text{remainder.}$$

∴ For all values $n = 0, 1, 2, 3 \text{---}$ & $n = -1, -2 \text{---}$.

we get $(0, 1, 2, 3, 4)$

∴ $(Z_5, +_5)$ is Cyclic Group.

∴ if 1 is generator ∴ it's inverse is also generator ∴ $a + a^{-1} = 0$

$$1 + a^{-1} = 0 \quad \therefore \quad a^{-1} = 4$$

∴ (1, 4) are generator for $(Z_5, +_5)$

Q Multiplication Modulo 5 (X_5)
Is (Z_5, X_5) is a Group?

$Z_5 = \{0, 1, 2, 3, 4\}$

Solution Composition Table

X_5	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	1	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Prop 1 Associativity : Z_5, X_5 is associative

Prop 2 Inverse Identity : $e = 1$ for multiplication $1 \in Z_5$

Prop 3 Inverse : For all $a \in Z_5$ Inverse exit
but for multiplicative inverse of 0 doesnot exist.
$a = 0 \in Z_5$ but $a^{-1} \notin$ doesnot exist in Z_5.

∴ Z_5, X_5 is not a group.
∴ It is not a abelian group and cyclic group.

But $Z_5^* = Z_5 - \{0\}$
then (Z_5^*, X_5) is a Group.

Q. $(Z_4, +_4)$ is Group?

$Z_4 = \{0, 1, 2, 3\}$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

→ Composition Table.

1 Prop Associative → It exist for addition.

2-Prop Identity → $e = 0 \in Z_4$

3-Prop Inverse → $a + a^{-1} = 0$

for $a = 1$ $a^{-1} = 3$

Similary for $a = 0, 2, 3$ $a^{-1} = 0, 2, 1$ resp.

$\therefore a^{-1} \in Z_4$ $\therefore$ Inverse exist.

$\therefore (Z_4, +_4)$ is a Group.

Q. Is $(Z_4, +_4)$ is Abelian? Yes.

Q. Is $(Z_4, +_4)$ is a cyclic Group? (Yes)

for $a = 0$ $a^n = n.a = n.0 = \{0\}$

For $a = 1$ $a^n = (n.a) = n.1 = \{0, 1, 2, 3\} \in Z_4$

$\therefore a = 1$ & 3 are generator of Z_4.

$\therefore (Z_4, +_4)$ is cyclic group

Q. (Z_4, X_4) Group, Abelian, Cyclic?

Subgroup Of Group

Let $(G, *)$ be a Group. A non empty subset H of G If the following conditions are satisfied.

1. Identity element $e \in H$ (for $+, \times$) → (*)
2. If $a, b \in H$ than $a * b \in H$ (closure property)
3. if $a \in H$ then $a^{-1} \in H$

Example Q. $G = (Z_5, +_5)$ & $H = (Z_4, +_4)$

$Z_5 = \{0, 1, 2, 3, 4\}$
$Z_4 = \{0, 1, 2, 3\}$
$Z_4 \subseteq Z_5$

Sol Here binary operation are differenet.
∴ H is not Subgroup of G because of different binary operation

Example $H = \{0, 2\}$ is subgroup of $(Z_4, +_4)$ under the operation addition modulo 4.

$H \subseteq Z_4$ this is true ∴ Check property one by one. (H is subset of Z_4)

→ Composition Table

$+_4$ Z_4	0	1	2	3
0	0	1	2	3
2	2	3	0	1

$+_4$	0	2
0	0	2
2	2	0

(1) 1 property identy $e = 0 \in Z_4$

(2) 2 property $a +_4 b \in H$

$0 +_4 0 \in H$ $0 +_4 2 \in H$, $2 +_4 2 \in H$.

∴ It satisfy.

(3) 3 property $a + a^{-1} = 0$

$2 + a^{-1} = 0$ $a^{-1} = 2$

∴ Inverse $\in H$. → ✓

∴ H is subgroup of $(Z_4, +_4)$.

Q $G = (Z, +)$ $H = (2Z, +)$ (2Z → even integer) Is $H \subseteq G$?
Is H is subgroup of $(Z, +)$?

Binary operation are same $G = \{\dots -2, -1, 0, 1, 2 \dots\}$
$\therefore H \subseteq G$ $H = \{\dots -2, 0, 2, 4, 6 \dots\}$

Now check conditions:
1- prop → Identity $e = 0 \in H$
2 prop → $a, b \in H$ then $a + b \in H$
$\therefore$ It satisfy.

3 prop Inverse → for $a + a^{-1} = 0$
$a = 0 \quad a^{-1} = 0$
for $a = 2, 4, 6 \quad a^{-1} = -2, -4, -6 \in H$.
$\therefore$ 3 property satisfy.

$\therefore$ H is subgroup of $[(Z, +) = G]$

Q $H = (3Z, +)$, $G = (Z, +)$ ~~How mean~~
$\therefore$ This also sub group of G.

→ $G = (Z, +)$ and $H = (mZ, +)$ $m > 1$
then H is Subgroup of G.

→ $(Z_m, +_m)$ is not a Subgroup of $(Z, +)$
($+_m$ → different binary operation, $+$ → different binary operation)

$(Z, +)$ & $(Q, +)$ is a subgroups
because $(Z \subseteq Q)$
Similarly for $(Q, +)$ & $(R, +)$