Cyclic group :-

① $(\mathbb{Z},+) \Rightarrow (1)$ & (-1) $G=(a)$

② $(\mathbb{Z}_n, \oplus_n) \Rightarrow (1)$ $\hookrightarrow$ generator

all elts that are rel prime to n

$a^0, a^1, a^2, a^3, \ldots$

e

① For any gp $(G,*)$ $\Rightarrow$ $\{a^n / n \in \mathbb{Z}\}$ forms a subgp
$a \in G$

② Every cyclic gp abelian

③ Every gp of prime order is cyclic

④ " " " " abelian

$o(G) = |G|$

$\boxed{\text{cyclic} \Rightarrow \text{abelian}}$, converse needn't be true

THEOREM:

Every subgroup of a cyclic group is cyclic.

Proof:-

Let $(G, \cdot)$ be a cyclic group. $G = (a)$ where $a \in G$ is generator

Let $(H, \cdot)$ be a subgroup of $(G, \cdot)$. P.T $(H, \cdot)$ is a cyclic group

Every elt of H can be written as some power a. ($\because$ H is a subgp of G

ie all elts of H are of the form $a^n, n \in \mathbb{Z}$

Let n_0 be the smallest integer s.t $a^{n_0} \in H$

I've to prove that $\underline{H = (a^{n_0})}$ | P.T a^{n_0} is the gen of H.

Let $x \in H \Rightarrow x = a^m, m \in \mathbb{Z}$.

Divsn algorithm $\Rightarrow m = q n_0 + r$ $\quad 0 \leq r < n_0$

I've to prove that $r = 0$

suppose, $r \neq 0$

$r = m - q n_0$

$$a^r = a^{m - q n_0} = a^m a^{-q n_0} = a^m \underbrace{(a^{n_0})^{-q}} \in H$$

I got $a^r \in H$, a contradiction

Bcz n_0 is the smallest integer s.t $a^{n_0} \in H$

Bt $r < n_0$ & $a^r \in H$ X

$\because a^m \in H$

$(a^{n_0})^q \in H$

$(a^{n_0})^{-q} \in H$

- Our assumptn is wrong

$\Rightarrow r \neq 0$ was our assumptn.

$\Rightarrow r = 0$

$\therefore x = a^m = a^{q n_0} = (a^{n_0})^q$

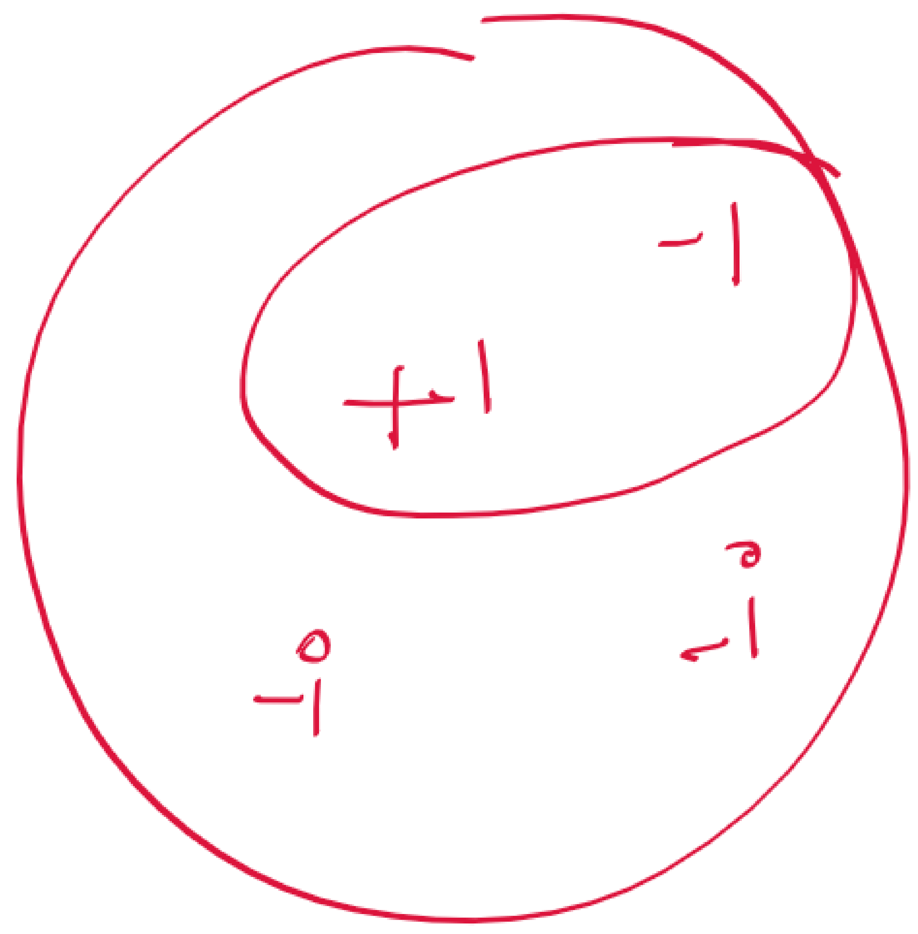
$\therefore \underline{H = (a^{n_0})}$

ex :- $\{1, -1, i, -i\} = G$

$G = (i)$

$H = \{1, -1\}$

$H = (-1)$



$\{i, -i\}$ is not a subgp at all

Dont have 'e'

closure

$i \times -i = 1 \notin$

ORDER OF AN ELEMENT:

The order of an element x of a group G is defined as the least positive integer n, if any, such that $x^n = e$. If there is no such positive integer, then the element is said to have infinite order. The order of x is denoted by $|x|$ or $o(x)$.

order of an elt ⇒

$o(a) \to$ least +ve integer s.t

$a^n = e$

$(G, *)$

$o(G) = |G|$

order of a group = no of elts in group

① $\underline{G = \{1, -1, i, -i\}}$ •

order of the group = 4
order of the generator = 4

$o(-1) = 2$ $\qquad (-1)^2 = e$

$\boxed{o(i) = 4}$ $\qquad (i)^{-} = e$

② $(Z_4, \oplus_4)$

→ (1)
→ (3)

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$o(Z_4) = 4$

order of the group

$o(2) \Rightarrow 2$

$2^0 = 0$
$2^1 = 2$
$2^2 = 0$

$o(3) = \underline{4}$

$3^1 = 3$.
$3^2 = 3 + 3 = 2$
$3^3 = 3 + 3 + 3 = 1$
$3^4 = 3 + 3 + 3 + 3 = 0 = e$

THEOREM:
For any element $x \in G$, $o(x) = o(\langle x \rangle)$.

$\underbrace{o(x)}_{\text{order of an elt } x} = \underbrace{o(\langle x \rangle)}_{\text{order of the subgp generated by the generator } x}$

OR

Let $(G, *)$ be a cyclic group with generator x. Then

$o(G) = o(x)$

Let G be a cyclic group ie $G = (x)$ with generator (x)

Thus every elt of G can be written as powers of x

Let $o(x) = n \Rightarrow x^n = e$

I've to prove that $o(G) = n$

All elts of G can be written as powers of x

$G = \underbrace{\{x^1, x^2, \ldots x^{n-1}, x^n = e\}}$

G has at most n elts

Prove that $x^i \neq x^j \quad 0 \leq i < j < n$

If $x^i = x^j$

$x^i x^{-i} = x^j x^{-i}$

$x^0 = x^{j-i}$

$e = x^{j-i}$ where $j - i < n$

x elt

$o(x) = n$

n is the least +ve integer s.t $x^n = e$

, contradiction

our assumpn is wrong

ie $x^i \neq x^j$

$G = \underbrace{\{x, x^2, x^3 \ldots x^n = e\}}$

No 2 elts are repeated

$\boxed{\therefore o(G) = n}$

Thm :-

order of an elt divides order of the group

OR

Let $(G,*)$ be any group. Let $a \in G$. Then

$o(a) \mid o(G)$

Proof :-

Let $(G,*)$ be a group, let $o(a)=n$ where $a \in G$

$n \to$ least +ve integer s.t $a^n = e$

P.T $n \mid o(G)$

we know that $H=(a)$ is a subgroup of G.

$=\{a, a^2, \ldots a^{n-1}, a^n=e\}$

$\because$ For any group $(G,*)$ & an elt $a \in G$. The subset $\{a^n / n \in Z\}$ is always a subgp of G

H is a cyclic subgp of G generated by the elt a

$o(H)=n$

prev thm

$o(\text{cyclic gp}) = o(\text{generator elt})$

we know that $o(H) \mid o(G)$

Lagrange's thm

$\Rightarrow n \mid o(G)$

$\Rightarrow o(a) \mid o(G)$

Result

Let G be a group of finite order. Let $a \in G$.

Then $a^{o(G)} = e$

$(Z_4, \oplus_4)$

$o(Z_4) = 4$

$2 \in G$

$2^4 = e$

proof

Let $o(a) = n$

$o(G) = qn$ ($\because$ pre thm $o(a) | o(G)$)

$\therefore$ LHS $= a^{o(G)} = a^{qn} = (a^n)^q = e^q$

$= e$

Cyclic gp :-

1. Every cyclic gp is abelian
2. Converse need not be true
3. Every group of prime order is cyclic
4. Every group of prime order is abelian
5. For any group $(G, *)$ and $a \in G$
   $\{a^n / n \in Z\}$ always forms a subgp of G

   But if G is cyclic and 'a' is the generator
   $\{a^n / n \in Z\} = G$

6. Subgp of a cyclic gp is cyclic
7. $o(\text{cyclic group}) = o(\text{generating elt})$
8. $o(a) \mid o(G)$ for any $a \in G$

$o(a) = o(G)$ where $G = (a)$