$(G, *)$ and a subgroup $(H, *)$ $\rightarrow a \in G$

$\rightarrow$ left coset $\left.\begin{matrix} \\ \\ \end{matrix}\right\}$ $aH = \{ah \mid h \in H\}$

Right coset $Ha = \{ha \mid h \in H$

1. Cosets are subsets of G, needn't be subgp
2. Any 2 right cosets have same no of elts
   Any 2 "
3. Any 2 left cosets $<$ disjoint, Identical $\}$ Don't share common elt
4. No of left cosets = No of right cosets
5. $G = \bigcup_{a \in G} Ha$

Lagrange's $\Longrightarrow$ Any subgp H, $o(H) \mid o(G)$

$G = Ha_1 \cup Ha_2 \ldots \cup Ha_k$

$o(G) = \underbrace{o(Ha_1)} + o(Ha_2) + \ldots + o(Ha_k)$ | · Any 2 right cosets are either disj & identi

$= o(Ha_1) + o(Ha_1) + \ldots + o(Ha_1)$ | $o(Ha_i)$ is same for i.

$= k\, o(Ha_1)$

$= k\, o(H)$

$o(H) \mid o(G)$

$k = \dfrac{o(G)}{o(H)} = i_G(H) = i(G:H)$

Index of H in G.

k = no of distinct right cosets of H in G

Let G be a group and x any element of G. The cyclic subgroup of G generated by x is defined to be

$$\boxed{\langle x \rangle = \{ x^n \mid n \in \mathbb{Z} \}.} \quad \text{subgp}$$

That is, $\langle x \rangle$ is the subset containing all powers (positive, negative, and zero) of x. Thus, every element of $\langle x \rangle$ is of the form x^k for some integer k, and vice-versa for every integer k, the element x^k is in $\langle x \rangle$. Clearly, it is a subgroup.

$(G,*) \Rightarrow x \in G$

$\{x^n / n \in Z\} = (x)$

$n \to 0$
$\to +ve$
$\to -ve$

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

$\{i^n / n \in Z\} \Rightarrow \{i^0, i^1, i^2, i^3, i^4, i^5, \dots\}$

✓ $(i) = \{1, i, -1, 1\}$ subg of G

✓ $(-1) = \{(-1)^0, (-1)^1, (-1)^2, (-1)^3, \dots\}$
$= \{-1, 1\}$ " " G

For a gp $(G,*)$ & an elt $x \in G$, The set $H = \{x^n / n \in Z\}$ always forms a subgp

proof:- $a, b \in H$
P.T $ab^{-1} \in H$
$a = x^m \quad b = x^n$
$m, n \in Z$
$ab^{-1} = x^m x^{-n}$
$= x^{m-n}$
$m-n \in Z$,
$x^{m-n} \in H$

Remark.
In any group, the identity element generates the trivial subgroup: $\langle e \rangle = \{e\}$. It is the only one that does (since for all $x \in G$, $x \in \langle x \rangle$).

Any element generates the same subgroup as its inverse: $\langle x \rangle = \langle x^{-1} \rangle$.

i) $(e) = \{e\}$

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

A group G is said to be cyclic if it is equal to the cyclic subgroup generated by one of its elements. That is, G is cyclic if there exists an element $g \in G$ such that $G = \langle g \rangle$. Then g is a generator of G.

cyclic gp :- $G = (a)$

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

$G = (i)$

$i^0 = 1 \quad i^2 = -1$
$i^1 = i \quad i^3 = -i$

$\therefore$ 'i' is a generator of G.

$\therefore (-1)$ is not a generator

$(-1)^0 = 1 \quad (-1)^3 = -1$
$(-1)^1 = -1$

$G = \{1, -1, i, -i\}$ $\cdot \to \times^n$

$H = \{1, -1$

$Ha \to$ operate on right side

$H_1 = \{1, -1\}$

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

$H_i = \{i, -i\}$

② $H_{-i} = \{-i, i\}$

There are 2 distict right cosets

$$i_G(H) = \frac{O(G)}{O(H)} = \frac{4}{2} = 2$$

$$\boxed{i_G(H) = 2}$$

Consequence of Lag thrm

$\to O(G) =$ prime no $= p$

$\to H$ is a subgp of G $\Rightarrow o(H) \mid p$

$\Rightarrow o(H) = 1$ or p

$\underbrace{H = \{e\}}_{\text{Trivial}}$ or $\underbrace{H = G}_{\text{Trivial}}$

$\therefore$ Any gp of prime order has no nontrivial subgp

② $G = \{1, \omega, \omega^2\}$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$\boxed{\omega^3 = 1}$

$\omega^4 = \omega^3 \cdot \omega$

$=$

G is generated by a single elt 'ω'

i) closure

ii) $e = 1$

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

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

$G = (\omega)$

$\omega^0 = 1$

$\omega^1 = \omega$

$\omega^2 = \omega^2$

$\omega^3 = 1$

③ $(Z_5, \oplus_5)$ $\quad Z = \{0, 1, 2, 3, 4\}$

$\oplus_5$	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

i) closed

ii) $e = 0$

iii) $1^{-1} = 4$

$4^{-1} = 1$

$3^{-1} = 2$

$2^{-1} = 3$

'0' can't be the generator

$\therefore G = (1)$

$1^0 = 0$ ✓ $\quad 1^3 = 3$ ✓

$1^1 = 1$ ✓ $\quad 1^4 = 4$ ✓

$1^2 = 1+1 = 2$ ✓ $\quad 1^5 = 0$

$\underbrace{1+1+1+1+1}_{0}$

$G = (2)$

$G = (3)$

$G = (4)$

$\therefore$ 1, 2, 3, 4 all are the gen of $(Z_5, \oplus_5)$

* $(Z_n, \oplus_n)$ is a cyclic gp, $\quad Z_n = (1)$

all the elts in, that are rel prime to n ex:- $(Z_8, \oplus_8) \Rightarrow$

$Z_8 = (1)$
$Z_8 = (3)$
$Z_8 = (5)$
$Z_8 = (7)$

- i) $(Z_n, \oplus_n)$ is cyclic group
The generators are the integers $< n$ which are rel prime to n

$(4) = \{0, 4\}$

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

$\therefore$ $(4) = \{0, 4\}$ is a subgp

* $\{a, e\}$ is a gp under some operatn
$a^{-1} = a$

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

* $a^3 = a * a * a$, $a^0 = e$

* $\{1, -1, i, -i\}$ is cyclic $(G, \cdot)$
$G = (i)$ and $G = (-i)$

* $(\{1, \omega, \omega^2\}, \cdot)$ $\quad G = (\omega)$ & $G = (\omega^2)$

* $(Z_n, \oplus_n) \longrightarrow$ $G = (1)$ & $G = ($nos rel prime to n$)$

4. $(Z_p, \oplus_p)$, p is prime no

$Z_p = (1)$

$Z_p =$ (all the elts expt identity)

ex:- $(Z_7, \oplus_7)$, the generators are $1, 2, 3, 4, 5, 6$

5. $(Z, +)$ is cyclic gp

$Z = (1)$

$Z = (-1)$

Theorem1 A cyclic group is abelian

abelian
$xy = yx$

proof

Let $(G, \circ)$ be a cyclic group

we're to prove that G is abelian ie $xy = yx$

Let $G = (a)$ where a is a generator.

$x, y \in G \Rightarrow x = a^m \quad y = a^n$ where $m, n \in \mathbb{Z}$

$$xy = \underbrace{a^m}_{\substack{m \text{ times} \\ \text{operatn}}} \underbrace{a^n}_{\substack{n \text{ times} \\ \text{operatn}}} = \underbrace{a^{m+n}}_{\substack{m+n \text{ times} \\ \text{operatn}}} = a^n \cdot a^m = yx$$

$xy = yx$

$\therefore$ Abelian

* Every cyclic gp is abelian
Bt the converse is not true. [Every abelian gp need not be cyclic

$(\{1, 3, 5, 7\}, \otimes_8) \rightarrow \boxed{\text{Klein's gp}}$

Abelian
Bt not cyclic

$\otimes_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

i) closed
ii) $e = 1$
iii) $3^{-1} = 3$, $5^{-1} = 5$, $7^{-1} = 7$ } Every elt is inverse of itself

$\therefore$ Abelian

'1' cant be generator

$(3) = \{1, 3\} \qquad (5) = \{1, 5\} \quad \ldots \quad (7) = \{1, 7\}$

$(\{1, 3, 5, 7\}, \otimes_8)$ is not cyclic

$\therefore$ Smallest noncyclic gp

Thm 2 :- Every group of prime order is abelian

Proof :-

consider a gp $(G,*)$ of prime order $\ni$ $o(G)=p$

I've to P.T $(G,*)$ is abelian.
It's enough to prove that $(G,*)$ is cyclic
$\because$ Every cyclic group is abelian
I've P.T $(G,*)$ is cyclic

$o(H) \mid \underbrace{o(G)}_{p}$

Since $o(G)=p$, G has $a \neq e$.

consider a subgp $H=(a)=\{a^n / n \in Z\}$

By Lag thm, $o(H)=1$ or p

$o(H)=1$ is not possible | $a \neq e$ and $a \in H$

Thus the only possiblity is $o(H)=p=o(G)$

H is a subgp of G and $o(H)=o(G)$

This is posible only when $H=G$

$G=(a)$

$\therefore$ G is cyclic

$\therefore$ G is abelian

1. Every cyclic gp is abelian
2. Every gp of prime order is cyclic
3. Every gp of prime order is abelian

Prob Any group with atmost 5 elts is abelian

Soln

I ve to show that any gp of ordr 1, 2, 3, 4, 5 are abelian

Since every gp of prime ordr is abelian, gps of ordr 2, 3, 5 are abelian. I've to prove only for 1, 4

when $o(G) = 1 \implies$ The only gp possible $G = (e)$

$\therefore$ Abelian

where $o(G) = 4 \implies$

Obviously there exists an elt $a \neq e$ in G

Consider $a \in G$, let $H = (a) = \{a^n / n \in \mathbb{Z}\}$ and

H is a subgp of G

$o(H) = 1, 2$ & 4 $(\because o(H) | o(G) = 4$

i) $o(H) = 1$ is not possible, $a \neq e$ and $a \in H$

ii) $o(H) = 4$: $H = G$

$\Rightarrow G$ is cyclic {'a' generates G)

$\Rightarrow G$ is abelian

iii) $o(H) = 2$:$\rightarrow$ $H = \{e, a\} \implies a^{-1} = a$

$G = \{e, a, b, c\}$

$a^{-1} = a$

$a^{-1} = a$

$b^{-1} = b$

$c^{-1} = c$

In this case

G is abelian

$\because$ Every elt is inv of itself

$a^{-1} = a$

$b^{-1} = c$

$c^{-1} = b$

$a * b = b * a$

$a * c = c * a$

$c * b = b * c$

i) $a * b = c$

Illearly $b * a = c$

$\therefore a * b = b * a$

ii) $b * c = e = c * b$

ii) $a * c = c * a$

$\therefore$ Abelian