Proof:— $a \in G$, $|a| = n$.

If $a^k = e \Rightarrow n/k$.

$\Rightarrow a^k = e = a^0 \Rightarrow a^{k-0} = e$

$\Rightarrow n/k - 0$ i.e., n/k.

Theorem:— Let $G = \langle a \rangle$, $|G| = n$.

Then $G = \langle a^k \rangle$ iff $gcd(k, n) = 1$

$\Rightarrow$ Let $gcd(k, n) = 1$

So $\exists$ two integers u, v s.t.

$$ku + nv = 1$$

$$a = a^1 = a^{ku+nv} = a^{ku} \cdot a^{nv}$$

$$= a^{ku} \cdot (a^n)^v = a^{ku} \cdot e = (a^k)^u$$

$a \in \langle a^k \rangle$.

So all powers of a belong to $\langle a^k \rangle$.

$G = \langle a \rangle = \langle a^k \rangle$.

$\left[|a^k| = \dfrac{|a|}{gcd(k,n)} = |a| = n, \text{ when } gcd(k,n) = 1 \right]$

$G = \langle a^k \rangle$.

Conversely, let $G = \langle a^k \rangle$.

If possible, let $gcd(k, n) = d > 1$.

$k = sd$ $\quad n = td$, $\quad t < n$.

$$(a^k)^t = (a^{sd})^t = (a^{td})^s = (a^n)^s = e.$$

$\Rightarrow |a^k| / t < n$.

$\Rightarrow a^k$ is not a generator of G, Contradiction.

$\therefore \quad gcd(k, n) = 1.$

Cor: — $G = Z_n = \langle 1 \rangle$.

$Z_n = \langle k \rangle$ iff $gcd(k, n) = 1$.

The set of generators of $Z_n = U(n)$.

Ex: 1) gen. of $Z_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\} = U(15)$.

2) $U(10) = \{1, 3, 7, 9\}$

$= \langle 3 \rangle = \langle 3^{-1} \rangle = \langle 7 \rangle$

$= \langle 3^k \rangle \quad gcd(k, 4) = 1$

$= \langle 3^3 \rangle = \langle 7 \rangle$

3) $U(14) = \{1, 3, 5, 9, 11, 13\} = \langle 3 \rangle$

$= \langle 3^5 \rangle = \langle$

$3, 9, 27, -3, -9$
$= -1, = 11, = 5$

$11 \equiv -3$

$11^2 = 9 = -5$

$11^3 = 1$

$\frac{121}{14}$

4) $|U(50)| = 20$.

$U(50) = \langle 3 \rangle = \langle 3^3 \rangle = \langle 3^7 \rangle = \langle 3^9 \rangle$

$= \langle 3^{11} \rangle = \langle 3^{13} \rangle = \langle 3^{17} \rangle = \langle 3^{19} \rangle$

Fundamental theorem of cyclic groups:-

Every subgroup of a cyclic group

is cyclic.

$G = \langle a \rangle$

$a^2 \in G$, $\langle a^2 \rangle$ smallest cyclic subgp of G generated by a^2.

$|U(50)| = 20$.

$U(50) = \{3, 9, 27, 31\}$

$= \{1, 3, 7, 9, 11, 13, 17, 19\}$

$H \leq U(50) = \langle 3 \rangle$

$3^1 \in H$

$H = \langle 3^1 \rangle$

$\langle 3^2 \rangle \neq U(50)$.

$\langle 3^2 \rangle \leq U(50)$ cyclic

$\langle 3^{19} \rangle = U(50)$

$\langle 3^{20} \rangle = \langle 1 \rangle \leq U(50)$ cyclic

---

Proof :— Let $G = \langle a \rangle$. Let $H \leq G$.

i) If $H = \{e_G\}$, then H is cyclic.

ii) If $H = G$, then H is cyclic.

iii) H is a proper nontrivial subgp of G.

Every element of H is of the from a^t, $t \in \mathbb{Z}$.

$a^{-5}, a^5 \in H$

$a^t \in H \Rightarrow a^{-t} \in H$ [inv]

H contains some (+)ve integral power of a.

Let m be the smallest (+)ve integer s.t. $a^m \in H$.

claim :— $H = \langle a^m \rangle$.

$\langle a^m \rangle \subseteq H$ [closure prop] ——— (1)

Let $b \in H$ [claim $b = (a^m)^q$ ——— (2) $k = m.q$]

$\Rightarrow b \in G = \langle a \rangle$

$\Rightarrow b = a^k$, $k \in \mathbb{Z}$.

By division algorithm, $\exists$ two integers q and r s.t.

$k = mq + r$, $0 \leq r < m$. ——— (2)

$a^k = a^{mq+r} = (a^m)^q \cdot a^r$

$\Rightarrow a^r = a^k \cdot (a^m)^{-q}$ [Inv prob]

$a^k = b \in H$, $(a^m)^{-q} \in H$ [clos]

$\Rightarrow a^r \in H$ [closure]

$0 \leq r < m$

So $r = 0$, otherwise m fails to be the least (+)ve integer s.t. $a^m \in H$.

from (2), $k = mq$

$\therefore b = a^k = (a^m)^q \in \langle a^m \rangle$

$\therefore H \subseteq \langle a^m \rangle$ ——— (3)

From (1) & (3),

$H = \langle a^m \rangle$, cyclic.