order

$Z_{36} = \langle 1 \rangle = \{0, 1, \ldots, 35\}$ — 36

$+ \pmod{36}$

$\langle 2 \rangle = \{2, 4, 6, 8, \ldots, 34, 0\}$ — $\frac{36}{2} = 18$

$\langle 3 \rangle = \{3, 6, 9, \ldots, 33, 0\}$ — 12

$\langle 4 \rangle = \{4, 8, 12, \ldots, 32, 0\}$ — 9

$\langle 6 \rangle = \{6, 12, 18, 24, 30, 0\}$ — 6

$\langle 9 \rangle = \{9, 18, 27, 0\}$ — 4

$\langle 12 \rangle = \{12, 24, 0\}$ — 3

$\langle 18 \rangle = \{18, 0\}$ — 2

$\langle 0 \rangle = \{0\}$ — $\frac{36}{36} = 1$

① Z_{36} has a unique subgroup H of order K, where K is a divisor of 36 $(|Z_{36}|)$.

② This subgroup H is generated by $\frac{36}{K}$.

$$H = \left\langle \frac{36}{K} \right\rangle.$$

$G = \langle a \rangle$, $|G| = 36 = |a|$

Unique subgp H of order K

$$H = \langle a^{36/K} \rangle.$$

$G = \langle a \rangle$

$\langle a^2 \rangle = \{a^2, a^4, \ldots, a^{34}, e\}$ of order 18

$\langle a^3 \rangle =$ of order 12

$\langle a^4 \rangle =$ 9

$\langle a^6 \rangle =$ 6

$\langle a^9 \rangle =$ 4

$\langle a^{12} \rangle =$ 3

$\langle a^{18} \rangle =$ 2

$\langle e \rangle =$ 1

Ex:— In D_n,

$H = \{ R_0, R_\alpha, R_{2\alpha}, \ldots, R_{(n-1)\alpha} \}$, $\alpha = \frac{360}{n}$.

cyclic group.

$H = \langle R_{\frac{360}{n}} \rangle = \langle R_{k \cdot \frac{360}{n}} \rangle$,

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

Theorem :— $G = \langle a \rangle$

If $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n and for each divisor k of n $\exists$ unique subgroup of order k of $\langle a \rangle$ — namely $\langle a^{n/k} \rangle$.

$\Rightarrow$ $|\langle a \rangle| = n$. $H \leq \langle a \rangle$

$H = \langle a^t \rangle$, for some $t \in \mathbb{N}$.

$(a^t)^n = (a^n)^t = e$

$|a^t| \mid n \Rightarrow |H| \mid n$.

$G = \langle a \rangle$, $|G| = n$.

Let k be a divisor of n.

$(a^{n/k})^k = e$ $(a^{n/k})^{k_1}$ [illegible]

$|a^{n/k}| = k$

$\langle a^{n/k} \rangle$ is a subgroup of order k.

Uniqueness :—

Let $\exists\ H \leq G$ of order k.

$H = \langle a^m \rangle$, m is the least (+)ve integer s.t. $a^m \in H$.

By div. algorithm,

$n = mq + r, \quad 0 \leq r < m.$

$a^n = e$

$\Rightarrow a^{mq+r} = e$

$\Rightarrow a^{mq} \cdot a^r = e$

$\Rightarrow a^r = a^{-mq} = (a^m)^{-q} \in H$

$\therefore r = 0$

$\therefore n = mq \Rightarrow m/n$

$|H| = k$

$\Rightarrow k = |\langle a^m \rangle| = \frac{n}{m}$

$\Rightarrow k = \frac{n}{m} \Rightarrow m = \frac{n}{k}.$

$H = \langle a^m \rangle = \langle a^{n/k} \rangle$

Thm :— If d is a (+)ve divisor of n. Then the number of elements

of order d in a cyclic group G of order n is $\phi(d)$.

$\Rightarrow$ We know $\exists$ unique subgroup H of order d say $\langle a \rangle$.

$H = \langle a \rangle = \langle a^k \rangle$, $\gcd(k,d) = 1$

a^k has order d, where $\gcd(k,d) = 1$.

$\therefore$ H has $\phi(d)$ no of elements of order d.

Ex :—

Z_{36} $\quad \langle 3 \rangle = \langle 15 \rangle = \langle 21 \rangle = \langle 33 \rangle$

has 4 elements of order 12.

$\phi(12)$.

Problem :— $U(2^n)$, $n \geq 3$ is not cyclic.

$\Rightarrow$ $U(n)$, $|n-1| = 2$

$U(2^n)$, $|2^n - 1| = 2$

$[\, 2^n - 1 \equiv -1 \pmod{2^n} \,]$

$|2^{n-1} - 1| = 2$??

$(a^{n-1} \quad)^2 = a^{2n-2}$ $\quad a^{n-1}$

$$(2^{n-1}-1)^2 = 2^{2n-2} - 2\cdot 2^n + 1$$

$$= 2^n(2^{n-2} - 1) + 1$$

$$(2^{n-1}-1)^2 \equiv 1 \pmod{2^n}$$

$$(2^{n-1}+1)^2 \equiv 1 \pmod{2^n}$$

In $U(2^n)$ atleast three elements has order 2;

(2^n-1), $(2^{n-1}-1)$, $(2^{n-1}+1)$

$U(8) \longrightarrow 3, 5, 7$

D_n has $\begin{cases} \text{even} \\ \text{odd} \end{cases}$ n $n+1$ elements of order 2

$U(4)$ is cyclic.

$U(4) = \{1, 3\} = \langle 3 \rangle$.

$U(4) \cong Z_2$

} isomorphic

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

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

$U(10) \cong Z_4$