Cyclic Groups

Recall: A group $(G,*)$ is cyclic if there exists $g \in G$ so that $G = \langle g \rangle = \{g^k : k \in \mathbb{Z}\}$

For any group $(G,*)$ and $a \in G$, set $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ as the cyclic subgroup generated by a.

Recall: Let $a \in G$ with $a^n = e$ for some $n \in \mathbb{Z}_{\geq 1}$. If $a^m \neq e$ for all $0 < m < n$, we say n is the order of a and write $|a| = n$.

Proposition: Let $a \in G$ with $|a| = n$.
5) $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$.

proof: $(\Rightarrow)$ we have $a^b \in \langle a^k \rangle = \{(a^k)^y : y \in \mathbb{Z}\} = \{a^{ky} : y \in \mathbb{Z}\}$ iff $\exists y$ w/ $b = yk \pmod n$.

$a^b \in \langle a^k \rangle \Rightarrow a^b = a^{ky}$
$\Rightarrow a^{b-ky} = a^0$
$\Rightarrow b - ky = 0$
$\Rightarrow b - ky \equiv 0 \pmod n$
$\Rightarrow b \equiv ky \pmod n$

Set $d = \gcd(n,k)$.
So $d = ns + kt$.
If $d \mid b$, then $b = du$ for some $u \in \mathbb{Z}$.
So $b = (ns + kt)u = nsu + ktu$.
If we set $y = tu$, this solves $b \equiv yk \pmod n$.

$b = nsu + ktu$
multiple of n
$b \equiv nsu + ktu \pmod n$
$b \equiv ktu \pmod n$
$b \equiv ky \pmod n$

$(\Leftarrow)$ Suppose we have a solution to $b \equiv yk \pmod n$.
We can write $b = yk + nz$ for some $z \in \mathbb{Z}$.
We have $d \mid k$, $d \mid n$, so $d \mid (yk + nz) = b$.
So $a^b \in \langle a^k \rangle$ iff $d \mid b$.

Exercise: Let $G = S_5$.
Compute $\langle \sigma \rangle$, $\sigma = (123)(45)$
What is $|\sigma|$?

$$\sigma^2 = (123)^2(45)^2 = (132)$$

$$\sigma^3 = (123)^3(45)^3 = (45)$$

$$\sigma^4 = (123)^4(45)^4 = (123)$$

$\sigma^5 = (123)^5(45)^5 = (132)(45$

$\sigma^6 = id$

<u>Example</u>: Consider the group $\mathbb{Z}/12\mathbb{Z}$. Calculate its subgroups.

$\mathbb{Z}/12\mathbb{Z} = \langle [1]_{12} \rangle$

Let H be any subgroup.

Let m be the smallest integer w/ $0 < m \leq 11$ so that $[m]_{12} \in H$.

Let $[n]_{12} \in H$ with $0 \leq n \leq 11$. Since m is the smallest, we actually have $m \leq n \leq 11$.

Write $n = mq + r$ for some $q, r \in \mathbb{Z}$ w/ $0 \leq r < m$.

Recall: Let $n \in \mathbb{Z}$.
Define $a \equiv b \pmod{n}$
For $a \in \mathbb{Z}$,
$[a]_n := \{b \in \mathbb{Z} : b \equiv a \pmod{n}\}$
$= \{b \in \mathbb{Z} : n \mid (b-a)\}$
$= \{a + nk : k \in \mathbb{Z}\}$
For each $a \in \mathbb{Z}$, we can write $a = nq + r$ w/ $0 \leq r \leq n$

We have $r = n - mq$.

Then $[r]_{12} = [n - mq]_{12} = [n]_{12} - q[m]_{12} \in H$ b/c H is subgroup.

But this gives $[r]_{12} \in H$, which is a contradiction unless $r = 0$. Thus $m \mid n$ and so $H = \langle [m]_{12} \rangle$

So $\langle [1]_{12} \rangle = \langle [a]_{12} \rangle = \langle [5]_{12} \rangle = \langle [7]_{12} \rangle = \langle [11]_{12} \rangle$ iff $\gcd(a, 12) = 1$.

$\langle [2]_{12} \rangle = \langle [b]_{12} \rangle = \langle [10]_{12} \rangle$ iff $\gcd(b, 12) = 2$.

$\langle [3]_{12} \rangle = \langle [c]_{12} \rangle = \langle [9]_{12} \rangle$ iff $\gcd(c, 12) = 3$.

$\langle [4]_{12} \rangle = \langle [d]_{12} \rangle = \langle [8]_{12} \rangle$ iff $\gcd(d, 12) = 4$.

$\langle [6]_{12} \rangle = \langle [e]_{12} \rangle$ iff $\gcd(e, 12) = 6$

$$\begin{tikzcd}
 & \mathbb{Z}/12\mathbb{Z} = \langle [1]_{12} \rangle = \langle [5]_{12} \rangle = \langle [7]_{12} \rangle = \langle [11]_{12} \rangle \arrow[dl, dash] \arrow[dr, dash] & \\
\langle [3]_{12} \rangle \arrow[d, dash] & & \langle [2]_{12} \rangle \arrow[d, dash] \\
\langle [6]_{12} \rangle \arrow[dr, dash] & & \langle [4]_{12} \rangle = \langle [8]_{12} \rangle \arrow[dl, dash] \\
 & \langle [0]_{12} \rangle &
\end{tikzcd}$$

Theorem: Let G be a finite cyclic group.

1) Any subgroup of G is cyclic
2) If $H \subseteq G$ is a subgroup, then $\#H \mid \#G$
3) For any divisor $d \mid \#G$, there is a unique subgroup H of G so that $\#H = d$. In particular, if $G = \langle a \rangle$, then $H = \langle a^{n/d} \rangle$.

proof: 1) Let H be a subgroup. $H \neq \{e_G\}$.

Let $G = \langle a \rangle$.

Let m be the smallest positive integer so that $a^m \in H$.

We want to show $H = \langle a^m \rangle$.

Let $a^n \in H$ w/ $n > 0$.

Write $n = mq + r$ for some $q, r \in \mathbb{Z}$, $0 \leq r < m$.

Note $r = n - mq$.

$a^r = a^{n-mq} = a^n (a^m)^{-q} \in H$ b/c H is a subgroup.

This forces $r = 0$ b/c $a^r \in H$ and $r < m$ where m is the smallest positive integer w/ $a^m \in H$. So $a^n = (a^m)^q \in \langle a^m \rangle$.