Properties of cyclic subgroups and groups

Proposition: Let G be a group and $g \in G$. The subset

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

is a subgroup of G.

Proof: If $H \subseteq G$ a subset, then H is a subgroup iff:

1) $H \neq \emptyset$
2) If $a, b \in H$, $ab^{-1} \in H$.

Clearly $\langle g \rangle \neq \emptyset$ since $g \in \langle g \rangle$.

if $a, b \in H$, then $a = g^r$ and $b = g^s$ so

$ab^{-1} = g^r(g^{-s}) = g^{r-s}$ and $r - s \in \mathbb{Z}$

so $g^{r-s} \in \langle g \rangle$. Therefore $\langle g \rangle$ is a subgroup of G.

Proposition: Let G be a group and $g \in G$. Then $\langle g \rangle$ is the smallest subgroup of G containing g, in the sense that, if $H \subset G$ is a subgroup, and $g \in H$, then $\langle g \rangle \subset H$.

Proof: if $H \subseteq G$ is a subgroup and $g \in H$, then

$g^r \in H$ for all $r = 1, 2, \ldots$

$g, g^2, g^3, \ldots \in H$ since H is closed under multiplication

$g^{-1} \in H$, $g^{-2}, g^{-3}, \ldots \in H$.

also $e \in H$.

so $\langle g \rangle \subseteq H$.

Proposition: A cyclic group is abelian.

Proof: Let $a, b \in G = \langle g \rangle$.

Then $a = g^r$

and $b = g^s$

for $r, s \in \mathbb{Z}$.

Therefore $ab = g^r g^s = g^{r+s} = g^{s+r} = g^s g^r = ba$.

So we see that G is abelian.

Proposition: Every subgroup of a cyclic group is cyclic.

Well ordering Principle: Every non-empty set of positive integers has a least element.

Proof: $G = \langle g \rangle$. $H \subseteq G$ is a subgroup.

- Case 1. $H = \{e\}$. In this case H is cyclic, it's $= \langle e \rangle$.
- Case 2. $H \neq \{e\}$. So there is an $h \in H$, with $h \neq e$.

Since G is cyclic, $h = g^r$ for some $r \in \mathbb{Z}$. Either $r > 0$ or $r < 0$. If $r < 0$, then $h^{-1} = g^{-r}$, and $h^{-1} \in H$. $-r > 0$.

$X = \{r \in \mathbb{Z}, r > 0 : g^r \in H\} \neq \emptyset$.

Let t be the smallest element of X.

$a = g^t$. Claim that $H = \langle a \rangle$. To see this,

pick $b \in H$. $b = g^s$ for some $s \in \mathbb{Z}$.

Write: $s = mt + r$ $\quad 0 \leq r < t$. division w/ remainder

$b = g^{mt+r} = g^{mt} \cdot g^r = a^m \cdot g^r$

$g^r = a^{-m} b \in H$

r must be 0 since t is smallest pos. integer with $g^t \in H$. If $r = 0$, we have $e = a^{-m} b$ or $b = a^m$,

$H = \langle a \rangle$ and H is cyclic.

Corollary: The subgroups of $\mathbb{Z}$ are $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$.

$H \subseteq \mathbb{Z}$. $\qquad H = \{0\}$ OR

Choose smallest positive integer in H. Call that n. It follows that

$$H = \langle n \rangle = n\mathbb{Z}.$$