<u>Thm</u> (Fundamental Theorem of Cyclic Groups) FTCG

Consider a cyclic group. Let a be a generator of the group. (Thus the group can be expressed $\langle a \rangle$.)

infinite or finite

1. Every subgroup of a cyclic group is cyclic.

2. If $\langle a \rangle$ has order n, the order of every subgroup of $\langle a \rangle$ is a divisor of n.

* 3. For each divisor d of n, there exists exactly one subgroup of $\langle a \rangle$ of order d, namely $\langle a^{n/d} \rangle$.

proof of FTCG:

1. Consider $\langle a \rangle$ and sps $H \leq \langle a \rangle$. (NTS: H is cyclic.)

need a generator

If $H = \{e\}$, done.

If $H \neq \{e\}$, there exists $a^t \in H$ for some $\underset{\text{nonzero}}{t} \in \mathbb{Z}$.

If $t < 0$, then $\underbrace{(a^t)^{-1}}_{a^{-t}} \in H$. Thus, there exists some positive power of a in H.

Note: every nonempty set of positive integers has a smallest element.

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

We will show that $H = \langle a^m \rangle$.

First $\langle a^m \rangle \subseteq H$ because $a^m \in H$ and H is closed.

generic element of H

OTOH, to see that $H \subseteq \langle a^m \rangle$, sps $a^s \in H$. Write

$s = mq + r$ where $0 \le r < m$. * Then

$$\underbrace{a^s}_{a^s \in H} = a^{mq+r} = \underbrace{(a^m)^q}_{a^m \in H} a^r$$

$\Rightarrow$ $a^r \in H$ (b/c $a^r = a^s (a^m)^{-q}$ and H closed)

$\Rightarrow$ $r = 0$ (b/c $0 \le r < m$)

smallest power in H

$\Rightarrow$ $a^s = a^{mq} = (a^m)^q \in \langle a^m \rangle$.

So $H \subseteq \langle a^m \rangle$ and we conclude that $H = \langle a^m \rangle$.

So: H is cyclic, as desired.