**Thm:** if \( |a| = \infty \)

Then \( a^n = a^m \Rightarrow n = m \).

**Proof** \( |a| = \infty \Rightarrow \exists \)

\( r > 0 \) s.t. \( a^r = e \).

**BWOC,** if \( a^n = a^m \) with \( n > m \)

\( wlog \Rightarrow a^{n-m} = e, \) so \( n-m=r \Rightarrow \)
Theorem: if \( |a| = n \), then
\[
a^i = a^j \iff n \mid i - j
\]

Proof: consider \( \langle a \rangle = \langle \sum_{r \in \mathbb{Z}} a^r \rangle \)

Note that by minimality of \( n \),
\( a^0, a^1, \ldots, a^{n-1} \) are distinct.

(reason - if \( 0 < k < j < n \)

then \( a^k = a^j \Rightarrow e = a^{j-k} \)

but \( j < n \Rightarrow j-k < n \) which contradicts the minimality of \( n \) )
Now let \( s \geq n \) then

\[
S = qn + r \quad \text{with} \quad 0 \leq r \leq n - 1
\]

So \( a^s = a^{qn+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r \in \{a_0, \ldots, a^{n-1}\} \)

\[
\therefore \quad \text{if } |a| = n, \quad <a> = \{a_0, \ldots, a^{n-1}\}
\]
Now prove theorem:

\[ i \implies \text{suppose } a^i = a^j \text{ with } i \leq j \]

\[ j - i \]

\[ \implies a^j = e, \text{ but } \]

\[ j - i = qn + r \text{ with } 0 \leq r \leq n-1 \]

\[ qn + r \]

so \( a^{qn+r} = e \implies a^r = e \)

but \( 0 \leq r < n \)

\[ \implies r = 0 \]

so \( j - i = qn \), i.e. \( n \mid i - j \)
\[ \leq \] suppose \( n \mid i - j \)

then \( i - j = gn \)

so \( a \cdot a^n = e \)

\( a \cdot a = e \)

\[ \Rightarrow i = j \] \( \checkmark \)

\[ \Rightarrow a = a \] \( \checkmark \)
Cor \quad |a| = n \text{ and } a^k = e

\text{then } n | k.

Proof: \quad a^k = e \implies

a^k = a^0 \implies n | k - 0 \implies

n | k \text{ by prev. Thrm.}
This boils down to:

if \(|a| = n\), then \(\langle a \rangle\) is just \(\mathbb{Z}_n^+\).

With the action in the exponents:

\[ \text{e.g., } \ |a| = 8, \quad a^6 \cdot a^2 = a^6 \cdot a^4 = a^{6+4} = a^{10} = a^2 \]

(exponent operations are just \(\mod 6\))
Theorem: Let $G = \langle a \rangle$, $|a| = n$, then $G = \langle a^k \rangle \iff (n,k) = 1$.

Proof: \quad \Rightarrow \quad \text{Suppose } G = \langle a^k \rangle$

\begin{align*}
\langle a \rangle &= \langle a^k \rangle, \quad \text{and } \text{BwOC } (n,k) = d > 1
\end{align*}
Then $k = td$, $n = sd$, with $s < n$

Thus

$$(a^k)^s = (a^{td})^s = (a^{ds})^t$$

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

$$\Rightarrow |a^k| < s < n, \text{ so } \langle a^k \rangle \neq G$$
\[
\exists \ x, y \ \text{such that} \ l = xn + yk
\]
Thus \( a = a' = a^{xn+yk} = a^xn \cdot a^yk \)
\[
= e \cdot (a^k)^y \in \langle a^k \rangle
\]
\[
\Rightarrow \langle a \rangle \subseteq \langle a^k \rangle \quad \text{by closure.}
\]
\[
\therefore \ G \leq \langle a^k \rangle \quad \text{but} \quad \langle a^k \rangle \leq G
\]
\[
G = \langle a^k \rangle
\]
Cor: \( k \) is a generator of \( \mathbb{Z}_n^+ \)

\[ \mathbb{Z}_n^+ \iff \gcd (k, n) = 1 \]

Proof: Since \( \mathbb{Z}_n = \langle 1 \rangle \)

and \( \langle 1^k \rangle = \langle k \rangle \), then applies

(addition-
so \( 1^k = 1+1+1\ldots \text{ k times} \))
**Important**

Theorem: If $G$ is cyclic, then $H \leq G \Rightarrow H$ is cyclic.

Furthermore, if $|G| = n$, then $|H| \mid |G|$, and if $k \mid n$

exists subgroup of order $k$, namely $\langle a^{n/k} \rangle$ where $G = \langle a \rangle$. 
Proof: Let $G = \langle a \rangle$, and $H \leq G$.

If $H = \{e\}$, then $H$ is cyclic and we're done.

Else, suppose $\exists \ b \neq e, b \in H$.

Then $b = a^t$ for some $t$, since $b \in G = \langle a \rangle$. 


$H$ is a subgroup, so $a^t \in H \Rightarrow a^{-t} \in H$, so $H$ has at least one element of the form $a^r$ with $r > 0$. Let $s$ be the smallest positive integer so that $a^s \in H$. 
Claim:  $H = \langle a^s \rangle$.

reason:  $a^s \in H \implies \langle a^s \rangle \leq H$
          by closure.

Now let $h \in H$, $h = a^k$ for some $k$ since $h \in G = \langle a \rangle$. 
Write $k = a^{s+r}$ for $0 \leq r < s$.

$\Rightarrow h = a^{s+r} = a^s \cdot a^r$

$\Rightarrow a^{-s} \cdot h = a^r$

Hence $h \in H$, so by closure, $a \cdot h \in H$

by the minimality of $s$, this $\Rightarrow r = 0$

so $h = a^s \in \langle a^s \rangle$.

$\therefore H \leq \langle a^s \rangle$

and hence $H$ is cyclic as claimed.