# Cyclic Groups

**Recall** A group $G$ is cyclic iff $\exists\ x \in G$ s.t. $G = \langle x \rangle$

**Example:** $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

$U_n = \langle \zeta \rangle$ where $\zeta = e^{2\pi i/n}$

$\mathbb{Z}_n = \langle \bar{1} \rangle$

**Example:** $D_4 = \{1, r, s, sr\}$

$D_4$ is not cyclic

$\langle 1 \rangle = \{1\}$
$\langle r \rangle = \{1, r\} \leftarrow r^2 = 1$
$\langle s \rangle = \{1, s\} \leftarrow s^2 = 1$
$\langle sr \rangle = \{1, sr\} \leftarrow (sr)^2 = 1$

none of these are $D_4$

* $D_4$ is abelian $xy = yx\ \forall\ x, y \in D_4$

**Theorem** Let $G$ be a group
If $G$ is cyclic, then $G$ is abelian

**Proof:** Since $G$ is cyclic $\exists\ g \in G$ where
$G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Let $a, b \in G$, then $a = g^k$ and $b = g^n$ where $k, n \in \mathbb{Z}$

So $ab = g^k g^n = g^{k+n} = g^{n+k} = g^n g^k = ba$

since $a$ & $b$ were arbitrary this shows that $G$ is abelian $\boxtimes$

Theorem: Let $G$ be a cyclic group

If $H$ is a subgroup of $G$, then $H$ is cyclic.

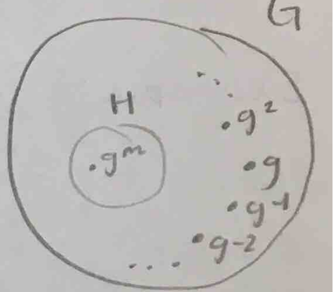
Proof: Let $e$ be the identity of $G$

If $H = \{e\}$, then $H = \langle e \rangle$. So $H$ is cyclic in this case } base case

For the remainder of the proof we assume $H \neq \{e\}$

since $G$ is cyclic we know $G = \langle g \rangle$ for some $g \in G$

since $H \neq \{e\}$ there must be some $g^n \in H$ where $n \neq 0$.




Since $H$ is a subgroup we know that $(g^n)^{-1} = g^{-n}$ is also in $H$, so $H$ must have some positive power of $g$ in $H$.

Let $m$ be the smallest positive integer s.t $g^m \in H$

Claim: $H$ is generated by $g^m \Rightarrow H = \langle g^m \rangle$

Since $g^m \in H$ and $H$ is closed under $*$ and inverses we know that.

$\langle g^m \rangle = \{\ldots, (g^m)^{-2}, (g^m)^{-1}, e, g^m, (g^m)^2, \ldots\}$