Cyclic Groups

Defn A group G is called **cyclic** if there is some $a \in G$ s.t. $G = \langle a \rangle$. In this case, a is called a **generator** of G.

recall: $\langle a \rangle = \{ a^i \mid i \in \mathbb{Z} \}$

Ex. $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\} = \langle 1 \rangle$ for any n.

1 is a generator

Ex. $\mathbb{Z}_9 = \langle 1 \rangle = \langle 4 \rangle$ ← multiple generators for cyclic groups

1 2 3 ...

$\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

3 4 8

Note: cyclic groups are abelian b/c

for all $k, m \in \mathbb{Z}$

$$a^k a^m = a^{k+m} = a^{m+k} = a^m a^k$$

generic elts of $\langle a \rangle$ ... and they commute.

Nonex D_3 is not cyclic.

↳ D_3 not abelian, so can't be cyclic

↳ alt, direct path: compute $\langle x \rangle$ for all $x \in D_3$

↳ none equals to D_3.