Cyclic Groups

- **Video:** A group G is cyclic if

$$G = \langle g \rangle$$

for some $g \in G$.

In other words, $\exists\ g \in G$ such that every element of G is of the form g^k for some $k \in \mathbb{Z}$.

- **Theorem:** If $G = \langle g \rangle$, then

$$\mathrm{ord}(g) = \underbrace{\#\text{ of elements in } G}_{\text{sometimes called "order of } G\text{"}}$$

Worksheet 16: Cyclic Groups

Math 335

Reporter:

Recorder:

Equity Manager:

---

1. To prove that a group G is cyclic, find an element $g \in G$ and calculate $\langle g \rangle = G$. For example:

   (a) Prove that $G = \mathbb{Z}$ is cyclic (where the operation is addition).

   In $\mathbb{Z}$,

   $$\langle 1 \rangle = \{\underbrace{0}_{\text{identity}}, 1, 2, 3, \ldots, \underbrace{-1}_{\text{inverse of } 1}, -2, -3, \ldots\} = \mathbb{Z},$$

   so $\mathbb{Z}$ is cyclic.

   (b) Prove that $G = \{\text{even integers}\}$ is cyclic (where the operation is addition).

   In G,

   $$\langle 2 \rangle = \{0, 2, 4, 6, \ldots, -2, -4, -6, \ldots\} = G,$$

   so G is cyclic.

2. **Open-ended question**: What cyclic groups do we know that have finitely many elements? What cyclic groups do we know that have infinitely many elements?

<u>Finitely many</u>	<u>Infinitely many</u>
$\mathbb{Z}_n$	$\mathbb{Z}$
U_4	$\{\text{even integers}\}$

3. Proving that a group G **isn't** cyclic is harder: you need to show that $\langle g \rangle$ is not equal to G for any $g \in G$. You could do this by trying every single g (as long as there are only finitely many of them), or you could look for a clever trick. For example:

(a) Prove that $G = S_3$ is not cyclic.

ord=1 $\langle e \rangle = \{e\}$

ord=2 $\langle (1,2) \rangle = \{e, (1,2)\}$

ord=2 $\langle (1,3) \rangle = \{e, (1,3)\}$

ord=2 $\langle (2,3) \rangle = \{e, (2,3)\}$

ord=3 $\langle (1,2,3) \rangle = \{e, (1,2,3), (1,3,2)\}$

ord=3 $\langle (1,3,2) \rangle = \{e, (1,3,2), (1,2,3)\}$

This calculates $\langle g \rangle$ for every $g \in S_3$, and none of them is all of S_3, so S_3 is NOT cyclic.

(b) (**Challenge**) Prove that $G = \mathbb{R}$ is not cyclic (where the operation is addition).

<u>Idea</u>: Argue that for any $g \in \mathbb{R}$, the subgroup $\langle g \rangle \subseteq \mathbb{R}$ consists either entirely of rational numbers (if g is rational) or entirely of irrational numbers and zero (if g is irrational). Either way, $\langle g \rangle$ isn't all of $\mathbb{R}$.