Lecture 8
Part 1: Cyclic groups and finitely generated groups
A group $H$ is cyclic if $H$ can be generated by a single element. In other words, there is some element $x \in H$ for which

$$H = \{x^\ell \mid \ell \in \mathbb{Z}\} = \langle x \rangle.$$
Finishing up from last time:

A group $H$ is **cyclic** if $H$ can be generated by a single element. In other words, there is some element $x \in H$ for which

$$H = \{ x^\ell \mid \ell \in \mathbb{Z} \} = \langle x \rangle.$$

Some facts for cyclic groups:

1. Order and order are the same: $|\langle x \rangle| = |x|$.
2. All cyclic groups of the same order are mutually isomorphic.
3. If $a > 0$, then $x$ and $x^a$ generate the same group exactly when $(a, |x|) = 1$. 
Theorem
Let $H = \langle x \rangle$ (i.e. suppose $H$ is cyclic).

1. Every subgroup of a cyclic group is itself cyclic.
   (Specifically, if $K \leq H$, then $K = \{1\}$ or $K = \langle x^d \rangle$ where $d$ is the smallest non-negative integer such that $x^d \in K$.)

2. If $|H| = \infty$, then for any distinct $a, b \in \mathbb{Z}_{\geq 0}$.
   $\langle x^a \rangle \neq \langle x^b \rangle$.

3. If $|H| = n$, then for every $a | n$, there is a unique subgroup of $H$ of order $a$.
   
   (*) This subgroup is generated by $x^d$ where $d = n/a$.
   
   (*) For every $m$, $\langle x^m \rangle = \langle x^{(m,n)} \rangle$.

Example: Consider $\mathbb{Z}_{12} = \langle x \rangle$. This theorem says that $\mathbb{Z}_{12}$ has exactly one subgroup of order $a = 1, 2, 3, 4, 6, \text{ and } 12$. They are

\[
\begin{align*}
a = 1 & : \{1\}, \\
a = 2 & : \langle x^6 \rangle, \\
a = 3 & : \langle x^4 \rangle = \langle x^8 \rangle, \\
a = 4 & : \langle x^3 \rangle = \langle x^9 \rangle, \\
a = 6 & : \langle x^2 \rangle = \langle x^{10} \rangle, \\
a = 12 & : \langle x \rangle = \langle x^5 \rangle = \langle x^7 \rangle = \langle x^{11} \rangle.
\end{align*}
\]
Generators and relations: two ways

Let $G$ be a group, and let $A$ be a subset of $G$. The relations are inherited from $G$, but what does $A$ generate?
Generators and relations: two ways

Let \( G \) be a group, and let \( A \) be a subset of \( G \). The relations are inherited from \( G \), but what does \( A \) generate?

We’ve seen: \( A \) generates the set of elements in \( G \) that look like

\[
a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_\ell^{\epsilon_\ell}, \quad a_i \in A, \, \epsilon_i = \pm 1, \, \ell \in \mathbb{Z}_{\geq 0}
\]
Generators and relations: two ways

Let $G$ be a group, and let $A$ be a subset of $G$. The relations are inherited from $G$, but what does $A$ generate?

We’ve seen: $A$ generates the set of elements in $G$ . . .

Let $\bar{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_\ell^{\epsilon_\ell} \mid a_i \in A, \epsilon_i = \pm 1, \ell \in \mathbb{Z}_{\geq 0}\}$. 
Generators and relations: two ways

Let $G$ be a group, and let $A$ be a subset of $G$. The relations are inherited from $G$, but what does $A$ generate?

We’ve seen: $A$ generates the set of elements in $G$ . . .

Let $\bar{A} = \{a_1^{\epsilon_1}a_2^{\epsilon_2} \cdots a_\ell^{\epsilon_\ell} \mid a_i \in A, \epsilon_i = \pm 1, \ell \in \mathbb{Z}_{\geq 0}\}$.

New definition: Consider all subgroups $H \leq G$ which contain $A$. Then $\langle A \rangle$ should be the smallest of these subgroups.
Let $G$ be a group, and let $A$ be a subset of $G$. The relations are inherited from $G$, but what does $A$ generate?

**We’ve seen:** $A$ generates the set of elements in $G$ . . .

Let $\bar{A} = \{ a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_\ell^{\epsilon_{\ell}} \mid a_i \in A, \epsilon_i = \pm 1, \ell \in \mathbb{Z}_{\geq 0} \}$.

**New definition:** Consider all subgroups $H \leq G$ which contain $A$. Then $\langle A \rangle$ should be the *smallest* of these subgroups, i.e.

$$A \subseteq \langle A \rangle, \text{ and if } A \subseteq H \text{ then } \langle A \rangle \leq H.$$
Generators and relations: two ways

Let $G$ be a group, and let $A$ be a subset of $G$. The relations are inherited from $G$, but what does $A$ generate?

**We’ve seen:** $A$ generates the set of elements in $G$ . . .

Let $\bar{A} = \{a_1^{\epsilon_1}a_2^{\epsilon_2} \cdots a_\ell^{\epsilon_\ell} \mid a_i \in A, \epsilon_i = \pm1, \ell \in \mathbb{Z}_{\geq 0}\}$.

**New definition:** Consider all subgroups $H \leq G$ which contain $A$. Then $\langle A \rangle$ should be the smallest of these subgroups, i.e.

\[ A \subseteq \langle A \rangle, \text{ and if } A \subseteq H \text{ then } \langle A \rangle \leq H. \]

(Does such a thing exist??)
For reference: \( \tilde{A} = \{ a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_\ell^{\epsilon_\ell} \mid a_i \in A, \epsilon_i = \pm 1, \ell \in \mathbb{Z}_{\geq 0} \} \).
For reference: \( \bar{A} = \{ a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_\ell^{\epsilon_\ell} \mid a_i \in A, \epsilon_i = \pm 1, \ell \in \mathbb{Z}_{\geq 0} \} \).

**Proposition**

*If \( A \) is a non-empty collection of subgroups of \( G \), then the intersection of all members of \( A \) is also a subgroup of \( G \), i.e.*

\[
\bigcap_{H \in A} H \leq G.
\]
For reference:  \( \bar{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_\ell^{\epsilon_\ell} | a_i \in A, \epsilon_i = \pm 1, \ell \in \mathbb{Z}_{\geq 0}\} \).

**Proposition**

*If \( A \) is a non-empty collection of subgroups of \( G \), then the intersection of all members of \( A \) is also a subgroup of \( G \), i.e.*

\[
\bigcap_{H \in A} H \leq G.
\]

**Definition**

*If \( A \) is a non-empty subset of \( G \), define the subgroup of \( G \) generated by \( A \) as*

\[
\langle A \rangle = \bigcap_{A \subset H} H.
\]
For reference: \( \tilde{A} = \{ a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_\ell^{\epsilon_\ell} \mid a_i \in A, \epsilon_i = \pm 1, \ell \in \mathbb{Z}_{\geq 0} \} \).

**Proposition**

If \( A \) is a non-empty collection of subgroups of \( G \), then the intersection of all members of \( A \) is also a subgroup of \( G \), i.e.

\[
\bigcap_{H \in A} H \leq G.
\]

**Definition**

If \( A \) is a non-empty subset of \( G \), define the subgroup of \( G \) generated by \( A \) as

\[
\langle A \rangle = \bigcap_{A \subseteq H, H \leq G} H.
\]

**Proposition**

In \( G \), the set of elements generated as words in \( a_i, a_i^{-1} \in A \) is the same as the smallest subgroup of \( G \) containing \( A \), i.e.

\[
\bar{A} = \langle A \rangle.
\]
Part 2: Quotient groups begin
Consider the map

\[ \varphi : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \]

\[ z \mapsto \bar{z}. \]
Consider the map

\[ \varphi : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \]

\[ z \mapsto \bar{z}. \]

\[ \{ \ldots, -8, -4, 0, 4, 8, \ldots \} \mapsto \{0\} \]
\[ \{ \ldots, -7, -3, 1, 5, 9, \ldots \} \mapsto \{1\} \]
\[ \{ \ldots, -6, -2, 2, 6, 10, \ldots \} \mapsto \{2\} \]
\[ \{ \ldots, -5, -1, 3, 7, 11, \ldots \} \mapsto \{3\} \]
Consider the map

$$\varphi : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$$

$$z \mapsto \overline{z}.$$ 

$$\{4z \mid z \in \mathbb{Z}\} = \{\ldots, -8, -4, 0, 4, 8, \ldots\} \mapsto \{0\}$$
$$\{4z + 1 \mid z \in \mathbb{Z}\} = \{\ldots, -7, -3, 1, 5, 9, \ldots\} \mapsto \{1\}$$
$$\{4z + 2 \mid z \in \mathbb{Z}\} = \{\ldots, -6, -2, 2, 6, 10, \ldots\} \mapsto \{2\}$$
$$\{4z + 3 \mid z \in \mathbb{Z}\} = \{\ldots, -5, -1, 3, 7, 11, \ldots\} \mapsto \{3\}$$
Consider the map

\[ \varphi : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \]

\[ z \mapsto \bar{z}. \]

\[ 4\mathbb{Z} = \{ 4z \mid z \in \mathbb{Z} \} = \{ \ldots, -8, -4, 0, 4, 8, \ldots \} \mapsto \{ \bar{0} \} \]

\[ 4\mathbb{Z} + 1 = \{ 4z + 1 \mid z \in \mathbb{Z} \} = \{ \ldots, -7, -3, 1, 5, 9, \ldots \} \mapsto \{ \bar{1} \} \]

\[ 4\mathbb{Z} + 2 = \{ 4z + 2 \mid z \in \mathbb{Z} \} = \{ \ldots, -6, -2, 2, 6, 10, \ldots \} \mapsto \{ \bar{2} \} \]

\[ 4\mathbb{Z} + 3 = \{ 4z + 3 \mid z \in \mathbb{Z} \} = \{ \ldots, -5, -1, 3, 7, 11, \ldots \} \mapsto \{ \bar{3} \} \]