Warmup

Recall, 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

**Multiplicative notation:** $H = \{x^\ell \mid \ell \in \mathbb{Z}\} = \langle x \rangle,$

**Additive notation:** $H = \{\ell x \mid \ell \in \mathbb{Z}\} = \langle x \rangle.$

You try: What are the cyclic subgroups of $S_4$?

---

Last time: Cyclic 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

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

**Proposition**

If $H = \langle x \rangle$, then $|H| = |x|$. Namely,
(1) $|H| = n$ iff $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all distinct,
(2) $|H| = \infty$ iff $x^a \neq x^b$ for all $a \neq b$.

**Theorem**

Any two cyclic subgroups of the same order are isomorphic. In particular, if $|\langle x \rangle| = |\langle y \rangle| < \infty$, then are both cyclic groups of order $n$, then

$\langle x \rangle \to \langle y \rangle$ defined by $x^k \mapsto y^k$

is an isomorphism; and if $|\langle x \rangle| = \infty$, then

$\mathbb{Z} \to \langle x \rangle$ defined by $k \mapsto x^k$

is an isomorphism.

**Notation:** Let $\mathbb{Z}_n$ be the cyclic group of order $n$ (under multiplication).
How many generators?

If $H = \langle x \rangle$, (read "$H$ is generated by $x$, with or without relations"), we call $x$ a **generator**, though it generally is not the only generating element.

**Example:** In $D_8$, $\langle r \rangle = \langle r^3 \rangle$.

**Example:** If $H = \langle x \rangle$, then $H = \langle x^{-1} \rangle = \{(x^{-1})^\ell \mid \ell \in \mathbb{Z}\}$.

**Proposition**

Let $H = \langle x \rangle$.

1. **Assume** $|x| = \infty$. Then $H = \langle x^a \rangle$ iff $a = \pm 1$.
2. **Assume** $|x| = n$. Then $H = \langle x^a \rangle$ iff $(a, n) = 1$.

   *In particular, the number of generators of $H$ is $\phi(n)$ (Euler’s phi function).*

**Lemma 1.** If $x^n = 1$ and $x^m = 1$, then $x^{(m,n)} = 1$.

**Lemma 2.** If $|x| = n$, then $|x^a| = n/(a, n)$. 
Subgroups of cyclic groups

Theorem
Let $H = \langle x \rangle$.

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

\[
\begin{align*}
    a &= 1 : \langle 1 \rangle, \\
    a &= 2 : \langle x^6 \rangle, \\
    a &= 3 : \langle x^4 \rangle = \langle x^8 \rangle, \\
    a &= 4 : \langle x^3 \rangle = \langle x^9 \rangle, \\
    a &= 6 : \langle x^2 \rangle = \langle x^{10} \rangle, \\
    a &= 12 : \langle x \rangle = \langle x^5 \rangle = \langle x^7 \rangle = \langle x^{11} \rangle.
\end{align*}
\]
A subgroup lattice is a graph whose nodes are the subgroups of a group $G$, with an edge drawn between every pair of subgroups $H$, $K$ satisfying

$$H \subseteq K \quad \text{and there are no} \quad H \subseteq L \subseteq K.$$ 

Generally, we draw bigger subgroups higher than lower subgroups.

**Example:** For $G = Z_{12} = \langle x \rangle$, we saw the subgroups are given by

$$1, \langle x^6 \rangle, \langle x^4 \rangle, \langle x^3 \rangle, \langle x^2 \rangle, \text{ and } \langle x \rangle = G.$$ 

So the subgroup lattice for $Z_{12}$ will have 6 vertices.

(In general, $Z_n$ will have one subgroup/vertex for every divisor of $n$.)

To draw the edges, you must compute the partial order of containments. (When justifying your work, show these computations!)

A partial (subgroup) lattice is a graph of the relative containment relationships of a subset of the subgroups of $G$. 

**Subgroup lattices**
Comparing lattices

lattice of $\mathbb{Z}_9 = \langle x \rangle$:

\[
\begin{align*}
\langle x \rangle & \rightarrow \langle x^3 \rangle \\
\langle x^3 \rangle & \rightarrow 1
\end{align*}
\]

lattice of $\mathbb{Z}_3 \times \mathbb{Z}_3 = \langle x \rangle \times \langle y \rangle$:

\[
\begin{align*}
\langle x \rangle \times \langle y \rangle & \rightarrow \langle (x, y) \rangle \\
\langle (x, y) \rangle & \rightarrow \langle x \rangle \times 1 \\
\langle x \rangle \times 1 & \rightarrow 1 \\
\langle (x, y) \rangle & \rightarrow 1
\end{align*}
\]

Conclusion: $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$ are not isomorphic!

Thm: If $G \cong H$, then $G$ and $H$ will have the same lattice. The reverse is not true (consider the lattice of $\mathbb{Z}_4$).

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 $H \leq G$ that contain $A$. Define $\langle A \rangle$ is the smallest of these subgroups, i.e.

$A \subseteq \langle A \rangle$, and if $A \subseteq H$ then $\langle A \rangle \leq H$.

(Does such a thing exist??)
For reference: \( \tilde{A} = \{a_1^{\varepsilon_1}a_2^{\varepsilon_2} \cdots a_\ell^{\varepsilon_\ell} \mid a_i \in A, \varepsilon_i = \pm 1, \ell \in \mathbb{Z}_{\geq 0} \} \).

**Proposition**

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

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

**Definition**

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

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

**Proposition**

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

\[
\tilde{A} = \langle A \rangle.
\]
Defining homomorphisms via generators

Suppose $G = \langle A \rangle$ and $H$ are groups. When does a function

\[ \varphi : A \to H \]

extend to a homomorphism \( \varphi : G \to H \)? Namely, you know

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

So if you know

1. the images of \( a_i \) for all \( a_i \in A \); and
2. \( \varphi \) is a homomorphism;

you know how to calculate

\[ \varphi(a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_{\ell}^{\epsilon_{\ell}}) = \varphi(a_1)^{\epsilon_1} \varphi(a_2)^{\epsilon_2} \cdots \varphi(a_{\ell})^{\epsilon_{\ell}}. \]

But is this map well-defined?

1. \( \varphi(G) \subseteq H \)? Yes! \( H \) is a group.
2. Independent of representatives? Maybe!
   You need to check that the relations hold!

Defining homomorphisms via generators

Define \( \varphi \) on \( A \) and extend via

\[ \varphi(a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_{\ell}^{\epsilon_{\ell}}) = \varphi(a_1)^{\epsilon_1} \varphi(a_2)^{\epsilon_2} \cdots \varphi(a_{\ell})^{\epsilon_{\ell}}. \]

Independent of representatives? Check relations . . .

Example: We know

\[ S_3 = \langle (12), (23) \mid (12)^2 = 1, (23)^2 = 1, (12)(23)(12) = (23)(12)(23) \rangle. \]

Which of the following extend to homomorphisms?

1. \( \varphi : S_3 \to D_6 \) defined by \( (12) \mapsto s, (23) \mapsto sr \)
2. \( \varphi : S_3 \to S_5 \) defined by \( (12) \mapsto (12), (23) \mapsto (23) \)
3. \( \varphi : S_3 \to S_2 \) defined by \( (12) \mapsto (12), (23) \mapsto 1 \)
4. \( \varphi : S_3 \to Z_2 = \langle x \rangle \) defined by \( (12) \mapsto x, (23) \mapsto x \)