Review:

A **homomorphism** is a map \( \varphi : G \to H \) between groups satisfying \( \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \) for all \( g_1, g_2 \in G \). An **isomorphism** is homomorphism that is also a bijection.

We showed that for any homomorphism \( \varphi : G \to H \), the image and the kernel of the map are subgroups of \( H \) and \( G \), respectively:

\[
\varphi(G) = \text{img}(\varphi) = \{ h \in H \mid h = \varphi(g) \text{ for some } g \in G \} \leq H;
\]

\[
\ker(\varphi) = \{ g \in G \mid \varphi(g) = 1_H \} \leq G.
\]

To check if \( H \subseteq G \) is a subgroup,

1. check that \( H \) contains at least one element; and
2. show that for any \( x, y \in H \), you also have that \( xy^{-1} \in H \).  
   *(Subgroup criterion)*

Review:

Let \( A \) be a non-empty subset of \( G \) (not nec. subgroup). The **centralizer** of \( A \) in \( G \) is

\[
C_G(A) = \{ g \in G \mid gag^{-1} = a \text{ for all } a \in A \}.
\]

Since

\[
gag^{-1} = a \iff ga = ag
\]

this is the set of elements which commute with all \( a \) in \( A \).

If \( A = \{a\} \), we write \( C_G(\{a\}) = C_G(a) \).

**Theorem**

*For any non-empty \( A \subseteq G \), \( C_A(G) \) is a subgroup of \( G \).*

The **center** of a group \( G \), denoted \( Z(G) \), is the set of elements which commute with everything in \( G \), i.e. \( Z(G) = C_G(G) \). So \( Z(G) \) is a subgroup of \( G \) of \( C_G(A) \) for all \( A \subseteq G \).
More special subgroups

Let \( A \subseteq G \), and fix \( g \in G \). Then define
\[
\begin{align*}
  gA &= \{ h \in G \mid h = ga \text{ for some } a \in A \}, \\
  Ag &= \{ h \in G \mid h = ag \text{ for some } a \in A \}, \text{ and} \\
  gA g^{-1} &= \{ h \in G \mid h = gag^{-1} \text{ for some } a \in A \}.
\end{align*}
\]

The normalizer of \( A \) in \( G \) is the set
\[
N_G(A) = \{ g \in G \mid gA g^{-1} = A \} = \{ g \in G \mid gA = Ag \}.
\]

**Think:** The centralizer is the set of \( g \in G \) that point-wise fixes \( A \) by conjugation, whereas the normalizer is the set of \( g \in G \) that set-wise fixes \( A \) by conjugation.

**Theorem.** For any \( A \subseteq G \), the normalizer \( N_G(A) \) is a subgroup of \( G \). Moreover, \( Z(G) \leq C_G(A) \leq N_G(A) \leq G \).
From last time, conjugation in $D_6$ looks like

<table>
<thead>
<tr>
<th>$xyx^{-1}$</th>
<th>1</th>
<th>$r$</th>
<th>$r^2$</th>
<th>$s$</th>
<th>$sr$</th>
<th>$sr^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>$r$</td>
<td>$r^2$</td>
<td>$s$</td>
<td>$sr$</td>
<td>$sr^2$</td>
</tr>
<tr>
<td>$r$</td>
<td>1</td>
<td>$r$</td>
<td>$r^2$</td>
<td>$sr$</td>
<td>$sr^2$</td>
<td>$s$</td>
</tr>
<tr>
<td>$r^2$</td>
<td>1</td>
<td>$r$</td>
<td>$r^2$</td>
<td>$sr^2$</td>
<td>$s$</td>
<td>$sr$</td>
</tr>
<tr>
<td>$s$</td>
<td>1</td>
<td>$r^2$</td>
<td>$r$</td>
<td>$s$</td>
<td>$sr^2$</td>
<td>$sr$</td>
</tr>
<tr>
<td>$sr$</td>
<td>1</td>
<td>$r^2$</td>
<td>$r$</td>
<td>$sr^2$</td>
<td>$sr$</td>
<td>$s$</td>
</tr>
<tr>
<td>$sr^2$</td>
<td>1</td>
<td>$r^2$</td>
<td>$r$</td>
<td>$sr$</td>
<td>$s$</td>
<td>$sr^2$</td>
</tr>
</tbody>
</table>
Conjugation in $D_8$ looks like

\[
\begin{array}{c|cccccc|c}
xyx^{-1} & 1 & r & r^2 & r^3 & s & sr & sr^2 & sr^3 \\
\hline
1 & 1 & r & r^2 & r^3 & s & sr & sr^2 & sr^3 \\
r & 1 & r & r^2 & r^3 & sl^2 & sl^3 & s & sr \\
r^2 & 1 & r & r^2 & r^3 & s & sr & sr^2 & sr^3 \\
r^3 & 1 & r & r^2 & r^3 & sl^2 & sl^3 & s & sr \\
s & 1 & r^3 & r^2 & r & s & sr^3 & sr^2 & sr \\
sr & 1 & r^3 & r^2 & r & sr^2 & sr & s & sr^3 \\
sr^2 & 1 & r^3 & r^2 & r & s & sr^3 & sr^2 & sr \\
sr^3 & 1 & r^3 & r^2 & r^2 & sr^2 & sr & s & sr^3 \\
\end{array}
\]
Computing $C_G(A)$, $Z(G)$, and $N_G(A)$

$$C_G(A) = \{ g \in G \mid ga = ag \text{ for all } a \in A \}.$$  
$$Z(G) = \{ g \in G \mid gh = hg \text{ for all } h \in g \}.$$  
$$C_G(A) = \{ g \in G \mid gA = Ag \}.$$  

Shortcut: If $g$ commutes with everything in a subset $A = \{a_1, a_2, \ldots, a_m\} \subseteq G$, then $g$ commutes with any word $a_{i_1}^{\pm 1} a_{i_2}^{\pm 1} \cdots a_{i_\ell}^{\pm 1}$, where $a_{i_j} \in A$.

So $C_G(A) = C_G(\langle A \rangle)$ and $N_G(A) = N_G(\langle A \rangle)$.

For example, if $S$ generates $G$, then $C_G(S) = Z(G)$.

Conversely, if $g_1, g_2, \ldots, g_\ell$ are all contained in $C_G(A)$, $Z(G)$, or $N_G(A)$, then so every word in $\langle g_1, g_2, \ldots, g_\ell \rangle$.

Example: $C_{D_{2n}}(r^2)$, for $n \geq 3$.

First,  
$$r(r^2) = (r^2)r, \quad \text{so } \langle r \rangle \subseteq C_{D_{2n}}(r^2).$$

On the other hand,  
$$sr^2 = r^{-2}s = r^{-n-2}s,$$

which is $r^2s$ if and only if $n = 4$. So we have one of the following:

1. If $n = 4$, then $s, r \in C_{D_8}(r^2)$. So $\langle s, r \rangle \leq C_{D_8}(r^2)$. But $\langle s, r \rangle = D_8$. So $D_8 = C_{D_8}(r^2)$.

2. If $n \neq 4$, then $s \notin C_{D_{2n}}(r^2)$.

Moreover,  
$$(sr^m)r^2 = r^{-2}(sr^m) = r^{n-2}(sr^m) \neq r^2(sr^m).$$

Since every element of $D_{2n}$ can be written as $r^m$ or $sr^m$ for some $0 \leq m \leq n - 1$, we have  
$$C_{D_{2n}}(r^2) = \langle r \rangle = \{1, r, r^2, \ldots, r^{n-1}\}.$$
Example: $Z(D_{2n}), n \geq 3$.

Relevant facts are
(1) the dihedral group $D_{2n}$ is generated by $\{s, r\}$, and
(2) every element of $D_{2n}$ can be written as $r^m$ or $sr^m$ for some $0 \leq m \leq n - 1$.

So we need to compute for which $m$ do we have

\[(i) \quad (r^m)s = s(r^m) \text{ and } r(r^m) = (r^m)r,\]

and for which $m$ do we have

\[(ii) \quad (sr^m)s = s(sr^m) \text{ and } r(sr^m) = (sr^m)r.\]

Both in (i) are satisfied exactly when $r^m = r^{-m}$ ($= r^{n-m}$), i.e. when $m = n - m$, so that $m = n/2$.

For (ii), the second condition always fails, since $r(sr^m) = sr^{m-1}$ and $n \geq 3$.

So

$Z(D_{2n}) = \begin{cases} \{1\} & \text{if } n \text{ is odd,} \\ \{1, r^n/2\} & \text{if } n \text{ is even.}\end{cases}$
More examples

(1) If $G$ is abelian, then
$Z(G) = G$, $C_G(A) = G$, $N_G(A) = G$, for all $A \subseteq G$.

(2) We saw in $G = D_8$, $Z(G) = \{1, r^2\}$, and for $A = \{1, r, r^2, r^3\}$,
$C_G(A) = A$ and $N_G(A) = G$.

(3) Claim: in $G = S_n$, if $A = \{(ij)|1 \leq 1 < j \leq n\}$, then
$C_G(A) = 1$ and $N_G(A) = G$.

Tips for computing $\sigma \tau \sigma^{-1}$:

Fact 1: If $(a_1 a_2 \cdots a_m)$ is a cycle in $S_n$, then
$\sigma(a_1 a_2 \cdots a_m)\sigma^{-1} = (\sigma(a_1)\sigma(a_2) \cdots \sigma(a_m))$.

Fact 2: If $\tau$ has cycle decomposition $\tau = c_1 c_2 \cdots c_r$, then
$\sigma \tau \sigma^{-1} = (\sigma c_1 \sigma^{-1})(\sigma c_2 \sigma^{-1}) \cdots (\sigma c_r \sigma^{-1})$.

Definition: the cycle type of a permutation $\tau$ is the list (in increasing order) of the cycle lengths in the cycle
decomposition of $\tau$. \hspace{1cm} (More later in Section 4.3)

For example, in $S_7$, the cycle type of $(152)(34)$ is $1, 1, 2, 3$. 

(More later in Section 4.3)
Mathematical aside: morphisms in general

In general in math, a (homo)morphism is just a map from one mathematical object to another of its own kind, which obeys the same rules (“structure-preserving”).

(Look up “category theory” if you ever want to feel like you’re doing all math, ever, all at once)

Examples:

1. We just defined homomorphisms of groups
2. Linear transformations are morphisms of vector spaces
3. Any map from one set to another is a morphism of sets (no rules!)

$$\text{Hom}(X,Y) = \{ \varphi : X \to Y \mid \varphi \text{ is structure-preserving} \}$$

Endomorphisms are morphisms from something to itself.

$$\text{End}(X) = \text{Hom}(X, X) = \{ \varphi : X \to X \}$$

Isomorphisms are bijective morphisms.

Automorphisms are bijective endomorphisms.

$$\text{Aut}(X) = \{ \varphi : X \leftrightarrow X \}$$

Group actions

Goal: Build automorphisms of sets (permutations) by using groups.

Fact: $\text{Aut}(A) = S_A$ for a set $A$.

Examples we already know:

1. The dihedral group permutes the set of symmetric states a regular $n$-gon can occupy.
2. The symmetric group $S_X$ permutes the objects of $X$.
3. The invertible matrices permute vectors in a vector space.
4. The symmetric group $S_n$ can also move vectors in $\mathbb{R}^n$ around via permutation matrices. (Recall representations)

Basically, if $A$ is the set we’re permuting, then the goal is to find homomorphisms from $G$ into $S_A$. 
A group action of a group $G$ on a set $A$ is a map from
\[
G \times A \to A
\]
\[
(g, a) \mapsto g \cdot a
\]

that satisfies
\[
g \cdot (h \cdot a) = (gh) \cdot a \quad \text{and} \quad 1 \cdot a = a \quad \text{(structure preserving)}
\]
for all $g, h \in G$, $a \in A$.

We say $G$ acts on $A$, denoted $G \acts A$. 
Two dihedral examples:

(1) The dihedral group \(D_8\) acts on \([4] = \{1, 2, 3, 4\}\) as follows: Label the vertices of the square. For \(g \in D_8\), let \(\sigma_g\) be the permutation given by \(\sigma_g(i)\) is the vertex appearing in \(i\)’s place after applying the symmetry \(g\).

\[
\begin{array}{cccc}
1 & 2 & 3 & 4 \\
2 & 3 & 4 & 1 \\
3 & 4 & 1 & 2 \\
4 & 1 & 2 & 3 \\
\end{array}
\quad
\begin{array}{cccc}
\sigma_1 = 1 & \sigma_r = (1234) & \sigma_{r^2} = (13)(24) & \sigma_{r^3} = (1432) \\
\sigma_s = (12)(34) & \sigma_{rs} = (13) & \sigma_{r^2s} = (14)(23) & \sigma_{r^3s} = (24) \\
\end{array}
\]

(2) Now consider the induced action on size two subsets of \([4]\).
New vocabulary for old examples:

1. The dihedral group acts on the set of symmetric states a regular $n$-gon can occupy by rotations and flips.
2. The symmetric group $S_X$ acts on $X$ by permutation.
3. The invertible matrices act on vector spaces.
4. The symmetric group $S_n$ also acts on $\mathbb{R}^n$ by permutation matrices.

More examples:

1. $\mathbb{R}^\times$ acts on $\mathbb{R}^n$ by scaling:
   \[ x \cdot (v_1, v_2, \ldots, v_n) = (xv_1, xv_2, \ldots, xv_n). \]

2. Any group $G$ acts on itself (let $A = G$) in several ways:
   - left regular action: $g \cdot a = ga$
   - right multiplication: $g \cdot a = ag^{-1}$
   - conjugation: $g \cdot a = gag^{-1}$

Note: The way we’ve been writing the action ($g \cdot a$) is called a left action. Sometimes it can be better to write $a \cdot g$ means $g$ is acting from the right.

The right regular action is $a \cdot g = ag$. (Different from the left action of right multiplication!)