Section 8 – Groups of permutation

Instructor: Yifan Yang

Fall 2006
Outline

1. Permutation groups
   - An example
   - Definitions
   - Symmetric groups

2. The symmetry groups of regular $n$-gons
   - The symmetry group of an equilateral triangle
   - The symmetry group of a square
   - The symmetry group of a regular $n$-gon

3. Cayley’s theorem
Outline

1. Permutation groups
   - An example
   - Definitions
   - Symmetric groups

2. The symmetry groups of regular $n$-gons
   - The symmetry group of an equilateral triangle
   - The symmetry group of a square
   - The symmetry group of a regular $n$-gon

3. Cayley’s theorem
An example

Let $G$ be a group with 3 elements. (For example, $G = \mathbb{Z}_3$ under addition.) Say, the group table is

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$b$</td>
<td>$e$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$e$</td>
<td>$a$</td>
</tr>
</tbody>
</table>

Observe that for $g \in G$ the multiplication of an element on the left by $g$ can be thought of as a function from $G$ to $G$. That is, for every $g \in G$ we can define a function $\lambda_g : G \mapsto G$ by $\lambda_g(h) = gh$. More explicitly, we have

- $\lambda_e: \begin{cases} e \mapsto e \\ a \mapsto a \\ b \mapsto b \end{cases}$
- $\lambda_a: \begin{cases} e \mapsto a \\ a \mapsto b \\ b \mapsto e \end{cases}$
- $\lambda_b: \begin{cases} e \mapsto b \\ a \mapsto e \\ b \mapsto a \end{cases}$
Let $G$ be a group with 3 elements. (For example, $G = \mathbb{Z}_3$ under addition.) Say, the group table is

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$b$</td>
<td>$e$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$e$</td>
<td>$a$</td>
</tr>
</tbody>
</table>

Observe that for $g \in G$ the multiplication of an element on the left by $g$ can be thought of as a function from $G$ to $G$. That is, for every $g \in G$ we can define a function $\lambda_g : G \mapsto G$ by $\lambda_g(h) = gh$. More explicitly, we have

- $\lambda_e : \begin{cases} e \mapsto e \\ a \mapsto a \\ b \mapsto b \end{cases}$
- $\lambda_a : \begin{cases} e \mapsto a \\ a \mapsto b \\ b \mapsto e \end{cases}$
- $\lambda_b : \begin{cases} e \mapsto b \\ a \mapsto a \\ b \mapsto e \end{cases}$
An example

Let $G$ be a group with 3 elements. (For example, $G = \mathbb{Z}_3$ under addition.) Say, the group table is

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$b$</td>
<td>$e$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$e$</td>
<td>$a$</td>
</tr>
</tbody>
</table>

Observe that for $g \in G$ the multiplication of an element on the left by $g$ can be thought of as a function from $G$ to $G$. That is, for every $g \in G$ we can define a function $\lambda_g : G \mapsto G$ by $\lambda_g(h) = gh$. More explicitly, we have

- $\lambda_e : \begin{cases} 
  e \mapsto e \\
  a \mapsto a \\
  b \mapsto b 
\end{cases}$
- $\lambda_a : \begin{cases} 
  e \mapsto a \\
  a \mapsto b \\
  b \mapsto e 
\end{cases}$
- $\lambda_b : \begin{cases} 
  e \mapsto b \\
  a \mapsto e \\
  b \mapsto a 
\end{cases}$
An example

Let $G$ be a group with 3 elements. (For example, $G = \mathbb{Z}_3$ under addition.) Say, the group table is

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$b$</td>
<td>$e$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$e$</td>
<td>$a$</td>
</tr>
</tbody>
</table>

Observe that for $g \in G$ the multiplication of an element on the left by $g$ can be thought of as a function from $G$ to $G$. That is, for every $g \in G$ we can define a function $\lambda_g : G \mapsto G$ by $\lambda_g(h) = gh$. More explicitly, we have

- $\lambda_e : \begin{cases} e \mapsto e \\ a \mapsto a \\ b \mapsto b \end{cases}$
- $\lambda_a : \begin{cases} e \mapsto a \\ a \mapsto b \\ b \mapsto e \end{cases}$
- $\lambda_b : \begin{cases} e \mapsto b \\ a \mapsto e \\ b \mapsto a \end{cases}$
An example

These functions $\lambda_g : G \mapsto G$ satisfy

$$\lambda_g \circ \lambda_h = \lambda_{gh}.$$ 

This is because

$$\lambda_g(\lambda_h(c)) = \lambda_g(hc) = g(hc) = (gh)c = \lambda_{gh}(c)$$

for all $c \in G$. This suggests that there is an isomorphism between $\langle G, \ast \rangle$ and $\langle \{\lambda_e, \lambda_a, \lambda_b\}, \circ \rangle$. Indeed, we have

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$b$</td>
<td>$e$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$e$</td>
<td>$a$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>$\lambda_e$</th>
<th>$\lambda_a$</th>
<th>$\lambda_b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda_e$</td>
<td>$\lambda_e$</td>
<td>$\lambda_a$</td>
<td>$\lambda_b$</td>
</tr>
<tr>
<td>$\lambda_a$</td>
<td>$\lambda_a$</td>
<td>$\lambda_b$</td>
<td>$\lambda_e$</td>
</tr>
<tr>
<td>$\lambda_b$</td>
<td>$\lambda_b$</td>
<td>$\lambda_e$</td>
<td>$\lambda_a$</td>
</tr>
</tbody>
</table>

From these we see that they are isomorphic.
These functions $\lambda_g : G \mapsto G$ satisfy

$$\lambda_g \circ \lambda_h = \lambda_{gh}.$$

This is because

$$\lambda_g(\lambda_h(c)) = \lambda_g(hc) = g(hc) = (gh)c = \lambda_{gh}(c)$$

for all $c \in G$. This suggests that there is an isomorphism between $\langle G, \ast \rangle$ and $\langle \{\lambda_e, \lambda_a, \lambda_b\}, \circ \rangle$. Indeed, we have

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$b$</td>
<td>$e$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$e$</td>
<td>$a$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>$\lambda_e$</th>
<th>$\lambda_a$</th>
<th>$\lambda_b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda_e$</td>
<td>$\lambda_e$</td>
<td>$\lambda_a$</td>
<td>$\lambda_b$</td>
</tr>
<tr>
<td>$\lambda_a$</td>
<td>$\lambda_a$</td>
<td>$\lambda_b$</td>
<td>$\lambda_e$</td>
</tr>
<tr>
<td>$\lambda_b$</td>
<td>$\lambda_b$</td>
<td>$\lambda_e$</td>
<td>$\lambda_a$</td>
</tr>
</tbody>
</table>

From these we see that they are isomorphic.
An example

These functions $\lambda_g : G \mapsto G$ satisfy

$$\lambda_g \circ \lambda_h = \lambda_{gh}.$$ 

This is because

$$\lambda_g(\lambda_h(c)) = \lambda_g(hc) = g(hc) = (gh)c = \lambda_{gh}(c)$$

for all $c \in G$. This suggests that there is an isomorphism between $\langle G, \star \rangle$ and $\langle \{\lambda_e, \lambda_a, \lambda_b\}, \circ \rangle$. Indeed, we have

<table>
<thead>
<tr>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$a$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\lambda_e$</th>
<th>$\lambda_a$</th>
<th>$\lambda_b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda_e$</td>
<td>$\lambda_a$</td>
<td>$\lambda_b$</td>
</tr>
<tr>
<td>$\lambda_a$</td>
<td>$\lambda_a$</td>
<td>$\lambda_b$</td>
</tr>
<tr>
<td>$\lambda_b$</td>
<td>$\lambda_b$</td>
<td>$\lambda_a$</td>
</tr>
</tbody>
</table>

From these we see that they are isomorphic.
These functions $\lambda_g : G \mapsto G$ satisfy

$$\lambda_g \circ \lambda_h = \lambda_{gh}.$$ 

This is because

$$\lambda_g(\lambda_h(c)) = \lambda_g(hc) = g(hc) = (gh)c = \lambda_{gh}(c)$$

for all $c \in G$. This suggests that there is an isomorphism between $\langle G, \ast \rangle$ and $\langle \{\lambda_e, \lambda_a, \lambda_b\}, \circ \rangle$. Indeed, we have

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>e</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>e</td>
<td>a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>$\lambda_e$</th>
<th>$\lambda_a$</th>
<th>$\lambda_b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda_e$</td>
<td>$\lambda_e$</td>
<td>$\lambda_a$</td>
<td>$\lambda_b$</td>
</tr>
<tr>
<td>$\lambda_a$</td>
<td>$\lambda_a$</td>
<td>$\lambda_b$</td>
<td>$\lambda_e$</td>
</tr>
<tr>
<td>$\lambda_b$</td>
<td>$\lambda_b$</td>
<td>$\lambda_e$</td>
<td>$\lambda_a$</td>
</tr>
</tbody>
</table>

From these we see that they are isomorphic.
Furthermore, the functions $\lambda_g$ are all one-to-one and onto, i.e., are permutations of the set $G$. This suggests the following construction of groups.
Furthermore, the functions $\lambda_g$ are all one-to-one and onto, i.e., are permutations of the set $G$. This suggests the following construction of groups.
Outline

1 Permutation groups
   - An example
   - Definitions
   - Symmetric groups

2 The symmetry groups of regular $n$-gons
   - The symmetry group of an equilateral triangle
   - The symmetry group of a square
   - The symmetry group of a regular $n$-gon

3 Cayley’s theorem
Definition (8.3)

Let $A$ be a set. A permutation of $A$ is a one-to-one and onto function from $A$ to $A$.

Theorem (8.5)

Let $A$ be a non-empty set. Then the set $S_A$ of all permutations of $A$ is a group under function composition.

Remark

Permutation groups are very important and basic objects in group theory. We will show later that every group $G$ is isomorphic to a subgroup of the permutation group $S_G$. 
Permutation groups

**Definition (8.3)**

Let $A$ be a set. A *permutation of $A$* is a one-to-one and onto function from $A$ to $A$.

**Theorem (8.5)**

Let $A$ be a non-empty set. Then the set $S_A$ of all permutations of $A$ is a group under function composition.

**Remark**

Permutation groups are very important and basic objects in group theory. We will show later that every group $G$ is isomorphic to a subgroup of the permutation group $S_G$. 
Definition (8.3)
Let $A$ be a set. A permutation of $A$ is a one-to-one and onto function from $A$ to $A$.

Theorem (8.5)
Let $A$ be a non-empty set. Then the set $S_A$ of all permutations of $A$ is a group under function composition.

Remark
Permutation groups are very important and basic objects in group theory. We will show later that every group $G$ is isomorphic to a subgroup of the permutation group $S_G$.
Proof of Theorem 8.3

We need to check four conditions.

1. **Closedness**: Proved in the next slide.
2. **Associativity**: This is clearly since function composition satisfies the associative law.
3. **Identity**: Let \( \iota : A \mapsto A \) be defined by \( \iota(a) = a \) for all \( a \in A \). Then \( \iota \) is an identity element in \( S_A \) since \( \iota \circ \sigma = \sigma \circ \iota = \sigma \) for all \( \sigma \in S_A \).
4. **Inverse**: Let \( \sigma \in S_A \). Define \( \tau : A \mapsto A \) as follows. For \( a \in A \), since \( \sigma \) is onto, there is an element \( a' \) in \( A \) such that \( \sigma(a') = a \). This \( a' \) is unique because \( \sigma \) is one-to-one. Define \( \tau : A \mapsto A \) by \( \tau(a) = a' \). Then \( \tau \) is one-to-one because \( \sigma \) is a function. Also \( \tau \) is onto because for \( b \in A \) we have \( \tau(a) = b \), where \( a = \sigma(b) \). Thus, \( \tau \) is also a permutation. Furthermore, it is easy to see that

\[
\tau \circ \sigma = \sigma \circ \tau = \iota.
\]
We need to check four conditions.

1. **Closedness**: Proved in the next slide.

2. **Associativity**: This is clearly since function composition satisfies the associative law.

3. **Identity**: Let \( \iota : A \rightarrow A \) be defined by \( \iota(a) = a \) for all \( a \in A \). Then \( \iota \) is an identity element in \( S_A \) since \( \iota \circ \sigma = \sigma \circ \iota = \sigma \) for all \( \sigma \in S_A \).

4. **Inverse**: Let \( \sigma \in S_A \). Define \( \tau : A \rightarrow A \) as follows. For \( a \in A \), since \( \sigma \) is onto, there is an element \( a' \) in \( A \) such that \( \sigma(a') = a \). This \( a' \) is unique because \( \sigma \) is one-to-one. Define \( \tau : A \rightarrow A \) by \( \tau(a) = a' \). Then \( \tau \) is one-to-one because \( \sigma \) is a function. Also \( \tau \) is onto because for \( b \in A \) we have \( \tau(a) = b \), where \( a = \sigma(b) \). Thus, \( \tau \) is also a permutation. Furthermore, it is easy to see that \( \tau \circ \sigma = \sigma \circ \tau = \iota \).
We need to check four conditions.

1. **Closedness:** Proved in the next slide.

2. **Associativity:** This is clearly since function composition satisfies the associative law.

3. **Identity:** Let \( \iota : A \mapsto A \) be defined by \( \iota(a) = a \) for all \( a \in A \). Then \( \iota \) is an identity element in \( S_A \) since \( \iota \circ \sigma = \sigma \circ \iota = \sigma \) for all \( \sigma \in S_A \).

4. **Inverse:** Let \( \sigma \in S_A \). Define \( \tau : A \mapsto A \) as follows. For \( a \in A \), since \( \sigma \) is onto, there is an element \( a' \) in \( A \) such that \( \sigma(a') = a \). This \( a' \) is unique because \( \sigma \) is one-to-one. Define \( \tau : A \mapsto A \) by \( \tau(a) = a' \). Then \( \tau \) is one-to-one because \( \sigma \) is a function. Also \( \tau \) is onto because for \( b \in A \) we have \( \tau(a) = b \), where \( a = \sigma(b) \). Thus, \( \tau \) is also a permutation. Furthermore, it is easy to see that \( \tau \circ \sigma = \sigma \circ \tau = \iota \).
Proof of Theorem 8.3

We need to check four conditions.

1. **Closedness**: Proved in the next slide.
2. **Associativity**: This is clearly since function composition satisfies the associative law.
3. **Identity**: Let $\iota : A \rightarrow A$ be defined by $\iota(a) = a$ for all $a \in A$. Then $\iota$ is an identity element in $S_A$ since $\iota \circ \sigma = \sigma \circ \iota = \sigma$ for all $\sigma \in S_A$.
4. **Inverse**: Let $\sigma \in S_A$. Define $\tau : A \rightarrow A$ as follows. For $a \in A$, since $\sigma$ is onto, there is an element $a'$ in $A$ such that $\sigma(a') = a$. This $a'$ is unique because $\sigma$ is one-to-one. Define $\tau : A \rightarrow A$ by $\tau(a) = a'$. Then $\tau$ is one-to-one because $\sigma$ is a function. Also $\tau$ is onto because for $b \in A$ we have $\tau(a) = b$, where $a = \sigma(b)$. Thus, $\tau$ is also a permutation. Furthermore, it is easy to see that $\tau \circ \sigma = \sigma \circ \tau = \iota$. 

Instructor: Yifan Yang
Proof of Theorem 8.3

We need to check four conditions.

1. **Closedness**: Proved in the next slide.

2. **Associativity**: This is clearly since function composition satisfies the associative law.

3. **Identity**: Let \( \iota : A \rightarrow A \) be defined by \( \iota(a) = a \) for all \( a \in A \). Then \( \iota \) is an identity element in \( S_A \) since \( \iota \circ \sigma = \sigma \circ \iota = \sigma \) for all \( \sigma \in S_A \).

4. **Inverse**: Let \( \sigma \in S_A \). Define \( \tau : A \rightarrow A \) as follows. For \( a \in A \), since \( \sigma \) is onto, there is an element \( a' \) in \( A \) such that \( \sigma(a') = a \). This \( a' \) is unique because \( \sigma \) is one-to-one. Define \( \tau : A \rightarrow A \) by \( \tau(a) = a' \). Then \( \tau \) is one-to-one because \( \sigma \) is a function. Also \( \tau \) is onto because for \( b \in A \) we have \( \tau(a) = b \), where \( a = \sigma(b) \). Thus, \( \tau \) is also a permutation. Furthermore, it is easy to see that

\[
\tau \circ \sigma = \sigma \circ \tau = \iota.
\]
Proof of Theorem 8.3

We need to check four conditions.

1. **Closedness**: Proved in the next slide.

2. **Associativity**: This is clearly since function composition satisfies the associative law.

3. **Identity**: Let \( \iota : A \rightarrow A \) be defined by \( \iota(a) = a \) for all \( a \in A \). Then \( \iota \) is an identity element in \( S_A \) since \( \iota \circ \sigma = \sigma \circ \iota = \sigma \) for all \( \sigma \in S_A \).

4. **Inverse**: Let \( \sigma \in S_A \). Define \( \tau : A \rightarrow A \) as follows. For \( a \in A \), since \( \sigma \) is onto, there is an element \( a' \) in \( A \) such that \( \sigma(a') = a \). This \( a' \) is unique because \( \sigma \) is one-to-one. Define \( \tau : A \rightarrow A \) by \( \tau(a) = a' \). Then \( \tau \) is one-to-one because \( \sigma \) is a function. Also \( \tau \) is onto because for \( b \in A \) we have \( \tau(a) = b \), where \( a = \sigma(b) \). Thus, \( \tau \) is also a permutation. Furthermore, it is easy to see that \( \tau \circ \sigma = \sigma \circ \tau = \iota \).
Proof of Theorem 8.3

We need to check four conditions.

1. **Closedness**: Proved in the next slide.
2. **Associativity**: This is clearly since function composition satisfies the associative law.
3. **Identity**: Let \( \iota : A \rightarrow A \) be defined by \( \iota(a) = a \) for all \( a \in A \). Then \( \iota \) is an identity element in \( S_A \) since \( \iota \circ \sigma = \sigma \circ \iota = \sigma \) for all \( \sigma \in S_A \).
4. **Inverse**: Let \( \sigma \in S_A \). Define \( \tau : A \rightarrow A \) as follows. For \( a \in A \), since \( \sigma \) is onto, there is an element \( a' \) in \( A \) such that \( \sigma(a') = a \). This \( a' \) is unique because \( \sigma \) is one-to-one. Define \( \tau : A \rightarrow A \) by \( \tau(a) = a' \). Then \( \tau \) is one-to-one because \( \sigma \) is a function. Also \( \tau \) is onto because for \( b \in A \) we have \( \tau(a) = b \), where \( a = \sigma(b) \). Thus, \( \tau \) is also a permutation. Furthermore, it is easy to see that \( \tau \circ \sigma = \sigma \circ \tau = \iota \).
Proof of Theorem 8.3

We need to check four conditions.

1. **Closedness**: Proved in the next slide.

2. **Associativity**: This is clearly since function composition satisfies the associative law.

3. **Identity**: Let $\iota : A \rightarrow A$ be defined by $\iota(a) = a$ for all $a \in A$. Then $\iota$ is an identity element in $S_A$ since $\iota \circ \sigma = \sigma \circ \iota = \sigma$ for all $\sigma \in S_A$.

4. **Inverse**: Let $\sigma \in S_A$. Define $\tau : A \rightarrow A$ as follows. For $a \in A$, since $\sigma$ is onto, there is an element $a'$ in $A$ such that $\sigma(a') = a$. This $a'$ is unique because $\sigma$ is one-to-one. Define $\tau : A \rightarrow A$ by $\tau(a) = a'$. Then $\tau$ is one-to-one because $\sigma$ is a function. Also $\tau$ is onto because for $b \in A$ we have $\tau(a) = b$, where $a = \sigma(b)$. Thus, $\tau$ is also a permutation. Furthermore, it is easy to see that $\tau \circ \sigma = \sigma \circ \tau = \iota$. 

Instructor: Yifan Yang

Section 8 – Groups of permutation
Proof of Theorem 8.3

We need to check four conditions.

1. **Closedness**: Proved in the next slide.
2. **Associativity**: This is clearly since function composition satisfies the associative law.
3. **Identity**: Let $\iota : A \mapsto A$ be defined by $\iota(a) = a$ for all $a \in A$. Then $\iota$ is an identity element in $S_A$ since $\iota \circ \sigma = \sigma \circ \iota = \sigma$ for all $\sigma \in S_A$.
4. **Inverse**: Let $\sigma \in S_A$. Define $\tau : A \mapsto A$ as follows. For $a \in A$, since $\sigma$ is onto, there is an element $a'$ in $A$ such that $\sigma(a') = a$. This $a'$ is unique because $\sigma$ is one-to-one. Define $\tau : A \mapsto A$ by $\tau(a) = a'$. Then $\tau$ is one-to-one because $\sigma$ is a function. Also $\tau$ is onto because for $b \in A$ we have $\tau(a) = b$, where $a = \sigma(b)$. Thus, $\tau$ is also a permutation. Furthermore, it is easy to see that $\tau \circ \sigma = \sigma \circ \tau = \iota$. 

Instructor: Yifan Yang
Proof of Theorem 8.3

We need to check four conditions.

1. **Closedness**: Proved in the next slide.

2. **Associativity**: This is clearly since function composition satisfies the associative law.

3. **Identity**: Let \( \iota : A \leftrightarrow A \) be defined by \( \iota(a) = a \) for all \( a \in A \). Then \( \iota \) is an identity element in \( S_A \) since \( \iota \circ \sigma = \sigma \circ \iota = \sigma \) for all \( \sigma \in S_A \).

4. **Inverse**: Let \( \sigma \in S_A \). Define \( \tau : A \leftrightarrow A \) as follows. For \( a \in A \), since \( \sigma \) is onto, there is an element \( a' \) in \( A \) such that \( \sigma(a') = a \). This \( a' \) is unique because \( \sigma \) is one-to-one. Define \( \tau : A \leftrightarrow A \) by \( \tau(a) = a' \). Then \( \tau \) is one-to-one because \( \sigma \) is a function. Also \( \tau \) is onto because for \( b \in A \) we have \( \tau(a) = b \), where \( a = \sigma(b) \). Thus, \( \tau \) is also a permutation. Furthermore, it is easy to see that \( \tau \circ \sigma = \sigma \circ \tau = \iota \).
Proof of Theorem 8.3

We need to check four conditions.

1. **Closedness**: Proved in the next slide.
2. **Associativity**: This is clearly since function composition satisfies the associative law.
3. **Identity**: Let $\iota : A \mapsto A$ be defined by $\iota(a) = a$ for all $a \in A$. Then $\iota$ is an identity element in $S_A$ since $\iota \circ \sigma = \sigma \circ \iota = \sigma$ for all $\sigma \in S_A$.
4. **Inverse**: Let $\sigma \in S_A$. Define $\tau : A \mapsto A$ as follows. For $a \in A$, since $\sigma$ is onto, there is an element $a'$ in $A$ such that $\sigma(a') = a$. This $a'$ is unique because $\sigma$ is one-to-one. Define $\tau : A \mapsto A$ by $\tau(a) = a'$. Then $\tau$ is one-to-one because $\sigma$ is a function. Also $\tau$ is onto because for $b \in A$ we have $\tau(a) = b$, where $a = \sigma(b)$. Thus, $\tau$ is also a permutation. Furthermore, it is easy to see that $\tau \circ \sigma = \sigma \circ \tau = \iota$. 

Instructor: Yifan Yang
Proof of closedness

To check that $S_A$ is closed under function composition. We need to check that if $\sigma$ and $\tau$ are one-to-one and onto functions from $A$ to $A$, then $\sigma \circ \tau$ is also one-to-one and onto.

Let us assume that $\sigma, \tau : A \mapsto A$ are one-to-one and onto.

1. **$\sigma \circ \tau$ is one-to-one**: Suppose that $\sigma(\tau(a)) = \sigma(\tau(b))$ for some $a, b \in A$. We need to show that this implies $a = b$. Since $\sigma$ is one-to-one, we have $\tau(a) = \tau(b)$. Also, $\tau$ is one-to-one. Thus, we conclude that $a = b$.

2. **$\sigma \circ \tau$ is onto**: Let $a$ be an element in $A$. Since $\sigma$ is onto, there exists $b$ in $A$ such that $\sigma(b)$. Also, $\tau$ is onto. Therefore there exists $c$ in $A$ such that $\tau(c) = b$. Then we have $\sigma(\tau(c)) = \sigma(b) = a$. This shows that $\sigma \circ \tau$ is onto.
Proof of closedness

To check that $S_A$ is closed under function composition. We need to check that if $\sigma$ and $\tau$ are one-to-one and onto functions from $A$ to $A$, then $\sigma \circ \tau$ is also one-to-one and onto. Let us assume that $\sigma, \tau : A \leftrightarrow A$ are one-to-one and onto.

1. $\sigma \circ \tau$ is one-to-one: Suppose that $\sigma(\tau(a)) = \sigma(\tau(b))$ for some $a, b \in A$. We need to show that this implies $a = b$. Since $\sigma$ is one-to-one, we have $\tau(a) = \tau(b)$. Also, $\tau$ is one-to-one. Thus, we conclude that $a = b$.

2. $\sigma \circ \tau$ is onto: Let $a$ be an element in $A$. Since $\sigma$ is onto, there exists $b$ in $A$ such that $\sigma(b)$. Also, $\tau$ is onto. Therefore there exists $c$ in $A$ such that $\tau(c) = b$. Then we have $\sigma(\tau(c)) = \sigma(b) = a$. This shows that $\sigma \circ \tau$ is onto.
Proof of closedness

To check that $S_A$ is closed under function composition. We need to check that if $\sigma$ and $\tau$ are one-to-one and onto functions from $A$ to $A$, then $\sigma \circ \tau$ is also one-to-one and onto.

Let us assume that $\sigma, \tau : A \mapsto A$ are one-to-one and onto.

1. **$\sigma \circ \tau$ is one-to-one:** Suppose that $\sigma(\tau(a)) = \sigma(\tau(b))$ for some $a, b \in A$. We need to show that this implies $a = b$. Since $\sigma$ is one-to-one, we have $\tau(a) = \tau(b)$. Also, $\tau$ is one-to-one. Thus, we conclude that $a = b$.

2. **$\sigma \circ \tau$ is onto:** Let $a$ be an element in $A$. Since $\sigma$ is onto, there exists $b$ in $A$ such that $\sigma(b)$. Also, $\tau$ is onto. Therefore there exists $c$ in $A$ such that $\tau(c) = b$. Then we have $\sigma(\tau(c)) = \sigma(b) = a$. This shows that $\sigma \circ \tau$ is onto.
Proof of closedness

To check that $S_A$ is closed under function composition. We need to check that if $\sigma$ and $\tau$ are one-to-one and onto functions from $A$ to $A$, then $\sigma \circ \tau$ is also one-to-one and onto.

Let us assume that $\sigma, \tau : A \mapsto A$ are one-to-one and onto.

1. $\sigma \circ \tau$ is one-to-one: Suppose that $\sigma(\tau(a)) = \sigma(\tau(b))$ for some $a, b \in A$. We need to show that this implies $a = b$. Since $\sigma$ is one-to-one, we have $\tau(a) = \tau(b)$. Also, $\tau$ is one-to-one. Thus, we conclude that $a = b$.

2. $\sigma \circ \tau$ is onto: Let $a$ be an element in $A$. Since $\sigma$ is onto, there exists $b$ in $A$ such that $\sigma(b)$. Also, $\tau$ is onto. Therefore there exists $c$ in $A$ such that $\tau(c) = b$. Then we have $\sigma(\tau(c)) = \sigma(b) = a$. This shows that $\sigma \circ \tau$ is onto.
Proof of closedness

To check that $S_A$ is closed under function composition. We need to check that if $\sigma$ and $\tau$ are one-to-one and onto functions from $A$ to $A$, then $\sigma \circ \tau$ is also one-to-one and onto.

Let us assume that $\sigma, \tau : A \mapsto A$ are one-to-one and onto.

1. $\sigma \circ \tau$ is one-to-one: Suppose that $\sigma(\tau(a)) = \sigma(\tau(b))$ for some $a, b \in A$. We need to show that this implies $a = b$.

   Since $\sigma$ is one-to-one, we have $\tau(a) = \tau(b)$. Also, $\tau$ is one-to-one. Thus, we conclude that $a = b$.

2. $\sigma \circ \tau$ is onto: Let $a$ be an element in $A$. Since $\sigma$ is onto, there exists $b$ in $A$ such that $\sigma(b)$. Also, $\tau$ is onto.

   Therefore there exists $c$ in $A$ such that $\tau(c) = b$. Then we have $\sigma(\tau(c)) = \sigma(b) = a$. This shows that $\sigma \circ \tau$ is onto.
To check that $S_A$ is closed under function composition. We need to check that if $\sigma$ and $\tau$ are one-to-one and onto functions from $A$ to $A$, then $\sigma \circ \tau$ is also one-to-one and onto. Let us assume that $\sigma, \tau : A \mapsto A$ are one-to-one and onto.

1. $\sigma \circ \tau$ is one-to-one: Suppose that $\sigma(\tau(a)) = \sigma(\tau(b))$ for some $a, b \in A$. We need to show that this implies $a = b$. Since $\sigma$ is one-to-one, we have $\tau(a) = \tau(b)$. Also, $\tau$ is one-to-one. Thus, we conclude that $a = b$.

2. $\sigma \circ \tau$ is onto: Let $a$ be an element in $A$. Since $\sigma$ is onto, there exists $b$ in $A$ such that $\sigma(b)$. Also, $\tau$ is onto. Therefore there exists $c$ in $A$ such that $\tau(c) = b$. Then we have $\sigma(\tau(c)) = \sigma(b) = a$. This shows that $\sigma \circ \tau$ is onto.
Proof of closedness

To check that $S_A$ is closed under function composition. We need to check that if $\sigma$ and $\tau$ are one-to-one and onto functions from $A$ to $A$, then $\sigma \circ \tau$ is also one-to-one and onto. Let us assume that $\sigma, \tau : A \mapsto A$ are one-to-one and onto.

1. $\sigma \circ \tau$ is one-to-one: Suppose that $\sigma(\tau(a)) = \sigma(\tau(b))$ for some $a, b \in A$. We need to show that this implies $a = b$. Since $\sigma$ is one-to-one, we have $\tau(a) = \tau(b)$. Also, $\tau$ is one-to-one. Thus, we conclude that $a = b$.

2. $\sigma \circ \tau$ is onto: Let $a$ be an element in $A$. Since $\sigma$ is onto, there exists $b$ in $A$ such that $\sigma(b)$. Also, $\tau$ is onto. Therefore there exists $c$ in $A$ such that $\tau(c) = b$. Then we have $\sigma(\tau(c)) = \sigma(b) = a$. This shows that $\sigma \circ \tau$ is onto.
Proof of closedness

To check that $S_A$ is closed under function composition. We need to check that if $\sigma$ and $\tau$ are one-to-one and onto functions from $A$ to $A$, then $\sigma \circ \tau$ is also one-to-one and onto. Let us assume that $\sigma, \tau : A \mapsto A$ are one-to-one and onto.

1. $\sigma \circ \tau$ is one-to-one: Suppose that $\sigma(\tau(a)) = \sigma(\tau(b))$ for some $a, b \in A$. We need to show that this implies $a = b$. Since $\sigma$ is one-to-one, we have $\tau(a) = \tau(b)$. Also, $\tau$ is one-to-one. Thus, we conclude that $a = b$.

2. $\sigma \circ \tau$ is onto: Let $a$ be an element in $A$. Since $\sigma$ is onto, there exists $b$ in $A$ such that $\sigma(b)$. Also, $\tau$ is onto. Therefore there exists $c$ in $A$ such that $\tau(c) = b$. Then we have $\sigma(\tau(c)) = \sigma(b) = a$. This shows that $\sigma \circ \tau$ is onto.
Proof of closedness

To check that $S_A$ is closed under function composition. We need to check that if $\sigma$ and $\tau$ are one-to-one and onto functions from $A$ to $A$, then $\sigma \circ \tau$ is also one-to-one and onto. Let us assume that $\sigma, \tau : A \mapsto A$ are one-to-one and onto.

1. $\sigma \circ \tau$ is one-to-one: Suppose that $\sigma(\tau(a)) = \sigma(\tau(b))$ for some $a, b \in A$. We need to show that this implies $a = b$. Since $\sigma$ is one-to-one, we have $\tau(a) = \tau(b)$. Also, $\tau$ is one-to-one. Thus, we conclude that $a = b$.

2. $\sigma \circ \tau$ is onto: Let $a$ be an element in $A$. Since $\sigma$ is onto, there exists $b$ in $A$ such that $\sigma(b)$. Also, $\tau$ is onto. Therefore there exists $c$ in $A$ such that $\tau(c) = b$. Then we have $\sigma(\tau(c)) = \sigma(b) = a$. This shows that $\sigma \circ \tau$ is onto.
Proof of closedness

To check that $S_A$ is closed under function composition. We need to check that if $\sigma$ and $\tau$ are one-to-one and onto functions from $A$ to $A$, then $\sigma \circ \tau$ is also one-to-one and onto. Let us assume that $\sigma, \tau : A \mapsto A$ are one-to-one and onto.

1. **$\sigma \circ \tau$ is one-to-one:** Suppose that $\sigma(\tau(a)) = \sigma(\tau(b))$ for some $a, b \in A$. We need to show that this implies $a = b$. Since $\sigma$ is one-to-one, we have $\tau(a) = \tau(b)$. Also, $\tau$ is one-to-one. Thus, we conclude that $a = b$.

2. **$\sigma \circ \tau$ is onto:** Let $a$ be an element in $A$. Since $\sigma$ is onto, there exists $b$ in $A$ such that $\sigma(b)$. Also, $\tau$ is onto. Therefore there exists $c$ in $A$ such that $\tau(c) = b$. Then we have $\sigma(\tau(c)) = \sigma(b) = a$. This shows that $\sigma \circ \tau$ is onto.
Outline

1. Permutation groups
   - An example
   - Definitions
   - Symmetric groups

2. The symmetry groups of regular \( n \)-gons
   - The symmetry group of an equilateral triangle
   - The symmetry group of a square
   - The symmetry group of a regular \( n \)-gon

3. Cayley’s theorem

Instructor: Yifan Yang

Section 8 – Groups of permutation
When \( A \) is a finite set with \( n \) elements, we may assume that \( A = \{1, 2, \ldots, n\} \). In this case, we adopt the following notations.

1. We let \( S_n \) denote the group of all permutations of the set \( \{1, \ldots, n\} \) of \( n \) elements. The group \( S_n \) is called the symmetric group on \( n \) letters.

2. For \( \sigma \in S_n \), we express \( \sigma \) in the form

\[
\sigma = \begin{pmatrix}
1 & 2 & \cdots & n \\
\sigma(1) & \sigma(2) & \cdots & \sigma(n)
\end{pmatrix}.
\]

3. For \( \sigma, \tau \in S_n \), we write \( \sigma \circ \tau \) by juxtaposition. That is, we write \( \sigma \tau \) in place of \( \sigma \circ \tau \).
Symmetric groups

When $A$ is a finite set with $n$ elements, we may assume that $A = \{1, 2, \ldots, n\}$. In this case, we adopt the following notations.

1. We let $S_n$ denote the group of all permutations of the set $\{1, \ldots, n\}$ of $n$ elements. The group $S_n$ is called the symmetric group on $n$ letters.

2. For $\sigma \in S_n$, we express $\sigma$ in the form

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

3. For $\sigma, \tau \in S_n$, we write $\sigma \circ \tau$ by juxtaposition. That is, we write $\sigma \tau$ in place of $\sigma \circ \tau$.
Symmetric groups

When $A$ is a finite set with $n$ elements, we may assume that $A = \{1, 2, \ldots, n\}$. In this case, we adopt the following notations.

1. We let $S_n$ denote the group of all permutations of the set $\{1, \ldots, n\}$ of $n$ elements. The group $S_n$ is called the symmetric group on $n$ letters.

2. For $\sigma \in S_n$, we express $\sigma$ in the form

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}. $$

3. For $\sigma, \tau \in S_n$, we write $\sigma \circ \tau$ by juxtaposition. That is, we write $\sigma \tau$ in place of $\sigma \circ \tau$. 
For example, for $n = 3$, the set $S_3$ has 6 elements. They are

\[
\sigma_1 : \begin{cases} 
1 \mapsto 1 \\
2 \mapsto 2 \\
3 \mapsto 3 
\end{cases} \quad \sigma_2 : \begin{cases} 
1 \mapsto 1 \\
2 \mapsto 3 \\
3 \mapsto 2 
\end{cases} \quad \sigma_3 : \begin{cases} 
1 \mapsto 2 \\
2 \mapsto 1 \\
3 \mapsto 3 
\end{cases} \\
\sigma_4 : \begin{cases} 
1 \mapsto 2 \\
2 \mapsto 3 \\
3 \mapsto 1 
\end{cases} \quad \sigma_5 : \begin{cases} 
1 \mapsto 3 \\
2 \mapsto 1 \\
3 \mapsto 2 
\end{cases} \quad \sigma_6 : \begin{cases} 
1 \mapsto 3 \\
2 \mapsto 2 \\
3 \mapsto 1 
\end{cases}
\]

In the new notations, they are represented by

\[
\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\
1 & 2 & 3 
\end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\
1 & 3 & 2 
\end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\
2 & 1 & 3 
\end{pmatrix} \\
\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\
2 & 3 & 1 
\end{pmatrix} \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\
3 & 1 & 2 
\end{pmatrix} \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\
3 & 2 & 1 
\end{pmatrix}
\]
Example

Let us compute

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \]

We have \( \sigma_2 \sigma_3(1) = \sigma_2(\sigma_3(1)) = \sigma_2(2) = 3 \). Also, \( \sigma_2 \sigma_3(2) = \sigma_2(\sigma_3(2)) = \sigma_2(1) = 1 \), and \( \sigma_2 \sigma_3(3) = \sigma_2(\sigma_3(3)) = \sigma_2(3) = 2 \). Therefore, we find

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5. \]
Example

Let us compute

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \]

We have \( \sigma_2 \sigma_3(1) = \sigma_2(\sigma_3(1)) = \sigma_2(2) = 3. \) Also, \( \sigma_2 \sigma_3(2) = \sigma_2(\sigma_3(2)) = \sigma_2(1) = 1, \) and \( \sigma_2 \sigma_3(3) = \sigma_2(\sigma_3(3)) = \sigma_2(3) = 2. \) Therefore, we find

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5. \]
Let us compute

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} . \]

We have \( \sigma_2 \sigma_3(1) = \sigma_2(\sigma_3(1)) = \sigma_2(2) = 3. \) Also, 
\( \sigma_2 \sigma_3(2) = \sigma_2(\sigma_3(2)) = \sigma_2(1) = 1, \) and 
\( \sigma_2 \sigma_3(3) = \sigma_2(\sigma_3(3)) = \sigma_2(3) = 2. \) Therefore, we find 

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5. \]
Example

Let us compute

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \]

We have \( \sigma_2 \sigma_3(1) = \sigma_2(\sigma_3(1)) = \sigma_2(2) = 3 \). Also, \( \sigma_2 \sigma_3(2) = \sigma_2(\sigma_3(2)) = \sigma_2(1) = 1 \), and \( \sigma_2 \sigma_3(3) = \sigma_2(\sigma_3(3)) = \sigma_2(3) = 2 \). Therefore, we find

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5. \]
Let us compute 

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \]

We have \( \sigma_2 \sigma_3(1) = \sigma_2(\sigma_3(1)) = \sigma_2(2) = 3. \) Also, \( \sigma_2 \sigma_3(2) = \sigma_2(\sigma_3(2)) = \sigma_2(1) = 1, \) and \( \sigma_2 \sigma_3(3) = \sigma_2(\sigma_3(3)) = \sigma_2(3) = 2. \) Therefore, we find 

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5. \]
Let us compute

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \]

We have \( \sigma_2 \sigma_3 (1) = \sigma_2 (\sigma_3 (1)) = \sigma_2 (2) = 3. \) Also, \( \sigma_2 \sigma_3 (2) = \sigma_2 (\sigma_3 (2)) = \sigma_2 (1) = 1, \) and \( \sigma_2 \sigma_3 (3) = \sigma_2 (\sigma_3 (3)) = \sigma_2 (3) = 2. \) Therefore, we find

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5. \]
Let us compute

$$\sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

We have $\sigma_2 \sigma_3(1) = \sigma_2(\sigma_3(1)) = \sigma_2(2) = 3$. Also, $\sigma_2 \sigma_3(2) = \sigma_2(\sigma_3(2)) = \sigma_2(1) = 1$, and $\sigma_2 \sigma_3(3) = \sigma_2(\sigma_3(3)) = \sigma_2(3) = 2$. Therefore, we find

$$\sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5.$$
Example

Let us compute

$$\sigma_2\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

We have $\sigma_2\sigma_3(1) = \sigma_2(\sigma_3(1)) = \sigma_2(2) = 3$. Also, $\sigma_2\sigma_3(2) = \sigma_2(\sigma_3(2)) = \sigma_2(1) = 1$, and $\sigma_2\sigma_3(3) = \sigma_2(\sigma_3(3)) = \sigma_2(3) = 2$. Therefore, we find

$$\sigma_2\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5.$$
Example

Let us compute

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \]

We have \( \sigma_2 \sigma_3(1) = \sigma_2(\sigma_3(1)) = \sigma_2(2) = 3. \) Also, 
\( \sigma_2 \sigma_3(2) = \sigma_2(\sigma_3(2)) = \sigma_2(1) = 1, \) and 
\( \sigma_2 \sigma_3(3) = \sigma_2(\sigma_3(3)) = \sigma_2(3) = 2. \) Therefore, we find

\[ \sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 \end{pmatrix} = \sigma_5. \]
Let us compute

\[ \sigma_2\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \]

We have \( \sigma_2\sigma_3(1) = \sigma_2(\sigma_3(1)) = \sigma_2(2) = 3. \) Also, \( \sigma_2\sigma_3(2) = \sigma_2(\sigma_3(2)) = \sigma_2(1) = 1, \) and \( \sigma_2\sigma_3(3) = \sigma_2(\sigma_3(3)) = \sigma_2(3) = 2. \) Therefore, we find

\[ \sigma_2\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5. \]
Example

Let us compute

$$\sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$ 

We have $\sigma_2 \sigma_3(1) = \sigma_2(\sigma_3(1)) = \sigma_2(2) = 3$. Also, $\sigma_2 \sigma_3(2) = \sigma_2(\sigma_3(2)) = \sigma_2(1) = 1$, and $\sigma_2 \sigma_3(3) = \sigma_2(\sigma_3(3)) = \sigma_2(3) = 2$. Therefore, we find

$$\sigma_2 \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5.$$
Let us compute

\[ \sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} . \]

We have \( \sigma_3 \sigma_2(1) = \sigma_3(\sigma_2(1)) = \sigma_3(1) = 2 \). Also, 
\( \sigma_3 \sigma_2(2) = \sigma_3(\sigma_2(2)) = \sigma_3(3) = 3 \), and 
\( \sigma_3 \sigma_2(3) = \sigma_3(\sigma_2(3)) = \sigma_3(2) = 1 \). Therefore, we find

\[ \sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_4 . \]
Let us compute

$$\sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$ 

We have $\sigma_3 \sigma_2(1) = \sigma_3(\sigma_2(1)) = \sigma_3(1) = 2$. Also, $\sigma_3 \sigma_2(2) = \sigma_3(\sigma_2(2)) = \sigma_3(3) = 3$, and $\sigma_3 \sigma_2(3) = \sigma_3(\sigma_2(3)) = \sigma_3(2) = 1$. Therefore, we find

$$\sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_4.$$
Let us compute

\[ \sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}. \]

We have \( \sigma_3 \sigma_2(1) = \sigma_3(\sigma_2(1)) = \sigma_3(1) = 2. \) Also, \( \sigma_3 \sigma_2(2) = \sigma_3(\sigma_2(2)) = \sigma_3(3) = 3, \) and \( \sigma_3 \sigma_2(3) = \sigma_3(\sigma_2(3)) = \sigma_3(2) = 1. \) Therefore, we find

\[ \sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_4. \]
Let us compute

$$\sigma_3\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}. $$

We have $\sigma_3\sigma_2(1) = \sigma_3(\sigma_2(1)) = \sigma_3(1) = 2$. Also, $\sigma_3\sigma_2(2) = \sigma_3(\sigma_2(2)) = \sigma_3(3) = 3$, and $\sigma_3\sigma_2(3) = \sigma_3(\sigma_2(3)) = \sigma_3(2) = 1$. Therefore, we find

$$\sigma_3\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_4.$$
Example

Let us compute

$$\sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$ 

We have $\sigma_3 \sigma_2(1) = \sigma_3(\sigma_2(1)) = \sigma_3(1) = 2$. Also, $\sigma_3 \sigma_2(2) = \sigma_3(\sigma_2(2)) = \sigma_3(3) = 3$, and $\sigma_3 \sigma_2(3) = \sigma_3(\sigma_2(3)) = \sigma_3(2) = 1$. Therefore, we find

$$\sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_4.$$
Let us compute

\[ \sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}. \]

We have \( \sigma_3 \sigma_2(1) = \sigma_3(\sigma_2(1)) = \sigma_3(1) = 2 \). Also, \( \sigma_3 \sigma_2(2) = \sigma_3(\sigma_2(2)) = \sigma_3(3) = 3 \), and \( \sigma_3 \sigma_2(3) = \sigma_3(\sigma_2(3)) = \sigma_3(2) = 1 \). Therefore, we find

\[ \sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_4. \]
Example

Let us compute

$$\sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$ 

We have $$\sigma_3 \sigma_2(1) = \sigma_3(\sigma_2(1)) = \sigma_3(1) = 2.$$ Also, $$\sigma_3 \sigma_2(2) = \sigma_3(\sigma_2(2)) = \sigma_3(3) = 3,$$ and $$\sigma_3 \sigma_2(3) = \sigma_3(\sigma_2(3)) = \sigma_3(2) = 1.$$ Therefore, we find

$$\sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_4.$$
Let us compute

$\sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$

We have $\sigma_3 \sigma_2(1) = \sigma_3(\sigma_2(1)) = \sigma_3(1) = 2$. Also, $\sigma_3 \sigma_2(2) = \sigma_3(\sigma_2(2)) = \sigma_3(3) = 3$, and $\sigma_3 \sigma_2(3) = \sigma_3(\sigma_2(3)) = \sigma_3(2) = 1$. Therefore, we find

$\sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_4.$
Example

Let us compute

\[ \sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}. \]

We have \( \sigma_3 \sigma_2(1) = \sigma_3 (\sigma_2(1)) = \sigma_3(1) = 2. \) Also, \( \sigma_3 \sigma_2(2) = \sigma_3 (\sigma_2(2)) = \sigma_3(3) = 3, \) and \( \sigma_3 \sigma_2(3) = \sigma_3 (\sigma_2(3)) = \sigma_3(2) = 1. \) Therefore, we find

\[ \sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_4. \]
Let us compute

\[\sigma_3\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.\]

We have \(\sigma_3\sigma_2(1) = \sigma_3(\sigma_2(1)) = \sigma_3(1) = 2\). Also, \(\sigma_3\sigma_2(2) = \sigma_3(\sigma_2(2)) = \sigma_3(3) = 3\), and \(\sigma_3\sigma_2(3) = \sigma_3(\sigma_2(3)) = \sigma_3(2) = 1\). Therefore, we find

\[\sigma_3\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_4.\]
Example

Let us compute

$$\sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

We have $\sigma_3 \sigma_2(1) = \sigma_3(\sigma_2(1)) = \sigma_3(1) = 2$. Also,
$\sigma_3 \sigma_2(2) = \sigma_3(\sigma_2(2)) = \sigma_3(3) = 3$, and
$\sigma_3 \sigma_2(3) = \sigma_3(\sigma_2(3)) = \sigma_3(2) = 1$. Therefore, we find

$$\sigma_3 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_4.$$
In the above examples, we have

\[ \sigma_2 \sigma_3 = \sigma_5, \]

and

\[ \sigma_3 \sigma_2 = \sigma_4. \]

Thus, \( S_3 \) is nonabelian. In fact, \( S_n \) is nonabelian for all \( n \geq 3 \).
In-class exercises

1. How many elements does $S_n$ have?

2. Compute

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}. $$

3. Compute

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}. $$
Outline

1. Permutation groups
   - An example
   - Definitions
   - Symmetric groups

2. The symmetry groups of regular \( n \)-gons
   - The symmetry group of an equilateral triangle
   - The symmetry group of a square
   - The symmetry group of a regular \( n \)-gon

3. Cayley’s theorem

Instructor: Yifan Yang
The group of symmetries of an equilateral triangle

How many ways in which we can place two copies of an equilateral triangle with vertices 1, 2, and 3 with vertices on top of vertices?
We have one identical placement, two rotations, and three reflections.
Observe that we can combine any two of the six actions to get another one.
The symmetry group of an equilateral triangle

We have one identical placement, two rotations, and three reflections. Observe that we can combine any two of the six actions to get another one.
The symmetry group of an equilateral triangle

We have one identical placement, two rotations, and three reflections. Observe that we can combine any two of the six actions to get another one.
The symmetry group of an equilateral triangle

We have one identical placement, two rotations, and three reflections.

Observe that we can combine any two of the six actions to get another one.
The symmetry group of an equilateral triangle

We have one identical placement, two rotations, and three reflections. Observe that we can combine any two of the six actions to get another one.
For example, we can rotate counterclockwise, reflect with respect to the center vertical line, and then rotate clockwise. Furthermore, it is clearly that every action has an inverse action. (For a clockwise rotation, the inverse is the counterclockwise rotation, and for a reflection, the inverse is the reflection itself.) Thus, the six actions form a group, called the group $D_3$ of symmetries of an equilateral triangle.
The symmetry group of an equilateral triangle

For example, we can rotate counterclockwise, reflect with respect to the center vertical line, and then rotate clockwise. Furthermore, it is clearly that every action has an inverse action. (For a clockwise rotation, the inverse is the counterclockwise rotation, and for a reflection, the inverse is the reflection itself.) Thus, the six actions form a group, called the group $D_3$ of symmetries of an equilateral triangle.
For example, we can rotate counterclockwise, reflect with respect to the center vertical line, and then rotate clockwise. Furthermore, it is clearly that every action has an inverse action. (For a clockwise rotation, the inverse is the counterclockwise rotation, and for a reflection, the inverse is the reflection itself.) Thus, the six actions form a group, called the group $D_3$ of symmetries of an equilateral triangle.
The symmetry group of an equilateral triangle

For example, we can rotate counterclockwise, reflect with respect to the center vertical line, and then rotate clockwise. Furthermore, it is clearly that every action has an inverse action. (For a clockwise rotation, the inverse is the counterclockwise rotation, and for a reflection, the inverse is the reflection itself.) Thus, the six actions form a group, called the group $D_3$ of symmetries of an equilateral triangle.
The symmetry group of an equilateral triangle

For example, we can rotate counterclockwise, reflect with respect to the center vertical line, and then rotate clockwise. Furthermore, it is clearly that every action has an inverse action. (For a clockwise rotation, the inverse is the counterclockwise rotation, and for a reflection, the inverse is the reflection itself.) Thus, the six actions form a group, called the group $D_3$ of symmetries of an equilateral triangle.
The symmetry group of an equilateral triangle

For example, we can rotate counterclockwise, reflect with respect to the center vertical line, and then rotate clockwise. Furthermore, it is clearly that every action has an inverse action. (For a clockwise rotation, the inverse is the counterclockwise rotation, and for a reflection, the inverse is the reflection itself.) Thus, the six actions form a group, called the group $D_3$ of symmetries of an equilateral triangle.
The symmetry group of an equilateral triangle

For example, we can rotate counterclockwise, reflect with respect to the center vertical line, and then rotate clockwise. Furthermore, it is clearly that every action has an inverse action. (For a clockwise rotation, the inverse is the counterclockwise rotation, and for a reflection, the inverse is the reflection itself.) Thus, the six actions form a group, called the group $D_3$ of symmetries of an equilateral triangle.
The group $D_3$ of symmetries of an equilateral triangle can be represented by $S_3$. Namely, each element of $D_3$ gives rise to a permutation of vertices. For example, in the clockwise rotation, the vertices 1, 2, and 3 change to 2, 3, and 1, respectively. Thus, it can be represented by $egin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. For the reflection with respect to the center vertical line, it is $egin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. 
The group $D_3$ of symmetries of an equilateral triangle can be represented by $S_3$. Namely, each element of $D_3$ gives rise to a permutation of vertices. For example, in the clockwise rotation, the vertices 1, 2, and 3 change to 2, 3, and 1, respectively.

Thus, it can be represented by $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. For the reflection with respect to the center vertical line, it is $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. 

Instructor: Yifan Yang
The group $D_3$ of symmetries of an equilateral triangle can be represented by $S_3$. Namely, each element of $D_3$ gives rise to a permutation of vertices. For example, in the clockwise rotation, the vertices 1, 2, and 3 change to 2, 3, and 1, respectively. Thus, it can be represented by $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. For the reflection with respect to the center vertical line, it is $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. 
The symmetry group of an equilateral triangle

The group $D_3$ of symmetries of an equilateral triangle can be represented by $S_3$. Namely, each element of $D_3$ gives rise to a permutation of vertices. For example, in the clockwise rotation, the vertices 1, 2, and 3 change to 2, 3, and 1, respectively.

Thus, it can be represented by \( \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \). For the reflection with respect to the center vertical line, it is \( \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \).
The group $D_3$ of symmetries of an equilateral triangle can be represented by $S_3$. Namely, each element of $D_3$ gives rise to a permutation of vertices. For example, in the clockwise rotation, the vertices 1, 2, and 3 change to 2, 3, and 1, respectively. Thus, it can be represented by \( \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \). For the reflection with respect to the center vertical line, it is \( \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \).
Outline

1. Permutation groups
   - An example
   - Definitions
   - Symmetric groups

2. The symmetry groups of regular \( n \)-gons
   - The symmetry group of an equilateral triangle
   - The symmetry group of a square
   - The symmetry group of a regular \( n \)-gon

3. Cayley’s theorem

Instructor: Yifan Yang

Section 8 – Groups of permutation
The symmetry group of a square

How many ways in which we can place two copies of a square with vertices on top of vertices?
The symmetry group of a square

We have one identical placement, three rotations, one reflection with respect to the center vertical line, one reflection with respect to the center horizontal line, two reflections with respect to the diagonals.
We have one identical placement, three rotations, one reflection with respect to the center vertical line, one reflection with respect to the center horizontal line, two reflections with respect to the diagonals.
The symmetry group of a square

We have one identical placement, three rotations, one reflection with respect to the center vertical line, one reflection with respect to the center horizontal line, two reflections with respect to the diagonals.
The symmetry group of a square

We have one identical placement, three rotations, one reflection with respect to the center vertical line, one reflection with respect to the center horizontal line, two reflections with respect to the diagonals.
The symmetry group of a square

We have one identical placement, three rotations, one reflection with respect to the center vertical line, one reflection with respect to the center horizontal line, two reflections with respect to the diagonals.
The symmetry group of a square

We have one identical placement, three rotations, one reflection with respect to the center vertical line, one reflection with respect to the center horizontal line, two reflections with respect to the diagonals.
The symmetry group of a square

In terms of permutations of vertices, they are

\[ \rho_0 = (1 \ 2 \ 3 \ 4) \]
\[ \rho_1 = (2 \ 3 \ 4 \ 1) \]
\[ \rho_2 = (1 \ 2 \ 3 \ 4) \]
\[ \rho_3 = (4 \ 1 \ 2 \ 3) \]
\[ \mu_1 = (1 \ 2 \ 3 \ 4) \]
\[ \mu_2 = (4 \ 3 \ 2 \ 1) \]
\[ \delta_1 = (1 \ 2 \ 3 \ 4) \]
\[ \delta_2 = (1 \ 4 \ 3 \ 2) \]

and form a subgroup of order 8 of \( S_4 \).
Outline

1. Permutation groups
   - An example
   - Definitions
   - Symmetric groups

2. The symmetry groups of regular $n$-gons
   - The symmetry group of an equilateral triangle
   - The symmetry group of a square
   - The symmetry group of a regular $n$-gon

3. Cayley’s theorem
The group of symmetries of a regular $n$-gon

Let $D_n$ be the group of symmetries of a regular $n$-gon. The group $D_n$ is called the $n$th dihedral group. Here are some facts about $D_n$.

1. $|D_n| = 2n$.
2. There is an element $\sigma \in D_n$ of order $n$, representing rotation by an angle $2\pi/n$.
3. Let $\tau$ be any element not in $\langle \sigma \rangle$. Then $\tau^2 = e$ since $\tau$ is a reflection.
4. Let $\tau$ be any element not in $\langle \sigma \rangle$. Then $\sigma \tau = \tau \sigma^{n-1}$. (In particular, $D_n$ is nonabelian if $n \geq 3$.)
The group of symmetries of a regular \( n \)-gon

Let \( D_n \) be the group of symmetries of a regular \( n \)-gon. The group \( D_n \) is called the \( n \)th dihedral group. Here are some facts about \( D_n \).

1. \(|D_n| = 2n.

2. There is an element \( \sigma \in D_n \) of order \( n \), representing rotation by an angle \( 2\pi/n \).

3. Let \( \tau \) be any element not in \( \langle \sigma \rangle \). Then \( \tau^2 = e \) since \( \tau \) is a reflection.

4. Let \( \tau \) be any element not in \( \langle \sigma \rangle \). Then \( \sigma \tau = \tau \sigma^{n-1} \). (In particular, \( D_n \) is nonabelian if \( n \geq 3 \).)
Let $D_n$ be the group of symmetries of a regular $n$-gon. The group $D_n$ is called the $n$th dihedral group. Here are some facts about $D_n$.

1. $|D_n| = 2n$.

2. There is an element $\sigma \in D_n$ of order $n$, representing rotation by an angle $2\pi/n$.

3. Let $\tau$ be any element not in $\langle \sigma \rangle$. Then $\tau^2 = e$ since $\tau$ is a reflection.

4. Let $\tau$ be any element not in $\langle \sigma \rangle$. Then $\sigma \tau = \tau \sigma^{n-1}$. (In particular, $D_n$ is nonabelian if $n \geq 3$.)
Let $D_n$ be the group of symmetries of a regular $n$-gon. The group $D_n$ is called the $n$th dihedral group. Here are some facts about $D_n$.

1. $|D_n| = 2n$.

2. There is an element $\sigma \in D_n$ of order $n$, representing rotation by an angle $2\pi/n$.

3. Let $\tau$ be any element not in $\langle \sigma \rangle$. Then $\tau^2 = e$ since $\tau$ is a reflection.

4. Let $\tau$ be any element not in $\langle \sigma \rangle$. Then $\sigma \tau = \tau \sigma^{n-1}$. (In particular, $D_n$ is nonabelian if $n \geq 3$.)
In-class exercises

1. What is the symmetry group of an isosceles triangle?
2. What is the symmetry group of a rectangle that is not a square?
3. What is the symmetry group of a rhombus that is not a square?
4. (For fun) What is the order of symmetric group of a regular tetrahedron?
Theorem (8.16)

Every group is isomorphic to a group of permutations. More precisely, every group $G$ is isomorphic to a subgroup of $S_G$.

Remark

The theorem means that the symmetric groups $S_n$ are the most basic objects in group theory. In theory, if one understands $S_n$ well, then he understands all the finite groups. In reality, many examples or counterexamples for a statement in group theory can be found in $S_n$. 
Theorem (8.16)

Every group is isomorphic to a group of permutations. More precisely, every group $G$ is isomorphic to a subgroup of $S_G$.

Remark

The theorem means that the symmetric groups $S_n$ are the most basic objects in group theory. In theory, if one understands $S_n$ well, then he understands all the finite groups. In reality, many examples or counterexamples for a statement in group theory can be found in $S_n$. 
Proof of Cayley’s theorem

The idea is already seen in the beginning of this section. Let $G$ be a group. For $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(g) = ag$. We claim that

1. $\lambda_a$ is a permutation of $G$,
2. $\lambda_a \circ \lambda_b = \lambda_{ab}$.

Suppose that these are true. Let $\hat{G} = \{ \lambda_a : a \in G \}$. We will show that

3. $\hat{G}$ is a subgroup of $S_G$.
4. Let $\phi : G \to \hat{G}$ defined by $\phi(a) = \lambda_a$ is an isomorphism.

Then we will be done.
The idea is already seen in the beginning of this section. Let $G$ be a group. For $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(g) = ag$. We claim that

1. $\lambda_a$ is a permutation of $G$,
2. $\lambda_a \circ \lambda_b = \lambda_{ab}$.

Suppose that these are true. Let $\hat{G} = \{\lambda_a : a \in G\}$. We will show that

3. $\hat{G}$ is a subgroup of $S_G$.
4. Let $\phi : G \to \hat{G}$ defined by $\phi(a) = \lambda_a$ is an isomorphism.

Then we will be done.
The idea is already seen in the beginning of this section. Let $G$ be a group. For $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(g) = ag$. We claim that

1. $\lambda_a$ is a permutation of $G$,
2. $\lambda_a \circ \lambda_b = \lambda_{ab}$.

Suppose that these are true. Let $\hat{G} = \{\lambda_a : a \in G\}$. We will show that

3. $\hat{G}$ is a subgroup of $S_G$.
4. Let $\phi : G \to \hat{G}$ defined by $\phi(a) = \lambda_a$ is an isomorphism.

Then we will be done.
Proof of Cayley’s theorem

The idea is already seen in the beginning of this section. Let $G$ be a group. For $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(g) = ag$. We claim that

1. $\lambda_a$ is a permutation of $G$,

2. $\lambda_a \circ \lambda_b = \lambda_{ab}$.

Suppose that these are true. Let $\hat{G} = \{\lambda_a : a \in G\}$. We will show that

3. $\hat{G}$ is a subgroup of $S_G$.

4. Let $\phi : G \to \hat{G}$ defined by $\phi(a) = \lambda_a$ is an isomorphism.

Then we will be done.
Proof of Cayley’s theorem

The idea is already seen in the beginning of this section. Let $G$ be a group. For $a \in G$, define $\lambda_a : G \rightarrow G$ by $\lambda_a(g) = ag$. We claim that

1. $\lambda_a$ is a permutation of $G$,
2. $\lambda_a \circ \lambda_b = \lambda_{ab}$.

Suppose that these are true. Let $\hat{G} = \{\lambda_a : a \in G\}$. We will show that

3. $\hat{G}$ is a subgroup of $S_G$.
4. Let $\phi : G \rightarrow \hat{G}$ defined by $\phi(a) = \lambda_a$ is an isomorphism.

Then we will be done.
The idea is already seen in the beginning of this section. Let $G$ be a group. For $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(g) = ag$. We claim that

1. $\lambda_a$ is a permutation of $G$,
2. $\lambda_a \circ \lambda_b = \lambda_{ab}$.

Suppose that these are true. Let $\hat{G} = \{\lambda_a : a \in G\}$. We will show that

3. $\hat{G}$ is a subgroup of $S_G$.
4. Let $\phi : G \to \hat{G}$ defined by $\phi(a) = \lambda_a$ is an isomorphism.

Then we will be done.
Proof of Cayley’s theorem

The idea is already seen in the beginning of this section. Let $G$ be a group. For $a \in G$, define $\lambda_a : G \rightarrow G$ by $\lambda_a(g) = ag$. We claim that

1. $\lambda_a$ is a permutation of $G$,
2. $\lambda_a \circ \lambda_b = \lambda_{ab}$.

Suppose that these are true. Let $\hat{G} = \{\lambda_a : a \in G\}$. We will show that

3. $\hat{G}$ is a subgroup of $S_G$.
4. Let $\phi : G \rightarrow \hat{G}$ defined by $\phi(a) = \lambda_a$ is an isomorphism.

Then we will be done.
Proof of Cayley’s theorem

The idea is already seen in the beginning of this section. Let $G$ be a group. For $a \in G$, define $\lambda_a : G \rightarrow G$ by $\lambda_a(g) = ag$. We claim that

1. $\lambda_a$ is a permutation of $G$,
2. $\lambda_a \circ \lambda_b = \lambda_{ab}$.

Suppose that these are true. Let $\hat{G} = \{ \lambda_a : a \in G \}$. We will show that

3. $\hat{G}$ is a subgroup of $S_G$.
4. Let $\phi : G \rightarrow \hat{G}$ defined by $\phi(a) = \lambda_a$ is an isomorphism.

Then we will be done.
Proof of Cayley’s theorem

The idea is already seen in the beginning of this section. Let $G$ be a group. For $a \in G$, define $\lambda_a : G \rightarrow G$ by $\lambda_a(g) = ag$. We claim that

1. $\lambda_a$ is a permutation of $G$,
2. $\lambda_a \circ \lambda_b = \lambda_{ab}$.

Suppose that these are true. Let $\hat{G} = \{\lambda_a : a \in G\}$. We will show that

3. $\hat{G}$ is a subgroup of $S_G$.
4. Let $\phi : G \rightarrow \hat{G}$ defined by $\phi(a) = \lambda_a$ is an isomorphism.

Then we will be done.
Proof of Cayley’s theorem

Proof of Claim 1. We need to show that for each \( a \in G \), \( \lambda_a \) is one-to-one and onto.

1. **one-to-one**: Suppose that \( \lambda_a(g) = \lambda_a(h) \). Then we have \( ag = ah \). By the cancellation law (Theorem 4.15), this implies that \( g = h \). Therefore \( \lambda_a \) is one-to-one.

2. **onto**: Let \( h \in G \). We need to show that there is an element \( g \) in \( G \) such that \( ag = h \). Clearly, \( a^{-1}h \) is such an element.

Proof of Claim 2. We need to show that \( \lambda_a \circ \lambda_b(g) = \lambda_{ab}(g) \) for all \( g \in G \). We have \( \lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg) \). By associativity, this is equal to \( (ab)g = \lambda_{ab}(g) \).
Proof of Claim 1. We need to show that for each \( a \in G \), \( \lambda_a \) is one-to-one and onto.

1. **One-to-one**: Suppose that \( \lambda_a(g) = \lambda_a(h) \). Then we have \( ag = ah \). By the cancellation law (Theorem 4.15), this implies that \( g = h \). Therefore \( \lambda_a \) is one-to-one.

2. **Onto**: Let \( h \in G \). We need to show that there is an element \( g \) in \( G \) such that \( ag = h \). Clearly, \( a^{-1}h \) is such an element.

Proof of Claim 2. We need to show that \( \lambda_a \circ \lambda_b(g) = \lambda_{ab}(g) \) for all \( g \in G \). We have \( \lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg) \). By associativity, this is equal to \( (ab)g = \lambda_{ab}(g) \).
Proof of Claim 1. We need to show that for each \( a \in G \), \( \lambda_a \) is one-to-one and onto.

1. **one-to-one**: Suppose that \( \lambda_a(g) = \lambda_a(h) \). Then we have \( ag = ah \). By the cancellation law (Theorem 4.15), this implies that \( g = h \). Therefore \( \lambda_a \) is one-to-one.

2. **onto**: Let \( h \in G \). We need to show that there is an element \( g \) in \( G \) such that \( ag = h \). Clearly, \( a^{-1}h \) is such an element.

Proof of Claim 2. We need to show that \( \lambda_a \circ \lambda_b(g) = \lambda_{ab}(g) \) for all \( g \in G \). We have \( \lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg) \). By associativity, this is equal to \( (ab)g = \lambda_{ab}(g) \).
Proof of Cayley’s theorem

Proof of Claim 1. We need to show that for each \( a \in G \), \( \lambda_a \) is one-to-one and onto.

1. **One-to-one**: Suppose that \( \lambda_a(g) = \lambda_a(h) \). Then we have \( ag = ah \). By the cancellation law (Theorem 4.15), this implies that \( g = h \). Therefore \( \lambda_a \) is one-to-one.

2. **Onto**: Let \( h \in G \). We need to show that there is an element \( g \) in \( G \) such that \( ag = h \). Clearly, \( a^{-1}h \) is such an element.

Proof of Claim 2. We need to show that \( \lambda_a \circ \lambda_b(g) = \lambda_{ab}(g) \) for all \( g \in G \). We have \( \lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg) \). By associativity, this is equal to \( (ab)g = \lambda_{ab}(g) \).
Proof of Claim 1. We need to show that for each $a \in G$, $\lambda_a$ is one-to-one and onto.

1. **One-to-one:** Suppose that $\lambda_a(g) = \lambda_a(h)$. Then we have $ag = ah$. By the cancellation law (Theorem 4.15), this implies that $g = h$. Therefore $\lambda_a$ is one-to-one.

2. **Onto:** Let $h \in G$. We need to show that there is an element $g$ in $G$ such that $ag = h$. Clearly, $a^{-1}h$ is such an element.

Proof of Claim 2. We need to show that $\lambda_a \circ \lambda_b(g) = \lambda_{ab}(g)$ for all $g \in G$. We have $\lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg)$. By associativity, this is equal to $(ab)g = \lambda_{ab}(g)$. 

Instructor: Yifan Yang  
Section 8 – Groups of permutation
Proof of Cayley’s theorem

Proof of Claim 1. We need to show that for each $a \in G$, $\lambda_a$ is one-to-one and onto.

1. **One-to-one**: Suppose that $\lambda_a(g) = \lambda_a(h)$. Then we have $ag = ah$. By the cancellation law (Theorem 4.15), this implies that $g = h$. Therefore $\lambda_a$ is one-to-one.

2. **Onto**: Let $h \in G$. We need to show that there is an element $g$ in $G$ such that $ag = h$. Clearly, $a^{-1}h$ is such an element.

Proof of Claim 2. We need to show that $\lambda_a \circ \lambda_b(g) = \lambda_{ab}(g)$ for all $g \in G$. We have $\lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg)$. By associativity, this is equal to $(ab)g = \lambda_{ab}(g)$. 
Proof of Cayley’s theorem

Proof of Claim 1. We need to show that for each \( a \in G \), \( \lambda_a \) is one-to-one and onto.

1. \textbf{one-to-one}: Suppose that \( \lambda_a(g) = \lambda_a(h) \). Then we have \( ag = ah \). By the cancellation law (Theorem 4.15), this implies that \( g = h \). Therefore \( \lambda_a \) is one-to-one.

2. \textbf{onto}: Let \( h \in G \). We need to show that there is an element \( g \) in \( G \) such that \( ag = h \). Clearly, \( a^{-1}h \) is such an element.

Proof of Claim 2. We need to show that \( \lambda_a \circ \lambda_b(g) = \lambda_{ab}(g) \) for all \( g \in G \). We have \( \lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg) \). By associativity, this is equal to \( (ab)g = \lambda_{ab}(g) \).
Proof of Claim 1. We need to show that for each \( a \in G \), \( \lambda_a \) is one-to-one and onto.

1. **one-to-one**: Suppose that \( \lambda_a(g) = \lambda_a(h) \). Then we have \( ag = ah \). By the cancellation law (Theorem 4.15), this implies that \( g = h \). Therefore \( \lambda_a \) is one-to-one.

2. **onto**: Let \( h \in G \). We need to show that there is an element \( g \) in \( G \) such that \( ag = h \). Clearly, \( a^{-1}h \) is such an element.

Proof of Claim 2. We need to show that \( \lambda_a \circ \lambda_b(g) = \lambda_{ab}(g) \) for all \( g \in G \). We have \( \lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg) \). By associativity, this is equal to \( (ab)g = \lambda_{ab}(g) \).
Proof of Cayley’s theorem

Proof of Claim 1. We need to show that for each $a \in G$, $\lambda_a$ is one-to-one and onto.

1. **One-to-one**: Suppose that $\lambda_a(g) = \lambda_a(h)$. Then we have $ag = ah$. By the cancellation law (Theorem 4.15), this implies that $g = h$. Therefore $\lambda_a$ is one-to-one.

2. **Onto**: Let $h \in G$. We need to show that there is an element $g$ in $G$ such that $ag = h$. Clearly, $a^{-1}h$ is such an element.

Proof of Claim 2. We need to show that $\lambda_a \circ \lambda_b(g) = \lambda_{ab}(g)$ for all $g \in G$. We have $\lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg)$. By associativity, this is equal to $(ab)g = \lambda_{ab}(g)$. 

Instructor: Yifan Yang

Section 8 – Groups of permutation
Proof of Cayley’s theorem

Proof of Claim 1. We need to show that for each \( a \in G \), \( \lambda_a \) is one-to-one and onto.

\( \boxed{1} \) \text{ one-to-one:} Suppose that \( \lambda_a(g) = \lambda_a(h) \). Then we have \( ag = ah \). By the cancellation law (Theorem 4.15), this implies that \( g = h \). Therefore \( \lambda_a \) is one-to-one.

\( \boxed{2} \) \text{ onto:} Let \( h \in G \). We need to show that there is an element \( g \) in \( G \) such that \( ag = h \). Clearly, \( a^{-1}h \) is such an element.

Proof of Claim 2. We need to show that \( \lambda_a \circ \lambda_b(g) = \lambda_{ab}(g) \) for all \( g \in G \). We have \( \lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg) \).

By associativity, this is equal to \( (ab)g = \lambda_{ab}(g) \).
Proof of Cayley’s theorem

Proof of Claim 1. We need to show that for each $a \in G$, $\lambda_a$ is one-to-one and onto.

1. **ono-to-one**: Suppose that $\lambda_a(g) = \lambda_a(h)$. Then we have $ag = ah$. By the cancellation law (Theorem 4.15), this implies that $g = h$. Therefore $\lambda_a$ is one-to-one.

2. **onto**: Let $h \in G$. We need to show that there is an element $g$ in $G$ such that $ag = h$. Clearly, $a^{-1}h$ is such an element.

Proof of Claim 2. We need to show that $\lambda_a \circ \lambda_b(g) = \lambda_{ab}(g)$ for all $g \in G$. We have $\lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = a(bg)$. By associativity, this is equal to $(ab)g = \lambda_{ab}(g)$. 
Proof of Cayley’s theorem

Proof of Claim 3. By Theorem 5.14 we need to check three conditions.

1. **closedness**: By Claim 2.

2. **identity**: By Claim 2 we have \( \lambda_g \circ \lambda_e = \lambda_{ge} = \lambda_g \) and \( \lambda_e \circ \lambda_g = \lambda_{eg} = \lambda_g \). Thus \( \lambda_e \) is the identity element.

3. **inverse**: By Claim 2, we have \( \lambda_{g^{-1}} \circ \lambda_g = \lambda_{g^{-1}g} = \lambda_e \) and likewise \( \lambda_g \circ \lambda_{g^{-1}} = \lambda_e \). Thus \( \lambda_{g^{-1}} \) is the inverse of \( \lambda_g \).
Proof of Claim 3. By Theorem 5.14 we need to check three conditions.

1. **closedness**: By Claim 2.

2. **identity**: By Claim 2 we have \( \lambda_g \circ \lambda_e = \lambda_{ge} = \lambda_g \) and \( \lambda_e \circ \lambda_g = \lambda_{eg} = \lambda_g \). Thus \( \lambda_e \) is the identity element.

3. **inverse**: By Claim 2, we have \( \lambda_{g^{-1}} \circ \lambda_g = \lambda_{g^{-1}g} = \lambda_e \) and likewise \( \lambda_g \circ \lambda_{g^{-1}} = \lambda_e \). Thus \( \lambda_{g^{-1}} \) is the inverse of \( \lambda_g \).
Proof of Claim 3. By Theorem 5.14 we need to check three conditions.

1. **closedness**: By Claim 2.

2. **identity**: By Claim 2 we have $\lambda_g \circ \lambda_e = \lambda_{ge} = \lambda_g$ and $\lambda_e \circ \lambda_g = \lambda_{eg} = \lambda_g$. Thus $\lambda_e$ is the identity element.

3. **inverse**: By Claim 2, we have $\lambda_{g^{-1}} \circ \lambda_g = \lambda_{g^{-1}g} = \lambda_e$ and likewise $\lambda_g \circ \lambda_{g^{-1}} = \lambda_e$. Thus $\lambda_{g^{-1}}$ is the inverse of $\lambda_g$. 
Proof of Claim 3. By Theorem 5.14 we need to check three conditions.

1. **Closedness**: By Claim 2.
2. **Identity**: By Claim 2 we have \( \lambda_g \circ \lambda_e = \lambda_{ge} = \lambda_g \) and \( \lambda_e \circ \lambda_g = \lambda_{eg} = \lambda_g \). Thus \( \lambda_e \) is the identity element.
3. **Inverse**: By Claim 2, we have \( \lambda_{g^{-1}} \circ \lambda_g = \lambda_{g^{-1}g} = \lambda_e \) and likewise \( \lambda_g \circ \lambda_{g^{-1}} = \lambda_e \). Thus \( \lambda_{g^{-1}} \) is the inverse of \( \lambda_g \).
Proof of Claim 3. By Theorem 5.14 we need to check three conditions.

1. **closedness**: By Claim 2.
2. **identity**: By Claim 2 we have $\lambda_g \circ \lambda_e = \lambda_{ge} = \lambda_g$ and $\lambda_e \circ \lambda_g = \lambda_{eg} = \lambda_g$. Thus $\lambda_e$ is the identity element.
3. **inverse**: By Claim 2, we have $\lambda_{g^{-1}} \circ \lambda_g = \lambda_{g^{-1}g} = \lambda_e$ and likewise $\lambda_g \circ \lambda_{g^{-1}} = \lambda_e$. Thus $\lambda_{g^{-1}}$ is the inverse of $\lambda_g$. 
Proof of Claim 3. By Theorem 5.14 we need to check three conditions.

1. **closedness:** By Claim 2.

2. **identity:** By Claim 2 we have $\lambda_g \circ \lambda_e = \lambda_{ge} = \lambda_g$ and $\lambda_e \circ \lambda_g = \lambda_{eg} = \lambda_g$. Thus $\lambda_e$ is the identity element.

3. **inverse:** By Claim 2, we have $\lambda_{g^{-1}} \circ \lambda_g = \lambda_{g^{-1}g} = \lambda_e$ and likewise $\lambda_g \circ \lambda_{g^{-1}} = \lambda_e$. Thus $\lambda_{g^{-1}}$ is the inverse of $\lambda_g$. 
Proof of Claim 4. We need to verify that the function $\phi : G \rightarrow \hat{G}$ defined by $\phi(a) = \lambda_a$ satisfies three conditions.

1. **one-to-one:** Suppose that $\phi(a) = \phi(b)$, that is, $\lambda_a = \lambda_b$. Then $\lambda_a(g) = \lambda_b(g)$ for all $g \in G$. In particular, we have $\lambda_a(e) = \lambda_b(e)$. From this we conclude that $a = b$.

2. **onto:** This is clear.

3. **homomorphy:** We need to show $\phi(ab) = \phi(a) \circ \phi(b)$, that is, $\lambda_{ab} = \lambda_a \circ \lambda_b$. But this is just Claim 2 proved earlier.
Proof of Cayley’s theorem.

Proof of Claim 4. We need to verify that the function \( \phi : G \to \hat{G} \) defined by \( \phi(a) = \lambda_a \) satisfies three conditions.

1. **one-to-one:** Suppose that \( \phi(a) = \phi(b) \), that is, \( \lambda_a = \lambda_b \). Then \( \lambda_a(g) = \lambda_b(g) \) for all \( g \in G \). In particular, we have \( \lambda_a(e) = \lambda_b(e) \). From this we conclude that \( a = b \).

2. **onto:** This is clear.

3. **homomorphy:** We need to show \( \phi(ab) = \phi(a) \circ \phi(b) \), that is, \( \lambda_{ab} = \lambda_a \circ \lambda_b \). But this is just Claim 2 proved earlier.
Proof of Claim 4. We need to verify that the function $\phi : G \to \hat{G}$ defined by $\phi(a) = \lambda_a$ satisfies three conditions.

1. **one-to-one**: Suppose that $\phi(a) = \phi(b)$, that is, $\lambda_a = \lambda_b$. Then $\lambda_a(g) = \lambda_b(g)$ for all $g \in G$. In particular, we have $\lambda_a(e) = \lambda_b(e)$. From this we conclude that $a = b$.

2. **onto**: This is clear.

3. **homomorphy**: We need to show $\phi(ab) = \phi(a) \circ \phi(b)$, that is, $\lambda_{ab} = \lambda_a \circ \lambda_b$. But this is just Claim 2 proved earlier.
Proof of Claim 4. We need to verify that the function $\phi : G \rightarrow \hat{G}$ defined by $\phi(a) = \lambda_a$ satisfies three conditions.

1. **one-to-one**: Suppose that $\phi(a) = \phi(b)$, that is, $\lambda_a = \lambda_b$. Then $\lambda_a(g) = \lambda_b(g)$ for all $g \in G$. In particular, we have $\lambda_a(e) = \lambda_b(e)$. From this we conclude that $a = b$.

2. **onto**: This is clear.

3. **homomorphy**: We need to show $\phi(ab) = \phi(a) \circ \phi(b)$, that is, $\lambda_{ab} = \lambda_a \circ \lambda_b$. But this is just Claim 2 proved earlier.
Proof of Claim 4. We need to verify that the function \( \phi : G \to \hat{G} \) defined by \( \phi(a) = \lambda_a \) satisfies three conditions.

1. one-to-one: Suppose that \( \phi(a) = \phi(b) \), that is, \( \lambda_a = \lambda_b \). Then \( \lambda_a(g) = \lambda_b(g) \) for all \( g \in G \). In particular, we have \( \lambda_a(e) = \lambda_b(e) \). From this we conclude that \( a = b \).

2. onto: This is clear.

3. homomorphy: We need to show \( \phi(ab) = \phi(a) \circ \phi(b) \), that is, \( \lambda_{ab} = \lambda_a \circ \lambda_b \). But this is just Claim 2 proved earlier.
Proof of Claim 4. We need to verify that the function $\phi : G \rightarrow \hat{G}$ defined by $\phi(a) = \lambda_a$ satisfies three conditions.

1. **one-to-one:** Suppose that $\phi(a) = \phi(b)$, that is, $\lambda_a = \lambda_b$. Then $\lambda_a(g) = \lambda_b(g)$ for all $g \in G$. In particular, we have $\lambda_a(e) = \lambda_b(e)$. From this we conclude that $a = b$.

2. **onto:** This is clear.

3. **homomorphy:** We need to show $\phi(ab) = \phi(a) \circ \phi(b)$, that is, $\lambda_{ab} = \lambda_a \circ \lambda_b$. But this is just Claim 2 proved earlier.
Proof of Claim 4. We need to verify that the function $\phi : G \to \hat{G}$ defined by $\phi(a) = \lambda_a$ satisfies three conditions.

1. **one-to-one**: Suppose that $\phi(a) = \phi(b)$, that is, $\lambda_a = \lambda_b$. Then $\lambda_a(g) = \lambda_b(g)$ for all $g \in G$. In particular, we have $\lambda_a(e) = \lambda_b(e)$. From this we conclude that $a = b$.

2. **onto**: This is clear.

3. **homomorphy**: We need to show $\phi(ab) = \phi(a) \circ \phi(b)$, that is, $\lambda_ab = \lambda_a \circ \lambda_b$. But this is just Claim 2 proved earlier.
Proof of Cayley’s theorem

Proof of Claim 4. We need to verify that the function \( \phi : G \to \hat{G} \) defined by \( \phi(a) = \lambda_a \) satisfies three conditions.

1. **one-to-one**: Suppose that \( \phi(a) = \phi(b) \), that is, \( \lambda_a = \lambda_b \). Then \( \lambda_a(g) = \lambda_b(g) \) for all \( g \in G \). In particular, we have \( \lambda_a(e) = \lambda_b(e) \). From this we conclude that \( a = b \).

2. **onto**: This is clear.

3. **homomorphism**: We need to show \( \phi(ab) = \phi(a) \circ \phi(b) \), that is, \( \lambda_{ab} = \lambda_a \circ \lambda_b \). But this is just Claim 2 proved earlier.
Homework

Do Problems 2, 6, 16, 20, 21, 32, 36, 42, 49, 52 of Section 8.