Warmup: Draw the symmetries for the triangle.

(1) How many symmetries are there?

(2) If we call the move “rotate clockwise” $r$, what is the order of $r$? Is there a way to write $r^{-1}$ in terms of some positive power of $r$?

(3) If we call the move “flip across a vertical axis” $s$, what is the order of $s$? Is there a way to write $s^{-1}$ in terms of some positive power of $s$?

(4) Note that $r^a s^b$ means “flip $b$ times and then rotate $a$ times” (read actions right to left like function composition). Now label each of the symmetries by some $r^a s^b$. Then label each of the symmetries by some $s^b r^a$, and then by $s^b r^{-a}$, and compare all three forms.

Repeat parts (1)–(4) for the square.
**Review:** Let $G$ be a set. A **binary operation** $\star$ on $G$ is a function

$$\star : G \times G \rightarrow G.$$ 

A **group** is a pair $(G, \star)$ consisting of a set $G$ and a binary operation $\star$ on $G$ such that:

1. $\star$ is **associative**, i.e. $(a \star b) \star c = a \star (b \star c)$;
2. there is an **identity** element $e \in G$, i.e.

$$e \star g = g = g \star e \quad \text{for all } g \in G;$$

3. every element of $G$ has an **inverse**; i.e. for all $g \in G$, there is an element $g^{-1}$ such that $gg^{-1} = e = g^{-1}g$.

**Favorite examples so far:**

1. $\mathbb{Z}^n$, $\mathbb{Q}^n$, $\mathbb{R}^n$, $\mathbb{C}^n$ under addition.
2. $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ under multiplication.
3. $\mathbb{Z}/n\mathbb{Z}$ under addition.
4. $(\mathbb{Z}/n\mathbb{Z})^\times = \{ a \in \mathbb{Z}/n\mathbb{Z} \mid a \text{ is relatively prime to } n \}$ under multiplication.
The **order** of a group $G$, denoted $|G|$, is the size of the underlying set.

For any element $x \in G$, if $x^n = e$ for some $n \in \mathbb{Z}_{>0}$, we say the **order of** $x$ is the smallest such $n$.

**Theorem**

1. An element $x \in G$ has order 1 if and only if $x = e$.
2. $x^m = e$ iff $|x|$ divides $m$. 
Let

\[ D_{2n} = \text{group of symmetries of a regular } 2n\text{-gon}, \]

where \textit{symmetries} means ways to move the \(2n\)-gon so that the outline ends looking the same, but the vertices have moved.

Some properties:

(1) There are always \(2n\) symmetries, i.e. \(D_{2n}\) has order \(2n\).

(2) The symmetries are, for example, generated by \(r = \text{“rotate clockwise } (360/n)°\text{”} \) and \(s = \text{“flip over a vertical axis”}\).

(3) The element \(r\) has order \(n\), and the element \(s\) has order 2.

(4) The elements \(r\) and \(s\) don’t commute, but they do satisfy

\[ rs = sr^{-1} \quad \text{and} \quad sr = r^{-1}s. \]
Group presentations

A subset of elements $S \subseteq G$ with the property that every element of $G$ can be written as a finite product of elements of $S$ and their inverses is called a set of generators of $G$. We write $\langle S \rangle = G$.

Ex: $D_{2n}$ is generated by $S = \{r, s\}$; $\mathbb{Z}$ is generated by 1; $\mathbb{Z}/n\mathbb{Z}$ is generated by $\bar{1}$.

Any equations that are satisfied in $G$ are called relations.

Ex: The generators $S = \{r, s\}$ satisfy $s^2 = r^n = 1$ and $rs = sr - 1$.

If a set of relations $R$ has the property that any relation in $G$ can be derived from those in $R$ then those generators and relations form a presentation of $G$, written $\langle \text{generators} | \text{relations} \rangle$.

In short, a presentation is everything you need to build the group.

Some examples:

$D_{12} = \langle r, s | r^6 = e, s^2 = e, r^{-1}s = sr \rangle$

$\mathbb{Z}/3\mathbb{Z} = \langle \bar{1} | \bar{1}^3 = e \rangle$ (Yes, weird notation!)

$\mathbb{Z} = \langle 1 | \emptyset \rangle = \langle 1 \rangle$ (If there are no relations, i.e. $R = \emptyset$, we write $G = \langle S \rangle$.)
Group presentations

A subset of elements $S \subseteq G$ with the property that every element of $G$ can be written as a finite product of elements of $S$ and their inverses is called a set of generators of $G$. We write $\langle S \rangle = G$.

Ex: $D_{2n}$ is generated by $S = \{r, s\}$
Group presentations

A subset of elements $S \subseteq G$ with the property that every element of $G$ can be written as a finite product of elements of $S$ and their inverses is called a set of generators of $G$. We write $\langle S \rangle = G$.

Ex: $D_{2n}$ is generated by $S = \{r, s\}$; $\mathbb{Z}$ is generated by 1.
Group presentations

A subset of elements $S \subseteq G$ with the property that every element of $G$ can be written as a finite product of elements of $S$ and their inverses is called a set of generators of $G$. We write $\langle S \rangle = G$.

Ex: $D_{2n}$ is generated by $S = \{r, s\}$; $\mathbb{Z}$ is generated by 1; $\mathbb{Z}/n\mathbb{Z}$ is generated by $\bar{1}$.
Group presentations

A subset of elements $S \subseteq G$ with the property that every element of $G$ can be written as a finite product of elements of $S$ and their inverses is called a set of generators of $G$. We write $\langle S \rangle = G$.

Ex: $D_{2n}$ is generated by $S = \{r, s\}$; $\mathbb{Z}$ is generated by 1; $\mathbb{Z}/n\mathbb{Z}$ is generated by $\bar{1}$.

Any equations that are satisfied in $G$ are called relations.
Group presentations

A subset of elements \( S \subseteq G \) with the property that every element of \( G \) can be written as a finite product of elements of \( S \) and their inverses is called a set of **generators** of \( G \). We write \( \langle S \rangle = G \).

**Ex:** \( D_{2n} \) is generated by \( S = \{r, s\} \); \( \mathbb{Z} \) is generated by 1; \( \mathbb{Z}/n\mathbb{Z} \) is generated by \( \overline{1} \).

Any equations that are satisfied in \( G \) are called **relations**.

**Ex:** The generators \( S = \{r, s\} \) satisfy \( s^2 = r^n = 1 \) and \( rs = sr^{-1} \).
Group presentations

A subset of elements $S \subseteq G$ with the property that every element of $G$ can be written as a finite product of elements of $S$ and their inverses is called a set of generators of $G$. We write $\langle S \rangle = G$.

**Ex:** $D_{2n}$ is generated by $S = \{r, s\}$; $\mathbb{Z}$ is generated by 1; $\mathbb{Z}/n\mathbb{Z}$ is generated by $\bar{1}$.

Any equations that are satisfied in $G$ are called relations.

**Ex:** The generators $S = \{r, s\}$ satisfy $s^2 = r^n = 1$ and $rs = sr^{-1}$.

If a set of relations $R$ has the property that any relation in $G$ can be derived from those in $R$ then those generators and relations form a presentation of $G$, written

\[ \langle \text{generators} \mid \text{relations} \rangle. \]

In short, a presentation is everything you need to build the group.
Group presentations

A subset of elements $S \subseteq G$ with the property that every element of $G$ can be written as a finite product of elements of $S$ and their inverses is called a set of generators of $G$. We write $\langle S \rangle = G$.

**Ex:** $D_{2n}$ is generated by $S = \{r, s\}$; $\mathbb{Z}$ is generated by 1; $\mathbb{Z}/n\mathbb{Z}$ is generated by $\bar{1}$.

Any equations that are satisfied in $G$ are called relations.

**Ex:** The generators $S = \{r, s\}$ satisfy $s^2 = r^n = 1$ and $rs = sr^{-1}$.

If a set of relations $R$ has the property that any relation in $G$ can be derived from those in $R$ then those generators and relations form a presentation of $G$, written

$$\langle \text{generators} \mid \text{relations} \rangle.$$ 

In short, a presentation is everything you need to build the group.

**Some examples:**

$$D_{12} = \langle r, s \mid r^6 = e, s^2 = e, r^{-1}s = sr \rangle$$
Group presentations

A subset of elements $S \subseteq G$ with the property that every element of $G$ can be written as a finite product of elements of $S$ and their inverses is called a set of generators of $G$. We write $\langle S \rangle = G$.

Ex: $D_{2n}$ is generated by $S = \{r, s\}$; $\mathbb{Z}$ is generated by 1; $\mathbb{Z}/n\mathbb{Z}$ is generated by $\bar{1}$.

Any equations that are satisfied in $G$ are called relations.

Ex: The generators $S = \{r, s\}$ satisfy $s^2 = r^n = 1$ and $rs = sr^{-1}$.

If a set of relations $R$ has the property that any relation in $G$ can be derived from those in $R$ then those generators and relations form a presentation of $G$, written

$$\langle \text{generators} \mid \text{relations} \rangle.$$ 

In short, a presentation is everything you need to build the group.

Some examples:

$$D_{12} = \langle r, s \mid r^6 = e, s^2 = e, r^{-1}s = sr \rangle$$

$$\mathbb{Z}/3\mathbb{Z} = \langle \bar{1} \mid \bar{1}^3 = e \rangle \text{ (Yes, weird notation!)}$$
Group presentations

A subset of elements \( S \subseteq G \) with the property that every element of \( G \) can be written as a finite product of elements of \( S \) and their inverses is called a set of generators of \( G \). We write \( \langle S \rangle = G \).

**Ex:** \( D_{2n} \) is generated by \( S = \{r, s\} \); \( \mathbb{Z} \) is generated by 1; \( \mathbb{Z}/n\mathbb{Z} \) is generated by \( \bar{1} \).

Any equations that are satisfied in \( G \) are called relations.

**Ex:** The generators \( S = \{r, s\} \) satisfy \( s^2 = r^n = 1 \) and \( rs = sr^{-1} \).

If a set of relations \( R \) has the property that any relation in \( G \) can be derived from those in \( R \) then those generators and relations form a presentation of \( G \), written

\[
\langle \text{generators} \mid \text{relations} \rangle.
\]

In short, a presentation is everything you need to build the group.

**Some examples:**

\[
D_{12} = \langle r, s \mid r^6 = e, s^2 = e, r^{-1}s = sr \rangle
\]

\[
\mathbb{Z}/3\mathbb{Z} = \langle \bar{1} \mid \bar{1}^3 = e \rangle \quad \text{(Yes, weird notation!)}
\]

\[
\mathbb{Z} = \langle 1 \mid \emptyset \rangle = \langle 1 \rangle
\]

(If there are no relations, i.e. \( R = \emptyset \), we write \( G = \langle S \rangle \).)
Intuition from linear algebra

Generators are like “spanning sets” from linear algebra.
Intuition from linear algebra

Generators are like “spanning sets” from linear algebra. For example, let $G = \mathbb{Z}^2$. Then $x = (1, 0)$ generates

$$x + x = (2, 0), x + x + x = (3, 0), \ldots,$$

and also

$$x^{-1} = (-1, 0) \quad x^{-1} + x^{-1} = (-2, 0), \ldots$$
Intuition from linear algebra

Generators are like “spanning sets” from linear algebra. For example, let \( G = \mathbb{Z}^2 \). Then \( x = (1, 0) \) generates

\[
x + x = (2, 0), \ x + x + x = (3, 0), \ldots,
\]

and also

\[
x^{-1} = (-1, 0) \quad x^{-1} + x^{-1} = (-2, 0), \ldots.
\]

Throwing in \( y = (0, 1) \) you also get

\[
y^{-1} = (0, -1), \ x + y = (1, 1), \ \text{etc.}
\]

So \( S = \{x, y\} \) generates \( \mathbb{Z}^2 \).
Intuition from linear algebra

Generators are like "spanning sets" from linear algebra. For example, let $G = \mathbb{Z}^2$. Then $x = (1, 0)$ generates

$$x + x = (2, 0), \ x + x + x = (3, 0), \ldots,$$

and also

$$x^{-1} = (-1, 0) \quad x^{-1} + x^{-1} = (-2, 0), \ldots.$$

Throwing in $y = (0, 1)$ you also get

$$y^{-1} = (0, -1), \ x + y = (1, 1), \ \text{etc}.$$

So $S = \{x, y\}$ generates $\mathbb{Z}^2$. The only additional information you need to define the group is that $xy = yx$. So

$$\mathbb{Z}^2 = \langle x, y \mid xy = yx \rangle.$$
Intuition from linear algebra

Generators are like “spanning sets” from linear algebra. For example, let $G = \mathbb{Z}^2$. Then $x = (1, 0)$ generates

$$x + x = (2, 0), x + x + x = (3, 0), \ldots,$$

and also

$$x^{-1} = (-1, 0) \quad x^{-1} + x^{-1} = (-2, 0), \ldots.$$  

Throwing in $y = (0, 1)$ you also get

$$y^{-1} = (0, -1), x + y = (1, 1), \text{ etc.}$$

So $S = \{x, y\}$ generates $\mathbb{Z}^2$. The only additional information you need to define the group is that $xy = yx$. So

$$\mathbb{Z}^2 = \langle x, y \mid xy = yx \rangle.$$  

A minimum set of generators is like a basis from linear algebra.  
CAUTION!! Minimum versus minimal: $\mathbb{Z} = \langle 1 \rangle = \langle 2, 3 \rangle$.  

Example

Let $G$ be the group

$$G = \langle a, b \mid a^2 = b^2 = e, aba = bab \rangle$$
Example

Let $G$ be the group

$$G = \langle a, b \mid a^2 = b^2 = e, aba = bab \rangle$$

Now $a^{-1} = a$ and $b^{-1} = b$. 
Example

Let $G$ be the group

$$G = \langle a, b \mid a^2 = b^2 = e, aba = bab \rangle$$

Now $a^{-1} = a$ and $b^{-1} = b$.

Other ways of writing $aba = bab$:

$$abab = ba \quad ababa = b \quad ababab = e \quad bbbaaaba = bab \cdots$$
Example

Let $G$ be the group

$$G = \langle a, b \mid a^2 = b^2 = e, aba = bab \rangle$$

Now $a^{-1} = a$ and $b^{-1} = b$.

Other ways of writing $aba = bab$:

$$abab = ba \quad ababa = b \quad ababab = e \quad bbbaaba = bab \cdots$$

Claim: $G$ has 6 elements.
Presentation problem

**Question:** When are two presentations \( \langle S_1 \mid R_1 \rangle \) and \( \langle S_2 \mid R_2 \rangle \) actually presentations for the same group?
Presentation problem

Question: When are two presentations $\langle S_1 \mid R_1 \rangle$ and $\langle S_2 \mid R_2 \rangle$ actually presentations for the same group? HARD
Presentation problem

**Question:** When are two presentations \( \langle S_1 \mid R_1 \rangle \) and \( \langle S_2 \mid R_2 \rangle \) actually presentations for the same group? **HARD**

**Claim:** If we let \( a = s \) and \( b = rs \), then

\[
\langle a, b \mid a^2 = b^2 = e, aba = bab \rangle = \langle r, s \mid r^3 = s^2 = e, rs = sr^{-1} \rangle = D_6
\]
The symmetric group

Let $X$ be a finite non-empty set, and let $S_X$ be the set of bijections from the set to itself, i.e. the set of permutations of the elements.
The symmetric group

Let $X$ be a finite non-empty set, and let $S_X$ be the set of bijections from the set to itself, i.e. the set of permutations of the elements. For example, if $X = \{1, 2, 3\}$ then $S_X$ contains

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & 2 & 3 \\
1 & 2 & 3 \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \uparrow & \downarrow \\
1 & 2 & 3 \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & 2 & 3 \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \downarrow \\
1 & 2 & 3 \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \uparrow & \downarrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \uparrow & \downarrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \uparrow & \uparrow \\
1 & \downarrow & \downarrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \downarrow \\
1 & \uparrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \downarrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \uparrow & \downarrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \downarrow \\
1 & \uparrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \uparrow & \downarrow \\
1 & \uparrow & \downarrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \uparrow & \uparrow \\
1 & \downarrow & \downarrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \uparrow & \uparrow \\
1 & \downarrow & \downarrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \uparrow & \downarrow \\
1 & \uparrow & \downarrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \downarrow \\
1 & \uparrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \downarrow \\
1 & \uparrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]

\[
\begin{array}{ccc}
1 & 2 & 3 \\
1 & \downarrow & \uparrow \\
1 & \downarrow & \uparrow \\
\end{array}
\]
The symmetric group

Let $X$ be a finite non-empty set, and let $S_X$ be the set of bijections from the set to itself, i.e. the set of permutations of the elements. For example, if $X = \{1, 2, 3\}$ then $S_X$ contains

$S_X$ forms a group under function composition.
The symmetric group

Let $X$ be a finite non-empty set, and let $S_X$ be the set of bijections from the set to itself, i.e. the set of permutations of the elements. For example, if $X = \{1, 2, 3\}$ then $S_X$ contains

$$\begin{array}{ccc}
1 & 2 & 3 \\
\uparrow & \uparrow & \uparrow \\
1 & 2 & 3 \\
\end{array} \quad \begin{array}{ccc}
1 & 2 & 3 \\
\downarrow & \rightarrow & \downarrow \\
1 & 2 & 3 \\
\end{array} \quad \begin{array}{ccc}
1 & 2 & 3 \\
\rightarrow & \downarrow & \rightarrow \\
1 & 2 & 3 \\
\end{array}
$$

$S_X$ forms a group under function composition.

- A permutation $\sigma$ followed by another permutation $\tau$ is $\tau \circ \sigma$, which is itself a permutation (binary operation)
The symmetric group

Let $X$ be a finite non-empty set, and let $S_X$ be the set of bijections from the set to itself, i.e. the set of permutations of the elements. For example, if $X = \{1, 2, 3\}$ then $S_X$ contains

$S_X$ forms a group under function composition.

- A permutation $\sigma$ followed by another permutation $\tau$ is $\tau \circ \sigma$, which is itself a permutation (binary operation)
- Function composition is associative.
The symmetric group

Let $X$ be a finite non-empty set, and let $S_X$ be the set of bijections from the set to itself, i.e. the set of permutations of the elements. For example, if $X = \{1, 2, 3\}$ then $S_X$ contains

\[
\begin{array}{c}
\begin{array}{ccc}
1 & 2 & 3 \\
\downarrow & \downarrow & \downarrow \\
\bullet & \bullet & \bullet \\
\end{array} & \begin{array}{ccc}
1 & 2 & 3 \\
\downarrow & \downarrow & \downarrow \\
\bullet & \bullet & \bullet \\
\end{array} & \begin{array}{ccc}
1 & 2 & 3 \\
\downarrow & \downarrow & \downarrow \\
\bullet & \bullet & \bullet \\
\end{array}
\end{array}
\]

$S_X$ forms a group under function composition.

- A permutation $\sigma$ followed by another permutation $\tau$ is $\tau \circ \sigma$, which is itself a permutation (binary operation).
- Function composition is associative.
- The bijection $x \mapsto x$ for all $x \in X$ serves as the identity.
The symmetric group

Let $X$ be a finite non-empty set, and let $S_X$ be the set of bijections from the set to itself, i.e. the set of permutations of the elements. For example, if $X = \{1, 2, 3\}$ then $S_X$ contains

$$S_X \text{ forms a group under function composition.}$$

- A permutation $\sigma$ followed by another permutation $\tau$ is $\tau \circ \sigma$, which is itself a permutation (binary operation)
- Function composition is associative.
- The bijection $x \mapsto x$ for all $x \in X$ serves as the identity.
- Every bijection is invertible.
The symmetric group

Let $X$ be a finite non-empty set, and let $S_X$ be the set of bijections from the set to itself, i.e. the set of permutations of the elements. For example, if $X = \{1, 2, 3\}$ then $S_X$ contains

$S_X$ forms a group under function composition.

- A permutation $\sigma$ followed by another permutation $\tau$ is $\tau \circ \sigma$, which is itself a permutation (binary operation)
- Function composition is associative.
- The bijection $x \mapsto x$ for all $x \in X$ serves as the identity.
- Every bijection is invertible.

The group $S_X$ is called the symmetric group on $X$. 
The symmetric group

When $X = [n] = \{1, 2, \ldots, n\}$ we denote $S_X$ by $S_n$, and call it the symmetric group of degree $n$. 

Fact: It turns out that $S_X$ is essentially the same group as $S_{|X|}$. (Later: they are isomorphic.)

Proposition: The order of $S_n$ is $|S_n| = n!$. 
The symmetric group

When $X = [n] = \{1, 2, \ldots, n\}$ we denote $S_X$ by $S_n$, and call it the symmetric group of degree $n$.

**Fact:** It turns out that $S_X$ is essentially the same group as $S_{|X|}$. (Later: they are *isomorphic*.)
The symmetric group

When $X = [n] = \{1, 2, \ldots, n\}$ we denote $S_X$ by $S_n$, and call it the symmetric group of degree $n$.

**Fact:** It turns out that $S_X$ is essentially the same group as $S_{|X|}$. (Later: they are *isomorphic*.)

**Proposition**

*The order of $S_n$ is $|S_n| = n!$.***
Some notation

Permutations can be represented in many ways:

\[ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \]

means \( \sigma(1) = 3 \), \( \sigma(2) = 4 \), etc.
Some notation

Permutations can be represented in many ways:

$$\sigma = \begin{array}{ccccccccc}
1 & 2 & 3 & 4 \\
\downarrow & \downarrow & \downarrow & \downarrow \\
1 & 2 & 3 & 4
\end{array}$$

means $\sigma(1) = 3$, $\sigma(2) = 4$, etc.

(Cauchy’s) two-line notation:

$$\sigma = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
3 & 4 & 2 & 1 & 7 & 6 & 5
\end{pmatrix}$$
Some notation

Permutations can be represented in many ways:

\[ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 \end{pmatrix} \]

means \( \sigma(1) = 3, \sigma(2) = 4, \) etc.

(Cauchy’s) two-line notation:

\[ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 2 & 1 & 7 & 6 & 5 \end{pmatrix} \]

One-line notation: \( \sigma = 3421765 \)
Permutations can be represented in many ways:

\[ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 2 & 1 & 7 & 6 & 5 \end{pmatrix} \] means \( \sigma(1) = 3, \sigma(2) = 4, \text{ etc.} \)

(Cauchy’s) two-line notation:

\[ \sigma = (1\ 3\ 2\ 4)(5\ 7)(6) \text{ or just } (1\ 3\ 2\ 4)(5\ 7) \]

One-line notation: \( \sigma = 3421765 \)
Cycle notation:
Some notation

Permutations can be represented in many ways:

\[ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \]

means \( \sigma(1) = 3, \sigma(2) = 4 \), etc.

(Cauchy’s) two-line notation:

\[ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 2 & 1 & 7 & 6 & 5 \end{pmatrix} \]

One-line notation: \( \sigma = 3421765 \)

Cycle notation:

\[ \sigma = (1 \ 3 \ 2 \ 4)(5 \ 7)(6) \]

denoted by \((1324)(57)(6)\)
or just \((1324)(57)\)
Multiplication of diagrams:

\[ \sigma = \begin{array}{ccccc}
1 & 2 & 3 & 4 & 5 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
1 & 2 & 3 & 4 & 5
\end{array} \quad \tau = \begin{array}{ccccc}
1 & 2 & 3 & 4 & 5 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
1 & 2 & 3 & 4 & 5
\end{array} \]
Cycles

A cycle is a string of integers what represents the element of $S_n$ that cyclically permutes these integers (and fixes all others).

Example: $(435)$ is the permutation in $S_n$ that sends 4 to 3, 3 to 5, 5 to 4, and everything else to itself.

Every permutation can be expressed as the product (composition) of cycles, usually in several ways.

Example: $(13) = (31) = (23)(12)(23)$ (draw the permutation diagrams)
Cycles

A cycle is a string of integers what represents the element of $S_n$ that cyclically permutes these integers (and fixes all others). Specifically,

$$(a_1 a_2 \ldots a_\ell) \text{ sends } a_1 \mapsto a_2 \quad a_2 \mapsto a_3 \quad \vdots \quad a_\ell \mapsto a_1$$

Example: $(435)$ is the permutation in $S_n$ that sends 4 to 3, 3 to 5, 5 to 4, and everything else to itself. Every permutation can be expressed as the product (composition) of cycles, usually in several ways. Example: $(13) = (31) = (23)(12)(23)$.
A cycle is a string of integers what represents the element of $S_n$ that cyclically permutes these integers (and fixes all others). Specifically, 

$$(a_1 a_2 \ldots a_\ell)$$ sends 

\[
\begin{align*}
    a_1 & \mapsto a_2 \\
    a_2 & \mapsto a_3 \\
    & \quad \vdots \\
    a_\ell & \mapsto a_1
\end{align*}
\]

**Example:** $(435)$ is the permutation in $S_n$ that sends 4 to 3, 3 to 5, 5 to 4, and everything else to itself.
Cycles

A cycle is a string of integers what represents the element of $S_n$ that cyclically permutes these integers (and fixes all others). Specifically,

$$(a_1 a_2 \ldots a_\ell) \quad \text{sends} \quad \begin{align*}
a_1 & \mapsto a_2 \\
da_2 & \mapsto a_3 \\
& \quad \vdots \\
da_\ell & \mapsto a_1
\end{align*}$$

**Example:** $(435)$ is the permutation in $S_n$ that sends 4 to 3, 3 to 5, 5 to 4, and everything else to itself.

Every permutation can be expressed as the product (composition) of cycles, usually in several ways.
Cycles

A cycle is a string of integers what represents the element of $S_n$ that cyclically permutes these integers (and fixes all others). Specifically,

$$(a_1 a_2 \ldots a_\ell) \quad \text{sends} \quad \begin{align*}
a_1 & \mapsto a_2 \\
a_2 & \mapsto a_3 \\
& \quad \quad \quad \vdots \\
a_\ell & \mapsto a_1
\end{align*}$$

Example: \((435)\) is the permutation in $S_n$ that sends 4 to 3, 3 to 5, 5 to 4, and everything else to itself.

Every permutation can be expressed as the product (composition) of cycles, usually in several ways.

Example: \((13) = (31) = (23)(12)(23)\)
(draw the permutation diagrams)
Algorithm for writing a permutation in cycles:

1. Start with “(1”.
2. If \( a \) is the last element of the cycle, either:
   (i) If \( \sigma(a) \) is the first element of the cycle, close the cycle. If there are any numbers left unused, start a new cycle with the least available number.
   (ii) If \( \sigma(a) \) is the not first element of the cycle, add \( \sigma(a) \) next in the cycle.
3. Repeat 2 until all numbers \( 1, \ldots, n \) appear in some cycle.
4. Delete any cycles of length 1.

\[
\sigma = \begin{array}{ccccc}
1 & 2 & 3 & 4 & 5 \\
1 & 2 & 3 & 4 & 5 \\
\end{array}
\] \quad \tau = \begin{array}{ccccc}
1 & 2 & 3 & 4 & 5 \\
1 & 2 & 3 & 4 & 5 \\
\end{array}
\]
Multiplying cycles:

Algorithm:
1. Start the first cycle of your answer with $a = 1$.
2. If the last number that you wrote in your answer is $a$, let $x = a$.
3. Look for the rightmost cycle with $x$ in it, and reset $x$ to its successor in that cycle.
4. Always moving left from cycle-to-cycle, look for the next cycle with $x$ in it and replace it with its successor.
5. When you run out of cycles, write $x$ as the successor of $a$ in your answer, unless...
6. If $x$ was the first element of the current cycle of your answer, then close the cycle, and start a new one with the least number not appearing yet in your answer.

If $\sigma = (1352)$ and $\tau = (123)(45)$ as before, then $\sigma\tau = (1352)(123)(45) =$
Multiplying cycles:

Algorithm:

1. Start the first cycle of your answer with \( a = 1 \).
2. If the last number that you wrote in your answer is \( a \), let \( x = a \).
3. Look for the rightmost cycle with a \( x \) in it, and reset \( x \) to its successor in that cycle.
4. Always moving left from cycle-to-cycle, look for the next cycle with \( x \) in it and replace it with it’s successor.
5. When you run out of cycles, write \( x \) as the successor of \( a \) in your answer, unless...
6. If \( x \) was the first element of the current cycle of your answer, then close the cycle, and start a new one with the least number not appearing yet in your answer.

If \( \sigma = (1352) \) and \( \tau = (123)(45) \) as before, then

\[
\sigma \tau = (1352)(123)(45) =
\]
You try:

(a) Write in cycle notation:

\[ \sigma_1 = (1, 2, 3, 4, 5, 6, 7) \]

\[ \sigma_2 = (1, 2, 3, 4, 5, 6, 7) \]

(b) Draw the maps (like the diagrams above) for

\[ \tau_1 = (1, 3, 7)(5, 2) \]

\[ \tau_2 = (1, 2)(3, 4)(5, 6) \]

(c) Use the cycle notation to compute \( \sigma_1 \sigma_2 \) and \( \tau_2 \tau_1 \). Check using the diagrams (stack \( \sigma_1 \) on top of \( \sigma_2 \) and resolve).