Fun fact. (outside of the curriculum)

You can use a set of generators to turn a group into a metric space! Defining a distance on a set is just a matter of coming up with a function $D : X \times X \to \mathbb{R}$ that satisfies

1. $d(x, x) = 0$,
2. $d(x, y) = d(x, y) > 0$ for all $x \neq y$, and
3. $d(x, y) + d(y, z) \geq d(x, z)$.

With a set of generators, we can define a distance on a group as follows. Pick a generating set $S$ for $G$. If $x \in G$, let the length $\ell_S(x)$ of $x$ be the length of the smallest word in $S$ and its inverses generating $x$.

The distance on $G$ is then $d(x, y) = \ell_S(x^{-1}y)$.

Example: Let $G = (\mathbb{Z}, +)$ and $S = \{1, 10, 100, 1000, \ldots \}$. Then $d(2, 4) = 2$ because $-2 + 4 = 2 = 1 + 1$. But $d(2, 10) = 3$ because $-2 + 10 = 8 = 10 + (-1) + (-1)$. 
Lecture 4

Isomorphisms and homomorphisms: When are two groups “the same”? 
From last time:

The symmetric group $S_n$ is the group of permutations of the set $\{1, \ldots, n\}$. We write elements either as diagrams (which multiply by concatenation)

$$
\sigma = \begin{array}{cccc}
1 & 2 & 3 & 4 \\
\downarrow & \downarrow & \downarrow & \downarrow \\
1 & 2 & 3 & 4
\end{array}
\begin{array}{cccc}
5 & 6 & 7 \\
\downarrow & \downarrow & \downarrow \\
5 & 6 & 7
\end{array}
$$

or in cycle decomposition (which multiplies by progressing right to left)

$$
\sigma = (1324)(57)
$$
Subgroups

Definition
A subset $H$ of a group $G$ is a subgroup if $H$ is a group under the same operation as in $G$. This is denoted $H \leq G$. 

Subgroups

Definition
A subset $H$ of a group $G$ is a **subgroup** if $H$ is a group under the same operation as in $G$. This is denoted $H \leq G$.

Examples:
* $\{0, 2, 4\}$ is a subgroup of $\mathbb{Z}_6$.
* $G$ and $e$ are subgroups of $G$. 
Subgroups

Definition
A subset $H$ of a group $G$ is a subgroup if $H$ is a group under the same operation as in $G$. This is denoted $H \leq G$.

Examples:
* $\{0, 2, 4\}$ is a subgroup of $\mathbb{Z}_6$.
* $G$ and $e$ are subgroups of $G$.

Non-examples:
* $\mathbb{Z}_{>0}$ is not a subgroup of $(\mathbb{Z}, +)$ (inverses)
* $\mathbb{R} \setminus \{0\}$ is not a subgroup of $(\mathbb{R}, +)$ (identity)
Subgroups

Definition
A subset $H$ of a group $G$ is a subgroup if $H$ is a group under the same operation as in $G$. This is denoted $H \leq G$.

Examples:
* $\{0, 2, 4\}$ is a subgroup of $\mathbb{Z}_6$.
* $G$ and $e$ are subgroups of $G$.

Non-examples:
* $\mathbb{Z}_{>0}$ is not a subgroup of $(\mathbb{Z}, +)$ (inverses)
* $\mathbb{R} \setminus \{0\}$ is not a subgroup of $(\mathbb{R}, +)$ (identity)

Theorem
A non-empty subset $H$ of a group $(G, \ast)$ is a subgroup if and only if $xy^{-1} \in H$ for any $x, y \in H$. 
Isomorphisms

Consider the subgroup of $S_6$ generated by

$$(1 \ 6 \ 5 \ 4 \ 3 \ 2) \quad \text{and} \quad (16)(25)(34)$$
Isomorphisms

Consider the subgroup of $S_6$ generated by

$$r = (1 \ 6 \ 5 \ 4 \ 3 \ 2) \quad \text{and} \quad s = (16)(25)(34)$$
Isomorphisms

Consider the subgroup of $S_6$ generated by

\[ r = (1 \ 6 \ 5 \ 4 \ 3 \ 2) \quad \text{and} \quad s = (16)(25)(34) \]

In some sense, this subgroup is the same as $D_{12}$, but in some sense, they’re not the same until I name them appropriately. Since we don’t want to call them the same, we call them isomorphic.
Definition

An **isomorphism** between two groups $G$ and $H$ is a bijection $\varphi : G \rightarrow H$ such that

$$ \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) $$

for all $g_1, g_2 \in G$. Two groups $G$ and $H$ are **isomorphic** if there exists an isomorphism between them. We write $G \cong H$. 

**Examples**

1. $G$ is always isomorphic to itself via the identity map, though there may be other maps. We call these automorphisms.
2. $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}_{>0}, \times)$ via the map $\varphi : x \rightarrow e^x$.

   Check: $\varphi$ is a bijection and $\varphi(x + y) = e^x e^y = \varphi(x) \varphi(y)$.
3. $S_X$ is isomorphic to $S_{|X|}$.
4. $S_3$ is isomorphic to $D_6$.

**Fun fact:** "isomorphism" is an equivalence relation.
Definition
An isomorphism between two groups $G$ and $H$ is a bijection $\varphi : G \rightarrow H$ such that

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$$

for all $g_1, g_2 \in G$. Two groups $G$ and $H$ are isomorphic if there exists an isomorphism between them. We write $G \cong H$.

Examples

1. $G$ is always isomorphic to itself via the identity map, though there may be other maps. We call these automorphisms.
Definition
An isomorphism between two groups \( G \) and \( H \) is a bijection \( \varphi : G \rightarrow H \) such that

\[ \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) \]

for all \( g_1, g_2 \in G \). Two groups \( G \) and \( H \) are isomorphic if there exists an isomorphism between them. We write \( G \cong H \).

Examples

1. \( G \) is always isomorphic to itself via the identity map, though there may be other maps. We call these automorphisms.

2. \((\mathbb{R}, +)\) is isomorphic to \((\mathbb{R}_{>0}, \times)\) via the map \( \varphi : x \rightarrow e^x \).
Definition
An isomorphism between two groups $G$ and $H$ is a bijection $\varphi : G \to H$ such that

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)$$

for all $g_1, g_2 \in G$. Two groups $G$ and $H$ are isomorphic if there exists an isomorphism between them. We write $G \cong H$.

Examples

1. $G$ is always isomorphic to itself via the identity map, though there may be other maps. We call these automorphisms.

2. $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}_{>0}, \times)$ via the map $\varphi : x \to e^x$. Check: $\varphi$ is a bijection and

$$\varphi(x + y) = e^{x+y} = e^x \times e^y = \varphi(x) \varphi(y).$$
Definition
An **isomorphism** between two groups $G$ and $H$ is a bijection $\varphi : G \to H$ such that

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$$

for all $g_1, g_2 \in G$. Two groups $G$ and $H$ are **isomorphic** if there exists an isomorphism between them. We write $G \cong H$.

Examples

1. $G$ is always isomorphic to itself via the identity map, though there may be other maps. We call these **automorphisms**.
2. $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}_{>0}, \times)$ via the map $\varphi : x \to e^x$. Check: $\varphi$ is a bijection and

   $$\varphi(x + y) = e^{x+y} = e^x \ast e^y = \varphi(x)\varphi(y).$$

3. $S_X$ is isomorphic to $S_{|X|}$. 
Definition
An isomorphism between two groups $G$ and $H$ is a bijection $\varphi : G \to H$ such that

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$$

for all $g_1, g_2 \in G$. Two groups $G$ and $H$ are isomorphic if there exists an isomorphism between them. We write $G \cong H$.

Examples

1. $G$ is always isomorphic to itself via the identity map, though there may be other maps. We call these automorphisms.
2. $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}_{>0}, \times)$ via the map $\varphi : x \to e^x$. Check: $\varphi$ is a bijection and

$$\varphi(x + y) = e^{x+y} = e^x \cdot e^y = \varphi(x)\varphi(y).$$

3. $S_X$ is isomorphic to $S_{|X|}$.
4. $S_3$ is isomorphic to $D_6$.

Fun fact: “isomorphism” is an equivalence relation.
Definition
An isomorphism between two groups $G$ and $H$ is a bijection $\varphi : G \rightarrow H$ such that

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$$

for all $g_1, g_2 \in G$. Two groups $G$ and $H$ are isomorphic if there exists an isomorphism between them. We write $G \cong H$.

Examples

1. $G$ is always isomorphic to itself via the identity map, though there may be other maps. We call these automorphisms.
2. $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}_{>0}, \times)$ via the map $\varphi : x \rightarrow e^x$. Check: $\varphi$ is a bijection and
   $$\varphi(x + y) = e^{x+y} = e^x \times e^y = \varphi(x)\varphi(y).$$
3. $S_X$ is isomorphic to $S_{|X|}$.
4. $S_3$ is isomorphic to $D_6$.

Fun fact: “isomorphism” is an equivalence relation.
Isomorphisms into matrix groups
(without proof... we’ll come back to these).

(1) Denote the linear transformation in \( \mathbb{R}^2 \) that rotates everything clockwise by \( \phi \) radians by \( r_\phi \) and the linear transformation that flips across the y-axis by \( s_y \), i.e.

\[
 r_\phi = \begin{pmatrix} \cos(\phi) & \sin(\phi) \\ -\sin(\phi) & \cos(\phi) \end{pmatrix} \quad \text{and} \quad s_y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}
\]

Then \( D_{2n} \) is isomorphic to the multiplicative group of matrices generated by \( r_{2\pi/n} \) and \( s_y \).
Isomorphisms into matrix groups
(without proof... we’ll come back to these).

(1) Denote the linear transformation in $\mathbb{R}^2$ that rotates everything clockwise by $\phi$ radians by $r_\phi$ and the linear transformation that flips across the y-axis by $s_y$, i.e.

$$r_\phi = \begin{pmatrix} \cos(\phi) & \sin(\phi) \\ -\sin(\phi) & \cos(\phi) \end{pmatrix} \quad \text{and} \quad s_y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Then $D_{2n}$ is isomorphic to the multiplicative group of matrices generated by $r_{2\pi/n}$ and $s_y$.

(2) The symmetric group $S_n$ is isomorphic to the multiplicative group of $n \times n$ matrices satisfying

\textit{every row and column has exactly one 1 and $n - 1$ 0's.}

(Map $\{1, \ldots, n\}$ to $\{v_1, \ldots, v_n\}$)
Definition
A homomorphism from a group $G$ to a group $H$ is a function $\varphi : G \to H$ such that

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$$

for all $g_1, g_2 \in G$. 

Examples:
1. Let $\varphi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ be given by reducing mod 6. Then $\varphi$ is a homomorphism that is not an isomorphism.
2. Let $\varphi : \mathbb{Z} \to \mathbb{R}$ be the inclusion map.
3. The determinant map $\det : \text{GL}_n(\mathbb{R}) \to \mathbb{R}$ is a homomorphism.
Definition
A homomorphism from a group $G$ to a group $H$ is a function $\varphi : G \rightarrow H$ such that

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$$

for all $g_1, g_2 \in G$.  

($\varphi$ is not nec. a bijection)
Definition
A homomorphism from a group $G$ to a group $H$ is a function $\varphi : G \to H$ such that

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$$

for all $g_1, g_2 \in G$.  

($\varphi$ is not nec. a bijection)

Examples:

1. Let $\varphi : \mathbb{Z} \to \mathbb{Z}_6$ be given by reducing mod 6. Then $\varphi$ is a homomorphism that is not an isomorphism.
Definition

A homomorphism from a group $G$ to a group $H$ is a function $\varphi : G \to H$ such that

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)$$

for all $g_1, g_2 \in G$. (\(\varphi\) is not nec. a bijection)

Examples:

1. Let $\varphi : \mathbb{Z} \to \mathbb{Z}_6$ be given by reducing mod 6. Then $\varphi$ is a homomorphism that is not an isomorphism.

2. Let $\varphi : \mathbb{Z} \to \mathbb{R}$ be the inclusion map.
Definition
A homomorphism from a group $G$ to a group $H$ is a function $\varphi : G \to H$ such that

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)$$

for all $g_1, g_2 \in G$. (\varphi is not nec. a bijection)

Examples:

1. Let $\varphi : \mathbb{Z} \to \mathbb{Z}_6$ be given by reducing mod 6. Then $\varphi$ is a homomorphism that is not an isomorphism.

2. Let $\varphi : \mathbb{Z} \to \mathbb{R}$ be the inclusion map.

3. The determinant map $\det : \text{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism.
Properties of homomorphisms

Theorem

Let \( \varphi : G \to H \) be a homomorphism of groups.

1. \( \varphi(e_G) = e_H \).
2. For any \( x \in G \), \( \varphi(x^{-1}) = \varphi(x)^{-1} \).
3. For any \( x \in G \), \( |\varphi(x)| |x| \).
4. The image of \( \varphi \),

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

is a subgroup of \( H \).

5. The kernel of \( \varphi \),

\[
\ker(\varphi) = \{ g \in G \mid \varphi(g) = e_H \}
\]

is a subgroup of \( G \).