Warm-up:

The quaternion group, denoted \( Q_8 \), is the set

\[
\{1, -1, i, -i, j, -j, k, -k\}
\]

with product \( \cdot \) given by

\[
1 \cdot a = a \cdot 1 = a \quad \forall a \in Q_8, \quad (-1) \cdot (-1) = 1,
\]

\[
i^2 = j^2 = k^2 = -1, \quad (-1) \cdot a = a \cdot (-1) = -a \quad \forall a \in Q_8,
\]

(Think: three copies of \( \mathbb{C} \))

\[
i \cdot j = k = -j \cdot i, \quad j \cdot k = i = -k \cdot j, \quad k \cdot i = j = -i \cdot k.
\]

(Think: cross-product with \( i = v_1, j = v_2, k = v_3 \))

You try:

1. Write the group table (multiplication table) for \( Q_8 \).
2. Compute the order of each of the 8 elements of \( Q_8 \).
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.
Let $G$ and $H$ be groups. A homomorphism is a function $\varphi : G \to H$ satisfying

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

“structure preserving” (*)

for all $g_1, g_2 \in G$. 

Let $G$ and $H$ be groups. A **homomorphism** is a function $\varphi : G \to H$ satisfying

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \quad \text{"structure preserving"} \quad (\ast)$$

for all $g_1, g_2 \in G$.

**Think:** a **linear map** $L : F^n \to F^m$ of vector spaces “preserves vector space structure”, i.e. for all $v, v' \in F^n$, $c \in F$ (a field),

$$L(cv) = cL(v) \quad \text{and} \quad L(v + v') = L(v) + L(v').$$
Let $G$ and $H$ be groups. A **homomorphism** is a function $\varphi : G \to H$ satisfying

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) \quad \text{“structure preserving”} \quad (*)$$

for all $g_1, g_2 \in G$.

**Think:** a **linear map** $L : F^n \to F^m$ of vector spaces “preserves vector space structure”, i.e. for all $v, v' \in F^n$, $c \in F$ (a field),

$$L(cv) = cL(v) \quad \text{and} \quad L(v + v') = L(v) + L(v').$$

In a group, the corresponding “structure” is the binary operation.
Let $G$ and $H$ be groups. A **homomorphism** is a function $\varphi : G \rightarrow H$ satisfying

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) \quad \text{“structure preserving”} \quad (*)$$

for all $g_1, g_2 \in G$.

**Think:** a **linear map** $L : F^n \rightarrow F^m$ of vector spaces “preserves vector space structure”, i.e. for all $v, v' \in F^n$, $c \in F$ (a field),

$$L(cv) = cL(v) \quad \text{and} \quad L(v + v') = L(v) + L(v').$$

In a group, the corresponding “structure” is the binary operation. Similarly, a homomorphism of fields would “preserve” both addition *and* multiplication.
Let $G$ and $H$ be groups. A **homomorphism** is a function $\varphi : G \to H$ satisfying

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \quad \text{“structure preserving”} \quad (*)$$

for all $g_1, g_2 \in G$.

**Think:** a *linear map* $L : F^n \to F^m$ of vector spaces “preserves vector space structure”, i.e. for all $v, v' \in F^n$, $c \in F$ (a field),

$$L(cv) = cL(v) \quad \text{and} \quad L(v + v') = L(v) + L(v').$$

In a group, the corresponding “structure” is the binary operation. Similarly, a homomorphism of fields would “preserve” both addition *and* multiplication.

An **isomorphism** is a bijective homomorphism.
Let $G$ and $H$ be groups. A **homomorphism** is a function $\varphi : G \rightarrow H$ satisfying

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) \quad \text{“structure preserving”} \quad (\ast)$$

for all $g_1, g_2 \in G$.

**Think:** a linear map $L : F^n \rightarrow F^m$ of vector spaces “preserves vector space structure”, i.e. for all $v, v' \in F^n$, $c \in F$ (a field),

$$L(cv) = cL(v) \quad \text{and} \quad L(v + v') = L(v) + L(v').$$

In a group, the corresponding “structure” is the binary operation. Similarly, a homomorphism of fields would “preserve” both addition and multiplication.

An **isomorphism** is a bijective homomorphism. Two groups $G$ and $H$ are **isomorphic**, written $G \cong H$, if there exists an isomorphism between them.
A homomorphism is a function $\varphi : G \rightarrow H$ satisfying

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) \quad \text{“structure preserving”} \quad (*)$$

for all $g_1, g_2 \in G$. An isomorphism is a bijective homomorphism. Examples of isomorphisms:

1. $G$ is always isomorphic to itself via the identity map.
A **homomorphism** is a function $\varphi : G \to H$ satisfying

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \quad \text{“structure preserving”} \quad (\ast)$$

for all $g_1, g_2 \in G$. An **isomorphism** is a bijective homomorphism. **Examples of isomorphisms:**

1. $G$ is always isomorphic to itself via the identity map. Note that may be other isomorphisms! An isomorphism $\varphi : G \to G$ is called an **automorphism**.
A **homomorphism** is a function \( \varphi : G \rightarrow H \) satisfying

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

“structure preserving” \((*)\)

for all \( g_1, g_2 \in G \). An **isomorphism** is a bijective homomorphism.

**Examples of isomorphisms:**

1. \( G \) is always isomorphic to itself via the identity map. Note that may be other isomorphisms! An isomorphism \( \varphi : G \rightarrow G \) is called an **automorphism**.
2. \((\mathbb{R}, +)\) is isomorphic to \((\mathbb{R}_{>0}, \times)\) via the map \( \varphi : x \rightarrow e^x \).
A **homomorphism** is a function \( \varphi : G \rightarrow H \) satisfying

\[
\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) \quad \text{“structure preserving”} \quad (*)
\]

for all \( g_1, g_2 \in G \). An **isomorphism** is a bijective homomorphism.

**Examples of isomorphisms:**

1. \( G \) is always isomorphic to itself via the identity map. Note that may be other isomorphisms! An isomorphism \( \varphi : G \rightarrow G \) is called an **automorphism**.

2. \( (\mathbb{R},+) \) is isomorphic to \( (\mathbb{R}_{>0}, \times) \) via the map \( \varphi : x \rightarrow e^x \).
   Check: \( \varphi \) is a bijection and
   \[
   \varphi(x + y) = e^{x+y} = e^x \times e^y = \varphi(x)\varphi(y).
   \]
A homomorphism is a function \( \varphi : G \to H \) satisfying

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

“structure preserving” \((*)\)

for all \( g_1, g_2 \in G \). An isomorphism is a bijective homomorphism.

Examples of isomorphisms:

1. \( G \) is always isomorphic to itself via the identity map. Note that may be other isomorphisms! An isomorphism \( \varphi : G \to G \) is called an automorphism.

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 \( S_{|X|} \).
A homomorphism is a function $\varphi : G \to H$ satisfying

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \quad \text{“structure preserving”} \quad (*)$$

for all $g_1, g_2 \in G$. An isomorphism is a bijective homomorphism.

Examples of isomorphisms:

1. $G$ is always isomorphic to itself via the identity map. Note that may be other isomorphisms! An isomorphism $\varphi : G \to G$ is called an automorphism.

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 $S_{|X|}$.

4. $S_3$ is isomorphic to $D_6$. 

A homomorphism is a function $\varphi : G \rightarrow H$ satisfying

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) \quad \text{“structure preserving”} \quad (\ast)$$

for all $g_1, g_2 \in G$. An isomorphism is a bijective homomorphism.

Examples of homomorphisms that aren’t isomorphisms:
A homomorphism is a function \( \varphi : G \rightarrow H \) satisfying

\[
\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \quad \text{“structure preserving”} \quad (*)
\]

for all \( g_1, g_2 \in G \). An isomorphism is a bijective homomorphism.

Examples of homomorphisms that aren’t isomorphisms:

1. Let \( \varphi : \mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z} \) be given by reducing mod 6.
A homomorphism is a function $\varphi : G \to H$ satisfying

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \quad \text{“structure preserving”} \quad (\star)$$

for all $g_1, g_2 \in G$. An isomorphism is a bijective homomorphism.

Examples of homomorphisms that aren’t isomorphisms:

1. Let $\varphi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ be given by reducing mod 6.
2. Let $\varphi : \mathbb{Z} \to \mathbb{R}$ be the inclusion map.
A homomorphism is a function $\varphi : G \rightarrow H$ satisfying

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \quad \text{“structure preserving” \quad (*)}$$

for all $g_1, g_2 \in G$. An isomorphism is a bijective homomorphism.

Examples of homomorphisms that aren’t isomorphisms:

1. Let $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$ be given by reducing mod 6.
2. Let $\varphi : \mathbb{Z} \rightarrow \mathbb{R}$ be the inclusion map.
3. The determinant map $\det : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$ is a homomorphism.
A homomorphism is a function $\varphi : G \to H$ satisfying

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \quad \text{“structure preserving”} \quad (*)$$

for all $g_1, g_2 \in G$. An isomorphism is a bijective homomorphism.

Examples of homomorphisms that aren’t isomorphisms:

1. Let $\varphi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ be given by reducing mod 6.
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.

Fact:

“$G \simeq H$ whenever $G \cong H$” is an interesting equivalence relation.
A homomorphism is a function $\varphi : G \rightarrow H$ satisfying

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \quad \text{“structure preserving”} \quad (*)$$

for all $g_1, g_2 \in G$. An isomorphism is a bijective homomorphism.

Examples of homomorphisms that aren’t isomorphisms:

1. Let $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$ be given by reducing mod 6.
2. Let $\varphi : \mathbb{Z} \rightarrow \mathbb{R}$ be the inclusion map.
3. The determinant map $\det : \operatorname{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$ is a homomorphism.

Fact:

“$G \sim H$ whenever $G \cong H$”

is an interesting equivalence relation. On the other hand,

“$G \sim H$ whenever there’s a homomorphism $\varphi : G \rightarrow H$”

is a completely uninteresting equivalence relation.
Representations

A homomorphism from a group $G$ to a matrix group $\text{GL}_n(F)$ is called a group representation.
Representations

A homomorphism from a group $G$ to a matrix group $\text{GL}_n(F)$ is called a group representation.

(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 $s_y$. 
Representations

A homomorphism from a group $G$ to a matrix group $\text{GL}_n(F)$ is called a group representation.

(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

*every row and column has exactly one 1 and $n - 1$ 0’s.*

(Since $S\{1,\ldots,n\} \cong S\{v_1,\ldots,v_n\}$)
Properties of homomorphisms

Theorem

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

1. $\varphi(1_G) = 1_H$.  

(On homework.)
Properties of homomorphisms

Theorem

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

1. \( \varphi(1_G) = 1_H \).
2. For any \( x \in G \), \( \varphi(x^{-1}) = \varphi(x)^{-1} \).
Properties of homomorphisms

Theorem

Let $\varphi : G \rightarrow H$ be a homomorphism of groups.

1. $\varphi(1_G) = 1_H$.
2. For any $x \in G$, $\varphi(x^{-1}) = \varphi(x)^{-1}$.
3. For any $x \in G$, $|\varphi(x)|$ divides $|x|$. 

(On homework.)
Properties of homomorphisms

Theorem
Let $\varphi : G \rightarrow H$ be a homomorphism of groups.

1. $\varphi(1_G) = 1_H$.
2. For any $x \in G$, $\varphi(x^{-1}) = \varphi(x)^{-1}$.
3. For any $x \in G$, $|\varphi(x)|$ divides $|x|$.
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 $H$. 
Properties of homomorphisms

Theorem

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

1. $\varphi(1_G) = 1_H$.
2. For any $x \in G$, $\varphi(x^{-1}) = \varphi(x)^{-1}$.
3. For any $x \in G$, $|\varphi(x)|$ divides $|x|$.
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 $\varphi$,

   $$\text{ker}(\varphi) = \{ g \in G \mid \varphi(g) = 1_H \}$$

   is a subgroup of $G$. (On homework.)
Recall, for all $x, y \in G$, we have $xy = yx$ if and only if $xyx^{-1} = 1$. We call the expression $xyx^{-1}$ the conjugation of $y$ by $x$. 
Recall, for all $x, y \in G$, we have $xy = yx$ if and only if $xyx^{-1} = 1$. We call the expression $xyx^{-1}$ the conjugation of $y$ by $x$. For example, conjugating elements of $D_6$ looks like

$\begin{array}{cccccc}
xyx^{-1} & 1 & r & r^2 & s & sr & sr^2 \\
1 & 1 & r & r^2 & s & sr & sr^2 \\
r & 1 & r & r^2 & sr & sr^2 & s \\
r^2 & 1 & r & r^2 & sr^2 & s & sr \\
s & 1 & r^2 & r & s & sr^2 & sr \\
sr & 1 & r^2 & r & sr^2 & sr & s \\
sr^2 & 1 & r^2 & r & sr & s & sr^2 \\
\end{array}$
Recall, for all $x, y \in G$, we have $xy = yx$ if and only if $xyx^{-1} = 1$. We call the expression $xyx^{-1}$ the **conjugation of $y$ by $x$**. For example, conjugating elements of $D_6$ looks like

\[
\begin{array}{c|cccccc}
  & 1 & r & r^2 & s & sr & sr^2 \\
\hline
 1 & 1 & r & r^2 & s & sr & sr^2 \\
\hline
r & 1 & r & r^2 & sr & sr^2 & s \\
\hline
r^2 & 1 & r & r^2 & sr^2 & s & sr \\
\hline
s & 1 & r^2 & r & s & sr^2 & sr \\
\hline
sr & 1 & r^2 & r & sr^2 & sr & s \\
\hline
sr^2 & 1 & r^2 & r & sr & s & sr^2 \\
\end{array}
\]

On the other hand, the subgroups of $D_6$ are

\[
\{1\}, \quad \{1, s\}, \quad \{1, sr\}, \quad \{1, sr^2\}, \quad \{1, r, r^2\}, \quad \text{and} \quad D_6.
\]
More special subgroups

Let $A$ be a non-empty subset of $G$ (not necessarily a subgroup). The centralizer of $A$ in $G$ is

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

Since

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

this is the set of elements which commute with all $a$ in $A$.

If $A = \{a\}$, we write $C_G(\{a\}) = C_G(a)$.
More special subgroups

Let $A$ be a non-empty subset of $G$ (not necessarily a subgroup). The centralizer of $A$ in $G$ is

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

Since

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

this is the set of elements which commute with all $a$ in $A$.

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

**Theorem**

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