1.6: Homomorphisms and Isomorphisms

The same group structure can appear in dramatically different ways.

\[ \mathbb{Z}/4\mathbb{Z} = \{ 0, 1, 2, 3 \} \text{ with } + \]

\[ (\mathbb{Z}/5\mathbb{Z})^* = \{ 1, 2, 3, 4 \} \text{ with } \times \]

There is a mapping \( j: \mathbb{Z}/4\mathbb{Z} \rightarrow 2 \in (\mathbb{Z}/5\mathbb{Z})^* \)

with the property

\[ 2^{j+k} = 2^j \cdot 2^k \]

Thus, the group tables have the same pattern

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>\times</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

Def: A mapping \( \phi: G_1 \rightarrow G_2 \) from one group \( G_1 \)
to another \( G_2 \) is a homomorphism if

\[ \phi(gh) = \phi(g) \phi(h) \text{ for all } g, h \in G_1 \]

It's an isomorphism if it is also a bijection.
Corollaries: 1) \( \varphi(2) = 1 \) in \( G_1 \) in \( G_2 \)
\[ \varphi(s^{-1}) = \varphi(s)^{-1} \]

Proof: (1) \( \varphi(1, 1) = \varphi(1) \varphi(1) \) by defn.

So \( \varphi(1) = \varphi(1) \varphi(1) \).

Cancel \( \varphi(1) \) on each side to get \( \varphi(1) = 1 \).

\( \varphi(s \cdot s^{-1}) = \varphi(s) \varphi(s^{-1}) \)
\[ = \varphi(1) = 1 \text{ by part (1)} \]

Hence \( \varphi(s^{-1}) = \varphi(s)^{-1} \).

\( D_6 \cong S_3 \): \( D_6 = \langle r, s \mid r^3 = s^2 = 1, \quad rs = s r^{-1} \rangle \)

Define \( \varphi: D_6 \to S_3 \)

by \( \varphi(r) = (1, 2, 3), \varphi(s) = (1, 2) \)

and extending by the homomorphism property,

\( \varphi(s^i r^j) = \varphi(s)^i \varphi(r)^j \).

This is well-defined provided \( \varphi(r) = 1 \),
\( \varphi(s)^2 = 1, \varphi(r) \varphi(s) = \varphi(s) \varphi(r)^{-1} \).
One can check this is true for $\varphi(2) = (1\ 2\ 3)$, $\varphi(3) = (1\ 2)$.

Since $(1\ 2\ 3)$ and $(1\ 2)$ generate $S_3$,

$\varphi$ is surjective.

Since $|D_6| = |S_3| = 6$, it's a bijection.

**Fact:** Let $G$ be a group with generators $s_1, \ldots, s_m$.

Let $H$ be another group with elements $r_1, \ldots, r_m$.

Suppose any relation among $s_1, \ldots, s_m$ in $G$
also holds for $r_1, \ldots, r_m$ in $H$.

Then there is a unique homomorphism $\varphi: G \to H$
satisfying $\varphi(s_j) = r_j$ for $j = 1, \ldots, m$. 
We say a group is cyclic if it is isomorphic to \((\mathbb{Z}/m\mathbb{Z})^+\) for some \(m \geq 1\).

This group is often denoted \(C_m\), the cyclic group of order \(m\).

Theorem: \((\mathbb{Z}/m\mathbb{Z})^\times\) is a cyclic group of order \(\varphi(m)\) precisely when \(m = 1, 2, 4, p^k\) or \(2p^k\) for an odd prime \(p\) and integer \(k \geq 1\).

Prop: If \(A\) and \(B\) are sets of the same cardinality, then \(\text{Bij}(A) \approx \text{Bij}(B)\) (are isomorphic).

Given a group \(G\), let \(\overline{G}\) be \(G\) with \(x \cdot y = y \cdot x\). Are \(G\) and \(\overline{G}\) isomorphic?
Dodecahedron: NOT (including reflections)
The group \( \Gamma \) of symmetries of the icosahedron is isomorphic to

\[ A_5 = \text{subgroup of "even" permutations in } S_5 \]

(A permutation is even if it is a composition of an even number of (not necessarily disjoint) 2-cycles (or transpositions)).

\( \Gamma \) is also isomorphic to \( \text{PSL}_2(\mathbb{F}_5) \)

\[ = \text{SL}_2(\mathbb{F}_5) / \{ \pm I \} \]

This will require more theory to prove.
\textbf{Defn:} The \underline{kernel} of a homomorphism of groups $\varphi: G \to H$ is
\[
\{ x \in G \mid \varphi(x) = 1 \text{ in } H \}.
\]

\textbf{Prop:} The kernel $\ker \varphi$ is a subgroup of $G$.

The \underline{image} $\text{im} \varphi$ is a subgroup of $H$.

\textbf{Proof:} Show there are closed under multiplication and inverse, and they contain $1$.

\textbf{Ex:} The \underline{determinant} is a homomorphism
\[
\text{det}: \text{GL}_n(F) \to F^x
\]

since $\text{det}(AB) = \text{det}(A) \text{det}(B)$, $\text{det}(I) = 1$.

The kernel is $\text{SL}_n(F)$.