Group Homomorphisms

Recall: for sets \( f : A \to B \)

Now, for groups: \( \phi : G \to G' \)

Injective, Bijective, Surjective

Well-defined

Homomorphisms

Injective

Isomorphism

Well-defined + (\( k \))

\( \phi(g \cdot h) = \phi(g) \cdot \phi(h) \)

Does the fn \( \phi : G \to G' \) satisfy...

1. \( \phi(e_G) = e_{G'} \)?
2. \( \phi(g^{-1}) = \phi(g)^{-1} \)?
3. \( \phi(g^k) = \phi(g)^k \)?

If the answer to any of these is "No" then \( \phi \) can't satisfy (*)!

Checking (1) - (3) isn't enough (in general) to know \( \phi \) satisfies (4).

These conditions are necessary, not sufficient.

**Ex.** \( \mathbb{Z} \xrightarrow{\text{mod} 2} \mathbb{Z} \) is not a homomorphism

Proof: It's a function, but it doesn't satisfy (*):

\[(x+y)^2 \neq x^2 + y^2 \quad \text{(e.g., } x = y = 1)\]

**Ex.** \( \mathbb{Z} \xrightarrow{\cdot} \mathbb{Z} \) is an endomorphism

Proof: Multiplication is a well-defined function, and (4) encodes distribution:

\[n \cdot (x+y) = n \cdot x + n \cdot y \quad \forall x, y \in \mathbb{Z} \]

This is called an "involution"

Ex. \( \mathbb{Z} \xrightarrow{-} \mathbb{Z} \) is an automorphism

Proof: Multiplication by -1 is a bijection (its inverse is itself!) and satisfies (4) by the previous ex.

Note: \( \mathbb{Z} \xrightarrow{\cdot} \mathbb{Z} \) is a different automorphism!

We can consider the set \( \text{Aut}(G) = \{ \text{automorphisms of } G \} \).

In fact:

**Prop.** \( \text{Aut}(G) \) is a group! (under composition)

Ex. What is \( \text{Aut}(\mathbb{Z}) \)? Claim \( \text{Aut}(\mathbb{Z}) = \langle 1 \rangle \approx \mathbb{Z} / \mathbb{Z} \)

Proof: We first establish \( \text{Aut}(\mathbb{Z}) = \langle 1 \rangle \) as a set. We've already discussed \( \mathbb{Z} \) so we just need to show \( \leq \). Let \( \phi \in \text{Aut}(\mathbb{Z}) \). Since \( \phi \) is a homomorphism, \( \phi(0) = 0 \) and \( \phi(n) = \phi(1+1+\ldots+1) = \phi(1) + \ldots + \phi(1) = n \cdot \phi(1) \). That is, \( \phi \) can be described...
as “multiplication by \(\phi(1)\). This is a bijection iff \(\phi(1) \in \{-1, 1\}\).

Now we show \(\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}\) as groups. Consider \(f: \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}\) which sends \(+1 \to 0\) and \(-1 \to 1\). (Note: this is the only choice since \(f(0) = 0\) necessarily.) To check \(f\) is a group homomorphism, the only non-trivial part to check is

\[
f(-1 \cdot -1) = f(id) = 0 = f(-1) + f(-1).
\]

\[\square\]

**Prop** \(\Phi: G \to G'\) is a group homomorphism, then

1. \(H \leq G \implies \Phi(H) \leq G'\)
2. \(H' \leq G' \implies \Phi^{-1}(H') \leq G\)

**Pf**

1. Let \(H \leq G\). Since \(e \in H\) and \(e\) is the group hom,

\[
e = \phi(e) \in \Phi(H).
\]

Now suppose \(g, g' \in \Phi(H)\). Then \(g = \phi(h)\) and \(g' = \phi(h')\) for some \(h, h' \in H\). Thus \(h \cdot h' \in H\) and

\[
g \cdot g' = \phi(h) \cdot \phi(h') = \phi(h \cdot h') \in \Phi(H).
\]

Finally, if \(g \in \Phi(H)\), so \(g = \phi(h)\) for some \(h \in H\), then \(h' \in H\) so

\[
g^{-1} = \phi(h)^{-1} = \phi(h^{-1}) \in \Phi(H).
\]

Hence \(\Phi(H) \leq G'\).

2. Now let \(H' \leq G'\). Since \(e \in H'\), we can consider \(\Phi^{-1}(e) = \{g \in G \mid \Phi(g) = e\}\), and since \(\Phi\) is a group hom, we know \(e \in \Phi^{-1}(e) \subseteq \Phi^{-1}(H')\). Now suppose \(g, g' \in \Phi^{-1}(H')\). By defn, \(\Phi(g), \Phi(g') \in H'\) so \(\Phi(g) \cdot \Phi(g') = \Phi(g \cdot g') \in H'\). Hence \(g \cdot g' \in \Phi^{-1}(H')\).

Finally, if \(g \in \Phi^{-1}(H')\), then \(\phi(g) \in H'\) so \(\phi(g)^{-1} = \phi(g^{-1}) \in H'\) and therefore \(g \in \Phi^{-1}(H')\).

\[\square\]

**Ex/Defn** The kernel of \(\Phi: G \to G'\) is \(\ker(\Phi) = \Phi^{-1}(e)\). We just showed \(\ker(\Phi) \leq G\).

**Prop** \(\Phi\) is injective \(\iff\ ker(\Phi) = e\).

**Pf** \((\Rightarrow)\) If \(x \in \ker(\Phi)\), then \(\Phi(x) = e = \phi(e)\), so injectivity implies \(x = e\).

\((\Leftarrow)\) Suppose \(\Phi(x) = \phi(y)\). Then \(e = \Phi(y) \Phi(x)^{-1} = \Phi(y) \phi(x)^{-1} = \Phi(y \phi(x^{-1}) = \phi(y \phi(x^{-1})^{-1}) \in \ker(\Phi)\).

So \(y \phi(x^{-1}) \in \ker(\Phi).\) If \(\ker(\Phi) = e\), this says \(y \phi(x^{-1}) = e\), i.e. \(y = \phi(x)\). So \(\Phi\) is injective.

**Ex/Defn** The image of \(\Phi: G \to G'\) is \(\text{im}(\Phi) = \Phi(G)\). We showed \(\text{im}(\Phi) \leq G'\).
**Prop.** \( \Phi \) is surjective \( \iff \text{im}\Phi = G' \).

**Pf.** (\( \Rightarrow \)) We know \( \mathcal{E} \), so just need to show \( \text{im}\Phi \supseteq G' \). Given \( g' \in G' \), \( \exists g \in \mathcal{G} \) s.t. \( \Phi(g) = g' \).

Since \( \Phi \) is surjective. Then by defn, \( g' \in \text{im}\Phi \).

(\( \Leftarrow \)) Let \( g' \in G' \). Then since \( G' = \text{im}\Phi = \{\Phi(g) | g \in \mathcal{G} \} \) there exists \( g \in \mathcal{G} \) s.t. \( g' = \Phi(g) \).

This is the defn of \( \Phi \) being surjective. \( \Box \)

**Rmk** \( \Phi : \mathcal{G} \to G' \) is gp isomorphism (1) if \( \Phi \) hom and (2) is bij.

\[ \text{and (2) holds } \iff \ker\Phi = e \in \mathcal{G} \]

\[ \text{im}\Phi = G' \]

(also \( \iff \exists \text{ inverse } \Phi' : G' \to \mathcal{G} \))

**Ex.** Consider the group \( G \) by Cayley table:

<table>
<thead>
<tr>
<th>*</th>
<th>e</th>
<th>( \text{( \star )} )</th>
<th>( \triangle )</th>
<th>( \ast )</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>( \text{( \star )} )</td>
<td>( \triangle )</td>
<td>( \ast )</td>
</tr>
<tr>
<td>( \text{( \star )} )</td>
<td>( \text{( \star )} )</td>
<td>e</td>
<td>( \ast )</td>
<td>( \triangle )</td>
</tr>
<tr>
<td>( \triangle )</td>
<td>( \triangle )</td>
<td>( \text{( \star )} )</td>
<td>e</td>
<td>( \ast )</td>
</tr>
<tr>
<td>( \ast )</td>
<td>( \ast )</td>
<td>( \triangle )</td>
<td>( \text{( \star )} )</td>
<td>e</td>
</tr>
</tbody>
</table>

**Claim** \( G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = K4 \) "klein 4 gp"

**Pf.** Define \( \Phi : G \to K4 \) by

\[ \begin{align*}
\heartsuit & \mapsto (0,0) & \bigstar & \mapsto (0,1) \\
\bigtriangleup & \mapsto (1,0) & \spadesuit & \mapsto (1,1).
\end{align*} \]

This is bijective, and can check it's a hom using the Cayley table. (exc)

**Note** Could have defined \( \Phi \) by

\[ \begin{align*}
\heartsuit & \mapsto (0,0) & \bigstar & \mapsto (1,0) \\
\bigtriangleup & \mapsto (0,1) & \spadesuit & \mapsto (1,1).
\end{align*} \]

This is a different isomorphism! (\( \cong \) isos not nec. unique)

Call it \( \Phi' \). Note \( \Phi' = \Phi \circ \text{swap} \), where \( \text{swap} \in \text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \) swaps the two factors; i.e. switches \((1,0) \leftrightarrow (0,1)\). (up to isomorphism)

**Q.** Given \( n \in \mathbb{Z}_{>1} \), how many groups are there of order \( n \)?

**A.** Well...

<table>
<thead>
<tr>
<th>( n )</th>
<th>e</th>
<th>( \text{( \star )} )</th>
<th>( \triangle )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>( \text{( \star )} )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>( \triangle )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>( \text{( \star )} )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 5 | \( \text{\( \star \)} \) \\
| 6 | \( \text{\( \star \)} \) |

Wikipedia has a list for \( n \leq 30 \)

in general, this is very hard!! (believed impossible in general)

\( \Rightarrow \) simplicity by adding restrictions:

- \( n = p \text{ prime} : \mathbb{Z}/p \)
- \( G \text{ is simple} : " \text{classification of finite} \text{ check out!} " \)
- \( G \text{ solvable} : " \text{simple gps} " (\text{monster group}) \)
- \( |G| = pq \text{ primes p,q} : " \text{...} " \)

Sylow Thms (to be discussed) will be helpful!
Group Work

(1) (a) Prove $\text{Aut}(G)$ is a group ($G$ is a group).
    (b) Given two groups $G, G'$, is $\text{Hom}(G, G') = \{ \phi: G \to G' \mid \phi \text{ hom}\} \text{ a group?}$
        If yes, prove it. If not, can you add conditions to make it a group?
        Bonus: When is the resulting group Abelian?
        
(2) Let $(A, +, 0)$ be an Abelian group and $u, v: A \to A$ homomorphisms. Define $f, g: A \to A$ by
    
    $f(a) = a - v(u(a))$ and $g(a) = a - u(v(a))$.
    
    Show $\ker f \cong \ker g$.

(3) Let $G$ be a finite group and $\phi: G \to G$ an automorphism s.t. $\phi(g) = g \circ g \circ e$.
    Prove (a) every $x$ in $G$ is of the form $g \circ \phi(g)$
    (b) if $\phi$ is an involution ($\phi \circ \phi = id$) then $\phi = i$ is inversion
        and $G$ is an Abelian group of odd order.