Homomorphisms

- A function \( f : G \to H \) from a group \( G \) to a group \( H \) is a **homomorphism** (or a **group map**) if \( f(ab) = f(a)f(b) \) for all \( a, b \in G \).

- A homomorphism is an **isomorphism** if it is bijective — equivalently, if it has an inverse.

- If \( G \) and \( H \) are groups, \( G \) and \( H \) are **isomorphic** if there is an isomorphism \( f : G \to H \). Isoomorphic groups are the same as groups.

- If \( f : G \to H \) is a group map, then \( f(1) = 1 \) and \( f(a^{-1}) = f(a)^{-1} \).

- The **kernel** of a group map \( f : G \to H \) is \( \ker f = \{ a \in G \mid f(a) = 1 \} \). \( \ker f \) is a subgroup of \( G \).

- The **image** of a group map \( f : G \to H \) is \( \text{im} f = \{ f(a) \mid a \in G \} \). \( \text{im} f \) is a subgroup of \( H \).

- Groups \( G \) and \( H \) are not isomorphic if they have different orders, or if one has a group-theoretic property that the othe doesn’t. For example, two groups are not isomorphic if one is abelian and the other is not; two groups are not isomorphic if the orders of elements of one are not the same as the orders of elements of the other.

Here are the operation tables for two groups of order 4:

<table>
<thead>
<tr>
<th>·</th>
<th>1</th>
<th>a</th>
<th>a²</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>a</td>
<td>a²</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>a²</td>
<td>1</td>
</tr>
<tr>
<td>a²</td>
<td>a²</td>
<td>1</td>
<td>a</td>
</tr>
</tbody>
</table>

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

There is an obvious sense in which these two groups are “the same”: You can get the second table from the first by replacing 0 with 1, 1 with \( a \), and 2 with \( a² \).

When are two groups the same?

You might think of saying that two groups are the same if you can get one group’s table from the other by substitution, as above. However, there are problems with this. In the first place, it might be very difficult to check — imagine having to write down a multiplication table for a group of order 256! In the second place, it’s not clear what a “multiplication table” is if a group is infinite.

**One way to implement a substitution is to use a function.** In a sense, a function is a thing which “substitutes” its output for its input. I’ll define what it means for two groups to be “the same” by using certain kinds of functions between groups. These functions are called **group homomorphisms**; a special kind of homomorphism, called an **isomorphism**, will be used to define “sameness” for groups.

**Definition.** Let \( G \) and \( H \) be groups. A **homomorphism** from \( G \) to \( H \) is a function \( \phi : G \to H \) such that

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

for all \( g_1, g_2 \in G \).

**Terminology.** Group homomorphisms are often referred to as **group maps** for short.

**Remarks.** 1. You have seen patterns like this before; for example, “The derivative of a sum is the sum of the derivatives”.

1
2. Group homomorphisms are to groups as linear transformations are to vector spaces. Consider the definitions:

<table>
<thead>
<tr>
<th>A group has a single binary operation:</th>
<th>A vector space has two operations:</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a \bullet b )</td>
<td>( \text{vector addition} \quad v + w )</td>
</tr>
<tr>
<td>A group homomorphism preserves the operation:</td>
<td>( \text{scalar multiplication} \quad k \cdot v )</td>
</tr>
<tr>
<td>( f(a \bullet b) = f(a) \bullet f(b) )</td>
<td>( \mathbb{L}(v + w) = \mathbb{L}(v) + \mathbb{L}(w) )</td>
</tr>
<tr>
<td></td>
<td>( \mathbb{L}(k \cdot v) = k \cdot \mathbb{L}(v) )</td>
</tr>
</tbody>
</table>

Example. (The identity map and inclusion maps are group maps) If \( G \) is a group, the identity map \( \text{id} : G \rightarrow G \) given by \( \text{id}(g) = g \) and the constant map \( 1 : G \rightarrow G \) given by \( 1(g) = 1 \) are homomorphisms.

Moreover, if \( H \leq G \), the inclusion map \( i : H \hookrightarrow G \) given by \( i(h) = h \) is a homomorphism.

Example. (Constant maps are usually not group maps) In general, constant maps aren’t homomorphisms. Consider the group \( \mathbb{Z} \) under addition, and look at \( f : \mathbb{Z} \rightarrow \mathbb{Z} \) given by \( f(n) = 3 \) for all \( n \). Then

\[
\begin{align*}
f(1 + 1) &= f(2) = 3, & \text{but} & & f(1) + f(1) &= 3 + 3 = 6.
\end{align*}
\]

Example. (Logs and exponentials) \( \exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \cdot) \) is a homomorphism from the reals under addition to the positive reals under multiplication.

The operation on the domain \( \mathbb{R} \) is addition, while the operation on the range \( \mathbb{R}^+ \) is multiplication. Therefore, to show \( \exp \) is a homomorphism, I have to show that

\[
\exp(x + y) = \exp(y) \cdot \exp(y) \quad \text{for all} \quad x, y \in \mathbb{R}.
\]

But \( \exp(x + y) = e^{x+y} \) and \( \exp(y) \cdot \exp(y) = e^x e^y \), so the equation to be verified comes down to the familiar identity \( e^{x+y} = e^x e^y \). Thus, \( \exp \) is a homomorphism.

Notice that \( \exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}, +) \) is not a homomorphism. In this case, I’m using addition as the operation on both the domain and range, so the homomorphism property would say “\( \exp(x + y) = \exp(x) + \exp(y) \)” — in other words, “\( e^{x+y} = e^x + e^y \)”.

This is not an identity; for example, if \( x = 1 \) and \( y = 1 \), \( e^{x+y} = e^2 \), while \( e^x + e^y = 2e \), and \( e^2 \neq 2e \).

In basic math courses, people often get sloppy and refer to “the function \( e^x \)”.

As this example shows, a function isn’t just a rule; it’s a rule together with a domain and a range. In many basic math situations, the domain and range don’t play a large role; in this situation they do.
Example. (Checking whether a function is a group map) Define $f : \mathbb{Z} \to \mathbb{Z}$ by

$$f(x) = 5x.$$ 

To show that $f$ is a homomorphism, let $x, y \in \mathbb{Z}$. Since the operation on $\mathbb{Z}$ is addition, I must show that $f(x + y) = f(x) + f(y)$. Check it:

$$f(x + y) = 5(x + y) = 5x + 5y = f(x) + f(y).$$

Therefore, $f$ is a homomorphism.

To show that a function is not a homomorphism, give a specific counterexample. For example, define $g : \mathbb{Z} \to \mathbb{Z}$ by

$$g(x) = x^2.$$ 

To show that $g$ is not a homomorphism, I must find $x, y \in \mathbb{Z}$ such that $g(x + y) \neq g(x) + g(y)$. I'll pick two values at random, say $x = 2$ and $y = 3$. Try it:

$$g(2 + 3) = g(5) = 5^2 = 25, \quad \text{but} \quad g(2) + g(3) = 2^2 + 3^2 = 4 + 9 = 13.$$ 

Since $g(2 + 3) \neq g(2) + g(3)$, $g$ is not a homomorphism. 

Example. (A group map on a matrix group) Let $M(2, \mathbb{R})$ be the group of $2 \times 2$ reals matrices under matrix addition. Let $\text{tr} : M(2, \mathbb{R}) \to \mathbb{R}$ denote the trace map:

$$\text{tr} \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = a + d.$$ 

Now

$$\text{tr} \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) + \text{tr} \left( \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \right) = \text{tr} \left( \begin{bmatrix} a + a' & b + b' \\ c + c' & d + d' \end{bmatrix} \right) = (a + a') + (d + d'),$$

$$\text{tr} \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) + \text{tr} \left( \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \right) = (a + d) + (a' + d').$$

Since $(a + a') + (d + d') = (a + d) + (a' + d')$, it follows that

$$\text{tr} \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) + \text{tr} \left( \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \right) = \text{tr} \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) + \text{tr} \left( \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \right).$$

Therefore, $\text{tr}$ is a homomorphism. 

Example. (Group maps and linear transformations) I observed earlier that group homomorphisms are analogous to linear transformations. In fact, a vector space is an abelian group under vector addition. Thinking of a vector space in this way, a linear transformation is a group homomorphism.

Remember that the definition of a linear transformation requires that

$$T(\vec{u} + \vec{v}) = T(\vec{u}) + T(\vec{v})$$

for all vectors $\vec{u}$ and $\vec{v}$. This means that $T$ is a group homomorphism.

Here’s a specific example. $\mathbb{R}^2$ is a 2-dimensional vector space. If you think about the axioms for a vector space, you can see that $\mathbb{R}^2$ is an abelian group under vector addition.

Consider the linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$T(x, y) = (2x + 3y, x + 2y).$$
In matrix form, this is
\[ T \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}. \]

Since matrix multiplication distributes over vector addition,
\[ T \left( \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} x' \\ y' \end{bmatrix} \right) = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} = T \begin{bmatrix} x \\ y \end{bmatrix} + T \begin{bmatrix} x' \\ y' \end{bmatrix}. \]

This gives a direct proof that \( T \) is a group homomorphism. \( \Box \)

Example. (A group map involving multiplication and addition) Let \( \mathbb{Q} \) be the group of rational numbers under addition; let \( \mathbb{Q}^+ \) be the group of positive rational numbers under multiplication. Define \( f : \mathbb{Q} \rightarrow \mathbb{Q}^+ \) by
\[ f(x) = 2^x. \]

I’ll check that \( f \) is a homomorphism. Note that since the operation on \( \mathbb{Q} \) is addition (+) and the operation on \( \mathbb{Q}^+ \) is multiplication (\( \cdot \)), I must show that
\[ f(x + y) = f(x) \cdot f(y) \text{ for all } x, y \in \mathbb{Q}. \]

Here’s the computation:
\[ f(x + y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y). \]

Therefore, \( f \) is a homomorphism. \( \Box \)

Lemma. Let \( \phi : G \rightarrow H \) be a group homomorphism. Then:

(a) \( \phi(1_G) = 1_H \), where \( 1_G \) is the identity in \( G \) and \( 1_H \) is the identity in \( H \).

(b) \( \phi(g^{-1}) = \phi(g)^{-1} \) for all \( g \in G \).

Proof.
\[ \phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G) \cdot \phi(1_G). \]

If I cancel \( \phi(1_G) \) off both sides, I obtain \( \phi(1_G) = 1_H \).

Now let \( g \in G \).
\[ \phi(g) \cdot \phi(g^{-1}) = \phi(g \cdot g^{-1}) = \phi(1_G) = 1_H \]
\[ \phi(g^{-1}) \cdot \phi(g) = \phi(g^{-1} \cdot g) = \phi(1_G) = 1_H \]

This shows that \( \phi(g^{-1}) \) is the inverse of \( \phi(g) \), i.e. \( \phi(g)^{-1} = \phi(g^{-1}) \). \( \Box \)

Warning. The properties in the last lemma are not part of the definition of a homomorphism. To show that \( f \) is a homomorphism, all you need to show is that \( f(a \cdot b) = f(a) \cdot f(b) \) for all \( a \) and \( b \). The properties in the lemma are automatically true of any homomorphism.

On the other hand, if you want to show a function is not a homomorphism, do a quick check: Does it send the identity to the identity? If not, then the lemma shows it’s not a homomorphism. \( \Box \)

Example. (Group maps must take the identity to the identity) Let \( \mathbb{Z} \) denote the group of integers with addition. The function \( f : \mathbb{Z} \rightarrow \mathbb{Z} \) given by
\[ f(x) = x + 1 \]
has $f(0) = 1$. Since the identity $0 \in \mathbb{Z}$ is not mapped to the identity $0 \in \mathbb{Z}$, $f$ cannot be a group homomorphism.

On the other hand, consider $g : \mathbb{Z} \to \mathbb{Z}$ given by

$$g(x) = x^2.$$ 

$g(0) = 0$, but this doesn’t mean that $g$ is a homomorphism. In fact,

$$g(1 + 1) = g(2) = 4, \text{ but } g(1) + g(1) = 1 + 1 = 2.$$ 

Since $g(1 + 1) \neq g(1) + g(1)$, $g$ is not a homomorphism.

The point is that simple-looking functions you may have seen in other math classes need not be homomorphisms. When in doubt, check the definition. ⊓⊔

There are several important subsets associated to a group homomorphism $\phi : G \to H$.

**Definition.** Let $\phi : G \to H$ be a group homomorphism.

(a) The **kernel** of $\phi$ is

$$\ker \phi = \{ g \in G \mid \phi(g) = 1 \}.$$ 

(b) The **image** of $\phi$ is (as usual)

$$\im \phi = \{ \phi(g) \mid g \in G \}.$$ 

(c) Let $H' < H$. The **inverse image** of $H'$ is (as usual)

$$\phi^{-1}(H') = \{ g \in G \mid \phi(g) \in H' \}.$$ 

**Warning.** The crummy notation $\phi^{-1}(H')$ does not imply that the inverse of $\phi$ exists. $\phi^{-1}(H')$ is simply the set of inputs which $\phi$ maps into $H'$; this is $\phi^{-1}$ applied to the set $H'$ if there is a $\phi^{-1}$ (but there need not be). ⊓⊔

**Lemma.** Let $\phi : G \to H$ be a group map.

(a) $\ker \phi$ is a subgroup of $G$.

(b) $\im \phi$ is a subgroup of $H$.

(c) If $H'$ is a subgroup of $H$, then $\phi^{-1}(H')$ is a subgroup of $G$.

**Proof.** (a) First,

$$\phi(1) = 1, \text{ so } 1 \in \ker \phi.$$ 

Suppose $g_1, g_2 \in \ker \phi$. Then

$$\phi(g_1 g_2) = \phi(g_1) \phi(g_2) = 1 \cdot 1 = 1.$$ 

Hence, $g_1 g_2 \in \ker \phi$.

Finally, suppose $g \in \ker \phi$. Then

$$\phi(g^{-1}) = \phi(g)^{-1} = 1^{-1} = 1.$$ 

Hence, $g^{-1} \in \ker \phi$. Therefore, $\ker \phi$ is a subgroup of $G$.

(b) Since $\phi(1) = 1$, $1 \in \im \phi$. 

\[5\]
Suppose \( \phi(g_1), \phi(g_2) \in \text{im} \phi \). Then
\[
\phi(g_1)\phi(g_2) = \phi(g_1g_2) \in \text{im} \phi.
\]

Finally, suppose \( \phi(g) \in \text{im} \phi \). Then
\[
\phi(g)^{-1} = \phi(g^{-1}) \in \text{im} \phi.
\]

Therefore, \( \text{im} \phi \) is a subgroup of \( H \). \( \Box \)

(c) Let \( H' \) be a subgroup of \( H \). I want to show that \( \phi^{-1} \) is a subgroup of \( G \). Reminder: The criterion for membership in \( \phi^{-1}(H') \) is that \( \phi \) takes the element into \( H' \).

Since \( 1 \in H' \) and \( \phi(1) = 1 \), it follows that \( 1 \in \phi^{-1}(H') \).

Suppose \( g_1, g_2 \in \phi^{-1}(H') \). This means that \( \phi(g_1) \) and \( \phi(g_2) \) are in \( H' \). Since \( H' \) is a subgroup, \( \phi(g_1)\phi(g_2) \) is in \( H' \) as well. But
\[
\phi(g_1)\phi(g_2) = \phi(g_1g_2).
\]

Therefore, \( \phi(g_1g_2) \) is in \( H' \), which means that \( g_1g_2 \in \phi^{-1}(H') \).

Finally, suppose \( g \in \phi^{-1}(H') \), so \( \phi(g) \in H' \). Since \( H' \) is a subgroup, \( \phi(g)^{-1} \in H' \). But \( \phi(g)^{-1} = \phi(g^{-1}) \), so \( g^{-1} \in H' \). This means that \( g^{-1} \in H' \).

Hence, \( \phi^{-1}(H') \) is a subgroup of \( G \). \( \Box \)

**Example. (A bijective group map)** For the homomorphism \( \exp: \mathbb{R} \to \mathbb{R}^+ \), \( \text{im} \exp = \mathbb{R}^+ \) and \( \ker \exp = \{0\} \). In fact, this map is bijective; the inverse is \( \ln: \mathbb{R}^+ \to \mathbb{R} \). \( \Box \)

**Example. (Finding the kernel and image)** Let
\[
S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}.
\]

Make \( S^1 \) into a group under multiplication of complex numbers. Each element \( z \in S^1 \) can be uniquely written in the form
\[
z = e^{2\pi it} = \cos 2\pi t + i \sin 2\pi t, \quad 0 \leq t < 1.
\]

The identity element is 1; the inverse of \( e^{2\pi it} \) is \( e^{-2\pi it} \).

Define \( \phi: \mathbb{R} \to S^1 \) by
\[
\phi(t) = e^{2\pi it}.
\]

By the remarks above, \( \text{im} \phi = S^1 \). To see that \( \phi \) is a homomorphism, note that
\[
\phi(s+t) = e^{2\pi i(s+t)} = e^{2\pi is}e^{2\pi it} = \phi(s)\phi(t).
\]

The kernel of \( \phi \) is
\[
\ker \phi = \{ t \in \mathbb{R} \mid e^{2\pi it} = 1 \}.
\]

Using \( e^{it} = \cos t + i \sin t \), you can see that \( \ker \phi = \mathbb{Z} \). \( \Box \)

**Definition.** Let \( G \) and \( H \) be groups. An **isomorphism** from \( G \) to \( H \) is a bijective homomorphism \( \phi: G \to H \). If there is an isomorphism \( \phi: G \to H \), \( G \) and \( H \) are **isomorphic**; notation: \( G \approx H \).

**Remarks.**

1. To say that two groups are isomorphic is to say that they are the same as groups. The elements of the two groups and the group operations may be different, but the two groups have the same structure. This means that if one has a certain group-theoretic property, the other will as well.
What is a group-theoretic property? A precise definition would be circular: a group-theoretic property is a property preserved by isomorphism. For this to be a useful concept, I’ll have to provide specific examples of properties that you can check.

2. Some older books define an isomorphism from $G$ to $H$ to be an injective homomorphism $\phi : G \to H$. That is, $\phi$ need not map $G$ onto $H$. One then says $G$ and $H$ are isomorphic if there is an isomorphism from $G$ onto $H$. Unfortunately, one then has the odd situation that there may be an isomorphism from $G$ to $H$, yet $G$ and $H$ may not be isomorphic! I’ll always use the word isomorphism to mean a bijective map.

Here is an easy way to tell that a group map is an isomorphism.

**Lemma.** A group map $\phi : G \to H$ is an isomorphism if and only if it is invertible. In this case, $\phi^{-1}$ is also a homomorphism, hence an isomorphism.

**Proof.** The first statement is trivial, since a map of sets is bijective if and only if it has an inverse.

Now suppose that $\phi : G \to H$ is an isomorphism. I must show the inverse $\phi^{-1} : H \to G$ is a homomorphism. Let $h_1, h_2 \in H$. I need to show that

$$\phi^{-1}(h_1 h_2) = \phi^{-1}(h_1) \phi^{-1}(h_2).$$

Since $\phi : G \to H$ is onto, there exist $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Then

$$\phi^{-1}(h_1 h_2) = \phi^{-1}(\phi(g_1) \phi(g_2)) = \phi^{-1}(\phi(g_1 g_2)) = g_1 g_2 = \phi^{-1}(h_1) \phi^{-1}(h_2).$$

Therefore, $\phi^{-1}$ is a homomorphism.

Since $\phi^{-1}$ is invertible — its inverse is $\phi$ — it is an isomorphism by the first part of the lemma. $\square$

**Example.** (A group isomorphism) Consider the exponential map $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ given by $\exp(x) = e^x$. By an earlier example, $\exp$ is a homomorphism from the reals under addition to the positive reals under multiplication.

The natural logarithm $\ln : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ inverts $\exp$:

$$\ln e^x = x, \quad e^{\ln y} = y \quad \text{for} \quad x \in \mathbb{R}, y \in \mathbb{R}^+. $$

By the lemma, $\exp$ is an isomorphism (as is $\ln$). The groups $(\mathbb{R}, +)$ and $\mathbb{R}^+$ are isomorphic. $\square$

**Example.** (A group isomorphism on the integers mod 2) Consider the set $G = \{-1, 1\}$. Make $G$ into a group using multiplication as the group operation.

Define a map $\phi : \mathbb{Z}_2 \to G$ by

$$\phi(0) = 1, \quad \phi(1) = -1.$$ 

Clearly, $\phi$ is invertible: Its inverse is

$$\phi^{-1}(1) = 0, \quad \phi^{-1}(-1) = 1.$$ 

I’ll show $\phi$ is a homomorphism, hence an isomorphism, by simply checking cases:

<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$\phi(a + b)$</th>
<th>$\phi(a) \phi(b)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1 \cdot 1 = 1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>1 \cdot (-1) = -1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>(-1) \cdot 1 = -1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>(-1) \cdot (-1) = 1</td>
</tr>
</tbody>
</table>
The brute force approach above can be used to construct an isomorphism from $\mathbb{Z}_2$ to any group of order 2. There is only one group of order 2, up to isomorphism.

What does it mean to say that isomorphic groups have the same group-theoretic properties? Here are some examples.

**Proposition.** Suppose $G$ and $H$ are isomorphic groups. If $G$ is abelian, so is $H$.

**Proof.** Let $h_1, h_2 \in H$. I must show that $h_1 h_2 = h_2 h_1$. Since $\phi$ is onto, there exist $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Then

$$h_1 h_2 = \phi(g_1) \phi(g_2) = \phi(g_1 g_2) = \phi(g_2 g_1) = \phi(g_2) \phi(g_1) = h_2 h_1.$$  

Therefore, $H$ is abelian.

**Example.** (Non-isomorphic groups) $S_3$ and $\mathbb{Z}_6$ are both groups of order 6. However, $\mathbb{Z}_6$ is abelian, while $S_3$ is nonabelian. Therefore, $S_3$ and $\mathbb{Z}_6$ are not isomorphic.

**Proposition.** Suppose $G$ and $H$ are isomorphic groups. If $G$ is finite, so is $H$. If $G$ is infinite, so is $H$. (More specifically, isomorphic groups have the same cardinality.

**Proof.** This is trivial, since $\phi$ puts $G$ and $H$ in 1-1 correspondence.

**Example.** (Groups of different cardinality aren’t isomorphic) $\mathbb{Z}$ and $\mathbb{R}$ cannot be isomorphic, since the integers are countable, while the reals are uncountable.

Note that two groups with the same order are not necessarily isomorphic. In the previous example, I showed that $S_3$ and $\mathbb{Z}_6$ are not isomorphic, even though both of them have order 6.

**Proposition.** Suppose $G$ and $H$ are isomorphic groups. If $G$ has a subgroup $K$ of order 42, so does $H$.

**Proof.** If $K < G$ and $|K| = 42$, then $\phi(K) < H$ and (since $\phi$ maps $K$ bijectively onto $\phi(K)$) $|\phi(K)| = 42$.

Obviously, there’s nothing special about “42”. If $G$ has a subgroup of order 117, so does $H$. If $G$ has a subgroup of order 91, so does $H$. And so on. This proposition is not very useful as is, and is just here to show you a property shared by isomorphic groups.

There are infinitely many properties that will be shared by isomorphic groups. In fact, you might say that a group-theoretic property is one that is necessarily shared by isomorphic groups.

However, the earlier examples show that some properties are not shared by isomorphic groups. For example, the elements of one group may be letters, while the elements of the other are numbers. “Having the same kind of elements” is not a group-theoretic property. Likewise, the operation in one group may be addition of numbers, while the operation in the other could be composition of functions. “Having the same kind of binary operation” is not a group-theoretic property.

**Example.** (Showing groups aren’t isomorphic by considering orders of elements) $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are not isomorphic. Both groups have 4 elements; however, every element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 1 or 2, while $\mathbb{Z}_4$ has two elements of order 4 (namely 1 and 3).
Having different numbers of elements of a given order is a group property. Since these groups differ in this respect, they aren’t isomorphic.

Similarly, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_8$ are all abelian groups of order 8. Look at the orders of the elements.

Every element of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has order 1 or 2. For if $(x, y, z) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, then

$$2 \cdot (x, y, z) = (2x, 2y, 2z) = (0, 0, 0).$$

Therefore, the order of $(x, y, z)$ divides 2, and the only positive divisors of 2 are 1 and 2. Every element of $\mathbb{Z}_2 \times \mathbb{Z}_4$ has order 1, 2, or 4. For if $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_4$, then

$$4 \cdot (x, y) = (4x, 4y) = (0, 0).$$

Therefore, the order of $(x, y)$ divides 4, and the only positive divisors of 2 are 1, 2, and 4. Note that $(0, 1)$ is an element of order 4. This means that $\mathbb{Z}_2 \times \mathbb{Z}_4$ can’t be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, since the latter has no elements of order 4.

$\mathbb{Z}_8$ has elements of order 8. (1 has order 8, for example.) Therefore, it can’t be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ or to $\mathbb{Z}_2 \times \mathbb{Z}_4$, since these two groups have no elements of order 8.

Therefore, the three groups aren’t isomorphic. □