Math 403 Chapter 6: Isomorphisms

1. **Introduction:** Consider the group $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and the group $U(10) = \{1, 3, 7, 9\}$. If we write down a Cayley table for each we get the following. In the $U(10)$ case the positions of the 9 and 7 have been switched and we will see why soon.

$\mathbb{Z}_4$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$U(10)$

$\cdot$	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

If we look closely at these two tables we might see that structurally they're exacly the same under the correspondance:

$\mathbb{Z}_4$	$\leftrightarrow$	$U(10)$
0	$\leftrightarrow$	1
1	$\leftrightarrow$	3
2	$\leftrightarrow$	9
3	$\leftrightarrow$	7

This means that calculations on one side match calculations on the other:

$\mathbb{Z}_4$	$\leftrightarrow$	$U(10)$
$2 + 3 = 1$	$\leftrightarrow$	$9 \cdot 7 = 3$
$1 + 3 = 0$	$\leftrightarrow$	$3 \cdot 7 = 9$

Also subgroups one one side match subgroups on the other:

$\mathbb{Z}_4$	$\leftrightarrow$	$U(10)$
$\{0, 2\} \leq \mathbb{Z}_4$	$\leftrightarrow$	$\{1, 9\} \leq U(10)$

As do orders:

$\mathbb{Z}_4$	$\leftrightarrow$	$U(10)$
$\lvert 2 \rvert = 2$	$\leftrightarrow$	$\lvert 9 \rvert = 2$

2. **Definition:** Given groups $(G, *_G)$ and $(H, *_H)$ we say that an *isomorphism* from G to H is a mapping $\phi : G \to H$ which is 1-1 and onto with:

$$\forall g_1, g_2 \in G \text{ we have } \phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2)$$

The use of $*_G$ and $*_H$ is to emphasize that the operation on the left takes place in G whereas the operation on the right takes place in H. Typically we'll just write:

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$$

With the understanding that $g_1 g_2$ is in G with G's operation because $g_1, g_2 \in G$ whereas $\phi(g_1)\phi(g_2)$ is in H with H's operation because $\phi(g_1), \phi(g_2) \in H$.

If an isomorphism exists then we say the groups are *isomorphic* and write $G \approx H$.

3. **Examples and Notes:**

   (a) The mapping $\phi : \mathbb{Z}_4 \to U(10)$ given by $\phi(0) = 1$, $\phi(1) = 3$, $\phi(2) = 9$ and $\phi(3) = 7$ is an isomorphism as the table suggests. Thus $\mathbb{Z}_4 \approx U(10)$.

   (b) We see that $\mathbb{Z} \approx 2\mathbb{Z}$ with the isomorphism $\phi(n) = 2n$.
   To see that ϕ is onto take $2a \in 2\mathbb{Z}$ and observe that $\phi(a) = 2a$. To see that ϕ is 1-1 suppose $\phi(a) = \phi(b)$ and then $2a = 2b$ so $a = b$. Then note that for any $a, b \in \mathbb{Z}$ we have:

$$\phi(a + b) = 2(a + b) = 2a + 2b = \phi(a) + \phi(b)$$

   (c) We see that $(\mathbb{R}^+, \cdot) \approx (\mathbb{R}, +)$ with the isomorphism $\phi(x) = \log(x)$.
   To see that ϕ is onto take $y \in \mathbb{R}$ and put $x = 10^y \in \mathbb{R}^+$ and observe that $\phi(x) = \phi(10^y) = \log(10^y) = y$. To see that ϕ is 1-1 suppose $\phi(x_1) = \phi(x_2)$ and then $\log(x_1) = \log(x_2)$ so $x_1 = x_2$. Then note that for any $x, y \in \mathbb{R}^+$ we have:

$$\phi(xy) = \log(xy) = \log(x) + \log(y) = \phi(x) + \phi(y)$$

   Note the different operations in each group.

   (d) Any two cyclic groups of order n are isomorphic.
   To see this let $G = \langle g \rangle = \{e = g^0, g, ..., g^{n-1}\}$ and $H = \langle h \rangle = \{e = h^0, h, ..., h^{n-1}\}$. Then we can define $\phi(g^k) = h^k$ for each $g^k \in \langle g \rangle$. To see that ϕ is onto take any element in $\langle h \rangle$ which has the form h^k for some $0 \leq k < n$ and observe that $\phi(g^k) = h^k$. To see that ϕ is 1-1 suppose $\phi(g^j) = \phi(g^k)$ and then $h^j = h^k$ and since $0 \leq j < n$ and $0 \leq k < n$ we have $j = k$ and so $g^j = g^k$. Then note that for any $g^j, g^k \in \langle g \rangle$ we have:

$$\phi(g^j g^k) = \phi(g^{j+k}) = h^{j+k} = h^j h^k = \phi(g^j)\phi(g^k)$$

   (e) Note that in rare cases you may define a function which isn't well-defined (and hence not really a function). For example if you tried to do $\phi : \mathbb{Z}_5 \to \mathbb{Z}_7$ with $\phi(n) = n$ you would have $\phi(0) = 0$ but also $\phi(0) = \phi(5) = 5$ so one elemement is mapping to two. This is less of an issue with isomorphism than with functions, though.

   (f) Note that the requirement that ϕ be 1-1 and onto are critical, otherwise $\phi : \mathbb{Z} \to \mathbb{Z}$ given by $\phi(n) = 0$ would certainly satisfy $\phi(a + b) = \phi(a) + \phi(b)$.

   (g) Proving that two groups are not isomorphic might seem challenging. If they have different orders then it's obvious since no ϕ could be 1-1 and onto. However if they have the same order how could we possibly show that no ϕ at all could have the desired property? We'll see that this is usually done by resorting to properties that must appear under an isomorphism and showing that one of those properties does not.

4. **Theorem (The Inverse of an Isomorphism):** Since $\phi : G \to H$ is a 1-1 and onto mapping we may define $\phi^{-1} : H \to G$ which is also 1-1 and onto by putting $\phi^{-1}(h) = g$ where $\phi(g) = h$. Then ϕ^{-1} is an isomorphism from H to G.
   Proof: The fact that ϕ^{-1} may be defined and is 1-1 and onto is clear. Observe that for $h_1, h_2 \in H$ we can find $g_1, g_2 \in G$ with $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$ and hence $\phi^{-1}(h_1) = g_1$ and $\phi^{-1}(h_2) = g_2$ and then we have

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

5. **Theorem (Properties of Isomorphisms on Elements):** Suppose $\phi : G \to H$ is an isomorphism. Then we have:

   (a) $\phi(g^k) = \phi(g)^k$
   Proof: Follows immediately from the definition of an isomorphism.

   (b) $\phi(e) = e$
   Proof: $\phi(e) = \phi(ee) = \phi(e)\phi(e)$ and cancel one of the $\phi(e)$.

   (c) $\phi(g^{-1}) = \phi(g)^{-1}$
   Proof: We have $e = \phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$ and left-multiply both sides by $\phi(g)^{-1}$.

   (d) For all $g \in G$ we have $|g| = |\phi(g)|$. As a consequence G and H must have the same number of elements of each order.
   Proof: Observe that $g^n = e$ iff $\phi(g^n) = \phi(e)$ iff $\phi(g)^n = e$ and the result follows immediately.

   (e) For all $g_1, g_2 \in G$ we have $g_1g_2 = g_2g_1$ iff $\phi(g_1)\phi(g_2) = \phi(g_2)\phi(g_1)$.
   Proof: Follows immediately from the definition of an isomorphism.

   (f) For $g \in G$ we have $G = \langle g \rangle$ iff $H = \langle \phi(g) \rangle$.
   Proof: Forward direction: If $G = \langle g \rangle$ we claim $H = \langle \phi(g) \rangle$. Let $h \in H$. Since ϕ is onto and $G = \langle g \rangle$ there is some $g^k \in G$ with $\phi(g^k) = h$ and then $h = \phi(g^k) = \phi(g)^k \in \langle \phi(g) \rangle$.
   Backward direction: Try it!

   Here are some examples which use this theorem:

   (a) **Example:** $\mathbb{Z}_4 \not\approx U(8)$ because $U(8)$ has three elements of order 2 but $\mathbb{Z}_4$ has only one element of order 2.

6. **Theorem (Properties of Isomorphisms on the Group and on Subgroups):** Suppose $\phi : G \to H$ is an isomorphism. Then we have:

   (a) $|G| = |H|$.
   Proof: This follows from the fact that an isomorphism must be 1-1 and onto.

   (b) G is cyclic iff H is cyclic.
   Proof: Follows from the previous theorem.

   (c) G is Abelian iff H is Abelian.
   Proof: Forward direction: Suppose G is Abelian. Let $h_1, h_2 \in H$. Then $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$ for some $g_1, g_2 \in G$. Then $h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2) = \phi(g_2g_1) = \phi(g_2)\phi(g_1) = h_2h_1$.
   Backward direction: Try it!

   (d) If $G' \leq G$ then $\phi(G') \leq H$.
   Proof: We use the one-step subgroup test. Suppose $h_1, h_2 \in \phi(G')$, then $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$ for some $g_1, g_2 \in G$. Then $h_1h_2^{-1} = \phi(g_1)\phi(g_2)^{-1} = \phi(g_1g_2^{-1}) \in \phi(G')$.

   (e) If $H' \leq H$ then $\phi^{-1}(H') \leq G$.
   Proof: Follows immediately from the previous with ϕ^{-1} in place of ϕ. Note: As a consequence G and H must have the same number of subgroups of each order.

   (f) We have $\phi(Z(G)) = Z(\phi(G))$.
   Proof: First we show $\phi(Z(G)) \subseteq Z(\phi(G))$. Suppose $g \in Z(G)$. We claim $\phi(g) \in Z(\phi(G))$. Given $\phi(x) \in \phi(G)$ observe that $\phi(x)\phi(g) = \phi(xg) = \phi(gx) = \phi(g)\phi(x)$. Showing the reverse subset direction is similar, using ϕ^{-1}.

Here are some examples which use this theorem:

(a) **Example:** $D_4 \not\cong S_4$ because $|D_4| = 8$ and $|S_4| = 24$.

(b) **Example:** $\mathbb{Z}_{24} \not\cong S_4$ because $\mathbb{Z}_{24}$ is Abelian but S_4 is not.

(c) **Example:** If $|G| = 100$ and G has two distinct subgroups of order 25 then G is not cyclic since a cyclic group of order 100 has a unique subgroup of order 25.

7. **Definition:** An *automorphism* of a group G is an isomorphism $\phi : G \to G$.

Example: If G is a cyclic group then an automorphism ϕ of G can be completely determined by choosing a generator of G and seeing where ϕ takes it. This is because once we know where that generator goes we know where every element goes. However a generator must map to a generator or else the mapping will not be 1-1. For example consider an automorphism of $\mathbb{Z}_{10}$. We know $\phi(0) = 0$ because it's the identity. If we look at the generator 1 we can choose to map this to $1, 3, 7, 9$ since those are the other generators. Once the choice is made then everything else follows. For example suppose we choose $\phi(1) = 3$. Then automatically we get:

$$\begin{aligned}
\phi(2) &= \phi(1+1) = 3+3 = 6 \\
\phi(3) &= \phi(1+1+1) = 3+3+3 = 9 \\
\phi(4) &= \phi(1+1+1) = 3+3+3+3 = 12 = 2 \\
\phi(5) &= ... = 15 = 5 \\
\phi(6) &= ... = 18 = 8 \\
\phi(7) &= ... = 21 = 1 \\
\phi(8) &= ... = 24 = 4 \\
\phi(9) &= ... = 27 = 7
\end{aligned}$$