Isomorphisms I

We've seen how two unequal (as sets) groups can be "essentially" the same group. For the examples we saw, this meant that the multiplication tables were the same except for the names of the elements.

Here's another example of two unequal yet essentially the same group; this time they are infinite.

Let G be the subgroup of $\mathrm{GL}_2(\mathbb{R})$ consisting of matrices of the type

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \qquad n \in \mathbb{Z}$$

This group is essentially the group $\mathbb{Z}$.

We now need to say precisely what is meant by "essentially the same." We need a functional definition - one that involves functions.

When two groups are essentially the same, that means if one were to rename the elements of the first group with the names of the elements in the second group in a particular way, one would get the same group structure (i.e., multiplication would work the same way).

The "rename" part is simplest to do with functions. If G_1 and G_2 are our groups, the renaming part can be expressed as a one-to-one and onto function $\phi\colon G_1 \to G_2$.

But it isn't just a simple renaming of elements we're after. We need to see the group structure (read: "multiplication table") preserved. That is expressed most simply as

$$\phi(g)\phi(h) = \phi(gh)$$

for all $g, h \in G_1$.

Examples: 1) Define $\phi\colon \mathbb{Z} \to G$ by

$$\phi(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

2) Define $\phi\colon S_3 \to \mathrm{GL}_2(\mathbb{Z}_2)$ by

$$\phi((1,2)) = \begin{pmatrix} [0]_2 & [1]_2 \\ [1]_2 & [0]_2 \end{pmatrix} \qquad \phi((1,2,3)) = \begin{pmatrix} [1]_2 & [1]_2 \\ [1]_2 & [0]_2 \end{pmatrix}$$

Why is this enough information to say what ϕ does to all six elements of S_3?

3) Define $\phi\colon \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ by $\phi([1]_6) = ([1]_2, [1]_3)$, and more generally

$$\phi(n[1]_6) = n([1]_2, [1]_3).$$

4) (The dorky example) The identity function on any group G is an isomorphism: $id\colon G \to G$.

(An isomorphism from a group to itself is called an *automorphism*.)

Two very simple properties of isomorphisms are:

Lemma 1: Suppose $\phi\colon G_1 \to G_2$ is an isomorphism. If $e \in G_1$ is the identity in G_1, then $\phi(e)$ is the identity in G_2. Also, for any $a \in G_1$,

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

Proof: Suppose e is the identity of G. Then since ϕ is an isomorphism,

$$\phi(e)\phi(e) = \phi(ee) = \phi(e).$$

By an earlier exercise, this implies that $\phi(e)$ is the identity in G_2.

Suppose $a \in G$. Since ϕ is an isomorphism,

$$\phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$$

and similarly

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

Since $\phi(e)$ is the identity in G_2, this implies that $\phi(a^{-1}) = \big(\phi(a)\big)^{-1}$. (Note how we never used the fact that ϕ is one-to-one and onto!)

Another simple yet important property of isomorphisms is

Lemma 2: Suppose $\phi\colon G_1 \to G_2$ is an isomorphism. Then there is an inverse function $\phi^{-1}\colon G_2 \to G_1$, and this is also an isomorphism.

Proof: Suppose $g, h \in G_2$. Since ϕ is one-to-one and onto, there are unique $a, b \in G_1$ with $\phi(a) = g$ and $\phi(b) = h$. This means that $\phi^{-1}(g) = a$ and $\phi^{-1}(h) = b$. Since ϕ is an isomorphism, $\phi(ab) = \phi(a)\phi(b) = gh$. This means that $\phi^{-1}(gh) = ab$. Thus,

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