15. Isomorphisms (continued)

We start by recalling the notions of an isomorphism between groups and the notion of isomorphic groups.

Definition. *Let G and G' be groups.*

(a) *A map $\varphi : G \to G'$ is called an isomorphism if*
   (i) *φ is bijective*
   (ii) *φ preserves group operation: $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in G$*

(b) *We say that G is isomorphic to G' if there exists an isomorphism $\varphi : G \to G'$. We write $G \cong G'$ if G is isomorphic to G'.*

The following result is left as a practice homework problem.

Claim 15.1. *The relation $\cong$ is an equivalence relation. In other words,*

(a) *(reflexivity) Any group G is isomorphic to itself: $G \cong G$ for any group G*
(b) *(symmetry) If G is isomorphic to G', then G' is isomorphic to G*
(c) *(transitivity) If G is isomorphic to G' and G' is isomorphic to G'', then G is isomorphic to G''.*

Since the relation $\cong$ is symmetric, we can safely use terminology "G and G' are isomorphic (to each other)" without worrying which of the two groups come first and which comes second.

Let us now look at some examples of isomorphisms.

Example 1. *Any two cyclic groups of the same order are isomorphic.*

We will prove this result for finite cyclic groups. The proof for infinite cyclic groups is similar (and actually easier). Since $(\mathbb{Z}_n, +)$ is a cyclic group of order n, by transitivity (Claim 15.1(c)) it suffices to prove the following theorem:

Theorem 15.2. *Let G be a finite cyclic group of order n. Then G is isomorphic to $(\mathbb{Z}_n, +)$*

Proof. Let x be a generator of G. By Theorem 13.1 we know that $G = \{e, x, \ldots, x^{n-1}\}$ and $x^n = e$. Define the map $\varphi : \mathbb{Z}_n \to G$ by setting

$$\varphi([i]) = x^i \text{ for all } i \in \mathbb{Z}.$$

We claim that φ is an isomorphism.

First we need to check that φ is well-defined, that is, if $[i] = [j]$, then $x^i = x^j$. So suppose that $[i] = [j]$ for some $i, j \in \mathbb{Z}$. This means that $j = i + nk$ for some $k \in \mathbb{Z}$, whence $x^j = x^{i+nk} = x^i x^{nk} = x^i (x^n)^k = x^i e^k = x^i$.

To prove that φ is an isomorphism, we need to show that it is bijective and that it preserves group operation. Bijectivity in this example is clear from the definition: indeed, we know that $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ and $G = \{e, x, \ldots, x^{n-1}\}$ (both lists without repetitions) and φ maps $[0]$ to $e = x^0$, $[1]$ to x^1 etc., so it is both injective and surjective.

$$\begin{array}{cccccccc}
\mathbb{Z}_n & = \{ & [0], & [1], & \ldots & [n-1] & \} \\
 & & \downarrow & \downarrow & \cdots & \downarrow & \\
G & = \{ & e, & x, & \ldots & x^{n-1} & \}
\end{array}$$

Since group operation in $\mathbb{Z}_n$ is addition, the condition that φ preserves group operation in this example should be rewritten as

$$\varphi([i] + [j]) = \varphi([i])\varphi([j]).$$

We shall compute both sides and see that they are equal. We have

$\varphi([i] + [j]) = \varphi([i + j]) = x^{i+j}$ (where the first equality holds by definition of group operation in $\mathbb{Z}_n$) while $\varphi([i])\varphi([j]) = x^i x^j = x^{i+j}$ (where the second equality holds by exponent laws). Thus, $\varphi([i] + [j]) = \varphi([i])\varphi([j])$, as desired. □

Example 2. *Let $G = (\mathbb{R}, +)$ (reals with addition) and $G' = (\mathbb{R}_{>0}, \cdot)$ (positive reals with multiplication). Then G and G' are isomorphic.*

By definition, we need to find a bijective map $\varphi : G \to G'$ such that $\varphi(x + y) = \varphi(x)\varphi(y)$ for all $x, y \in \mathbb{R}$. We let φ be the exponential function ($\varphi(x) = e^x$). The fact that this φ has required properties is a fact from analysis (so we omit the formal proof here).

In the first two examples our goal was to show that two given groups are isomorphic. In the following example we consider certain map φ from some group G to itself and show that φ is an isomorphism. Of course, the point here is not to show that G is isomorphic to itself (for which we could just use the identity map). Nevertheless, the result of this example is useful, as we will see later.

Example 3. *Let G be any group, fix $g \in G$, and define $\varphi : G \to G$ by $\varphi(x) = gxg^{-1}$ for all $x \in G$. Then φ is an isomorphism (from G to itself).*

Proof. First we check that φ respects group operation:

$$\varphi(x)\varphi(y) = (gxg^{-1})(gyg^{-1}) = gx(gg^{-1})yg^{-1} = gxyg^{-1} = \varphi(xy).$$

To prove bijectivity of φ, we can do either of the following:

(i) show that φ is injective and surjective

(ii) find the inverse function $\psi : G \to G$, that is, a function $\psi : G \to G$ such that $\psi(\varphi(x)) = x$ for all $x \in G$ and also $\varphi(\psi(x)) = x$ for all $x \in G$.

We will use method (ii) below. Looking at the formula for φ, it is not difficult to guess that the inverse map ψ should be given by $\psi(x) = g^{-1}xg$. Now we formally verify that ψ defined in this way is indeed the inverse: $\psi(\varphi(x)) = \psi(gxg^{-1}) = g^{-1}(gxg^{-1})g = g^{-1}gxg^{-1}g = x$ and similarly $\varphi(\psi(x)) = \varphi(g^{-1}xg) = g(g^{-1}xg)g^{-1} = gg^{-1}xgg^{-1} = x$. □

Let us now discuss how to prove that two given groups are not isomorphic. Doing this directly from definition is usually impossible (one cannot go over all possible maps between groups and show directly that none of them can be both bijective and operation-preserving). Of course, two groups cannot be isomorphic if they have different orders. If two groups G and G' have the same order, but we suspect that they are not isomorphic, a standard way to proceed is to try to find certain group-theoretic property (P) which is preserved under isomorphisms and such that G has property (P) while G' does not (or vice versa).

The following result which will be included in HW#7 turns out particularly useful in this context:

Proposition 15.3 (Isomorphisms preserve orders of elements)**.** *Let G and G' be groups and let $\varphi : G \to G'$ be an isomorphism. Then $o(g) = o(\varphi(g))$ for all $g \in G$.*

As an immediate consequence of this proposition, we find a sufficient condition for two groups to be NON-isomorphic.

Corollary 15.4. *Let G and G' be groups, and suppose there exists $k \in \mathbb{N}$ such that G has an element of order k while G' has no element of order k. Then G and G' are not isomorphic.*

Example 4. *Let $G = (\mathbb{R}, +)$ and $H = (\mathbb{R} \setminus \{0\}, \cdot)$ (nonzero reals with multiplication). Then G and H are not isomorphic.*

Proof. Note that the group H has an element of order 2, namely -1 since $-1 \neq 1$, but $(-1)^2 = 1$. On the other hand, G has no element of order 2: if $x \in G = \mathbb{R}$ is an element of order 2, we would have $x \neq 0$, but $2x = 0$ (recall that operation in G is addition) which cannot happen in real numbers. Thus, applying Corollary 15.4 with $k = 2$, we conclude that G and H are not isomorphic. □