More isomorphisms, and kernels

In this lecture we continue our study of homomorphisms and isomorphisms and also introduce the important notion of the *kernel* of an homomorphism.

Recall that an isomorphism is a 1-1 and onto homomorphism $\phi : G \to G'$. The homomorphism property says that $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$. Define a relation on groups: write $G \cong G'$ if there is an isomorphism $\phi : G \to G'$.

▶ **The relation $G \cong G'$ is an equivalence relation on the collection of all groups.**

In proving this we will introduce a number of important properties of isomorphisms.

First, given any group G, consider the map $\phi : G \to G$ given by $\phi(a) = a$, the "identity" homomorphism. This is clearly an isomorphism, so $G \cong G$, i.e. the relation is reflexive. The identity homomorphism is sometimes written $\mathrm{id}_G = \phi : G \to G$.

Next, suppose $G \cong G'$, i.e. there is an isomorphism $\phi : G \to G'$. Consider the inverse map of ϕ, denoted $\phi' : G' \to G$. This is defined as follows. Let $a' \in G'$. We would like to desribe $\phi'(a')$. Because ϕ is onto, there is an $a \in G$ with $\phi(a) = a'$, and this a is unique as ϕ is 1-1. Then we define $\phi'(a')$ by $\phi'(a') = a$. We see that ϕ' is characterized by the relation $\phi'(\phi(a)) = a$ for all $a \in G$. You can check that ϕ' is 1-1 and onto, and also $\phi(\phi'(a')) = a'$ for all $a' \in G'$. Next, given $a', b' \in G'$, let $a, b \in G$ such that $\phi(a) = a'$, $\phi(b) = b'$. Then

$$\phi'(a'b') = \phi'(\phi(a)\phi(b)) = \phi'(\phi(ab)) = ab = \phi'(a')\phi'(b')$$

Therefore $\phi' : G' \to G$ is an isomorphism, and so $G' \cong G$. The map ϕ' is called the *inverse* isomorphism of ϕ. The inverse isomorphism is sometimes written $\phi^{-1} : G' \to G$. This establishes symmetry of the relation $\cong$.

In general, if $\phi : G \to G'$ and $\phi' : G' \to G''$ are homomorphisms, the composition map $\phi' \circ \phi : G \to G''$ is also a homomorphism. Indeed, if $a, b \in G$ then we compute

$$(\phi' \circ \phi)(ab) = \phi'(\phi(ab)) = \phi'(\phi(a)\phi(b)) = \phi'(\phi(a))\phi'(\phi(b)) = (\phi' \circ \phi)(a)(\phi' \circ \phi)(b)$$

If $G \cong G'$ and $G' \cong G''$ by isomorphisms $\phi : G \to G'$ and $\phi' : G' \to G''$ then $\phi' \circ \phi$ is an isomorphism, as you may check. This establishes transitivity. Thus $\cong$ is an equivalence relation.

We say two groups G and G' are *isomorphic* if $G \cong G'$. A useful criterion for $\phi : G \to G'$ to be an isomorphism is as follows.

▶ **Let $\phi : G \to G'$ be a homomorphism. Then ϕ is an isomorphism if and only if there exists a homomorphism $\phi' : G' \to G$ such that**

$$\phi' \circ \phi = \mathrm{id}_G \qquad \text{and} \qquad \phi \circ \phi' = \mathrm{id}_{G'}$$

Indeed if ϕ is an isomorphism, then the inverse isomorphism considered above provides such a map ϕ'. Conversely, if ϕ is a homomorphism and such a ϕ' in the statement exists, let us check that ϕ is 1-1 and onto. First, let $a' \in G'$. Then $a' = (\phi \circ \phi')(a') = \phi(\phi'(a'))$. Thus ϕ is onto. Second, suppose $a, b \in G$ and $\phi(a) = \phi(b)$. Then applying ϕ' we get $a = \phi'(\phi(a)) = \phi'(\phi(b)) = b$ and thus ϕ is 1-1. We conclude that ϕ is an isomorphism.

In fact in the above statement, ϕ' is always uniquely determined as being the inverse isomorphism of ϕ that we considered earlier.

Most of the properties of groups that we are interested in are preserved under isomorphisms.

▶ **Let G and G' be isomorphic groups. Then:**

(i) If G is abelian, then G' is abelian.

(ii) If G is cyclic, then G' is cyclic.

(iii) If G is finite, then so is G' and $|G| = |G'|$.

The verification is left as an exercise.

Let $\phi : G \to G'$ be a homomorphism. We define the *kernel* of ϕ to be

$$\ker(\phi) = \{a \in G : \phi(a) = e'\} \subset G$$

▶ **Let $\phi : G \to G'$ be a homomorphism. Then $\ker(\phi)$ is a normal subgroup of G.**

To see this, first note $\phi(e) = e'$, so $e \in \ker(\phi)$. Next, let $a, b \in \ker(\phi)$. This means $\phi(a) = e'$ and $\phi(b) = e'$ where $e' \in G'$ is the identity. Then

$$\phi(ab) = \phi(a)\phi(b) = e'e' = e'$$

and so $ab \in \ker(\phi)$. Similarly, $\phi(a^{-1}) = \phi(a)^{-1} = (e')^{-1} = e'$ and so $a^{-1} \in \ker(\phi)$. Therefore $\ker(\phi)$ is a subgroup of G. Next, let $a \in \ker(\phi)$, and let $g \in G$ be any element. Then

$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)e'\phi(g)^{-1} = e'$$

This shows $g \cdot \ker(\phi) \cdot g^{-1} \subset \ker(\phi)$. Therefore $\ker(\phi)$ is normal.

The following is a sort of converse to the above result:

▶ **Let G be a group and $N \subset G$ a normal subgroup. Then there is a homomorphism ϕ from G to some other group such that $\ker(\phi) = N$.**

In fact we can take the homomorphism ϕ to be one that we have seen before:

$$\phi : G \to G/N$$

defined by $\phi(a) = aN$ for each $a \in G$. The kernel of this homomorphism is the set of $a \in G$ such that $\phi(a) = N$, i.e. $aN = N$. But these are exactly the a that are in the coset N. Thus $\ker(\phi) = N$. This proves what we claimed.

Finally, the following shows that kernels are useful for understanding isomorphisms.

▶ **An onto homomorphism $\phi : G \to G'$ is an isomorphism if and only if $\ker(\phi) = \{e\}$.**

First, suppose ϕ is an isomorphism. If $a \in \ker(\phi)$ then $\phi(a) = e'$. But $\phi(e) = e'$ also, so $\phi(e) = \phi(a)$ implies $e = a$, as ϕ is 1-1. This shows $\ker(\phi) = \{e\}$.

Conversely, suppose $\ker(\phi) = \{e\}$. We aim to show ϕ is 1-1. Suppose $\phi(a) = \phi(b)$. Then

$$e' = \phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1})$$

and in particular $ab^{-1} \in \ker(\phi)$. Since $\ker(\phi) = \{e\}$ we must have $ab^{-1} = e$, or equivalently $a = b$. Thus ϕ is 1-1. By assumption ϕ is onto, and thus it is an isomorphism.