

Exercise #16 and Homomorphisms

When we first looked at isomorphisms, we proved the following result.

Lemma: Suppose $\phi: G_1 \rightarrow G_2$ is an isomorphism. If $e \in G_1$ is the identity in G_1 , then $\phi(e)$ is the identity in G_2 . For any $a \in G_1$,

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

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 $\phi(a^{-1}) = (\phi(a))^{-1}$. (Note how we never used the fact that ϕ is one-to-one and onto!)

Indeed, we never needed ϕ to be one-to-one or onto for this lemma. We only used the property

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

Now recall the function f from S_n to $\{-1, 1\}$ we constructed when looking at even and odd permutations. We now know that S_n is a group. The image $\{-1, 1\}$ is also a group with the usual multiplication of integers. One of the main points of our construction was showing that

$$f(\sigma \circ \tau) = f(\sigma) \cdot f(\tau)$$

for all permutations $\sigma, \tau \in S_n$. So our function f has that same property.

This property is what preserves the “groupness,” so to speak. In general, we only want to look at functions from one group to another which preserve the “groupness.” But we don’t want to restrict our attention to just one-to-one and onto functions.

Definition: Suppose G_1 and G_2 are groups. A function $\phi: G_1 \rightarrow G_2$ is called a *homomorphism* if

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

for all $a, b \in G$.

Examples: 1) Define $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_2$ by

$$\phi(z) = \begin{cases} [0]_2 & \text{if } z \text{ is even,} \\ [1]_2 & \text{if } z \text{ is odd.} \end{cases}$$

2) More generally, define $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ by $\phi(z) = [z]_n$.

3) Define $\phi: S_n \rightarrow \{-1, 1\}$ by

$$\phi(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

4) Suppose G_1 and G_2 are any two groups. Define $\phi: G_1 \times G_2 \rightarrow G_1$ by $\phi(a, b) = a$.

5) This is a more “generic” example. Suppose $\phi: G_1 \rightarrow G_2$ is a homomorphism and H is a subgroup of G_1 . Then as a function we can restrict ϕ to just H , giving (technically speaking) another homomorphism which takes H into G_2 . A typical notation for this “new” homomorphism is $\phi|_H$.

Definition/Lemma: If $\phi: G_1 \rightarrow G_2$ is a homomorphism, the collection of elements of G_1 which ϕ sends to the identity of G_2 is a subgroup of G_1 ; it is called the *kernel* of ϕ .

Proof: Suppose a and b are elements of G_1 in the kernel of ϕ , in other words,

$$\phi(a) = \phi(b) = e_2,$$

where e_2 is the identity element of G_2 . Then by our first lemma

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} = e_2e_2^{-1} = e_2.$$

So ab^{-1} is also in the kernel. By Corollary 3.2.3, this is enough to show that the kernel is a subgroup.

It's quite handy to know what the kernel of a homomorphism is, since

Lemma: A homomorphism $\phi: G_1 \rightarrow G_2$ is one-to-one if and only if the kernel consists of only the identity element of G_1 .

Proof: Let e_1 be the identity element of G_1 and let e_2 be the identity element of G_2 .

Suppose ϕ is one-to-one. By our first lemma we know that e_1 is definitely in the kernel; $\phi(e_1) = e_2$. Since ϕ is one-to-one, no other element $a \in G$ has $\phi(a) = e_2$. Thus, the kernel of ϕ is just $\{e_1\}$.

Suppose now that the kernel of ϕ is just $\{e_1\}$. If $a, b \in G$ and $\phi(a) = \phi(b)$, then

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} = \phi(a)(\phi(a))^{-1} = e_2.$$

This means that ab^{-1} is in the kernel, so $ab^{-1} = e_1$ and $a = b$. Thus, ϕ is one-to-one.

An application of this stuff is a proof for exercise #16 from section 3.6. We start with the homomorphism $f: S_n \rightarrow \{-1, 1\}$. The kernel of f is the subgroup of even permutations of S_n , A_n . If H is any subgroup of S_n , we can restrict f to H and the kernel will now be the subgroup of H consisting of all even permutations in H .