NORMAL SUBGROUPS AND HOMOMORPHISMS

$$f(xy) = f(x)\,f(y)$$

Previously, we talked about what it means for two groups to be isomorphic, and we explained that this means that they have the same structure and essentially are identical except for whatever labels are used to describe the elements. We now want to look at a slightly more general concept, that of two groups being *homomorphic*.

The word *homomorphic* means "same shape," and so let's discuss what we mean when we say that two groups, G_1 and G_2, have the same shape. If we are going to say that these two groups have the same shape, then we need some sort of connection between them, and, of course, the way in which we connect two sets in mathematics is with a function. Thus, let's assume that we have a function from G_1 onto G_2, $f : G_1 \to G_2$. Recall that the word "onto" in math simply means that G_2 is the entire range of our function. Thus, for any $y \in G_2$, there exists an $x \in G_1$ such that $f(x) = y$.

At this point, let's reminds ourselves that groups are not merely sets, they are sets with binary operations defined on them. That is, in each set we have a way of combining two elements to get a third element. And now, using the multiplication defined within each group, we can explain what we mean when we say that the two groups have the same shape. By this we mean that not only do we have a function *f* from G_1 onto G_2, but it is also the case that if in G_1 we have that $ab = c$, then in G_2 we will have that $f(a)f(b) = f(c)$. This means that multiplication in one group will correspond to multiplication in the other group. Also, another way to write this last equation is as $f(a)f(b) = f(ab)$ or $f(ab) = f(a)f(b)$, and any function *f* from G_1 onto G_2 with this kind of property is what we call a *homormorphism*.

There are several easy theorems to prove about homomorphisms, and I'll start with one that shows that a homormorphism takes the identity element in one group to the identity element in the other group.

Theorem: Let $f : G_1 \to G_2$ be a homomorphism from G_1 onto G_2, and suppose e_1 is the identity element in G_1 and e_2 is the identity element in G_2. Then $f(e_1) = e_2$.

Proof: Let $a \in G_1$. Then $a = ae_1$. Hence, $f(a) = f(ae_1) = f(a)f(e_1)$. From this we can conclude that $f(a)^{-1} f(a) = f(a)^{-1} f(a) f(e_1) \Rightarrow e_2 = e_2 f(e_1) \Rightarrow e_2 = f(e_1)$. □

Another fact that is easy to prove about homomorphisms is that they take the inverse in one group to the inverse in the other group. In other words, $f(a^{-1}) = f(a)^{-1}$. This is easy to prove, but for now we'll just assume it's true so that we can get on with showing you why normal subgroups are so important and, also, what they have to do with homomorphisms. We'll begin with the following definition.

Definition: If $f : G_1 \to G_2$ is a homomorphism from G_1 onto G_2, then the *kernel* of the homomorphism is the set of all elements that get sent to e_2 (the identity in G_2) by the homomorphism.

This next theorem is one that I'm going to prove just for finite groups even though it is actually true for all groups. I'll let you extend the result to all groups as an exercise.

Theorem: Let G_1 and G_2 be finite groups, let $f : G_1 \to G_2$ be a homomorphism from G_1 onto G_2, and let $K = \{x \in G_1 \mid f(x) = e_2\}$. Then K is a subgroup of G_1.

Proof: Since we are assuming that our groups are finite, to show that K is a subgroup of G_1 requires us only to show that K is closed under multiplication. Thus, suppose $x, y \in K$. Then $f(xy) = f(x)f(y) = e_2 e_2 = e_2$, the identity element in G_2. Therefore, $xy \in K$ and K is a subgroup of G_1 since K is closed under multiplication. □

Now that we know that the kernel of a homomorphism is a subgroup of our group, we're next going to show that it is a normal subgroup. Recall that this means that for any $a \in G_1$, we have that $aKa^{-1} = K$. Also, at this point we'll drop the requirement that our groups be finite as we'll assume that you either have or soon will have taken time to extend the result of the previous theorem.

Theorem: Let G_1 and G_2 be groups, let $f : G_1 \to G_2$ be a homomorphism from G_1 onto G_2, and let $K = \{x \in G_1 \mid f(x) = e_2\}$. Then K is a normal subgroup of G_1.

Proof: To prove this, it will suffice to show that if $a \in G_1$ and $x \in K$, then $axa^{-1} \in K$. However, this should be a very obvious fact to us at this point since $f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)f(x)f(a)^{-1} = f(a)e_2 f(a)^{-1} = f(a)f(a)^{-1} = e_2$. Therefore, $axa^{-1} \in K$ and K is a normal subgroup of G_1, $K \triangleleft G_1$. □

We may now begin to explain why normal subgroups are so important in group theory. They reason is because they have a very important connection with homomorphisms. In fact, it can be shown that not only is the kernel of a homomorphism a normal subgroup, but it is also the case that every normal subgroup gives rise to a homomorphism from one group onto another. Thus, if we know what the normal subgroups of a given group are, then we know what kinds of homomorphisms are possible with respect to that group.

Now let's look at a few simple examples. Let's denote the set of integers by $\mathbb{Z} = \left\{ \begin{matrix} \vdots \\ -2 \\ -1 \\ 0 \\ 1 \\ 2 \\ \vdots \end{matrix} \right\}$ and the integers modulo 2 by $\mathbb{Z}_2 = \left\{ \begin{matrix} 0 \\ 1 \end{matrix} \right\}$, let our group operations be the usual addition, and let's define a homomorphism $f : \mathbb{Z} \to \mathbb{Z}_2$ by $f(x) = \begin{cases} 0 & \text{if } x \text{ is even} \\ 1 & \text{if } x \text{ is odd} \end{cases}$. Then, given that this is a homomorphism, its kernel is the set of all even integers, and we know that this kernel is both a subgroup and a normal subgroup of $\mathbb{Z}$. (Actually, we get normality for free in this case because $\mathbb{Z}$ is abelian, and that means that all of its subgroups are normal.)

Notice that in our new group $\mathbb{Z}_2 = \left\{ \begin{matrix} 0 \\ 1 \end{matrix} \right\}$, all the particular information about our integers has been lost except for whether the integer is even or odd. In other words, if I tell you that $f(x) = 0$, then all you know about *x* is that it's some even integer. In mathematics, we often like to write the set of even integers as $2\mathbb{Z} = \left\{ \begin{matrix} \vdots \\ -4 \\ -2 \\ 0 \\ 2 \\ 4 \\ \vdots \end{matrix} \right\}$, and the group that our homomorphism has given back to us we write as $\mathbb{Z}/2\mathbb{Z}$. This last expression looks like division, and that's exactly how we want to think about it, only in this case, we are saying that we are taking the integers and we are dividing out the differences between the even integers.

That means that we're creating a new structure in which all even integers appear the same and all odd integers appear the same. In this instance, in the new structure we have two cosets, one consisting of the even integers and one consisting of the odd integers, and we can add them by simply saying that *even* + *even* = *even*, and *odd* + *even* = *odd*. This results in a group that is isomorphic to the integers modulo 2, $\mathbb{Z}_2$. This new structure is called a quotient structure or a quotient group, and if you take a formal course on abstract algebra, then you'll spend a lot of time on these things.

However, in this work I only want to give you an introduction to the basic idea, and no more! Thus, here are the big ideas:

1. Every normal subgroup N of a group G gives rise to a homomorphism, $x \to xN$.
2. This homomorphism also results in a quotient structure or quotient group that we write as G / N .
3. In this quotient structure G / N , all the elements of the subgroup N appear as identical or indistinguishable from one another.
4. If we start with an onto homomorphism $f : G \to H$, then K, the kernel of f, is a normal subgroup of G.
5. The structure of G / K is identical to the structure of H. In other words, G / K is isomorphic to H, $G / K \simeq H$.

Well, this is taking us deeper into the depths of abstract algebra than we need to go at this point, but, nonetheless, I do want to show you one particular homomorphism that can lead to some interesting results regarding Rubik's cube. In particular, let's fix $a \in G$ and let's suppose that $x \in G$ is just any element in *G*. Then we can define a homomorphism $f_a : G \to G$ by $f_a(x) = axa^{-1}$. We claim that this function is not only a homomorphism, but it's also a one-to-one homomorphism. That means it's an isomorphism. Furthermore whenever we have an isomorphism from a group *G* back onto itself, we call it an *automorphism*.

Previously, we used automorphisms to help us discover new patterns that we can make on the surface of Rubik's cube. For example, suppose we have a sequence of moves that we'll just call *Y* that happens to produce a pleasing pattern. Now let's suppose that we have another sequence of moves that we'll call *X*. Then f_X defines an automorphism from the Rubik's cube group to the Rubik's cube group, and if we're lucky, then XYX^{-1} will transform the pattern *Y* into another pleasing pattern.

And now, let's close by showing that $f_a : G \to G$ defined by $f_a(x) = axa^{-1}$ is an automorphism.

Theorem: Let G be a group, fix $a \in G$, and define $f_a : G \to G$ by $f_a(x) = axa^{-1}$. Then $f_a : G \to G$ is an automorphism.

Proof: We'll first show that $f_a : G \to G$ is one-to-one. Thus, suppose that $x, y \in G$ and that $f_a(x) = f_a(y)$. Then $f_a(x) = f_a(y) \Rightarrow axa^{-1} = aya^{-1} \Rightarrow a^{-1}(axa^{-1})a = a^{-1}(aya^{-1})a \Rightarrow x = y$. Hence, $f_a : G \to G$ is one-to-one. To show that $f_a : G \to G$ is onto, let $x \in G$. Then $a^{-1}xa \in G$, and $f_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x$. Now let's consider $f_a(xy)$. By definition, $f_a(xy) = a(xy)a^{-1} = ax(a^{-1}a)ya^{-1} = (axa^{-1})(aya^{-1}) = f_a(x)\, f_a(y)$. Therefore, $f_a : G \to G$ is a homomorphism, and it now follows that $f_a : G \to G$ is an automorphism. □

And as a final note, this particular type of automorphism is so special in group theory that we give it a particular name. We call it an *inner automorphism*.