10 Group Homomorphisms

All modern theories of nuclear and electromagnetic interactions are based on group theory.

ANDREW WATSON, *New Scientist*

Definition and Examples

In this chapter, we consider one of the most fundamental ideas of algebra—homomorphisms. The term *homomorphism* comes from the Greek words *homo*, "like," and *morphe,* "form." We will see that a homomorphism is a natural generalization of an isomorphism and that there is an intimate connection between factor groups of a group and homomorphisms of a group. The concept of group homomorphisms was introduced by Camille Jordan in 1870, in his influential book *Traité des Substitutions*.

Definition Group Homomorphism
A *homomorphism* ϕ from a group G to a group $\overline{G}$ is a mapping from G into $\overline{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b)$ for all a, b in G.

Before giving examples and stating numerous properties of homomorphisms, it is convenient to introduce an important subgroup that is intimately related to the image of a homomorphism. (See property 4 of Theorem 10.1.)

Definition Kernel of a Homomorphism
The *kernel* of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G \mid \phi(x) = e\}$. The kernel of ϕ is denoted by Ker ϕ.

■ **EXAMPLE 1** Any isomorphism is a homomorphism that is also onto and one-to-one. The kernel of an isomorphism is the trivial subgroup. ■

■ **EXAMPLE 2** Let $\mathbf{R}^*$ be the group of nonzero real numbers under multiplication. Then the determinant mapping $A \rightarrow \det A$ is a homomorphism from $GL(2, \mathbf{R})$ to $\mathbf{R}^*$. The kernel of the determinant mapping is $SL(2, \mathbf{R})$. ■

■ **EXAMPLE 3** The mapping ϕ from $\mathbf{R}^*$ to $\mathbf{R}^*$, defined by $\phi(x) = |x|$, is a homomorphism with Ker $\phi = \{1, -1\}$. ■

■ **EXAMPLE 4** Let $\mathbf{R}[x]$ denote the group of all polynomials with real coefficients under addition. For any f in $\mathbf{R}[x]$, let f' denote the derivative of f. Then the mapping $f \rightarrow f'$ is a homomorphism from $\mathbf{R}[x]$ to itself. The kernel of the derivative mapping is the set of all constant polynomials. ■

■ **EXAMPLE 5** The mapping ϕ from Z to Z_n, defined by $\phi(m) = m \bmod n$, is a homomorphism (see Exercise 11 in Chapter 0). The kernel of this mapping is $\langle n \rangle$. ■

■ **EXAMPLE 6** The mapping $\phi(x) = x^2$ from $\mathbf{R}^*$, the nonzero real numbers under multiplication, to itself is a homomorphism, since $\phi(ab) = (ab)^2 = a^2b^2 = \phi(a)\phi(b)$ for all a and b in R^*. (See Exercise 5.) The kernel is $\{1, -1\}$. ■

■ **EXAMPLE 7** The mapping $\phi(x) = x^2$ from $\mathbf{R}$, the real numbers under addition, to itself is not a homomorphism, since $\phi(a + b) = (a + b)^2 = a^2 + 2ab + b^2$, whereas $\phi(a) + \phi(b) = a^2 + b^2$. ■

When defining a homomorphism from a group in which there are several ways to represent the elements, caution must be exercised to ensure that the correspondence is a function. (The term *well-defined* is often used in this context.) For example, since $3(x + y) = 3x + 3y$ in Z_6, one might believe that the correspondence $x + \langle 3 \rangle \rightarrow 3x$ from $Z/\langle 3 \rangle$ to Z_6 is a homomorphism. But it is not a function, since $0 + \langle 3 \rangle = 3 + \langle 3 \rangle$ in $Z/\langle 3 \rangle$ but $3 \cdot 0 \neq 3 \cdot 3$ in Z_6.

For students who have had linear algebra, we remark that every linear transformation is a group homomorphism and the nullspace is the same as the kernel. An invertible linear transformation is a group isomorphism.

Properties of Homomorphisms

Theorem 10.1 Properties of Elements Under Homomorphisms

Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let g be an element of G. Then

1. *ϕ carries the identity of G to the identity of $\overline{G}$.*
2. *$\phi(g^n) = (\phi(g))^n$ for all n in Z.*
3. *If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.*
4. *Ker ϕ is a subgroup of G.*
5. *$\phi(a) = \phi(b)$ if and only if $a\text{Ker } \phi = b\text{Ker } \phi$.*
6. *If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g\text{Ker } \phi$.*

PROOF The proofs of properties 1 and 2 are identical to the proofs of properties 1 and 2 of isomorphisms in Theorem 6.2. To prove property 3, notice that properties 1 and 2 together with $g^n = e$ imply that $e = \phi(e) = \phi(g^n) = (\phi(g))^n$. So, by Corollary 2 to Theorem 4.1, we have $|\phi(g)|$ divides n.

By property 1 we know that Ker ϕ is not empty. So, to prove property 4, we assume that $a, b \in$ Ker ϕ and show that $ab^{-1} \in$ Ker ϕ. Since $\phi(a) = e$ and $\phi(b) = e$, we have $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} = ee^{-1} = e$. So, $ab^{-1} \in$ Ker ϕ.

To prove property 5, first assume that $\phi(a) = \phi(b)$. Then $e = (\phi(b))^{-1}\phi(a) = \phi(b^{-1})\phi(a) = \phi(b^{-1}a)$, so that $b^{-1}a \in$ Ker ϕ. It now follows from property 5 of the lemma in Chapter 7 that $b\text{Ker } \phi = a\text{Ker } \phi$. Reversing this argument completes the proof.

To prove property 6, we must show that $\phi^{-1}(g') \subseteq g\text{Ker } \phi$ and that $g\text{Ker } \phi \subseteq \phi^{-1}(g')$. For the first inclusion, let $x \in \phi^{-1}(g')$, so that $\phi(x) = g'$. Then $\phi(g) = \phi(x)$ and by property 5 we have $g\text{Ker } \phi = x\text{Ker } \phi$ and therefore $x \in g\text{Ker } \phi$. This completes the proof that $\phi^{-1}(g') \subseteq g\text{Ker } \phi$. To prove that $g\text{Ker } \phi \subseteq \phi^{-1}(g')$, suppose that $k \in$ Ker ϕ. Then $\phi(gk) = \phi(g)\phi(k) = g'e = g'$. Thus, by definition, $gk \in \phi^{-1}(g')$. ∎

Since homomorphisms preserve the group operation, it should not be a surprise that they preserve many group properties.

Theorem 10.2 Properties of Subgroups Under Homomorphisms

Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let H be a subgroup of G. Then

1. $\phi(H) = \{\phi(h) \mid h \in H\}$ *is a subgroup of* $\overline{G}$.
2. *If H is cyclic, then $\phi(H)$ is cyclic.*
3. *If H is Abelian, then $\phi(H)$ is Abelian.*
4. *If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$.*
5. *If $|\text{Ker } \phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$.*
6. *If $|H| = n$, then $|\phi(H)|$ divides n.*
7. *If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a subgroup of G.*
8. *If $\overline{K}$ is a normal subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a normal subgroup of G.*
9. *If ϕ is onto and Ker $\phi = \{e\}$, then ϕ is an isomorphism from G to $\overline{G}$.*

PROOF First note that the proofs of properties 1, 2, and 3 are identical to the proofs of properties 4, 3, and 2, respectively, of Theorem 6.3, since those proofs use only the fact that an isomorphism is an operation-preserving mapping.

To prove property 4, let $\phi(h) \in \phi(H)$ and $\phi(g) \in \phi(G)$. Then $\phi(g)\phi(h)\phi(g)^{-1} = \phi(ghg^{-1}) \in \phi(H)$, since H is normal in G.

Property 5 follows directly from property 6 of Theorem 10.1 and the fact that all cosets of Ker $\phi = \phi^{-1}(e)$ have the same number of elements.

To prove property 6, let ϕ_H denote the restriction of ϕ to the elements of H. Then ϕ_H is a homomorphism from H onto $\phi(H)$. Suppose $|\text{Ker } \phi_H| = t$. Then, by property 5, ϕ_H is a t-to-1 mapping. So, $|\phi(H)|t = |H|$.

To prove property 7, we use the One-Step Subgroup Test. Clearly, $e \in \phi^{-1}(\overline{K})$, so that $\phi^{-1}(\overline{K})$ is not empty. Let $k_1, k_2 \in \phi^{-1}(\overline{K})$. Then, by the definition of $\phi^{-1}(\overline{K})$, we know that $\phi(k_1), \phi(k_2) \in \overline{K}$. Thus, $\phi(k_2)^{-1} \in \overline{K}$ as well and $\phi(k_1k_2^{-1}) = \phi(k_1)\phi(k_2)^{-1} \in \overline{K}$. So, by definition of $\phi^{-1}(\overline{K})$, we have $k_1k_2^{-1} \in \phi^{-1}(\overline{K})$.

To prove property 8, we use the normality test given in Theorem 9.1. Note that every element in $x\phi^{-1}(\overline{K})x^{-1}$ has the form xkx^{-1}, where $\phi(k) \in \overline{K}$. Thus, since $\overline{K}$ is normal in $\overline{G}$, $\phi(xkx^{-1}) = \phi(x)\phi(k)(\phi(x))^{-1} \in \overline{K}$, and, therefore, $xkx^{-1} \in \phi^{-1}(\overline{K})$.

Finally, property 9 follows directly from property 5. ∎

A few remarks about Theorems 10.1 and 10.2 are in order. Students should remember the various properties of these theorems in words. For example, properties 2 and 3 of Theorem 10.2 say that the homomorphic image of a cyclic group is cyclic and the homomorphic image of an Abelian group is Abelian. Property 4 of Theorem 10.2 says that the homomorphic image of a normal subgroup of G is normal in the image of G. Property 5 of Theorem 10.2 says that if ϕ is a homomorphism from G to $\overline{G}$, then every element of $\overline{G}$ that gets "hit" by ϕ gets hit the same number of times as does the identity. The set $\phi^{-1}(g')$ defined in property 6 of Theorem 10.1 is called the *inverse image of* g' (or the *pullback* of g'). Note that the inverse image of an element is a coset of the kernel and that every element in that coset has the same image. Similarly, the set $\phi^{-1}(\overline{K})$ defined in property 7 of Theorem 10.2 is called the *inverse image* of $\overline{K}$ (or the *pullback* of $\overline{K}$).

Property 6 of Theorem 10.1 is reminiscent of something from linear algebra and differential equations. Recall that if x is a particular solution to a system of linear equations and S is the entire solution set of the corresponding homogeneous system of linear equations, then $x + S$ is the entire solution set of the nonhomogeneous system. In reality, this statement is just a special case of property 6. Properties 1 and 6 of Theorem 10.1 and property 5 of Theorem 10.2 are pictorially represented in Figure 10.1.

The special case of property 8 of Theorem 10.2, where $\overline{K} = \{e\}$, is of such importance that we single it out.

Corollary Kernels Are Normal

Let ϕ be a group homomorphism from G to $\overline{G}$. Then Ker ϕ is a normal subgroup of G.

The next two examples illustrate several properties of Theorems 10.1 and 10.2.

EXAMPLE 8 Consider the mapping ϕ from $\mathbf{C}^*$ to $\mathbf{C}^*$ given by $\phi(x) = x^4$. Since $(xy)^4 = x^4y^4$, ϕ is a homomorphism. Clearly, Ker $\phi = \{x \mid x^4 = 1\} = \{1, -1, i, -i\}$. So, by property 5 of Theorem 10.2, we know that ϕ is a 4-to-1 mapping. Now let's find all elements that map to, say, 2. Certainly, $\phi(\sqrt[4]{2}) = 2$. Then, by property 6 of Theorem 10.1, the set of all elements that map to 2 is $\sqrt[4]{2}\,\text{Ker}\ \phi = \left\{\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}\,i, -\sqrt[4]{2}\,i\right\}$.

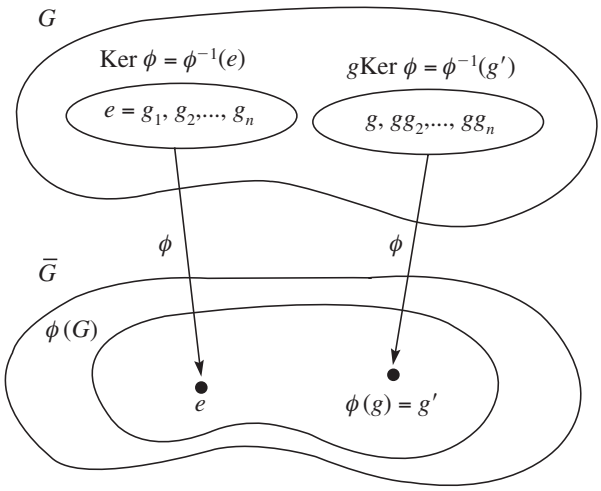


Figure 10.1

Finally, we verify a specific instance of property 3 of Theorem 10.1 and of property 2 and property 6 of Theorem 10.2. Let $H = \langle \cos 30° + i \sin 30° \rangle$. It follows from DeMoivre's Theorem (Example 7 in Chapter 0) that $|H| = 12$, $\phi(H) = \langle \cos 120° + i \sin 120° \rangle$, and $|\phi(H)| = 3$. ∎

■ **EXAMPLE 9** Define $\phi: Z_{12} \to Z_{12}$ by $\phi(x) = 3x$. To verify that ϕ is a homomorphism, we observe that in Z_{12}, $3(a + b) = 3a + 3b$ (since the group operation is addition modulo 12). Direct calculations show that Ker $\phi = \{0, 4, 8\}$. Thus, we know from property 5 of Theorem 10.2 that ϕ is a 3-to-1 mapping. Since $\phi(2) = 6$, we have by property 6 of Theorem 10.1 that $\phi^{-1}(6) = 2 + \text{Ker } \phi = \{2, 6, 10\}$. Notice also that $\langle 2 \rangle$ is cyclic and $\phi(\langle 2 \rangle) = \{0, 6\}$ is cyclic. Moreover, $|2| = 6$ and $|\phi(2)| = |6| = 2$, so $|\phi(2)|$ divides $|2|$ in agreement with property 3 of Theorem 10.1. Letting $\overline{K} = \{0, 6\}$, we see that the subgroup $\phi^{-1}(\overline{K}) = \{0, 2, 4, 6, 8, 10\}$. This verifies property 7 of Theorem 10.2 in this particular case. ∎

The next example illustrates how one can easily determine all homomorphisms from a cyclic group to a cyclic group.

■ **EXAMPLE 10** We determine all homomorphisms from Z_{12} to Z_{30}. By property 2 of Theorem 10.1, such a homomorphism is completely specified by the image of 1. That is, if 1 maps to a, then x maps to xa. Lagrange's Theorem and property 3 of Theorem 10.1 require that $|a|$ divide both 12 and 30. So, $|a| = 1$, 2, 3, or 6. Thus, $a = 0$, 15, 10, 20, 5, or 25. This gives us a list of candidates for the homomorphisms. That each of these six possibilities yields an operation-preserving, well-defined function can now be verified by direct calculations. [Note that gcd(12, 30) = 6. This is not a coincidence!] ∎

■ **EXAMPLE 11** The mapping from S_n to Z_2 that takes an even permutation to 0 and an odd permutation to 1 is a homomorphism. Figure 10.2 illustrates the telescoping nature of the mapping. ■

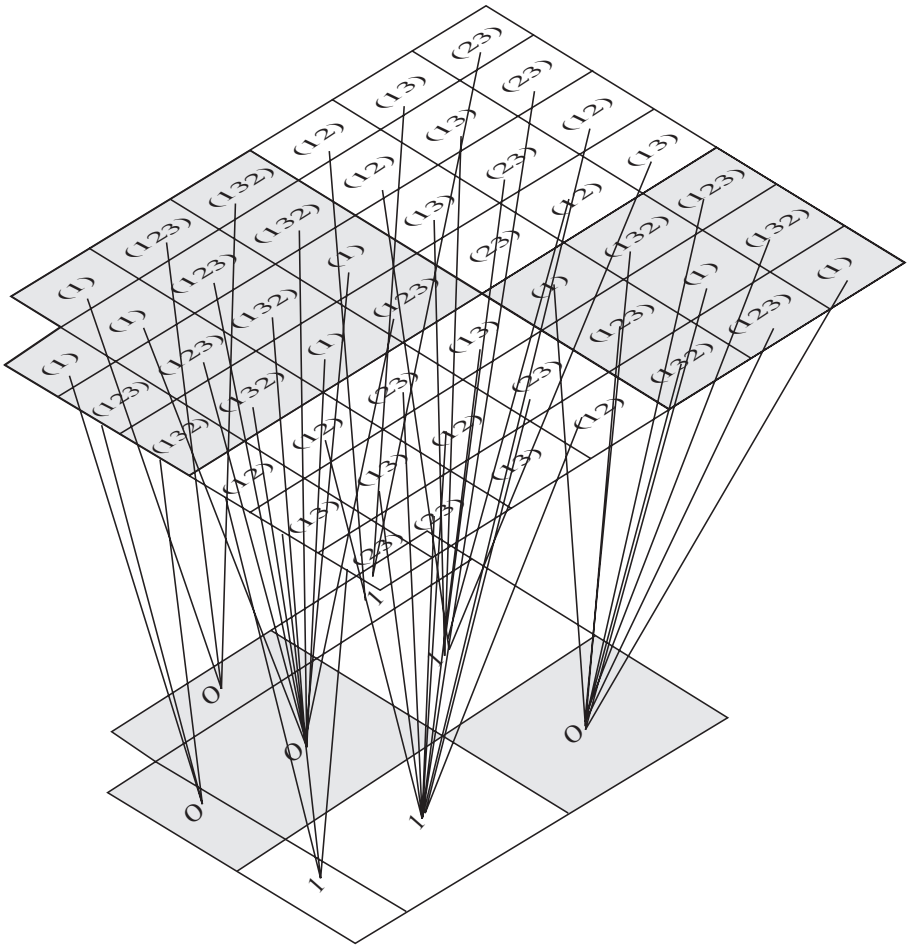


Figure 10.2 Homomorphism from S_3 to Z_2.

The First Isomorphism Theorem

In Chapter 9, we showed that for a group G and a normal subgroup H, we could arrange the Cayley table of G into boxes that represented the cosets of H in G, and that these boxes then became a Cayley table for G/H. The next theorem shows that for any homomorphism ϕ of G and the normal subgroup Ker ϕ, the same process produces a Cayley table isomorphic to the homomorphic image of G. Thus, homomorphisms, like factor groups, cause a *systematic* collapse of a group to a simpler but closely related group. This can be likened to viewing a group through the reverse end of a telescope—the general features of the group are present, but the apparent size is diminished. The important

relationship between homomorphisms and factor groups given below is often called the Fundamental Theorem of Group Homomorphisms.

Theorem 10.3 First Isomorphism Theorem (Jordan, 1870)

Let ϕ be a group homomorphism from G to $\overline{G}$. Then the mapping from $G/\text{Ker}\ \phi$ to $\phi(G)$, given by $g\text{Ker}\ \phi \to \phi(g)$, is an isomorphism. In symbols, $G/\text{Ker}\ \phi \approx \phi(G)$.

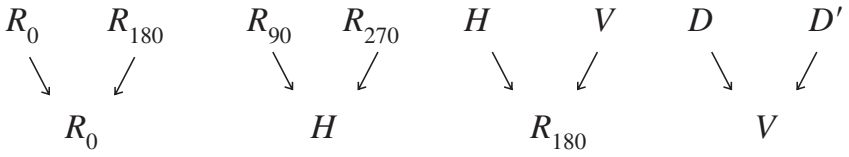
PROOF Let us use ψ to denote the correspondence $g\text{Ker}\,\phi \to \phi(g)$. That ψ is well defined (that is, the correspondence is independent of the particular coset representative chosen) and one-to-one follows directly from property 5 of Theorem 10.1. To show that ψ is operation-preserving, observe that $\psi(x\text{Ker}\ \phi\ y\text{Ker}\ \phi) = \psi(xy\text{Ker}\ \phi) = \phi(xy) = \phi(x)\ \phi(y) = \psi(x\text{Ker}\ \phi)\psi(y\text{Ker}\ \phi)$. ∎

The next corollary follows directly from Theorem 10.3, property 1 of Theorem 10.2, and Lagrange's Theorem.

Corollary

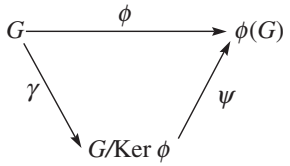
If ϕ is a homomorphism from a finite group G to $\overline{G}$, then $|\phi(G)|$ divides $|G|$ and $|\overline{G}|$.

EXAMPLE 10 To illustrate Theorem 10.3 and its proof, consider the homomorphism ϕ from D_4 to itself given by



Then Ker $\phi = \{R_0, R_{180}\}$, and the mapping ψ in Theorem 10.3 is $R_0\text{Ker}\ \phi \to R_0$, $R_{90}\text{Ker}\ \phi \to H$, $H\text{Ker}\ \phi \to R_{180}$, $D\text{Ker}\ \phi \to V$. It is straight-forward to verify that the mapping ψ is an isomorphism. ∎

Mathematicians often give a pictorial representation of Theorem 10.3, as follows:



where $\gamma: G \to G/\text{Ker } \phi$ is defined as $\gamma(g) = g\text{Ker } \phi$. The mapping γ is called the *natural mapping* from G to $G/\text{Ker } \phi$. Our proof of Theorem 10.3 shows that $\psi\gamma = \phi$. In this case, one says that the preceding diagram is *commutative.*

As a consequence of Theorem 10.3, we see that all homomorphic images of G can be determined using G. We may simply consider the various factor groups of G. For example, we know that the homomorphic image of an Abelian group is Abelian because the factor group of an Abelian group is Abelian. We know that the number of homomorphic images of a cyclic group G of order n is the number of divisors of n, since there is exactly one subgroup of G (and therefore one factor group of G) for each divisor of n. (Be careful: The number of homomorphisms of a cyclic group of order n need not be the same as the number of divisors of n, since different homomorphisms can have the same image.)

An appreciation for Theorem 10.3 can be gained by looking at a few examples.

EXAMPLE 13 $Z/\langle N\rangle \approx Z_N$

Consider the mapping from Z to Z_n defined in Example 5. Clearly, its kernel is $\langle n\rangle$. So, by Theorem 10.3, $Z/\langle n\rangle \approx Z_n$. ∎

EXAMPLE 14 The Wrapping Function

Recall the wrapping function W from trigonometry. The real number line is wrapped around a unit circle in the plane centered at (0, 0) with the number 0 on the number line at the point (1, 0), the positive reals in the counterclockwise direction and the negative reals in the clockwise direction (see Figure 10.3). The function W assigns to each real number a the point a radians from (1, 0) on the circle. This mapping is a homomorphism from the group $\mathbf{R}$ under addition onto the circle group (the group of complex numbers of magnitude 1 under multiplication). Indeed, it follows from elementary facts of trigonometry that $W(x) = \cos x + i \sin x$ and $W(x + y) = W(x)W(y)$. Since W is periodic of period 2π, Ker $W = \langle 2\pi\rangle$. So, from the First Isomorphism Theorem, we see that $\mathbf{R}/\langle 2\pi\rangle$ is isomorphic to the circle group. ∎

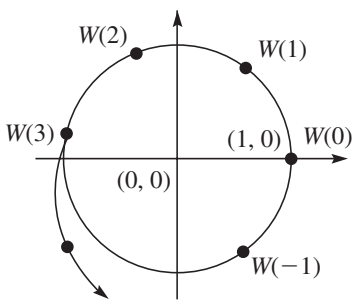


Figure 10.3

Our next example is a theorem that is used repeatedly in Chapters 24 and 25.

EXAMPLE 15 The *N*/*C* Theorem

Let H be a subgroup of a group G. Recall that the normalizer of H in G is $N(H) = \{x \in G \mid xHx^{-1} = H\}$ and the centralizer of H in G is $C(H) = \{x \in G \mid xhx^{-1} = h \text{ for all } h \text{ in } H\}$. Consider the mapping from $N(H)$ to $\text{Aut}(H)$ given by $g \to \phi_g$, where ϕ_g is the inner automorphism of H induced by g [that is, $\phi_g(h) = ghg^{-1}$ for all h in H]. This mapping is a homomorphism with kernel $C(H)$. So, by Theorem 10.3, $N(H)/C(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$. ∎

As an application of the N/C Theorem, we will show that every group of order 35 is cyclic.

EXAMPLE 16 Let G be a group of order 35. By Lagrange's Theorem, every nonidentity element of G has order 5, 7, or 35. If some element has order 35, G is cyclic. So we may assume that all nonidentity elements have order 5 or 7. However, not all such elements can have order 5, since elements of order 5 come 4 at a time (if $|x| = 5$, then $|x^2| = |x^3| = |x^4| = 5$) and 4 does not divide 34. Similarly, since 6 does not divide 34, not all nonidentity elements can have order 7. So, G has elements of order 7 and order 5. Since G has an element of order 7, it has a subgroup of order 7. Let us call it H. In fact, H is the only subgroup of G of order 7, for if K is another subgroup of G of order 7, we have by Exercise 7 of the Supplementary Exercises for Chapters 5–8 that $|HK| = |H||K|/|H \cap K| = 7 \cdot 7/1 = 49$. But, of course, this is impossible in a group of order 35. Since for every a in G, aHa^{-1} is also a subgroup of G of order 7 (see Exercise 1 of the Supplementary Exercises for Chapters 1–4), we must have $aHa^{-1} = H$. So, $N(H) = G$. Since H has prime order, it is cyclic and therefore Abelian. In particular, $C(H)$ contains H. So, 7 divides $|C(H)|$ and $|C(H)|$ divides 35. It follows, then, that $C(H) = G$ or $C(H) = H$. If $C(H) = G$, then we may obtain an element x of order 35 by letting $x = hk$, where h is a nonidentity element of H and k has order 5. On the other hand, if $C(H) = H$, then $|C(H)| = 7$ and $|N(H)/C(H)| = 35/7 = 5$. However, 5 does not divide $|\text{Aut}(H)| = |\text{Aut}(Z_7)| = 6$. This contradiction shows that G is cyclic. ∎

The corollary of Theorem 10.2 says that the kernel of every homomorphism of a group is a normal subgroup of the group. We conclude this chapter by verifying that the converse of this statement is also true.

Theorem 10.4 Normal Subgroups Are Kernels

Every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, a normal subgroup N is the kernel of the mapping $g \to gN$ from G to G/N.

PROOF Define $\gamma: G \to G/N$ by $\gamma(g) = gN$. (This mapping is called the *natural homomorphism* from G to G/N.) Then, $\gamma(xy) = (xy)N = xNyN = \gamma(x)\gamma(y)$. Moreover, $g \in \text{Ker } \gamma$ if and only if $gN = \gamma(g) = N$, which is true if and only if $g \in N$ (see property 2 of the lemma in Chapter 7). ∎

Examples 13, 14, and 15 illustrate the utility of the First Isomorphism Theorem. But what about homomorphisms in general? Why would one care to study a homomorphism of a group? The answer is that, just as was the case with factor groups of a group, homomorphic images of a group tell us *some* of the properties of the original group. One measure of the likeness of a group and its homomorphic image is the size of the kernel. If the kernel of the homomorphism of group G is the identity, then the image of G tells us everything (group theoretically) about G (the two being isomorphic). On the other hand, if the kernel of the homomorphism is G itself, then the image tells us nothing about G. Between these two extremes, some information about G is preserved and some is lost. The utility of a particular homomorphism lies in its ability to preserve the group properties we want, while losing some inessential ones. In this way, we have replaced G by a group less complicated (and therefore easier to study) than G; but, in the process, we have saved enough information to answer questions that we have about G itself. For example, if G is a group of order 60 and G has a homomorphic image of order 12 that is cyclic, then we know from properties 5, 7, and 8 of Theorem 10.2 that G has normal subgroups of orders 5, 10, 15, 20, 30, and 60. To illustrate further, suppose we are asked to find an infinite group that is the union of three proper subgroups. Instead of attempting to do this directly, we first make the problem easier by finding a finite group that is the union of three proper subgroups. Observing that $Z_2 \oplus Z_2$ is the union of $H_1 = \langle 1, 0\rangle$, $H_2 = \langle 0, 1\rangle$, and $H_3 = \langle 1, 1\rangle$, we have found our finite group. Now all we need do is think of an infinite group that has $Z_2 \oplus Z_2$ as a homomorphic image and pull back H_1, H_2, and H_3, and our original problem is solved. Clearly, the mapping from $Z_2 \oplus Z_2 \oplus Z$ onto $Z_2 \oplus Z_2$ given by $\phi(a, b, c) = (a, b)$ is such a mapping, and therefore $Z_2 \oplus Z_2 \oplus Z$ is the union of $\phi^{-1}(H_1) = \{(a, 0, c,) \mid a \in Z_2, c \in Z\}$, $\phi^{-1}(H_2) = \{(0, b, c) \mid b \in Z_2, c \in Z\}$, and $\phi^{-1}(H_3) = \{(a, a, c) \mid a \in Z_2, c \in Z\}$.

Although an isomorphism is a special case of a homomorphism, the two concepts have entirely different roles. Whereas isomorphisms allow us to look at a group in an alternative way, homomorphisms act as investigative tools. The following analogy between homomorphisms and photography may be instructive.[†] A photograph of a person cannot tell us the person's exact height, weight, or age. Nevertheless, we *may* be able to decide from a photograph whether the person is tall or short, heavy or thin, old or young, male or female. In the same way, a homomorphic image of a group gives us *some* information about the group.

In certain branches of group theory, and especially in physics and chemistry, one often wants to know all homomorphic images of a group that are matrix groups over the complex numbers (these are called *group representations*). Here, we may carry our analogy with photography one step further by saying that this is like wanting photographs of a person from many different angles (front view, profile, head-to-toe view, close-up, etc.), as well as x-rays! Just as this composite information from the photographs reveals much about the person, several homomorphic images of a group reveal much about the group.

Exercises

The greater the difficulty, the more glory in surmounting it. Skillful pilots gain their reputation from storms and tempests.

EPICURUS

1. Prove that the mapping given in Example 2 is a homomorphism.

2. Prove that the mapping given in Example 3 is a homomorphism.

3. Prove that the mapping given in Example 4 is a homomorphism.

4. Prove that the mapping given in Example 11 is a homomorphism.

5. Let $\mathbf{R}^*$ be the group of nonzero real numbers under multiplication, and let r be a positive integer. Show that the mapping that takes x to x^r is a homomorphism from $\mathbf{R}^*$ to $\mathbf{R}^*$ and determine the kernel. Which values of r yield an isomorphism?

6. Let G be the group of all polynomials with real coefficients under addition. For each f in G, let $\int f$ denote the antiderivative of f that passes through the point $(0, 0)$. Show that the mapping $f \to \int f$ from G to G is a homomorphism. What is the kernel of this mapping? Is this mapping a homomorphism if $\int f$ denotes the antiderivative of f that passes through $(0, 1)$?

[†]*All perception of truth is the detection of an analogy.* Henry David Thoreau, *Journal.*

7. If ϕ is a homomorphism from G to H and σ is a homomorphism from H to K, show that $\sigma\phi$ is a homomorphism from G to K. How are Ker ϕ and Ker $\sigma\phi$ related? If ϕ and σ are onto and G is finite, describe [Ker $\sigma\phi$: Ker ϕ] in terms of $|H|$ and $|K|$.

8. Let G be a group of permutations. For each σ in G, define

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

Prove that sgn is a homomorphism from G to the multiplicative group $\{+1, -1\}$. What is the kernel? Why does this homomorphism allow you to conclude that A_n is a normal subgroup of S_n of index 2?

9. Prove that the mapping from $G \oplus H$ to G given by $(g, h) \to g$ is a homomorphism. What is the kernel? This mapping is called the *projection* of $G \oplus H$ onto G.

10. Let G be a subgroup of some dihedral group. For each x in G, define

$$\phi(x) = \begin{cases} +1 & \text{if } x \text{ is a rotation,} \\ -1 & \text{if } x \text{ is a reflection.} \end{cases}$$

Prove that ϕ is a homomorphism from G to the multiplicative group $\{+1, -1\}$. What is the kernel?

11. Prove that $(Z \oplus Z)/(\langle (a, 0) \rangle \times \langle (0, b) \rangle)$ is isomorphic to $Z_a \oplus Z_b$.

12. Suppose that k is a divisor of n. Prove that $Z_n/\langle k \rangle \approx Z_k$.

13. Prove that $(A \oplus B)/(A \oplus \{e\}) \approx B$.

14. Explain why the correspondence $x \to 3x$ from Z_{12} to Z_{10} is not a homomorphism.

15. Suppose that ϕ is a homomorphism from Z_{30} to Z_{30} and Ker $\phi = \{0, 10, 20\}$. If $\phi(23) = 9$, determine all elements that map to 9.

16. Prove that there is no homomorphism from $Z_8 \oplus Z_2$ onto $Z_4 \oplus Z_4$.

17. Prove that there is no homomorphism from $Z_{16} \oplus Z_2$ onto $Z_4 \oplus Z_4$.

18. Can there be a homomorphism from $Z_4 \oplus Z_4$ onto Z_8? Can there be a homomorphism from Z_{16} onto $Z_2 \oplus Z_2$? Explain your answers.

19. Suppose that there is a homomorphism ϕ from Z_{17} to some group and that ϕ is not one-to-one. Determine ϕ.

20. How many homomorphisms are there from Z_{20} onto Z_8? How many are there to Z_8?

21. If ϕ is a homomorphism from Z_{30} onto a group of order 5, determine the kernel of ϕ.

22. Suppose that ϕ is a homomorphism from a finite group G onto $\overline{G}$ and that $\overline{G}$ has an element of order 8. Prove that G has an element of order 8. Generalize.

23. Suppose that ϕ is a homomorphism from Z_{36} to a group of order 24.

a. Determine the possible homomorphic images.

b. For each image in part a, determine the corresponding kernel of ϕ.

24. Suppose that $\phi: Z_{50} \to Z_{15}$ is a group homomorphism with $\phi(7) = 6$.

a. Determine $\phi(x)$.

b. Determine the image of ϕ.

c. Determine the kernel of ϕ.

d. Determine $\phi^{-1}(3)$. That is, determine the set of all elements that map to 3.

25. How many homomorphisms are there from Z_{20} onto Z_{10}? How many are there to Z_{10}?

26. Determine all homomorphisms from Z_4 to $Z_2 \oplus Z_2$.

27. Determine all homomorphisms from Z_n to itself.

28. Suppose that ϕ is a homomorphism from S_4 onto Z_2. Determine Ker ϕ. Determine all homomorphisms from S_4 to Z_2.

29. Suppose that there is a homomorphism from a finite group G onto Z_{10}. Prove that G has normal subgroups of indexes 2 and 5.

30. Suppose that ϕ is a homomorphism from a group G onto $Z_6 \oplus Z_2$ and that the kernel of ϕ has order 5. Explain why G must have normal subgroups of orders 5, 10, 15, 20, 30, and 60.

31. Suppose that ϕ is a homomorphism from $U(30)$ to $U(30)$ and that Ker $\phi = \{1, 11\}$. If $\phi(7) = 7$, find all elements of $U(30)$ that map to 7.

32. Find a homomorphism ϕ from $U(30)$ to $U(30)$ with kernel $\{1, 11\}$ and $\phi(7) = 7$.

33. Suppose that ϕ is a homomorphism from $U(40)$ to $U(40)$ and that Ker $\phi = \{1, 9, 17, 33\}$. If $\phi(11) = 11$, find all elements of $U(40)$ that map to 11.

34. Find a homomorphism ϕ from $U(40)$ to $U(40)$ with kernel $\{1, 9, 17, 33\}$ and $\phi(11) = 11$.

35. Prove that the mapping $\phi: Z \oplus Z \to Z$ given by $(a, b) \to a - b$ is a homomorphism. What is the kernel of ϕ? Describe the set $\phi^{-1}(3)$ (that is, all elements that map to 3).

36. Suppose that there is a homomorphism ϕ from $Z \oplus Z$ to a group G such that $\phi((3, 2)) = a$ and $\phi((2, 1)) = b$. Determine $\phi((4, 4))$ in terms of a and b. Assume that the operation of G is addition.

37. Prove that the mapping $x \to x^6$ from $\mathbf{C}^*$ to $\mathbf{C}^*$ is a homomorphism. What is the kernel?

38. For each pair of positive integers m and n, we can define a homomorphism from Z to $Z_m \oplus Z_n$ by $x \to (x \bmod m, x \bmod n)$. What is the kernel when $(m, n) = (3, 4)$? What is the kernel when $(m, n) = (6, 4)$? Generalize.

39. (Second Isomorphism Theorem) If K is a subgroup of G and N is a normal subgroup of G, prove that $K/(K \cap N)$ is isomorphic to KN/N.

40. (Third Isomorphism Theorem) If M and N are normal subgroups of G and $N \leq M$, prove that $(G/N)/(M/N) \approx G/M$.

41. Let $\phi(d)$ denote the Euler phi function of d (see page 79). Show that the number of homomorphisms from Z_n to Z_k is $\Sigma\phi(d)$, where the sum runs over all common divisors d of n and k. [It follows from number theory that this sum is actually $\gcd(n, k)$.]

42. Let k be a divisor of n. Consider the homomorphism from $U(n)$ to $U(k)$ given by $x \to x \bmod k$. What is the relationship between this homomorphism and the subgroup $U_k(n)$ of $U(n)$?

43. Determine all homomorphic images of D_4 (up to isomorphism).

44. Let N be a normal subgroup of a finite group G. Use the theorems of this chapter to prove that the order of the group element gN in G/N divides the order of g.

45. Suppose that G is a finite group and that Z_{10} is a homomorphic image of G. What can we say about $|G|$? Generalize.

46. Suppose that Z_{10} and Z_{15} are both homomorphic images of a finite group G. What can be said about $|G|$? Generalize.

47. Suppose that for each prime p, Z_p is the homomorphic image of a group G. What can we say about $|G|$? Give an example of such a group.

48. (For students who have had linear algebra.) Suppose that x is a particular solution to a system of linear equations and that S is the entire solution set of the corresponding homogeneous system of linear equations. Explain why property 6 of Theorem 10.1 guarantees that $x + S$ is the entire solution set of the nonhomogeneous system. In particular, describe the relevant groups and the homomorphism between them.

49. Let N be a normal subgroup of a group G. Use property 7 of Theorem 10.2 to prove that every subgroup of G/N has the form H/N, where H is a subgroup of G. (This exercise is referred to in Chapter 24.)

50. Show that a homomorphism defined on a cyclic group is completely determined by its action on a generator of the group.

51. Use the First Isomorphism Theorem to prove Theorem 9.4.

52. Let α and β be group homomorphisms from G to $\overline{G}$ and let $H = \{g \in G \mid \alpha(g) = \beta(g)\}$. Prove or disprove that H is a subgroup of G.

53. Let $Z[x]$ be the group of polynomials in x with integer coefficients under addition. Prove that the mapping from $Z[x]$ into Z given by $f(x) \to f(3)$ is a homomorphism. Give a geometric description of the kernel of this homomorphism. Generalize.

54. Prove that the mapping from $\mathbf{R}$ under addition to $GL(2, \mathbf{R})$ that takes x to

$$\begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix}$$

is a group homomorphism. What is the kernel of the homomorphism?

55. Suppose there is a homomorphism ϕ from G onto $Z_2 \oplus Z_2$. Prove that G is the union of three proper normal subgroups.

56. If H and K are normal subgroups of G and $H \cap K = \{e\}$, prove that G is isomorphic to a subgroup of $G/H \oplus G/K$.

57. Suppose that H and K are distinct subgroups of G of index 2. Prove that $H \cap K$ is a normal subgroup of G of index 4 and that $G/(H \cap K)$ is not cyclic.

58. Suppose that the number of homomorphisms from G to H is n. How many homomorphisms are there from G to $H \oplus H \oplus \cdots \oplus H$ (s terms)? When H is Abelian, how many homomorphisms are there from $G \oplus G \oplus \cdots \oplus G$ (s terms) to H?

59. Prove that every group of order 77 is cyclic.

60. Determine all homomorphisms from Z onto S_3. Determine all homomorphisms from Z to S_3.

61. Suppose G is an Abelian group under addition with the property that for every positive integer n the set $nG = \{ng | g \in G\} = G$. Show that every proper subgroup of G is properly contained in a proper subgroup of G. Name two familiar groups that satisfy the hypothesis.

62. Let p be a prime. Determine the number of homomorphisms from $Z_p \oplus Z_p$ into Z_p.

Computer Exercise

A computer lets you make more mistakes faster than any invention in human history—with the possible exceptions of handguns and tequila.

MITCH RATLIFFE

Software for the computer exercise in this chapter is available at the website:

http://www.d.umn.edu/~jgallian

1. This software determines the homomorphisms from Z_m to Z_n. (Recall that a homomorphism from Z_m is completely determined by the image of 1.) Run the program for $m = 20$ with various choices for n. Run the program for $m = 15$ with various choices for n. What relationship do you see between m and n and the number of homomorphisms from Z_m to Z_n? For each choice of m and n, observe the smallest positive image of 1. Try to see the relationship between this image and the values of m and n. What relationship do you see between the smallest positive image of 1 and the other images of 1? Test your conclusions with other choices of m and n.