2.2 Homomorphisms

We have learned what groups and subgroups are and encountered several different kinds of groups: cyclic and noncyclic, Abelian and non-Abelian, finite and infinite. We have not, however, studied maps between groups. Since groups are not just plain sets, but rather are sets equipped with an operation that satisfies certain axioms, the maps we are interested in are ones that "respect" or "preserve" the operations on the groups involved.

2.2.1 EXAMPLE We look at three different functions from $\mathbb{Z}$ to $\mathbb{Z}$ and identify some properties of these functions. Let the functions f, g, $h : \mathbb{Z} \to \mathbb{Z}$ be given by

(1) $f(x) = x^2$
(2) $g(x) = x + 1$
(3) $h(x) = 2x$

In case (1), the image of f is not a subgroup of $\mathbb{Z}$. Also, if we take two elements $x, y \in \mathbb{Z}$, add them first, and then apply f, the result is not the same as if we first applied f to them and then added: $f(x) + f(y) = x^2 + y^2 \neq (x + y)^2 = f(x + y)$.
In case (2), the image of g is a subgroup of $\mathbb{Z}$, and in fact is $\mathbb{Z}$ itself, but again $g(x + y) = (x + y + 1) \neq (x + 1) + (y + 1) = g(x) + g(y)$.
In case (3), finally, the image of h is $2\mathbb{Z}$, which is a subgroup of $\mathbb{Z}$, and also we have $h(x + y) = 2(x + y) = 2x + 2y = h(x) + h(y)$. This is the only case where the function respects or preserves the group structure. ◇

2.2.2 DEFINITION A map ϕ: $G \to G'$ from a group G to a group G' is called a **homomorphism** if

$$\phi(ab) = \phi(a)\phi(b) \text{ for all } a, b \in G$$

Note that in $\phi(ab)$ the product is being taken in G, while in $\phi(a)\phi(b)$ the product is being taken in G'. ○

2.2.3 EXAMPLE In Example 2.2.1, h is a homomorphism, while f and g are not. Note also that besides $h(x + y) = h(x) + h(y)$ we have $h(0) = 0$, and $h(-x) = -h(x)$. ◇

2.2.4 EXAMPLE The map ϕ: $\mathbb{Z} \to \mathbb{Z}$ given by $\phi(x) = 5x$ is a homomorphism since $\phi(x + y) = 5(x + y) = 5x + 5y = \phi(x) + \phi(y)$. ◇

2.2.5 EXAMPLE The map ϕ: $\mathbb{R}^* \to \mathbb{Z}_2$ given by

$$\phi(x) = \begin{cases} 0 \text{ if } x > 0 \\ 1 \text{ if } x < 0 \end{cases}$$

is a homomorphism. To check this, note that if x and y are both positive, then xy is positive and $\phi(xy) = 0 = 0 + 0 = \phi(x) + \phi(y)$. Also, if x and y are both negative, then xy is positive and $\phi(xy) = 0 = 1 + 1 = \phi(x) + \phi(y)$. Also, if x is positive and y is negative, then xy is negative and $\phi(xy) = 1 = 0 + 1 = \phi(x) + \phi(y)$, and similarly in the opposite case where x is negative and y is positive. ◇

2.2.6 EXAMPLE For any group G, the **identity** map is always a homomorphism, since if ϕ: $G \to G$ is the identity $\phi(x) = x$, then $\phi(xy) = xy = \phi(x)\phi(y)$. ◇

2.2.7 EXAMPLE For any groups G and G', the map ϕ: $G \to G'$ given by $\phi(x) = e'$, where e' is the identity element of G', is a homomorphism, called the **trivial** homomorphism between G and G'. For we have $\phi(xy) = e' = e'\cdot e' = \phi(x)\phi(y)$.◇

2.2.8 EXAMPLE For any group G and any $a \in G$, consider the map ϕ: $\mathbb{Z} \to \langle a \rangle$, called the **exponential map**, given by $\phi(n) = a^n$. Then ϕ is a homomorphism, since $\phi(n + m) = a^{n+m} = a^n a^m = \phi(n)\phi(m)$. ◇

2.2.9 EXAMPLE Let ϕ: $\mathbb{Z} \to \mathbb{Z}_5$ be defined by $\phi(n)$ = the remainder of n mod 5. So, for instance, we have $\phi(7) = 2$, $\phi(8) = 3$, $\phi(7 + 8) = \phi(15) = 0$, and $\phi(7) + \phi(8) = 2 + 3 = 0$ in $\mathbb{Z}_5$. For any n, m in $\mathbb{Z}$ we can apply the division algorithm to write $n = q5 + \phi(n)$ and $m = p5 + \phi(m)$. We then have $n + m = (q + p)5 + (\phi(n) + \phi(m))$, and $\phi(n + m)$ is the sum of $\phi(n)$ and $\phi(m)$ in $\mathbb{Z}_5$, so ϕ is a homomorphism. ◇

2.2.10 PROPOSITION For any groups G, G', and G'', suppose ϕ: $G \to G'$ and ψ: $G' \to G''$ are both homomorphisms. Then the composite map $\psi \circ \phi(x) = \psi(\phi(x))$ is a homomorphism from G to G''.

Proof Consider any x, $y \in G$. We have $\psi \circ \phi(xy) = \psi(\phi(xy)) = \psi(\phi(x)\phi(y)) = \psi(\phi(x))\psi(\phi(y)) = \psi \circ \phi(x)\psi \circ \phi(y)$. □

A homomorphism ϕ: $G \to G'$ determines a special subgroup of G that plays a very important role in understanding the homomorphism.

2.2.11 DEFINITION Let ϕ: $G \to G'$ be a homomorphism and let e' be the identity in G'. Then the **kernel** of ϕ is the set $\{x \in G \mid \phi(x) = e'\}$, denoted Kern ϕ ○

2.2.12 EXAMPLE The kernel of ϕ: $\mathbb{Z} \to \mathbb{Z}_5$ in Example 2.2.9 is Kern $\phi = 5\mathbb{Z}$. ◇

2.2.13 EXAMPLE The kernel of ϕ: $\mathbb{Z} \to \langle a \rangle$ in Example 2.2.8 is Kern $\phi = \{n \mid |a| \text{ divides } n\}$. ◇

2.2.14 EXAMPLE The kernel of ϕ: $\mathbb{R}^* \to \mathbb{Z}_5$ in Example 2.2.5 is Kern $\phi = \{x \in \mathbb{R}^* \mid x \text{ is positive}\}$. ◇

After the examples we have already seen, the following list of properties of homomorphisms should not be surprising.

2.2.15 PROPOSITION (Basic group homomorphism properties) Let ϕ: $G \to G'$ be a homomorphism. Then

(1) $\phi(e) = e'$, where e is the identity of G and e' the identity of G'.

(2) $\phi(a^{-1}) = (\phi(a))^{-1}$ for any $a \in G$.

(3) $\phi(a^n) = \phi(a)^n$ for any $n \in \mathbb{Z}$.

(4) If $|a|$ is finite, then $|\phi(a)|$ divides $|a|$.

(5) If H is a subgroup of G, then $\phi(H) = \{\phi(x) \mid x \in H\}$ is a subgroup of G'.

(6) If K is a subgroup of G', then $\phi^{-1}(K) = \{x \in G \mid \phi(x) \in K\}$ is a subgroup of G.

Proof (1) Since $\phi(e)\phi(e) = \phi(ee) = \phi(e) = e'\phi(e)$, we have $\phi(e) = e'$ by cancellation.

(2) Since $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e) = e' = \phi(a)(\phi(a))^{-1}$, we have $\phi(a^{-1}) = (\phi(a))^{-1}$ by cancellation.

(3) $\phi(a^n) = \phi(a)^n$ can be proved for $n > 0$ by induction, and then the statement for $n = 0$ follows by (1) and for $n < 0$ follows by (2). (See Execise 19.)

(4) Let $|a| = n$. Then by (3) we have $\phi(a)^n = \phi(a^n) = \phi(e) = e'$. Hence by Corollary 1.3.12, $|\phi(a)|$ divides n.

(5) Let $u, v \in \phi(H) = \{u \in G' \mid u = \phi(x)$ for some $x \in H\}$, and let $x, y \in H$ be such that $u = \phi(x)$ and $v = \phi(y)$. Then $xy^{-1} \in H$ since H is a subgroup, and $uv^{-1} = \phi(x)\phi(y)^{-1} = \phi(xy^{-1}) \in \phi(H)$. Hence by the subgroup test $\phi(H)$ is a subgroup of G'.

(6) We again use the subgroup test. Let $x, y \in \phi^{-1}(K)$. We have $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} \in K$. Hence $xy^{-1} \in \phi^{-1}(K)$ and $\phi^{-1}(K)$ is a subgroup of G. □

2.2.16 PROPOSITION Let ϕ: $G \to G'$ be a homomorphism. Then Kern ϕ is a subgroup of G.

Proof This is immediate from Proposition 2.2.15, part (6). (See Exercise 20.) □

2.2.17 PROPOSITION Let ϕ: $G \to G'$ be a homomorphism. Then ϕ is one to one if and only if the kernel is trivial, Kern $\phi = \{e\}$.

Proof ($\Rightarrow$) Suppose ϕ is one to one and suppose $x \in$ Kern ϕ. Then $\phi(x) = e' = \phi(e)$, hence $x = e$ and Kern $\phi = \{e\}$.
($\Leftarrow$) Suppose Kern $\phi = \{e\}$ and suppose for some $x, y \in G$ we have $\phi(x) = \phi(y)$. Then $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = \phi(y)\phi(y)^{-1} = e'$. It follows that $xy^{-1} \in$ Kern $\phi = \{e\}$, hence $xy^{-1} = e$, so $x = y$ and ϕ is one to one. □

2.2.18 DEFINITION A homomorphism ϕ: $G \to G'$ that is one to one and onto is called an **isomorphism**. Two groups G and G' are called **isomorphic**, written $G \cong G'$, if there exists some isomorphism ϕ: $G \to G'$. ○

To show that two groups G and G' are isomorphic, we need to do four things:

(1) Define a map ϕ: $G \to G'$.

(2) Show that ϕ is a homomorphism.

(3) Show that ϕ is one to one.

(4) Show that ϕ is onto.

The following example illustrates these four steps.

2.2.19 EXAMPLE $\mathbb{Z}$ and $3\mathbb{Z}$ are isomorphic groups. We carry out the four steps just indicated:

(1) Define $\phi: \mathbb{Z} \to 3\mathbb{Z}$ by $\phi(x) = 3x$.

(2) We have $\phi(x + y) = 3(x + y) = 3x + 3y = \phi(x) + \phi(y)$, so ϕ is a homomorphism.

(3) $\phi(x) = 0$ if and only if $3x = 0$, hence if and only if $x = 0$. So Kern $\phi = \{0\}$ and by Proposition 2.2.17 ϕ is one to one.

(4) Given $u \in 3\mathbb{Z}$, $u = 3x$ for some $x \in \mathbb{Z}$, so $u = \phi(x)$, and ϕ is onto. ◇

2.2.20 EXAMPLE $\mathbb{R}$, the real numbers under addition, is isomorphic to $\mathbb{R}^+$, the positive real numbers under multiplication. Again we carry out four steps to verify this claim:

(1) Let $\phi: \mathbb{R} \to \mathbb{R}^+$ be the exponential function $\phi(x) = \exp x = e^x$.

(2) $\phi(x + y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$, so ϕ is a homomorphism.

(3) The identity element in $\mathbb{R}^+$ is 1. Hence if $x \in$ Kern ϕ, then $\phi(x) = 1$, which is to say $e^x = 1$, which implies $x = 0$. So Kern $\phi = \{0\}$ and ϕ is one to one.

(4) For $u \in \mathbb{R}^+$, let $x = \ln u$, the natural logarithm of u. Then $\phi(x) = e^x = e^{\ln u} = u$, and ϕ is onto. ◇

2.2.21 EXAMPLE In Example 2.2.19, the map $\phi^{-1}: 3\mathbb{Z} \to \mathbb{Z}$, with $\phi^{-1}(u) = u/3$, is an isomorphism between $3\mathbb{Z}$ to $\mathbb{Z}$. In Example 2.2.20, the map $\phi^{-1}: \mathbb{R}^+ \to \mathbb{R}$, with $\phi^{-1}(u) = \ln u$, is an isomorphism between $\mathbb{R}^+$ and $\mathbb{R}$. ◇

2.2.22 PROPOSITION Let $\phi: G \to G'$ and $\psi: G' \to G''$ be isomorphisms. Then

(1) The composition $\psi \circ \phi: G \to G''$ is an isomorphism.

(2) The identity map $\phi: G \to G$ is an isomorphism.

(3) The inverse $\phi^{-1}: G' \to G$ is an isomorphism.

Proof (1) $\psi \circ \phi$ is a homomorphism by Proposition 2.2.10, and we know from Theorem 0.1.15 that a composition of one-to-one maps is one to one, and a composition of onto maps is onto.

(2) and (3) are left to the reader (as Exercise 21). □

2.2.23 PROPOSITION Let $G \cong G'$. Then

(1) $|G| = |G'|$.

(2) G is Abelian if and only if G' is Abelian.

(3) G is cyclic if and only if G' is cyclic.

(4) G has k elements of order n if and only if G' has k elements of order n.

Proof Let $\phi: G \to G'$ be an isomorphism.

(1) Since ϕ is a one-to-one and onto map between G and G', $|G| = |G'|$.

(2) Suppose G is Abelian and let $u, v \in G'$. Since ϕ is onto, there are $x, y \in G$ with $\phi(x) = u$, $\phi(y) = v$.

Then $uv = \phi(x)\phi(y) = \phi(xy)$ and $\phi(xy) = \phi(yx) = \phi(y)\phi(x) = vu$ since G is Abelian. So $uv = vu$ and G' is Abelian. If G' is Abelian, then, $\phi(xy) = \phi(x)\phi(y) = \phi(y)\phi(x) = \phi(yx)$, and since ϕ is one to one, $xy = yx$ and G is Abelian.

Before proving (3) and (4), we note the following:

Claim For any $a \in G$, $|a| = |\phi(a)|$.

Proof of Claim Suppose a is an element of order n in G, and let m be the order of $\phi(a)$ in G'. By Proposition 2.2.15, part (4), m divides $|a| = n$. But since $\phi(a^m) = \phi(a)^m = e'$, the identity of G', and since ϕ is one to one, we must have $a^m = e$, and so $n = |a|$ divides m. Thus a and $\phi(a)$ have the same order $n = m$.

(3) If $G = \langle a \rangle$ is cyclic, then by the claim $|\phi(a)| = |a| = |G| = |G'|$, so $G' = \langle \phi(a) \rangle$ and is cyclic. If $G' = \langle b \rangle$ and is cyclic, then since ϕ is onto there is an $a \in G$ with $\phi(a) = b$. But then $|a| = |\phi(a)| = |b| = |G'| = |G|$, and $G = \langle a \rangle$ and is cyclic.

(4) Suppose $a_1, a_2, \ldots, a_k$ are k distinct elements of order n in G. Then since ϕ is one to one, $\phi(a_1), \phi(a_2), \ldots, \phi(a_k)$ are all distinct, and by the claim, are all of order n. If $a_1, a_2, \ldots, a_k$ are *all* the elements of G of order n, then $\phi(a_1), \phi(a_2), \ldots, \phi(a_k)$ will be *all* the elements of G' of order n. For consider any other element u of G'. Since ϕ is onto, $u = \phi(x)$ for some $x \in G$, and u is distinct from all the $\phi(a_i)$, x is distinct from all the a_i. Since the a_i were all the elements of G of order n, we have $|u| = |\phi(x)| = |x| \neq n$. □

2.2.24 LEMMA Let G and H be cyclic groups of the same finite order n, and let a be any generator of G and b any generator of H. Then there is an isomorphism $\phi: G \to H$ with $\phi(a) = b$.

Proof We have $G = \langle a \rangle$, where $|G| = n$, so by Corollary 1.3.13

$$G = \{e, a, a^2, \ldots, a^{n-1}\}$$

where these elements are all distinct. Define a map $\phi: G \to H$ by $\phi(a^i) = b^i$ for $0 \leq i < n$.

Claim ϕ is an isomorphism.

Poof of Claim Left to the reader (as Exercise 39). □

2.2.25 PROPOSITION Let $G = \langle a \rangle$ be a cyclic group. Then

(1) If $|G| = \infty$, then $G \cong \mathbb{Z}$.

(2) If $|G| = n$, then $G \cong \mathbb{Z}_n$.

Proof (1)If $G = \langle a \rangle$, where $|a| = \infty$, let $\phi: \mathbb{Z} \to G$ be the exponential homomorphism as in Example 2.2.8, defined by $\phi(k) = a^k$. Since $|a| = \infty$, $a^k = e$ if and only if $k = 0$. Hence Kern $\phi = \{0\}$ and ϕ is one to one. Since G is cyclic, every $u \in G$ is of the form $u = a^k$ for some $k \in \mathbb{Z}$. Hence $u = \phi(k)$ and ϕ is onto. So ϕ is an isomorphism from $\mathbb{Z}$ to G, and by Proposition 2.2.22, ϕ^{-1} is an isomorphism from G to $\mathbb{Z}$.

(2) This is immediate from the preceding lemma. □

2.2.26 EXAMPLE D_4 and $\mathbb{Z}_8$ are not isomorphic, because D_4 is non-Abelian, and $\mathbb{Z}_8$ is Abelian. ◇

2.2.27 EXAMPLE $U(10) = \{1, 3, 7, 9\}$ and $U(12) = \{1, 5, 7, 11\}$ are not isomorphic, because $U(10)$ is cyclic and $U(12)$ is noncyclic. ◇

2.2.28 EXAMPLE $\mathbb{Q}$ under addition is not isomorphic to $\mathbb{Q}^*$ under multiplication. For suppose there is an isomorphism $\phi: \mathbb{Q} \to \mathbb{Q}^*$. Since ϕ is onto, there exists some $a \in \mathbb{Q}$ such that $\phi(a) = 2$. Consider the rational number $r = \phi(a/2)$. We have $r^2 = \phi(a/2)\phi(a/2) = \phi(a/2 + a/2) = \phi(a) = 2$, which is impossible. ◇

Exercises 2.2

In Exercises 1 through 10, determine whether or not the indicated map ϕ is a homomorphism, and in the cases where ϕ is a homomorphism, determine Kern ϕ.

1. $\phi: \mathbb{Z} \to \mathbb{Z}$, where $\phi(n) = n - 1$

2. $\phi: \mathbb{Z} \to \mathbb{Z}$, where $\phi(n) = 3n$

3. $\phi: \mathbb{R}^* \to \mathbb{R}^*$ (under multiplication), where $\phi(x) = |x|$

4. ϕ: GL(2,$\mathbb{R}$) $\to \mathbb{R}^*$, where GL(2, $\mathbb{R}$) is the general linear group of 2×2 invertible matrices and $\phi(A) = \det A$

5. $\phi: S_3 \to \mathbb{Z}_2$, where

$$\phi(\sigma) = \begin{cases} 0 \text{ if } \sigma \text{ is an even permutation} \\ 1 \text{ if } \sigma \text{ is an odd permutation} \end{cases}$$

6. $\phi: D_4 \to \mathbb{Z}_2$, where $D_4 = \{\rho_0, \rho, \rho^2, \rho^3, \tau, \rho\tau, \rho^2\tau, \rho^3\tau\}$ is the dihedral group, and $\phi(\rho^i) = 0$, $\phi(\rho^i\tau) = 1$, for all i, $0 \le i \le 3$

7. $\phi: \mathbb{R} \to$ GL(2, $\mathbb{R}$), where $\mathbb{R}$ is the group of real numbers under addition, GL(2, $\mathbb{R}$) is as in Exercise 4, and

$$\phi(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$

8. $\phi: G \to G$, where G is any group, and $\phi(x) = x^{-1}$

9. $\phi: \mathbb{Z}_6 \to \mathbb{Z}_2$, where $\phi(x)$ = the remainder of x mod 2

10. $\phi: \mathbb{Z}_7 \to \mathbb{Z}_2$, where $\phi(x)$ = the remainder of x mod 2

In Exercises 11 through 15, compute the indicated values for the indicated homomorphisms.

11. $\phi(27)$, where $\phi: \mathbb{Z} \to \mathbb{Z}_5$ is as in Example 2.2.9