11

Homomorphisms

One of the basic ideas of algebra is the concept of a homomorphism, a natural generalization of an isomorphism. If we relax the requirement that an isomorphism of groups be bijective, we have a homomorphism.

11.1 Group Homomorphisms

A ***homomorphism*** between groups $(G, \cdot)$ and $(H, \circ)$ is a map $\phi : G \to H$ such that

$$\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2)$$

for $g_1, g_2 \in G$. The range of ϕ in H is called the ***homomorphic image*** of ϕ.

Two groups are related in the strongest possible way if they are isomorphic; however, a weaker relationship may exist between two groups. For example, the symmetric group S_n and the group $\mathbb{Z}_2$ are related by the fact that S_n can be divided into even and odd permutations that exhibit a group structure like that $\mathbb{Z}_2$, as shown in the following multiplication table.

	even	odd
even	even	odd
odd	odd	even

We use homomorphisms to study relationships such as the one we have just described.

Example 11.1 Let G be a group and $g \in G$. Define a map $\phi : \mathbb{Z} \to G$ by $\phi(n) = g^n$. Then ϕ is a group homomorphism, since

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n).$$

This homomorphism maps $\mathbb{Z}$ onto the cyclic subgroup of G generated by g. $\square$

Example 11.2 Let $G = GL_2(\mathbb{R})$. If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in G, then the determinant is nonzero; that is, $\det(A) = ad - bc \neq 0$. Also, for any two elements A and B in G, $\det(AB) = \det(A)\det(B)$.

Using the determinant, we can define a homomorphism $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ by $A \mapsto \det(A)$. $\square$

Example 11.3 Recall that the circle group $\mathbb{T}$ consists of all complex numbers z such that $|z| = 1$. We can define a homomorphism ϕ from the additive group of real numbers $\mathbb{R}$ to $\mathbb{T}$ by $\phi : \theta \mapsto \cos\theta + i \sin\theta$. Indeed,

$$\begin{aligned}
\phi(\alpha + \beta) &= \cos(\alpha + \beta) + i \sin(\alpha + \beta) \\
&= (\cos\alpha \cos\beta - \sin\alpha \sin\beta) + i(\sin\alpha \cos\beta + \cos\alpha \sin\beta) \\
&= (\cos\alpha + i \sin\alpha)(\cos\beta + i \sin\beta) \\
&= \phi(\alpha)\phi(\beta).
\end{aligned}$$

Geometrically, we are simply wrapping the real line around the circle in a group-theoretic fashion. $\square$

The following proposition lists some basic properties of group homomorphisms.

Proposition 11.4 *Let $\phi : G_1 \to G_2$ be a homomorphism of groups. Then*

1. *If e is the identity of G_1, then $\phi(e)$ is the identity of G_2;*
2. *For any element $g \in G_1$, $\phi(g^{-1}) = [\phi(g)]^{-1}$;*
3. *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2;*
4. *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2) = \{g \in G_1 : \phi(g) \in H_2\}$ is a subgroup of G_1. Furthermore, if H_2 is normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.*

Proof. (1) Suppose that e and e' are the identities of G_1 and G_2, respectively; then

$$e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e).$$

By cancellation, $\phi(e) = e'$.

(2) This statement follows from the fact that

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

(3) The set $\phi(H_1)$ is nonempty since the identity of G_2 is in $\phi(H_1)$. Suppose that H_1 is a subgroup of G_1 and let x and y be in $\phi(H_1)$. There exist elements $a, b \in H_1$ such that $\phi(a) = x$ and $\phi(b) = y$. Since

$$xy^{-1} = \phi(a)[\phi(b)]^{-1} = \phi(ab^{-1}) \in \phi(H_1),$$

$\phi(H_1)$ is a subgroup of G_2 by Proposition 3.31, p. 40.

(4) Let H_2 be a subgroup of G_2 and define H_1 to be $\phi^{-1}(H_2)$; that is, H_1 is the set of all $g \in G_1$ such that $\phi(g) \in H_2$. The identity is in H_1 since $\phi(e) = e'$. If a and b are in H_1, then $\phi(ab^{-1}) = \phi(a)[\phi(b)]^{-1}$ is in H_2 since H_2 is a subgroup of G_2. Therefore, $ab^{-1} \in H_1$ and H_1 is a subgroup of G_1. If H_2 is normal in G_2, we must show that $g^{-1}hg \in H_1$ for $h \in H_1$ and $g \in G_1$. But

$$\phi(g^{-1}hg) = [\phi(g)]^{-1}\phi(h)\phi(g) \in H_2,$$

since H_2 is a normal subgroup of G_2. Therefore, $g^{-1}hg \in H_1$. $\blacksquare$

Let $\phi : G \to H$ be a group homomorphism and suppose that e is the identity of H. By Proposition 11.4, p. 140, $\phi^{-1}(\{e\})$ is a subgroup of G. This subgroup is called the ***kernel*** of ϕ and will be denoted by $\ker\phi$. In fact, this subgroup is a normal subgroup of G since the trivial subgroup is normal in H. We state this result in the following theorem, which says that with every homomorphism of groups we can naturally associate a normal subgroup.

Theorem 11.5 *Let $\phi : G \to H$ be a group homomorphism. Then the kernel of ϕ is a normal subgroup of G.*

Example 11.6 Let us examine the homomorphism $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ defined by $A \mapsto \det(A)$. Since 1 is the identity of $\mathbb{R}^*$, the kernel of this homomorphism is all 2×2 matrices having determinant one. That is, $\ker \phi = SL_2(\mathbb{R})$. □

Example 11.7 The kernel of the group homomorphism $\phi : \mathbb{R} \to \mathbb{C}^*$ defined by $\phi(\theta) = \cos\theta + i \sin\theta$ is $\{2\pi n : n \in \mathbb{Z}\}$. Notice that $\ker \phi \cong \mathbb{Z}$. □

Example 11.8 Suppose that we wish to determine all possible homomorphisms ϕ from $\mathbb{Z}_7$ to $\mathbb{Z}_{12}$. Since the kernel of ϕ must be a subgroup of $\mathbb{Z}_7$, there are only two possible kernels, $\{0\}$ and all of $\mathbb{Z}_7$. The image of a subgroup of $\mathbb{Z}_7$ must be a subgroup of $\mathbb{Z}_{12}$. Hence, there is no injective homomorphism; otherwise, $\mathbb{Z}_{12}$ would have a subgroup of order 7, which is impossible. Consequently, the only possible homomorphism from $\mathbb{Z}_7$ to $\mathbb{Z}_{12}$ is the one mapping all elements to zero. □

Example 11.9 Let G be a group. Suppose that $g \in G$ and ϕ is the homomorphism from $\mathbb{Z}$ to G given by $\phi(n) = g^n$. If the order of g is infinite, then the kernel of this homomorphism is $\{0\}$ since ϕ maps $\mathbb{Z}$ onto the cyclic subgroup of G generated by g. However, if the order of g is finite, say n, then the kernel of ϕ is $n\mathbb{Z}$. □

11.2 The Isomorphism Theorems

Although it is not evident at first, factor groups correspond exactly to homomorphic images, and we can use factor groups to study homomorphisms. We already know that with every group homomorphism $\phi : G \to H$ we can associate a normal subgroup of G, $\ker \phi$. The converse is also true; that is, every normal subgroup of a group G gives rise to homomorphism of groups.

Let H be a normal subgroup of G. Define the ***natural*** or ***canonical homomorphism***

$$\phi : G \to G/H$$

by

$$\phi(g) = gH.$$

This is indeed a homomorphism, since

$$\phi(g_1 g_2) = g_1 g_2 H = g_1 H g_2 H = \phi(g_1)\phi(g_2).$$

The kernel of this homomorphism is H. The following theorems describe the relationships between group homomorphisms, normal subgroups, and factor groups.

Theorem 11.10 **First Isomorphism Theorem.** *If $\psi : G \to H$ is a group homomorphism with $K = \ker \psi$, then K is normal in G. Let $\phi : G \to G/K$ be the canonical homomorphism. Then there exists a unique isomorphism $\eta : G/K \to \psi(G)$ such that $\psi = \eta\phi$.*

Proof. We already know that K is normal in G. Define $\eta : G/K \to \psi(G)$ by $\eta(gK) = \psi(g)$. We first show that η is a well-defined map. If $g_1K = g_2K$, then for some $k \in K$, $g_1k = g_2$; consequently,

$$\eta(g_1K) = \psi(g_1) = \psi(g_1)\psi(k) = \psi(g_1k) = \psi(g_2) = \eta(g_2K).$$

Thus, η does not depend on the choice of coset representatives and the map $\eta : G/K \to \psi(G)$ is uniquely defined since $\psi = \eta\phi$. We must also show that η is a homomorphism. Indeed,

$$\begin{aligned} \eta(g_1Kg_2K) &= \eta(g_1g_2K) \\ &= \psi(g_1g_2) \\ &= \psi(g_1)\psi(g_2) \\ &= \eta(g_1K)\eta(g_2K). \end{aligned}$$

Clearly, η is onto $\psi(G)$. To show that η is one-to-one, suppose that $\eta(g_1K) = \eta(g_2K)$. Then $\psi(g_1) = \psi(g_2)$. This implies that $\psi(g_1^{-1}g_2) = e$, or $g_1^{-1}g_2$ is in the kernel of ψ; hence, $g_1^{-1}g_2K = K$; that is, $g_1K = g_2K$. ■

Mathematicians often use diagrams called ***commutative diagrams*** to describe such theorems. The following diagram "commutes" since $\psi = \eta\phi$.

$$\begin{tikzcd} G \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & H \\ & G/K \arrow[ur, "\eta"'] & \end{tikzcd}$$

Example 11.11 Let G be a cyclic group with generator g. Define a map $\phi : \mathbb{Z} \to G$ by $n \mapsto g^n$. This map is a surjective homomorphism since

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n).$$

Clearly ϕ is onto. If $|g| = m$, then $g^m = e$. Hence, $\ker\phi = m\mathbb{Z}$ and $\mathbb{Z}/\ker\phi = \mathbb{Z}/m\mathbb{Z} \cong G$. On the other hand, if the order of g is infinite, then $\ker\phi = 0$ and ϕ is an isomorphism of G and $\mathbb{Z}$. Hence, two cyclic groups are isomorphic exactly when they have the same order. Up to isomorphism, the only cyclic groups are $\mathbb{Z}$ and $\mathbb{Z}_n$. □

Theorem 11.12 Second Isomorphism Theorem. *Let H be a subgroup of a group G (not necessarily normal in G) and N a normal subgroup of G. Then HN is a subgroup of G, $H \cap N$ is a normal subgroup of H, and*

$$H/H \cap N \cong HN/N.$$

Proof. We will first show that $HN = \{hn : h \in H, n \in N\}$ is a subgroup of G. Suppose that $h_1n_1, h_2n_2 \in HN$. Since N is normal, $(h_2)^{-1}n_1h_2 \in N$. So

$$(h_1n_1)(h_2n_2) = h_1h_2((h_2)^{-1}n_1h_2)n_2$$

is in HN. The inverse of $hn \in HN$ is in HN since

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1}).$$

Next, we prove that $H \cap N$ is normal in H. Let $h \in H$ and $n \in H \cap N$. Then $h^{-1}nh \in H$ since each element is in H. Also, $h^{-1}nh \in N$ since N is normal in G; therefore, $h^{-1}nh \in H \cap N$.

Now define a map ϕ from H to HN/N by $h \mapsto hN$. The map ϕ is onto, since any coset $hnN = hN$ is the image of h in H. We also know that ϕ is a homomorphism because

$$\phi(hh') = hh'N = hNh'N = \phi(h)\phi(h').$$

By the First Isomorphism Theorem, the image of ϕ is isomorphic to $H/\ker\phi$; that is,

$$HN/N = \phi(H) \cong H/\ker\phi.$$

Since

$$\ker\phi = \{h \in H : h \in N\} = H \cap N,$$

$HN/N = \phi(H) \cong H/H \cap N$. ■

Theorem 11.13 Correspondence Theorem. *Let N be a normal subgroup of a group G. Then $H \mapsto H/N$ is a one-to-one correspondence between the set of subgroups H containing N and the set of subgroups of G/N. Furthermore, the normal subgroups of G containing N correspond to normal subgroups of G/N.*

Proof. Let H be a subgroup of G containing N. Since N is normal in H, H/N makes is a factor group. Let aN and bN be elements of H/N. Then $(aN)(b^{-1}N) = ab^{-1}N \in H/N$; hence, H/N is a subgroup of G/N.

Let S be a subgroup of G/N. This subgroup is a set of cosets of N. If $H = \{g \in G : gN \in S\}$, then for $h_1, h_2 \in H$, we have that $(h_1N)(h_2N) = h_1h_2N \in S$ and $h_1^{-1}N \in S$. Therefore, H must be a subgroup of G. Clearly, H contains N. Therefore, $S = H/N$. Consequently, the map $H \mapsto H/N$ is onto.

Suppose that H_1 and H_2 are subgroups of G containing N such that $H_1/N = H_2/N$. If $h_1 \in H_1$, then $h_1N \in H_1/N$. Hence, $h_1N = h_2N \subset H_2$ for some h_2 in H_2. However, since N is contained in H_2, we know that $h_1 \in H_2$ or $H_1 \subset H_2$. Similarly, $H_2 \subset H_1$. Since $H_1 = H_2$, the map $H \mapsto H/N$ is one-to-one.

Suppose that H is normal in G and N is a subgroup of H. Then it is easy to verify that the map $G/N \to G/H$ defined by $gN \mapsto gH$ is a homomorphism. The kernel of this homomorphism is H/N, which proves that H/N is normal in G/N.

Conversely, suppose that H/N is normal in G/N. The homomorphism given by

$$G \to G/N \to \frac{G/N}{H/N}$$

has kernel H. Hence, H must be normal in G. ■

Notice that in the course of the proof of Theorem 11.13, p. 143, we have also proved the following theorem.

Theorem 11.14 Third Isomorphism Theorem. *Let G be a group and N and H be normal subgroups of G with $N \subset H$. Then*

$$G/H \cong \frac{G/N}{H/N}.$$

Example 11.15 By the Third Isomorphism Theorem,

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}).$$

Since $|\mathbb{Z}/mn\mathbb{Z}| = mn$ and $|\mathbb{Z}/m\mathbb{Z}| = m$, we have $|m\mathbb{Z}/mn\mathbb{Z}| = n$. $\square$

Sage. Sage can create homomorphisms between groups, which can be used directly as functions, and then queried for their kernels and images. So there is great potential for exploring the many fundamental relationships between groups, normal subgroups, quotient groups and properties of homomorphisms.

11.3 Exercises

1. Prove that $\det(AB) = \det(A)\det(B)$ for $A, B \in GL_2(\mathbb{R})$. This shows that the determinant is a homomorphism from $GL_2(\mathbb{R})$ to $\mathbb{R}^*$.

2. Which of the following maps are homomorphisms? If the map is a homomorphism, what is the kernel?

(a) $\phi : \mathbb{R}^* \to GL_2(\mathbb{R})$ defined by

$$\phi(a) = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$$

(b) $\phi : \mathbb{R} \to GL_2(\mathbb{R})$ defined by

$$\phi(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

(c) $\phi : GL_2(\mathbb{R}) \to \mathbb{R}$ defined by

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a + d$$

(d) $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ defined by

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ad - bc$$

(e) $\phi : \mathbb{M}_2(\mathbb{R}) \to \mathbb{R}$ defined by

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = b,$$

where $\mathbb{M}_2(\mathbb{R})$ is the additive group of 2×2 matrices with entries in $\mathbb{R}$.

3. Let A be an $m \times n$ matrix. Show that matrix multiplication, $x \mapsto Ax$, defines a homomorphism $\phi : \mathbb{R}^n \to \mathbb{R}^m$.

4. Let $\phi : \mathbb{Z} \to \mathbb{Z}$ be given by $\phi(n) = 7n$. Prove that ϕ is a group homomorphism. Find the kernel and the image of ϕ.

5. Describe all of the homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$.

6. Describe all of the homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}_{12}$.

7. In the group $\mathbb{Z}_{24}$, let $H = \langle 4 \rangle$ and $N = \langle 6 \rangle$.

(a) List the elements in HN (we usually write $H + N$ for these additive groups) and $H \cap N$.

(b) List the cosets in HN/N, showing the elements in each coset.

(c) List the cosets in $H/(H \cap N)$, showing the elements in each coset.

(d) Give the correspondence between HN/N and $H/(H \cap N)$ described in the proof of the Second Isomorphism Theorem.

8. If G is an abelian group and $n \in \mathbb{N}$, show that $\phi : G \to G$ defined by $g \mapsto g^n$ is a group homomorphism.

9. If $\phi : G \to H$ is a group homomorphism and G is abelian, prove that $\phi(G)$ is also abelian.

10. If $\phi : G \to H$ is a group homomorphism and G is cyclic, prove that $\phi(G)$ is also cyclic.

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

12. If a group G has exactly one subgroup H of order k, prove that H is normal in G.

13. Prove or disprove: $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}$.

14. Let G be a finite group and N a normal subgroup of G. If H is a subgroup of G/N, prove that $\phi^{-1}(H)$ is a subgroup in G of order $|H| \cdot |N|$, where $\phi : G \to G/N$ is the canonical homomorphism.

15. Let G_1 and G_2 be groups, and let H_1 and H_2 be normal subgroups of G_1 and G_2 respectively. Let $\phi : G_1 \to G_2$ be a homomorphism. Show that ϕ induces a homomorphism $\overline{\phi} : (G_1/H_1) \to (G_2/H_2)$ if $\phi(H_1) \subset H_2$.

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

17. Let $\phi : G_1 \to G_2$ be a surjective group homomorphism. Let H_1 be a normal subgroup of G_1 and suppose that $\phi(H_1) = H_2$. Prove or disprove that $G_1/H_1 \cong G_2/H_2$.

18. Let $\phi : G \to H$ be a group homomorphism. Show that ϕ is one-to-one if and only if $\phi^{-1}(e) = \{e\}$.

19. Given a homomorphism $\phi : G \to H$ define a relation $\sim$ on G by $a \sim b$ if $\phi(a) = \phi(b)$ for $a, b \in G$. Show this relation is an equivalence relation and describe the equivalence classes.

11.4 Additional Exercises: Automorphisms

1. Let $\text{Aut}(G)$ be the set of all automorphisms of G; that is, isomorphisms from G to itself. Prove this set forms a group and is a subgroup of the group of permutations of G; that is, $\text{Aut}(G) \leq S_G$.

2. An ***inner automorphism*** of G,

$$i_g : G \to G,$$

is defined by the map

$$i_g(x) = gxg^{-1},$$

for $g \in G$. Show that $i_g \in \text{Aut}(G)$.

3. The set of all inner automorphisms is denoted by $\mathrm{Inn}(G)$. Show that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$.

4. Find an automorphism of a group G that is not an inner automorphism.

5. Let G be a group and i_g be an inner automorphism of G, and define a map

$$G \to \mathrm{Aut}(G)$$

by

$$g \mapsto i_g.$$

Prove that this map is a homomorphism with image $\mathrm{Inn}(G)$ and kernel $Z(G)$. Use this result to conclude that

$$G/Z(G) \cong \mathrm{Inn}(G).$$

6. Compute $\mathrm{Aut}(S_3)$ and $\mathrm{Inn}(S_3)$. Do the same thing for D_4.

7. Find all of the homomorphisms $\phi : \mathbb{Z} \to \mathbb{Z}$. What is $\mathrm{Aut}(\mathbb{Z})$?

8. Find all of the automorphisms of $\mathbb{Z}_8$. Prove that $\mathrm{Aut}(\mathbb{Z}_8) \cong U(8)$.

9. For $k \in \mathbb{Z}_n$, define a map $\phi_k : \mathbb{Z}_n \to \mathbb{Z}_n$ by $a \mapsto ka$. Prove that ϕ_k is a homomorphism.

10. Prove that ϕ_k is an isomorphism if and only if k is a generator of $\mathbb{Z}_n$.

11. Show that every automorphism of $\mathbb{Z}_n$ is of the form ϕ_k, where k is a generator of $\mathbb{Z}_n$.

12. Prove that $\psi : U(n) \to \mathrm{Aut}(\mathbb{Z}_n)$ is an isomorphism, where $\psi : k \mapsto \phi_k$.