5 *Homomorphisms*

Last Updated: 13 February 2023

Recognizing the maps that preserve a mathematical structure is as essential as defining the objects themselves. Many constructions are conveniently expressed and unified when visualized in terms of objects and the structure-preserving maps between them.

5.0 Ring homomorphisms

Which maps preserve ring structures? To be compatible with ring structures, a map must align addition, multiplication, additive identities, and multiplicative identities in the source and target. However, the formal definition just requires the following.

The word "homomorphism" comes from the Greek prefix *homos* meaning 'same' and the Greek suffix *morphe* meaning 'form' or 'shape'. This term appeared as early as 1892 and was attributed to the German mathematician Felix Klein.

Definition 5.0.0. Let R and S be two rings. A map $\varphi\colon R \to S$ is a ***ring homomorphism*** if, for all elements a and b in R, we have

$$\varphi(a+b) = \varphi(a) + \varphi(b)\,, \quad \varphi(a\,b) = \varphi(a)\,\varphi(b)\,, \quad \text{and} \quad \varphi(1_R) = 1_S\,.$$

A homomorphism from a ring R to itself an *endomorphism*.

We frequently omit the adjective 'ring' when it is clear from the context.

Problem 5.0.1. Let R be a ring and let u be a unit in R. Confirm that the map $\varphi\colon R \to R$ defined, for any element a in the ring R, by $\varphi(a) = u\,a\,u^{-1}$ is an endomorphism.

When R is a commutative ring, this endomorphism is the identity map.

Solution. For any elements a and b in the ring R, we have

$$\begin{aligned} \varphi(a+b) &= u\,(a+b)\,u^{-1} = u\,a\,u^{-1} + u\,b\,u^{-1} = \varphi(a) + \varphi(b)\,, \\ \varphi(a\,b) &= u\,(a\,b)\,u^{-1} = (u\,a\,u^{-1})\,(u\,b\,u^{-1}) = \varphi(a)\,\varphi(b)\,, \end{aligned}$$

and $\varphi(1) = u\,1\,u^{-1} = 1$, so φ is a ring homomorphism. □

Example 5.0.2. Let R be a commutative ring. For any element b in R, the evaluation map $\operatorname{ev}_b\colon R[x] \to R$ described in Definition 4.0.7 is a ring homomorphism.

The evaluation map is *not* ring homomorphism from $R \times R[x]$ to R because there is an $m \in \mathbb{N}$ such that $\operatorname{ev}_{a+b}(x^m) \neq \operatorname{ev}_a(x^m) + \operatorname{ev}_b(x^m)$.

Ring homomorphisms implicitly preserve the additive identity.

Lemma 5.0.3. *Any ring homomorphism $\varphi\colon R \to S$ satisfies $\varphi(0_R) = 0_S$.*

Proof. The properties of the additive identity and a homomorphism give $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$. Adding the additive inverse $-\varphi(0_R)$ to both sides yields

$$\begin{aligned} 0_S = \varphi(0_R) - \varphi(0_R) &= \varphi(0_R) + \varphi(0_R) - \varphi(0_R) \\ &= \varphi(0_R) + 0_S = \varphi(0_R)\,. \end{aligned}$$ □

Ring homomorphisms elevate the integers as a special source.

Problem 5.0.4. Let R be a ring. Show that there is a unique ring homomorphism from $\mathbb{Z}$ to R.

The identity map is the unique ring endomorphism of $\mathbb{Z}$.

Solution. Let $\varphi\colon \mathbb{Z} \to R$ be a ring homomorphism. For any nonnegative integer m, we first prove, by induction on m, that

$$\varphi(m) = m\,1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{m \text{ times}} = \sum_{j=1}^{m} 1_R\,.$$

Lemma 5.0.3 establishes that $\varphi(0) = 0_R$, so the base case holds. Assume that $\varphi(m) = m\,1_R$. The properties of a ring homomorphism give $\varphi(m+1) = \varphi(m) + \varphi(1) = m\,1_R + 1_R = (m+1)\,1_R$ completing the induction step. For negative integers, we have

$$0_R = \varphi(0) = \varphi(m-m) = \varphi(m) + \varphi(-m) = m\,1_R + \varphi(-m)\,.$$

We deduce that $\varphi(-m) = -m\,1_R = m\,(-1_R)$. Since associativity of addition in R implies that $(m\,n)\,1_R = (m\,1_R)(n\,1_R)$, we see that the map defined by $m \mapsto m\,1_R$ is also compatible with multiplication. Therefore, the only ring homomorphism from $\mathbb{Z}$ to R satisfies $m \mapsto m\,1_R$ for all integers m. $\square$

Problem 5.0.5. Show that complex conjugation determines an endomorphism of $\mathbb{C}$.

Solution. For any complex numbers $z = a + b\,\mathrm{i}$ and $w = c + d\,\mathrm{i}$ where a, b, c, and d are real numbers, we have

$$\begin{aligned}
\overline{z+w} = \overline{(a+c) + (b+d)\,\mathrm{i}} &= (a+c) - (b+d)\,\mathrm{i} \\
&= (a - b\,\mathrm{i}) + (c - d\,\mathrm{i}) = \overline{z} + \overline{w}\,, \\
\overline{z\,w} = \overline{(ac-bd) + (ad+bd)\,\mathrm{i}} &= (ac-bd) - (ad+bd)\,\mathrm{i} \\
&= (a - b\,\mathrm{i})(c - d\,\mathrm{i}) = \overline{z}\,\overline{w}\,,
\end{aligned}$$

and $\overline{1} = \overline{1 + 0\,\mathrm{i}} = 1 - 0\,\mathrm{i} = 1$. $\square$

Problem 5.0.6. Let ℓ be a positive integer. Prove that there are no ring homomorphisms from the quotient $\mathbb{Z}/\langle \ell \rangle$ to $\mathbb{Z}$.

Solution. Suppose that $\varphi\colon \mathbb{Z}/\langle \ell \rangle \to \mathbb{Z}$ is a ring homomorphism. Lemma 5.0.3 and the definition of a ring homomorphism imply that $\varphi([0]_\ell) = 0$ and $\varphi([1]_\ell) = 1$. However, we would have

$$\ell = \sum_{j=1}^{\ell} 1 = \sum_{j=1}^{\ell} \varphi([1]_\ell) = \varphi\left(\sum_{j=1}^{\ell} [1]_\ell\right) = \varphi([\ell]_\ell) = \varphi([0]_\ell) = 0\,,$$

which is a contradiction. $\square$

The family of all ring homomorphisms has a few key properties.

Proposition 5.0.7. *Let Q, R, S, and T be rings.*

(i) *The identity function $\mathrm{id}_R\colon R \to R$ is a ring homomorphism.*
(ii) *For any two ring homomorphisms $\varphi\colon R \to S$ and $\psi\colon S \to T$, the composition $\psi\,\varphi\colon R \to T$ is also a ring homomorphism.*
(iii) *For any three ring homomorphisms $\theta\colon Q \to R$, $\varphi\colon R \to S$, and $\psi\colon S \to T$, we have $\psi\,(\varphi\,\theta) = (\psi\,\varphi)\,\theta$.*

Proof. Let a and b be elements in the ring R.

(i) Since

$$\mathrm{id}_R(a+b) = a+b = \mathrm{id}_R(a) + \mathrm{id}_R(b) \qquad \mathrm{id}_R(1_R) = 1_R$$
$$\mathrm{id}_R(a\,b) = a\,b = \mathrm{id}_R(a)\,\mathrm{id}_R(b)$$

the identity map is a ring homomorphism.

(ii) Since

$$\begin{aligned}(\psi\,\varphi)(a+b) &= \psi\big(\varphi(a+b)\big) = \psi\big(\varphi(a)+\varphi(b)\big)\\ &= \psi\big(\varphi(a)\big) + \psi\big(\varphi(b)\big) = (\psi\,\varphi)(a) + (\psi\,\varphi)(b)\\ (\psi\,\varphi)(a\,b) &= \psi\big(\varphi(a\,b)\big) = \psi\big(\varphi(a)\,\varphi(b)\big)\\ &= \psi\big(\varphi(a)\big)\,\psi\big(\varphi(b)\big) = (\psi\,\varphi)(a)\,(\psi\,\varphi)(b)\\ (\psi\,\varphi)(1_R) &= \psi\big(\varphi(1_R)\big) = \psi(1_S) = 1_T\end{aligned}$$

the composition $\psi\,\varphi$ is a ring homomorphism.

(iii) Composition of functions is associative: for any element c in the ring Q, we have

$$\big(\psi\,(\varphi\,\theta)\big)(c) = \psi\big((\varphi\,\theta)(c)\big) = \psi\Big(\varphi\big(\theta(c)\big)\Big) = (\psi\,\varphi)\big(\theta(c)\big) = \big((\psi\,\varphi)\,\theta\big)(c)$$

so $\psi\,(\varphi\,\theta) = (\psi\,\varphi)\,\theta$. □.

Example 5.0.8. Let S be a subring of a ring R. By definition, the canonical injection $S \to R$ is a ring homomorphism.

Proposition 5.0.9. *For any ring homomorphism $\varphi\colon R \to S$, the image $\varphi(R)$ is a subring of S.*

Proof. Let c and d be elements in the image $\varphi(R)$. By definition, there are elements a and b in R such that $\varphi(a) = c$ and $\varphi(b) = d$. Hence, the properties of a ring homomorphism give

$$c - d = \varphi(a) - \varphi(b) = \varphi(a-b) \quad \text{and} \quad c\,d = \varphi(a)\,\varphi(b) = \varphi(a\,b)\,,$$

so $c - d$ and $c\,d$ are both in the image $\varphi(R)$. Since $\varphi(1_R) = 1_S$, the multiplicative identity 1_S is also in the image $\varphi(R)$. Therefore, Proposition 3.1.2 shows that the image $\varphi(R)$ is a subring of S. □

Exercises

Problem 5.0.10. For any ring R, prove that there is a unique ring homomorphism from R to the zero ring. Moreover, prove that the only ring homomorphism from the zero ring is the identity map.

Problem 5.0.11. Let $\varphi\colon R \to S$ be a surjective ring homomorphism. When R is commutative, demonstrate that S is also commutative.

Problem 5.0.12. Confirm that there exists a ring homomorphism from $\mathbb{Z}/\langle m\rangle$ to $\mathbb{Z}/\langle n\rangle$ if and only if n divides m.

5.1 Ideals

What is the most significant substructure of a ring? Special subsets of a ring that are closed under addition and multiplication play an oversized role in the development of ring theory.

Definition 5.1.0. A nonempty subset I of a ring R is a *(two-sided) ideal* if, for any elements f and g in I and any element r in R, the three elements $f - g$, $r\,f$, and $f\,r$ all belong to I.

In honor of Kummer's ideal numbers, Richard Dedekind introduced in 1876 both the concept and the term "ideal" to number theory.

Remark 5.1.1. Let I be an ideal in a ring R. Since I is nonempty, there exists a ring element f in I, so $0_R\,f = 0_R$ lies in I.

Example 5.1.2. For any ring R, both R and $\{0_R\}$ are ideals. When ordered by inclusion, the ring itself is the largest ideal and the singleton $\{0_R\}$ is the smallest.

Example 5.1.3. Let f be a element in a ring R such that $r\,f = f\,r$ for all ring elements r in R. The set of all multiplies of r is an ideal, called *the principal ideal* generated by r and denoted by $\langle r \rangle$.

Lemma 5.1.4. *For any family $\{I_j \mid j \in \mathcal{J}\}$ of ideals in a ring R, the intersection $I := \bigcap_{j\in\mathcal{J}} I_j$ is also an ideal of R.*

Proof. Since $0_R \in I_j$ for all $j \in \mathcal{J}$, we see that $I \neq \varnothing$. Suppose that the ring elements f and g belong I. The definition of intersection implies that f and g belong to the ideal I_j for all $j \in \mathcal{J}$. Since I_j is an ideal of R for all $j \in \mathcal{J}$, it follows that, for all $r \in R$, we have $f - g \in I_j$, $r\,f \in I_j$, and $f\,r \in I_j$. We conclude that $f - g \in I$, $r\,f \in I$, and $f\,r \in I$, which show that I is an ideal. □

Definition 5.1.5. For any nonempty subset $\mathcal{X}$ of a ring R, there exists a unique smallest ideal $\langle \mathcal{X} \rangle$ containing $\mathcal{X}$. This ideal is the ideal *generated by* $\mathcal{X}$.

The ideal $\langle \mathcal{X} \rangle$ is the intersection of all ideals in R that contain $\mathcal{X}$.

Problem 5.1.6. In the ring of integers, show that $\langle 4, 6 \rangle = \langle 2 \rangle$.

Solution. Since $-1(4) + 6 = 2$, it follows that $\langle 2 \rangle \subseteq \langle 4, 6 \rangle$. For any integers a and b, the equation $a(4) + b(6) \equiv 0 \mod 2$ implies that $\langle 2 \rangle \supseteq \langle 4, 6 \rangle$, so we deduce that $\langle 4, 6 \rangle = \langle 2 \rangle$ □

Problem 5.1.7. Let R be a commutative ring. For any elements $f_1, f_2, \dots, f_m$ in R, show that

$$\langle f_1, f_2, \dots, f_m \rangle = \{r_1\,f_1 + r_2\,f_2 + \cdots + r_m\,f_m \mid r_1, r_2, \dots, r_m \in R\}.$$

Solution. We first show the given set is an ideal. Consider elements g and g' from this set. There exists $r_1, r_2, \dots, r_m, r_1', r_2', \dots, r_m'$ in R such that

$$g = r_1\,f_1 + r_2\,f_2 + \cdots + r_m\,f_m \quad \text{and} \quad g' = r_1'\,f_1 + r_2'\,f_2 + \cdots + r_m'\,f_m\,.$$

For any element s in R, we have

$$\begin{aligned} g - g' &= (r_1 - r_1')\,f_1 + (r_2 - r_2')\,f_2 + \cdots + (r_m - r_m')\,f_m \\ s\,g &= (s\,r_1)\,f_1 + (s\,r_2)\,f_2 + \cdots + (s\,r_m)\,f_m \\ g\,s &= (r_1\,s)\,f_1 + (r_2\,s)\,f_2 + \cdots + (r_m\,s)\,f_m\,. \end{aligned}$$

It remains to show that this ideal is the smallest containing the elements $f_1, f_2, \dots, f_m$ in R. For any elements $r_1, r_2, \dots, r_m$ in R, any ideal that contains the elements $f_1, f_2, \dots, f_m$ will contain the multiplies $r_1\,f_1, r_2\,f_2, \dots, r_m\,f_m$ and the sum $r_1\,f_1 + r_2\,f_2 + \cdots + r_m\,f_m$. Hence, any ideal containing the elements $f_1, f_2, \dots, f_m$ will contain the given set. □

Problem 5.1.8. Describe all ideals in the ring $\mathbb{Z}/\langle 6\rangle$.

Solution. The principal ideals are

$$\begin{aligned} \langle [0]_6\rangle &= \{[0]_6\}\,, & \langle [1]_6\rangle &= \{[0]_6, [1]_6, \dots, [5]_6\} = \langle [5]_6\rangle\,, \\ \langle [3]_6\rangle &= \{[0]_6, [3]_6\}\,, & \langle [2]_6\rangle &= \{[0]_6, [2]_6, [4]_6\} = \langle [4]_6\rangle\,. \end{aligned}$$

We verify that these are the only ideals. Since every ideal contains $[0]_6$, there are 2^5 distinct subsets to consider. Any ideal that contains both $[m]_6$ and $[m \pm 1]_6$ also contains $[1]_6 = [m \pm 1]_6 \mp [m]_6$ and must be $\langle [1]_6\rangle$. Any ideal that contains $[2]_6 = [4]_6 + [4]_6$ or $[4]_6 = [2]_6 + [2]_6$ must contain both. Given these constraints, we see that the four principal ideals are the only ideals in $\mathbb{Z}/\langle 6\rangle$. □

As this tedious case study reveals, we need better tools for analyzing the ideals in a ring.

Problem 5.1.9. In $\mathbb{Z}[x]$, verify that $\langle 6, x^2\rangle$ is not a principal ideal.

Solution. Suppose there exists a polynomial f in $\mathbb{Z}[x]$ such that $\langle f\rangle = \langle 6, x^2\rangle$. There would exist polynomials g and h such that $f\,g = 6$ and $f\,h = x^2$. The first equation would imply that $\deg(f) = 0$ and the second equation would thereby imply that $\deg(h) = 2$. Comparing the leading coefficients in the second equation, we would see that f divides 1, so $f = \pm 1$. However, we would have $\langle \pm 1\rangle = \mathbb{Z}[x] \neq \langle 6, x^2\rangle$ which is a contradiction. □

The next definiton and proposition start to uncover the deep relationship between ideals and ring homomorphisms.

Definition 5.1.10. The *kernel* of a ring homomorphism $\varphi\colon R \to S$ is th set $\operatorname{Ker}(\varphi) := \{r \in R \mid \varphi(r) = 0_S\}$.

Proposition 5.1.11. *For any ring homomorphism $\varphi\colon R \to S$, the kernel* $\operatorname{Ker}(\varphi)$ *is an ideal in R.*

Proof. Suppose that the ring elements f and g belong to $\operatorname{Ker}(\varphi)$. For any element r in R, we have

$$\begin{aligned} \varphi(f - g) &= \varphi(f) - \varphi(g) = 0_S - 0_S = 0_S \\ \varphi(r\,f) &= \varphi(r)\,\varphi(f) = \varphi(r)\,0_S = 0_S \\ \varphi(f\,r) &= \varphi(f)\,\varphi(r) = 0_S\,\varphi(r) = 0_S\,, \end{aligned}$$

so the kernel is an ideal. □

Corollary 5.1.12. *A ring homomorphism is injective if and only if its kernel is the zero ideal.*

Proof. Let $\varphi\colon R \to S$ be a ring homomorphism.

$\Leftarrow$: Suppose that φ is injective. Lemma 5.0.3 establishes that $\varphi(0_R) = 0_S$. Injectivity ensures that 0_R is the only ring element sent to 0_S. Thus, we have $\operatorname{Ker}(\varphi) = \langle 0\rangle$.

$\Rightarrow$: Suppose that the kernel of φ is zero. For any elements f and g in R, the equation $\varphi(f) = \varphi(g)$ is equivalent to $\varphi(f - g) = \varphi(f) - \varphi(g) = 0_S$. Since $\operatorname{Ker}(\varphi) = \langle 0\rangle$, we deduce that $f - g = 0_R$ and $f = g$, so φ is injective. □.

Corollary 5.1.13. *For any ring homomorphism $\varphi\colon R \to S$, we have* $\operatorname{Ker}(\varphi) = R$ *if and only if we have* $S = 0$.

Proof. Since $\varphi(1_R) = 1_S$, we have $\operatorname{Ker}(\varphi) = R$ if and only if $1_S = 0_S$ which is equivalent to $S = 0$. □

Exercises

Problem 5.1.14. Let $\mathrm{U}_3(\mathbb{Z})$ be the subset of all upper triangular (3×3)-matrices with integer entries;

$$\mathrm{U}_3(\mathbb{Z}) := \left\{ \begin{bmatrix} a_1 & a_2 & a_3 \\ 0 & a_3 & a_4 \\ 0 & 0 & a_6 \end{bmatrix} \,\middle|\, a_1, a_2, \dots, a_6 \in \mathbb{Z} \right\}.$$

(i) Verify that $\mathrm{U}_3(\mathbb{Z})$ is a subring of the ring of all (3×3)-matrices with integer entries.

(ii) Given the matrix

$$\mathbf{N} := \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

let $\eta\colon \mathbb{Z}[x] \to \mathrm{U}_3(\mathbb{Z})$ be the ring homomorphism defined by

$$\eta(a_m\, x^m + \cdots + a_1\, x + a_0) = a_m\, \mathbf{N}^m + \cdots + a_1\, \mathbf{N} + a_0\, \mathbf{I}.$$

Find a polynomial f in $\mathbb{Z}[x]$ such that $\operatorname{Ker}(\psi) = \langle f \rangle$.

5.2 Quotient Rings

Is every ideal the kernel of a ring homomorphism? Ideals provide a rich source of new rings.

Definition 5.2.0. Let I be an ideal in a ring R. For any elements a and b in R, define the relation $\sim_I$ on R by $a \sim_I b$ if the difference $b - a$ is an element in I.

Example 5.2.1. When $R = \mathbb{Z}$ and $I = \langle \ell \rangle$ for some positive integer ℓ, we have $m \sim_I n$ if and only if $m \equiv n \mod \ell$.

Proposition 5.2.2. *For any ideal I in a ring R, the relation $\sim_I$ is an equivalence relation.*

Proof. Let a, b, and c be elements in the ring R.
(Reflexive) Since $a - a = 0$ and $0 \in I$, we have $a \sim_I a$.
(Symmetric) Suppose that $a \sim_I b$. Since $b - a \in I$, $-1 \in R$, and $(-1)(b - a) = a - b \in I$, we have $b \sim_I a$.
(Transitive) Suppose that $a \sim_I b$ and $b \sim_I c$. It follows that $b - a \in I$ and $c - b \in I$, so $(b - a) + (c - b) = c - a \in I$, so $a \sim_I c$. □

Definition 5.2.3. Let I be an ideal in a ring R. For any element a in R, the *coset*, denoted by $a + I := \{a + r \mid r \in I\}$, is the equivalence class of a with respect to the relation $\sim_I$. The set of equivalence classes in R relative to the relation $\sim_I$ is denoted by $R/I := R/{\sim_I}$.

As with $\mathbb{Z}/\langle \ell \rangle$, we want the quotient set R/I to be a ring.

Theorem 5.2.4. *Let I be an ideal in a ring R. The quotient R/I is a ring with addition and multiplication defined, for any elements a and b in R, by $(a+I)+(b+I)=(a+b)+I$ and $(a+I)(b+I)=(a\,b)+I$ respectively. Moreover, the canonical map $\pi\colon R \to R/I$ defined, for any element a in R, by $\pi(a)=a+I$, is a surjective ring homomorphism and satisfies* $\operatorname{Ker}(\pi)=I$.

Proof. We first show that the binary operations on R/I are well-defined. Given elements a, b, c, and d in R such that $b \sim_I a$ and $d \sim_I c$, we need to prove that $(b+d) \sim_I (a+c)$ and $(b\,d) \sim_I (a\,c)$. Since $a-b \in I$ and $c-d \in I$, it follows that

$$(a-b)+(c-d) = (a+d)-(b+d) \in I \qquad \text{and}$$
$$(a-b)c + b(c-d) = (a\,c)-(b\,d) \in I\,,$$

so we have $(b+d) \sim_I (a+c)$ and $(b\,d) \sim_I (a\,c)$. As binary operations are well-defined on the quotient, the required properties on R/I are inherited directly from those on the ring R. In particular, the additive identity is $0+I$ and the multiplicative identity is $1+I$.

For any elements a and b in the original ring R, the definitions for addition and multiplication on the quotient ring R/I give

$$\begin{aligned} \pi(a+b) &= (a+b)+I = (a+I)+(b+I) = \pi(a)+\pi(b) \\ \pi(a\,b) &= (a\,b)+I = (a+I)(b+I) = \pi(a)\,\pi(b) \\ \pi(1) &= 1+I\,, \end{aligned}$$

so the canonical map $\pi\colon R \to R/I$ is a ring homomorphism. As every coset in R/I has the form $a+I$ for some element a in R, the map π is surjective. Finally, the element a in R belongs to $\operatorname{Ker}(\varphi)$ if and only if $a+I = 0+I$ or equivalently $a = a-0 \in I$. Therefore, we conclude that $\operatorname{Ker}(\varphi) = I$. □

Exercises

Problem 5.2.5. Consider the ideal $I := \langle 1+2\,\mathrm{i} \rangle$ in the ring $\mathbb{Z}[\mathrm{i}] := \{a + b\,\mathrm{i} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ of Gaussian integers. Let $R := \mathbb{Z}[\mathrm{i}]/I$ be the quotient ring.

(i) Are the cosets $\mathrm{i}+I$ and $2+I$ equal in R?
(ii) Are the cosets $4+I$ and $-1+I$ equal in R?
(iii) How many elements does R have?
(iv) Is R a field?