

5 Homomorphisms

Copyright © 2026, Gregory G. Smith
Last Updated: 2026-10-09

Recognizing the maps that preserve a mathematical structure is as essential as defining the objects themselves. Many constructions are most naturally expressed and unified when viewed 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 function must marry the addition and multiplication operations, as well as the additive and multiplicative identities, in the source and target rings. The definition requires the following.

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

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

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

5.0.1 Problem. Show that conjugation is an endomorphism of the field $\mathbb{C}$ of complex numbers.

Solution. For all $z = a + bi, w = c + di \in \mathbb{C}$ with $a, b, c, d \in \mathbb{R}$, we have

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

$$\text{and } \bar{1} = \overline{1 + 0i} = 1 - 0i = 1. \quad \square$$

5.0.2 Remark. Let R be a commutative ring. For every $b \in R$, the evaluation map $\text{ev}_b: R[x] \rightarrow R$ described in Definition 4.0.6 is a ring homomorphism.

Ring homomorphisms automatically preserve the additive identity, additive inverses, and units.

5.0.3 Proposition. Let $\varphi: R \rightarrow S$ be a ring homomorphism.

(additive identity) We have $\varphi(0_R) = 0_S$.

(additive inverses) For all $a \in R$, we have $\varphi(-a) = -\varphi(a)$.

(units) For all $a \in R^\times$, we have $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Proof. The properties of the additive identity and a ring homomorphism give $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$. By adding the additive inverse $-\varphi(0_R)$ to both sides, we obtain

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

The properties of additive inverses and a ring homomorphism give $\varphi(-a) + \varphi(a) = \varphi(-a + a) = \varphi(0) = 0$. Thus, the uniqueness of additive inverses in S shows that $\varphi(-a) = -\varphi(a)$.

The word “homomorphism” comes from the Greek prefix *homo*s meaning ‘same’ and the Greek word *morphe* meaning ‘form’ or ‘shape’. The term appeared as early as 1892 and is attributed to the German mathematician **Felix Klein**.

It is common to omit the adjective ‘ring’ when the type of homomorphism is clear from the context.

By definition, the conjugate of a complex number is the number with an equal real part and an imaginary part equal in magnitude but opposite in sign: when $z := a + bi$ where a and b are real, its conjugate is $\bar{z} := a - bi$.

When R is nonzero, the map $R \times R[x] \rightarrow R$ given by $(b, f) \mapsto \text{ev}_b(f)$ is *not* a ring homomorphism: $(0, x) + (1, 0) = (1, x)$ maps to $\text{ev}_1(x) = 1$, whereas $\text{ev}_0(x) + \text{ev}_1(0) = 0$.

The properties of units and a ring homomorphism give

$$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(1) = 1 \quad \text{and} \quad \varphi(a^{-1})\varphi(a) = 1.$$

The uniqueness of inverses yields $\varphi(a^{-1}) = \varphi(a)^{-1}$. $\square$

Ring homomorphisms single out the integers as a special source.

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

In particular, the identity map is the unique ring endomorphism of $\mathbb{Z}$.

Solution. We treat uniqueness and existence separately.

(uniqueness) Suppose that $\varphi: \mathbb{Z} \rightarrow R$ is a ring homomorphism. For all $m \in \mathbb{N}$, we first prove, by induction on m , that

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

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

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

so $\varphi(-m) = -(m 1_R) = m(-1_R) = (-m) 1_R$. Thus, the only ring homomorphism from $\mathbb{Z}$ to R satisfies $m \mapsto m 1_R$ for all $m \in \mathbb{Z}$.

(existence) Consider the map from $\mathbb{Z}$ to R defined by $m \mapsto m 1_R$ for all $m \in \mathbb{Z}$. The associativity of addition and distributivity in R imply that $(m+n) 1_R = m 1_R + n 1_R$ and $(mn) 1_R = (m 1_R)(n 1_R)$, so the map defined by $m \mapsto m 1_R$ is compatible with addition and multiplication. By definition, we have $1 \mapsto 1_{\mathbb{Z}} 1_R = 1_R$. Thus, the map $m \mapsto m 1_R$ is a ring homomorphism from $\mathbb{Z}$ to R . $\square$

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

More generally, there are no ring homomorphisms from a ring having positive characteristic to a ring having characteristic zero.

Solution. Suppose that $\varphi: \mathbb{Z}/\langle \ell \rangle \rightarrow \mathbb{Z}$ is a ring homomorphism. The definition of a ring homomorphism and Proposition 5.0.3 would imply that $\varphi([1]_{\ell}) = 1$ and $\varphi([0]_{\ell}) = 0$. It would follow that

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

which is a contradiction. $\square$

5.0.6 Remark. A nonempty subset S of a ring R is a subring if and only if the inclusion map $S \rightarrow R$ is a ring homomorphism.

5.0.7 Proposition. For any ring homomorphism $\varphi: R \rightarrow S$, 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

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

so the difference $c - d$ and the product cd are in the image $\varphi(R)$. As $\varphi(1_R) = 1_S$, the multiplicative identity 1_S is also in $\varphi(R)$. Thus, Proposition 3.1.2 shows that the image $\varphi(R)$ is a subring of S . $\square$

5.1 Ideals

What is the most significant substructure of a ring? Special subsets of a ring play an oversized role in the development of ring theory.

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

5.1.1 Remark. For every ring R , both R and $\{0_R\}$ are ideals. When ordered by inclusion, the ring itself is the largest ideal whereas the singleton $\{0_R\}$ is the smallest.

5.1.2 Remark. When R is a commutative ring, a nonempty subset I is an ideal if and only if, for all $f, g \in I$ and all $r, s \in R$, the R -linear combination $rf + sg$ belongs to I .

5.1.3 Definition. When an element f in a ring R satisfies $rf = fr$ for every element $r \in R$, its *principal ideal* is $\langle f \rangle := \{rf \in R \mid r \in R\}$.

5.1.4 Lemma. For every 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. As $0_R \in I_j$ for all $j \in \mathcal{J}$, we have $0_R \in I$ and $I \neq \emptyset$. Suppose that $f, g \in I$. The definition of intersection implies that $f, g \in I_j$ 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 obtain $f + g \in I_j$, $rf \in I_j$, and $fr \in I_j$. We conclude that $f + g \in I$, $rf \in I$, and $fr \in I$, which shows that I is an ideal. $\square$

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

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

Solution. Since $-1(4) + 6 = 2$, it follows that $\langle 2 \rangle \subseteq \langle 4, 6 \rangle$. Conversely, since both 4 and 6 belong to $\langle 2 \rangle$, we have $\langle 2 \rangle \supseteq \langle 4, 6 \rangle$. We conclude that $\langle 4, 6 \rangle = \langle 2 \rangle$ $\square$

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

Solution. Suppose that there exists $f \in \mathbb{Z}[x]$ such that $\langle f \rangle = \langle 6, x^2 \rangle$. There would exist $g, h \in \mathbb{Z}[x]$ such that $gf = 6$ and $hf = x^2$. The first equation would imply that $\deg(f) = 0$ and the second would thereby imply that $\deg(h) = 2$. Comparing the coefficients of x^2 in the second equation, we would see that f divides 1, so $f = \pm 1$. This would give the contradiction $\langle 6, x^2 \rangle = \langle \pm 1 \rangle \neq \langle 6, x^2 \rangle$. $\square$

5.1.8 Problem. For all $f_1, f_2, \dots, f_m$ in a commutative ring R , show that $\langle f_1, f_2, \dots, f_m \rangle = \{r_1 f_1 + r_2 f_2 + \dots + r_m f_m \mid r_1, r_2, \dots, r_m \in R\}$.

Solution. We first show that the given set is an ideal. Consider 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 $g = r_1 f_1 + r_2 f_2 + \dots + r_m f_m$ and $g' = r'_1 f_1 + r'_2 f_2 + \dots + r'_m f_m$. For all $s, s' \in R$, we see that

$$sg - s'g' = (sr_1 - s'r'_1)f_1 + (sr_2 - s'r'_2)f_2 + \dots + (sr_m - s'r'_m)f_m$$

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

One-sided ideals (namely left ideals and right ideals) will not be considered in this document.

The ideal $\langle \mathcal{X} \rangle$ is the intersection of all ideals in R that contain $\mathcal{X}$. In particular, we have $\langle \emptyset \rangle = \{0_R\}$.

If there were elements p and q in $\mathbb{Z}[x]$ such that $p(6) + q(x^2) = 1$, then comparing constant coefficients would imply that $q = 0$ and 6 is a unit in $\mathbb{Z}$ which is absurd.

also belongs to the set, so the set is an ideal.

It remains to show that this ideal is the smallest containing the given elements. For all $r_1, r_2, \dots, r_m \in R$, every ideal containing $f_1, f_2, \dots, f_m$ also contains $((r_1 f_1 + r_2 f_2) + r_3 f_3) + \dots + r_m f_m$, so any ideal containing these elements contains the given set. $\square$

5.1.9 Problem. 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. Every ideal containing 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 $\mathbb{Z}/\langle 6 \rangle$. $\square$

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

The subsequent definition and proposition begin to reveal the deep relationship between ideals and ring homomorphisms.

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

5.1.11 Proposition. For every ring homomorphism $\varphi: R \rightarrow S$, the kernel $\text{Ker}(\varphi)$ is an ideal of R .

Proof. Suppose that $f, g \in \text{Ker}(\varphi)$. For all $r \in R$, it follows that

$$\begin{aligned} \varphi(f + g) &= \varphi(f) + \varphi(g) = 0 + 0 = 0, \\ \varphi(r f) &= \varphi(r) \varphi(f) = \varphi(r) (0) = 0, \quad \text{and} \\ \varphi(f r) &= \varphi(f) \varphi(r) = (0) \varphi(r) = 0, \end{aligned}$$

so the kernel is an ideal. $\square$

5.1.12 Corollary. A ring homomorphism $\varphi: R \rightarrow S$ is injective if and only if its kernel $\text{Ker}(\varphi)$ is the zero ideal.

Proof. Suppose that the map φ is injective. Proposition 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 $\text{Ker}(\varphi) = \langle 0_R \rangle$.

Conversely, suppose that the kernel of φ is zero. For all $f, g \in R$, the properties of a ring homomorphism show that $\varphi(f) = \varphi(g)$ is equivalent to $\varphi(f - g) = \varphi(f) - \varphi(g) = 0_S$. As $\text{Ker}(\varphi) = \langle 0 \rangle$, we deduce that $f - g = 0_R$ and $f = g$, so φ is injective. $\square$

5.1.13 Corollary. For every ring homomorphism $\varphi: R \rightarrow S$, the target ring S is the zero ring if and only if $\text{Ker}(\varphi) = R$.

Proof. Since $\varphi(1_R) = 1_S$, we have $\text{Ker}(\varphi) = R$ if and only if $1_S = 0_S$ which is equivalent to S being the zero ring. $\square$

5.2 Quotient Rings

Is every ideal the kernel of a ring homomorphism? To answer this question, we show that ideals are a rich source of new rings.

5.2.0 Definition. Let R be a commutative ring. For each ideal I in R , the corresponding binary relation on R is defined by $a \sim_I b$, for all $a, b \in R$, if the difference $b - a$ is an element in I .

5.2.1 Remark. When $R = \mathbb{Z}$ and $I = \langle \ell \rangle$ for some $\ell \in \mathbb{N}$, we have $m \sim_I n$ if and only if $m \equiv n \pmod{\ell}$.

5.2.2 Proposition. For every ideal I in a commutative ring R , the binary relation $\sim_I$ is an equivalence relation.

Proof. Consider $a, b, c \in R$.

(reflexive) Since $a - a = 0$ and $0_R \in I$, we deduce that $a \sim_I a$.

(symmetric) Suppose that $a \sim_I b$. Since $b - a \in I$, $-1 \in R$, and $(-1)(b - a) = a - b \in I$, we see that $b \sim_I a$.

(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 $(b - a) + (c - b) = c - a \in I$. We see that $a \sim_I c$. $\square$

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

5.2.4 Problem. Show that the polynomials in $\mathbb{Q}[x]$ of degree less than 2 form a complete system of distinct representatives for the quotient $\mathbb{Q}[x]/\langle x^2 + 1 \rangle$.

Solution. For each polynomial $f \in \mathbb{Q}[x]$, division with remainder implies that there exist $q, r \in \mathbb{Q}[x]$ such that $f = (x^2 + 1)q + r$ and $0 \leq \deg(r) < 2$ or $r = 0$. Since $f - r \in \langle x^2 + 1 \rangle$, every coset in the quotient $\mathbb{Q}[x]/\langle x^2 + 1 \rangle$ is represented by $r + \langle x^2 + 1 \rangle$ for some $r \in \mathbb{Q}[x]$ where $0 \leq \deg(r) < 2$ or $r = 0$. The difference of any two polynomials of degree less than 2 also has degree less than 2, so any two cosets in $\mathbb{Q}[x]/\langle x^2 + 1 \rangle$ are represented different polynomials of degree less than 2 are distinct. $\square$

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

5.2.5 Theorem. Let I be an ideal in a commutative ring R . The quotient R/I is a commutative ring with addition and multiplication defined, for all $a, b \in R$, by $(a+I) + (b+I) = (a+b)+I$ and $(a+I)(b+I) = (ab)+I$ respectively. The canonical map $\pi: R \rightarrow R/I$ defined, for every $a \in R$, by $\pi(a) := a + I$, is a surjective ring homomorphism such that $\text{Ker}(\pi) = I$.

For any ring R , the quotient $R/\langle 0_R \rangle$

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

$$\begin{aligned} (a - b) + (c - d) &= (a + d) - (b + d) \in I & \text{and} \\ (a - b)c + b(c - d) &= (ac) - (bd) \in I, \end{aligned}$$

so $(b+d) \sim_I (a+c)$ and $(bd) \sim_I (ac)$. Since the binary operations are well-defined, 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 all $a, b \in R$, the definitions for addition and multiplication on the quotient ring R/I give

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

so the map $\pi: R \rightarrow R/I$ is a ring homomorphism. As every coset in R/I has the form $a+I$ for some $a \in R$, the map π is surjective. Finally, the element $a \in R$ belongs to $\text{Ker}(\pi)$ if and only if $a+I = 0+I$ or equivalently $a = a-0 \in I$. We conclude that $\text{Ker}(\pi) = I$. $\square$

Not all quotient rings are distinct.

5.2.6 Problem. Demonstrate that $\mathbb{Z}/\langle 6 \rangle$ and $\mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 3 \rangle$ are the “same ring”.

Proof. One may verify that the map from the quotient ring $\mathbb{Z}/\langle 6 \rangle$ to the product ring $\mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 3 \rangle$ defined by

One can prove that only 1 of 720 = 6! bijections is a ring isomorphism.

$$\begin{array}{lll} [0]_6 \mapsto ([0]_2, [0]_3) & [2]_6 \mapsto ([0]_2, [2]_3) & [4]_6 \mapsto ([0]_2, [1]_3) \\ [1]_6 \mapsto ([1]_2, [1]_3) & [3]_6 \mapsto ([1]_2, [0]_3) & [5]_6 \mapsto ([1]_2, [2]_3) \end{array}$$

is a bijective ring homomorphism by constructing the addition and multiplication tables for these rings:

+	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

+	$([0]_2, [0]_3)$	$([1]_2, [1]_3)$	$([0]_2, [2]_3)$	$([1]_2, [0]_3)$	$([0]_2, [1]_3)$	$([1]_2, [2]_3)$
$([0]_2, [0]_3)$	$([0]_2, [0]_3)$	$([1]_2, [1]_3)$	$([0]_2, [2]_3)$	$([1]_2, [0]_3)$	$([0]_2, [1]_3)$	$([1]_2, [2]_3)$
$([1]_2, [1]_3)$	$([1]_2, [1]_3)$	$([0]_2, [2]_3)$	$([1]_2, [0]_3)$	$([0]_2, [1]_3)$	$([1]_2, [2]_3)$	$([0]_2, [0]_3)$
$([0]_2, [2]_3)$	$([0]_2, [2]_3)$	$([1]_2, [0]_3)$	$([0]_2, [1]_3)$	$([1]_2, [2]_3)$	$([0]_2, [0]_3)$	$([1]_2, [1]_3)$
$([1]_2, [0]_3)$	$([1]_2, [0]_3)$	$([0]_2, [1]_3)$	$([1]_2, [2]_3)$	$([0]_2, [0]_3)$	$([1]_2, [1]_3)$	$([0]_2, [2]_3)$
$([0]_2, [1]_3)$	$([0]_2, [1]_3)$	$([1]_2, [2]_3)$	$([0]_2, [0]_3)$	$([1]_2, [1]_3)$	$([0]_2, [2]_3)$	$([1]_2, [0]_3)$
$([1]_2, [2]_3)$	$([1]_2, [2]_3)$	$([0]_2, [0]_3)$	$([1]_2, [1]_3)$	$([0]_2, [2]_3)$	$([1]_2, [0]_3)$	$([0]_2, [1]_3)$

×	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

×	$([0]_2, [0]_3)$	$([1]_2, [1]_3)$	$([0]_2, [2]_3)$	$([1]_2, [0]_3)$	$([0]_2, [1]_3)$	$([1]_2, [2]_3)$
$([0]_2, [0]_3)$	$([0]_2, [0]_3)$	$([0]_2, [0]_3)$	$([0]_2, [0]_3)$	$([0]_2, [0]_3)$	$([0]_2, [0]_3)$	$([0]_2, [0]_3)$
$([1]_2, [1]_3)$	$([0]_2, [0]_3)$	$([1]_2, [1]_3)$	$([0]_2, [2]_3)$	$([1]_2, [0]_3)$	$([0]_2, [1]_3)$	$([1]_2, [2]_3)$
$([0]_2, [2]_3)$	$([0]_2, [0]_3)$	$([0]_2, [2]_3)$	$([0]_2, [1]_3)$	$([0]_2, [0]_3)$	$([0]_2, [2]_3)$	$([0]_2, [1]_3)$
$([1]_2, [0]_3)$	$([0]_2, [0]_3)$	$([1]_2, [0]_3)$	$([0]_2, [0]_3)$	$([1]_2, [0]_3)$	$([0]_2, [0]_3)$	$([1]_2, [0]_3)$
$([0]_2, [1]_3)$	$([0]_2, [0]_3)$	$([0]_2, [1]_3)$	$([0]_2, [2]_3)$	$([0]_2, [0]_3)$	$([0]_2, [1]_3)$	$([0]_2, [2]_3)$
$([1]_2, [2]_3)$	$([0]_2, [0]_3)$	$([1]_2, [2]_3)$	$([0]_2, [1]_3)$	$([1]_2, [0]_3)$	$([0]_2, [2]_3)$	$([1]_2, [1]_3)$

$\square$

We need better ways for identifying equivalent rings.

5.3 Exercises

5.3.1 Problem. Determine which of the following statements are true. If a statement is false, provide a counterexample and, if possible, salvage it by modifying the statement so that it becomes true.

- i. The composition of two ring homomorphisms is a ring homomorphism.
- ii. For every ring homomorphism $\varphi: R \rightarrow S$ and every ideal I in R , the image $\varphi(I)$ is an ideal in S .
- iii. For every ring homomorphism $\varphi: R \rightarrow S$, the equation $\varphi(ab) = 0$ always implies that $\varphi(a) = 0$ or $\varphi(b) = 0$.
- iv. For every finite ring R and every ring homomorphism $\varphi: R \rightarrow S$, the image $\varphi(R)$ is finite.
- v. Every subring of a ring is an ideal.
- vi. Every ideal of a ring is generated by a single element.
- vii. The quotient map $\pi: R \rightarrow R/I$ is injective if and only if $I = 0$.
- viii. The quotient ring R/I is the zero ring implies that $I = R$.
- ix. Every ring is isomorphic to a quotient of a polynomial ring.
- x. If the quotient ring R/I is a domain, then R is also a domain.

5.3.2 Problem. For every ring R , prove that there exists 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.

5.3.3 Problem. Let $\varphi: R \rightarrow S$ be a surjective ring homomorphism. When source ring R is commutative, demonstrate that S is also commutative.

5.3.4 Problem. Establish the following properties for the family of ring homomorphisms.

- (composition) For all ring homomorphisms $\varphi: R \rightarrow S$ and $\psi: S \rightarrow T$, the composition map $\psi \circ \varphi: R \rightarrow T$ is a ring homomorphism.
- (identity) The identity map $\text{id}_R: R \rightarrow R$ is always a ring homomorphism. Moreover, for every ring homomorphism $\varphi: R \rightarrow S$, we also have $\text{id}_S \circ \varphi = \varphi = \varphi \circ \text{id}_R$.
- (associativity) For all ring homomorphisms $\theta: Q \rightarrow R$, $\varphi: R \rightarrow S$, and $\psi: S \rightarrow T$, we have
- $$\psi \circ (\varphi \circ \theta) = (\psi \circ \varphi) \circ \theta.$$

5.3.5 Problem. Let m and n be positive integers. Verify 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 .

5.3.6 Problem. In a commutative ring, demonstrate that the set of nilpotent elements forms an ideal.

5.3.7 Problem. Let $U_3(\mathbb{Z})$ be the subset of all upper triangular (3×3) -matrices with integer entries;

$$U_3(\mathbb{Z}) := \left\{ \begin{bmatrix} a_1 & a_2 & a_3 \\ 0 & a_3 & a_4 \\ 0 & 0 & a_6 \end{bmatrix} \mid a_1, a_2, \dots, a_6 \in \mathbb{Z} \right\}.$$

- i. Verify that $U_3(\mathbb{Z})$ 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 $\eta: \mathbb{Z}[x] \rightarrow U_3(\mathbb{Z})$ be the ring homomorphism defined by

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

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

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

- i. Are the cosets $i + I$ 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?