RING HOMOMORPHISMS AND THE ISOMORPHISM THEOREMS

BIANCA VIRAY

When learning about groups it was helpful to understand how different groups relate to each other. We would like to do so for rings, so we need some way of moving between different rings.

Definition 1. *Let $R = (R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ be rings. A set map $\phi\colon R \to S$ is a (ring) homomorphism if*

(1) $\phi(r_1 +_R r_2) = \phi(r_1) +_S \phi(r_2)$ *for all* $r_1, r_2 \in R$,
(2) $\phi(r_1 \cdot_R r_2) = \phi(r_1) \cdot_S \phi(r_2)$ *for all* $r_1, r_2 \in R$, *and*
(3) $\phi(1_R) = 1_S$.

For simplicity, we will often write conditions (1) *and* (2) *as* $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ *and* $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$ *with the particular addition and multiplication implicit.*

Remark 1. *If $\phi\colon (R, +, \cdot) \to (S, +, \cdot)$ is a ring homomorphism then $\phi\colon (R, +) \to (S, +)$ is a group homomorphism.*

Example 1. *If R is any ring and $S \subset R$ is a subring, then the inclusion $i\colon S \hookrightarrow R$ is a ring homomorphism.*

Exercise 1. *Prove that*

$$\varphi\colon \mathbb{Q} \to \mathrm{M}_n(\mathbb{Q}), \quad \varphi(a) = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a \end{pmatrix}$$

is a ring homomorphism.

Exercise 2. *Let F be a field and let $a \in F$. Prove that*

$$\varphi\colon F[x] \to F, \quad \varphi(f(x)) = f(a)$$

is a ring homomorphism.

Exercise 3. *Let $n \in \mathbb{Z}$ be a positive integer. Prove that*

$$\varphi\colon \mathbb{Z} \to \mathbb{Z}, \quad \varphi(a) = na$$

is not *a ring homomorphism.*

Exercise 4. *Let R be a ring and let I be an ideal. Prove that*

$$\varphi\colon R \to R/I, \quad \varphi(r) = r + I$$

is a ring homomorphism.

Exercise 5. *Determine if the following maps are homomorphisms.*

(1) $\phi\colon \mathrm{M}_2(\mathbb{R}) \to \mathbb{R}, \quad \phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a$
(2) $\phi\colon \mathrm{M}_2(\mathbb{R}) \to \mathbb{R}, \quad \phi(A) = \mathrm{Tr}(A)$
(3) $\phi\colon \mathrm{M}_2(\mathbb{R}) \to \mathbb{R}, \quad \phi(A) = \det(A)$

The three defininings properties of a ring homomorphism imply other important properties.

Lemma 1. *Let $\phi\colon R \to S$ be a ring homomorphism. Then*
(1) $\phi(0_R) = 0_S$,
(2) $\phi(-r) = -\phi(r)$ *for all* $r \in R$,
(3) *if* $r \in R^\times$ *then* $\phi(r) \in S^\times$ *and* $\phi(r^{-1}) = \phi(r)^{-1}$, *and*
(4) *if* $R' \subset R$ *is a subring, then* $\phi(R')$ *is a subring of* S.

Proof. Statements (1) and (2) hold because of Remark 1. We will repeat the proofs here for the sake of completeness.

Since $0_R + 0_R = 0_R$, $\phi(0_R) + \phi(0_R) = \phi(0_R)$. Then since S is a ring, $\phi(0_R)$ has an additive inverse, which we may add to both sides. Thus we obtain

$$\phi(0_R) = \phi(0_R) + \phi(0_R) + -\phi(0_R) = \phi(0_R) + -\phi(0_R) = 0_S,$$

as desired.

Let $r \in R$. Since $r + -r = -r + r = 0_R$, we have

$$\phi(r) + \phi(-r) = \phi(-r) + \phi(r) = \phi(0_R) = 0_S,$$

where the last equality comes from (1). Thus $\phi(-r) = -\phi(r)$ as additive inverses are unique.

Now let $r \in R^\times$. Then there exists $r^{-1} \in R$ such that $r \cdot r^{-1} = r^{-1} \cdot r = 1_R$. Then since ϕ is a ring homomorphism we have

$$\phi(r) \cdot \phi(r^{-1}) = \phi(r^{-1})\phi(r) = \phi(1_R) = 1_S.$$

Thus $\phi(r)$ has a multiplicative inverse and it is $\phi(r^{-1})$.

Lastly, let $R' \subset R$ be a subring. To show that $\phi(R')$ is a subring we must show that $1_S \in \phi(R')$ and for all $s_1, s_2 \in \phi(R')$, $s_1 - s_2$ and $s_1 s_2$ are also in $\phi(R')$. Since $s_1, s_2 \in \phi(R')$, there exists $r_1, r_2 \in R'$ such that $\phi(r_1) = s_1$ and $\phi(r_2) = s_2$. Thus

$$s_1 - s_2 = \phi(r_1) - \phi(r_2) = \phi(r_1) + \phi(-r_2) = \phi(r_1 - r_2), \quad \text{and} \quad s_1 s_2 = \phi(r_1)\phi(r_2) = \phi(r_1 r_2).$$

Since R' is a subring, $r_1 - r_2$ and $r_1 r_2$ are contained in R'. Hence $s_1 - s_2$ and $s_1 s_2$ are in $\phi(R')$. Furthermore, $1_R \in R'$ so $1_S = \phi(1_R) \in \phi(R')$. Therefore, $\phi(R')$ is a subring of S. □

Exercise 6. *Let $\phi\colon R \to S$ be a ring homomorphism. If $r \in R$ is a zero divisor, is $\phi(r)$ a zero divisor in S? If yes, then prove this statement. If no, give an example of a ring homomorphism ϕ and a zero divisor $r \in R$ such that $\phi(r)$ is not a zero divisor.*

As in the case of groups, homomorphisms that are bijective are of particular importance.

Definition 2. *Let R and S be rings and let $\phi\colon R \to S$ be a set map. We say that ϕ is a (ring) isomorphism if*
(1) *ϕ is a (ring) homomorphism and*
(2) *ϕ is a bijection on sets.*

We say that two rings R_1 and R_2 are isomorphic if there exists an isomorphism between them.

Lemma 2. *Let R and S be rings and let $\phi\colon R \to S$ be an isomorphism. Then:*

(1) ϕ^{-1} *is an isomorphism,*
(2) $r \in R$ *is a unit if and only if* $\phi(r)$ *is a unit of* S*,*
(3) $r \in R$ *is a zero divisor if and only if* $\phi(r)$ *is a zero divisor of* S*,*
(4) R *is commutative if and only if* S *is commutative,*
(5) R *is an integral domain if and only if* S *is an integral domain, and*
(6) R *is a field if and only if* S *is a field.*

Exercise 7. *Prove Lemma 2.*

Exercise 8. *Prove that* $\mathbb{Z}[x]$ *and* $\mathbb{R}[x]$ *are not isomorphic.*

1. Kernel, image, and the isomorphism theorems

A ring homomorphism $\varphi\colon R \to S$ yields two important sets.

Definition 3. *Let* $\phi\colon R \to S$ *be a ring homomorphism. The* kernel *of* ϕ *is*

$$\ker \phi := \{r \in R : \phi(r) = 0\} \subset R$$

and the image *of* ϕ *is*

$$\operatorname{im} \phi := \{s \in S : s = \phi(r) \text{ for some } r \in R\} \subset S.$$

Exercise 9. *Let* R *and* S *be rings and let* $\phi\colon R \to S$ *be a homomorphism. Prove that* ϕ *is injective if and only if* $\ker \phi = \{0\}$*.*

Theorem 3 (First isomorphism theorem)**.** *Let* R *and* S *be rings and let* $\phi\colon R \to S$ *be a homomorphism. Then:*

(1) *The kernel of* ϕ *is an* ideal *of* R*,*
(2) *The image of* ϕ *is a* subring *of* S*,*
(3) *The map*

$$\varphi\colon R/\ker \phi \to \operatorname{im} \phi \subset S, \quad r + \ker \phi \mapsto \phi(r)$$

is a well-defined isomorphism.

Proof. The image of ϕ is a subring by Lemma 1. Let us prove that $\ker \phi$ is an ideal. By Lemma 1, $\phi(0) = 0$ so $0 \in \ker \phi$ and hence the kernel is nonempty. Let $a, b \in \ker \phi$ and let $r \in R$. Then since ϕ is a homomorphism we have

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b) = 0 + 0 = 0, \\ \phi(ra) &= \phi(r)\phi(a) = \phi(r) \cdot 0 = 0, \\ \phi(ar) &= \phi(a)\phi(r) = 0 \cdot \phi(r) = 0. \end{aligned}$$

Thus $a + b, ra$, and ar are in $\ker \phi$ and so $\ker \phi$ is an ideal.

Consider the map φ. We first show that it is well-defined. Let $r, r' \in R$ be such that $r - r' \in \ker \phi$, i.e., such that $r + \ker \phi = r' + \ker \phi$. Then

$$\phi(r) = \phi(r' + (r - r')) = \phi(r') + \phi(r - r') = \phi(r') + 0 = \phi(r'),$$

so φ is well defined. Let $r_1 + I, r_2 + I \in R/I$. Then since ϕ is a homomorphism we have:

$$\begin{aligned}\varphi(r_1 + I + r_2 + I) &= \varphi(r_1 + r_2 + I) = \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) \\ &= \varphi(r_1 + I) + \varphi(r_2 + I) \\ \varphi((r_1 + I)(r_2 + I)) &= \varphi(r_1 r_2 + I) = \phi(r_1 r_2) = \phi(r_1)\phi(r_2) \\ &= \varphi(r_1 + I)\varphi(r_2 + I) \\ \varphi(1 + I) &= \phi(1) = 1.\end{aligned}$$

Therefore φ is a homomorphism.

Let us prove that φ is bijective. If $r + \ker\phi \in \ker\varphi$, then $\varphi(r + I) = \phi(r) = 0$ and so $r \in \ker\phi$ or equivalently $r + \ker\phi = \ker\phi$. Thus $\ker\varphi$ is trivial and so by Exercise 9, φ is injective. Let $s \in \operatorname{im}\phi$. Then there exists an $r \in R$ such that $\phi(r) = s$ or equivalently that $\varphi(r + \ker\phi) = s$. Thus $s \in \operatorname{im}\varphi$ and so φ is surjective. Hence φ is an isomorphism as desired. □

Exercise 10. *Compute the kernel of φ where φ is as in* (1) *Exercise 1,* (2) *Exercise 2, and* (3) *Exercise 4.*

Theorem 4 (Second isomorphism theorem)**.** *Let R be a ring, let $S \subset R$ be a subring, and let I be an ideal of R. Then:*

(1) *$S + I := \{s + a : s \in S, a \in I\}$ is a subring of R,*
(2) *$S \cap I$ is an ideal of S, and*
(3) *$(S + I)/I$ is isomorphic to $S/(S \cap I)$.*

Proof. **(1)**: S is a subring and I is an ideal so $1 + 0 \in S + I$. Let $s_1 + a_1$ and $s_2 + a_2$ be elements of $S + I$. Then

$$(s_1+a_1)-(s_2+a_2) = \underbrace{(s_1 - s_2)}_{\in S} + \underbrace{(a_1 - a_2)}_{\in I} \quad \text{and} \quad (s_1+a_1)(s_2+a_2) = \underbrace{s_1 s_2}_{\in S} + \underbrace{s_1 a_2 + a_1 s_2 + a_1 a_2}_{\in I}.$$

Hence $S + I$ is a subring of R.

(2): The intersection $S \cap I$ is nonempty since 0 is contained in I and S. Let $a_1, a_2 \in S \cap I$ and let $s \in S$. Then $a_1 + a_2 \in S \cap I$ since S and I are both closed under addition. Furthermore sa_1 and $a_1 s$ are in $S \cap I$ since I is closed under multiplication from $R \supset S$ and S is closed under multiplication. Therefore $S \cap I$ is an ideal of S.

(3): Consider the map $\phi\colon S \to (S+I)/I$ which sends an element s to $s + I$. This is a ring homomorphism by definition of addition and multiplication in quotient rings. We claim that it is surjective with kernel $S \cap I$, which would complete the proof by the first isomorphism theorem. Consider elements $s \in S$ and $a \in I$. Then $s + a + I = s + I$ since $a \in I$, so $s + a + I \in \operatorname{im}\phi$ and hence ϕ is surjective. Let $s \in S$ be an element of $\ker\phi$. Then $s + I = I$ which holds if and only if $s \in I$ or equivalently if $s \in S \cap I$. Thus $\ker\phi = S \cap I$ and we have our desired result. □

Theorem 5 (Third isomorphism theorem)**.** *Let R be a ring and let $J \subset I$ be ideals of R. Then I/J is an ideal of R/J and*

$$\frac{R/J}{I/J} \cong R/I.$$

Proof. Since I and J are ideals, they are nonempty and so $I/J = \{a + J : a \in I\}$ is also nonempty. Let $a_1, a_2 \in I$ and let $r \in R$. By definition of addition and multiplication of cosets, we have

$$\begin{aligned}(a_1 + J) + (a_2 + J) &= (a_1 + a_2) + J,\\ (r + J)(a_1 + J) &= ra_1 + J, \text{ and}\\ (a_1 + J)(r + J) &= a_1 r + J.\end{aligned}$$

Since I is an ideal, $a_1 + a_2, ra_1$, and $a_1 r$ are contained in I so I/J is an ideal of R/J.

Consider the map $\phi\colon R/J \to R/I$ that sends $r + J$ to $r + I$. We claim that this is a well-defined surjective homomorphism with kernel equal to I/J. (See Exercise 11.) Then $(R/J)/(I/J)$ is isomorphic to R/I by the first isomorphism theorem. □

Exercise 11. *We will use the notation from Theorem 5. Prove that the map* $\phi\colon R/J \to R/I, \quad r + J \mapsto r + I$ *is a well-defined surjective homomorphism with kernel equal to* I/J.

Exercise 12. *Prove that* $\mathbb{Q}(\sqrt{-5})$ *is isomorphic to* $\mathbb{Q}[x]/\langle x^2 - 2x + 6\rangle$.