6 *Isomorphisms*

Recognizing the maps that perserve a mathematical structure allows one to compare objects and identify equivalence ones.

6.0 Isomorphisms

When are two ring the same? From the viewpoint of ring theory, when may we identify two rings?

Definition 6.0.0. A ring homomorphism $\varphi\colon R \to S$ is called an *isomorphism* if there exists a ring homomorphism $\psi\colon S \to R$ such that $\psi\,\varphi = \mathrm{id}_R$ and $\varphi\,\psi = \mathrm{id}_S$. An isomorphism that is also an endomorphism is called an *automorphism*.

The words "isomorphism" and "automorphism" come from the Greek prefix *isos* meaning 'equal', the Latin/Greek prefix *auto* meaning 'self', and the Greek suffix *morphe* meaning 'form' or 'shape'.

Problem 6.0.1. Show that complex conjugation is an automorphism of the field $\mathbb{C}$ of complex numbers.

Proof. Problem 5.0.5 establishes that complex conjugation is an endomorphism. For any complex numbers $z = a + b\,\mathrm{i}$, we have

$$\overline{\overline{z}} = \overline{\overline{a + b\,\mathrm{i}}} = \overline{a - b\,\mathrm{i}} = a + b\,\mathrm{i} = z\,.$$

Therefore, complex conjugation is an idempotent operator (or equivalently, its own inverse) and thereby an automorphism. □

Proposition 6.0.2. *A ring homomorphism $\varphi\colon R \to S$ is an isomorphism if and only if the map φ is a bijection.*

A bijection is an isomorphism of sets.

Proof. We prove each implication separately.

$\Leftarrow$: Suppose that the map $\varphi\colon R \to S$ is a ring isomorphism. By definition, there exists another ring homomorphism $\psi\colon S \to R$ such that $\psi\,\varphi = \mathrm{id}_R$ and $\varphi\,\psi = \mathrm{id}_S$. In particular, the underlying map of sets has an inverse, so it is a bijection.

$\Rightarrow$: Suppose that the underlying map of set is a bijection. It follows that there exists a map $\psi\colon S \to R$ of sets such that $\psi\,\varphi = \mathrm{id}_R$ and $\varphi\,\psi = \mathrm{id}_S$. It remains to show that the map ψ is a ring homomorphism. Since φ is a ring homomorphism, it follows that, for all elements a and b in the ring S, we have

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

Applying ψ to both side of these equations gives

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

so ψ is a ring homomorphism. □

Definition 6.0.3. Two ring R and S are *isomorphic*, denoted by $R \cong S$, if there exists a ring isomorphism $\varphi\colon R \to S$.

Proposition 6.0.4. *Being isomorphic is an equivalence relation.*

Proof. Let R, S, and T be rings.
(Reflexive) The identity map $\mathrm{id}_R\colon R \to R$ is a ring homomorphism and its own inverse, so id_R is a ring isomorphism and $R \cong R$.
(Symmetric) Suppose that $R \cong S$. There are ring homomorphisms $\varphi\colon R \to S$ and $\psi\colon S \to R$ such that $\psi\,\varphi = \mathrm{id}_R$ and $\varphi\,\psi = \mathrm{id}_S$. In particular, the ring isomorphism $\psi\colon S \to R$ implies that $S \cong R$.
(Transitive) Suppose that $R \cong S$ and $S \cong T$. By definition, there exist ring isomorphisms $\varphi\colon R \to S$ and $\theta\colon S \to T$. Since the composition $\theta\,\varphi$ is a ring homomorphism and

$$\varphi^{-1}\,\theta^{-1}\,\theta\,\varphi = \varphi^{-1}\,\mathrm{id}_S\,\varphi = \varphi^{-1}\,\varphi = \mathrm{id}_R$$
$$\theta\,\varphi\,\varphi^{-1}\,\theta^{-1} = \theta\,\mathrm{id}_S\,\theta^{-1} = \theta\,\theta^{-1} = \mathrm{id}_T\,,$$

the composition $\theta\,\varphi\colon R \to T$ is a ring isomorphism and $R \cong T$. □

Problem 6.0.5. Show that $\mathbb{Z}/\langle 6\rangle$ and $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 3\rangle$ are isomorphic.

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

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

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

is an isomorphism by constructing the addition and multiplication tables for these rings. □

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Table 6.1: Addition and multiplication tables for the quotient ring $\mathbb{Z}/\langle 6\rangle$ and the product ring $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 3\rangle$; for brevity, the brackets in the equivalence classes are omitted

+	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(0,0)	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(1,1)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)	(0,0)
(0,2)	(0,2)	(1,0)	(0,1)	(1,2)	(0,0)	(1,1)
(1,0)	(1,0)	(0,1)	(1,2)	(0,0)	(1,1)	(0,2)
(0,1)	(0,1)	(1,2)	(0,0)	(1,1)	(0,2)	(1,0)
(1,2)	(1,2)	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)

×	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(1,1)	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(0,2)	(0,0)	(0,2)	(0,1)	(0,0)	(0,2)	(0,1)
(1,0)	(0,0)	(1,0)	(0,0)	(1,0)	(0,0)	(1,0)
(0,1)	(0,0)	(0,1)	(0,2)	(0,0)	(0,1)	(0,2)
(1,2)	(0,0)	(1,2)	(0,1)	(1,0)	(0,2)	(1,1)

Ring isomorphism preserve all ring-theoretic properties.

Proposition 6.0.6. *Let $\varphi\colon R \to S$ be a ring isomorphism. An element b in the ring R is a zero divisor if and only if the element $\varphi(b)$ in S is a zero divisor. Similarly, an element b in R is a unit if and only if the element $\varphi(b)$ in S is a unit.*

Proof. Suppose that the element b in R is a zero divisor. There exists a nonzero element a in R such that $a\,b = 0_R$ or $b\,a = 0_R$. Since φ is a ring homomorphism, we have

$$\begin{aligned}\varphi(a)\,\varphi(b) &= \varphi(a\,b) = \varphi(0_R) = 0_S \\ \varphi(b)\,\varphi(a) &= \varphi(b\,a) = \varphi(0_R) = 0_S\,.\end{aligned}$$

As φ is an isomorphism, injectivity implies that $\varphi(a) \neq \varphi(0_R) = 0_S$. Therefore, the element $\varphi(b)$ is a zero divisor in S. Applying the same argument to $\varphi^{-1}\colon S \to R$ gives the converse implication.

Suppose that the element b in R is a unit. There exists a element a in R such that $a\,b = b\,a = 1_R$. Since φ is a ring homomorphism, we have

$$\begin{aligned}\varphi(a)\,\varphi(b) &= \varphi(a\,b) = \varphi(1_R) = 1_S \\ \varphi(b)\,\varphi(a) &= \varphi(b\,a) = \varphi(1_R) = 1_S\,.\end{aligned}$$

Therefore, the element $\varphi(b)$ is a unit in S. Again, applying the same argument to $\varphi^{-1}\colon S \to R$ gives the converse implication. □

Corollary 6.0.7. *Let R and S be isomorphic rings. The ring R is a domain if and only if the ring S is a domain. Similarly, the ring R is a field if and only if the ring S is a field.* □

Exercises

Problem 6.0.8 (2-out-of-6 property)**.** Let $\theta\colon Q \to R$, $\varphi\colon R \to S$, and $\psi\colon S \to T$ be ring homomorphisms. When the compositions $\varphi\,\theta$ and $\psi\,\varphi$ are ring isomorphisms, prove that θ, φ, θ, and $\psi\,\varphi\,\theta$ are also ring isomorphisms.

6.1 Isomorphism Theorems

What is the most important source of isomorphisms? Original formulated by Emmy Noether in 1927, the isomorphism theorems describe the relations between quotients, homomorphisms, and subobjects. Although we focus on rings, versions of these theorems exist for many algebraic structures including groups and vector spaces.

We start by observing that a ring homomorphism descends to quotient rings whenever the image of an ideal on the source is contained in the an ideal on the target.

Induced Map Lemma 6.1.0. *Let $\varphi \colon R \to S$ be a ring homomorphism. For any ideal I in the ring R and any ideal J in the ring S satisfying $\varphi(I) \subseteq J$, the induced map $\overline{\varphi} \colon R/I \to S/J$, defined for any ring element r in R by $\overline{\varphi}(r + I) = \varphi(r) + J$, is a well-defined ring homomorphism.*

Proof. Let r and s be elements in the ring R. When $r \sim_I s$, we have $r - s \in I$ and $\varphi(r) - \varphi(s) \in \varphi(I) = \varphi(r - s) \subseteq J$. Hence, we deduce that $\varphi(r) \sim_J \varphi(s)$ and $\overline{\varphi}$ is well-defined.

Since φ is a ring homomorphism, we also have

$$\begin{aligned}
\overline{\varphi}\big((r + I) + (s + I)\big) &= \overline{\varphi}\big((r + s) + I\big) \\
&= \varphi(r + s) + J \\
&= \big(\varphi(r) + \varphi(s)\big) + J \\
&= \big(\varphi(r) + J\big) + \big(\varphi(s) + J\big) = \overline{\varphi}(r + I) + \overline{\varphi}(s + I)\,, \\
\overline{\varphi}\big((r + I)(s + I)\big) &= \overline{\varphi}\big((r\,s) + I\big) \\
&= \varphi(r\,s) + J \\
&= \big(\varphi(r)\,\varphi(s)\big) + J \\
&= \big(\varphi(r) + J\big)\big(\varphi(s) + J\big) = \overline{\varphi}(r + I)\,\overline{\varphi}(s + I)\,, \\
\overline{\varphi}(1_R + I) &= \varphi(1_R) + J = 1_S + J\,.
\end{aligned}$$

Thus, $\overline{\varphi} \colon R/I \to S/J$ is a ring homomorphism. □

The kernel and image of a homomorphism are related by an isomorphism.

First Isomorphism Theorem 6.1.1. *Let $\varphi \colon R \to S$ be a ring homomorphism with kernel $I := \operatorname{Ker}(\varphi)$. The induced map $\widetilde{\varphi} \colon R/I \to \operatorname{Im}(\varphi)$, defined for any element r in R by $\widetilde{\varphi}(r + I) = \varphi(r)$, is a well-defined ring isomorphism. Writing $\pi \colon R \to R/I$ for the canonical surjection and $\operatorname{id}_S|_{\operatorname{Im}(\varphi)} \colon \operatorname{Im}(\varphi) \to S$ for the canonical injection, we also have the canonical decomposition $\varphi = \operatorname{id}_S|_{\operatorname{Im}(\varphi)}\,\widetilde{\varphi}\,\pi$.*

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & S \\
R/I \arrow[r, "\widetilde{\varphi}"] & \operatorname{Im}(\varphi) \arrow[u, "\operatorname{id}_S|_{\operatorname{Im}(\varphi)}"']
\end{tikzcd}$$

Figure 6.1: Commutative diagram arising from First Isomorphism Theorem 6.1.1

Proof. The Induced Map Lemma 6.1.0, with the ideal $J := \langle 0_S \rangle$ in the ring S, shows that the induced map $\widetilde{\varphi}$ is a well-defined ring homomorphism. For any element r in the ring R, the coset $r + I$ belongs to $\operatorname{Ker}(\widetilde{\varphi})$ if and only if $0_S = \widetilde{\varphi}(r + I) = \varphi(r)$ which means $r \in \operatorname{Ker}(\varphi)$. We deduce that $\operatorname{Ker}(\widetilde{\varphi}) = \langle 0 + I \rangle$ in the quotient ring R/I, so Corollary 5.1.12 shows that the induced map $\widetilde{\varphi}$ is injective. By definition, the induced map $\widetilde{\varphi}$ surjects onto $\operatorname{Im}(\varphi)$. Hence, Proposition 6.0.2 demonstrates that $\widetilde{\varphi}$ is a ring isomorphism. The second part follows from the definition of the induced map $\widetilde{\varphi}$. □

Problem 6.1.2. Confirm that $\mathbb{Z}[\mathrm{i}]/\langle 1+3\,\mathrm{i}\rangle \cong \mathbb{Z}/\langle 10\rangle$.

Solution. Let $\varphi\colon \mathbb{Z} \to \mathbb{Z}[\mathrm{i}]/\langle 1+3\,\mathrm{i}\rangle$ be the unique ring homomorphism. Since $\mathrm{i} = (-1)(-\mathrm{i}) = (3\mathrm{i})(-\mathrm{i}) = 3$ in $\mathbb{Z}[\mathrm{i}]/\langle 1+3\mathrm{i}\rangle$, the coset containing the Gaussian integer $a + b\,\mathrm{i}$ is the coset containing the integer $a + 3b$, so the map φ is surjective. Given an integer m in $\operatorname{Ker}(\varphi)$, it follows that m is in $\langle 1+3\,\mathrm{i}\rangle$. Hence, there are integers c and d such that $m = (c + d\,\mathrm{i})(1+3\,\mathrm{i}) = (c-3d) + (3c+d)\mathrm{i}$. We deduce that $3c = -d$ and $m = c + 3(-d) = c + 3(3c) = 10c$. We conclude that $\operatorname{Ker}(\varphi) \subseteq \langle 10\rangle$. We also have $3^2 = -1$ or $10 = 0$ in $\mathbb{Z}[\mathrm{i}]/\langle 1+3\,\mathrm{i}\rangle$, so $\langle 10\rangle \subseteq \operatorname{Ker}(\varphi)$. Thus, the First Isomorphism Theorem 6.1.1 yields the isomorphism $\mathbb{Z}/\langle 10\rangle \cong \mathbb{Z}[\mathrm{i}]/\langle 1+3\,\mathrm{i}\rangle$. □

Problem 6.1.3. Prove that the ring $\mathbb{C}[x,y]/\langle x\,y\rangle$ is isomorphic to the subring of the product $\mathbb{C}[x] \times \mathbb{C}[y]$ consisting of the pairs $\big(f(x), g(x)\big)$ such that $f(0) = g(0)$.

Solution. The First Isomorphism Theorem gives $\mathbb{C}[x,y]/\langle y\rangle \cong \mathbb{C}[x]$ because the ideal $\langle y\rangle$ is the kernel of the map $\mathrm{ev}_{y=0}\colon \mathbb{C}[x,y] \to \mathbb{C}[x]$. By symmetry, we also have $\mathbb{C}[x,y]/\langle x\rangle \cong \mathbb{C}[y]$. Consider the map $\mathbb{C}[x,y] \to \mathbb{C}[x] \times \mathbb{C}[y]$ defined by $f(x,y) \mapsto \big(f(x,0), f(0,y)\big)$. Its kernel is $\langle x\rangle \cap \langle y\rangle = \langle x\,y\rangle$. The First Isomorphism Theorem 6.1.1 completes the proof. □

Aside from the First Isomorphism Theorem 6.1.1, there are no methods for recognizing a quotient ring, because it will usually not be a familiar ring.

The two quotient rings arising from an ideal and a subring in a ring are related by an isomorphism.

Second Isomorphism Theorem 6.1.4. *Let R be a ring. For all ideals I in R and all subrings S of R, the sum $S + I$ is a subring of R, the set I is an ideal in the subring $S + I$, the intersection $S \cap I$ is an ideal in the subring S, and the map $\widetilde{\eta}\colon S/(S \cap I) \to (S + I)/I$, defined for any element s in S by $\widetilde{\eta}(s + S \cap I) = s + I$, is a well-defined ring isomorphism.*

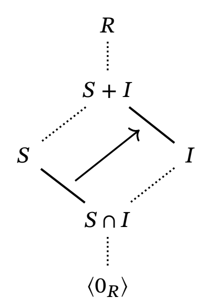

Figure 6.2: Hasse diagram arising from Second Isomorphism Theorem 6.1.4

Proof. We first show that $S + I := \{s + g \mid s \in S \text{ and } g \in I\}$ is a subring of the ring R. Consider elements r and s in the subring S and elements f and g in the ideal I. It follows that the element $(r+f)-(s+g) = (r-s)+(f-g)$ belongs to $S+I$ because $r-s \in S$ and $f - g \in I$. The element $(r+f)(s+g) = r\,s + r\,g + f\,s + f\,g$ also belongs to $S + I$ because $r\,s \in S$, and $r\,g + f\,s + f\,g \in I$. Since $1_R \in S$ and $0_R \in I$, we see that $1_R = 1_R + 0_R \in S + I$. Thus, the subset $S + I$ is a subring of R.

Since I is an ideal in R and $S + I$ is a subring of R, we deduce that I is also an ideal in $S + I$. We next show that $S \cap I$ is an ideal in subring S. For any elements f and g in $S \cap I$ and any element s in S, the elements $f - g$, $s\,f$, and $f\,s$ all belong to both the ideal I and the subring S. Since these three elements belong to $S \cap I$, we deduce that $S \cap I$ is an ideal in the subring S.

Lastly, consider the map $\eta \colon S \to (S+I)/I$ defined for any element s in S by $\eta(s) := s + I$. For any elements r and s in S, we have $\eta(r+s) = (r+s)+I = (r+I)+(s+I)$, $\eta(rs) = (rs)+I = (r+I)(s+I)$, and $\eta(1_S) = 1_S + I$, so the map η is a ring homomorphism. From the definition of the sum $S + I$, we see that the map η is surjective. We claim that $\operatorname{Ker}(\eta) = S \cap I$.

$\subseteq$: Suppose that $f \in \operatorname{Ker}(\eta)$. It follows that $f+I = \eta(f) = 0+I = I$, so we deduce that $f \in I$. As $\operatorname{Ker}(\eta) \subseteq S$, we have $f \in S$ which implies that $f \in S \cap I$ and $\operatorname{Ker}(\eta) \subseteq S \cap I$.

$\supseteq$: Suppose that $f \in S \cap I$. As $f \in I$, we have $\eta(f) = f + I = I$, so we see that $f \in \operatorname{Ker}(\eta)$ and $\operatorname{Ker}(\eta) \supseteq S \cap I$.

Since $\operatorname{Ker}(\eta) = S \cap I$ and η is surjective, the First Isomorphism Theorem 6.1.1 proves that the induced map $\widetilde{\eta} \colon S/(S \cap I) \to (S+I)/I$ is a ring isomorphism. □

Exercises

Problem 6.1.5. Each quotient ring R/I in the left column of Table 6.2 is isomorphic to a ring S in the right column. Match each quotient ring with its isomorphic partner and prove that they are isomorphic be describing a surjective ring homomorphism $\varphi \colon R \to S$ with kernel I.

The matching is neither injective nor surjective.

R/I	S
$\dfrac{\mathbb{Z}[x]}{\langle 8, 12, x \rangle}$	$\dfrac{\mathbb{Z}}{\langle 3 \rangle}$
$\dfrac{\mathbb{Q}[x]}{\langle x^2 - 2 \rangle}$	$\dfrac{\mathbb{Z}}{\langle 4 \rangle}$
$\dfrac{\mathbb{R}[x]}{\langle x - \sqrt{2} \rangle}$	$\dfrac{\mathbb{Z}}{\langle 8 \rangle}$
$\dfrac{\mathbb{R}[x]}{\langle x^2 + x + 2 \rangle}$	$\mathbb{Z}$
$\dfrac{\mathbb{R}[x]}{\langle x^2 \rangle}$	$\mathbb{Q}$
$\dfrac{\mathbb{R}[x,y]}{\langle y - 1 \rangle}$	$\mathbb{R}$
$\dfrac{\mathbb{R}[x,y]}{\langle y - 1, x + 9 \rangle}$	$\mathbb{C}$
$\dfrac{\mathbb{R}[x,y]}{\langle y - 1, x^2 + 9 \rangle}$	$\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$
	$\mathbb{Z}[x]$
	$\mathbb{Q}[x]$
	$\mathbb{R}[x]$
	$\mathbb{C}[x]$
	$\left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$

Table 6.2: Table of quotient rings and rings

6.2 Ideals in a Quotient Ring

How are the ideals in a quotient ring related to the ideals in its ambient ring? Every ring homomorphism produces a bijection between certain ideals in its source and all ideals in its target.

Correspondence Theorem 6.2.0. *Let $\varphi\colon R \to S$ be a ring homomorphism with kernel $K := \operatorname{Ker}(\varphi)$.*

(i) *For any ideal J in S, the preimage $\varphi^{-1}(J) := \{r \in R \mid \varphi(r) \in J\}$ is an ideal in R containing the ideal K.*

(ii) *For any ideal J is S, the composition of the map $\varphi\colon R \to S$ and the canonical surjection $\pi\colon S \to S/J$ induces an injective ring homomorphism $\widetilde{\pi\varphi}\colon R/\varphi^{-1}(J) \to S/J$. When φ is surjective, the map $\widetilde{\pi\varphi}$ is a ring isomorphism.*

(iii) *Assume that φ is surjective. The maps $I \mapsto \varphi(I)$ and $J \mapsto \varphi^{-1}(J)$ are inverse inclusion-preserving bijections between the set of ideals in R containing K and the set of ideals in S.*

Proof.

(i): For any elements f and g in the preimage $\varphi^{-1}(J)$ and any element r in the ring R, the elements $\varphi(f+g) = \varphi(f) + \varphi(g)$, $\varphi(r\,f) = \varphi(r)\,\varphi(f)$, and $\varphi(f\,r) = \varphi(f)\,\varphi(r)$ belong to the ideal J, so $f+g$, $r\,f$, and $f\,r$ belong to the preimage $\varphi^{-1}(J)$. Hence, the subset $\varphi^{-1}(J)$ is an ideal in the ring R. Since $0_S \in J$ and $\varphi^{-1}(0_S) = K$, the preimage $\varphi^{-1}(J)$ contains the ideal K.

(ii): The Induced Map Lemma 6.1.0 demonstrates that the map $\widetilde{\pi\varphi}\colon R/\varphi^{-1}(J) \to S/J$ is a well-defined ring homomorphism. Since $\operatorname{Ker}(\pi) = J$, it follows that $\operatorname{Ker}(\pi\,\varphi) = \varphi^{-1}(J)$ and $\operatorname{Ker}(\widetilde{\pi\varphi}) = \langle 0 + \varphi^{-1}(J)\rangle$, so this induced map is also injective. When φ is surjective, the composition $\pi\,\varphi$ is also surjective, whence $\widetilde{\pi\varphi}$ is surjective.

(iii): Assume that the map φ is surjective. We show that, for any ideal I in R, the image $\varphi(I)$ is an ideal S. For any elements p and q in the image $\varphi(I)$ and any element s in S, there exists elements f and g in the ideal I and an element r in the ring R such that $\varphi(f) = p$, $\varphi(g) = q$, and $\varphi(r) = s$. The elements $p + q = \varphi(f) + \varphi(g) = \varphi(f+g)$, $s\,p = \varphi(r)\,\varphi(f) = \varphi(r\,f)$, and $p\,s = \varphi(f)\,\varphi(r) = \varphi(f\,r)$ belong to the image $\varphi(I)$, so the subset $\varphi(I)$ is an ideal in the ring S. Since $\varphi(K) = \langle 0_S\rangle$, the image of any ideal contained in the kernel K is zero ideal in S.

The preceding paragraph shows that the map $I \mapsto \varphi(I)$ sends any ideal I in the ring R containing K to the ideal $\varphi(I)$ in the ring S. Conversely, part (i) shows that the map $J \mapsto \varphi^{-1}(J)$ sends any ideal J in the ring S to the ideal $\varphi^{-1}(J)$ in the ring R containing K. These maps composite in either order to an identity map. Finally, both images and preimages preserve inclusions. □

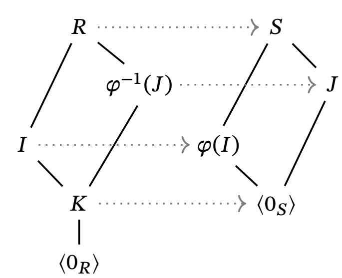

Figure 6.3: Hasse diagram of ideals in the Correspondence Theorem

Problem 6.2.1. Describe all ideals in the ring $\mathbb{Z}/\langle 6\rangle$.

Solution. Given the inclusions $\langle 6\rangle \subset \langle 2\rangle$ and $\langle 6\rangle \subset \langle 3\rangle$, the Induced Map Lemma 6.1.0 shows that the identity map $\mathrm{id}_{\mathbb{Z}} \colon \mathbb{Z} \to \mathbb{Z}$ induces ring homomorphisms $\varphi \colon \mathbb{Z}/\langle 6\rangle \to \mathbb{Z}/\langle 2\rangle$ and $\psi \colon \mathbb{Z}/\langle 6\rangle \to \mathbb{Z}/\langle 3\rangle$ where $\operatorname{Ker}(\varphi) = \langle [2]_6\rangle$ and $\operatorname{Ker}(\psi) = \langle [3]_6\rangle$. Since both $\mathbb{Z}/\langle 2\rangle$ and $\mathbb{Z}/\langle 3\rangle$ are fields, they contain only two distinct ideals, namely the zero ideal and the whole ring. Hence, the Correspondence Theorem 6.2.0 shows that $\langle [2]_6\rangle$ and $\langle [1]_6\rangle$ are the ideals in $\mathbb{Z}/\langle 6\rangle$ containing $\langle [2]_6\rangle$, and $\langle [3]_6\rangle$ and $\langle [1]_6\rangle$ are the ideals in $\mathbb{Z}/\langle 6\rangle$ containing $\langle [3]_6\rangle$. Since $[4]_6\,[2]_6 = [2]_6$ and $[5]_6$ is a unit, we conclude that the four ideals in $\mathbb{Z}/\langle 6\rangle$ are $\langle [0]_6\rangle$, $\langle [2]_6\rangle$, $\langle [3]_6\rangle$, and $\langle [1]_6\rangle$. □

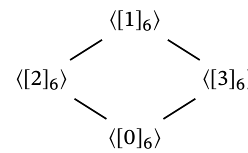

Figure 6.4: Hasse diagram of ideals in the quotient ring $\mathbb{Z}/\langle 6\rangle$

Problem 6.2.2. For any positive integer m, describe all ideals in the quotient ring $\mathbb{C}[x]/\langle x^m\rangle$.

Solution. For any nonnegative integer m, let $I_m := \langle x^m\rangle$ be an ideal in $\mathbb{C}[x]$. We prove, by induction on m, that the $m+1$ ideals in the quotient ring $\mathbb{C}[x]/I_m$ are

$$\langle 0 + I_m\rangle, \langle x^{m-1} + I_m\rangle, \langle x^{m-2} + I_m\rangle, \dots, \langle x + I_m\rangle, \langle 1 + I_m\rangle \,.$$

When $m = 1$, the First Isomorphism Theorem 6.1.1 establishes that $\mathbb{C}[x]/\langle x\rangle \cong \mathbb{C}$. Since $\mathbb{C}$ is a field, the only ideals are $\langle 0\rangle$ and $\langle 1\rangle$, which establishes the base case. Assume that k is an integer greater than 1. Given the inclusion $I_{k+1} \subset I_k$, the Induced Map Lemma 6.1.0 shows that the identity map $\mathrm{id}_{\mathbb{C}[x]} \colon \mathbb{C}[x] \to \mathbb{C}[x]$ induces a ring homomorphism $\varphi \colon \mathbb{C}[x]/I_{k+1} \to \mathbb{C}[x]/I_k$ where $\operatorname{Ker}(\varphi) = \langle x^k + I_{k+1}\rangle$. Hence, the induction hypothesis and the Correspondence Theorem 6.2.0 establish that the $k+1$ ideals in the ring $\mathbb{C}[x]/\langle x^{k+1}\rangle$ containing $\langle x^k + I_{k+1}\rangle$ are

$$\begin{aligned} \varphi^{-1}(\langle 0 + I_k\rangle) &= \langle x^k + I_{k+1}\rangle \\ \varphi^{-1}(\langle x^{k-1} + I_k\rangle) &= \langle x^{k-1} + I_{k+1}\rangle \\ &\ \vdots \\ \varphi^{-1}(\langle 1 + I_k\rangle) &= \langle 1 + I_{k+1}\rangle \,. \end{aligned}$$

It remains to show that $\langle 0 + I_{k+1}\rangle$ is the only other ideal in the ring $\mathbb{C}[x]/I_{k+1}$. Hence, it suffices to prove that any nonzero ideal contains the ideal $\langle x^k + I_{k+1}\rangle$. A nonzero polynomial f in $\mathbb{C}[x]$ of degree at most k has the form $f = a_k\, x^k + a_{k+1}\, x^{k-1} + \cdots + a_\ell\, x^\ell$ where ℓ is a nonnegative integer ℓ, $a_k, a_{k-1}, \dots, a_\ell$ are complex numbers, and $a_\ell \neq 0$. Since $(a_\ell^{-1}\, x^{k-\ell}\, f) \,\%\, x^{k+1} = x^k$, it follows that $\langle x^k + I_{k+1}\rangle \subseteq \langle f + I_{k+1}\rangle$. □

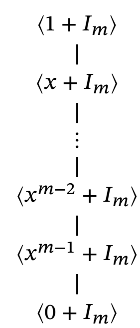

Figure 6.5: Hasse diagram of ideals in the ring $\mathbb{C}[x]/I_m$

One can show that every element in $\mathbb{C}[x]/I_m$ is either nilpotent or a unit.

The quotient rings arising from nested ideals in a ring are also related by an isomorphism.

Third Isomorphism Theorem 6.2.3. *Let I be an ideal in the ring R.*

(i) *Every ideal in the ring R/I has the form $J/I := \{r + I \mid r \in J\}$ for some ideal J in R containing I.*

(ii) *For any ideal J in R containing I, the composition of the canonical surjections $R \to R/I$ and $R/I \to (R\,/\,I)/(J\,/\,I)$ induces a ring isomorphism $R/J \to (R\,/\,I)/(J\,/\,I)$.*

Proof. We obtain both parts by applying the Correspondence Theorem to the canonical surjection $\pi \colon R \to R/I$. □