2.2 Isomorphism Theorems

We again have theorems describing the relations between quotients, homomorphisms, and subobjects.

2.2.1 Theorem. *Let I be an ideal in a commutative ring R. The quotient R/I inherits a multiplication such that canonical map $\pi : R \to R/I$ is a surjective ring homomorphism.*

Sketch of Proof. For all $a, b \in R$, multiplication on the abelian group R/I is defined by $(a+I)(b+I) := ab+I$. Suppose that $a+I = a'+I$ and $b+I = b'+I$ for some $a', b' \in I$. It follows that $a - a' \in I$ and $b - b' \in I$. To show that multiplication is well-defined, we must show $(a'+I)(b'+I) = a'b'+I = ab+I$ or $ab - a'b' \in I$. Indeed, we have $ab - a'b' = ab - a'b + a'b - a'b' = (a-a')b + a'(b-b') \in I$. By Corollary 1.7.13, it remains to verify that this product is associative, commutative, distributive and that the identity is $1 + I$. □

2.2.2 Corollary. *Let $\varphi : R \to R'$ be a ring homomorphism. For any ideal I in the ring R and any ideal I' in the ring R' satisfying $\varphi(I) \subseteq I'$, the induced map $\overline{\varphi} : R/I \to R'/I'$ is a ring homomorphism.*

Proof. Since $\overline{\varphi}(1+I) = \varphi(1)+I' = 1+I'$, it suffices by Corollary 1.7.14 to check that the map $\overline{\varphi}$ is compatible with multiplicative;

$$\begin{aligned}\overline{\varphi}\big((a+I)(b+I)\big) &= \overline{\varphi}(ab+I) = \varphi(ab) + I' = \varphi(a)\,\varphi(b) + I' \\ &= \big(\varphi(a) + I'\big)\big(\varphi(b) + I'\big) = \overline{\varphi}(a+I)\,\overline{\varphi}(b+I)\,. \end{aligned}$$ □

2.2.3 Theorem (First Isomorphism). *Let $\varphi : R \to S$ be a ring homomorphism with kernel $I := \operatorname{Ker}(\varphi)$. The induced map $\widetilde{\varphi} : R/I \to \operatorname{Im}(\varphi)$ defined by $\widetilde{\varphi}(r+I) = \varphi(r)$ is an isomorphism. Writing $\pi : R \to R/I$ for the canonical surjection and $\iota : \operatorname{Im}(\varphi) \to S$ for the canonical injection, we also have $\varphi = \iota \circ \widetilde{\varphi} \circ \pi$.*

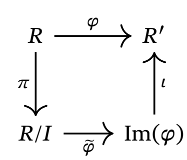

Figure 2.1: Commutative diagram arising from Theorem 2.2.3

Proof. Since $\widetilde{\varphi}(1+I) = \varphi(1) = 1$, it suffices by Theorem 1.8.1 to check that the map $\widetilde{\varphi}$ is compatible with multiplicative;

$$\begin{aligned}\widetilde{\varphi}\big((a+I)(b+I)\big) &= \widetilde{\varphi}(ab+I) = \varphi(ab) \\ &= \varphi(a)\,\varphi(b) = \widetilde{\varphi}(a+I)\,\widetilde{\varphi}(b+I)\,. \end{aligned}$$ □

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

Solution. Let $\varphi : \mathbb{Z} \to \mathbb{Z}[\mathrm{i}]/\langle 1+3\mathrm{i}\rangle$ 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 $a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ equal the coset containing $a + 3b$, so φ is surjective. Given $n \in \operatorname{Ker}(\varphi)$, we have $n \in \langle 1+3\mathrm{i}\rangle$. Hence, there are $c, d \in \mathbb{Z}$ such that $n = (c+d\mathrm{i})(1+3\mathrm{i}) = (c-3d) + (3c+d)\mathrm{i}$. Since $n \in \mathbb{Z}$, we see that $3c = -d$ and $n = c + 3(-d) = c + 3(3c) = 10c$. We conclude that $\mathrm{Ker}(\varphi) \subseteq \langle 10 \rangle$. We also have $3^2 = -1$ or $10 = 0$ in $\mathbb{Z}[\mathrm{i}]/\langle 1 + 3\mathrm{i} \rangle$, so $\langle 10 \rangle \subseteq \mathrm{Ker}(\varphi)$. Therefore, the First Isomorphism Theorem yields the isomorphism $\mathbb{Z}/\langle 10 \rangle \cong \mathbb{Z}[\mathrm{i}]/\langle 1 + 3\mathrm{i} \rangle$. □

2.2.5 Problem. Prove that the ring $\mathbb{C}[x, y]/\langle xy \rangle$ 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 $f(0) = g(0)$.

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

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 $\mathrm{ev}_{y=0} : \mathbb{C}[x, y] \to \mathbb{C}[x]$. Similarly, we have $\mathbb{C}[x, y]/\langle x \rangle \cong \mathbb{C}[y]$. Consider $\mathbb{C}[x, y] \to \mathbb{C}[x]\times\mathbb{C}[y]$ given by $f(x, y) \mapsto \big(f(x, 0), f(0, y)\big)$. The kernel is $\langle x \rangle \cap \langle y \rangle = \langle xy \rangle$. The First Isomorphism Theorem completes the proof. □

2.2.6 Theorem (Second Isomorphism). *Let R be a commutative ring. For all ideals I in R and all subrings $S \subseteq R$, the sum $S + I$ is a subring of R, I is an ideal in $S + I$, $S \cap I$ is an ideal of S, and there is a ring isomorphism $S/(S \cap I) \cong (S + I)/I$.*

Proof. Since $\varphi(1_S) = 1_S + I$, it suffices by Theorem 1.8.5 to check that the map $\varphi : S \to (S + I)/I$ defined by $\varphi(s) := s + I$ is compatible with multiplicative; $\varphi(st) = st + I = (s + I)(t + I) = \varphi(s)\,\varphi(t)$. □

2.2.7 Theorem (Third Isomorphism). *Let I and J be two ideals in a commutative ring R such that $I \subseteq J$. The quotient J/I is an ideal of the quotient ring R/I and we have the isomorphism $R/J \cong (R/I)/(J/I)$.*

Proof. Since $\varphi(1_R + I) = 1_R + J$, it suffices by Theorem 1.8.6 to check that $\varphi : R/I \to R/J$ defined by $\varphi(r + I) = s + J$ is compatible with multiplicative; $\varphi(rs + I) = rs + J = (r + J)(s + J) = \varphi(r)\,\varphi(s)$. □

Compare with Theorem 1.8.7.

2.2.8 Theorem (Correspondence). *Let I be an ideal in R. The canonical map $\pi : R \to R/I$ induces a bijection between the set of all subrings of R (respectively, the set of all ideals) containing I and the set of all subrings (respectively, the set of all ideals) of quotient ring R/I.* □

2.2.9 Proposition. *For a nonzero ring R, the following are equivalent:*

(a) *R is a field;*

(b) *the only ideals in R are $\langle 0 \rangle$ and $\langle 1 \rangle$;*

(c) *every ring homomorphism from R to a nonzero ring is injective.*

Proof.

(a) ⇒ (b) Let I be a nonzero ideal in R. Choose $0 \neq a \in I \subseteq R$. The ring element a is a unit, so we have $R = \langle 1 \rangle \subseteq \langle a \rangle \subseteq I \subseteq R$.

(b) ⇒ (c) For any ring homomorphism $\varphi : R \to R'$, the kernel $\mathrm{Ker}(\varphi)$ is a proper ideal. We have $\mathrm{Ker}(\varphi) = \langle 0 \rangle$ and the map φ is injective.

(c) ⇒ (a) If $x \in R$ is not a unit, then $\langle x \rangle \neq \langle 1 \rangle$ and $S = R/\langle x \rangle$ is not the zero ring. Let $\pi : R \to S$ be the canonical map. By hypothesis, the map π is injective so $\langle x \rangle = \langle 0 \rangle$ and $x = 0$. □

2.3 Maximal and Prime Ideals

Some ideals have greater significance.

2.3.1 Definition. An ideal I in a commutative ring R is ***maximal*** if $I \neq \langle 1 \rangle = R$ and there is no proper ideal J in R such that $I \subset J \subset R$.

2.3.2 Proposition. *An ideal I in R is maximal if and only if the quotient ring R/I is a field.*

Proof.
($\Rightarrow$) Suppose that I is maximal ideal. Consider the coset $a + I$ in R for some $a \in R \setminus I$. Since $a \in a + I$ and $a \notin I$, maximality implies that $a + I = R$, so $ra + f = 1$ for some $r \in R$ and $f \in I$. It follows that $(r+I)(a+I) = ra+I = (1-f)+I = 1+I$ which demonstrates that $\langle a \rangle + I$ is a unit in the quotient ring R/I.
($\Leftarrow$) Suppose that the quotient R/I is a field. It follows that, for any element $0 \neq 1 \in R/I$, we have $I \neq R$. The only ideals in a field are $\langle 0 \rangle$ and $\langle 1 \rangle$, so the Theorem 2.2.8 shows that there are no ideals in R properly between I and R. Thus, the ideal I is maximal. □

2.3.3 Example. The maximal ideals in the ring $\mathbb{Z}$ are the principal ideals generated by prime integers. ◇

2.3.4 Definition. A ***partially ordered set*** or ***poset*** P is a set together with a reflexive, antisymmetric, transitive binary relation $\preccurlyeq$. Two elements $x, y \in P$ are ***comparable*** if $x \preccurlyeq y$ or $y \preccurlyeq x$. A ***chain*** is a poset in which any two elements are comparable. A subset of a poset is a chain if it is a chain when regarded as a subposet.

Partially ordered sets may not have maximal elements. For example, real numbers $\mathbb{R}$, with the usual ordering, has no maximal elements.

2.3.5 Lemma (Zorn). *Any nonempty partially order set, such that every chain has an upper bound, has a maximal element.* □

Zorn's Lemma is equivalent to the axiom of choice or the well-ordering principle. Kazimierz Kuratowski (1922) proved a variant and Max Zorn (1935) proposed it as a new axiom of set theory.

2.3.6 Theorem (Krull). *Any proper ideal in a commutative ring lies in a maximal ideal.*

Proof. Fix a commutative ring R. Let $\mathcal{S}$ be the set of all ideals J in R that contain the ideal I and are not equal to R. Since $I \in \mathcal{S}$, the set $\mathcal{S}$ is nonempty. Partially order $\mathcal{S}$ by inclusion. Let C be a chain in $\mathcal{S}$; given $J, J' \in C$, either $J \subseteq J'$ or $J' \subseteq J$. We claim that $J^* = \bigcup_{J \in C} J$ is an upper bound of C. We clearly have $J \subseteq J^*$ for all $J \in C$, so it remains to prove J^* is a proper ideal. If $f, g \in J^*$ and $r \in R$, then $f, g \in J$ for some $J \in C$ and $rf + g \in J \subseteq J^*$ so J is an ideal. If $J^* = R$, then we would have $1 \in J^*$ and $1 \in J$ for some $J \in C$ which contradicts the fact that J is proper. Since every chain of $\mathcal{S}$ has an upper bound, Zorn's Lemma completes the proof. □

Wolfgang Krull (1929) first proved the Theorem 2.3.6 by transfinite induction.

2.3.7 Definition. An ideal I in commutative ring R is ***prime*** if the quotient ring R/I is a domain.

A maximal ideal J in a commutative ring R is prime because the quotient R/J is a field. It follows that every ideal R other than R is contained in at least one prime ideal.

The prime ideals in the ring $\mathbb{Z}$ are principal ideals generated by primes and the zero ideal.

2.3.8 Proposition. *An ideal I prime if and only if $I \neq \langle 1 \rangle$ and the relation $fg \in I$ implies $f \in I$ or $g \in I$.*

Proof. For any $f \in R$, let $\overline{f}$ denote its image under the canonical map $\pi : R \to R/I$.

(⇒) If $fg \in I$ then we have $\overline{f}\,\overline{g} = 0 \in R/I$. Since R/I is a domain, it follows that $\overline{f} = 0$ or $\overline{g} = 0$, so either $f \in I$ or $g \in I$.

(⇐) Suppose that $\overline{f}\,\overline{g} = 0$ for some $\overline{f}, \overline{g} \in R/I$. Choose elements $f, g \in R$ such that $\overline{f} = f + I$ and $\overline{g} = g + I$. It follows that $0 = \overline{f}\,\overline{g} = (f + I)(g + I) = fg + I$ so we deduce that $fg \in I$. By hypothesis, we have $f \in I$ or $g \in I$, which implies that $\overline{f} = 0$ or $\overline{g} = 0$. Therefore, the quotient ring R/I is a domain. □

2.3.9 Remark. Let $\varphi : R \to R'$ be a ring homomorphism and let I' be an ideal of R'. Set $I := \varphi^{-1}(I')$. The induced ring homomorphism $\overline{\varphi} : R/I \to R'/I'$ is injective. If I' is a prime ideal, then the quotient ring R'/I' is a domain. Since the quotient ring R/I is isomorphic to a subring of R'/I', it is also a domain and the ideal I is a prime ideal.

Two ideals I and J in a commutative ring R are ***comaximal*** if $I + J = R$. For this to be true, it is necessary and sufficient that $I + J$ be contained in no prime ideal. In other words, no prime ideal contains both I and J. Thus, two distinct maximal ideals are comaximal.

2.3.10 Lemma. *Let $I, J_1, J_2, \dots, J_n$ be ideals in a ring R. When $R = I + J_j$ for all j, we have $R = I + J_1 J_2 \cdots J_n = I + (J_1 \cap J_2 \cap \cdots \cap J_n)$.*

Proof. Since $IJ_j \subseteq I \cap J_j$, it suffices to prove that $R = I + J_1 J_2 \cdots J_n$. By induction, it suffices to consider the case $n = 2$. By hypothesis, we have $f, f' \in I$, $g_1 \in J_1$ and $g_2 \in J_2$ such that $1 = f + g_1 = f' + g_2$. It follows that $1 = f' + (f + g_1)g_2 = (f' + fg_2) + g_1 g_2 \in I + J_1 J_2$ whence we obtain $R = I + J_1 J_2$. □

The earliest version of Theorem 2.3.11, with $R = \mathbb{Z}$, appears in the work of the Chinese mathematician Sun Zi. Nothing is known about this mathematician except for his text *Sunzi suanjing*. Dating this is made more difficult since it is not known how much the text was changed or added to over time.

2.3.11 Theorem (Chinese Remainder). *For any ideals $I_1, I_2, \dots, I_n$ in a commutative ring R, the following are equivalent:*

- *for all $k \neq j$, the ideal I_k and I_j are comaximal;*
- *the canonical ring homomorphism $\varphi : R \to \prod_j (R/I_j)$ is surjective.*

If these conditions hold, then we have $I = \bigcap_j I_j = \prod I_j$ and the canonical map $\overline{\varphi} : R/I \to \prod_j (R/I_j)$ is bijective.

Sketch of Proof. Suppose that the elements $f \in I$ and $g \in J$ satisfy $1 = f + g$. It follows that $\varphi(f) = (f + I, 1 - g + J) = (I, 1 + J)$ and $\varphi(g) = (1 - f + I, g + J) = (1 + I, J)$. For any $r, s \in R$, we have $\varphi(sf + rg) = \varphi(s)\,\varphi(f) + \varphi(r)\,\varphi(g) = (r + I, s + J)$, which establishes that φ is surjective. Moreover, for all $h \in I \cap J$, we have $h = hf + hg$ but $hf \in IJ$ and $hg \in IJ$. It follows that $h \in IJ$ and $I \cap J \subseteq IJ$. The inclusion $IJ \subseteq I \cap J$ is trivial.

Conversely, suppose that the map φ is surjective. Hence, there exists an element $f \in R$ such that $\varphi(f) = (0 + I, 1 + J)$. We deduce that $f \in I$ and $f = 1 - g$ for some $g \in J$.

For the general case, use induction. □