6.3 Sun Zi's Remainder Theorem

When can we factor a ring? In certain circumstances, one may decompose a ring into a product of its quotients.

Definition 6.3.0. A ring element r is *idempotent* if $r^2 = r$. In a ring R, a *trivial* idempotent is either the additive identity 0_R or the multiplicative identity 1_R, both which are always idempotent. Two idempotents r and s in R are *orthogonal* if $r\,s = s\,r = 0_R$.

Problem 6.3.1. Show that $\mathbb{Z}/\langle 4\rangle$ is not isomorphic to $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$.

Solution. Let $\varphi\colon R \to S$ be a ring isomorphism. For any idempotent r in R, we have $\varphi(r)^2 = \varphi(r)\,\varphi(r) = \varphi(r^2) = \varphi(r)$, so the image $\varphi(r)$ is an idempotent in S. The product ring $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$ has a pair of non-trivial orthogonal idempotents which sum to the multiplicative identity:

$$([1]_2,[0]_2)^2 = ([1]_2,[0]_2)\,, \qquad ([1]_2,[0]_2)([0]_2,[1]_2) = ([0]_2,[0]_2)\,,$$
$$([0]_2,[1]_2)^2 = ([0]_2,[1]_2)\,, \quad ([1]_2,[0]_2) + ([0]_2,[1]_2) = ([0]_2,[1]_2)\,.$$

In contrast, the ring $\mathbb{Z}/\langle 4\rangle$ has only the trivial idempotents:

$$[0]_4^2 = [0]_4\,, \quad [1]_4^2 = [1]_4\,, \quad [2]_4^2 = [4]_4 = [0]_4\,, \quad [3]_4^2 = [9]_4 = [1]_4\,.$$

We conclude that $\mathbb{Z}/\langle 4\rangle$ is not isomorphic to $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$. □

Definition 6.3.2. For any ideals I and J in a ring R, their *sum* is the set $I + J := \{f + g \mid f \in I \text{ and } g \in J\}$. When R is commutative, their product is

$$I\,J := \{f_1\,g_1 + f_2\,g_2 + \dots + f_m\,g_m \mid f_1, f_2, \dots, f_m \in I \text{ and } g_1, g_2, \dots, g_m \in J\}\,.$$

The sum and product of ideals are more than just sets.

Proposition 6.3.3. *Let I and J be ideals in the ring R. The sum $I + J$ is the smallest ideal containing both I and J. When R is commutative. the product $I\,J$ is an ideal contained in $I \cap J$.*

Proof. For any elements h_1 and h_2 in the sum $I + J$, there exists elements f_1 and f_2 in the ideal I and elements g_1 and g_2 in the ideal J such that $h_1 = f_1 + g_1$ and $h_2 = f_2 + g_2$. Given an element r in the ring R, the elements $h_1 + h_2 = (f_1 + f_2) + (g_1 + g_2)$, $r\,h_1 = (r\,f_1) + (r\,g_1)$, and $h_1\,r = (f_1\,r) + (g_1\,r)$ belong to the set $I + J$, so the sum $I + J$ is an ideal.

Suppose that K is an ideal that contains I and J. It follows that K must contain all elements f in I and all g in J. Since K is an ideal it must contain all $f + g$ where $f \in I$ and $g \in J$. In particular, we have $I + J \subseteq K$, so $I + J$ is the smallest ideal containing I and J.

For any elements h and h' in the product $I\,J$, there are elements $f_1, f_2, \dots, f_m, f_1', f_2', \dots, f_m'$ in I and $g_1, g_2, \dots, g_m, g_1', g_2', \dots, g_m'$ in J such that $h = \sum_{j=1}^{m} f_j\,g_j$ and $h' = \sum_{j=1}^{m} f_j'\,g_j'$. Given an element r in the ring R, the elements

$$h + h' = f_1\,g_1 + f_2\,g_2 + \dots + f_m\,g_m + f_1'\,g_1' + f_2'\,g_2' + \dots + f_m'\,g_m'\,,$$
$$r\,h = (r\,f_1)\,g_1 + (r\,f_2)\,g_2 + \dots + (r\,f_m)\,g_m\,, \text{ and}$$
$$h\,r = f_1\,(g_1\,r) + f_2\,(g_2\,r) + \dots + f_m\,(g_m\,r)$$

belong to the set $I\,J$, so the product $I\,J$ is an ideal. By definition, we also have $I\,J \subseteq I \cap J$. □

We record two technical observations.

Lemma 6.3.4. *Let $J, I_1, I_2, \dots, I_n$ be ideals in a commutative ring R. When $R = J + I_j$ for all $1 \leqslant j \leqslant n$, we have*

$$R = J + I_1\,I_2 \cdots I_n = J + (I_1 \cap I_2 \cap \cdots \cap I_n)\,.$$

Proof. Since $J\,I_j \subseteq J \cap I_j$ for all $1 \leqslant j \leqslant n$, it suffices to prove that $R = J + I_1\,I_2 \cdots I_n$. By induction, it suffices to consider the case $n = 2$. By hypothesis, there exists elements f_1 and f_2 in the ideal J, an element g_1 in I_1, and an element g_2 in I_2 such that $1 = f_1 + g_1 = f_2 + g_2$. It follows that

$$1 = f_2 + (f_1 + g_1)\,g_2 = (f_2 + f_1\,g_2) + g_1\,g_2 \in J + I_1\,I_2\,,$$

whence $R = J + I_1\,I_2$. □

Lemma 6.3.5. *For any ideals $I_1, I_2, \dots, I_n$ in a commutative ring R such that $I_j + I_k = R$ for all $j \neq k$, we have $I_1 \cap I_2 \cap \cdots \cap I_n = I_1\,I_2 \cdots I_n$.*

Proof. Proposition 6.3.3 implies that $I_1\,I_2\, \cdots I_n \subseteq I_1 \cap I_2 \cap \cdots \cap I_n$, so it suffices to prove that $I_1\,I_2\, \cdots I_n \supseteq I_1 \cap I_2 \cap \cdots \cap I_n$. We proceed by induction on n. When $n = 2$, there exists an element f_1 in I_1 and an element f_2 in I_2 such that $f_1 + f_2 = 1$. When $g \in I_1 \cap I_2$, we have $g = g\,(f_1 + f_2) = g\,f_1 + g\,f_2 \in I_1\,I_2$, so $I_1 \cap I_2 \subseteq I_1\,I_2$. Since Lemma 6.3.4 shows that $R = I_n + (I_1\,I_2 \cdots I_{n-1})$, the base case and the induction hypothesis give

$$\begin{aligned} I_1 \cap I_2 \cap \cdots \cap I_{n-1} \cap I_n &= (I_1 \cap I_2 \cap \cdots \cap I_{n-1}) \cap I_n \\ &= (I_1 \cap I_2 \cap \cdots \cap I_{n-1})\,I_n \\ &= (I_1\,I_2 \cdots I_{n-1})\,I_n = I_1\,I_2 \cdots I_{n-1}\,I_n\,. \end{aligned}$$ □

We now characterize rings are a product of quotient rings.

Sun Zi's Remainder Theorem 6.3.6. *For any positive integer n and any ideals $I_1, I_2, \dots, I_n$ in a commutative ring R, the following are equivalent.*

(a) *The map $\pi \colon R \to \prod_{j=1}^{n} R/I_j$, whose components are the canonical surjections, is ring isomorphism.*
(b) *There are elements $e_1, e_2, \dots, e_n$ in R such that, for all $1 \leqslant j \leqslant n$, we have $e_j^2 = e_j$, $e_j\,e_k = 0$ for all $j \neq k$, $1_R = e_1 + e_2 + \cdots + e_n$, and $I_j = \langle 1 - e_j \rangle$.*
(c) *For all $j \neq k$, we have $I_j + I_k = R$ and $I_1\,I_2 \cdots I_n = \langle 0_R \rangle$.*
(d) *For all $j \neq k$, we have $I_j + I_k = R$ and $I_1 \cap I_2 \cap \cdots \cap I_n = \langle 0_R \rangle$.*

The earliest version of Theorem 6.3.6, 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*.

Proof.

(a) ⇒ (b): Since R is isomorphic to $\prod_{j=1}^{n} R/I_j$, there is an element e_j in R corresponding to the element $(0, 0, \dots, 0, 1_{R/I_j}, 0, \dots, 0)$ in the product $\prod_{j=1}^{n} R/I_j$. It follows that, for all $1 \leqslant j \leqslant n$, we have $e_j^2 = e_j$, $e_j\,e_k = 0$ for all $j \neq k$, and $1_R = e_1 + e_2 + \cdots + e_n$. Since the ideal I_j is the kernel of the canonical surjection $\pi_j \colon R \to R/I_j$, we also have $I_j = \langle 1 - e_j \rangle$.

(b) ⇒ (c): Suppose that there exists element e_j with the given properties. For any $j \neq k$, we have $1 - e_j \in I_j$, $e_j\,(1 - e_k) \in I_k$, so $1 \in I_j + I_k$ and $R = I_j + I_k$. Moreover, for any elements $r_1, r_2, \dots, r_n \in R$, we have

$$\begin{aligned} r_1\,(1-e_1)\,r_2\,(1-e_2)\cdots r_n\,(1-e_n) &= (r_1\,r_2\cdots r_n)\big((1-e_1)\,(1-e_2)\cdots(1-e_n)\big) \\ &= (r_1\,r_2\cdots r_n)\big(1-(e_1+e_2+\cdots+e_n)\big) = 0\,, \end{aligned}$$

whence $I_1\,I_2\cdots I_n = \langle 0\rangle$.

(c) ⇒ (d): This follows from Lemma 6.3.5.

(d) ⇒ (a): The kernel of the map $\pi\colon R \to \prod_{j=1}^{n} R/I_j$, whose components are the canonical surjective ring homomorphisms, is clearly $I_1 \cap I_2 \cap \cdots \cap I_n$, so π is injective. To prove surjectivity, we show that, for any elements $r_1, r_2, \dots r_n$ in R, there exists an element r in R such that $r \sim_{I_j} r_j$ for all $1 \leqslant j \leqslant n$. We proceed by induction on n. The base case $n = 1$ is trivial. By the induction hypothesis, there exists an element s in R such that $s \sim_{I_j} r_j$ for all $1 \leqslant j \leqslant n-1$. We seek an element of the form $s+z \in R$ where $z \sim_{I_j} 0$ for all $1 \leqslant j \leqslant n-1$ and $s + z \sim_{I_n} r_n$. In other words, the element z belongs to $\bigcap_{j=1}^{n-1} I_j$ and $r_n - y - z \in I_n$. Lemma 6.3.4 demonstrates that $R = I_n + (I_1 \cap I_2 \cap \cdots \cap I_{n-1})$, so the existence of the element z follows. □

Exercises

Problem 6.3.7.

(i) Prove that $\mathbb{Z}/\langle 60\rangle$ is isomorphic to $\mathbb{Z}/\langle 3\rangle \times \mathbb{Z}/\langle 4\rangle \times \mathbb{Z}/\langle 5\rangle$.

(ii) Exhibit elements e_1, e_2, and e_3 in $\mathbb{Z}/\langle 60\rangle$ such that

$$e_1^2 = e_1 \quad e_2^2 = e_2 \quad e_3^2 = e_3 \quad e_2\,e_3 = 0 \quad e_1\,e_3 = 0 \quad e_1\,e_2 = 0$$

and $[1]_{60} = e_1 + e_2 + e_3$.

7 Fields

Last Updated: 11 March 2023

Fields are probably the most widely used rings. For domains, the fraction field is the smallest field in which it can be embedded. Moreover, fields are characterized by their ideals and the ring homomorphisms.

7.0 Rings of Fractions

How are rational numbers constructed from integers? There is a formal way to introduce "demoninators" in a commutative ring.

Definition 7.0.0. Let R be a commutative ring. A subset D of R is *multiplicative* if every finite product of elements in D belongs to D.

This is the same as saying that $1_R \in D$ and the product of two elements of D belongs to D.

Examples 7.0.1.
- For any element r in the commutative ring R, the set $\{r^n \mid n \in \mathbb{N}\}$ of nonnegative powers is multiplicative.
- The set of elements in a commutative ring R that are not zero divisors is multiplicative.
- The intersection of multiplicative subsets is multiplicative. The intersection of all multiplicative subsets containing a set is the multiplicative set it generates.

The multiplicative set generated by a given subset consists of all the finite products of its elements.

Theorem 7.0.2. *For any multiplicative subset D in a commutative ring R, there exists a commutative ring $R[D^{-1}]$, called the* ring of fractions with demoninators in D*, and a ring homomorphism $\eta\colon R \to R[D^{-1}]$ with the following universal property:*
- *the elements in the set $\eta(D)$ are units in $R[D^{-1}]$;*
- *for any ring homomorphism $\psi\colon R \to S$ such that the elements in the set $\psi(D)$ are units in S, there exists a unique ring homomorphism $\widehat{\psi}\colon R[D^{-1}] \to S$ such that $\psi = \widehat{\psi}\,\eta$.*

$$\begin{tikzcd} R \arrow[r, "\psi"] \arrow[d, "\eta"'] & S \\ R[D^{-1}] \arrow[ur, "\widehat{\psi}"'] & \end{tikzcd}$$

Figure 7.1: Commutative diagram arising from Theorem 7.0.2

Proof. Consider the set $R \times D$ with the relation:

$$(r,d) \sim (s,e) \Leftrightarrow \text{there exists } c \in D \text{ such that } c\,(r\,e - s\,d) = 0.$$

We see that this relation is reflexive and symmetric. It is transitive because the equations $c\,(r\,e - s\,d) = 0$ and $b\,(s\,f - t\,e) = 0$ yield

$$\begin{aligned} c\,b\,e\,(r\,f - t\,d) &= b\,f\,c\,r\,e - c\,d\,b\,t\,e + b\,f\,c\,s\,d - b\,f\,c\,s\,d \\ &= b\,f\,\big(c\,(r\,e - s\,d)\big) + c\,d\,\big(b\,(s\,f - t\,e)\big) = 0 \end{aligned}$$

and $c\,b\,e \in D$. Let $R[D^{-1}] := (R \times D)/\sim$ be the quotient set under the equivalence relation. For any ordered pair (r,d), we write r/d for the equivalent class containing the pair (r,d) in $R[D^{-1}]$.

Two elements in $R[D^{-1}]$ can always be written in the form f/d and g/d with $f, g \in R$ and $d \in D$ with the same denominator. Given f/d and g/e is $R[D^{-1}]$, we have $f/d = f\,e/d\,e$ and $g/e = g\,d/d\,e$.

Consider two equivalence classes $f = r/d$ and $g = s/e$ in $R[D^{-1}]$. We claim that the equivalent classes $(r\,e + s\,d)/(d\,e)$ and $(r\,s)/(d\,e)$ are independent of the chosen representatives for f and g. Given another representative $f = r'/d'$, there exists c in D such that $c\,(r\,d' - r'\,d) = 0$ whence

$$\begin{aligned} c\big((r\,e + s\,d)(d'\,e) - (r'\,e + s\,d')(d\,e)\big) &= e^2\big(c\,(r\,d' - r'\,d)\big) = 0\,, \\ c\big((r\,s)(d'e) - (r'\,s)(d\,e)\big) &= e\,s\big(c\,(r\,d' - r'\,d)\big) = 0\,, \end{aligned}$$

In other words, we have $(r\,e + s\,d, d\,e) \sim (r'\,e + s\,d', d'\,e)$ and $(r\,s, d\,e) \sim (r'\,s, d'\,e)$. Hence, the binary operations on $R[D^{-1}]$ defined by

$$(f, g) \mapsto f + g = \frac{r\,e + s\,d}{d\,e} \qquad \text{and} \qquad (f, g) \mapsto fg = \frac{r\,s}{d\,e}$$

are well-defined. One verify that these two operations make $R[D^{-1}]$ into a commutative ring as follows:

$$\Big(\frac{r}{d}+\frac{s}{e}\Big)+\frac{t}{f} = \frac{r\,e+s\,d}{d\,e}+\frac{t}{f} = \frac{(r\,e+s\,d)\,f + t\,(d\,e)}{d\,e\,f} = \frac{r\,e\,f + s\,d\,f + t\,d\,e}{d\,e\,f} = \frac{r}{d}+\frac{s\,f+t\,e}{e\,f} = \frac{r}{d}+\Big(\frac{s}{e}+\frac{t}{f}\Big)$$

$$\frac{r}{d} + \frac{s}{e} = \frac{r\,e + s\,f}{d\,e} = \frac{s\,f + r\,e}{d\,e} = \frac{s}{e} + \frac{r}{d}$$

$$\frac{r}{d} + \frac{0}{1} = \frac{r\,1 + d\,0}{d\,1} = \frac{r}{d}$$

$$\frac{r}{d} + \frac{-r}{d} = \frac{r\,d - r\,d}{d^2} = \frac{0}{d^2} = \frac{0}{1}$$

$$\frac{r}{d}\Big(\Big(\frac{s}{e}\Big)\Big(\frac{t}{f}\Big)\Big) = \frac{r}{d}\Big(\frac{s\,t}{e\,f}\Big) = \frac{r\,s\,t}{d\,e\,f} = \Big(\frac{r\,s}{d\,e}\Big)\frac{t}{f} = \Big(\Big(\frac{r}{d}\Big)\Big(\frac{s}{e}\Big)\Big)\frac{t}{f}$$

$$\Big(\frac{r}{d}\Big)\Big(\frac{s}{e}\Big) = \frac{r\,s}{d\,e} = \frac{s\,r}{e\,d} = \Big(\frac{s}{e}\Big)\Big(\frac{r}{d}\Big)$$

$$\Big(\frac{1}{1}\Big)\Big(\frac{r}{d}\Big) = \frac{r}{d} = \Big(\frac{r}{d}\Big)\Big(\frac{1}{1}\Big)$$

$$\frac{r}{d}\Big(\frac{s}{e} + \frac{t}{f}\Big) = \frac{r}{d}\Big(\frac{s\,f + t\,e}{e\,f}\Big) = \frac{r\,(s\,f + t\,e)}{d\,e\,f} = \frac{r\,s}{d\,e} + \frac{r\,t}{d\,f} = \Big(\frac{r}{d}\Big)\Big(\frac{s}{e}\Big) + \Big(\frac{r}{d}\Big)\Big(\frac{r}{g}\Big)\,.$$

The additive identity is $0/1$ and the multiplicative identity is $1/1$.

Next, the map $\eta\colon R \to R[d^{-1}]$ defined by $\eta(r) = r/1$ is a ring homomorphism because we have

$$\eta(r + s) = \frac{r + s}{1} = \frac{r}{1} + \frac{s}{1} = \eta(r) + \eta(s)\,, \quad \eta(r\,s) = \frac{r\,s}{1} = \Big(\frac{r}{1}\Big)\Big(\frac{s}{1}\Big) = \eta(r)\,\eta(s)\,,$$

and $\eta(1) = 1/1$. For any element d in D, the multiplicative inverse of the element $d/1$ in $R[D^{-1}]$ is $1/d$.

Finally, consider a ring homomorphism $\psi\colon R \to S$ such that the elements in the image $\psi(D)$ are units. There exists a map $\widehat{\psi}\colon R[D^{-1}] \to S$ defined, for any equivalence class r/d in $R[D^{-1}]$, by $\widehat{\psi}(r/d) := \psi(r)\big(\psi(d)\big)^{-1}$. When $r/d = r'/d'$, there exists an element c in D such that $c\,(r\,d' - r'\,d) = 0$ which implies that $\psi(c)\,\big(\psi(r)\psi(d') - \psi(r')\psi(d)\big) = 0$. As $\psi(c)$, $\psi(d)$ and $\psi(d')$ are units, we obtain $\psi(r)\big(\psi(d)\big)^{-1} = \psi(r')\big(\psi(d')\big)^{-1}$. Since

$$\begin{aligned} \widehat{\psi}(r/d + s/e) &= \widehat{\psi}\big((r\,e + s\,d)/(d\,e)\big) = \psi(r\,e + s\,d)\big(\psi(d\,e)\big)^{-1} \\ &= \big(\psi(r)\,\psi(e) + \psi(s)\,\psi(d)\big)\big(\psi(d)\big)^{-1}\big(\psi(e)\big)^{-1} \\ &= \psi(r)\big(\psi(d)\big)^{-1} + \psi(s)\big(\psi(e)\big)^{-1} = \widehat{\psi}(r/d) + \widehat{\psi}(s/e)\,, \\ \widehat{\psi}\big((r/d)(s/e)\big) &= \widehat{\psi}\big((r\,s)/(d\,e)\big) = \psi(r\,s)\big(\psi(d\,e)\big)^{-1} \\ &= \psi(r)\,\psi(s)\,\big(\psi(d)\big)^{-1}\,\big(\psi(e)\big)^{-1} \\ &= \psi(r)\big(\psi(d)\big)^{-1}\,\psi(s)\,\big(\psi(e)\big)^{-1} = \widehat{\psi}(r/d)\,\widehat{\psi}(s/e)\,, \end{aligned}$$

and $\widehat{\psi}(1/1) = \psi(1_R)\big(\psi(1_R)\big)^{-1} = 1_S\big(1_S\big)^{-1} = 1_S$, the map ψ' is a ring homomorphism. By construction, we have $\widehat{\psi}\,\eta = \psi$. Moreover, the map $\widehat{\psi}$ is determined by this equation because we have both $\widehat{\psi}(r/s) = \widehat{\psi}\big((r/1)(1/s)\big) = \widehat{\psi}(r/1)\,\widehat{\psi}(1/s) = \psi(r)\,\widehat{\psi}(1/s)$ and $1 = \widehat{\psi}(1/1) = \widehat{\psi}(1/s)\,\widehat{\psi}(s/1) = \widehat{\psi}(1/s)\,\psi(s)$. □

Remark 7.0.3. The kernel of the unique map $\eta\colon R \to R[D^{-1}]$ is the set elements r in R such that there exists d in D such that $r\,d = 0$. For the map η to be injective, it is necessary and sufficient that the set D contain no zero divisor in R.

When $0 \in D$, the ring $R[D^{-1}]$ is the zero ring.

Definition 7.0.4. When multiplicative set D consists of the nonzero divisors in commutative ring R, the ring $R[D^{-1}]$ is the *total ring of fractions*. When R is a domain, the ring $R[D^{-1}]$ is the *field of fractions* of R.

Exercises

Problem 7.0.5. Consider two multiplicative subsets D and E a commutative ring R satisfying $D \subseteq E$. Let $\varphi\colon R[D^{-1}] \to R[E^{-1}]$ be the ring homomorphism defined, for any fraction r/d in $R[D^{-1}]$, by $\varphi(r/d) = r/d$. Show that the following are equivalent:

(a) The map φ is a ring isomorphism.
(b) For any element e in E, the fraction $e/1$ is a unit in $R[D^{-1}]$.
(c) For any element e in E, there exists an element s in R such that $e\,s \in D$.

7.1 Recognizing Fields

How do we identify fields among all commutative rings? Fields are characterized via their ideals and their ring homomorphisms.

Theorem 7.1.0. *For any nonzero commutative ring R, the following are equivalent:*

(a) *The ring 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 $0 \neq r \in I$. The ring element r is a unit, so $R = \langle 1\rangle = \langle r\rangle \subseteq I \subseteq R$ and $I = R$.

(b) ⇒ (c): Let S be a nonzero ring. For any ring homomorphism $\varphi\colon R \to S$, the ideal $\operatorname{Ker}(\varphi)$ is a proper ideal. It follows that $\operatorname{Ker}(\varphi) = \langle 0\rangle$ and the map φ is injective.

(c) ⇒ (a): Consider an element r in R that is not a unit. Hence, we have $\langle r\rangle \neq \langle 1\rangle$ and $S := R\big/\langle r\rangle$ is not the zero ring. Let $\pi\colon R \to S$ be the canonical surjection. By hypothesis, the map π is injective, so $\langle r\rangle = \operatorname{Ker}(\varphi) = \langle 0\rangle$ and $r = 0$. □

As a counterpoint to the previous theorem, we also want to determine when a quotient ring is a field and when there exists a surjective ring homomorphism onto a field.

Definition 7.1.1. Let R be a ring. By an abuse of language, an ideal I is *maximal* if its a maximal element (under inclusion) in the set of ideals distinct from R. In other words, an ideal I is maximal if and only if $I \neq \langle 1 \rangle$ and the only ideals containing I are I and R.

Corollary 7.1.2. *An ideal I in a commutative ring R is maximal if and only if the quotient ring R/I is a field.*

Proof. The Correspondence Theorem 6.2.0 shows that the ideals in R containing I are in bijection with the ideals in the quotient ring R/I. Theorem 7.1.0 demonstrates that the ring R/I is a field if and only if and only if it has two ideals: $\langle 0 \rangle$ and $\langle 1 \rangle$. It follows that the only ideals containing I are I and R if and only if the quotient ring R/I is a field. □

Remark 7.1.3. Theorem 2.2.4 demonstrates that the maximal ideals in the ring $\mathbb{Z}$ are precisely the principal ideals generated by a prime integer.

Theorem 7.1.4 (Krull 1929). *Every nonzero commutative ring R has a maximal ideal. Moreover, every proper ideal I in R is contained in a maximal ideal.*

Corollary 7.1.5. *There exists a surjective ring homomorphism from any nonzero commutative ring to a field.*

Proof. Let R be a nonzero commutative ring. By Theorem 7.1.4, there exists a maximal ideal M in R. Since Corollary 7.1.2 shows that the quotient ring R/M is a field, the canonical surjection $\pi \colon R \to R/I$ provides the desired ring homomorphism. □

To prove Theorem 7.1.4 requires an new axiom from set theory.

Definition 7.1.6. A *partially ordered set* or *poset* $\mathcal{X}$ is a set together with an order relation $\preccurlyeq$ such that

Reflexive: For any element $x \in \mathcal{X}$, we have $x \preccurlyeq x$.
Antisymmetric: The relations $x \preccurlyeq y$ and $y \preccurlyeq x$ imply that $x = y$.
Transitive: The relations $x \preccurlyeq y$ and $y \preccurlyeq z$ imply that $x \preccurlyeq z$.

Two elements x and y in $\mathcal{X}$ are *comparable* if $x \preccurlyeq y$ or $y \preccurlyeq x$. A *chain* in $\mathcal{X}$ is a subset where any two elements are comparable. An *upper bound* for a nonempty subset $\mathcal{Y}$ of $\mathcal{X}$ is an element x in $\mathcal{X}$ such that, for any element y in $\mathcal{Y}$, we have $y \preccurlyeq x$. A *maximal element* of a nonempty subset $\mathcal{Y}$ is an element y in $\mathcal{Y}$ such that, for any element z in $\mathcal{Y}$, we have $z \preccurlyeq y$.

The adjective "partial" indicates that not every pair of elements in a partially ordered set is required to be comparable under the order relation. In other words, there may be elements x and y such that neither $x \preccurlyeq y$ nor $y \preccurlyeq x$ hold.

Examples 7.1.7. Standard examples of posets include

- the real numbers ordered by the standard inequality $\leqslant$,
- the set of subsets of a given set ordered by inclusion $\subseteq$,

- the set of nonnegative integers ordered by divisibility, and
- the set of ideals in a commutative ring ordered by inclusion.

Remark 7.1.8. Posets may not have maximal elements. For example, real numbers $\mathbb{R}$, with the usual ordering, has no maximal elements.

Axiom 7.1.9 (Zorn's Lemma)**.** Any nonempty poset, in which every chain has an upper bound, has a maximal element. ■

Remark 7.1.10. Zorn's Lemma is a strengthening of the Well-Order Principle 0.2.6 or the Principle of Induction 0.0.0.

Proof of Krull's Theorem. The second statement implies the first, because the ideal $\langle 0 \rangle$ is a proper ideal in any nonzero ring.

Let I be a proper ideal in R. Consider the set $\mathcal{X}$ of all ideals in R that contain I and are not equal to R. Since $I \in \mathcal{X}$, the set $\mathcal{X}$ is nonempty. Partially order $\mathcal{X}$ by inclusion. Suppose that C is a chain in $\mathcal{X}$: for any ideals J and K in C, we have either $J \subseteq K$ or $K \subseteq J$. We claim that $J^* := \bigcup_{J \in C} J$ is an upper bound of C. For any ideal J in C, we clearly have $J \subseteq J^*$. It remains to prove that J^* is a proper ideal. For any elements f and g in J^* and any element r in R, it follows that f and g in J for some ideal J in the chain C. Since the elements $f + g$ and $r\,f$ both belong to J, the elements $f + g$ and $r\,f$ also belong to J^*, so J^* is an ideal. If $J^* = R$, then we would have $1 \in J^*$ and $1 \in J$ for some ideal J in the chain C which contradicts assumption that $J \neq R$. As every chain in $\mathcal{X}$ has an upper bound, Zorn's Lemma provides a maximal element. □

Remark 7.1.11. Zorn's Lemma is needed to prove that every vector space has a basis and that every field has an algebraic closure.

Exercises

Problem 7.1.12. Prove that $\mathbb{Z}/\langle 512 \rangle$ has exactly one maximal ideal.

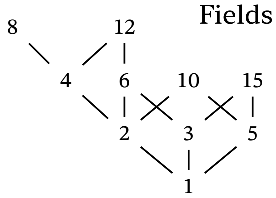

Figure 7.2: Part of the Hasse diagram for the poset $\mathbb{N}$ ordered by divisibility

Zorn's Lemma is equivalent to the Axiom of Choice. Kazimierz Kuratowski (1922) proved a variant and Max Zorn (1935) proposed it as a new axiom of set theory.