

5 Rings and Ideals

Copyright © 2025 by Gregory G. Smith
Last updated: 2025-10-09

Rings were devised as a common generalization for structures in number theory and the study of polynomial equations. Although their **conceptualization** began in the 1870s, the structural approach was solidified with the work of **Emmy Noether (1921)**.

5.0 Commutative Rings

A ring is an algebraic structure on a single underlying set with two binary operations. We emphasize the commutative case.

5.0.2 Definition. A *ring* is a nonempty set R with a pair of binary operations (called addition and multiplication) such that (*additive group*) under addition, R is an abelian group;

(*associativity*) $a(bc) = (ab)c$ and $1a = a1 = a$;

(*distributivity*) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

for any elements a, b , and c in R . A ring is *commutative* if $ab = ba$ for any elements a and b in R .

5.0.3 Example. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all commutative rings under the usual addition and multiplication. The quaternions $\mathbb{H}$ form a noncommutative ring. $\diamond$

5.0.4 Example. For any positive integer m , the quotient $\mathbb{Z}/\langle m \rangle$ is a commutative ring where the operations are inherited from $\mathbb{Z}$. $\diamond$

5.0.5 Example. Let R be a ring and let X be a set. The maps from X to R equipped with the pointwise operations form the *product ring* $R^X = \prod_{x \in X} R$. For any functions $f: X \rightarrow R$ and $g: X \rightarrow R$, the sum $f + g: X \rightarrow R$ and the product $fg: X \rightarrow R$ are defined by $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all x in X . The constant functions $x \mapsto 0_R$ and $x \mapsto 1_R$ are the additive and multiplicative identities respectively. $\diamond$

5.0.6 Example. The set of polynomials in the indeterminate x with coefficients in a commutative ring R form the *polynomial ring* $R[x]$. For any $a_n, a_{n-1}, \dots, a_0$ in R and any $b_m, b_{m-1}, \dots, b_0$ in R , addition is defined by

$$(a_n x^n + a_{n-1} x^{n-1} + \dots + a_0) + (b_n x^n + b_{n-1} x^{n-1} + \dots + b_0) \\ := (a_n + b_n) x^n + (a_{n-1} + b_{n-1}) x^{n-1} + \dots + (a_0 + b_0),$$

and multiplication is defined by

$$(a_n x^n + a_{n-1} x^{n-1} + \dots + a_0)(b_m x^m + b_{m-1} x^{m-1} + \dots + b_0) \\ := (a_n b_m) x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \dots + a_0 b_0.$$

In the product, the coefficient of x^k is $\sum_{i=0}^k a_{k-i} b_i$ in R . $\diamond$

5.0.7 Example. The set of formal power series in the indeterminate x with coefficients in a commutative ring R forms the commutative

David Hilbert (1897) introduced the word “ring” (more precisely “Zahlring”) into mathematics. Rather than a ‘hollow circular object’, think of an ‘organization acting to further its own interests’ such as a *criminal ring* or *spy ring*, or an ‘enclosed space’ such as a *circus ring* or *boxing ring*.

Contrary to some antiquated sources, rings *always* have a multiplicative identity 1. **Bjorn Poonen (2019)** makes a compelling argument for this convention. Nevertheless, “ring-like” structures lacking a multiplicative identity (customarily called algebras) do arise naturally.

Square matrices with entries in a commutative ring under the usual matrix operations form the quintessential noncommutative ring.

One may assume that the nonnegative integers n and m satisfy $n \geq m$ and $b_n = b_{n-1} = \dots = b_{m+1} = 0$.

ring $R[[x]]$. For any elements $a_0, a_1, a_2, \dots$ in R and any $b_0, b_1, b_2, \dots$ in R , addition and multiplication are defined by

$$\begin{aligned} \left(\sum_{j=0}^{\infty} a_j x^j \right) + \left(\sum_{j=0}^{\infty} b_j x^j \right) &:= \sum_{j=0}^{\infty} (a_j + b_j) x^j, \\ \left(\sum_{j=0}^{\infty} a_j x^j \right) \left(\sum_{j=0}^{\infty} b_j x^j \right) &:= \sum_{j=0}^{\infty} \left(\sum_{k=0}^j a_k b_{j-k} \right) x^j. \end{aligned} \quad \diamond$$

5.0.8 Lemma (Basic properties). *Let R be a commutative ring.*

(multiplication by 0) *For any element a in R , we have $0a = 0$.*

(multiplication by -1) *When $-a$ denotes the additive inverse of the element a in R , we have $(-1)(-a) = a$.*

(zerodivisors) *When the nonnegative integer n satisfies*

$$n1 = \underbrace{1 + 1 + \dots + 1}_{n \text{ times}} = 0$$

in R , we have $na = 0$ for any element a in R .

(binomial formula) *For any pair of elements a and b in R , and any nonnegative integer n , we have*

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

For any integers n and k , the **binomial coefficient** $\binom{n}{k}$ is defined to be the number of subsets of the set $[n] := \{1, 2, \dots, n\}$ having cardinality k .

Proof. Distributivity in the ring R gives $0a = (0 + 0)a = 0a + 0a$. Adding the additive inverse $-0a$ to both sides yields $0a = 0$.

Multiplication by 0 and distributivity in the ring R establish that $0 = (0)(-a) = (-1 + 1)(-a) = (-1)(-a) + (-a)$. Adding a to both sides proves that $(-1)(-a) = a$.

The multiplicative identity and the associativity of multiplication in the ring R give $na = n(1a) = (n1)a = 0a = 0$.

We proceed by induction on n . For the base case $n = 0$, we have $(a + b)^0 = 1 = \binom{0}{0} a^0 b^0$. The induction hypothesis and the addition identity for binomial coefficients give

$$\begin{aligned} (a + b)^{n+1} &= (a + b)(a + b)^n = (a + b) \left(\sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \right) \\ &= \left(\sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} \right) + \left(\sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1} \right) \\ &= \sum_{k=0}^{n+1} \left[\binom{n}{k-1} + \binom{n}{k} \right] a^k b^{n+1-k} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}. \quad \square \end{aligned}$$

5.0.9 Example. Suppose that R is a ring with $1 = 0$. For any element a in R , it follows that $a = 1a = 0a = 0$, so R consists of a single element. This ring is predictably called the **zero ring**. $\diamond$

5.0.10 Definition. A subset S of a ring R is a **subring** if the restriction of addition and multiplication on R induces a ring structure on S with the same multiplicative identity.

The inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are all subrings. Every subring of $\mathbb{Z}$ or $\mathbb{Z}/\langle m \rangle$ contains 1 and hence must be equal to the whole ring.

5.1 Homomorphisms and Fields

The set maps that preserve ring structures are just special group homomorphisms, so their inherent traits are very similar.

5.1.1 Definition. Let R and S be rings. A *ring homomorphism* is a map $\varphi : R \rightarrow S$ such that, for any elements a and b in R , we have

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

A nonzero ring is not a group under multiplication. Not insisting that $\varphi(1_R) = 1_S$ leads to pathologies.

5.1.2 Remark. The composition of ring homomorphisms is a ring homomorphism. The methods used to prove Proposition 2.0.6 show that a ring homomorphism is isomorphism if and only if it is a bijective homomorphism.

5.1.3 Example. Let R be a ring. The map $n \mapsto n \cdot 1_R$ is the unique ring homomorphism from $\mathbb{Z}$ to R . In particular, the identity map is the unique ring endomorphism of the ring $\mathbb{Z}$. $\diamond$

For any nonnegative integer n , we set

$$n \cdot 1_R := \sum_{i=1}^n 1_R = 1_R + 1_R + \cdots + 1_R,$$

$$(-n) \cdot 1_R := - \sum_{i=1}^n 1_R,$$

5.1.4 Example. Complex conjugation $z = a + bi \mapsto \bar{z} = a - bi$ is an automorphism of the ring $\mathbb{C}$. $\diamond$

5.1.5 Example. Let R be a commutative ring and let a be an element in R . The *evaluation map* $\text{ev}_a : R[x] \rightarrow R$ defined by $\text{ev}_a(f) = f(a)$ is a ring homomorphism. $\diamond$

Unlike normal groups and group homomorphisms, the kernel of a ring homomorphism is not a distinguished type of subring.

5.1.6 Definition. A subset I of a commutative ring R is an *ideal* if it is an additive subgroup and, for any r in R and any a in I , the product ra belongs to I . Equivalently, a subset I is an ideal if, for any r and s in R and any a and b in I , the element $ra + sb$ lies in I .

Richard Dedekind (1871) introduced both the concept and the term “ideal”.

5.1.7 Example. For any ring R , both R and $\{0\}$ are ideals. $\diamond$

5.1.8 Example. For any element r in R , the set of multiples of r is the ideal $\langle r \rangle$, which is called the *principal ideal* generated by r . $\diamond$

5.1.9 Remark. Every intersection of ideals is an ideal; compare with Lemma 1.2.8. For any subset X of a ring R , there exists a unique smallest ideal $\langle X \rangle$ containing X called the ideal *generated by* X .

5.1.10 Proposition. Let $\varphi : R \rightarrow S$ be a ring homomorphism. The kernel $\text{Ker}(\varphi) := \{r \in R \mid \varphi(r) = 0\}$ is an ideal in R and the image $\text{Im}(\varphi)$ is a subring of S . When R and S are nonzero rings, we have $\text{Ker}(\varphi) \neq R$.

Corollary 2.0.10 implies that a ring homomorphism is injective if and only if its kernel is trivial.

Proof. For any element r in R and any a in $\text{Ker}(\varphi)$, compatibility with multiplication gives $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$, so $ra \in \text{Ker}(\varphi)$. As Proposition 2.0.8 shows that $\text{Ker}(\varphi)$ is an additive subgroup of R , we deduce that $\text{Ker}(\varphi)$ is an ideal. Since $1_R \notin \text{Ker}(\varphi)$ unless $S = 0$ or $R = 0$, the kernel is a proper ideal when R and S are nonzero rings.

For any a' and b' in $\text{Im}(\varphi)$, there exists a and b in R such that $\varphi(a) = a'$ and $\varphi(b) = b'$, so $\varphi(ab) = \varphi(a)\varphi(b) = a'b' \in \text{Im}(\varphi)$. As Proposition 2.0.8 shows that $\text{Im}(\varphi)$ is an additive subgroup of S containing 1_S , so this image is a subring. $\square$

5.1.11 Definition. A ring element is a **unit** if it has a multiplicative inverse. The set $R^\times$ of all units in a commutative ring R forms an abelian group under multiplication.

For instance, we have $\mathbb{Z}^\times = \{1, -1\} \cong \mu_2$ and $(\mathbb{Z}/\langle 6 \rangle)^\times = \{1, 5\} \cong \mu_2$.

5.1.12 Proposition. A formal power series $f := \sum_{n=0}^{\infty} r_n x^n$ in $R[[x]]$ is a unit if and only if the coefficient r_0 of the monomial x^0 is a unit in R .

Proof. When $g = \sum_{n \geq 0} s_n x^n$ in $R[[x]]$ satisfies $fg = 1$, the definition of multiplication in $R[[x]]$ implies that $r_0 s_0 = 1$, so r_0 is a unit in R .

Suppose that r_0 is a unit in R . Recursively defining the element s_n in R , for all nonnegative integers n , by

$$s_0 := r_0^{-1}, \quad s_1 := r_0^{-1}(-r_1 s_0), \quad \dots, \quad s_n := r_0^{-1} \left(- \sum_{i=1}^n r_i s_{n-i} \right),$$

we obtain $\left(\sum_{n=0}^{\infty} r_n x^n \right) \left(\sum_{n=0}^{\infty} s_n x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n r_k s_{n-k} \right) x^n = 1$. $\square$

Rings with the maximal set of units are especially important.

5.1.13 Definition. A **field** is a nonzero commutative ring in which every nonzero element is a unit.

5.1.14 Definition. A ring R is a **domain** if its nonzero and the product of nonzero elements in R is nonzero.

5.1.15 Proposition. Every field is a domain.

Proof. Let a and b be elements in a field. Whenever $ab = 0$ and $a \neq 0$, it follows that $b = a^{-1}(ab) = a^{-1}(0) = 0$. $\square$

5.1.16 Proposition. Any finite domain is a field.

Proof. Let R be a finite domain and let a be a nonzero element in R . The map $x \mapsto ax$ is injective, because R is a domain. Since R is finite, it is also surjective. Hence, there exists b in R such that $ab = 1$. As a was arbitrary, the domain R is a field. $\square$

5.1.17 Proposition. The quotient ring $\mathbb{Z}/\langle m \rangle$ is a domain if and only if the integer m is a prime.

Proof. Suppose that m is prime. For any integer p and q satisfying $pq \equiv 0 \pmod{m}$, it follows m divides p or q , so either $p \equiv 0 \pmod{m}$ or $q \equiv 0 \pmod{m}$. Thus, the quotient ring $\mathbb{Z}/\langle m \rangle$ is a domain.

Suppose that m is not prime. Hence, there exists integers p and q such that $m = pq$ and $1 < p \leq q < m$. It follows that $p \not\equiv 0 \pmod{m}$ and $q \not\equiv 0 \pmod{m}$, but $pq \equiv 0 \pmod{m}$. Therefore, the quotient ring $\mathbb{Z}/\langle m \rangle$ is not a domain. $\square$

Some of our favourite sets of numbers including $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields. However, the ring $\mathbb{Z}$ is a domain but not a field.

Combining Propositions 5.1.16–5.1.17, we see that $\mathbb{Z}/\langle m \rangle$ is a field if and only if m is a prime. For a prime number p , the finite field $\mathbb{Z}/\langle p \rangle$ is frequently denoted by $\mathbb{F}_p$.

5.2 Isomorphism Theorems

Just as with groups, ring theory has basic results describing some universal features of homomorphisms, quotients, and subobjects.

5.2.1 Theorem. *Let I be an ideal in a commutative ring R . The quotient R/I inherits multiplication from R and the canonical map $\pi: R \rightarrow R/I$, defined by $\pi(r) = r + I$ for any r in R , is a surjective ring homomorphism.*

Sketch of proof. For any a and b in R , multiplication on the quotient R/I is defined by $(a + I)(b + I) := ab + I$. Consider $a + I = a' + I$ and $b + I = b' + I$ for some a' and b' in R , so that $a - a' \in I$ and $b - b' \in I$. To demonstrate 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 2.3.13, it remains to verify that this product is associative, commutative, distributive, with $1 + I$ as the identity. $\square$

5.2.2 Corollary. *Let $\varphi: R \rightarrow S$ be a ring homomorphism. For any ideal I in R and any ideal J in S satisfying $\varphi(I) \subseteq J$, the map $\bar{\varphi}: R/I \rightarrow S/J$, defined by $\bar{\varphi}(r + I) = \varphi(r) + J$ for any r in R , is a ring homomorphism.*

Proof. As $\bar{\varphi}(1_R + I) = \varphi(1_R) + J = 1_S + J$, it suffices by Corollary 2.3.14 to check that the map $\bar{\varphi}$ is compatible with multiplication:

$$\begin{aligned} \bar{\varphi}((a + I)(b + I)) &= \bar{\varphi}(ab + I) = \varphi(ab) + J = \varphi(a)\varphi(b) + J \\ &= (\varphi(a) + J)(\varphi(b) + J) = \bar{\varphi}(a + I)\bar{\varphi}(b + I). \end{aligned} \quad \square$$

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

Proof. As $\tilde{\varphi}(1_R + I) = \varphi(1_R) = 1_S$, it suffices by Theorem 3.0.1 to check that the map $\tilde{\varphi}$ is compatible with multiplication:

$$\begin{aligned} \tilde{\varphi}((a + I)(b + I)) &= \tilde{\varphi}(ab + I) = \varphi(ab) \\ &= \varphi(a)\varphi(b) = \tilde{\varphi}(a + I)\tilde{\varphi}(b + I). \end{aligned} \quad \square$$

5.2.4 Example. We claim that $\mathbb{Z}[i]/\langle 1 + 3i \rangle \cong \mathbb{Z}/\langle 10 \rangle$. To prove this claim, consider the unique ring homomorphism $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}[i]/\langle 1 + 3i \rangle$. Since $i = (-1)(-i) = (3i)(-i) = 3$ in $\mathbb{Z}[i]/\langle 1 + 3i \rangle$, the coset containing $a + bi \in \mathbb{Z}[i]$ equals the coset containing $a + 3b$, so φ is surjective. For any $n \in \text{Ker}(\varphi)$, we see that $n \in \langle 1 + 3i \rangle$. Hence, there are integers c and d such that $n = (c + di)(1 + 3i) = (c - 3d) + (3c + d)i$. Since $n \in \mathbb{Z}$, we see that $3c = -d$ and $n = c + 3(-d) = c + 3(3c) = 10c$. We conclude that $\text{Ker}(\varphi) \subseteq \langle 10 \rangle$. We also have $3^2 = -1$ or $10 = 0$ in $\mathbb{Z}[i]/\langle 1 + 3i \rangle$, so $\langle 10 \rangle \subseteq \text{Ker}(\varphi)$. Therefore, the First Isomorphism Theorem yields the isomorphism $\mathbb{Z}/\langle 10 \rangle \cong \mathbb{Z}[i]/\langle 1 + 3i \rangle$. $\diamond$

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ \pi \downarrow & & \uparrow \iota \\ R/I & \xrightarrow{\tilde{\varphi}} & \text{Im}(\varphi) \end{array}$$

Figure 5.1: Commutative diagram arising from Theorem 5.2.3

5.2.5 Example. We claim 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 $(f(x), g(y))$ such that $f(0) = g(0)$. 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 $\text{ev}_{y=0} : \mathbb{C}[x, y] \rightarrow \mathbb{C}[x]$. Similarly, we have $\mathbb{C}[x, y]/\langle x \rangle \cong \mathbb{C}[y]$. Consider the map $\mathbb{C}[x, y] \rightarrow \mathbb{C}[x] \times \mathbb{C}[y]$ defined, for all f in $\mathbb{C}[x, y]$, by $f(x, y) \mapsto (f(x, 0), f(0, y))$. The kernel is $\langle x \rangle \cap \langle y \rangle = \langle xy \rangle$. The First Isomorphism Theorem completes the proof. $\diamond$

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

5.2.6 Second Isomorphism Theorem. Let R be a commutative ring. For all ideals I in R and all subrings S in 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. Consider the map $\varphi : S \rightarrow (S + I)/I$ defined by $\varphi(s) := s + I$ for any s in S . As $\varphi(1_S) = 1_S + I$, it suffices by Theorem 3.0.4 to check that this map is compatible with multiplication:

$$\varphi(st) = st + I = (s + I)(t + I) = \varphi(s)\varphi(t). \quad \square$$

5.2.7 Third Isomorphism Theorem. Let I and J be nested ideals in a commutative ring R . 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. Consider the map $\varphi : R/I \rightarrow R/J$ defined by $\varphi(r + I) = r + J$ for all r in R . As $\varphi(1_R + I) = 1_R + J$, it suffices by Theorem 3.0.5 to check that this map is compatible with multiplication:

$$\varphi(rs + I) = rs + J = (r + J)(s + J) = \varphi(r + I)\varphi(s + I). \quad \square$$

5.2.8 Correspondence Theorem. Let I be an ideal in R . The canonical map $\pi : R \rightarrow R/I$ 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 . $\blacksquare$

Compare with Theorem 3.0.6.

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

- R is a field;
- the only ideals in R are $\langle 0 \rangle$ and $\langle 1 \rangle$;
- every ring homomorphism from R to a nonzero ring is injective.

Proof.

$a \Rightarrow b$: Let I be a nonzero ideal in R and let a be a nonzero element in I . As R is a field, the element a is a unit, so $R = \langle 1 \rangle \subseteq \langle a \rangle \subseteq I \subseteq R$.
 $b \Rightarrow c$: For any ring homomorphism $\varphi : R \rightarrow S$, the kernel $\text{Ker}(\varphi)$ is a proper ideal. It follows that $\text{Ker}(\varphi) = \langle 0 \rangle$, so φ is injective.
 $c \Rightarrow a$: Suppose a in R is not a unit. It follows that $\langle a \rangle \neq \langle 1 \rangle$ and $S = R/\langle a \rangle$ is a nonzero ring. Let $\pi : R \rightarrow S$ be the canonical map. The map π being injective gives $\langle a \rangle = \text{Ker}(\pi) = \langle 0 \rangle$ and $a = 0$. $\square$

5.3 Maximal and Prime Ideals

Some ideals have greater significance.

5.3.1 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 $I \subset J \subset R$.

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

Proof. By definition, the ideal I in R is maximal if and only if it is contained in two ideal: I and R . Theorem 5.2.8 shows that the ideals in R containing the ideal I correspond to the ideals in the quotient ring R/I . Proposition 5.2.9 demonstrates that R/I is a field if and only if and only if it has two ideals: $\langle 0 \rangle$ and $\langle 1 \rangle$. $\square$

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

Surprisingly, the existence of a maximal ideal in all commutative rings impinges upon the latent axioms of set theory.

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

5.3.5 Zorn's Lemma. Any nonempty partially order set, such that every chain has an upper bound, has a maximal element. $\square$

5.3.6 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. $\square$

Weakening the condition on the associated quotient ring leads to possibly a more influential type of ideals.

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

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

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

Wolfgang Krull (1929) first proved the Theorem 5.3.6 by transfinite induction. Hodges (1979) shows that Krull's Theorem is equivalent to Zorn's Lemma.

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.

5.3.8 Proposition. *An ideal I is 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 element f in R , let $\bar{f}$ denote its image under the canonical map $\pi: R \rightarrow R/I$.

Suppose that I is a prime ideal. When the product fg is in the ideal I , it follows that $\bar{f}\bar{g} = 0 \in R/I$. Since R/I is a domain, it follows that $\bar{f} = 0$ or $\bar{g} = 0$, so either $f \in I$ or $g \in I$.

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

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

5.3.10 Definition. The ideals I and J in a commutative ring R are *comaximal* if $I + J = R$. Equivalently, no prime ideal in R contains both I and J .

5.3.11 Theorem. *Let n be a positive integer. 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 ideals I_k and I_j are comaximal;*
 - the canonical ring homomorphism $\varphi: R \rightarrow \prod_j (R/I_j)$ is surjective.*
- If these conditions hold, then we have $I = \bigcap_j I_j = \prod I_j$ and the canonical map $\bar{\varphi}: R/I \rightarrow \prod_j (R/I_j)$ is bijective.*

Sketch of proof. Suppose that $n = 2$. Set $I := I_1$ and $J := I_2$. Consider the elements f in I and g in J such that $1_R = f + g$. It follows that

$$\varphi(f) = (f + I, 1 - g + J) = (I, 1 + J),$$

$$\varphi(g) = (1 - f + I, g + J) = (1 + I, J).$$

For any elements r and s in R , we see that

$$\varphi(sf + rg) = \varphi(s)\varphi(f) + \varphi(r)\varphi(g) = (r + I, s + J),$$

which establishes that φ is surjective. Moreover, for any h in the intersection $I \cap J$, 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, proceed by induction on n . $\square$

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

Any two distinct maximal ideals are comaximal.

The earliest version of Theorem 5.3.11, 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*.

5.4 Exercises

5.4.1 Problem. Determine which of the following statements are true. If a statement is false, then provide a counterexample.

- i. The empty set $\emptyset$ has a unique ring structure.
- ii. A subset S of a ring R is a subring if and only if it is a subgroup under addition, closed under multiplication, and contains 1_R .
- iii. The intersection of any family of subrings is also a subring.
- iv. Let X be any subset of a commutative ring R . The set of elements r in R such that $rx = 0$ for all x in X is an ideal.
- v. For any unit a in a ring R , the map $x \mapsto axa^{-1}$ is a ring endomorphism of R .
- vi. There exists a ring homomorphism from any nonzero commutative ring to a field.
- vii. Any subring of a domain is also a domain.
- viii. There is a domain containing exactly 10 elements.
- ix. For any relatively prime integers m and n , the ideals $\langle m \rangle$ and $\langle n \rangle$ in $\mathbb{Z}$ are comaximal.

5.4.2 Problem. Let $\mathbb{F}_4$ denote the set of all (2×2) -matrices of the form

$$\begin{bmatrix} a & b \\ b & a+b \end{bmatrix}$$

where a and b are elements in $\mathbb{Z}/\langle 2 \rangle$.

- i. Establish that $\mathbb{F}_4$ is a commutative ring under the usual matrix operations.
- ii. Demonstrate that $\mathbb{F}_4$ is a field with exactly four elements.

5.4.3 Problem. Let R be a commutative ring. An element r in R is *nilpotent* if $r^n = 0$ for some positive integer n .

- i. For any nilpotent element r in R , prove that $1 - r$ is a unit in R .
- ii. Prove the set of all nilpotent elements in R is an ideal.

5.4.4 Problem. Let R be a commutative ring and consider elements f and g in R . Show that the canonical image of the product fg in the quotient ring $R/\langle f - f^2g \rangle$ is an idempotent. Give an example where this idempotent is distinct from 0 and 1.

5.4.5 Problem. Let R and S be commutative rings and let $\varphi: R \rightarrow S$ and $\psi: R \rightarrow S$ be ring homomorphisms. Is the set of all elements f in R such that $\varphi(f) = \psi(f)$ a subring of R ?

Can the false statements be salvaged in some way? In other words, can one find a closely related nontrivial true statement.

Bibliography

- Arnold, Vladimir I. 1998. *On teaching mathematics*, Russian Math. Surveys 53, no. 1, 229–236.
- Cayley, Arthur. 1854. *On the theory of groups, as depending on the symbolic equation $\theta^n = 1$* , Phil. Mag. (4) 42, no. 7, 40–47.
- . 1893. *Note on the so-called quotient G/H in the theory of groups*, Amer. J. Math. 15, no. 4, 387–388.
- Cauchy, Augustin Louis. 1844. *Mémoire sur les arrangements que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre*, Exercices d'analyse et de physique mathématique 3, 151–252.
- Chevalley, Claude. 1943. *On the theory of local rings*, Ann. of Math. (2) 44, 690–708.
- Cox, David A. 2011. *Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first*, Amer. Math. Monthly 118, no. 1, 3–21.
- Dedekind, Richard. 1871. *Supplement X*, in *Vorlesungen über Zahlentheorie* by Peter Gustav Lejeune Dirichlet, Braunschweig: Vieweg.
- de Groot, Johannes. 1959. *Groups represented by homeomorphism groups*, Math. Ann. 138, 80–102.
- Dyck, Walther. 1882. *Gruppentheoretische Studien*, Math. Ann. 20, no. 1, 1–44.
- Eisenstein, Gotthold. 1850. *Über die Irreducibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt*, J. Reine Angew. Math. 39, 160–179.
- Frucht, Roberto. 1939. *Herstellung von Graphen mit vorgegebener abstrakter Gruppe*, Compositio Math. 6, 239–250.
- Galois, Évariste. 1846. *Œuvres Mathématiques*, J. Math. Pures Appl. XI, 381–444.
- Granville, Andrew. 2024. *It is not "Bézout's identity"*. available at [arXiv:2406.15642](https://arxiv.org/abs/2406.15642) [math.HO].
- Hilbert, David. 1890. *Über die Theorie der algebraischen Formen*, Mathematische Annalen 36, 473–534.
- . 1897. *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung 4, no. I–XVIII, 175–546.
- Hodges, Wilfrid. 1979. *Krull implies Zorn*, J. London Math. Soc. (2) 19, no. 2, 285–287.
- Jordan, Camille. 1861. *Mémoire sur le nombre des valeurs des fonctions*, Journal de l'École polytechnique 22, 113–194.
- . 1870. *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris. 667 p.
- Klein, Felix. 1884. *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Teubner, Leipzig.
- Krull, Wolfgang. 1929. *Idealtheorie in Ringen ohne Endlichkeitsbedingung*, Math. Ann. 101, no. 1, 729–744.
- Lagrange, Joseph-Louis. 1771. *Suite des réflexions sur la résolution algébrique des équations. Section troisième. De la résolution des équations du cinquième degré & des degrés ultérieurs*, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin 5, no. 4, 138–254.
- . 1795. *Leçon Cinquième. Sur l'usage des courbes dans la solution des problèmes*, Leçons Élémentaires sur les Mathématiques. Republished in Serret, Joseph-Alfred, ed. (1877). *Oeuvres de Lagrange*. Vol. 7. Gauthier-Villars. pp. 271–287.
- Miller, George Abram. 1910. *On a method due to Galois*, The Quarterly Journal of Pure and Applied Mathematics 41, 382–384.
- Möbius, August F. 1832. *Über eine besondere Art von Umkehrung der Reihen*, J. Reine Angew. Math. 9, 105–123.
- Noether, Emmy. 1921. *Idealtheorie in Ringbereichen*, Math. Ann. 83, no. 1-2, 24–66.
- . 1927. *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Math. Ann. 96, no. 1, 26–61.
- Novikov, Pëtr Sergeevich. 1955. *Ob algoritmičeskoj nerazrešimosti problemy toždestva slov v teorii grupp*, Izdat. Akad. Nauk SSSR, Moscow. Trudy Mat. Inst. Steklov. no. 44.

- Poonen, Bjorn. 2019. *Why all rings should have a 1*, Math. Mag. 92, no. 1, 58–62.
- Sabidussi, Gert. 1960. *Graphs with given infinite group*, Monatsh. Math. 64, 64–67.
- Schönemann, Theodor. 1846. *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, J. Reine Angew. Math. 32, 93–105.
- Smith, Henry J. S. 1861. *On systems of linear indeterminate equations and congruences*, Philos. Trans. Roy. Soc. . 151, 293–32.
- Sylow, Ludwig. 1872. *Théorèmes sur les groupes de substitutions*, Math. Ann. 5, no. 4, 584–594.
- Waring, Edward. 1779. *Problems concerning interpolations*, Philosophical Transactions of the Royal Society 69, 59–67.
- Wielandt, Helmut. 1959. *Ein Beweis für die Existenz der Sylowgruppen*, Arch. Math. 10, no. 1, 401–402.
- Zorn, Max. 1935. *A remark on method in transfinite algebra*, Bull. Amer. Math. Soc. 41, no. 10, 667–670.