Modern Algebra: Comprehensive

Connor Castillo

February 4, 2026

Contents

1 Introduction

1.1 Definition and Axioms

Definition 1.1. A **ring** $(R, +, \cdot)$ is a set equipped with two binary operations such that

i) $(R, +)$ is an abelian group,

ii) Multiplication is associative, i.e. $(ab)c = a(bc)$ for all $a, b, c \in R$,

iii) Multiplication distributes over addition from the left and right

iv) Multiplicative and Additive Identity contained in R

If multiplication is commutative, we say that R is a **commutative ring**.

This definition naturally brings fields into question. The biggest distinction between a field and a ring is that a field is always a commutative ring, and can be thought of us two groups with distribution. By definition, we didn't specify that the multiplication operation forms a group. This is because not all elements of the ring have multiplicative inverses.

Definition 1.2. Any element $a \in R$ with a multiplicative inverse a^{-1} is a **unit**.

Example 1.1. Consider the set of integers $\mathbb{Z}$. By definition, this is a ring. However, notice that the only units of this ring are 1 and -1. An example is

$$2 \cdot x = 1$$

has no solutions in $\mathbb{Z}$.

Non-Example 1.1. Now consider $2\mathbb{Z}$, the set of all event integers. This fails to satisfy the properties of a ring, as it does not contain the multiplicative identity.In the case that an identity like this is not contained within the set, we have a side classification known as a **rng**, pronounced "rung."

Proposition 1.1 (Absorbing Property of Zero). For any $a \in R$ we have that $0 \cdot a = a \cdot 0 = 0$.

Proof. Let $a \in R$. Since $0 = 0 + 0$, distributivity gives

$$a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0.$$

Adding the additive inverse of $a \cdot 0$ to both sides yields

$$0 = a \cdot 0.$$

■

Definition 1.3. Let $(R, +, \cdot)$ be a ring. A subset $S \subseteq R$ is called a **subring** of R if

i) S is closed under addition and multiplication,

ii) $(S, +)$ is a subgroup of $(R, +)$.

In a sense, we can think of the subring as having an analog definition from subgroups. That is, they are simply subsets of the larger ring R that is it itself a complete ring.

1.2 Subrings

Proposition 1.2 (Subring Test). If $1 \in S$ and S is closed under subtraction and multiplication, then S is a subring of R

Proof. Assume $1 \in S$ and S is closed under subtraction and multiplication. Then we must have that $1 - 1 = 0$. Thus, $0 \in S$. To produce additive inverses, we simply subtract an element $a \in S$ from 0. Then finally, we can express addition in S for two elements $a, b \in S$ as

$$a + b = a - (-b) \in S$$

Since commutativity and associativity are inherited from R, this shows that S is a subring. $\blacksquare$

Example 1.2. Show that the set of Gaussian integers

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$. Observe that

$$0 = 0 + 0i \in \mathbb{Z}[i] \quad \text{and} \quad 1 = 1 + 0i \in \mathbb{Z}[i].$$

Let $a + bi, c + di \in \mathbb{Z}[i]$.
First, we'll show closure under subtraction:

$$(a + bi) - (c + di) = (a - c) + (b - d)i \in \mathbb{Z}[i].$$

Now we'll show closure under multiplication:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i],$$

since $ac - bd, ad + bc \in \mathbb{Z}$. By the subring test, $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

Example 1.3. Show that The set of rational numbers $\frac{a}{b}$, where b is not divisible by 3 when written in reduced form, is a subring of $\mathbb{Q}$.
Define

$$S = \left\{ \frac{a}{b} : a \in \mathbb{Z},\ b \in \mathbb{Z} \setminus 3\mathbb{Z} \right\}.$$

First, note that

$$1 = \frac{1}{1} \in S,$$

since 1 is not divisible by 3. Let $\frac{a}{b}, \frac{c}{d} \in S$, where b and d are not divisible by 3.

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}.$$

Since b and d are not divisible by 3, their product bd is also not divisible by 3.

Thus $\frac{ad-bc}{bd} \in S$.

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Again, bd is not divisible by 3, so $\frac{ac}{bd} \in S$. By the subring test, S is a subring of $\mathbb{Q}$.

1.3 Polynomial Rings R[x]

Definition 1.4. Let R be a commutative ring with $1 \in R$. The **polynomial ring** over R in the **indeterminate** x, denoted $R[x]$, is the set

$$R[x] = \left\{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : n \in \mathbb{Z}_{\geq 0}, a_i \in R\right\}$$

where n is the **degree** of the polynomial

Since the monomials x^k are linearly independent variables, two polynomials are equivalent if and only if their coefficients are the same. Fundamentally, the structure of the polynomial ring isn't determined reliant on the variable x whatsoever. The elements of $R[x]$ are really just sequences of coefficients from R.

Remark 1.1. Note that when we say R is a subring, we're specifically saying that R is embedded into the polynomial ring as constant polynomials. Their sequence representation is just

$$a \in R \to (a, 0, 0, 0, ...)$$

Proposition 1.3. There is a unique commutative ring structure on the set of polynomials $R[x]$ having these properties:

i) Addition of polynommials is defined

ii) Multiplication of polynomials is defined

iii) R becomes a subring of $R[x]$, when the elements R are identified with constant polynomials.

Proof. We first show that $R[x]$ is a ring under polynomial addition and multiplication.Let

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{and} \quad g(x) = \sum_{j=0}^{m} b_j x^j$$

be polynomials in $R[x]$.
Closure under addition: Define

$$(f+g)(x) = \sum_{k=0}^{\max\{n,m\}} (a_k + b_k)x^k,$$

where missing coefficients are taken to be zero. Since $a_k + b_k \in R$, we have $f + g \in R[x]$.
Closure under multiplication: Define

$$(fg)(x) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) x^k.$$

Each coefficient $\sum_{i+j=k} a_i b_j$ lies in R, so $fg \in R[x]$. Addition and multiplication are associative and distributive because these properties hold in R, and the zero and unit elements are the constant polynomials 0 and 1, respectively. Hence $R[x]$ is a ring. Finally, identify each real number $a \in R$ with the constant polynomial a. Under this identification, addition and multiplication in R agree with those in $R[x]$, so R is a subring of $R[x]$. ■

Proposition 1.4 (Division Algorithm). Given polynomials $f(x)$ and $g(x)$ with f being monic, we can find unique polynomials $q(x)$ and $r(x)$ with $\deg(r) < \deg(f)$ such that

$$g(x) = f(x)q(x) + r(x)$$

Remark 1.2. We adopt the convention $\deg(0) = -\infty$. This choice preserves standard degree identities, such as

$$\deg(f \cdot 0) = \deg(f) + \deg(0),$$

which would otherwise fail. With this convention, the degree condition $\deg(r) < \deg(f)$ in the Division Algorithm remains meaningful even when the remainder $r = 0$, allowing the proof of uniqueness to proceed without a separate case.

Proof. Subtracting the two expressions for $g(x)$ gives

$$0 = f(x)\Big(q(x) - q'(x)\Big) + \Big(r(x) - r'(x)\Big).$$

Rearranging,

$$f(x)\Big(q(x) - q'(x)\Big) = r'(x) - r(x).$$

If $q(x) - q'(x) \neq 0$, then the left-hand side is a nonzero multiple of $f(x)$ and hence has degree at least $\deg(f)$. However, since $\deg(r), \deg(r') < \deg(f)$, the right-hand side satisfies

$$\deg\Big(r'(x) - r(x)\Big) < \deg(f).$$

This is impossible unless

$$q(x) - q'(x) = 0.$$

Thus $q(x) = q'(x)$, and substituting back yields $r(x) = r'(x)$. ■

Corollary 1.1. Division with a remainder can be done whenever the leading coefficient of f is a unit. In particular, it can be done whenever the coefficient ring is a field and $f \neq 0$.

Example 1.4. Consider the polynomials

$$f(x) = 2x^2 + 3x + 1 \quad \text{and} \quad g(x) = x + 1$$

over $\mathbb{Z}[x]$.
- The leading coefficient of $g(x)$ is 1, which is a unit in $\mathbb{Z}$. - Perform polynomial division:

$$2x^2 + 3x + 1 = (x + 1)(2x + 1) + 0$$

- Quotient: $q(x) = 2x + 1$, Remainder: $r(x) = 0$.

2 Ideals and Quotient Rings

2.1 Ideals

Previously, in group theory, we used normal subgroups to construct quotient groups. We now seek to develop analogous conditions for subrings to construct quotient rings. Recall that we may partition a ring through individual cosets that are *equivalence classes* of the form

$$r + S = \{r + s : s \in S\}$$

If we define these to be the exact elements of a quotient ring R/S we must have that

$$(r_1 + S)(r_2 + S) \in R/S$$
$$(r_1 + S) + (r_2 + S) \in R/S$$

The second equation implies that S must be closed under addition. The first equation implies that we must have

$$(r_1 + s)(r_2 + s') \in ab + S$$
$$r_1 r_2 + r_1 s' + s r_2 + s s' \in r_1 r_2 + S$$

Notice that ss' is already in S and $r_1 r_2$ cancels out. This leaves us with

$$r_1 s' + s r_2 \in S \implies r_1 s' \in S \text{ and } s r_2 \in S$$

which describes the exact conditions needed for S to be used to form a quotient ring.

Definition 2.1. Let R be a ring. A subset $I \subseteq R$ is called an **ideal** if:

i) I is closed under addition;

ii) for all $r \in R$ and $i \in I$, we have

$$ri \in I \quad \text{and} \quad ir \in I.$$

An ideal I is called **proper** if $I \neq R$ (equivalently, $1 \notin I$). The ideal is considered to be **principal** if there exists $a \in R$ such that

$$I = (a) := \{ra : r \in R\}$$

2.2 Quotient Rings

Definition 2.2. Let R be a ring and let $I \trianglelefteq R$ be an ideal. The **quotient ring** (or **factor ring**) R/I is the set

$$R/I := \{r + I : r \in R\},$$

with addition and multiplication defined by

$$(r + I) + (s + I) = (r + s) + I, \qquad (r + I)(s + I) = rs + I.$$

The formation of the quotient ring allows us to simplify structures of rings to analyze similarities and differences.

Example 2.1. Let $R = \mathbb{R}[x]$.
The ideal generated by $x^2 + 1$ is

$$(x^2 + 1) = \{(x^2 + 1)f(x) : f(x) \in \mathbb{R}[x]\}.$$

The quotient ring

$$\mathbb{R}[x]/(x^2 + 1)$$

satisfies the relation $x^2 = -1$ and is isomorphic to $\mathbb{C}$.

Theorem 2.1 (Canonical Projections). Let R be a ring and $I \trianglelefteq R$ be an ideal. Then define the canonical projection

$$\pi : R \to R/I, \quad \pi(r) = r + I$$

Then

1. π is a homomorphism
2. π is surjective
3. $\ker(\pi) = I$

Proof. Let $r, s \in R$.

1. Additivity:

$$\pi(r+s) = (r+s) + I = (r+I) + (s+I) = \pi(r) + \pi(s)$$

2. Multiplicativity:

$$\pi(rs) = (rs+I) = (r+I)(s+I) = \pi(r)\pi(s)$$

3. Identity:

$$\pi(1) = 1 + I$$

Thus, π is a homomorphism. Surjectivity is trivial in how we define the map. Now consider the kernel. By definition

$$\ker(\varphi) = \{r \in R : \pi(r) = 0 + I\} = \{r \in R : r \in I\} = I$$

■

2.3 Integral Domains

Corollary 2.1. Every ring homomorphism $\varphi : K \to R$ from a field K with $\varphi \neq 0$ is injective.

Proof. The kernel $\ker(\varphi)$ is an ideal of K. Since fields have no proper ideals, we must have $\ker(\varphi) = \{0\}$, hence φ is injective. ■

Proposition 2.1. A commutative ring R is a field if and only if it has no proper ideals.

Proof. ($\Rightarrow$) If R is a field, then every nonzero element is a unit. Thus any ideal containing a nonzero element must contain 1, and hence must equal R.
($\Leftarrow$) If R has no proper ideals and $a \neq 0$, then $(a) = R$. Thus $1 \in (a)$, so there exists $b \in R$ with $ba = 1$, showing that a is a unit. Hence R is a field. ■

3 Ring Morphisms

3.1 Ring Homomorphisms

Definition 3.1. Given two rings R, S, a function $\varphi : R \to S$ is a ring homomorphism if

i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

ii) $\varphi(ab) = \varphi(a)\varphi(b)$

iii) $\varphi(1_R) = 1_S$

Notice that, by this definition, we're specifically examining the homomorphism on both operations. The definition of the kernel and image remains invariant under this definition. Furthermore, the property relating to injectivity by way of the kernel criterion remains the same as well.

Proposition 3.1. Let $\varphi : R \to S$ be a ring homomorphism. Then $\ker(\varphi)$ is an ideal of R.

Proof. Let $a \in \ker(\varphi)$ and $r \in R$. Then

$$\varphi(ar) = \varphi(a)\varphi(r) = 0\varphi(r) = 0, \quad \varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$$

so $ar, ra \in \ker(\varphi)$. Since $\ker(\varphi)$ is a subring, it must be true that $\ker(\varphi)$ is closed under addition. Thus, $\ker(\varphi)$ is an ideal. ∎

Theorem 3.1 (Substitution Principle). If R is a ring and $r \in R$, then there exists a ring homomorphism

$$\varphi : R[x] \to R, \quad f(x) \mapsto f(r)$$

who's kernel is $(p(x))$, where $p(x)$ is the minimal polynomial satisfied by r.

Proof. Every polynomial $f(x) \in R[x]$ can be written uniquely as

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{with } a_i \in R.$$

Define a map $\Phi : R[x] \to R'$ by

$$\Phi(f) := \sum_{i=0}^{n} \varphi(a_i)\alpha^i.$$

This map is well-defined since $\varphi(a_i) \in R'$ and $\alpha^i \in R'$, and R' is closed under addition and multiplication. For any $r \in R$ (viewed as a constant polynomial),

$$\Phi(r) = \varphi(r),$$

so $\Phi|_R = \varphi$. Moreover,

$$\Phi(x) = \varphi(1)\alpha = \alpha.$$

Now let

$$f(x) = \sum a_i x^i, \quad g(x) = \sum b_i x^i.$$

Additivity:

$$\begin{aligned} \Phi(f+g) &= \Phi\Big(\sum (a_i + b_i)x^i\Big) \\ &= \sum \varphi(a_i + b_i)\alpha^i \\ &= \sum (\varphi(a_i) + \varphi(b_i))\alpha^i \\ &= \Phi(f) + \Phi(g). \end{aligned}$$

Multiplicativity:

$$\begin{aligned}
\Phi(fg) &= \Phi\left(\sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k\right) \\
&= \sum_k \varphi\left(\sum_{i+j=k} a_i b_j\right) \alpha^k \\
&= \sum_k \sum_{i+j=k} \varphi(a_i)\varphi(b_j)\alpha^{i+j} \\
&= \left(\sum_i \varphi(a_i)\alpha^i\right)\left(\sum_j \varphi(b_j)\alpha^j\right) \\
&= \Phi(f)\Phi(g).
\end{aligned}$$

Thus Φ is a ring homomorphism. Finally, suppose $\Psi : R[x] \to R'$ is another ring homomorphism such that $\Psi|_R = \varphi$ and $\Psi(x) = \alpha$. Then for any $f(x) = \sum a_i x^i$,

$$\Psi(f) = \sum \Psi(a_i)\Psi(x)^i = \sum \varphi(a_i)\alpha^i = \Phi(f),$$

so $\Psi = \Phi$. Hence Φ is unique. ■

The substitution principle emphasizes the idea that evaluations of polynomials via *substitution* of x with a value α is not random. Every substitution that respects the ring rules is a ring homormophism and in fact, there is exactly one homomorphism for each choice of coefficient map and variable. Now, let $R' = R$, $\varphi = \mathrm{id}_R$, and $\alpha = a \in R$ in the Substitution Principle. The resulting homomorphism

$$\Phi : R[x] \to R$$

satisfying $\Phi|_R = \mathrm{id}_R$ and $\Phi(x) = a$ is exactly the *evaluation map*

$$\mathrm{ev}_a(f) = f(a).$$

3.2 Isomorphism Theorems

Theorem 3.2 (Mapping Property). Let R, S be rings and let

$$\varphi : R \to S$$

be a ring homomorphism. If $I \subseteq \ker(\varphi)$, then there exists a unique ring homomorphism

$$\overline{\varphi} : R/I \to S$$

such that $\varphi = \overline{\varphi} \circ \pi$ where $\pi : R \to R/I$ is the canonical projection map.

Not every homomorphism sends elements of an ideal to 0. The mapping property requires $I \subseteq \ker \varphi$; only then does the quotient R/I allow a well-defined factorization. Otherwise, cosets could map ambiguously.

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & S \\
R/I \arrow[ur, "\overline{\varphi}"'] &
\end{tikzcd}$$

Figure 1: Diagram of the mapping property in action

Proof. First, define the map

$$\overline{\varphi}(r + I) = \varphi(r)$$

Now suppose $r + I = r' + I$. Then

$$r - r' \in I \subseteq \ker(\varphi)$$

so

$$\varphi(r-r')=0 \implies \varphi(r)=\varphi(r')$$

Hence, $\overline{\varphi}$ is well defined. Now, let us confirm that the map is in fact a homomorphism. Let $r, s \in R$.

1. Additivity:

$$\overline{\varphi}((r+I)+(s+I))=\overline{\varphi}(r+s+I)=\varphi(r+s)=\varphi(r)+\varphi(s)=\overline{\varphi}(r+I)+\overline{\varphi}(s+I)$$

2. Multiplicity:

$$\overline{\varphi}((r+I)(s+I))=\overline{\varphi}(rs+I)=\varphi(r)\varphi(s)=\overline{\varphi}(r+I)\overline{\varphi}(s+I)$$

3. Identity:

$$\overline{\varphi}(1+I)=\varphi(1)=1$$

Thus, $\overline{\varphi}$ is a ring homomorphism. So notice then that

$$(\overline{\varphi}\circ\pi)(r)=\overline{\varphi}(r+I)=\varphi(r)$$

so $\varphi=\overline{\varphi}\circ\pi$. Now, suppose $\psi : R/I \to S$ is any ring homomorphism with $\varphi=\psi\circ\pi$. Then for any $r+I \in R/I$,

$$\psi(r+I)=\psi(\pi(r))=\varphi(r)=\overline{\varphi}(r+I)$$

Thus, $\psi=\overline{\varphi}$, proving uniqueness. ■

Corollary 3.1 (First Isomorphism Theorem). Let $\varphi : R \to S$ be a ring homomorphism. Then

$$R/\ker(\varphi) \cong \mathrm{im}\varphi$$

The use of the kernel as the ideal to quotient by is key for inducing injectivity, as all elements that map to 0 are collapsed to a singular representation.

Theorem 3.3 (Correspondence Theorem). Let R be a ring and let $I \trianglelefteq R$ be an ideal. Then there is a one to one correspondence between

1. Ideals of R containing I
2. Ideals of the quotient ring R/I

The correspondence is given by

$$J \mapsto J/I = \{j + I : j \in J\}, \quad \overline{J} \mapsto \pi^{-1}(\overline{J}) = \{r \in R : r + I \in J\}$$

Proof. Let R be a ring and $I \trianglelefteq R$ be an ideal. Then let J be an ideal of R such that $I \subseteq J$. Define a map

$$\psi(r) = r + I$$

Return to J. Under the map ψ, we have that J becomes

$$J/I = \{j + I : j \in J\}$$

We'll now show that this resulting set is an ideal of R/I. Let $r + I \in R/I$ and $j + I \in J$. Then we have that

$$(r + I)(j + I) = (rj + I)$$

Because J was an ideal, we have that $rj \in J$. Thus, it must be true that $rj + I \in J/I$. Therfore, J/I is absorbs via multiplication. Next, let $j_1 + I, j_2 + I \in J/I$. Then

$$j_1 + I + j_2 + I = (j_1 + j_2) + I$$

Since J is an ideal, $j_1 + j_2 \in J$. Thus, J/I is closed under addition. Therfore, J/I is an ideal. Thus, J/I is an ideal. Conversely, if $K \trianglelefteq R/I$, then the preimage

$$\pi^{-1}(K) = \{r \in R : r + I \in K\}$$

is an ideal of R containing I. Moreover, these assignments are inverse to each other:

$$\pi^{-1}(J/I) = J \quad \text{and} \quad \pi(\pi^{-1}(K)) = K.$$

Hence there is a bijection between ideals of R containing I and ideals of R/I, given by

$$J \longleftrightarrow J/I.$$

■

4 Product Rings