Ring Theory Notes:
Rings, Units, and Polynomial Rings

Ryan Hausner

Fall 2026

Contents

1 Rings **2**
- 1.1 Definition of a Ring . . . 2
- 1.2 Basic Properties . . . 2
- 1.3 Examples of Rings . . . 2
- 1.4 Algebraic and Transcendental Numbers . . . 2

2 Zero Divisors, Units, and Fields **3**
- 2.1 Zero Divisors . . . 3
- 2.2 Units . . . 3
- 2.3 The Zero Ring . . . 3
- 2.4 Fields and Integral Domains . . . 3

3 Polynomial Rings **3**
- 3.1 Polynomials with Coefficients in a Ring . . . 3
- 3.2 Degree and Leading Coefficient . . . 4
- 3.3 Addition and Multiplication of Polynomials . . . 4
- 3.4 Division with Remainder . . . 4

4 Homomorphisms and Ideals **5**
- 4.1 Homomorphisms . . . 5
- 4.2 Ideals, Principal Ideals . . . 6

1 Rings

1.1 Definition of a Ring

Definition 1.1 (Ring)**.** A *ring* is a set R with two operations, addition and multiplication, $R \times R \to R$, such that:

1. $(R, +)$ is an abelian group, with identity denoted 0.
2. Multiplication is associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. The distributive laws hold: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.
4. There exists an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

R is said to be *commutative*[1] if it also satisfies:

5. $ab = ba$ for all $a, b \in R$.

Definition 1.2 (Subring)**.** A subset $S \subseteq R$ is a *subring* if it is closed under addition, subtraction, and multiplication, and $1 \in S$.

1.2 Basic Properties

Proposition 1.3 (Arithmetic in a Ring)**.** *Let R be a ring. For all $a, b \in R$ and $k \in \mathbb{Z}$:*

1. $0 \cdot a = a \cdot 0 = 0$.
2. $(-a) \cdot b = a \cdot (-b) = -ab$.
3. $(-a)(-b) = ab$.
4. $(k \cdot a)b = k(ab) = a(k \cdot b)$.

1.3 Examples of Rings

Example 1.4 (Familiar Rings)**.** $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$ are rings. An example of a noncommutative ring is the ring of $n \times n$ matrices.

Example 1.5 (The Gaussian Integers)**.**

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Example 1.6 (The Subring of $\mathbb{C}$ Generated by α)**.** Let $\alpha \in \mathbb{C}$. Define

$$\mathbb{Z}[\alpha] := \{a_n \alpha^n + \cdots + a_1 \alpha + a_0 \mid n \geq 0,\ a_i \in \mathbb{Z}\}.$$

We call this the subring of $\mathbb{C}$ generated by α.

1.4 Algebraic and Transcendental Numbers

Definition 1.7 (Algebraic and Transcendental Numbers)**.** We say $\alpha \in \mathbb{C}$ is *algebraic* if it is a root of a nonzero polynomial with integer coefficients. Otherwise, α is *transcendental*.

Example 1.8. The numbers π and e are transcendental.

[1] In this class, all rings are assumed to be commutative unless otherwise stated. So when referring to a ring, it must satisfy 1–5.

2 Zero Divisors, Units, and Fields

2.1 Zero Divisors

Definition 2.1 (Zero Divisor)**.** Let R be a ring. A nonzero element $a \in R$ is called a *zero divisor* if there exists $b \in R$, $b \neq 0$, such that $a \cdot b = 0$.

Example 2.2. In $\mathbb{Z}_6$, $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$, so $\bar{2}$ and $\bar{3}$ are zero divisors.

Remark 2.3 (Cancellation Law). If R is a ring with no zero divisors and $a \neq 0$, then $ab = ac \implies b = c$. This is not true in general: in $\mathbb{Z}_6$, $\bar{2} \cdot \bar{3} = \bar{2} \cdot \bar{0}$ but $\bar{3} \neq \bar{0}$.

2.2 Units

Definition 2.4 (Unit)**.** Let R be a ring. An element $a \in R$ is said to be a *unit* if there exists $c \in R$ such that $a \cdot c = c \cdot a = 1$.

Example 2.5. In $\mathbb{Z}$, the units are 1 and -1: $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = 1$. In $\mathbb{Z}[i]$, the units are $1, -1, i, -i$.

Remark 2.6 (The Group of Units). Let R be a ring. Then $R^\times = \{a \in R \mid a \text{ is a unit}\}$ is a group under multiplication.

2.3 The Zero Ring

Proposition 2.7 (The Zero Ring)**.** *A ring R in which $0 = 1$ is the zero ring.*

Proof. Suppose $1 = 0$. Then for any element $a \in R$, $a = 1 \cdot a = 0 \cdot a = 0$. So every element of the ring is 0. □

2.4 Fields and Integral Domains

Definition 2.8 (Field)**.** A *field* is a commutative ring in which $0 \neq 1$ and every nonzero element is a unit. An example of a field is $\mathbb{R}$.

Definition 2.9 (Integral Domain)**.** A commutative ring in which $1 \neq 0$ and which has no zero divisors is called an *integral domain*.

3 Polynomial Rings

In this section, R is a commutative ring with identity 1, with $1 \neq 0$.

3.1 Polynomials with Coefficients in a Ring

Definition 3.1 (Polynomial)**.** A *polynomial* with coefficients in R is a formal linear combination

$$a_n x^n + \cdots + a_1 x + a_0, \qquad a_i \in R.$$

Definition 3.2 (The Polynomial Ring $R[x]$)**.**

$$R[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid n \geq 0,\ a_i \in R,\ i = 0, \ldots, n\}.$$

The monomials x^i are assumed to be linearly independent; that is, if

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \qquad g(x) = b_m x^m + \cdots + b_1 x + b_0,$$

then

$$f(x) = g(x) \iff a_i = b_i \ \ \forall i.$$

Equivalently, we can write $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_i \in R$ and only finitely many coefficients nonzero. The polynomial is then determined by its associated vector of coefficients $a = (a_0, a_1, a_2, \ldots, a_n)$.

3.2 Degree and Leading Coefficient

Definition 3.3 (Degree of a Polynomial)**.** The *degree* of a nonzero polynomial f, denoted $\deg(f)$, is the largest integer n such that the coefficient a_n of x^n is nonzero. A polynomial of degree 0 is called a *constant polynomial*.

Definition 3.4 (Leading Coefficient, Monic Polynomial)**.** The nonzero coefficient of highest degree of a polynomial is its *leading coefficient*. A *monic* polynomial is one whose leading coefficient is 1.

Example 3.5. Let $R = \mathbb{R}$ and $f(x) = 5x^2 + 0 \cdot x^3 + 1$. The leading coefficient is 5, and f is not monic.

3.3 Addition and Multiplication of Polynomials

Definition 3.6 (Operations on Polynomials)**.** Let $f(x) = a_0 + a_1 x + \cdots$ and $g(x) = b_0 + b_1 x + \cdots$. Define the following operations.

1. **Addition:**
$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots = \sum_{k \geq 0} (a_k + b_k) x^k.$$
Its associated vector is $a + b = (a_0 + b_0,\ a_1 + b_1,\ \ldots)$.

2. **Multiplication:**
$$f(x)g(x) = \sum_{i,j} a_i b_j x^{i+j} = p_0 + p_1 x + p_2 x^2 + \cdots, \qquad \text{where } p_k = \sum_{i+j=k} a_i b_j.$$
Its associated vector is $(a_0 b_0,\ a_0 b_1 + a_1 b_0,\ a_0 b_2 + a_1 b_1 + a_2 b_0,\ \ldots)$.

Proposition 3.7 (Ring Structure on $R[x]$)**.** *There is a unique commutative ring structure on $R[x]$ such that addition and multiplication are defined as above. R is a subring of $R[x]$.*

3.4 Division with Remainder

Proposition 3.8 (Division with Remainder)**.** *Let $g \in R[x]$, and let $f \in R[x]$ be monic. There exist unique polynomials $q, r \in R[x]$ such that*

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

where r is either zero or satisfies $\deg(r) < \deg(f)$.

Example 3.9. Let $g(x) = 3x^2 + 1$ and $f(x) = x$. Write $g(x) = 3x \cdot x + 1$; then $q(x) = 3x$, $r(x) = 1$, and $\deg(r) < \deg(f)$.

Example 3.10. Let $g(x) = 3x^2 + 1$ and $f(x) = x + 1$. By polynomial long division, $q(x) = 3x - 3$ and $r(x) = 4$.

Example 3.11. Let $g(x) = 5x^4 + 10x^2 + 1$ and $f(x) = x^2 + 1$. Left as an exercise.

4 Homomorphisms and Ideals

4.1 Homomorphisms

Definition 4.1. $f : R \to R'$ is a ring homomorphism if:

1. $f(a+b) = f(a) + f(b)$
2. $f(ab) = f(a)f(b)$
3. $f(1_R) = 1_{R'}$

$\forall a, b \in R$

Definition 4.2 (Substitution Principle)**.** Let $f : R \to R'$ be a ring homomorphism:

1. Let $\alpha \in R'$. There is a unique ring homomorphism $\phi : R[x] \to R'$ that agrees with f at constant polynomials ($\phi(r) = f(r) \forall r \in R$) and $\phi(x) = \alpha$.
2. More generally, given $\alpha_1, \cdots, \alpha_n \in R'$. There is a unique ring homomorphism

$$\phi : R[x_1, \cdots, x_n] \to R'$$

that agrees with f at constant polynomials and $\phi(x_i) = \alpha_i \forall i = 1, \cdots, n$.

Proof. **Uniqueness.** Suppose first that ϕ as in the statement exists. Since ϕ is a ring homomorphism with $\phi(a) = f(a)$ for $a \in R$ and $\phi(x) = \alpha$,

$$\phi\Big(\sum_{i\geq 0} a_i x^i\Big) = \sum_{i\geq 0} \phi(a_i x^i) = \sum_{i\geq 0} \phi(a_i)\, \phi(x)^i = \sum_{i\geq 0} f(a_i)\, \alpha^i.$$

Hence if ϕ' were another ring homomorphism with the same properties, we would get

$$\phi\Big(\sum_{i\geq 0} a_i x^i\Big) = \phi'\Big(\sum_{i\geq 0} a_i x^i\Big)$$

for every polynomial, so $\phi = \phi'$.

Existence. Define

$$\phi : R[x] \to R', \qquad \sum_{i\geq 0} a_i x^i \longmapsto \sum_{i\geq 0} f(a_i)\, \alpha^i.$$

We show this is a ring homomorphism.

- *Identity:* $\phi(1) = f(1) = 1$.
- *Addition:* for $g, h \in R[x]$, it is clear that $\phi(g+h) = \phi(g) + \phi(h)$.
- *Multiplication:* let $g = \sum_i a_i x^i$ and $h = \sum_j b_j x^j$. Then

$$\begin{aligned}
\phi(g \cdot h) &= \phi\Big(\Big(\sum_i a_i x^i\Big)\Big(\sum_j b_j x^j\Big)\Big) = \phi\Big(\sum_{i,j} a_i b_j x^{i+j}\Big) \\
&= \sum_{i,j} f(a_i b_j)\, \alpha^{i+j} = \sum_{i,j} f(a_i) f(b_j)\, \alpha^i \alpha^j \\
&= \Big(\sum_i f(a_i)\, \alpha^i\Big)\Big(\sum_j f(b_j)\, \alpha^j\Big) = \phi(g)\, \phi(h).
\end{aligned}$$

□

Take $\psi : \mathbb{Z} \to \mathbb{F}_p, a \to \bar{a}$. This extends to a ring homomorphism: $\Phi : \mathbb{Z}[x] \to \mathbb{F}_p[x]$. This sends $a_o + a_1x + \cdots + a_nx^n \to \bar{a_0} + \bar{a_1}x + \cdots \bar{a_n}x^n = \bar{f}(x)$. We call $\bar{f}(x)$ the residue of f mod p.

Proposition 4.3. *Let $x = (x_1, \cdots, x_n), y = (y_1, \cdots, y_n)$ There is a unique isomorphism*

$$R[x, y] \to R[x][y], x_i \to x_i, y_j \to y_j$$

Corollary 4.4. *Let $f(x, y), g(x, y)$ be polynomials of two variables. Suppose that, regarded as a polynomial in y, f is monic of degree m. Then $\exists! q(x, y), R(x, y) \in R[x]$ such that $g = f \cdot q + R$ and $R = 0$ if $deg_y(R) < m$.*

Example 4.5. $f(x, y) = y^2 - x, g(x, y) = y^4 + y + 1$ in $R[x, y]$. $y^4 + y + 1 = (y^2 - x)(y^2 + x) + (x^2 + y + 1)$

Definition 4.6. An ideal of a ring R is a nonempty subset $I \subseteq R$ such that

1. I is closed under addition.
2. If $s \in I$ and $r \in R \implies rs \in I$

Example 4.7. In $\mathbb{Z}, (3) = 3\mathbb{Z} = \{..., -6, -3, 0, 3, 6, ...\}$ This is an ideal. In $R[x]$, $(x) = \{xf(x) | f(x) \in R[x]\}$ is an ideal.

4.2 Ideals, Principal Ideals

Recall: A ring homomorphism is a function $\phi : R \to R'$ such that $\forall a, b \in R$:

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$
3. $\phi(1_R) = 1_{R'}$

In particular, ϕ is injective if and only if, $\ker(\phi) = \{0_R\}$

Definition 4.8. Let R be a ring. We say that $I \subseteq R$ is an ideal of R if $I \neq \emptyset$ and

1. I is closed under addition, $\forall a, b \in I, a + b \in I$
2. $\forall r \in R, a \in I$, $ra \in I$

Proposition 4.9. *Let $\phi : R \to R'$ be a ring homomorphism, then ker(ϕ) is an ideal of R*

Proof. Since $\phi : R^+ \to R'^+$ is a group homomorphism, we have that $\phi(0_R) = 0_{R'}$, hence $0_R \in \ker(\phi)$. Thus, $\ker(\phi) \neq \emptyset$. Let $a, b \in \ker(\phi)$. Then

$$\phi(a + b) = \phi(a) + \phi(b) = 0_{R'} + 0_{R'} = 0_{R'}$$

Let $r \in R$ and $a \in \ker(\phi)$ We evaluate $\phi(r \cdot a) = \phi(r) \cdot \phi(a) = \phi(r) \cdot 0_{R'} = 0_{R'}$, since $\phi(a) \in \ker(\phi)$. Thus, $\ker(\phi)$ is an ideal of R. □

Definition 4.10 (Principal Ideal)**.** Let R be a ring and $r \in R$. The principal ideal generated by r is $(r) \coloneqq \{a \cdot r | a \in R\}$.

Example 4.11. $n \in \mathbb{Z} : (n) = \{kn | k \in \mathbb{Z}\} = \{\cdots, -2n, n, 0, n, 2n, 3n, \cdots\}$. (2) is the multiples of even integers.

Example 4.12. $x - 2 \in \mathbb{R}[x]$. $(x - 2) = \{(x - 2) \cdot p(x) | p(x) \in \mathbb{R}[x]\} = \{Q(x) \in \mathbb{R}[x] | Q(2) = 0\}$

Definition 4.13. Let R be a ring and $r_1, \cdots, r_n \in R$. The ideal generated by $r_1, \cdots, r_n$ is the smallest ideal of R containing $r_1, \cdots, r_n$. Explicitly, $(r_1, \cdots, r_n) = \{a_1r_1 + \cdots + a_nr_n | a_1, \cdots, a_n \in R\}$

Example 4.14. $(2,3) \in \mathbb{Z}$: $\{2a+3b | a,b \in Z\}$. Since $2,3$ are coprime, the ideal generated by $(2,3) = \mathbb{Z}$.

Remark 4.15. Let $I \subseteq R$ be an ideal. Then $I = R \iff 1 \in I$.

Proof. If $I = R$, then $1 \in R = I$. If $1 \in I$, then $\forall r \in R$, we have $r = 1 \cdot r \in I$. □

In the previous example $1 = 2(-1) + 3(1)$.

Example 4.16. $\phi : \mathbb{Z}[x] \to \mathbb{F}_p$, $\phi(x) \to \bar{\phi(x)}$. We claim that $\ker(\phi) = (p, x)$.

Proof. $p \in \ker(\phi)$. Indeed $\phi(p) = \bar{p} = \bar{0}$. $x \in \ker(\phi)$, so $\phi(x) = \bar{0}$. It follows that $(p,x) \subseteq \ker(\phi)$.

$$\phi(p \cdot Q(x) + x \cdot G(x)) = \phi(p) \cdot \phi(Q(x)) + \phi(x) \cdot \phi(G(x)) = \bar{0}$$

We are left to prove that $\ker(\phi) \subseteq (p,x)$. Let now $f(x) \in \ker(\phi)$. Write $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Then $\phi(f(x)) = \bar{f(0)} = \bar{a_0} = \bar{0}$. Hence a_0 is a multiple of p. That is, $\exists l \in \mathbb{Z}$ such that $a_0 = l \cdot p$. Thus $f(x) = l \cdot p + x(a_1 + a_2 x + \cdots + a_n x^{n-1} \in (p,x)$. □

Example 4.17. In $\mathbb{C}[x,y]$, consider the ideal (x^3, x^2y, xy^2, y^3). This is the ideal whose elements are polynomials of total degree ≥ 3.