MATH 3022: Algebra II
(Ring Theory)

Joe Tran

February 8, 2024

Contents

Chapter 1

Introduction to Ring Theory

In MATH 3021 Algebra I, we have studied sets with a single binary operation satisfying certain axioms, but now we are interested in working with sets that have two binary operations. For example, one of the most natural algebraic structures to study is the integers with the operations of addition and multiplication. These operations are related to one another by the distributive property. If we consider a set with two such related binary operations satisfying certain axioms, we have an algebraic structure called a ring. In a ring, we add and multiply elements such as real numbers, complex numbers, matrices, and functions.

1.1 Rings

Definition 1.1.1. A nonempty set R is called a *ring* if it has two closed binary operations, addition and multiplication that satisfy the following conditions:

1. For all $a, b \in R$, $a + b = b + a$

2. For all $a, b, c \in R$, $(a + b) + c = a + (b + c)$

3. There exists an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$.

4. For every element $a \in R$, there exists an element $-a \in R$ such that $a + (-a) = 0$.

5. For all $a, b, c \in R$, $(ab)c = a(bc)$.

6. For all $a, b, c \in R$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

We denote that R is a ring with addition and multiplication by $(R, +, \cdot)$.

The last condition is called the *distributive axiom*, and it relates the binary operations of both addition and multiplication. The axioms (1) to (4) require that a ring needs to be an abelian group under addition, so we could have also defined a ring to be an abelian group $(R, +)$, together with a second binary operation satisfying the fifth and sixth conditions given above.

Definition 1.1.2. If there exists an element $1 \in R$ such that $1 \neq 0$ and $1a = a1 = a$ for every $a \in R$, then R is a ring with *identity*.

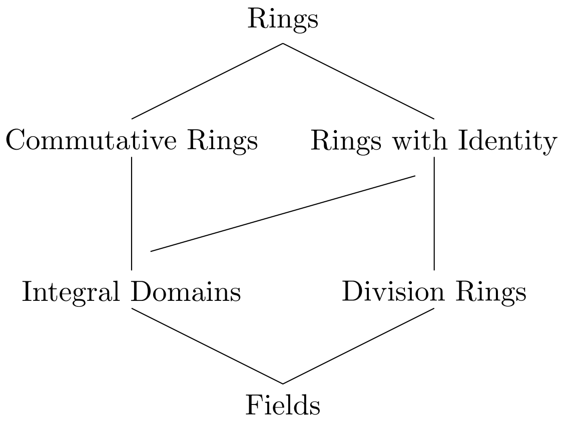
Definition 1.1.3. A ring for which $ab = ba$ for all $a, b \in R$ is called a *commutative ring*.

Definition 1.1.4. A commutative ring R with identity is called an *integral domain* if for every $a, b \in R$ such that $ab = 0$, either $a = 0$ or $b = 0$.

Definition 1.1.5. A *division ring* R with an identity in which every nonzero element R is a unit, i.e. for each $a \in R$ with $a \neq 0$, there exists a unique a^{-1} such that $a^{-1}a = aa^{-1} = 1$.

Definition 1.1.6. A commutative division ring is called a *field*.

Below shows the relationship among rings, integral domains, division rings, and fields.



Example 1.1.7. As we have mentioned, the integers form a ring. In fact, $\mathbb{Z}$ is an integral domain. Indeed, if $ab = 0$ for $a, b \in \mathbb{Z}$, then either $a = 0$ or $b = 0$. However, $\mathbb{Z}$ is not a field. That is, there is no such integer that is the multiplicative inverse of 2, since $\frac{1}{2}$ is not an integer. The only integers with multiplicative inverses are 1 and -1.

Example 1.1.8. Under the ordinary operations of addition and multiplication, all of these familiar number systems are rings: The rationals $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are fields.

Notation 1.1.9. Whenever we are working with real numbers or complex numbers, we will denote $\mathbb{K}$ to be either the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$. That is, $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$.

Notation 1.1.10. Whenever we are working with fields, we will denote it by $\mathbb{F}$. For example, $\mathbb{F} = \mathbb{Q}$, $\mathbb{F} = \mathbb{R}$ and $\mathbb{F} = \mathbb{C}$ are all fields.

Example 1.1.11. Recall that $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ is the *integer modulo* n and back in MATH 3021, we have defined the operations $+_n$ and $\cdot_n$, where

$$a +_n b := a + b \pmod{n}$$

and

$$a \cdot_n b := a \cdot b \pmod{n}$$

We can define the product of two elements $a, b \in \mathbb{Z}_n$ by $a \cdot_n b$. This product make the abelian group into a ring. Indeed, $\mathbb{Z}_n$ is a commutative ring.

However, $\mathbb{Z}_n$ fails to be an integral domain. For example, consider $3, 4 \in \mathbb{Z}_{12}$. Then $3 \cdot_{12} 4 = 0$ then we see that the product of two nonzero elements in the ring can be equal to zero.

Definition 1.1.12. A nonzero element a in a commutative ring R is called a *zero divisor* if there exists a nonzero element $b \in R$ such that $ab = 0$.

Example 1.1.13. In Example 1.1.11, we have that 3 and 4 are zero divisors of $\mathbb{Z}_{12}$.

Notation 1.1.14. We denote the set of all continuous functions from $[a, b]$ to $\mathbb{K}$ by $\mathcal{C}([a, b])$ and for arbitrary domain and range, we denote it by $\mathcal{C}(X, Y)$. That is,

$$\mathcal{C}([a, b]) = \{\text{all continuous functions } f : [a, b] \to \mathbb{K}\}$$

and

$$\mathcal{C}(X, Y) = \{\text{all continuous functions } f : X \to Y\}$$

Example 1.1.15. $\mathcal{C}([a, b])$ is a commutative ring. Indeed, we can add or multiply two functions by adding or multiplying the values of the functions. Let $f, g \in \mathcal{C}([a, b])$ be functions defined by $f(x) = x^2$ and $g(x) = \cos(x)$. Then $(f + g)(x) = f(x) + g(x) = x^2 + \cos(x) \in \mathcal{C}([a, b])$ and $(fg)(x) = f(x)g(x) = x^2 \cos(x) \in \mathcal{C}([a, b])$.

Notation 1.1.16. We denote the set of $n \times n$ matrices with $\mathbb{K}$-entries by $\mathcal{M}_n(\mathbb{K})$. That is,

$$\mathcal{M}_n(\mathbb{K}) = \{\text{all } n \times n \text{ matrices with } \mathbb{K}\text{-entries}\}$$

Example 1.1.17. The $n \times n$ with entries $\mathbb{K} = \mathbb{R}$ form a ring under the usual operations of matrix addition and multiplication. However, this ring is noncommuative, since it is usually the case that $AB = BA$. Also, note that we can have $AB = 0$ whenever neither A nor B is zero.

Example 1.1.18. Let us denote the following matrices

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \mathbf{i} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \mathbf{j} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \quad \mathbf{k} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

where $i^2 = -1$. These elements satisfy the following conditions:

- $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$
- $\mathbf{ij} = \mathbf{k}$
- $\mathbf{jk} = \mathbf{i}$
- $\mathbf{ki} = \mathbf{j}$
- $\mathbf{ji} = -\mathbf{k}$
- $\mathbf{kj} = -\mathbf{i}$
- $\mathbf{ik} = -\mathbf{j}$

Notation 1.1.19. Let $\mathbb{H}$ denote the elements of the form $a + \mathbf{i}b + \mathbf{j}c + \mathbf{k}d$, where $a, b, c, d \in \mathbb{R}$. Equivalently, we can say that

$$\mathbb{H} = \left\{ \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix} : \alpha = a + id, \beta = b + ic \in \mathbb{C} \right\}$$

We can define addition and multiplication on $\mathbb{H}$ either by usual matrix operations or in terms of the generators 1, $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$. Indeed,

$$\begin{aligned} &(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) + (a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) \\ &= (a_1 + a_2) + (b_1 + b_2)\mathbf{i} + (c_1 + c_2)\mathbf{j} + (d_1 + d_2)\mathbf{k} \end{aligned}$$

and also

$$(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k})(a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$$

where

$$\begin{aligned}\alpha &= a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2\\ \beta &= a_1b_2 + a_2b_1 + c_1d_2 - d_1c_2\\ \gamma &= a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2\\ \delta &= a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2\end{aligned}$$

After having a look at plenty of examples of types of rings, let us prove the following properties about rings.

Proposition 1.1.20. *Let R be a ring and let $a, b \in R$. Then the following hold*

1. $a0 = 0a = 0$
2. $a(-b) = (-a)b = -ab$
3. $(-a)(-b) = ab$

Proof. To see that (1) is true, note that

$$a0 = a(0+0) = a0 + a0$$

and therefore, $a0 = 0$. Similarly, we also have that $0a = 0$.

To see that (2) is true, observe that

$$ab + a(-b) = a(b-b) = a0 = 0$$

and therefore, $a(-b) = -ab$. Similarly, we also have that $(-a)b = 0$.

Note that (3) follows from (2) since

$$(-a)(-b) = -(a(-b)) = -(-ab) = ab$$

□

Just as we have subgroups of groups, we have an analogous class of substructures for rings.

Definition 1.1.21. A *subring* S of a ring R is a subset S of R such that S is also a ring under the inherited operations from R. We denote S is a subring of R as $S \leq R$.

The following proposition gives us some easy criteria for determining whether or not a subset of a ring is a subring.

Proposition 1.1.22. *Let R be a ring and $S \subset R$. Then $S \leq R$ if and only if the following conditions are satisfied:*

1. *$S \neq \emptyset$.*

2. *If $r, s \in S$, $rs \in S$.*

3. *If $r, s \in S$, $r - s \in S$.*

Proof. Assume that $S \leq R$. We need to show that the three conditions hold. Note that because S is a subring of R, then S is also a ring, so it cannot be empty. To see that the second and third conditions hold, note that since S is a subring of R, the operations are preserved.

Conversely, if the three conditions hold, we must show that S is a subring under the same operations as R. But these conditions are satisfied because of the axioms we have defined for a ring. □

Just like with groups, the following is an immediate consequence of Proposition 1.1.22.

Corollary 1.1.23. *Let R be a ring with identity and suppose $S \leq R$ if and only if $S \neq \emptyset$ and whenever $r, s, t \in S$, then $r - st \in S$.*

Example 1.1.24. The ring $n\mathbb{Z}$ is a subring of $\mathbb{Z}$. Notice that even though the original ring may have an identity, we do not require that its subring have an identity. We have the following chain of subrings:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Example 1.1.25. Let $R = \mathcal{M}_2(\mathbb{R})$ and let $\mathcal{T}_2(\mathbb{R})$ denote the set of upper triangular matrices in R, i.e.

$$\mathcal{T}_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\}$$

Then $\mathcal{T}_2(\mathbb{R}) \leq \mathcal{M}_2(\mathbb{R})$. Indeed, if

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \quad B = \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \quad C = \begin{bmatrix} g & h \\ 0 & k \end{bmatrix}$$

Then by Corollary 1.1.23, $\mathcal{T}_2(\mathbb{R}) \neq \emptyset$, and

$$A - BC = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} - \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \begin{bmatrix} g & h \\ 0 & k \end{bmatrix} = \begin{bmatrix} a - dg & b - dh - ek \\ 0 & c - kf \end{bmatrix} \in \mathcal{T}_2(\mathbb{R})$$

1.2 Integral Domains and Fields

In this section, we will be focusing on two types of rings, namely the integral domain (Definition 1.1.4) and fields (Definition 1.1.6).

Example 1.2.1. If $i^2 = -1$, then the set $\mathbb{Z}[i] = \{m + in : a, b \in \mathbb{Z}\}$ forms a ring known as the Gaussian integers. It can be shown that the Gaussian integers are a subring of the complex numbers, i.e. $\mathbb{Z}[i] \leq \mathbb{C}$ since they are closed under addition and multiplication. Let $\alpha = a + ib$ be a unit in $\mathbb{Z}[i]$. THen $\overline{\alpha} = a - ib$ is also a unit since if $\alpha\beta = 1$, then $\overline{\alpha\beta} = 1$. If $\beta = c + id$, then

$$1 = \alpha\beta\overline{\alpha\beta} = (a^2 + b^2)(c^2 + d^2)$$

Therefore, $a^2 + b^2$ must be either 1 or -1; or equivalently, $a + ib = \pm 1$, or $a + ib = \pm i$. Therefore, units of this ring are ± 1 and $\pm i$. Furthermore, the Gaussian integers are not a field, but it is an integral domain.

Example 1.2.2. The set of matrices

$$F = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}$$

with entries in $\mathbb{Z}_2$ form a field.

Example 1.2.3. The set $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field. The inverse of $a + b\sqrt{2}$ in $\mathbb{Q}[\sqrt{2}]$ is

$$\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$

We have the following alternative characterization of integral domains.

Proposition 1.2.4 (Cancellation Law)**.** *Let D be a commutative ring with identity. Then D is an integral domain if and only if for every nonzero elements $d \in D$ with $da = db$, then $a = b$.*

Proof. Let D be an integral domain. Then D has no zero divisors. Let $da = db$ with $d \neq 0$. Then $d(a - b) = 0$, so $a - b = 0$ and thus $a = b$.

Conversely, suppose that the cancellation law is possible in D. That is, suppose that $da = db$ implies $a = b$. Let $da = 0$. If $d \neq 0$, then $da = d0$, or $a = 0$. Therefore, d cannot be a zero divisor. □

Theorem 1.2.5 (Wedderburn)**.** *Every finite integral domain is a field.*

Proof. Let D be a finite integral domain and D^* denote the nonzero elements of D. Then we need to show that every element in D^* has an inverse. Let $a \in D^*$ be arbitrary. Define $\lambda_a : D^* \to D^*$ given by $\lambda_a(d) = ad$. We have seen this map previously when we were talking about Group Theory and Cayley's Theorem. This map also makes sense because if $a \neq 0$ and $d \neq 0$, then $ad \neq 0$. The map λ_a is also well defined, since for $d_1, d_2 \in D^*$,

$$ad_1 = \lambda_a(d_1) = \lambda_a(d_2) = ad_2$$

which implies $d_1 = d_2$ by the cancellation law (Proposition 1.2.4). Since D^* is a finite set, the map λ_a must also be onto. Therefore, there exists a $d \in D^*$ such that $\lambda_a(d) = ad = 1$. Therefore, a has a left inverse. Since D is commutative, d must also be a right inverse for a. Consequently, D is a field. □

Definition 1.2.6. For any nonnegative integer n and any element r in a ring R, we write

$$\underbrace{r + r + \cdots + r}_{n \text{ times}} = nr$$

We define the *characteristic of a ring R* to be the least positive integer n such that $nr = 0$ for all $r \in R$. If no such integer exists, then the characteristic of R is defined to be 0. We will denote the characteristic of R by $\operatorname{char}(R)$.

Example 1.2.7. For every prime p, $\mathbb{Z}_p$ is a field of characteristic p. Note that every nonzero element in $\mathbb{Z}_p$ has an inverse, and so $\mathbb{Z}_p$ is a field. If a is any nonzero element in the field, then $pa = 0$, since the order of any nonzero element in the abelian group $\mathbb{Z}_p$ is p.

Lemma 1.2.8. *Let R be a ring with identity. If 1 has order n, then the characteristic of R is n.*

Proof. If 1 has order n, then n is the least positive integer such that $n1 = 0$. Thus, for any $r \in R$,

$$nr = n(1r) = (n1)r = 0r = 0$$

On the other hand, if no positive n exists such that $n1 = 0$, then the characteristic of R is zero. □

We finish this section off with the following theorem.

Theorem 1.2.9. *The characteristic of an integral domain is either prime or zero.*

Proof. Let D be an integral domain and suppose that the characteristic of D is n with $n \neq 0$. If n is not prime, then $n = ab$ where $1 < a < n$ and $1 < b < n$. By Lemma 1.2.8, we consider the case when $n1 = 0$. Since $0 = n1 = (ab)1 = (a1)(b1)$ and there are no zero divisors in D, either $a1 = 0$ or $b1 = 0$. Hence, the characteristic of D must be less than n, which is a contradiction. Therefore, n must be prime. □

1.3 Ring Homomorphisms and Ideals

Recall that when we were talking about groups, a *homomorphism* is a mapping that preserves the operation of the group. That is, if $(G, *)$ and $(H, \star)$ are groups, then if the mapping $\phi : (G, *) \to (H, \star)$ satisfies

$$\phi(x * y) = \phi(x) \star \phi(y)$$

Then ϕ is said to be a homomorphism, and when such a homomorphism exists, we say that $(G, *)$ is homomorphic to $(H, \star)$ and denote $(G, *) \simeq (H, \star)$.

Furthermore, recall that if ϕ is a homomorphism and also it satisfies the property of being a bijection, then ϕ is said to be an *isomorphism.* If such a ϕ exists, then we say that the groups $(G, *)$ are isomorphic to $(H, \star)$, i.e. $(G, *) \simeq (H, \star)$.

In this section, we will study the ring homomorphisms and introduce the concept of ideals. From now on, whenever we are working with rings, we will be clear that the notation that we are using is $(R, +, \cdot)$ to indicate that R is the ring and $(+, \cdot)$ are the two binary operations that are associated to ring, but for shorthand notation we will just say that R is a ring.

Definition 1.3.1. Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be rings with the respective binary operations. Then a *ring homomorphism* is a mapping $\phi : R \to S$ that satisfies:

$$\begin{cases} \phi(x + y) = \phi(x) + \phi(y) \\ \phi(x \cdot y) = \phi(x) \cdot \phi(y) \end{cases}$$

for all $x, y \in R$. Furthermore, if ϕ is a bijection, then we say that ϕ is a *ring isomorphism.*

We also introduced the concept of the *kernel* when talking about homomorphisms for, but we also have the concept of the kernel for rings as well.

Definition 1.3.2. For any ring homomorphism $\phi : R \to S$, we define the *ring kernel* to be the set

$$\ker(\phi) = \{r \in R : \phi(r) = 0\}$$

Example 1.3.3. For any integer $n \in \mathbb{Z}$, we can define a ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_n$ by $\phi(x) = x \pmod{n}$. This is a ring homomorphism because for any $x, y \in \mathbb{Z}$,

$$\begin{aligned} \phi(x+y) &= (x+y) \pmod{n} \\ &= x \pmod{n} + y \pmod{n} \\ &= \phi(x) + \phi(y) \end{aligned}$$

and

$$\begin{aligned} \phi(x \cdot y) &= (x \cdot y) \pmod{n} \\ &= x \pmod{n} \cdot y \pmod{n} \\ &= \phi(x) \cdot \phi(y) \end{aligned}$$

Furthermore, the kernel of ϕ is the set

$$\ker(\phi) = \{k \in \mathbb{Z} : \phi(k) = 0\} = n\mathbb{Z}$$

Example 1.3.4. Recall that

$$\mathcal{C}([a,b]) = \{f : [a,b] \to \mathbb{R} : f \text{ is continuous}\}$$

For any $x \in [a,b]$, we define a ring homomorphism $\phi_x : \mathcal{C}([a,b]) \to \mathbb{R}$ given by the mapping $\phi_x(f) = f(x)$. This is a ring homomorphism since

$$\phi_x(f+g) = (f+g)(x) = f(x) + g(x) = \phi_x(f) + \phi_x(g)$$

and

$$\phi_x(fg) = (fg)(x) = f(x)g(x) = \phi_x(f)\phi_x(g)$$

Ring homomorphisms of this form are called *evaluation homomorphisms.*

In the next proposition, we will examine some fundamental properties of ring homomorphisms.

Proposition 1.3.5. *Let $\phi : R \to S$ be a ring homomorphism.*

1. *If R is a commutative ring, then $\phi(R)$ is a commutative ring.*

2. *$\phi(0) = 0$.*

3. *Let 1_R and 1_S be the identities for R and S, respectively. If ϕ is onto, then $\phi(1_R) = 1_S$.*

4. *If R is a field and $\phi(R) \neq 0$, then $\phi(R)$ is a field.*

Proof. Let $\phi : R \to S$ be a ring homomorphism, and let $x, y \in R$ be arbitrary. To see that (1) is true, observe that because R is a commutative ring and because ϕ is a homomorphism, then $xy = yx$, and thus

$$\phi(x)\phi(y) = \phi(xy) = \phi(yx) = \phi(y)\phi(x)$$

Therefore, $\phi(R)$ is a commutative ring.

To see that (2) is true, let $x \in R$ be arbitrary. Then

$$0 \cdot \phi(0) = 0 = \phi(0 \cdot 0) = \phi(0)\phi(0)$$

Then by the cancellation law, $\phi(0) = 0$.

To see that (3) is true, assume that 1_R and 1_S are identities for R and S, respectively. Then

$$1_S\phi(1_R) = \phi(1_R) = \phi(1_R \cdot 1_R) = \phi(1_R)\phi(1_R)$$

Then by the cancellation law, $\phi(1_R) = 1_S$.

To see that (4) is true, let $x \in R$ be a nonzero element such that $\phi(x) \neq 0$. Then because R is a field and $x \neq 0$, then there exists an $x^{-1} \in R$ such that $1_R = x \cdot x^{-1} = x^{-1} \cdot x$. Then observe that because ϕ is a homomorphism,

$$\phi(x) \cdot \phi(x^{-1}) = \phi(x) \cdot [\phi(x)]^{-1} = 1_S$$

Therefore, $\phi(R)$ is also a field. □

In group theory, we found that normal subgroups play a special role. These subgroups have nice characteristics that make them more interesting to study than arbitrary subgroups. In ring theory, the objects corresponding to normal subgroups are a special class of subrings called ideals.

Definition 1.3.6. An *ideal* in a ring R is a subring $I \leq R$ such that if $a \in I$ and $r \in R$, then $ar, ra \in I$, i.e. $rI \in I$ and $Ir \subset I$ for all $r \in R$. We denote that I is an ideal of R as $I \trianglelefteq R$.

Example 1.3.7. Every ring has at least two ideals, namely the *trivial ideals* $\{0\}$ and R.

Let R be a ring with identity and suppose that $I \lhd R$ such that $1 \in I$. Since for any $r \in R$, $r1 = r \in I$, by the definition of an ideal, then $I = R$.

Example 1.3.8. If a is any element in a commutative ring R with identity, then the set

$$\langle a \rangle = \{ar : r \in R\}$$

is an ideal of R. Indeed, $\langle a \rangle$ is nonempty since both $0 = a0$ and $a = a1$ are in $\langle a \rangle$. The sum of two elements in $\langle a \rangle$ is in $\langle a \rangle$ since $ar + ar' = a(r + r')$. The inverse of ar is $-ar = a(-r) \in \langle a \rangle$. Finally, if we multiply an element $ar \in \langle a \rangle$ by an arbitrary element $s \in R$, we have $s(ar) = a(sr)$. Therefore, $\langle a \rangle$ satisfies the definition of an ideal.

If R is a commutative ring with identity, then an ideal of the form $\langle a \rangle = \{ar : r \in R\}$ is called a *principal ideal.*

Theorem 1.3.9. *Every ideal in the ring of integers $\mathbb{Z}$ is a principal ideal.*

Proof. The zero ideal $\{0\}$ is a principal ideal since $\langle 0 \rangle = \{0\}$. If I is any nonzero ideal in $\mathbb{Z}$, then I must contain some positive integer m. There exists a least positive integer n in I, by the Well-Ordering Principal. Now let $a \in I$. By the division algorithm, there exists q, r such that

$$a = nq + r$$

where $0 \leq r < n$. This equation suggests that $r = a - nq \in I$, but $r = 0$ since n is the least positive element in I, so $a = nq$, and thus, $I = \langle n \rangle$, as required. □

Example 1.3.10. The set $n\mathbb{Z}$ is ideal in the ring of integers. If $na \in n\mathbb{Z}$ and $b \in \mathbb{Z}$, then $nab \in n\mathbb{Z}$. In fact, by Theorem 1.3.9, these are the only ideals of $\mathbb{Z}$.

Proposition 1.3.11. *The kernel of any ring homomorphism $\phi : R \to S$ is an ideal in R.*

Proof. We know from group theory that $\ker(\phi)$ is an additive subgroup of R. Suppose that $r \in R$ and $a \in \ker(\phi)$. Then we must show that ar and ra are in $\ker(\phi)$. However,

$$\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$$

and similarly,

$$\phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0$$

as desired. □

Remark 1.3.12. In our definition of an ideal, we have required that $rI \subset I$ and $Ir \subset I$ for all $r \in R$. Such ideals are sometimes referred to as *two-sided ideals*. We can also consider *one-sided ideals*; that is, we may require only that either $rI \subset I$ or $Ir \subset I$ for $r \in R$ hold, but not both. Such ideals are called *left ideals* and *right ideals*, respectively. Of course, in a commutative ring, any ideal must be two-sided.

Theorem 1.3.13. *Let $I \lhd R$. The factor group R/I is a ring with multiplication defined by*

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

Proof. We already know that R/I is an abelian group under addition. Let $r+I$ and $s+I$ be in R/I. We need to show that $(r+I)(s+I) = rs+I$ is independent of the choice of coset. That is, if $r' \in r+I$ and $s' \in s+I$, then $r's' \in rs+I$. Since $r' \in r+I$, then there exists an $a \in I$ such that $r' = r+a$. Similarly, there exists a $b \in I$ such that $s' = s+b$. Then observe

$$r's' = (r+a)(s+b) = rs + as + rb + ab$$

and $as + rb + ab \in I$, since I is an ideal. Consequently, we obtain that $r's' \in rs + I$. □

The ring R/I in Theorem 1.3.13 is called the *factor ring* or *quotient ring*. Just as with group homomorphisms and normal subgroups, there is a relationship between ring homomorphisms and ideals.

Theorem 1.3.14. *Let $I \lhd R$. The map $\phi : R \to R/I$ defined by $\phi(r) = r+I$ is a surjective ring homomorphism with kernel I.*

Proof. Clearly, ϕ is a surjective abelian group homomorphism. Finally, it remains to show that ϕ works under ring multiplication. If $r, s \in R$, then

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

as required. □

The map $\phi : R \to R/I$ is called the *natural homomorphism* or *canonical homomorphism*. In ring theory, we have isomorphism theorems relating ideals and ring homomorphisms similar to the isomorphism theorems for groups that relate normal subgroups and homomorphisms.

Theorem 1.3.15 (The First Isomorphism Theorem)**.** *Let $\psi : R \to S$ be a ring homomorphism. Then $\ker(\psi)$ is an ideal of R. If $\phi : R \to R/\ker(\psi)$ is the canonical homomorphism, then there exists a unique isomorphism $\eta : R/\ker(\psi) \to \psi(R)$ such that $\psi = \eta\phi$.*

Proof. Let $K = \ker(\phi)$. By the First Isomorphism Theorem for groups, there exists a well-defined group homomorphism $\eta : R/K \to \psi(R)$ defined by $\eta(r+K) = \psi(r)$ for the additive abelian groups R and R/K. To show that this is a ring homomorphism, we need only show that $\eta((r+K)(s+K)) = \eta(r+K)\eta(s+K)$. Indeed,

$$\begin{aligned}\eta((r+K)(s+K)) &= \eta(rs+K)\\ &= \psi(rs)\\ &= \psi(r)\psi(s)\\ &= \eta(r+K)\eta(s+K)\end{aligned}$$

as desired. □

Theorem 1.3.16 (The Second Isomorphism Theorem)**.** *Let R be a ring, let $I \leq R$ and $J \lhd R$. Then $I \cap J$ is an ideal of I, and*

$$I/(I \cap J) \simeq (I+J)/J$$

Theorem 1.3.17 (The Third Isomorphism Theorem)**.** *Let R be a ring and $I, J \lhd R$ where $J \subset I$. Then*

$$R/I \simeq \frac{R/J}{I/J}$$

Theorem 1.3.18 (Correspondence Theorem)**.** *Let R be a ring and let $I \lhd R$. Then $S \mapsto S/I$ is a bijection between $S \leq R$ containing I and $R/I \leq R$. Furthermore, the ideals of R containing I correspond to ideals of R/I.*

1.4 Maximal and Prime Ideals

Notation 1.4.1. We denote that I is a proper ideal of R as $I \blacktriangleleft R$, and we denote that M is a maximal ideal of R by $M \overset{\max}{\lhd} R$

Definition 1.4.2. A proper ideal M of a ring R is a *maximal ideal* of R if the ideal M if a proper subset of any ideal of R except R itself. That is, $M \overset{\max}{\lhd} R$ if for any I properly containing M, $I = R$.

The following theorem completely characterizes maximal ideals for commutative rings with identity in terms of their corresponding factor rings.

Theorem 1.4.3. *Let R be a commutative ring with identity and $M \lhd R$. Then $M \overset{\max}{\lhd} R$ if and only if R/M is a field.*

Proof. Let $M \overset{\max}{\lhd} R$. If R is a commutative ring then R/M must also be a commutative ring. Clearly, $1+M$ acts as an identity for R/M. We must also show that every nonzero element in R/M admits an inverse. If $a+M$ is a nonzero element in R/M, then $a \notin M$. Let $I = \{ra + m : r \in R, m \in M\}$. We will show that $I \lhd R$. The set I is nonempty since $0a + 0 = 0$ is in I. If $r_1 a + m_1, r_2 a + m_2 \in I$, then

$$(r_1 a + m_1) - (r_2 a + m_2) = (r_1 - r_2)a + (m_1 - m_2) \in I$$

Also, for any $r \in R$, it is true that $rI \subset I$ and so I is closed under multiplication and satisfies the necessary conditions to be an ideal. Therefore, by Proposition 1.1.22 and the definition of an ideal, I is an ideal property containing M. Since M is a maximal ideal, $I = R$. Consequently, by the definition of I, there must exist an $m \in M$ and $b \in R$ such that $1 = ab + m$ and therefore,

$$1 + M = ab + M = ba + M = (a + M)(b + M)$$

Conversely, suppose that M is an ideal and R/M is a field. Then it contains at least two elements, namely $0 + M = M$ and $1 + M$. Hence, $M \blacktriangleleft R$. Let I be any ideal properly containing M. We need to show that $I = R$. Let $a \in I \backslash M$. Since $a+M \neq 0 \in R/M$, then there exists an element $b+M \in R/M$ such that $(a+M)(b+M) = ab+M = 1+M$. Consequently, there exists an element $m \in M$ such that $ab+m = 1$, and $1 \in I$. Therefore, $r1 = r \in I$ for all $r \in R$, and consequently, $I = R$. □

Example 1.4.4. Let $p\mathbb{Z} \lhd \mathbb{Z}$ where p is prime. Then $p\mathbb{Z}$ is a maximal ideal since $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p$ is a field.

Definition 1.4.5. A proper ideal P in a commutative ring R is called a *prime ideal*, and we denote it as $P \overset{p}{\lhd} R$ if whenever $ab \in P$, then either $a \in P$ or $b \in P$.

Remark 1.4.6. It is possible to define prime ideals in a noncommuative ring.

Example 1.4.7. Consider $R = \mathbb{Z}_{12}$ and let $P = \{0, 2, 4, 6, 8, 10\}$. Then the set $P \overset{p}{\lhd} \mathbb{Z}_{12}$. In fact, $P \overset{\max}{\lhd} \mathbb{Z}_{12}$ as well. That is, if we take any element $a, b \in P$ such that $ab \in P$, then either $a \in P$ or $b \in P$.

Proposition 1.4.8. *Let R be a commutative ring with identity $1 \neq 0$. Then $P \overset{p}{\lhd} R$ if and only if R/P is an integral domain.*

Proof. Assume that $P \lhd R$ and R/P is an integral domain. Suppose that $ab \in P$. If $a + P, b + P \in R/P$ such that $(a + P)(b + P) = 0 + P = P$, then either $a + P = P$ or $b + P = P$. This means that $a \in P$ or $b \in P$, which shows that P must be prime.

Conversely, assume that P is prime and

$$(a + P)(b + P) = ab + P = 0 + P = P$$

Then $ab \in P$. If $a \notin P$, then $b \in P$ by definition of a prime ideal. Hence, $b + P = 0 + P$ and R/P is an integral domain. □

Example 1.4.9. Every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$. The factor ring $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ is an integral domain if and only if n is prime. Indeed, it is a field. Hence, the nonzero prime ideals in $\mathbb{Z}$ are the ideals $p\mathbb{Z}$ where p is prime.

Since every field is an integral domain (Theorem 1.2.5), we have the following consequence.

Corollary 1.4.10. *Every maximal ideal in a commutative ring with identity is also a prime ideal.*

Chapter 2

Polynomials

Most people are fairly familiar with polynomials by the time they begin to study abstract algebra. When we examine polynomial expressions such as

$$p(x) = x^3 - 3x + 2 \quad q(x) = 3x^2 - 6x + 5$$

we have a pretty good idea of what $p(x) + q(x)$ and $p(x)q(x)$ mean. We just add and multiply polynomials as functions, that is,

$$\begin{aligned}(p+q)(x) &= p(x) + q(x)\\ &= (x^3 - 3x + 2) + (3x^2 - 6x + 5)\\ &= x^3 + 3x^2 - 9x + 7\end{aligned}$$

and

$$\begin{aligned}(pq)(x) &= p(x)q(x)\\ &= (x^3 - 3x + 2)(3x^2 - 6x + 5)\\ &= 3x^5 - 6x^4 - 4x^3 + 24x^2 - 27x + 10\end{aligned}$$

In this chapter, we will emphasize the algebraic structure of polynomials by studying polynomial rings. We can prove many results of polynomials by studying polynomial rings. We can prove many results for polynomial rings that are similar to the theorems we proved for integers. Analogues of prime numbers, the division algorithm, and the Euclidean algorithm exist for polynomials.

2.1 Polynomial Rings

Throughout this chapter we shall assume that R is a commutative ring with identity.

Definition 2.1.1. Any expression of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $a_i \in R$ and $a_n \neq 0$, is called the *polynomial over* R with *indeterminate* x.

Definition 2.1.2. Let R be a ring. For each $0 \leq i \leq n$, $a_i \in R$ is called the *coefficients* of the polynomial f, and $a_n \in R$ is called the *leading coefficient.*

Definition 2.1.3. A polynomial is said to be *monic* if the leading coefficient is 1.

Definition 2.1.4. If n is the largest nonnegative number for which $a_n \neq 0$, we say that the *degree of* f is n, and denote it as $\deg(f) = n$. If no such n exists, i.e. f is the zero polynomial, then the degree of f is said to be $-\infty$.

Notation 2.1.5. We denote the set of all polynomials with coefficients in a ring R as $R[x]$.

Definition 2.1.6. If $p(x) = \sum_{i=0}^{n} a_i x^i$ and $q(x) = \sum_{i=0}^{m} b_i x^m$ are two polynomials in $R[x]$, then we say that $p(x)$ is *equal* to $q(x)$, if $n = m$, and for every $0 \leq i \leq n$, $a_i = b_i$.

We define polynomial addition and polynomial multiplication over R as follows: Let $p(x)$ and $q(x)$ be polynomials in $R[x]$ given by

$$p(x) = \sum_{i=0}^{n} a_i x^i \quad q(x) = \sum_{i=0}^{m} b_i x^i$$

Then we define polynomial addition as

$$(p+q)(x) = c_0 + c_1 x + \cdots + c_k x^k$$

where for each $0 \leq i \leq n$, $c_i = a_i + b_i$. Similarly, we define polynomial multiplication as

$$(pq)(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}$$

where for each $0 \leq i \leq n$, $c_i = \sum_{k=0}^{i} a_k b_{i-k}$.

Remark 2.1.7. Note that in some cases, the coefficients may be zero, except for the leading coefficient.

Example 2.1.8. Let $p(x) = 3{+}2x^3$ and $q(x) = 2{-}x^2{+}4x^4$ be polynomials in $\mathbb{Z}[x]$. Then by applying polynomial addition and polynomial multiplication over $\mathbb{Z}$, then

$$\begin{aligned}(p+q)(x) &= (3+2x^3)+(2-x^2+4x^4)\\ &= (3+2)+(0+0)x+(0-1)x^2+(2+0)x^3+(0+4)x^4\\ &= 5-x^2+2x^3+4x^4\end{aligned}$$

and

$$\begin{aligned}(pq)(x) &= (3+2x^3)(2-x^2+4x^4)\\ &= 6-3x^2+4x^3+12x^4-2x^5+8x^7\end{aligned}$$

Example 2.1.9. Let $p(x) = 3{+}3x^3$ and $q(x) = 4{+}4x^2{+}4x^4$ be polynomials in $\mathbb{Z}_{12}[x]$. Then

$$\begin{aligned}(p+q)(x) &= (3+3x^3)+(4+4x^2+4x^4)\\ &= 7+4x^2+3x^3+4x^4\end{aligned}$$

and $(pq)(x) = 0$.

Remark 2.1.10. In Example 2.1.9, we see that when we multiply the two polynomials $p(x)$ and $q(x)$ together, we end up with the zero polynomial. In this case, we cannot expect $R[x]$ to be an integral domain if R is not an integral domain.

Proposition 2.1.11. *Let R be a commutative ring with identity. Then $R[x]$ is a commutative ring with identity.*

Proof. To show that $R[x]$ is a commutative ring with identity, we first need to show that $R[x]$ is an abelian group under polynomial addition. In this case, $f(x) = 0$ is the additive identity. If $p(x) = \sum_{i=0}^{n} a_i x^i$ is a polynomial in $R[x]$, then the inverse is simply the additive inverse $-p(x) = \sum_{i=0}^{n}(-a_i)x^i = -\sum_{i=0}^{n} a_i x^i$. Showing that $R[x]$ is associative and abelian under addition follow immediately from the definition of polynomial addition and from the fact that R is also abelian and commutative under addition.

To show that polynomial multiplication is associative, let

$$p(x) = \sum_{i=0}^{n} a_i x^i \quad q(x) = \sum_{i=0}^{m} b_i x^i \quad r(x) = \sum_{i=0}^{\ell} c_i x^i$$

Then

$$\begin{aligned}
[(pq)r](x) &= \left[\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right)\right]\left(\sum_{i=0}^{\ell} c_i x^i\right) \\
&= \left[\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i\right]\left(\sum_{i=0}^{\ell} c_i x^i\right) \\
&= \sum_{i=0}^{n+m+\ell}\left[\sum_{j=0}^{i}\left(\sum_{k=0}^{j} a_k b_{j-k}\right) c_{i-j}\right] x^i \\
&= \sum_{i=0}^{n+m+\ell}\left(\sum_{i=j+k+s} a_j b_k c_s\right) x^i \\
&= \sum_{i=0}^{n+m+\ell}\left[\sum_{j=0}^{i} a_j\left(\sum_{k=0}^{i-j} b_k c_{i-j-k}\right)\right] x^i \\
&= \left(\sum_{i=0}^{n} a_i x^i\right)\left[\sum_{i=0}^{m+\ell}\left(\sum_{j=0}^{i} b_j c_{i-j}\right) x^i\right] \\
&= \left(\sum_{i=0}^{n} a_i x^i\right)\left[\left(\sum_{i=0}^{m} b_i x^i\right)\left(\sum_{i=0}^{\ell} c_i x^i\right)\right] \\
&= [p(qr)](x)
\end{aligned}$$

The commutativity and distributive properties of polynomial multiplication are proven in a similar manner. □

Proposition 2.1.12. *Let $p(x)$ and $q(x)$ be polynomials in $R[x]$, where R is an integral domain. Then $\deg(p) + \deg(q) = \deg(pq)$. Furthermore, $R[x]$ is an integral domain.*

Proof. Let $p(x)$ and $q(x)$ be two polynomials given by

$$p(x) = \sum_{i=0}^{n} a_i x^i \quad q(x) = \sum_{i=0}^{m} b_i x^i$$

with $a_n \neq 0$ and $b_m \neq 0$. Then $\deg(p) = n$ and $\deg(q) = m$ respectively. The leading term of $p(x)q(x)$ is $a_m b_n x^{m+n}$, which cannot be zero because R is an integral domain. Therefore, $\deg(pq) = n + m$, and $p(x)q(x) \neq 0$. Since $p(x) \neq 0$ and $q(x) \neq 0$ imply that $p(x)q(x) \neq 0$, we know that $R[x]$ must also be an integral domain. □

Suppose we want to consider polynomials of two or more variables. Let R be a ring and suppose that x and y are indeterminates. Then we denote the polynomial ring over x and y as $(R[x])[y]$. Although it is straightforward, it is also a tedious task to show that $(R[x])[y] \simeq R([y])[x]$. We will denote the ring instead, by $R[x, y]$. The ring $R[x, y]$ is called the *ring of polynomials in two indeterminates x and y with coefficients in R.* We can also denote the *ring of polynomials in n indeterminates with coefficients in R*, and we denote it by $R[x_1, x_2, ..., x_n]$.

Theorem 2.1.13. *Let R be a commutative ring with identity and $\alpha \in R$, then we have a ring homomorphism $\phi_\alpha : R[x] \to R$ defined by*

$$\phi_\alpha(p(x)) = p(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0$$

where $p(x) = a_nx^n + \cdots + a_0$. The map ϕ_α is called the evaluation homomorphism at *α.*

Proof. To show that ϕ_α is a ring homomorphism, let $p(x) = \sum_{i=0}^{n} a_ix^i$ and $q(x) = \sum_{i=0}^{m} b_ix^i$ be polynomials in $R[x]$. Then it is elementary to see that

$$\phi_\alpha(p(x) + q(x)) = \phi_\alpha(p(x)) + \phi_\alpha(q(x))$$

For the multiplication, note that

$$\begin{aligned}\phi_\alpha(p(x))\phi_\alpha(q(x)) &= p(\alpha)q(\alpha)\\ &= \left(\sum_{i=0}^{n} a_i\alpha^i\right)\left(\sum_{i=0}^{m} b_i\alpha^i\right)\\ &= \sum_{i=0}^{n+m}\left(\sum_{k=0}^{i} a_kb_{i-k}\right)\alpha^i\\ &= \phi_\alpha(p(x)q(x))\end{aligned}$$

□

2.2 The Division Algorithm for Polynomials

Recall that the division algorithm for integers says that if $a, b \in \mathbb{Z}$ with $b > 0$, then there exists unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r$$

where $0 \le r < b$. The algorithm for polynomials has several important consequences. The proof is very similar to the corresponding proof for integers.

Theorem 2.2.1 (The Division Algorithm)**.** *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{F}[x]$ where $\mathbb{F}$ is a field and $g(x)$ is a nonzero polynomial. Then there exists unique $q(x), r(x) \in \mathbb{F}[x]$ such that*

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

where either $\deg(r) < \deg(g)$*, or $r(x)$ is the zero polynomial.*

Proof. We will first consider the existence of $q(x)$ and $r(x)$. If $f(x)$ is the zero polynomial, then clearly,

$$0 = 0 \cdot g(x) + 0$$

hence both q and r must also be the zero polynomial. On the other hand, let us assume that $f(x)$ is not the zero polynomial, and suppose that $\deg(f) = n$ and $\deg(g) = m$. If $m > n$, then we can let $q(x) = 0$ and $r(x) = f(x)$. Hence, we assume that $m \leq n$ and proceed by induction on n. If

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\ g(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \end{aligned}$$

the polynomial

$$f'(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$

has degree less than n or is the zero polynomial. By induction there exist polynomials $q'(x)$ and $r(x)$ such that

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

where $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x)$. Now let

$$q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}$$

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

Now to show that $q(x)$ and $r(x)$ are unique, suppose that there exist two other polynomials $q_1(x)$ and $r_1(x)$ such that $f(x) = g(x)q_1(x) + r_1(x)$ with $\deg(r_1) < \deg(g)$ or $r_1(x) = 0$, so that

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x)$$

and

$$g(x)[q(x) - q_1(x)] = r_1(x) - r(x)$$

If $q(x) - q_1(x)$ is not the zero polynomial, then

$$\deg(g(q - q_1)) = \deg(r_1 - r) \geq \deg(g)$$

However, the degrees of both $r(x)$ and $r_1(x)$ are strictly less than the degree of $g(x)$. Therefore, $r(x) = r_1(x)$ and $q(x) = q_1(x)$. □

Example 2.2.2. At this point, we should be familiar with long division from high school mathematics. Suppose we divide $x^3 - x^2 + 2x - 3$ by $x - 2$. Then

$$\begin{array}{rrrrr}
 & & x^2 & +x & +4 \\ \cline{2-5}
x-2 \big) & x^3 & -x^2 & +2x & -3 \\
 & -x^3 & +2x^2 & & \\ \cline{2-3}
 & & x^2 & +2x & \\
 & & -x^2 & +2x & \\ \cline{3-4}
 & & & 4x & -3 \\
 & & & -4x & +8 \\ \cline{4-5}
 & & & & 5
\end{array}$$

and so by Theorem 2.2.1, $x^3 - x^2 + 2x - 3 = (x - 2)(x^2 + x + 4) + 5$.

Definition 2.2.3. Let $p(x)$ be a polynomial in $\mathbb{F}[x]$ and let $\alpha \in \mathbb{F}$. We say that α is a *zero* or *root* of $p(x)$ if $p(x)$ is in the kernel of the evaluation homomorphism ϕ_α. That is, α is a zero of $p(x)$ if $p(\alpha) = 0$.

Corollary 2.2.4 (The Factor Theorem)**.** *Let $\mathbb{F}$ be a field. An element $\alpha \in \mathbb{F}$ is a zero of $p(x) \in \mathbb{F}[x]$ if and only if $x - a$ is a factor of $p(x)$ in $\mathbb{F}[x]$.*

Proof. Suppose that $\alpha \in \mathbb{F}$ and $p(\alpha) = 0$. By Theorem 2.2.1, there exists polynomials $q(x)$ and $r(x)$ such that

$$p(x) = (x - \alpha)q(x) + r(x)$$

and the degree of $r(x)$ must be less than the degree of $x - \alpha$. Since the degree of $r(x)$ is less than 1, $r(x) = a$ for $a \in \mathbb{F}$. Therefore,

$$p(x) = (x - \alpha)q(x) + r(x)$$

But

$$0 = p(\alpha) = 0 \cdot q(\alpha) + a = 0$$

Consequently, $p(x) = (x - \alpha)q(x)$ and $x - \alpha$ and $x - \alpha$ is a factor of $p(x)$.

Conversely, suppose that $x-\alpha$ is a factor of $p(x)$, i.e. $p(x) = (x-\alpha)q(x)$. Then $p(\alpha) = 0 \cdot q(\alpha) = 0$. □

Corollary 2.2.5. *Let $\mathbb{F}$ be a field. A nonzero polynomial $p(x)$ of degree n in $\mathbb{F}[x]$ can have at most n distinct zeros in $\mathbb{F}$.*

Proof. We will use induction on the degree of $p(x)$. If $\deg(p) = 0$, then $p(x)$ is a constant polynomial and has no zeros. Let $\deg(p) = 1$. Then $p(x) = ax + b$ for some $a, b \in \mathbb{F}$. If α_1 and α_2 are zeros of $p(x)$, then $a\alpha_1 + b = a\alpha_2 + b$ or $\alpha_1 = \alpha_2$.

Now assume that $\deg(p) > 1$. If $p(x)$ does not have a zero in $\mathbb{F}$, then we are done. On the other hand, if α is a zero of $p(x)$, then $p(x) = (x - \alpha)q(x)$ for some $q(x) \in \mathbb{F}[x]$ by Corollary 2.2.4. The degree of $q(x)$ is $n - 1$ is Proposition 2.1.12. Let β be some other zero of $p(x)$ that is distinct from α. Then $p(\beta) = (\beta - \alpha)q(\beta) = 0$. Since $\alpha \neq \beta$ and $\mathbb{F}$ is a field, $q(\beta) = 0$. By our inductive hypothesis, $q(x)$ can have at most $n - 1$ zeros in $\mathbb{F}$ that are distinct from α. Therefore, $p(x)$ has at most n distinct zeros of $\mathbb{F}$. □

Definition 2.2.6. Let $\mathbb{F}$ be a field. A monic polynomial $d(x)$ is a *greatest common divisor* of polynomials $p(x), q(x) \in \mathbb{F}[x]$ if $d(x)$ evenly divides both $p(x)$ and $q(x)$; and, if for any other polynomial $d'(x)$ dividing both $p(x)$ and $q(x)$, then $d'(x) \mid d(x)$. We write $d(x) = \gcd(p(x), q(x))$.

Definition 2.2.7. We say that two polynomials $p(x)$ and $q(x)$ are *relatively prime* if $\gcd(p(x), q(x)) = 1$.

Just as we have Bézout's Theorem for integers, we have a similar outcome for polynomials as well.

Proposition 2.2.8 (Bézout's Theorem)**.** *Let $\mathbb{F}$ be a field and suppose that $d(x)$ is a greatest common divisor of two polynomials $p(x)$ and $q(x)$ in $\mathbb{F}[x]$. Then there exists polynomials $r(x)$ and $s(x)$ such that*

$$d(x) = r(x)p(x) + s(x)q(x)$$

Furthermore, the greatest common divisor of two polynomials is unique.

Proof. Let $d(x)$ be the monic polynomial of smallest degree in the set

$$S = \{f(x)p(x) + g(x)q(x) : f(x), g(x) \in \mathbb{F}[x]\}$$

We can write $d(x) = r(x)p(x) + s(x)q(x)$ for two polynomials $r(x)$ and $s(x)$ in $\mathbb{F}[x]$. We need to show that $d(x)$ divides both $p(x)$ and $q(x)$. We shall first show that $d(x)$ divides $p(x)$. By the division algorithm (Theorem 2.2.1), there exists polynomials $a(x)$ and $b(x)$ such that $p(x) = a(x)d(x) + b(x)$ where $b(x)$ is either the zero polynomial or $\deg(b) < \deg(d)$. Therefore,

$$\begin{aligned} b(x) &= p(x) - a(x)d(x) \\ &= p(x) - a(x)[r(x)p(x) + s(x)q(x)] \\ &= p(x) - a(x)r(x)p(x) - a(x)s(x)q(x) \\ &= p(x)(1 - a(x)r(x)) + q(x)(-a(x)s(x)) \end{aligned}$$

is a linear combination of $p(x)$ and $q(x)$ and therefore must be in S. However, $b(x)$ must be the zero polynomial since $d(x)$ was chosen to be of the smallest degree; consequently, $d(x)$ divides $p(x)$. An analogous argument shows that $d(x)$ must divide $q(x)$ and hence, $d(x)$ is a common divisor of $p(x)$ and $q(x)$.

Next, to show that $d(x)$ is the greatest common divisor of $p(x)$ and $q(x)$, suppose that $d'(x)$ is another common divisor of $p(x)$ and $q(x)$. We will show that $d'(x) \mid d(x)$. Since $d'(x)$ is a common divisor of $p(x)$ and $q(x)$, there exist polynomials $u(x)$ and $v(x)$ such that $p(x) = u(x)d'(x)$ and $q(x) = v(x)d'(x)$. Therefore,

$$\begin{aligned} d(x) &= r(x)p(x) + s(x)q(x) \\ &= r(x)u(x)d'(x) + s(x)v(x)d'(x) \\ &= d'(x)[r(x)u(x) + s(x)v(x)] \end{aligned}$$

Since $d'(x) \mid d(x)$, $d(x)$ is the greatest common divisor of $p(x)$ and $q(x)$.

Finally, we must show that the greatest common divisor of $p(x)$ and $q(x)$ is unique. Suppose that $d'(x)$ is another greatest common divisor of $p(x)$ and $q(x)$. We have just shown that there exists polynomials $u(x)$ and $v(x)$ in $\mathbb{F}[x]$ such that

$$d(x) = d'(x)[r(x)u(x) + s(x)v(x)]$$

Since

$$\deg(d) = \deg(d') + \deg[ru + sv]$$

and $d(x)$ and $d'(x)$ are both greatest common divisors, $\deg(d) = \deg(d')$. Since $d(x)$ and $d'(x)$ are both monic polynomials of the same degree, then $d(x) = d'(x)$. □

2.3 Irreducible Polynomials

Index