Chapter 4

Rings of Polynomials

Introduction

Throughout this chapter we shall assume that $\mathbb{A}$ is a commutative ring with identity $1 \neq 0$.

4.1 Definitions

Definition 4.1.1.
Any expression of the form

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

where $a_i \in \mathbb{A}$ and $a_n \neq 0$, is called a polynomial over $\mathbb{A}$ with indeterminate x.

1. *The elements $a_0, a_1, \ldots, a_n$ are called the coefficients of P.*
2. *The coefficient a_n is called the **leading coefficient**.*
3. *A polynomial is called **monic** if the leading coefficient is* 1.
4. *If n is the largest nonnegative number for which $a_n \neq 0$, we say that the degree of P is n and write* $\deg P(x) = n$.
5. *If $f = 0$ is the zero polynomial, then the degree of P is defined to be $-\infty$.*

6. *We will denote the set of all polynomials with coefficients in a ring* $\mathbb{A}$ *by* $\mathbb{A}[x]$.

7. *Two polynomials are equal exactly when their corresponding coefficients are equal; that is, if we let*

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$

and

$$q(x) = b_0 + b_1x + \cdots + b_nx^n,$$

then $p(x) = q(x)$ *if and only if* $a_i = b_i$ *for all* $i = 1, 2, ..., n$.

To show that the set of all polynomials forms a ring, we must first define addition and multiplication. We define the sum of two polynomials as follows. Let

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$

and

$$q(x) = b_0 + b_1x + \cdots + b_mx^m.$$

Then the sum of $p(x)$ and $q(x)$ is

$$p(x) + q(x) = c_0 + c_1x + \cdots + c_kx^k,$$

where $c_i = a_i + b_i$ for each i. We define the product of $p(x)$ and $q(x)$ to be

$$p(x)q(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n},$$

where

$$c_i = \sum_{k=0}^{i} a_kb_{i-k} = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0.$$

for each i. Notice that in each case some of the coefficients may be zero.

Example 4.1.1.
Suppose that

$$p(x) = 3 + 0x + 0x^2 + 2x^3 + 0x^4$$

and

$$q(x) = 2 + 0x - x^2 + 0x^3 + 4x^4$$

are polynomials in $\mathbb{Z}[x]$*. If the coefficient of some term in a polynomial is zero, then we usually just omit that term. In this case, we would write*

$$p(x) = 3 + 2x^3 \quad \textit{and} \quad q(x) = 2 - x^2 + 4x^4.$$

The sum of these two polynomials is

$$p(x) + q(x) = 5 - x^2 + 2x^3 + 4x^4.$$

The product,

$$p(x)q(x) = (3 + 2x^3)(2 - x^2 + 4x^4) = 6 - 3x^2 + 4x^3 + 12x^4 - 2x^5 + 8x^7,$$

can be calculated either by determining the c_i*'s in the definition or by simply multiplying polynomials in the same way as we have always done.*

Theorem 4.1.1.
Let $\mathbb{A}$ *be a commutative ring with identity. Then* $\mathbb{A}[x]$ *is a commutative ring with identity.*

Proof 4.1.1.
Our first task is to show that $\mathbb{A}[x]$ *is an abelian group under polynomial addition. The zero polynomial,* $f(x) = 0$*, is the additive identity. Given a polynomial* $p(x) = \sum_{i=0}^{n} a_i x^i$*, the inverse of* $p(x)$ *is easily verified to be*

$$-p(x) = \sum_{i=0}^{n} (-a_i) x^i = -\sum_{i=0}^{n} a_i x^i.$$

Commutativity and associativity follow immediately from the definition of polynomial addition and from the fact that addition in $\mathbb{A}$ *is both commutative and associative.*

To show that polynomial multiplication is associative, let

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

Then

$$\begin{aligned} [p(x)q(x)]r(x) &= \left[\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right)\right]\left(\sum_{i=0}^{p} c_i x^i\right) \\ &= \left[\sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i\right]\left(\sum_{i=0}^{p} c_i x^i\right) \end{aligned}$$

$$= \sum_{i=0}^{m+n+p} \left(\sum_{j=0}^{i} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) c_{i-j} \right) x^i$$
$$= \sum_{i=0}^{m+n+p} \left(\sum_{j+k+l=i} a_j b_k c_l \right) x^i$$
$$= \sum_{i=0}^{m+n+p} \left(\sum_{j=0}^{i} a_j \left(\sum_{k=0}^{i-j} b_k c_{i-j-k} \right) \right) x^i$$
$$= \left(\sum_{i=0}^{m} a_i x^i \right) \left(\sum_{i=0}^{n+p} \left(\sum_{j=0}^{i} b_j c_{i-j} \right) x^i \right)$$
$$= \left(\sum_{i=0}^{m} a_i x^i \right) \left[\left(\sum_{i=0}^{n} b_i x^i \right) \left(\sum_{i=0}^{p} c_i x^i \right) \right]$$
$$= p(x)[q(x)r(x)].$$

The commutativity and distribution properties of polynomial multiplication are proved in a similar manner. We shall leave the proofs of these properties as an exercise.

Proposition 4.1.1.
Let $p(x)$ and $q(x)$ be polynomials in $\mathbb{A}[x]$, where $\mathbb{A}$ is an integral domain. Then

1. $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$
2. $\deg(p(x) + q(x)) \leq \max(\deg(p(x)), \deg(q(x)))$

Furthermore, $\mathbb{A}[x]$ is an integral domain.

Proof 4.1.2.

1. *Suppose that we have two nonzero polynomials*

$$p(x) = a_m x^m + \cdots + a_1 x + a_0$$

and

$$q(x) = b_n x^n + \cdots + b_1 x + b_0$$

with $a_m \neq 0$ and $b_n \neq 0$. The degrees of p and q are m and n, respectively. The leading term of $p(x)q(x)$ is $a_m b_n x^{m+n}$, which cannot be zero since $\mathbb{A}$ is an integral domain; hence, the degree of $p(x)q(x)$ is $m+n$, 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 $\mathbb{A}[x]$ must also be an integral domain.

2. *Trivial.*

Let $\mathbb{U}(\mathbb{A})$ denote the units (invertible elements) of $\mathbb{A}$.

Proposition 4.1.2.
If $\mathbb{A}$ is an integral domain, then the units of $\mathbb{A}[X]$ are exactly the constant polynomials $P = a$ where $a \in \mathbb{U}(\mathbb{A})$.

Proof 4.1.3.
Let P be invertible in $\mathbb{A}[X]$. There exists $Q \in \mathbb{A}[X]$ such that $PQ = 1$. Thus, $\deg(P) + \deg(Q) = 0$ implies $\deg(P) = \deg(Q) = 0$. Hence, P and Q are constant invertible elements.

4.2 Polynomial Arithmetic

4.2.1 Associated Polynomials

Definition 4.2.1.
Two polynomials P and Q in $\mathbb{A}[X]$ are said to be associated if there exists $a \in \mathbb{U}(\mathbb{A})$ such that $P = aQ$.

Example 4.2.1.
The set of polynomials associated with $X^2 + 1$ in $\mathbb{Z}[X]$ is

$$\{X^2 + 1, -(X^2 + 1)\}$$

since the only units in $\mathbb{Z}$ are 1 and -1.

Proposition 4.2.1.

1. *The relation "being associated" is an equivalence relation on $\mathbb{A}[X]$.*

2. *If P and Q are associated and have the same leading coefficient, then $P = Q$.*

3. *If $\mathbb{A}$ is a field, then every polynomial P is associated with a unique unitary polynomial.*

4.2.2 Division

Definition 4.2.2.
Let $P, Q \in \mathbb{A}[X]$. We say that P divides Q, denoted as $P|Q$, if there exists $R \in \mathbb{A}[X]$ such that $Q = PR$.

Example 4.2.2.

1. *The polynomial $X - 1$ divides $X^2 - 1$ in $\mathbb{Z}[X]$.*
2. *The polynomial $X - 3$ does not divide $X^2 - 1$ in $\mathbb{Z}[X]$.*

Proposition 4.2.2.
Let $P, Q, R, S \in A[X]$.

1. *If $P|Q$ and $Q|R$, then $P|R$.*
2. *If $P|Q$ and $P|R$, then $P|(Q + R)$.*
3. *If $P|Q$ and $Q \neq 0$, then $\deg(P) \leq \deg(Q)$.*
4. *If $P|Q$ and $R|S$, then $PR|QS$.*
5. *If $P|Q$, then $P^n|Q^n$ for all $n \geq 1$.*

Proposition 4.2.3.
Let $P, Q, R, S \in A[X]$.

1. *If $P|Q$ and $Q|P$, then P and Q are associated.*
2. *If P is associated with R and Q is associated with S, then $P|Q \iff R|S$.*

4.2.3 Euclidean Division

Theorem 4.2.1. *(Euclidean Division)*
Let $A, B \in \mathbb{K}[X]$ be two polynomials with coefficients in a field $\mathbb{K}$ such that $B \neq 0$. Then there exists a unique pair (Q, R) of $\mathbb{K}[X]$ such that $A = BQ + R$ and $\deg(R) < \deg(B)$.

Example 4.2.3.
Let $A = x^3 + x + 1$ and $B = x + 1$. Then we have $A = B(x^2 - x + 2) - 1$.

Recall that a subset I of a ring $\mathbb{A}$ is an ideal if the following two conditions hold:

1. $(I, +)$ is a subgroup of $(A, +)$,

2. For every $a \in A$, $aI \subset I$. In other words, for all $a \in A$ and $x \in I$, $ax \in I$.

Theorem 4.2.2.
The ring $\mathbb{K}[X]$ is principal (In other words, every ideal $I \subseteq \mathbb{K}[X]$ can be written as $I = (P(X))$ for some $P(X) \in \mathbb{K}[X]$).

Proof 4.2.1.
Let I be an ideal of $\mathbb{K}[X]$ containing a nonzero polynomial. We want to show that I is principal, i.e., there exists a polynomial P such that I is exactly the set of multiples of P. Let $D = \{\deg(S) \mid S \in I, S \neq 0\}$. This is a non-empty subset of $\mathbb{N}$, so it has a minimum n. Let P be a polynomial of degree n in I. Since I is an ideal, all multiples of P are in I. Conversely, we want to show that every element of I is a multiple of P. So let $A \in I$. We know there exist Q, R such that $A = PQ + R$ with $\deg(R) < n$. Since $-PQ \in I$, we have $R = A - PQ \in I$. As $\deg(R) < n$, by the definition of n, we have $R = 0$, i.e., $A = PQ$, and A is indeed a multiple of P.

4.2.4 Irreducible Polynomials

Recall that the invertible polynomials in $\mathbb{A}[X]$ are the constant polynomials $P = a \in \mathbb{U}(A)$. Thus, since all non-zero elements in a field are invertible, the invertible polynomials in $\mathbb{K}[X]$ are the non-zero constant polynomials.

Definition 4.2.3.
A polynomial $P \in \mathbb{K}[X]$ is called irreducible if it is not invertible and if the equality $P = QR$ implies that either Q or R is invertible.

We say that a polynomial P is reducible if it is not irreducible.

Example 4.2.4.

1. *The polynomial $P(X) = 3$ is invertible in $\mathbb{Q}[X]$, so it is not irreducible.*

2. *The polynomial $P(X) = X^2 + 1$ is irreducible if we consider it as an element of $\mathbb{R}[X]$, but it is reducible if we consider it as an element of $\mathbb{C}[X]$, because $X^2 + 1 = (X - i)(X + i)$.*

The notion of irreducible polynomials depends on the field $\mathbb{K}$.

Proposition 4.2.4.

1. *Reducible polynomials in* $\mathbb{K}[X]$ *have degree greater than or equal to* 2.
2. *All polynomials of degree* 1 *are irreducible.*

4.2.5 Greatest Common Divisor

Let $P_1, ..., P_n \in \mathbb{K}[X]$. Since $\mathbb{K}[X]$ is principal, the ideal

$$< P_1, ..., P_n >= \{P_1A_1 + P_2A_2 + \cdots + P_nA_n \mid A_1, A_2, \ldots, A_n \in \mathbb{K}[X]\}.$$

is generated by a unique unit polynomial P. This polynomial is called the **greatest common divisor** *gcd* of P_i and is denoted

$$P = \gcd(P_1, ..., P_n).$$

Proposition 4.2.5. ***Properties of*** *gcd*
Let $P, Q \in \mathbb{K}[X]$. *Then*

1. $\gcd(P, Q)$ *is a common divisor of* P *and* Q.
2. *If* D *is another common divisor of* P *and* Q, *then* D *divides* $\gcd(P, Q)$.
3. *There exist polynomials* $(U, V) \in \mathbb{K}[X]^2$ *such that*

$$PU + QV = \gcd(P, Q).$$

Definition 4.2.4.
Let $P, Q \in \mathbb{K}[X]$. *We say that* P *and* Q *are coprime if* $\gcd(P, Q) = 1$.

In other words, if $\gcd(P, Q) = 1$, then only non-zero constants divide both P and Q.

4.2.6 Factorization

Theorem 4.2.3.
Let $P \in \mathbb{K}[X]$ be a non-zero polynomial. Then P decomposes uniquely up to the order of factors as:

$$P = \alpha P_1^{\alpha_1} P_2^{\alpha_2} ... P_n^{\alpha_n}$$

where P_i are distinct, unit, irreducible polynomials in $\mathbb{K}[X]$ and $\alpha \in \mathbb{K}^*$ is the leading coefficient of P.

Example 4.2.5.
Consider the polynomial $P = x^2 + 1$. Then P exists in both $\mathbb{R}[X]$ and $\mathbb{C}[X]$. However, care must be taken as its factorization differs in these two rings:

1. *P factors as $(X - i) \cdot (X + i)$ in $\mathbb{C}[X]$.*
2. *P is irreducible in $\mathbb{R}[X]$.*

Proposition 4.2.6.
Let P and Q be two non-zero polynomials. Let $P = aP_1^{\alpha_1} P_2^{\alpha_2} ... P_n^{\alpha_n}$ and $Q = bP_1^{\beta_1} P_2^{\beta_2} ... P_n^{\beta_n}$ be their decompositions into irreducible factors where $\alpha_i, \beta_i \geq 0$ for all $i \in \{1, ..., n\}$. Then

$$P \text{ divides } Q \Leftrightarrow \alpha_j \leq \beta_j \text{ for all } 1 \leq j \leq n$$

.

4.3 Polynomial Functions

Let $P \in \mathbb{K}[X]$. We denote by f_P the polynomial function associated with P, defined as:

$$\begin{aligned} f_P : \mathbb{K} &\longrightarrow \mathbb{K} \\ x &\mapsto P(x). \end{aligned}$$

Definition 4.3.1.
Let $P \in \mathbb{K}[X]$. We say that $x \in \mathbb{K}$ is a root of P if $f_P(x) = 0$ (or $P(x) = 0$).

Proposition 4.3.1.
Let $P \in \mathbb{K}[X]$ and $\alpha \in \mathbb{K}$. Then α is a root of P if and only if the polynomial $(x - \alpha)$ divides P.

Definition 4.3.2.
Let $P \in \mathbb{K}[X]$ and let α be a root of P. We say that α has multiplicity k if and only if $(x-\alpha)^k$ divides P and $(x-\alpha)^{k+1}$ does not divide P.

In other words, α is a root of P of multiplicity k if and only if
$P = (x-\alpha)^k Q$ and $Q(\alpha) \neq 0$.

Example 4.3.1.
To determine the multiplicity of a root, we can perform successive Euclidean divisions. Let $P = x^3 - 3x^2 + 4$. It can be verified easily that 2 is a root of P. Furthermore, we find $P(x) = (x-2)^2 Q(x)$ with $Q(x) = x+1$ and $Q(2) \neq 0$.

Theorem 4.3.1.
Let $P \in \mathbb{K}[X]$ and $\alpha_1, ..., \alpha_r$ be pairwise distinct roots of multiplicative $k_1, ..., k_r$, respectively. Then, there exists $Q \in \mathbb{K}[X]$ such that

$$P = (x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}...(x-\alpha_r)^{k_r}Q$$

and $Q(\alpha_i) \neq 0$ for all i. In particular, P has a degree of at least $k_1 + ... + k_r$.