6 Polynomial Rings

We introduce a class of rings called the polynomial rings, describing computation, factorization and divisibility in such rings. For the case where the coefficients come from an integral domain, the corresponding polynomials also form an integral domain.

**Definition 6.1.** Let \( R \) be an integral domain. A polynomial \( f(x) \) in indeterminate \( x \) with coefficients in \( R \) has the form

\[
f(x) = f_0 + f_1 x + \cdots + f_n x^n,
\]

where \( n \) is a nonnegative integer and \( f_i \in R \) for each \( i \). If \( f_n \neq 0 \) we say that \( f(x) \) has degree \( n \) and write \( \deg f = n \).

We denote by \( R[x] \) the set of all polynomials with coefficients in \( R \).

**Example 6.1.** Let \( f(x) = \frac{3/2^3}{x} + 2ix^2 - \frac{5}{2}. \) Then \( f \) is a polynomial with complex coefficients, so \( f \in \mathbb{C}[x] \). On the other hand

\[
g(x) = \frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots
\]

is not a polynomial, since it doesn’t have finite degree. \( g(x) \) is an example of a power series.

We can use the addition and multiplication as defined on the ring \( R \) to define operations of addition and multiplication in \( R[x] \). As we’ll soon see, with these operations, the set \( R[x] \) has the structure of a ring. We’ll mostly consider the case where \( R \) is a field, in which case \( R[x] \) is an integral domain.

Addition of polynomials is defined by

\[
f + g = (f_0 + g_0) + (f_1 + g_1)x + \cdots + (f_n + g_n)x^n
\]

(6.1) and multiplication of polynomials is defined by

\[
f g = f_0 g_0 + (f_1 g_0 + f_0 g_1)x + (f_0 g_2 + f_1 g_1 + f_2 g_0)x^2 + \cdots + (f_0 g_i + f_1 g_{i-1} + \cdots + f_i g_0)x^i + \cdots + f_n g_m x^{n+m}
\]

(6.2)

where \( f = f_0 + f_1 x + \cdots + f_n x^n \), \( g = g_0 + g_1 x + \cdots + g_m x^m \), and W.L.O.G., \( n \) and \( m \) are a pair of non-negative integers satisfying \( n \geq m \). (If \( i \geq m \) then \( g_i = 0 \).)

If \( f = f' \) and \( g = g' \) for some \( f, f', g, g' \in R[x] \) then \( f_i = f'_i, g_i = g'_i \) for each \( i \), so

\[
(f + g) + h = (f_0 + g_0 + h_0) + (f_1 + g_1 + h_1)x + \cdots + (f_n + g_n + h_n)x^n,
\]

\[
= (f'_0 + g'_0 + h_0) + (f'_1 + g'_1 + h_1)x + \cdots + (f'_n + g'_n + h_n)x^n,
\]

\[
= f' + g' + h,
\]

since addition is well-defined on \( R \). It follows that addition is well-defined on \( R[x] \). Similarly, multiplication is well-defined on \( R[x] \).

If \( f, g, h \in R[x] \) then

\[
(f + g) + h = ((f_0 + g_0) + h_0) + ((f_1 + g_1) + h_1)x + \cdots + ((f_n + g_n) + h_n)x^n,
\]

\[
= (f_0 + (g_0 + h_0)) + (f_1 + (g_1 + h_1))x + \cdots + ((f_n + (g_n + h_n))x^n,
\]

\[
= f + (g + h),
\]

since addition is associative in \( R \). Similarly, we can show that multiplication of polynomials over a ring is associative.

\( R[x] \) has an additive identity, namely 0, the additive identity of \( R \), and the additive inverse of \( f = f_0 + f_1 x + \cdots + f_n x^n \) is given by

\[
-f = -f_0 + (-f_1)x + \cdots + (-f_n)x^n.
\]

All this tells us the following:
Lemma 6.1. \( R[x] \) is a ring with the operations of polynomial addition and multiplication as defined in Equations 6.1, 6.2.

If \( R \) is unital and commutative, then so is \( R[x] \). If \( F \) is a field then since \( F \) has no zero divisors, it is straightforward to show that degree \((fg) = \text{degree } f + \text{degree } g \) for all \( f, g \in F[x] \). Since \( R \) is unital and commutative, it can be shown that

**Lemma 6.2.** If \( F \) is a field then \( F[x] \) is an integral domain.

Given nonzero polynomials \( a, b \in F[x] \), we say that \( a \) is a **divisor** of \( b \) in \( F[x] \), expressed \( a | b \), if \( b = ac \) for some \( c \in F[x] \). If \( c \notin F^* \) we say that \( a \) is a **proper divisor** of \( b \). Since \( F[x] \) is an I.D., if \( f, g \in F[x] \) then \( f | g \) and \( g | f \) if and only if \( f = ug \) for some \( u \in F^* \).

**Definition 6.2.** Let \( f, g \in F[x] \). A **common divisor** of \( f, g \) in \( F[x] \) is an polynomial \( d \in F[x] \) such that \( d | f \) and \( d | g \). A common divisor \( d \) of \( f, g \) is called a **greatest common divisor** (gcd) of \( f \) and \( g \) if any other common divisor of \( f \) and \( g \) is also a divisor of \( d \).

If \( d \) is a gcd of \( f \) and \( g \) then we write \( d = \gcd(f, g) \), which is unique in \( F[x] \), up to multiplication by nonzero elements of \( F \) (the units of \( F[x] \)). If \( \gcd(f, g) = 1 \) we say that \( f \) and \( g \) are **coprime**.

The polynomial \( f = f_0 + f_1 x + \cdots + f_n x^n \) chosen to represent the gcd of a pair of polynomials has \( f_n = 1 \). Such a polynomial is called **monic**.

A non-constant polynomial \( f \in F[x] \) is called **irreducible** if it has no proper divisors. Irreducibles in \( F[x] \) play a role similar to the prime numbers in \( \mathbb{Z} \). If \( f | gh \) for some \( g, h \in F[x] \) and \( f \) is irreducible, then \( f | g \) or \( f | h \).

**Theorem 6.1.** (Division Algorithm in \( F[x] \)) Let \( f, g \in F[x], g \neq 0 \). Then there exist \( m, r \in F[x] \) satisfying \( f = mg + r \) with \( 0 \leq \text{degree } r < \text{degree } g \), or \( r = 0 \).

**Proof.** Let \( S = \{ f - mg : m \in F[x] \} \). If \( 0 \in S \) then \( r = 0 \) gives the required element, so assume otherwise. Let \( r = f - mg \neq 0 \) have minimal degree in \( S \). Let degree \( r = \ell \), degree \( g = k \) and suppose that \( \ell - k = d \geq 0 \). Then

\[
   r - \left( \frac{r_j}{g_k} x^d \right) g = f - (m_0 + \frac{r_j}{g_k} x^d)g \in S,
\]

where \( r_i, g_j \) are the \( i \)th and \( j \)th coefficients of \( r \) and \( g \), respectively, and degree\( (r - \left( \frac{r_j}{g_k} x^d \right) g) < \ell \), unless \( r - \left( \frac{r_j}{g_k} x^d \right) g = 0 \). The former contradicts the minimality of \( r \) in \( S \), and the latter the fact that \( 0 \notin S \). The result follows.

The Euclidean algorithm is a technique for computing the gcd of a pair of polynomials. If \( f, g \in F[x], f, g \neq 0 \) and degree \( f \geq \text{degree } g \), then repeated applications of the division algorithm yields

\[
   f = m_1 g + r_1, \quad g = m_2 r_1 + r_2, \quad r_1 = m_3 r_2 + r_3, \quad \ldots \quad r_{i} = m_{i+2} r_{i-1} + r_{i+2}, \quad \ldots \quad r_{k-2} = m_{k} r_{k-1} + r_{k}, \quad r_{k-1} = m_{k+1} r_{k} + 0,
\]

with degree \( r_k < \text{degree } r_{k-1} < \cdots < \text{degree } r_1 < \text{degree } g \) and \( r_k \neq 0 \). Since we have generated a sequence of strictly decreasing positive integers, the process must terminate in a finite number of steps (in fact in at
most \( t \) steps where \( t \) is the difference in the degrees of \( f \) and \( g \). Note that \( r_k \) divides \( r_{k-1} \) in \( F[x] \), and hence \( r_{k-2} = m_k r_{k-1} + r_k \). Repeat this argument to see that \( r_k \) divides each remainder \( r_i \), and finally \( f \) and \( g \) in \( F[x] \). If \( d \) is a common divisor of \( f \) and \( g \) then \( d \) divides \( r_1, r_2, \ldots, r_k \), so \( r_k \) is the greatest common divisor of \( f \) and \( g \).

**Example 6.2.** Let \( f = x^6 + 2x^4 + x^3 + 2x^2 + x + 1, g = x^3 + x^2 + x + 1 \) be a pair of rational polynomials. Then, implementing the Euclidean algorithm we obtain the equations:

\[
\begin{align*}
f &= xg + x^2 + 1, \\
g &= (x + 1)r_1 + 0,
\end{align*}
\]

so \( x^2 + 1 \) is the gcd of \( f \) and \( g \) in \( \mathbb{Q}[x] \).

**Theorem 6.2.** Let \( f, g \in F[x] \). Then \( f \) and \( g \) have a well-defined gcd, say \( d = \gcd(f, g) \), and there exist \( s, t \in F[x] \) such that \( fs + gt = d \). Moreover, \( d \) is unique up to multiplication by units in \( F \).

**Proof.** Let \( S = \{ fs + gt : s, t \in F[x] \} \). Clearly \( f, g \in S \), so \( S \neq \emptyset \). Let \( d \in S \) have minimal degree and suppose \( d = fs_0 + gt_0 \) for some \( s_0, t_0 \in F[x] \). We claim that \( d = \gcd(f, g) \). Let \( w = fs_1 + gt_1 \in S \). From the D.A. in \( F[x] \), there exist \( m, r \in R \) such that \( w = md + r \) and \( r = 0 \) or degree \( r < \) degree \( d \). But then

\[
r = w - md = (s_1 - ms_0)f + (t_1 - mt_0)g \in S.
\]

It follows by the minimality of \( d \) in \( S \) that \( r = 0 \). Thus \( d \) divides every element of \( S \), so, in particular, \( d | f, g \). On the other hand, if \( c \) is a common divisor of \( f \) and \( g \) then \( c|(fs + gt) \) for all \( s, t \in F[x] \), so any common divisor of \( f, g \) also divides \( d \). Thus \( d = \gcd(f, g) \).

To see that \( \gcd(f, g) \) is unique, suppose that \( e \) is also a gcd of \( f \) and \( g \) in \( F[x] \). Then \( d | e \) and \( e | d \) in \( F[x] \), and in particular degree \( d = \) degree \( e \). It follows that \( e \) is a unit multiple of \( d \) in \( F[x] \).

**Definition 6.3.** An I.D. \( R \) is called a **unique factorization domain (U.F.D)** if every non-zero non-unit in \( R \) can be expressed uniquely (up to multiplication by a unit) as a finite product of irreducibles in \( R \).

**Example 6.3.** The ring of integers forms a U.F.D. - every number can be uniquely expressed as a finite product of prime numbers, and up to multiplication by \( \pm 1 \) (the units of \( \mathbb{Z} \)), this can be done in only one way.

**Theorem 6.3.** \( F[x] \) is a U.F.D.

By convention, if \( f \in F[x] \) we express its factorization as

\[
f = \delta f_1 f_2 \cdots f_t,
\]

where each \( f_i \) is monic and irreducible in \( F[x] \) and \( \delta \) is a constant in \( F \).

**Definition 6.4.** If \( f \in F[x] \) and \( f(\alpha) = 0 \) for some \( \alpha \) in an extension field of \( F \), we say that \( \alpha \) is a **root** of \( f \).

**Theorem 6.4.** (The Factor Theorem) Let \( f \in F[x] \) and let \( \alpha \in F \). Then \( \alpha \) is a root of \( f \), if and only if \( (x - \alpha)|f \) in \( F[x] \).

**Proof.** From the D.A., there exist \( g, r \in F[x] \) such that \( f = (x - \alpha)g + r \), and either degree \( r < \) degree \( (x - \alpha) = 1 \), or \( r = 0 \). Then \( r \) is constant, since and \( f(\alpha) = (\alpha - \alpha)g(\alpha) + r(\alpha) = r(\alpha) = 0 \). Then \( r = 0 \) and \( x - \alpha \) divides \( f \) in \( F[x] \).

This gives us a criterion for irreducibility.

**Corollary 6.1.** (Root Test) Let \( f \in F[x] \) and let degree \( f \in \{2, 3\} \). Then \( f \) has no roots in \( F \) if and only if \( f \) is irreducible in \( F[x] \).

There are a number of classical results which help us to determine whether or not an integer polynomial is reducible over the rationals.
Theorem 6.5. (Rational Root Test) Let \( f = f_0 + f_1 x + \cdots + f_n x^n \in \mathbb{Z}[x] \). If \( \alpha = r/s \in \mathbb{Q}, (r, s) = 1 \) is a root of \( f \) then \( r \) divides \( f_0 \) and \( s \) divides \( f_n \).

Proof. If \( r/s \in \mathbb{Q} \) with \( \gcd(r, s) = 1 \) and \( r/s \) is a root of \( f \) then

\[ f(r/s) = f_0 + f_1(r/s) + \cdots + f_n(r/s)^n = 0, \]

and hence

\[ f_0 s^n + f_1 r s^{n-1} + \cdots + f_n r^{n-1} s = -f_n r^n. \]

Since \( r, s \) have no factors in common, \( s \) divides \( f_n \). Similarly, \( r \) divides \( f_0 \).

\[ \square \]

Definition 6.5. Let \( f = f_0 + f_1 x + \cdots + f_n x^n \in \mathbb{Z}[x] \). Then we say that \( f \) is primitive if the gcd of \( f_0, f_1, \ldots, f_n \) in \( \mathbb{Z} \) is 1.

Lemma 6.3. If \( f, g \in \mathbb{Z}[x] \) are primitive, then so is \( fg \).

Theorem 6.6. (Gauss’ Lemma) If the primitive polynomial \( f \in \mathbb{Z}[x] \) can be factored as \( f = gh, g, h \in \mathbb{Q}[x] \), then there exist \( g_1, h_1 \in \mathbb{Z}[x] \) such that \( f = g_1 h_1 \).

We can state Gauss’ Lemma in another way.

Corollary 6.2. A polynomial \( f \) in \( \mathbb{Z}[x] \) is irreducible in \( \mathbb{Z}[x] \) if and only if it is irreducible in \( \mathbb{Q}[x] \).

Example 6.4. Let \( f = x^3 + 2x + 1 \in \mathbb{Q}[x] \). From the rational root test (RRT), if \( f \) has a rational root it is one of \( \pm 1 \). From the root test, since \( f \) has degree 3, it is irreducible if and only if \( f \) has no rational roots. Since \( f(1), f(-1) \neq 0 \), we deduce that \( f \) is irreducible over \( \mathbb{Q} \).

Theorem 6.7. (Eisenstein’s Criterion) Let \( f = f_0 + f_1 x + \cdots + f_n x^n \in \mathbb{Z}[x] \). If there exists a prime \( p \in \mathbb{Z} \) such that

\[ p \nmid f_0, p \nmid f_1, \ldots, p \nmid f_{n-1}, p \nmid f_n \]

Then \( f \) is irreducible.

Proof. Let \( p \in \mathbb{Z}, f \in \mathbb{Z}[x] \) be as in the statement of the theorem. We may assume that \( f \) is primitive. Suppose \( f = gh \) for some \( g, h \in \mathbb{Z}[x] \). Then \( f_0 = gh_0 \). We may assume that \( p \nmid g_0 \), which implies that \( p \) does not divide \( h_0 \). Since \( f \) is primitive, \( p \) does not divide all the coefficients of \( g \). Let \( 0 < j < n \) be the least integer such that \( p \nmid g_j \). Then

\[ f_j = g_0 h_j + g_1 h_{j-1} + \cdots + g_n h_0, \]

so \( p \nmid f_j, g_0, g_1, \ldots, g_{j-1} \), and, since \( p \) does not divide \( g_j \), \( p \nmid h_0 \), giving a contradiction. We deduce that \( f \) is irreducible over \( \mathbb{Q} \).

\[ \square \]

Let \( f \in F[x] \). Then \( f(x) = g(x)h(x) \) for some \( g, h \in F[x] \) if and only if \( f(x+a) = g(x+a)h(x+a) \) for some \( a \in F \), in which case \( g(x+a), h(x+a) \in F[x] \). It follows that \( f \) is irreducible in \( F[x] \) if and only if \( f(x+a) \) is irreducible in \( F[x] \) for all \( a \in F \). It is sometimes convenient to use this substitution method to change the form of a polynomial to one which can be more easily identified as irreducible or reducible.

Example 6.5. Let \( f = x^4 + 1 \in \mathbb{Q}[x] \). Then \( f(x) \) is irreducible in \( \mathbb{Q}[x] \) if and only if \( f(x+1) \) is irreducible in \( \mathbb{Q}[x] \). Now

\[ f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2, \]

which is irreducible in \( \mathbb{Q}[x] \) by Eisenstein’s irreducibility criterion with \( p = 2 \).

Theorem 6.8. Let \( f \in \mathbb{R}[x] \) and let \( \alpha \in \mathbb{C} \) be a root of \( f \). Then \( \bar{\alpha} \) is also a root of \( f \).

Proof.

\[ f(\bar{\alpha}) = f_0 + f_1 \bar{\alpha} + f_1 \bar{\alpha}^2 + \cdots + f_n \bar{\alpha}^n \]

\[ = f_0 + f_1 \alpha + f_1 \alpha^2 + \cdots + f_n \alpha^n = 0. \]

\[ \square \]
This means that no odd degree polynomial $f$ is irreducible in $\mathbb{R}[x]$: if $f$ has no real roots and $\alpha$ is a root of $f$ then $x^2 + 2\text{Re}(\alpha) + |\alpha|^2$ divides $f$ in $\mathbb{R}[x]$.

It turns out that every polynomial of degree $f$ over the complex numbers factorizes as a product of $n$ linear factors over $\mathbb{C}$. A field with this property is called \textbf{algebraically closed}.

\textbf{Theorem 6.9.} (The Fundamental Theorem of Algebra) Every polynomial of degree $n$ in $\mathbb{C}[x]$ has exactly $n$ (not necessarily distinct) roots in $\mathbb{C}$.