Polynomials Over $\mathbb{R}$

0.1 Introduction

In mathematics, expressions of the form $x^2 + 2x + 1$ or $x^3 - 1$ are called *polynomials*. They are built using a symbol x and coefficients taken from a certain set. In Chapter 1, we introduced set notation. In this chapter, we consider the set of polynomials. We will start by introducing the polynomials with coefficients in the set of real numbers $\mathbb{R}$. We will explore some of their properties that are analogous with the set of integers $\mathbb{Z}$. Then, we will generalize the notation to polynomials over an arbitrary *field* (we will introduce the definition of a field in Chapter 11) and consider their respective factorizations.

Definition 0.1.1

polynomial, indeterminate, coefficient, term, $\mathbb{R}[x]$

A **polynomial** in x with coefficients in $\mathbb{R}$ is an expression of the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $n \geq 0$ is an integer, and

- x is a symbol called an **indeterminate**, and
- $a_0, a_1, \ldots, a_n$ are elements of $\mathbb{R}$.

Each individual a_i is called a **coefficient** of the polynomial, and each individual expression of the form $a_i x^i$ is called a **term** of the polynomial.

We use the notation $\mathbb{R}[x]$ to denote the set of all polynomials with coefficients in $\mathbb{R}$.

Example 1

As examples of polynomials in $\mathbb{R}[x]$, we have

- $-x^2 + \sqrt{7}x - 1$.
- $\frac{1}{2}x^5 - \frac{5}{13}x^4 + x^3 - x^2 + 5x + \frac{3}{2}$.
- $5x^4 + 0x^3 + 1x^2 + 0x - 2$. We would usually express the term $1x^2$ simply as x^2 and omit the terms $0x^3$ and $0x$, and write the polynomial more simply as $5x^4 + x^2 - 2$.

One of the most important properties of a polynomial is its *degree*, which we define next.

Definition 0.1.2
degree of polynomial

Let $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial in $\mathbb{R}[x]$, where $n \geq 0$ is an integer, and $a_n \neq 0$. Then the polynomial is said to have **degree** n and we write $\deg f(x) = n$. In other words, the degree of a polynomial is the largest power of x that has a non-zero coefficient.

The **zero polynomial** has all of its coefficients equal to zero, and its degree is undefined.

A **constant polynomial** is a polynomial that is either the zero polynomial or a polynomial of degree 0. Polynomials of degree 1, 2 and 3 are called **linear polynomials**, **quadratic polynomials**, and **cubic polynomials**, respectively.

Example 2

As examples of the degree of polynomials, we have

- $2x^3 + \sqrt{2}x^2 - \frac{7\pi}{2}x + \frac{1}{5}$ is a cubic polynomial.
- $-x^2 + \sqrt{7}x - 1$ is a quadratic polynomial.
- $\frac{1}{2}x^5 - \frac{5}{13}x^4 + x^3 - x^2 + 5x + \frac{3}{2}$ is a polynomial of degree 5.
- $0x^3 + 0x^2 + 3x + 0$ is a linear polynomial, since the largest power of x with a non-zero coefficient is $x = x^1$.
- π is a constant non-zero polynomial and its degree is 0.
- 0 is a constant zero polynomial and its degree is undefined.

We end the section by defining what it means for two polynomials to be *equal*.

Definition 0.1.3
equal polynomials

The polynomials $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, and $b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$ in $\mathbb{R}[x]$ are **equal** if and only if $a_k = b_k$ for all $k = 0, 1, \ldots, n$.

0.2 Arithmetic with Polynomials

Arithmetic can be done with polynomials just as you have done in high school. When working with polynomials, we will sometimes use both function notation and summation notation. That is, we use $f(x)$ to denote an element of $\mathbb{R}[x]$, and write

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

We begin this section by formally defining the addition and the multiplication of polynomials. The notation "$\max\{m, n\}$" denotes the *maximum* of m and n.

Definition 0.2.1

addition and multiplication of polynomials

Let

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

be polynomials in $\mathbb{R}[x]$. Without loss of generality, we suppose that $m \leq n$ and write

$$f(x) = a_n x^n + \cdots + a_{m+1}x^{m+1} + a_m x^m + a_{m-1}x^{m-1} + a_1 x + a_0,$$

where $a_n = \cdots = a_{m+1} = 0$.

- **Addition** of $f(x)$ and $g(x)$ is defined by

$$f(x) + g(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

- **Multiplication** of $f(x)$ and $g(x)$ is defined by

$$\begin{aligned} f(x)g(x) &= (a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0)(b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + c_l x^l + \cdots + a_m b_n x^{m+n}, \end{aligned}$$

  where

$$c_l = a_0 b_l + a_1 b_{l-1} + \cdots + a_{l-1} b_1 + a_l b_0.$$

Example 3

In $\mathbb{R}[x]$, for $f(x) = x^2 + 7x - 1$ and $g(x) = \sqrt{2}x^3 + 4x^2 - 3x$, we obtain

$$\begin{aligned} f(x) + g(x) &= \sqrt{2}x^3 + 5x^2 + 4x - 1, \\ f(x)g(x) &= \sqrt{2}x^5 + (4 + 7\sqrt{2})x^4 + (25 - \sqrt{2})x^3 - 25x^2 + 3x. \end{aligned}$$

Next we give a very useful lemma about the degree of a product of two non-zero polynomials.

Lemma 1

(Degree of a Product (DP))

For all non-zero polynomials $f(x)$ and $g(x)$ in $\mathbb{R}[x]$, we have

$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

Proof: Let m and n be arbitrary non-negative integers. Let $f(x) = a_m x^m + \cdots + a_1 x + a_0$ and $g(x) = b_n x^n + \cdots + b_1 x + b_0$ be arbitrary polynomials in $\mathbb{R}[x]$ of degree m and n, respectively, so we have $a_m \neq 0$ and $b_n \neq 0$. Now from the definition of multiplication, we have $f(x)g(x) = c_{m+n}x^{m+n} + \cdots + c_1 x + c_0$, where $c_{m+n} = a_m b_n$. Since a_m and b_n are non-zero real numbers, it follows that $c_{m+n} = a_m b_n$ is also non-zero. We therefore conclude that $\deg f(x)g(x) = m + n = \deg f(x) + \deg g(x)$. □

0.3 Polynomial Divisibility

In this section, as well as in the following two sections, we will explore some properties about the set of polynomials $\mathbb{R}[x]$ that are similar to the set of integers $\mathbb{Z}$. We first consider division of polynomials. We define what it means for one polynomial to divide another in a similar way as for the integers.

Definition 0.3.1
divides, factor in $\mathbb{R}[x]$

For polynomials $f(x)$ and $g(x)$ over $\mathbb{R}$, we say that $g(x)$ **divides** $f(x)$ or $g(x)$ is a **factor** of $f(x)$, and we write $g(x) \mid f(x)$, if there exists a polynomial $q(x)$ such that $f(x) = q(x)g(x)$.

Example 4

As examples of polynomial division in $\mathbb{R}[x]$, we have

- $x - 1$ divides $x^3 - x^2$, because $x^3 - x^2 = x^2(x - 1)$.
- $x^2 - \sqrt{2}x + 1$ divides $x^4 + 1$, because $x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$.
- Any *non-zero* constant polynomial c divides any polynomial $f(x) \in \mathbb{R}[x]$, because $f(x) = \left(\frac{1}{c}f(x)\right)c$.
- The only polynomial that divides the zero polynomial is the zero polynomial itself.

It turns out that there is a lot of similarity between the division of integers and the division of polynomials. The following two results resemble Propositions 7 and 9, respectively, stated in Section 3.4. We leave their proofs as exercises.

Proposition 2

(Transitivity of Divisibility for Polynomials (TDP))

For all polynomials $f(x), g(x), h(x)$ in $\mathbb{R}[x]$, if $f(x) \mid g(x)$ and $g(x) \mid h(x)$, then $f(x) \mid h(x)$.

Proposition 3

(Divisibility of Polynomial Combinations (DPC))

For all polynomials $f(x), g(x), h(x)$ in $\mathbb{R}[x]$, if $f(x) \mid g(x)$ and $f(x) \mid h(x)$, then $f(x) \mid (a(x)g(x) + b(x)h(x))$ for all polynomials $a(x), b(x)$ in $\mathbb{R}[x]$.

0.4 The Division Algorithm for Polynomials

Another thing that polynomials and integers have in common is that when we divide one polynomial by another, we get a quotient polynomial and a remainder polynomial. The result that describes precisely what happens is called the Division Algorithm for Polynomials, and is stated next. This result is not proved in this course. Note that we use the notation $q(x)$ for the *quotient polynomial*, and $r(x)$ for the *remainder polynomial*, to emphasize the similarity with the Division Algorithm for integers that we have already seen, as Proposition 3 in Section 6.1.

Proposition 4 **(Division Algorithm for Polynomials (DAP))**

For all polynomials $f(x)$ and $g(x)$ in $\mathbb{R}[x]$ with $g(x)$ not the zero polynomial, there exist unique polynomials $q(x)$ and $r(x)$ in $\mathbb{R}[x]$ such that

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

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

Note that $g(x)$ divides $f(x)$ when the remainder $r(x)$ from DAP is the zero polynomial, or when $f(x)$ and $g(x)$ are both the zero polynomial.

Given a polynomial $f(x)$ and a non-zero polynomial $g(x)$, in order to find the quotient and remainder polynomials $q(x)$ and $r(x)$ featured in DAP, we use a process called *long division*. This process starts with the largest powers of x in $f(x)$ and $g(x)$, and is demonstrated in the following pair of examples. The following is an example of DAP for polynomials in $\mathbb{R}[x]$,

Example 5 **(Long Division of Polynomials over $\mathbb{R}$)**

What are the quotient and remainder polynomials when $f(x) = 3x^4 + x^3 - 4x^2 - x + 5$ is divided by $g(x) = x^2 + 1$ in $\mathbb{R}[x]$?

Before we begin, we would expect from the Division Algorithm for Polynomials that the remainder polynomial is either the zero polynomial, or has degree at most one. Now we carry out the long division:

$$\begin{array}{rrr|rrrrrrrrr}
 & & & & & & & 3x^2 & + & x & - & 7 \\ \cline{4-12}
x^2 & + & 1 & 3x^4 & + & x^3 & - & 4x^2 & - & x & + & 5 \\
 & & & 3x^4 & & & + & 3x^2 & & & & \\ \cline{4-12}
 & & & & & x^3 & - & 7x^2 & - & x & + & 5 \\
 & & & & & x^3 & & & + & x & & \\ \cline{6-12}
 & & & & & & - & 7x^2 & - & 2x & + & 5 \\
 & & & & & & - & 7x^2 & & & - & 7 \\ \cline{7-12}
 & & & & & & & & - & 2x & + & 12
\end{array}$$

Thus, the quotient polynomial is $q(x) = 3x^2 + x - 7$ and the remainder polynomial is $r(x) = -2x + 12$, of degree 1, and we can check that indeed $f(x) = q(x)g(x) + r(x)$.

Definition 0.4.1
polynomial equation, root

A **polynomial equation** is an equation of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

which will often be written as $f(x) = 0$, where $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$. An element $c \in \mathbb{R}$ is called a **root** of the polynomial $f(x)$ if $f(c) = 0$ (equivalently, if c is a solution of the polynomial equation $f(x) = 0$).

We now apply the Division Algorithm for Polynomials to prove a very useful result for polynomials over $\mathbb{R}$.

Proposition 5 **(Remainder Theorem (RT))**

For all polynomials $f(x) \in \mathbb{R}[x]$ and all $c \in \mathbb{R}$, the remainder polynomial when $f(x)$ is divided by $x - c$ is the constant polynomial $f(c)$.

Proof: Let $f(x)$ be an arbitrary polynomial in $\mathbb{R}[x]$ and c be an arbitrary element of $\mathbb{R}$. Applying the Division Algorithm for Polynomials with $g(x) = x - c$, there exist unique polynomials $q(x)$ and $r(x)$ such that

$$f(x) = q(x)(x - c) + r(x),$$

where $\deg r(x) < \deg(x - c) = 1$ or $r(x)$ is the zero polynomial. Therefore, the remainder $r(x)$ is a constant polynomial (which could be zero), and we will denote it by r_0. Hence we have

$$f(x) = q(x)(x - c) + r_0,$$

and substituting $x = c$ into this equation gives $f(c) = r_0$. □

Example 6 Find the remainder when $f(x) = 12x^{12} - 7x^{11} + 4x^9 - 11x^5 + 2x^2 - x + 2$ is divided by $x + 1$.

Solution: Instead of doing long division, we use the Remainder Theorem, by calculating

$$\begin{aligned} f(-1) &= 12(-1)^{12} - 7(-1)^{11} + 4(-1)^9 - 11(-1)^5 + 2(-1)^2 - (-1) + 2 \\ &= 12 - 7(-1) + 4(-1) - 11(-1) + 2 - (-1) + 2 \\ &= 12 + 7 - 4 + 11 + 2 + 1 + 2 \\ &= 31. \end{aligned}$$

Hence the remainder is 31.

The Remainder Theorem immediately implies the following corollary about linear factors of a polynomial.

Corollary 6 **(Factor Theorem (FT))**

For all polynomials $f(x) \in \mathbb{R}[x]$ and all $c \in \mathbb{R}$, the linear polynomial $x - c$ is a factor of the polynomial $f(x)$ if and only if $f(c) = 0$ (equivalently, c is a root of the polynomial $f(x)$).

The Factor Theorem gives us a linear factor $x - c$ of a polynomial $f(x)$ over $\mathbb{R}$ whenever c is a root of $f(x)$.

0.5 Polynomial Factorization

Recall how in Section 6.6 we defined the notion of a *prime number* and how we proved that every integer $n > 1$ can be written as a product of primes. It turns out that an analogous result holds for polynomials, and the so-called *irreducible polynomials* in $\mathbb{R}[x]$ play a role similar to a role that primes play in $\mathbb{Z}$.

Definition 0.5.1

reducible, irreducible polynomial

A polynomial $f(x) \in \mathbb{R}[x]$ of positive degree is a **reducible polynomial** in $\mathbb{R}[x]$ when we can write $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{R}[x]$ and $1 \leq \deg g(x), \deg h(x) < \deg f(x)$. Otherwise, we say $f(x)$ is an **irreducible polynomial** in $\mathbb{R}[x]$.

Example 7

As examples of reducible and irreducible polynomials in $\mathbb{R}[x]$, we have

- $x^2 - 1 = (x+1)(x-1)$ is reducible in $\mathbb{R}[x]$.
- $x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$ is reducible in $\mathbb{R}[x]$.
- $x + \pi$ is irreducible in $\mathbb{R}[x]$.
- $x^2 + 1$ is irreducible in $\mathbb{R}[x]$.

The following proposition is a generalization of Proposition 11 (Prime Factorization) from Section 6.6. We will leave its proof as an exercise.

Proposition 7

(Factorization Into Irreducible Polynomials (FIIP))

Every polynomial in $\mathbb{R}[x]$ of positive degree can be written as a product of irreducible polynomials.

Later in Chapter 11 we will learn that all irreducible polynomials in $\mathbb{R}[x]$ have either degree 1 or degree 2. In other words, every polynomial in $\mathbb{R}[x]$ of degree at least 3 is guaranteed to be reducible.