CHAPTER I: FUNDAMENTALS

Section 3: Polynomials

Definition: ***Polynomials*** with real coefficients are expressions of the form $\sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$, where the a_i are elements of $\mathbb{R}$. (In fact, we don't have to use $\mathbb{R}$. We could use $\mathbb{Q}$, $\mathbb{C}$ or any other *field*; fields are algebraic systems that we will cover shortly.) The ***degree*** of a polynomial is n, the largest index i such that $a_i \neq 0$. If $f \in \mathbb{R}[x]$, the degree of f is often denoted by $\deg(f)$. The ***leading coefficient*** is a_n and the ***leading term*** is $a_n x^n$. If $a_n = 1$, the polynomial is said to be ***monic***. The set of all polynomials with coefficients in $\mathbb{R}$ is denoted by $\mathbb{R}[x]$. Addition and multiplication of polynomials is defined by the familiar rules:

$$\left(\sum_i a_i x^i\right) + \left(\sum_i b_i x^i\right) = \sum_i (a_i + b_i) x^i \text{, and}$$

$$\left(\sum_i a_i x^i\right) \cdot \left(\sum_j b_j x^j\right) = \sum_i \sum_j (a_i b_j) x^{i+j}.$$

Example 1:

$$(3x^5 + 4x - 1) + (x^3 - 8x^2 + 2x + 7) = 3x^5 + x^3 - 8x^2 + 6x + 6$$

and

$$(3x^5 + 4x - 1) \cdot (x^3 - 8x^2 + 2x + 7) = 3x^8 - 24x^7 + 6x^6 + 21x^5 + 4x^4 - 33x^3 + 16x^2 + 26x - 7$$

Also, the degrees of these polynomials are 5 and 3 respectively and the leading coefficients are 3 and 1 respectively (making the second polynomial monic).

The real numbers $\mathbb{R}$ can be viewed as a subset of $\mathbb{R}[x]$ and the operations on $\mathbb{R}[x]$ extend to those on $\mathbb{R}$; that is, for any two real numbers, their sum and product as elements of $\mathbb{R}$ agree with their sum and product as elements of $\mathbb{R}[x]$.

Proposition 1: Addition and multiplication on $\mathbb{R}[x]$ satisfy all the following properties:

(a) Addition in $\mathbb{R}[x]$ is commutative and associative; that is, for all $f, g, h \in \mathbb{R}[x]$, $f + g = g + f$ and $f + (g + h) = (f + g) + h$.

(b) The additive identity is 0; that is, $0 + f = f$ for all $f \in \mathbb{R}[x]$.

(c) Every element $f \in \mathbb{R}[x]$ has an additive inverse $-f$ satisfying $f + (-f) = 0$.

(d) Multiplication in $\mathbb{R}[x]$ is commutative and associative; that is, for all $f, g, h \in \mathbb{R}[x]$, $fg = gf$ and $f(gh) = (fg)h$.

(e) The multiplicative identity is 1; that is, $1f = f$ for all $f \in \mathbb{R}[x]$.

(f) The distributive law holds: for all $f, g, h \in \mathbb{R}[x]$, $f(g + h) = fg + fh$.

Proof: We prove part (f) here and leave some of the others as exercises. Let $f(x) = \sum_i a_i x^i$, $g(x) = \sum_j b_j x^j$, and $h(x) = \sum_j c_j x^j$. Then

$$\begin{aligned}
f(x)\big(g(x) + h(x)\big) &= \sum_i a_i x^i \left(\sum_j b_j x^j + \sum_j c_j x^j \right) \\
&= \sum_i a_i x^i \left(\sum_j (b_j + c_j) x^i \right) \\
&= \sum_i \sum_j a_i (b_j + c_j) x^{i+j} \\
&= \sum_i \sum_j (a_i b_j + a_i c_j) x^{i+j} \\
&= \sum_i \sum_j (a_i b_j) x^{i+j} + \sum_i \sum_j (a_i c_j) x^{i+j} \\
&= \sum_i a_i x^i \sum_j b_j x^i + \sum_i a_i x^i \sum_j c_j x^i \\
&= f(x)g(x) + f(x)h(x)
\end{aligned}$$

Proposition 2: Let $f, g \in \mathbb{R}[x]$.

(a) $\deg(fg) = \deg(f) + \deg(g)$.

(b) $\deg(f + g) \le \max\{\deg(f), \deg(g)\}$.

Proof: left as an exercise.

Definition: Just as it was in the ordinary integers, we say that a polynomial f ***divides*** a polynomial g (or that g is ***divisible*** by f) if there is a polynomial h such that $fh = g$. As before, we write $f \mid g$ for "f divides g."

Now we come to the analogue of prime numbers. What polynomials should be considered "unfactorable?" Keep in mind that it is always possible to factor our any nonzero constant element (in other words, $f(x) = c(c^{-1}f(x))$ for all $c \neq 0$ and $f \in \mathbb{R}[x]$). But these are trivial factorizations. A nontrivial factorization $f(x) = g(x)h(x)$ is one in which both of the factors have positive degree (or equivalently, each factor has degree less than $\deg(f)$). This gives us our analogue for "prime" polynomials, called *irreducible* polynomials.

Definition: A polynomial $f \in \mathbb{R}[x]$ is ***irreducible*** if $\deg(f) > 0$ and it cannot be written as a product of two polynomials each with strictly smaller (but still positive) degree.

Theorem 3: Every polynomial $f \in \mathbb{R}[x]$ of positive degree can be written as a product of irreducible polynomials.

> **Proof**: (By induction on the degree of f). Every polynomial of degree 1 is irreducible already, so the theorem holds. Now suppose $\deg(f) \geq 2$ and assume that every polynomial with positive degree less than $\deg(f)$ can be written as the product of irreducible polynomials. If f itself is not irreducible, then we can write it as the product of two polynomials g and h with smaller degrees. But by our inductive hypothesis, both g and h can be written as the product of irreducible polynomials, thus f can be also.

Theorem 4: $\mathbb{R}[x]$ contains infinitely many irreducible polynomials. (In fact, $K[x]$ contains infinitely many irreducible polynomials for any field K.)

> **Proof**: This is trivial for $\mathbb{R}[x]$. For every $c \in \mathbb{R}$, $x - c$ is an irreducible polynomial. This would also hold for any infinite field. However, there exist fields (again, we'll get to this in the next section) with only a finite number of elements. But then we can apply the same sort of logic that proves there are infinitely many prime numbers and show there are infinitely many irreducible polynomials.

Remark: It is not true in general that every $K[x]$ has irreducible polynomials of arbitrarily large degree. In $\mathbb{C}[x]$, every irreducible polynomial has degree 1 and in $\mathbb{R}[x]$, every irreducible polynomial has degree less than 3. But in $\mathbb{Q}[x]$, it is true that there exist irreducible polynomials of arbitrarily large degree. Also, if K is a finite field, then clearly $K[x]$ only contains finitely many polynomials of any particular degree. Since we know there are infinitely many irreducible polynomials in $K[x]$ (by the last theorem), they must have arbitrarily large degrees.

As we have seen, there are many similarities between the integers (and the notions of addition/multiplication, prime, divisibility) and the polynomials. It also true that we can apply a version of the division algorithm. Recall that for integers, the Division Algorithm states that given two integers a and b, there exist two other integers q (called the quotient) and r (called the remainder) such that $a = bq + r$ and $0 \le r < b$. For polynomials, this looks like this:

Proposition 5 (Division Algorithm): Let $f, g \in \mathbb{R}[x]$. Then there exist polynomials q and r in $\mathbb{R}[x]$ such that $f = gq + r$ and $\deg(r) < \deg(g)$.

Corollary: Let $f \in \mathbb{R}[x]$ and $a \in \mathbb{R}$. Then there is a polynomial $q \in \mathbb{R}[x]$ such that $f(x) = q(x)(x-a) + f(a)$. Hence, $f(a) = 0$ if and only if $x - a$ divides f.