3.2 Factoring polynomials

In this section, we present several fundamental facts about polynomials, including an equivalent form of the Fundamental Theorem of Algebra. While these facts should be familiar to you, they nonetheless require careful formulation and proof. Before stating these results, though, we first present a review of the main concepts needed in order to more carefully work with polynomials.

Let \( n \in \mathbb{Z}_{+} \cup \{0\} \) be a non-negative integer, and let \( a_0, a_1, \ldots, a_n \in \mathbb{C} \) be complex numbers. Then we call the expression

\[
p(z) = a_n z^n + \cdots + a_1 z + a_0
\]

a polynomial in the variable \( z \) with coefficients \( a_0, a_1, \ldots, a_n \). If \( a_n \neq 0 \), then we say that \( p(z) \) has degree \( n \) (denoted \( \deg(p(z)) = n \)), and we call \( a_n \) the leading term of \( p(z) \). Moreover, if \( a_n = 1 \), then we call \( p(z) \) a monic polynomial. If, however, \( n = a_0 = 0 \), then we call \( p(z) = 0 \) the zero polynomial and set \( \deg(0) = -\infty \).

Finally, by a root (a.k.a. zero) of a polynomial \( p(z) \), we mean a complex number \( z \) such that, upon setting \( z = z \), we obtain the zero polynomial \( p(z_0) = 0 \). Note, in particular, that every complex number is a root of the zero polynomial.

Convention dictates that

1. a degree zero polynomial be called a constant polynomial,
2. a degree one polynomial be called a linear polynomial,
3. a degree two polynomial be called a quadratic polynomial,
4. a degree three polynomial be called a **cubic polynomial**, 
5. a degree four polynomial be called a **quadric polynomial**, 
6. a degree five polynomial be called a **quintic polynomial**, 

and so on.

Addition and multiplication of polynomials is a direct generalization of the addition and multiplication of real numbers, and degree interacts with these operations as follows:

**Lemma 3.2.1.** Let \( (p(z)) \) and \( (q(z)) \) be non-zero polynomials. Then

1. \( \deg(p(z) \pm q(z)) \leq \max\{\deg(p(z)), \deg(q(z))\} \)
2. \( \deg(p(z)q(z)) = \deg(p(z)) + \deg(q(z)) \).

**Theorem 3.2.2.**

Given a positive integer \( n \in \mathbb{Z}_+ \) and any choice of \( a_0, a_1, \ldots, a_n \in \mathbb{C} \) with \( a_n \neq 0 \), define the function \( f: \mathbb{C} \to \mathbb{C} \) by setting

\[
\forall \, z \in \mathbb{C}, \quad f(z) = a_n z^n + \cdots + a_1 z + a_0.
\]

In other words, \( f \) is a polynomial function of degree \( n \). Then

1. given any complex number \( w \in \mathbb{C} \), we have that \( f(w) = 0 \) if and only if there exists a polynomial function \( g: \mathbb{C} \to \mathbb{C} \) of degree \( n-1 \) such that \( \forall \, z \in \mathbb{C}, \quad f(z) = (z - w) g(z) \).
2. there are at most \( n \) distinct complex numbers \( w \) for which \( f(w) = 0 \). In other words, \( f \) has at most \( n \) distinct roots.
3. (Fundamental Theorem of Algebra, restated) there exist exactly \( (n + 1) \) complex numbers \( w \in \mathbb{C} \) (not necessarily distinct) such that \( \forall \, z \in \mathbb{C}, \quad f(z) = w_0 (z - w_1) \cdots (z - w_n) \). In other words, every polynomial function with coefficients over \( \mathbb{C} \) can be factored into linear factors over \( \mathbb{C} \).

**Proof.**

1. Let \( w \in \mathbb{C} \) be a complex number.

\((\Longrightarrow)\) Suppose that \( f(w) = 0 \). Then, in particular, we have that

\[
\forall \, \begin{align*}
\alpha_n w^n &+ \cdots + \alpha_1 w + \alpha_0 = 0.
\end{align*}
\]

Since this equation is equal to zero, it follows that, given any \( z \in \mathbb{C} \),

\begin{verbatim}
\begin{align*}
f(z) & = a_n z^n + \cdots + a_1 z + a_0 \\
& - (a_n w^n + \cdots + a_1 w + a_0) \\
& = a_n (z^n - w^n) + \cdots + a_1 (z - w) + a_0 - a_n w^n.
\end{align*}
\end{verbatim}
\[
\begin{align*}
+a_{n-1}(z^{n-1}-w^{n-1}) \\
&= a_{n}(z - w)\sum_{k = 0}^{n - 1}z^{k}w^{n - 1 - k} \\
&+ a_{n-1}(z - w)\sum_{k = 0}^{n - 2}z^{k}w^{n - 2 - k} \\
&+ \cdots \\
&= z - w)\sum_{m = 1}^{n} \left( a_m \sum_{k = 0}^{m - 1}z^{k}w^{m -1 - k} \right).
\end{align*}
\]

Thus, upon setting
\[
g(z) = \sum_{m = 1}^{n} \left( a_m \sum_{k = 0}^{m - 1}z^{k}w^{m -1 - k} \right),
\forall \, z \in \mathbb{C},
\]
we have constructed a degree \((n - 1)\) polynomial function \((g)\) such that \( \forall \, f(z) = (z - w) g(z), \forall z \in \mathbb{C}. \)

\((\text{"Longleftarrow"})\) Suppose that there exists a polynomial function \((g:\mathbb{C}\to\mathbb{C})\) of degree \((n-1)\) such that
\[
f(z) = (z - w) g(z), \forall z \in \mathbb{C}.
\]
Then it follows that \((f(w) = (w - w)g(w) = 0)\), as desired.

2. We use induction on the degree \((n)\) of \((f)\).

If \((n = 1)\), then \((f(z) = a_{1}z + a_{0})\) is a linear function, and the equation \((a_{1}z + a_{0} = 0)\) has the unique solution \((z = -a_{0}/a_{1})\). Thus, the result holds for \((n = 1)\).

Now, suppose that the result holds for \((n - 1)\). In other words, assume that every polynomial function of degree \((n - 1)\) has at most \((n - 1)\) roots. Using the Fundamental Theorem of Algebra (Theorem (3.1.1)), we know that there exists a complex number \((w \in \mathbb{C})\) such that \((f(w) = 0)\). Moreover, from Part~1 above, we know that there exists a polynomial function \((g)\) of degree \((n - 1)\) such that
\[
f(z) = (z - w) g(z), \forall z \in \mathbb{C}.
\]
It then follows by the induction hypothesis that \((g)\) has at most \((n - 1)\) distinct roots, and so \((f)\) must have at most \((n)\)
distinct roots.

3. This part follows from an induction argument on \((n)\) that is virtually identical to that of Part~2, and so the proof is left as an exercise to the reader.

Contributors

- Isaiah Lankham, Mathematics Department at UC Davis
- Bruno Nachtergaele, Mathematics Department at UC Davis
- Anne Schilling, Mathematics Department at UC Davis

Both hardbound and softbound versions of this textbook are available online at WorldScientific.com.