Math 524: Linear Algebra

Notes #4 — Polynomials

Peter Blomgren
⟨blomgren.peter@gmail.com⟩

Department of Mathematics and Statistics
Dynamical Systems Group
Computational Sciences Research Center
San Diego State University
San Diego, CA 92182-7720

http://terminus.sdsu.edu/

Spring 2020

Outline

1. Student Learning Targets, and Objectives
   - SLOs: Polynomials
2. Polynomials :: Essentials
   - Complex Variables (Quick Review)
   - Uniqueness of Coefficients for Polynomials
   - Fundamental Theorem of Algebra and Polynomial Factorization
3. Problems, Homework, and Supplements
   - Suggested Problems
   - Assigned Homework
   - Supplements

Student Learning Targets, and Objectives

Target Division Algorithm for Polynomials

- **Objective** Know that the quotient-remainder form of division "looks essentially the same" for polynomial and scalars

Target Factorization of Polynomials over $\mathbb{C}$ and $\mathbb{R}$

- **Objective** Be able to identify, at least in the abstract, zeros and factors for polynomials
- **Objective** Understand how the structure of the polynomial factorization theorems over $\mathbb{C}$ and $\mathbb{R}$ differ, and the impact on the existence (or lack thereof) of real zeros for polynomials.

Introduction

We need some polynomial properties in order to effectively discuss and understand operators.

This is a quick overview of properties and results, many of which we have seen in other contexts.

We consider polynomials in real and/or complex variables; so as usual $\mathbb{F} \in \{\mathbb{C}, \mathbb{R}\}$.

We start off with some additional notation relating to complex numbers.

Complex Conjugate and Absolute Value

Definition (Notation — $\mathrm{Re}(z)$, $\mathrm{Im}(z)$)

For $z \in \mathbb{C}$, $z = a + bi$, $a, b \in \mathbb{R}$

- The **real part** of z, denoted $\mathrm{Re}(z)$, is defined by $\mathrm{Re}(z) = a$
- The **imaginary part** of z, denoted $\mathrm{Im}(z)$, is defined by $\mathrm{Im}(z) = b$

Definition (Complex Conjugate z^* (or $\overline{z}$), absolute value (or magnitude) $|z|$)

For $z \in \mathbb{C}$,

- The **complex conjugate** is defined by $z^* = \mathrm{Re}(z) - \mathrm{Im}(z)\, i$
- The **magnitude** of z is defined by $|z| = \sqrt{(\mathrm{Re}(z))^2 + (\mathrm{Im}(z))^2}$

Properties of Complex Numbers

Theorem (Properties of Complex Numbers)

Let $w, z \in \mathbb{C}$, *then:*

- $z + z^* = 2\mathrm{Re}(z)$
- $z - z^* = 2(\mathrm{Im}(z))i$
- $zz^* = |z|^2 = (\mathrm{Re}(z))^2 + (\mathrm{Im}(z))^2$
- $(w + z)^* = w^* + z^*$, *and* $(wz)^* = w^* z^*$
- $(z^*)^* = z$
- $|\mathrm{Re}(z)| \leq |z|$, *and* $|\mathrm{Im}(z)| \leq |z|$
- $|z^*| = |z|$
- $|wz| = |w|\,|z|$
- $|w + z| \leq |w| + |z|$

Uniqueness of Coefficients for Polynomials

$p : \mathbb{F} \mapsto \mathbb{F}$ is called a polynomial $p \in \mathcal{P}(\mathbb{F})$ with coefficients in $\mathbb{F}$ is there exists $a_0, a_1, \ldots, a_m \in \mathbb{F}$:

$$p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m$$

$\forall z \in \mathbb{F}$. If $a_m \neq 0$, then $\deg(p) = m$.

Theorem (If a Polynomial is the Zero Function, then all Coefficients are 0)

Suppose $a_0, a_1, \ldots, a_m \in \mathbb{F}$, *if*

$$a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m = 0, \quad \forall z \in \mathbb{F}$$

then $a_0 = a_1 = \cdots = a_m = 0$.

The zero-polynomial has $\deg(p) = -\infty$

Uniqueness of Coefficients for Polynomials

Theorem (Theorem $\Rightarrow$ Unique Coefficients)

The coefficients of a polynomial are **uniquely determined**.

If a polynomial had two different sets of coefficients, then subtracting the two representations of the polynomial would give a contradiction to the previous theorem.

Another way of stating the same thing is to say that $\{1, z, \ldots, z^m\}$ is a basis for $\mathcal{P}_m(\mathbb{F})$:

Basis

$\Rightarrow$ linear independence

$\Rightarrow$ only linear combination to equal 0 has all zero coefficients.

The Division Algorithm for Polynomials

If $p, s \in \mathbb{Z}^+$, $s \neq 0$, then there exist $q, r \in \mathbb{Z}^+ : p = sq + r$, and $r < s$. ([QUOTIENT-REMAINDER THEOREM] w/o all the details)

The analogous result for polynomials:

Theorem (Division Algorithm for Polynomials)

Suppose $p, s \in \mathcal{P}(\mathbb{F})$, with $s \neq 0$. The $\exists! q, r \in \mathcal{P}(\mathbb{F})$: $p = sq + r$, and $\deg(r) < \deg(s)$.

We can use some of our linear map "tools" to prove the result... which makes it worth doing.

Proof :: Division Algorithm for Polynomials

Proof (Division Algorithm for Polynomials)

Let $n = \deg(p)$ and $m = \deg(s)$. If $n < m$, then take $q = 0$ and $r = p$ to get the desired result. Thus we can assume that $n \geq m$.

Uniqueness — Let $T \in \mathcal{L}(\mathcal{P}_{n-m}(\mathbb{F}) \times \mathcal{P}_{m-1}(\mathbb{F}), \mathcal{P}_n(\mathbb{F}))$ be defined by:
$T(\,(q,r)\,) = sq + r$, If $(q,r) \in \mathrm{null}(T)$, then $sq + r = 0$
$\Rightarrow (q = 0, r = 0)$. (If not, then $\deg(sq) \geq m \Rightarrow sq \neq -r$.)
Thus $\dim(\mathrm{null}(T)) = 0$. $\surd$

Existence — We know

$$\begin{aligned} \dim(\mathcal{P}_{n-m}(\mathbb{F}) \times \mathcal{P}_{m-1}(\mathbb{F})) &= \dim(\mathcal{P}_{n-m}(\mathbb{F})) + \dim(\mathcal{P}_{m-1}(\mathbb{F})) \\ &= (n-m+1) + (m-1+1) = (n+1) \end{aligned}$$

With help from [The Fundamental Theorem of Linear Maps] it now follows that $\dim(\mathrm{range}(T)) = (n+1)$, and $(n+1) = \dim(\mathcal{P}_n(\mathbb{F}))$, therefore $\mathrm{range}(T) = \mathcal{P}_n(\mathbb{F})$; and we have existence of $q \in \mathcal{P}_{n-m}(\mathbb{F})$, and $r \in \mathcal{P}_{m-1}(\mathbb{F})$ so that $p = T(q,r) = sq + r$. $\surd$

Zeros of Polynomials

Definition (Zero of a Polynomial)

A scalar $\lambda \in \mathbb{F}$ is called a **zero** (or **root**) is a polynomial $p \in \mathcal{P}(\mathbb{F})$, if $p(\lambda) = 0$.

Definition (Factor)

A polynomial $s \in \mathcal{P}(\mathbb{F})$ is called a **factor** of $p \in \mathcal{P}(\mathbb{F})$, if $\exists\ q \in \mathcal{P}(\mathbb{F})$ such that $p = sq$.

Theorem (Each Zero of a Polynomial Corresponds to a Degree-1 Factor)

Suppose $p \in \mathcal{P}(\mathbb{F})$ and $\lambda \in \mathbb{F}$. Then $p(\lambda) = 0$ if and only if $\exists q \in \mathcal{P}(\mathbb{F})$:

$$p(z) = (z - \lambda)q(z),\ \forall z \in \mathbb{F}.$$

The proof is a simple application of the Division Algorithm.

Zeros of Polynomials

Theorem (A Polynomial Has At Most As Many Zeros As Its Degree)

Suppose $p \in \mathcal{P}(\mathbb{F})$, with $\deg(P) \geq 0$. Then p has at most m distinct zeros in $\mathbb{F}$.

The proof gives us an excuse to use mathematical induction!

Proof (A Polynomial Has At Most As Many Zeros As Its Degree)

$\mathbf{m = 0}$: $p(z) = a_0 \neq 0$, which has no zeros. $\surd$

$\mathbf{m = 1}$: $p(z) = a_0 + a_1 z$, $a_1 \neq 0$; $\lambda = -a_0/a_1$ is the one zero.

$\mathbf{m > 1}$: Assume the theorem is true $\forall q \in \mathcal{P}_{m-1}(\mathbb{F})$. Let $p \in \mathcal{P}_m(\mathbb{F})$, if p has a zero $\lambda \in \mathbb{F}$, then (previous theorem) $\exists q \in \mathcal{P}_{m-1}(\mathbb{F})$:

$$p(z) = (z - \lambda) q(z), \ \forall z \in \mathbb{F}.$$

$\deg(q) = (m-1)$. We have: $\{\text{zeros of } p\} = \{\lambda\} \cup \{\text{zeros of } q\}$.
$\#\text{zeros}(p) = 1 + \#\text{zeros}(q) \leq 1 + (m-1) = m$. $\surd$

Fundamental Theorem of Algebra

Theorem (Fundamental Theorem of Algebra)

Every non-constant polynomial with complex coefficients has a zero.

For a proof, see a course on Complex Analysis *(e.g.* [MATH 532]*)*.

Whereas there are formulas for the roots of polynomials of degrees 2, 3, and 4; the Abel-Ruffini theorem states

Theorem (Abel-Ruffini Theorem)

There is no algebraic solution — that is, solution in radicals — to the general polynomial equations of degree five or higher with arbitrary coefficients.

The theorem is named after Paolo Ruffini, who provided an incomplete proof in 1799, and Niels Henrik Abel, who provided a proof in 1824. (Galois later proved more general statements, and provided a construction of a polynomial of degree 5 whose roots cannot be expressed in radicals from its coefficients.)

Factorization of a Polynomials Over $\mathbb{C}$

Theorem (Factorization of a Polynomial Over $\mathbb{C}$)

If $p \in \mathcal{P}(\mathbb{F})$ is a non-constant polynomial, then p has a unique factorization (except for the order to the factors, which does not matter, due to the commutativity of multiplication of complex numbers) of the form:

$$p(z) = c(z - \lambda_1) \dots (z - \lambda_m)$$

where $c, \lambda_1, \dots, \lambda_m \in \mathbb{C}$.

The proof relies on [THE FUNDAMENTAL THEOREM OF ALGEBRA], and mathematical induction... it does not provide any good excuses to exercise our linear algebra skills, so we skip it.

Factorization of a Polynomials Over $\mathbb{R}$

A polynomial with real coefficients may have no real zeros. For example, the polynomial $1 + x^2$ has no real zeros.

The failure of the Fundamental Theorem of Algebra over $\mathbb{R}$ accounts for the differences between operators on real and complex vector spaces.

(To be explored in (painful?) detail...)

Polynomials with Real Coefficients have Complex Zeros in Pairs

Theorem (Polynomials with Real Coefficients have Complex Zeros in Pairs)

Suppose $p \in \mathcal{P}(\mathbb{F})$ is a polynomial with real coefficients. If $\lambda \in \mathbb{C}$ is a zero of p, then so is z^*.

Proof (Polynomials with Real Coefficients have Complex Zeros in Pairs)

Let $p \in \mathcal{P}(\mathbb{F})$ be a polynomial with real coefficients, and $\lambda \in \mathbb{C}$ a zero of p, then:

$$\begin{aligned} \sum_{k=0}^{m} a_k \lambda^k &= 0 && \text{take the complex conjugate} \\ \sum_{k=0}^{m} a_k (\lambda^*)^k &= 0 && \text{and there it is! } \surd \end{aligned}$$

Factorization of a Polynomial Over $\mathbb{R}$

Polynomial factorization over $\mathbb{R}$ is not nearly as pretty as factorization over $\mathbb{C}$:

Theorem (Factorization of a Polynomial Over $\mathbb{R}$)

Let $p \in \mathcal{P}(\mathbb{R})$ is a non-constant polynomial. Then p has a unique factorization of the form

$$p(x) = c(x-\lambda_1)\dots(x-\lambda_m)(x^2+b_1x+c_1)\dots(x^2+b_Mx+c_M)$$

where $c, \lambda_1, \dots, \lambda_m, b_1, \dots, b_M, c_1, \dots, c_M \in \mathbb{R}$, with $b_k^2 < 4c_k$ $k = 1, \dots, M$.

Theorem (Factorization of a Polynomial Over $\mathbb{C}$)

If $p \in \mathcal{P}(\mathbb{F})$ is a non-constant polynomial, then p has a unique factorization of the form

$$p(z) = c(z-\lambda_1)\dots(z-\lambda_m)$$

where $c, \lambda_1, \dots, \lambda_m \in \mathbb{C}$.

$\langle\langle\langle$ Live Math $\rangle\rangle\rangle$

e.g. 4-$\{5^{@}, 8, 11^{+}\}$

Suggested Problems

4—2, 3, 5$^{@}$, 8, 11^{+}

These problems have a strong linear algebra "flavor," the rest deal more with polynomial / complex arithmetic properties.

$^{@}$-marked problem are really good, but may be just a bit too much for homework

$^{+}$-marked problems have longer/more challenging solutions.

Assigned Homework

HW#4, Due 3/6/2020, 12:00pm, GMCS-587

4—2, 3

Supplements

⟨PLACEHOLDER⟩