Polynomials

Lecture 12

Dept. of Math., SUSTech

2023.03

Polynomials

Introduction

- This short chapter contains material on polynomials that we will need to understand operators.
- Many of the results in this chapter will already be familiar to you from other courses.
- They are included here for completeness.
- Division Algorithm for Polynomials.
- Factorization of polynomials over $\mathbb{C}$.
- Factorization of polynomials over $\mathbb{R}$.

Complex Conjugate and Absolute Value

Before discussing polynomials with complex or real coefficients, we need to learn a bit more about the complex numbers.

$z = a + bi$

$\overline{z} = a - bi$

4.2 Definition $\operatorname{Re} z$, $\operatorname{Im} z$

Suppose $z = a + bi$, where a and b are real numbers.

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

Thus for every complex number z, we have

$$z = \operatorname{Re} z + (\operatorname{Im} z)i$$

Complex Conjugate

4.3 Definition ***complex conjugate,*** $\bar{z}$***, absolute value,*** $|z|$

Suppose $z \in \mathbf{C}$.

- The ***complex conjugate*** of $z \in \mathbf{C}$, denoted $\bar{z}$, is defined by

$$\bar{z} = \operatorname{Re} z - (\operatorname{Im} z)i.$$

- The ***absolute value*** of a complex number z, denoted $|z|$, is defined by

$$|z| = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2}.$$

Note that $|z|$ is a nonnegative number for every $z \in \mathbb{C}$. The real and imaginary parts, complex conjugate, and absolute value have the following properties:

Properties of Complex Numbers

4.5 Properties of complex numbers

Suppose $w, z \in \mathbf{C}$. Then

sum of z and $\bar{z}$

$$z + \bar{z} = 2 \operatorname{Re} z;$$

difference of z and $\bar{z}$

$$z - \bar{z} = 2(\operatorname{Im} z)i;$$

product of z and $\bar{z}$

$$z\bar{z} = |z|^2;$$

additivity and multiplicativity of complex conjugate

$$\overline{w + z} = \bar{w} + \bar{z} \text{ and } \overline{wz} = \bar{w}\bar{z};$$

conjugate of conjugate

$$\bar{\bar{z}} = z;$$

Properties of Complex Numbers

real and imaginary parts are bounded by $|z|$

$$|\operatorname{Re} z| \le |z| \text{ and } |\operatorname{Im} z| \le |z|$$

absolute value of the complex conjugate

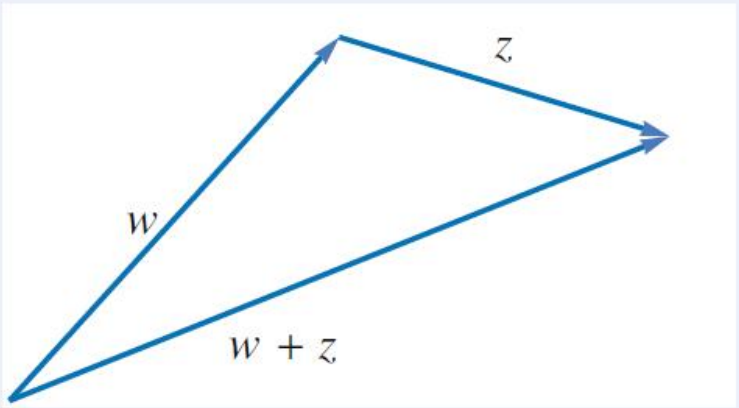
$$|\bar{z}| = |z|;$$

multiplicativity of absolute value

$$|wz| = |w|\,|z|;$$

Triangle Inequality

$$|w + z| \le |w| + |z|.$$



The routine verifications of the assertions above are left to the reader.

Uniqueness of Coefficients for Polynomials

Recall that a function $p : \mathbb{F} \to \mathbb{F}$ is called a polynomial with coefficients in $\mathbb{F}$ if there exists $a_0, \cdots, a_m \in \mathbb{F}$ such that

$p \in \mathbb{F}^{\mathbb{F}}$

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

for all $z \in \mathbb{F}$.

$p(z) = b_0 + b_1 z + \cdots + b_m z^m$

$\Rightarrow 0 = (a_0 - b_0) + (a_1 - b_1) z + \cdots + (a_m - b_m) z^m.$

4.7 If a polynomial is the zero function, then all coefficients are 0

Suppose $a_0, \ldots, a_m \in \mathbf{F}$. If

$$a_0 + a_1 z + \cdots + a_m z^m = 0$$

for every $z \in \mathbf{F}$, then $a_0 = \cdots = a_m = 0$.

Zero polynomial

Remarks

The result above implies that the coefficients of a polynomial are uniquely determined (because if a polynomial had two sets of coefficients, then subtracting the two representations of the polynomial would give a contradiction to the result above).

Proof

Proof.

We will prove the contrapositive. If not all the coefficients are 0, then by changing m we can assume $a_m \neq 0$. Let

$$z = \frac{|a_0| + |a_1| + \cdots + |a_{m-1}|}{|a_m|} + 1.$$

Note that $|z| \geqslant 1$, and thus $z^j \leq z^{m-1}$ for $j = 0, 1, 2, \cdots, m-1$. Using Triangular Inequality, we have

$$|a_0 + a_1 z + \cdots + a_{m-1} z^{m-1}| \leq (|a_0| + |a_1| + \cdots + |a_{m-1}|) z^{m-1} < |a_m z^m|.$$

$< (|a_0| + |a_1| + \cdots + |a_{m-1}| + |a_m|) z^{m-1}$

Thus $a_0 + a_1 z + \cdots + a_{m-1} z^{m-1} \neq -a_m z^m$. Hence we conclude that $a_0 + a_1 z + \cdots + a_{m-1} z^{m-1} + a_m z^m \neq 0$. □

The Division Algorithm for Polynomials (带余除法)

If p and s are nonnegative integers, with $s \neq 0$, then there exist nonnegative integers q and r such that $p = sq + r$ and $r < s$. Think of dividing p by s, getting quotient q with remainder r. Our next task is to prove an analogous result for polynomials.

$p, s \in \mathcal{P}(\mathbb{F})$ $s \neq 0$

$p = sq + r$ $\deg p = n$ $\deg s = m$

$\deg q = n - m$.

4.8 Division Algorithm for Polynomials

Suppose that $p, s \in \mathcal{P}(\mathbf{F})$, with $s \neq 0$. Then there exist unique polynomials $q, r \in \mathcal{P}(\mathbf{F})$ such that

$$p = sq + r$$

and $\deg r < \deg s$.

$T(q, r) = sq + r$

$T: \mathcal{P}_{n-m}(\mathbb{F}) \times \mathcal{P}_m(\mathbb{F}) \to \mathcal{P}_n(\mathbb{F})$

$(q, r) \longmapsto sq + r = p$

This result can be proved without linear algebra, but the proof given here using linear algebra is appropriate for a linear algebra textbook.

Proof

Proof.

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 $n \geq m$.

Define $T : \mathscr{P}_{n-m}(\mathbb{F}) \times \mathscr{P}_{m-1}(\mathbb{F}) \to \mathscr{P}_n(\mathbb{F})$ by **T(q,r)=sq+r.** The reader can easily verify that T is a linear map. If $(q, r) \in \text{null } T$, then $sq + r = 0$, which implies that $q = 0$ and $r = 0$. Thus $\dim \text{null } T = 0$.

From 3.76 we have

$$\dim(\mathscr{P}_{n-m}(\mathbb{F}) \times \mathscr{P}_{m-1}(\mathbb{F})) = (n-m+1)+(m-1+1) = n+1.$$

The Fundamental Theorem of Linear Maps and the equation displayed above now imply that $\dim \text{range } T = n+1$, which equals $\dim \mathscr{P}_n(\mathbb{F})$. Thus range $T = \mathscr{P}_n(\mathbb{F})$, and hence there exist $q \in \mathscr{P}_{n-m}(\mathbb{F})$ and $r \in \mathscr{P}_{m-1}(\mathbb{F})$ such that $p = T(q, r) = sq + r$. □

Zeros of Polynomials

The solutions to the equation $p(z) = 0$ play a crucial role in the study of a polynomial $p \in \mathscr{P}(\mathbb{F})$. Thus these solutions have a special name.

4.9 Definition ***zero of a polynomial***

A number $\lambda \in \mathbf{F}$ is called a ***zero*** (or ***root***) of a polynomial $p \in \mathcal{P}(\mathbf{F})$ if

$$p(\lambda) = 0.$$

4.10 Definition ***factor***

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

We begin by showing that λ is a zero of a polynomial of $p \in \mathscr{L}(\mathbb{F})$ if and only if $z - \lambda$ is a factor of p.

Each zero of a polynomial corresponds to a degree-1 factor

4.11 Each zero of a polynomial corresponds to a degree-1 factor

Suppose $p \in \mathcal{P}(\mathbf{F})$ and $\lambda \in \mathbf{F}$. Then $p(\lambda) = 0$ if and only if there is a polynomial $q \in \mathcal{P}(\mathbf{F})$ such that

$$p(z) = (z - \lambda)q(z)$$

for every $z \in \mathbf{F}$.

Polynomials do not have too many zeros.

4.12 A polynomial has at most as many zeros as its degree

Suppose $p \in \mathcal{P}(\mathbf{F})$ is a polynomial with degree $m \geq 0$. Then p has at most m distinct zeros in $\mathbf{F}$.

Proof

Proof If $m = 0$, then $p(z) = a_0 \neq 0$ and so p has no zeros.

If $m = 1$, then $p(z) = a_0 + a_1 z$, with $a_1 \neq 0$, and thus p has exactly one zero, namely, $-a_0/a_1$.

Now suppose $m > 1$. We use induction on m, assuming that every polynomial with degree $m - 1$ has at most $m - 1$ distinct zeros. If p has no zeros in $\mathbf{F}$, then we are done. If p has a zero $\lambda \in \mathbf{F}$, then by 4.11 there is a polynomial q such that

$$p(z) = (z - \lambda)q(z)$$

for all $z \in \mathbf{F}$. Clearly $\deg q = m - 1$. The equation above shows that if $p(z) = 0$, then either $z = \lambda$ or $q(z) = 0$. In other words, the zeros of p consist of λ and the zeros of q. By our induction hypothesis, q has at most $m - 1$ distinct zeros in $\mathbf{F}$. Thus p has at most m distinct zeros in $\mathbf{F}$. ■

Fundamental Theorem of Algebra

The next result, although called the Fundamental Theorem of Algebra, uses analysis in its proof. The short proof presented here uses tools from complex analysis. If you have not had a course in complex analysis, this proof will almost certainly be meaningless to you.

4.13 Fundamental Theorem of Algebra

Every nonconstant polynomial with complex coefficients has a zero.

Proof Let p be a nonconstant polynomial with complex coefficients. Suppose p has no zeros. Then $1/p$ is an analytic function on $\mathbf{C}$. Furthermore, $|p(z)| \to \infty$ as $|z| \to \infty$, which implies that $1/p \to 0$ as $|z| \to \infty$. Thus $1/p$ is a bounded analytic function on $\mathbf{C}$. By Liouville's theorem, every such function is constant. But if $1/p$ is constant, then p is constant, contradicting our assumption that p is nonconstant. ■

Factorization of Polynomials over $\mathbb{C}$

So far we have been handling polynomials with complex coefficients and polynomials with real coefficients simultaneously through our convection that $\mathbb{F}$ denotes $\mathbb{R}$ or $\mathbb{C}$. Now we will see some differences between these two cases.

4.14 Factorization of a polynomial over $\mathbf{C}$

If $p \in \mathcal{P}(\mathbf{C})$ is a nonconstant polynomial, then p has a unique factorization (except for the order of the factors) of the form

$$p(z) = c(z - \lambda_1) \cdots (z - \lambda_m),$$

where $c, \lambda_1, \ldots, \lambda_m \in \mathbf{C}$.

Proof. existence → P125.

Induction+Uniqueness. □

Factorization of Polynomials over $\mathbb{R}$

4.15 Polynomials with real coefficients have zeros in pairs

Suppose $p \in \mathcal{P}(\mathbf{C})$ is a polynomial with real coefficients. If $\lambda \in \mathbf{C}$ is a zero of p, then so is $\bar{\lambda}$.

Proof Let

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

where $a_0, \ldots, a_m$ are real numbers. Suppose $\lambda \in \mathbf{C}$ is a zero of p. Then

$$a_0 + a_1 \lambda + \cdots + a_m \lambda^m = 0.$$

Take the complex conjugate of both sides of this equation, obtaining

$$a_0 + a_1 \bar{\lambda} + \cdots + a_m \bar{\lambda}^m = 0,$$

where we have used basic properties of complex conjugation (see 4.5). The equation above shows that $\bar{\lambda}$ is a zero of p. ■

Factorization of a Quadratic Polynomial

We want a factorization theorem for polynomials with real coefficients. First we need to characterize the polynomials of degree 2 with real coefficients that can be written as the product of two polynomials of degree 1 with real coefficients.

4.16 Factorization of a quadratic polynomial

Suppose $b, c \in \mathbf{R}$. Then there is a polynomial factorization of the form

$$x^2 + bx + c = (x - \lambda_1)(x - \lambda_2)$$

with $\lambda_1, \lambda_2 \in \mathbf{R}$ if and only if $b^2 \geq 4c$.

Proof.

Completing the square. □

Factorization of Polynomials over $\mathbb{R}$

In the next result, either m or M may equal 0. The numbers $\lambda_1, \cdots, \lambda_m$ are precisely the real zeros of p, for these are the only real values of x for which the right side of the equation in the next result equals 0.

Factorization of Polynomials over $\mathbb{R}$:

4.17 Factorization of a polynomial over $\mathbf{R}$

Suppose $p \in \mathcal{P}(\mathbf{R})$ is a nonconstant polynomial. Then p has a unique factorization (except for the order of the factors) of the form

$$p(x) = c(x - \lambda_1) \cdots (x - \lambda_m)(x^2 + b_1 x + c_1) \cdots (x^2 + b_M x + c_M),$$

where $c, \lambda_1, \ldots, \lambda_m, b_1, \ldots, b_M, c_1, \ldots, c_M \in \mathbf{R}$, with $b_j^2 < 4c_j$ for each j.

一些有趣的结论

Theorem

对于 $\mathscr{P}(\mathbb{F})$ 中的任意两个多项式 $f(x)$ 和 $g(x)$, 在 $\mathscr{P}(\mathbb{F})$ 中存在一个最大公因子 $d(x)=(f(x),g(x))$, 且 $d(x)$ 可以表示为 $f(x)$ 和 $g(x)$ 的一个组合, 即有 $\mathscr{P}(\mathbb{F})$ 中的多项式 $u(x),v(x)$ 使

$$d(x)=u(x)f(x)+v(x)g(x).$$

该定理可以用辗转相除法证明. $\mathscr{P}(\mathbb{F})$ 中的多项式 $f(x),g(x)$ 称为互素(也称为互质)的, 如果 $(f(x),g(x))=1$.

Theorem

$\mathscr{P}(\mathbb{F})$ 中的任意两个多项式 $f(x)$ 和 $g(x)$ 互素的充分必要条件是有 $\mathscr{P}(\mathbb{F})$ 中的多项式 $u(x),v(x)$ 使

$$u(x)f(x)+v(x)g(x)=1.$$

一个例子

Example

设

$$f(x) = x^4 + 3x^3 - x^2 - 4x - 3,$$
$$g(x) = 3x^3 + 10x^2 + 2x - 3.$$

求 $(f(x), g(x))$, 并求 $u(x), v(x)$ 使

$$(f(x), g(x)) = u(x)f(x) + v(x)g(x).$$

Solution.

$$(f(x), g(x)) = x + 3,\ u(x) = \frac{3}{5}x - 1,\ v(x) = -\frac{1}{5}x^2 + \frac{2}{5}x.$$

有理系数多项式

下面介绍关于有理数域上一元多项式的一些结论.

Theorem

设

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

是一个整系数多项式, 而 $\frac{r}{s}$ 是它的一个有理根, 其中 r, s 互素, 那么必有 $s|a_n$, $r|a_0$. 特别地, 如果 $f(x)$ 的首项系数 $a_n = 1$, 那么 $f(x)$ 的有理根都是整根, 而且是 a_0 的因子.

艾森斯坦(Eisenstein) 判别法

Theorem

*(艾森斯坦(Eisenstein) 判别法)*设

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

是一个整系数多项式, 如果有一个素数 p, 使得

$$(1)\ p \nmid a_n,$$
$$(2)\ p \mid a_{n-1}, a_{n-2}, \cdots, a_0,$$
$$(3)\ p^2 \nmid a_0,$$

那么 $f(x)$ 在有理数上是不可约的.

Homework Assignment 12

Chapter 4: 3, 4, 5, 6, 7, 8, 9, 11.