Section 2.3: Polynomial Rings

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 8510, Abstract Algebra I

Overview: why we need to formalize polynomials

We all know "what a polynomial is", but how do we formalize such an object?

Here is a partial list of potential pitfalls, from things that "should be true that aren't", to flawed proof techniques.

Over $\mathbb{H}$, the degree-2 polyomial $f(x) = x^2 + 1$ has 6 roots: $\pm i, \pm j, \pm k$.

What does it means to plug an $n \times n$ matrix into a polynomial? For example,

$$f(x, y) = (x + y)^2 = x^2 + 2xy + y^2,$$
$$f(A, B) = (A + B)^2 = A^2 + AB + BA + B^2 \neq A^2 + 2AB + B^2.$$

Cayley-Hamilton theorem

Every $n \times n$ matrix satisfies its characteristic polynomial, i.e., $p_A(A) = 0$.

Flawed proof

Since $p_A(\lambda) = \det(A - \lambda I)$, just plug in $\lambda = A$:

$$p_A(A) = \det(A - AI) = \det(A - A) = \det 0 = 0.$$

Single variable polynomials

Intuitive informal definition

Let R be a ring. A polynomial in one variable over R is

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \qquad a_i \in R.$$

Here, x is a "variable" that can be assigned values from R or a subring $S \subset R$.

Let $P(R)$ be the set of sequences over R, where all but finitely many entries are 0. We write

$$a = (a_i) = (a_0, a_1, a_2, \dots), \qquad a_i \in R.$$

If $a, b \in P(R)$, define operations:

$$a + b = (a_i + b_i)$$

$$ab = \Big(\sum_{j=0}^{i} a_j b_{i-j}\Big) = (a_0 b_0,\ a_0 b_1 + a_1 b_0,\ a_0 b_2 + a_1 b_1 + a_2 b_0,\ \dots)$$

Proposition (exercise)

If R is a ring, then $P(R)$ is a ring. It is commutative iff R is, and it has 1 iff R does, in which case $1_{P(R)} = (1_R, 0, 0, \dots)$.

Single variable polynomials

Let R be a ring with 1, and set $x = (0, 1, 0, 0, \dots) \in P(R)$.

Note: $x^2 = (0, 0, 1, 0, 0, \dots)$, $x^3 = (0, 0, 0, 1, 0, \dots) \in P(R)$, etc.

Set $x^0 := 1_{P(R)}$. The map

$$R \longrightarrow P(R), \qquad a \longmapsto (a, 0, 0, \dots)$$

is 1–1, so we may identify R with a subring of $P(R)$, with $1_R = 1_{P(R)}$. Now, we may write

$$a = (a_0, a_1, a_2, \dots) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

for each $a \in P(R)$.

We call x an indeterminate, and write $R[x] = P(R)$.

Write $f(x)$ for $a \in R[x]$, called a polynomial with coefficients in R. If $a_n \neq 0$ but $a_m = 0$ for all $m > n$, say $f(x)$ has degree n, and leading coefficient a_n.

If $f(x)$ has leading coefficient 1, it is monic. The zero polynomial $0 := (0, 0, \dots)$ has degree $-\infty$. Polynomials of non-positive degree are constants.

Single variable polynomials

Proposition

Let R be a ring with 1, and $f, g \in R[x]$. Then

1. $\deg(f(x)+g(x)) \leq \max\{\deg f(x), \deg g(x)\}$, and
2. $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$.

Moreover, equality holds in (b) if R has no zero divisors.

Corollary 1

If R has no zero divisors, then $f(x) \in R[x]$ is a unit iff $f(x) = r$ with $r \in U(R)$.

Corollary 2

$R[x]$ is an integral domain iff R is an integral domain.

Theorem (division algorithm)

Suppose R is commutative with 1 and $f, g \in R[x]$. If $g(x)$ has leading coefficient b, then there exists $k \geq 0$ and $q(x), r(x) \in R[x]$ such that

$$b^k f(x) = q(x)g(x) + r(x), \qquad \deg r(x) < \deg g(x).$$

If b is not a zero divisor in R, then $q(x)$ and $r(x)$ are unique. If $b \in U(R)$, we may take $k = 0$.

The polynomials $q(x)$ and $r(x)$ are called the quotient and remainder.

Proof (details done on board)

Non-trival case: $\deg f(x) = m \geq \deg g(x) = n$.

Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$, $g(x) = b_0 + \cdots + b_n x^n$, (let $a = a_m$, $b = b_n$).

We induct on m, with the degree $< m$ polynomial $f_1(x) := bf(x) - ax^{m-n}g(x)$.

Write $b^{k-1} f_1(x) = p(x)g(x) + r(x)$, and plug into $b^k f(x) = b^{k-1} \cdot bf(x)$. $\square$

The division algorithm also holds when R is not commutative, as long as b is a unit.

Substitution

Henceforth, R and S are assumed to be commutative with 1.

Theorem

Suppose $\theta\colon R \to S$ is a homomorphism with $\theta(1_R) = 1_S$ and $a \in S$. Then there exists a unique evaluation map $E_a\colon R[x] \to S$ such that

(i) $E_a(r) = \theta(r)$, for all $r \in R$,

(ii) $E_a(x) = a$.

Though θ need not be 1–1, it is usually the canonical inclusion. In this case,

$$E_a(f(x)) = r_0 + r_1 a + \cdots + r_n a^n,$$

which we call $f(a)$. The image of E_a is $R[a] = \{f(a) \mid f(x) \in R[x]\}$.

Remainder theorem

Suppose R is commutative with unity, $f(x) \in R[x]$, and $a \in R$. Then the remainder of $f(x)$ divided by $g(x) = x - a$ is $r = f(a)$.

Proof

Write $f(x) = q(x)(x - a) + r$, and substitute a for x. □

Algebraic and transcendental elements

Corollary: Factor theorem

Suppose R is commutative with unity, $f(x) \in R[x]$, $a \in R$, and $f(a) = 0$. Then $x - a$ is a factor of $f(x)$, i.e., $f(x) = q(x)(x-a)$ for some $q(x) \in R[x]$.

Note that this *fails* if:

- R is not commutative: recall $f(x) = x^2 + 1$ in $\mathbb{H}[x]$.
- R does not have 1: consider $2x^2 + 4x + 2$ in $2\mathbb{Z}[x]$.

Definition

If $R \subseteq S$ with $1_R = 1_S$, then $a \in S$ is algebraic over R if $f(a) = 0$ for some nonzero $f(x) \in R[x]$, and transcendental otherwise.

Remark

$a \in S$ is algebraic over R iff E_a is not 1–1.

Polynomials in several indeterminates

Let $I = \{0, 1, 2, 3, \dots, \}$ and $I^n = I \times \cdots \times I$ (n copies).

Informally, think of element of I^n as "exponent vectors" of monomials, e.g.,

$$(0,3,4) \text{ corresponds to } x_1^0 x_2^3 x_3^4.$$

Write 0 for $(0, \dots, 0) \in I^n$. Addition on I^n is defined component-wise.

Over a fixed ring R, polynomials can be encoded as functions

$$P_n(R) = \{a \colon I^n \to R \mid a(x) = 0 \text{ all but finitely many } x \in I^n\}$$

Note that elements in $P_n(R)$ specify the coefficients of monomials, e.g.,

$$a(0,3,4) = -6 \quad \text{corresponds to } \; -6x_1^0 x_2^3 x_3^4.$$

For example, in $\mathbb{Z}[x_1, x_2, x_3]$, the polynomial $f(x_1, x_2, x_3) = -6x_1^0 x_2^3 x_3^4 + 12x_1^5 - 9$ is

$$a(i_1, i_2, i_3) = \begin{cases} -6 & (i_1, i_2, i_3) = (0,3,4) \\ 12 & (i_1, i_2, i_3) = (5,0,0) \\ -9 & (i_1, i_2, i_3) = (0,0,0) \\ 0 & \text{otherwise.} \end{cases}$$

Polynomials in several indeterminates

Functions in $P_n(R)$ are added componentwise, and multiplied as

$$(ab)(i) := \sum \big\{ a(j)b(k) \mid j,k \in I^n,\ j+k=i \big\}, \qquad a,b \in P_n(R), \quad i \in I^n.$$

The following is straightforward but tedious.

Proposition

$P_n(R)$ is a ring. It is commutative iff R is, and has 1 iff R does.

Each $r \in R$ defines a constant polynomial via a function $a_r \in P_n(R)$, where

$$a_1 \colon I^n \longrightarrow R, \qquad a_r(i) = \begin{cases} r & i = (0,\dots,0) \\ 0 & \text{otherwise.} \end{cases}$$

Note that the identity function is $1 := a_1 \in P_n(R)$.

It is easy to check that $a_r + a_s = a_{r+s}$ and $a_r a_s = a_{rs}$, and so the map

$$R \longrightarrow P_n(R), \qquad r \longmapsto a_r$$

is 1–1. As such, we may identify r with $a_r \in P_n(R)$ and view R as a subring of $P_n(R)$.

Polynomials in several indeterminates

If R has 1, then let

$$e_k := (0, 0, \dots, 0, \underbrace{1}_{\text{pos. } i}, 0, \dots, 0) \in I^n.$$

Define the indeterminates $x_k \in P_n(R)$ as

$$x_k(i) = \begin{cases} 1 & i = e_k \\ 0 & \text{otherwise.} \end{cases}$$

Often, if $n = 2$ or 3, we use $x = x_1$, $y = x_2$, $z = x_3$, etc.

Note that

$$x_k^2(i) = \begin{cases} 1 & i = 2e_k \\ 0 & \text{otherwise,} \end{cases} \qquad x_k^m(i) = \begin{cases} 1 & i = me_k \\ 0 & \text{otherwise.} \end{cases}$$

(Secretly: $(1, 0, \dots, 0) \mapsto x_1^1 x_2^0 \cdots x_n^0 = x_1$ and $(m, 0, \dots, 0) \mapsto x_1^m x_2^0 \cdots x_n^0 = x_1^m$.)

It is easy to check that $x_i x_j = x_j x_i$ (i.e., these commute as functions $I^n \to R$).

Every $a \in P_n(R)$ can be written uniquely using functions with one-point support, which are called monomials.

Polynomials in several indeterminates

The degree of $a = rx_1^{i_1} \cdots x_n^{i_n}$ is $\deg a = i_1 + \cdots + i_n$.

If a is a sum of monomials, then say $\deg = \max\{\deg a_i \mid 1 \leq i \leq m\}$.

Also, say that $\deg 0 = -\infty$, and if all a_i's have the same degree, then $a \in P_n(R)$ is homogeneous.

The elements of $P_n(R)$ are called polynomials in the n commuting indeterminates $x_1, \dots, x_n$.

We write $R[x_1, \dots, x_n]$ for $P_n(R)$ and denotes elements by $f(x_1, \dots, x_n)$, etc.

Often we write $x := (x_1, \dots, x_n)$ and $f(x) := f(x_1, \dots x_n)$.

Proposition

Let R be a ring with 1 and $f(x), g(x) \in R[x_1, \dots, x_n]$. Then

(a) $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$,

(b) $\deg(f(x)g(x)) \leq \deg f(x) \cdot \deg g(x)$.

Moreover, equality holds in (b) if R has no zero divisors.

Substitution for multivariable polynomials

Theorem

Suppose $\theta\colon R \to S$ is a homomorphism with $\theta(1_R) = 1_S$ and $a = (a_1, \dots, a_n) \in S^n$. Then there exists a unique evaluation map $E_a\colon R[x] \to S$ such that

(i) $E_a(r) = \theta(r)$, for all $r \in R$,

(ii) $E_a(x_i) = a_i$, for all $i = 1, \dots, n$.

Proof (sketch)

Define $E(rx_1^{i_1} \cdots x_n^{i_n}) = \theta(r)a_1^{i_1} \cdots a_n^{i_n}$ for monomials; extend naturally to polynomials.

Remarks

1. If θ is 1–1, then E_a "substitutes" elements from S in place of the x_i's, by

$$f(x_1, \dots, x_n) \stackrel{E_a}{\longmapsto} f(a_1, \dots, a_n).$$

2. This is easily extended to an arbitrary number of variables.
3. We could have defined $R[x_1, \dots, x_n]$ abstractly via a universal mapping property.
4. Another construction: Define $R[x_1, x_2] = (R[x_1])[x_2]$, etc.

Substitution for multivariable polynomials

Definition

Elements $a_1, \dots, a_n \in S$ are algebraically dependent over R if $f(a_1, \dots, a_n) = 0$ for some nonzero $f(x) \in R[x_1, \dots, x_n]$.

Otherwise, they are algebraically independent over R.

Examples

1. $a_1 = \sqrt{3}$, $a_2 = \sqrt{5}$ are algebraically dependent over $\mathbb{Z}$. Consider $f(x, y) = (x^2 - 3)(y^2 - 5)$.
2. $a_1 = \sqrt{\pi}$, $a_2 = 2\pi + 1$ are algebraically dependent over $\mathbb{Z}$. Consider $f(x, y) = 2x^2 - y + 1$.
3. It is "unknown" whether $a_1 = \pi$, $a_2 = e$ are algebraically dependent over $\mathbb{Z}$.

Remarks

1. $a \in S$ algebraically independent over $R \iff a$ transcendental over R.
2. $a_1, \dots, a_n \in S$ algebraically indep. over $R \implies a_1, \dots, a_n$ transcendental over R.

Hilbert's basis theorem

If a 0 exponent occurs in a monomial, we suppress writing the indeterminate.

For example, $5x_1^0x_2^1x_3^0x_4^8 = 5x_2x_4^8$. By doing this, we can consider

$$R[x_1] \subseteq R[x_1,x_2] \subseteq R[x_1,x_2,x_3] \subseteq \cdots$$

We write

$$R[x_1,x_2,x_3,\dots] = \bigcup_{i=1}^{\infty} R[x_1,\dots,x_k].$$

Not surprisingly, this ring has non-finitely generated ideals, e.g., $I = (x_1,x_2,\dots)$.

Perhaps surprisingly, this is *not* the case in $R[x_1,\dots,x_n]$.

Hilbert's basis theorem

Every ideal in $R[x_1,\dots,x_n]$ is finitely generated.

We will prove this in the next section. (It's more natural to do on the board.)