Lecture 8 — Polynomials, Part 1

Holden Lee

1/29/2011

1 What is a polynomial?

In this section, we will formally define polynomials. (As this is somewhat abstract, feel free to skip on first reading.) In general we will use R to denote a ring and K to denote a field; in later sections the reader may substitute K with either the rationals $\mathbb{Q}$, reals $\mathbb{R}$, or complex numbers $\mathbb{C}$ without too much loss in generality.

Before we can define a polynomial, we have to decide what coefficients we allow. Often we will just work with real numbers, but it is helpful to have the freedom to choose between $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ (integers modulo p), and so forth. The set of coefficients should form a ring, where addition and multiplication satisfy all the properties we expect them to. We need this before we can think of defining addition and multiplication for polynomials.

Definition 1.1: A **ring** is a set R with the operations of addition ($+$) and multiplication ($\times$) satisfying:

1. R is an abelian group under addition. That is, the following hold:
   (a) (Associativity) $(a+b)+c = a+(b+c)$.
   (b) (Commutativity) $a+b = b+a$.
   (c) (Additive identity) There exists an (unique) element 0 such that $a+0 = 0+a = a$ for any a.
   (d) (Additive inverse) For every a there exists an (unique) element $-a$ such that $a+(-a) = (-a)+a = 0$.
2. Multiplication satisfies similar properties, except the last:
   (a) (Associativity) $(ab)c = a(bc)$.
   (b) (Commutativity) $ab = ba$.
   (c) (Multiplicative identity) There exists an (unique) element 1 such that $1a = a1 = a$.
3. Multiplication distributes over addition; that is, $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$.

A **field** is a ring such that every nonzero element has a multiplicative inverse: if $a \neq 0$ then there exists an (unique) element a^{-1} such that $aa^{-1} = a^{-1}a = 1$.

Examples of fields are $\mathbb{C}, \mathbb{R}, \mathbb{Q}$, and $\mathbb{Z}/p\mathbb{Z}$. In later sections, unless otherwise specified, we will only consider polynomials over a field.

Now we can go ahead to define polynomials.

Definition 1.2: The **polynomial ring** $R[x]$ is the set of expressions of the form $\sum_{n=0}^{\infty} a_n x^n$ where $a_n \in R$ and only a finite number of a_n are nonzero. Addition is defined by adding corresponding terms and multiplication is defined using the distributive law (i.e. multiplying every term in the first polynomial by every term in the second, and adding up all the terms).

It is simple to verify that $R[x]$ is a ring (just check all the properties... the only one of much substance is associativity). By repeating this process we can get polynomials in multiple variables ($R[x, y] = R[x][y]$, etc.).

Often we think of polynomials as functions, that is we can evaluate the polynomial at any $x \in R$.

Proposition 1.3: (Substitution) Given any $t \in R$, there is a function $R[x] \to R$ that sends a polynomial $P(x) = \sum_{n=0}^{\infty} a_n x^n$ to its value at t, $\sum_{n=0}^{\infty} a_n t^n$. We call this value $P(t)$.

This extends in a straightforward manner to polynomials in more variables. A word of caution: two polynomials may give the same function, but are still different when considered as polynomials—because two polynomials are equal iff all their coefficients are equal. For example, we know from Fermat's Little Theorem that $x^p - x = 0$ for all $x \in \mathbb{Z}/p\mathbb{Z}$. Hence as functions, $x^p - x$ and 0 are indistinguishable. However they are not the same polynomial.

In abstract algebra, we often formulate Proposition 1.3 in the following way:

Proposition 1.4 (Universal Mapping Property)**:** $R[x_1, \ldots, x_n]$ is the unique ring, up to isomorphism, with the following property: Given $t_1, \ldots, t_n \in R$, there is a unique ring homomorphism from $R[x_1, \ldots, x_n]$ to R sending x_i to t_i.

(A ring homomorphism φ is a function which preserves addition, multiplication and 1, i.e. $\varphi(a + b) = \varphi(a) + \varphi(b), \varphi(ab) = \varphi(a)\varphi(b), \varphi(1) = 1$. An isomorphism is a homomorphism with an inverse.)

Here's some basic definitions (that you probably already know):

Definition 1.5: A **zero** (or root) of $P(x)$ is a value t such that $P(t) = 0$.

The **degree** of a polynomial $P(x) = \sum_{n \geq 0} a_n x^n$ is the largest n such that $a_n \neq 0$. (The degree of 0 is said to be $-\infty$.)

A polynomial is **monic** if its leading coefficient is 1.

Now that we have the theory of polynomials on a solid footing, we can move on to more concrete concepts!

2 Values and Zeros

Proposition 2.1: Let K be a field (such as $\mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}, \ldots$). If $p \in K[x]$ and $p(x_0) = 0$, then $p(x) = (x - x_0)q(x)$ for some polynomial q.

Proof. By division with remainder, we can write

$$p(x) = (x - x_0)q(x) + r(x)$$

where the remainder term $r(x)$ has strictly smaller degree than $x - x_0$. Hence $r(x)$ is a constant. Substitute $x = x_0$ to get

$$0 = r(x_0).$$

Therefore, $r(x) = 0$. □

Note that the same idea also proves the Remainder Theorem (how?).

Now if we know that $r_1, \ldots, r_n$ are roots of $p(x)$, then we can factor $p(x) = (x - r_1)\ldots(x - r_n)q(x)$. In particular, if $p(x)$ has degree at most n, then $p(x) = c(x - r_1)\ldots(x - r_n)$ for some constant c.

This gives the following fundamental facts.

Theorem 2.2:

1. Over a field, a polynomial of degree at most n that is zero for $n+1$ values of x is identically 0. In other words, a polynomial of degree $n > 0$ can have at most n zeros.
2. Two polynomials of degree at most n that are equal for $n + 1$ values of x are identically equal.
3. A polynomial which is zero for infinitely many values is identically 0.

Proof.

1. If the zeros are $r_1, \ldots, r_{n+1}$ then as above we factor $p(x) = (x - r_1)\cdots(x - r_{n+1})q(x)$. Since $p(x)$ has degree at most n, we must have $q(x) = 0$.
2. If $p(x) = q(x)$ for $n + 1$ values of x, then applying part 1 to $p(x) - q(x)$ shows that $p(x) - q(x) = 0$.
3. Immediate since every nonzero polynomial has finite degree.

□

Now comes our first strategy for tackling polynomial problems.

Get something in the form $Q(x) = 0$ and factor based on roots. Plug in a value to get the leading coefficient. Alternatively "guess" a polynomial satisfying the equations, and use Theorem 2.2 to show it is correct.

Example 2.3: A polynomial P of degree n satisfies $P(x) = \frac{x}{x+1}$ for $x = 0, 1, \ldots, n$. Find $P(n + 1)$.

Solution. Rearrange to get

$$(x + 1)P(x) - x = 0 \text{ for } x = 0, 1, \ldots, n.$$

Since this equation has roots $x = 0, 1, \ldots, n$, and the left-hand side has degree $n + 1$,

$$(x + 1)P(x) - x = kx(x - 1)\cdots(x - n)$$

for some integer k. Then

$$P(x) = \frac{kx(x - 1)\cdots(x - n) + x}{x + 1}.$$

The numerator must be divisible by $x + 1$ so must have $x = -1$ as a zero. Plugging in, we get $(-1)^{n+1}(n + 1)!k - 1 = 0$, or $k = \frac{(-1)^{n+1}}{(n+1)!}$. Plugging in $x = n + 1$ gives

$$P(n + 1) = \begin{cases} 1, & n \text{ odd} \\ \frac{n}{n+2}, & n \text{ even.} \end{cases}$$

□

Alternatively, we can find an explicit, although somewhat messy, formula for a polynomial given its values.

Theorem 2.4 (Lagrange Interpolation)**:** Given $n+1$ points $(x_0, y_0), \ldots, (x_n, y_n)$ with distinct x-coordinates, there exists exactly one polynomial f of degree at most n so that $f(x_i) = y_i$ for $i = 0, 1, \ldots, n$. This polynomial is given by the following:

$$P(x) = \sum_{i=0}^{n} \left[y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j} \right].$$

Proof. Note that the ith term in the sum ($0 \leq i \leq n$) is engineered so that it has a zero at x_j for $j \neq i$. Thus, only the ith term contributes to the sum evaluated at x_i. We have

$$P(x_i) = y_i \prod_{j \neq i} \frac{x_i - x_j}{x_i - x_j} = y_i.$$

(The constant $y_i \prod_{j \neq i} \frac{1}{x_i - x_j}$ just so this would happen.) Hence P satisfies the conditions of the problem.

Uniqueness follows at once from Theorem 2.2(2). □

Here's an example.

Example 2.5: Let $r \geq 3$. Prove that there does not exists a real polynomial of degree at most n so that $|p(x) - r^x| < 1$ for $x = 0, 1, \ldots, n+1$.

Proof. Suppose $|p(x) - r^x| < 1$ for $x = 0, 1, \ldots, n$. Let $y_i = p(i)$ for $0 \leq i \leq n$. By the Lagrange Interpolation Formula,

$$p(x) = \sum_{i=0}^{n} \left[y_i \prod_{j \neq i} \frac{x - j}{i - j} \right].$$

When $r^i - 1 \leq y_i \leq r^i + 1$, $p(n+1)$ is maximized when we take $y_i = r^i - 1$ when the product is negative (i.e. when $n - i$ is odd) and y_i when the product is positive (i.e. when $n - i$ is even):

$$\begin{aligned}
p(n+1) &< \sum_{i=0}^{n} (r^i + (-1)^{n-i}) \prod_{j \neq i} \frac{(n+1) - j}{i - j} \\
&= \sum_{i=0}^{n} (r^i + (-1)^{n-i})(-1)^{n-i} \frac{(n+1)!}{i!(n+1-i)!} \\
&= \sum_{i=0}^{n} \left[\binom{n+1}{i} r^i (-1)^{n-i} + \binom{n+1}{i} \right] \\
&= -((r-1)^{n+1} - r^{n+1}) + (2^{n+1} - 1) \qquad \text{by the Binomial Theorem} \\
&= r^{n+1} - 1 + 2^{n+1} - (r-1)^{n+1} \leq r^{n+1} - 1
\end{aligned}$$

Note an alternate solution is to use Lagrange Interpolation with $n+2$ points and show that the coefficient of x^{n+1} cannot be 0. □

Next we introduce the derivative. Although the motivation for the derivative comes from calculus, for polynomials it can be defined purely in algebraic terms, and its properties can be proved algebraically. Hence it is useful even for polynomials over rings where there is no clear notion of distance, such as $\mathbb{Z}/p\mathbb{Z}$.

Definition 2.6: Let $f(x) = \sum_{n\geq 0} a_n x^n$ be a polynomial. The **d**erivative of $f(x)$ is defined as

$$f'(x) = \sum_{n\geq 1} n a_n x^{n-1}.$$

The following can easily be verified by the reader.

Proposition 2.7: Let f, g be two polynomials and c be a constant. Then

1. (Linearity) $(cf+g)' = cf' + g'$.
2. (Product rule) $(fg)' = f'g + fg'$.
3. (Chain rule) $(f \circ g)' = (f' \circ g)g'$.

Derivatives are useful in detecting repeated zeros. We assume the field is $\mathbb{R}$ or $\mathbb{C}$.

Proposition 2.8: If $(x-a)^n$ is the highest power of $x-a$ dividing f (we write $(x-a)^n || f$), then $(x-a)^{n-1} || f'$. Thus, a is a root of f of multiplicity n iff $f(a), f'(a), \ldots, f^{(n-1)}(a)$ are all zero but $f^{(n)}(a)$ is not.

Proof. Writing $f = (x-a)^n g$ where $x - a \nmid g$, we see by the product rule that $f'(x) = n(x-a)^{n-1}g + (x-a)^n g'$, so the statement follows. The second part follows by repeatedly taking derivatives. □

2.1 Problems

1. Let $r \neq 0$ be a real number. A polynomial P of degree n satisfies $P(x) = r^x$ for $x = 0, 1, \ldots, n$. Find $P(n+1)$.

2. n points $Q_1, \ldots, Q_n$ are equally spaced on a circle of radius 1 centered at O. Point P is on ray OQ_1 so that $OP = 2$. Find the product

$$\prod_{k=1}^{n} PQ_k$$

in closed form, in terms of n.

3. (AwesomeMath Team Contest 2010) Let $n \geq 2$. How many polynomials $Q(x)$ of degree at most $n-1$ are there such that

$$x(x-1)\cdots(x-n)Q(x) + x^2 + 1$$

is the square of a polynomial?

4. (APMO 2009/2) Let a_1, a_2, a_3, a_4, a_5 be real numbers satisfying the following equations:

$$\frac{a_1}{k^2+1} + \frac{a_2}{k^2+2} + \frac{a_3}{k^2+3} + \frac{a_4}{k^2+4} + \frac{a_5}{k^2+5} = \frac{1}{k^2}$$

for $k = 1, 2, 3, 4, 5$. Find the value of $\frac{a_1}{37} + \frac{a_2}{38} + \frac{a_3}{39} + \frac{a_4}{40} + \frac{a_5}{41}$.

5. (UM 2002/3) Imagine ducks as points in a plane. Three ducks are said to be in a row if a straight line passes through all three ducks. Three ducks, Huey, Dewey, and Louie, each waddle along a different straight line in the plane, each at his own constant speed. Although their paths may cross, the ducks never bump into each other. Prove that if at three separate times the ducks are in a row, then they are always in a row.

6. (IMC 2008/B4) Let $f(x), g(x)$ be nonconstant polynomials with integer coefficients such that $g(x)$ divides $f(x)$. Prove that if the polynomial $f(x) = 2008$ has at least 81 distinct integer roots, then the degree of $g(x)$ is greater than 5.

7. (USAMO 2002/3) Prove that any monic polynomial of degree n with real coefficients is the average of two monic polynomials of degree n with n real zeros.

8. (Putnam 1956) The nonconstant polynomials $f(z)$ and $g(z)$ with complex coefficients have the same set of numbers for their zeros but possibly with different multiplicities. The same is true of the polynomials $f(z) + 1$ and $g(z) + 1$. Prove that $f(z) = g(z)$. (Hint: take derivatives)

3 Symmetric Polynomials and Vieta's Formulas

Often we want to evaluate symmetric functions of the roots without actually computing them. Vieta's formula allows us to do this. First, a definition.

Definition 3.1: A **symmetric polynomial** in n variables $P(x_1, \ldots, x_n)$ is such that, for any permutation $x_{\sigma(1)}, \ldots, x_{\sigma(n)}$ of the variables $x_1, \ldots, x_n$, we have

$$P(x_1, \ldots, x_n) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

An **elementary symmetric polynomial** (or function, or sum) is one in the form

$$s_j = \sum_{1 \le i_1 < \ldots < i_j \le n} x_{i_1} \cdots x_{i_j}$$

for some $0 \le j \le n$. (Note $s_0 = 1$.)

For example, $x_1^2 x_2 + x_1 x_2^2 + x_2^2 x_3 + x_2 x_3^2 + x_3^2 x_1 + x_3 x_1^2$ is a symmetric polynomial in 3 variables.

Theorem 3.2 (Vieta's Formula)**:** Let $r_1, \ldots, r_n$ be the roots of $P(x) = \sum_{i=0}^{n} a_i x^i$, and let

$$s_j = \sum_{1 \le i_1 < \ldots < i_j \le n} r_{i_1} \cdots r_{i_j}.$$

Then $s_j = (-1)^j \frac{a_{n-j}}{a_n}$.

Proof. We can factor the polynomial as

$$P(x) = a_n(x - r_1)(x - r_2) \cdots (x - r_n).$$

Dividing by a_n gives

$$\left(x^n + \frac{a_{n-1}}{a_n} x^{n-1} + \cdots + \frac{a_1}{a_n} x + \frac{a_0}{a_n}\right) = (x - r_1)(x - r_2) \cdots (x - r_n).$$

In the expansion of the right-hand side, the terms containing x^{n-j} are of the form $(-r_{i_1})\cdots(-r_{i_j})x^{n-j}$—they contain a product of j roots. Summing them up, the coefficient of x^{n-j} is $(-1)^j s_j$. Setting this equal to the coefficient on the left-hand side, $\frac{a_{n-j}}{a_n}$, gives the desired result. □

Example 3.3: Let r_1, r_2 be the roots of the quadratic $ax^2 + bx + c = 0$. Find

1. $r_1 + r_2$
2. $r_1^2 + r_2^2$
3. $r_1^3 + r_2^3$

Solution.

1. From Vieta's formula, $r_1 + r_2 = -\frac{b}{a}$.
2. Also from Vieta's formula, $r_1 r_2 = \frac{c}{a}$. We need to combine these two expressions in some way to form $r_1^2 + r_2^2$. The following identity does the trick.

$$r_1^2 + r_2^2 = (r_1 + r_2)^2 - 2r_1 r_2.$$

   Thus $r_1^2 + r_2^2 = \left(-\frac{b}{a}\right)^2 - 2\left(\frac{c}{a}\right) = \frac{b^2-2ac}{a^2}$.
3. Noting the cube, we first cube $r_1 + r_2$ to get $r_1^3 + 3r_1^2 r_2 + 3r_1 r_2^2 + r_2^3$. We need to get rid of $3r_1^2 r_2 + 3r_1 r_2^2$. But we are in luck, since this equals $3r_1 r_2(r_1 + r_2)$. Hence

$$r_1^3 + r_2^3 = (r_1 + r_2)^3 - 3r_1 r_2(r_1 + r_2).$$

   (Another way to see this is to use the factorization $r_1^3+r_2^3 = (r_1+r_2)(r_1^2-r_1r_2+r_2^2) = (r_1 + r_2)((r_1 + r_2)^2 - 3r_1 r_2)$.) We get $r_1^3 + r_2^3 = \left(-\frac{b}{a}\right)^3 - 3\left(\frac{c}{a}\right)\left(-\frac{b}{a}\right) = \frac{-b^3+3abc}{a^3}$.

The examples above suggest that no matter what symmetric polynomial in the roots we are given, we can always write it in terms of the elementary symmetric functions, by simply matching the "highest degree term" at each step and then focusing on the remaining terms, of smaller degree. This is indeed true, and holds for arbitrarily many variables.

Theorem 3.4 (Fundamental Theorem of Symmetric Polynomials)**:** Let $P \in R[x_1, \ldots, x_n]$ be a symmetric polynomial in n variables. Then there exists a polynomial $Q \in R[x_1, \ldots, x_n]$ such that

$$P(x_1, \ldots, x_n) = Q(s_1, \ldots, s_n),$$

where s_i is the ith elementary symmetric polynomials. In other words, every symmetric polynomial can be written in terms of elementary symmetric polynomials.

Note that Q has coefficients in the same ring as P: for example, if P has integer coefficients, then Q will have integer coefficients as well.

Proof. We induct on the degree and the number of variables. For $\deg P = 0$ or $n = 1$ the assertion is obvious (in the latter case x_1 is the sole elementary symmetric polynomial and $P = Q$). Now assume the assertion proved for polynomials of the same number of variables but with smaller degree than P, and proved for polynomials of fewer variables

than P. Consider $P(x_1, \ldots, x_{n-1}, 0)$ as a polynomial in $n-1$ variables. Since it is symmetric in $x_1, \ldots, x_{n-1}$, by the induction hypothesis it can be written as

$$P(x_1, \ldots, x_{n-1}, 0) = R(s'_1, \ldots, s'_{n-1})$$

where $s'_j = \sum_{1 \le i_1 < \ldots < i_j \le n-1} x_{i_1} \cdots x_{i_j}$. Then $P(x_1, \ldots, x_n) - R(s_1, \ldots, s_{n-1})$ is zero when $x_n = 0$ (because then $s_j = s'_j$), so

$$P(x_1, \ldots, x_{n-1}, x_n) - R(s_1, \ldots, s_{n-1}) = x_n S(x_1, \ldots, x_n).$$

Since P and R are symmetric polynomials in the x_i, so is $x_n S(x_1, \ldots, x_n)$. Since x_n divides $x_n S(x_1, \ldots, x_n)$ and this polynomial is symmetric, so do x_j for all $1 \le j \le n$. Then $x_n S(x_1, \ldots, x_n) = x_1 \cdots x_n T(x_1, \ldots, x_n)$ for some symmetric T. Since T has smaller degree, it can be written in terms of symmetric polynomials by the induction hypothesis, say as $U(s_1, \ldots, s_n)$. Then

$$P(x_1, \ldots, x_n) = R(s_1, \ldots, s_{n-1}) + s_n U(s_1, \ldots, s_n)$$

is the desired representation. □

Note the proof gives a constructive way to find the representation.

Finally, a particularly interesting case is when the symmetric polynomial is a sum of powers, $x_1^j + \cdots + x_n^j$. In this case we can use the following formula to find the representation in terms of elementary symmetric functions.

Theorem 3.5 (Newton Sums)**:** Let s_j denote the jth elementary symmetric polynomial in $x_1, \ldots, x_n$ and p_j denote the power sum $x_1^j + \cdots + x_n^j$. (By definition, $p_0 = n$ and $s_0 = 1$). Note that if $j > n$, then s_j is defined to be 0.

Then for all $m \ge 1$,

$$\sum_{k=0}^{m} (-1)^k s_k p_{m-k} = s_0 p_m - s_1 p_{m-1} + \cdots + (-1)^{m-1} s_{m-1} p_1 + (-1)^m s_m p_0 = 0.$$

3.1 Problems

1. (AIME1 2001/3) Find the sum of the roots of the equation $x^{2001} + \left(\frac{1}{2} - x\right)^{2001} = 0$ (given that there are no multiple roots).

2. Find the sum of the squares of the reciprocals of the roots of $x^5 + 3x^4 + 5x^3 + 7x^2 + 9x + 11 = 0$.

3. Given that the zeros of $x^3 + ax^2 + bx + c = 0$ are r_1, r_2, r_3, find the monic cubic polynomials whose roots are...

   (a) $\frac{1}{r_1}, \frac{1}{r_2}, \frac{1}{r_3}$

   (b) $r_1 + r_2, r_2 + r_3, r_3 + r_1$

   (c) r_1^2, r_2^2, r_3^2

4. (AIME2 2008/7) Let r, s, and t be the three roots of the equation

   $$8x^3 + 1001x + 2008 = 0.$$

   Find $(r+s)^3 + (s+t)^3 + (t+r)^3$.

5. (AIME1 2005/8) The equation

$$2^{333x-2} + 2^{111x+2} = 2^{222x+1} + 1$$

has three real roots. Given that their sum is $\frac{m}{n}$ where m and n are relatively prime positive integers, find $m+n$.

6. (AIME2 2003/9) Consider the polynomials $P(x) = x^6 - x^5 - x^3 - x^2 - x$ and $Q(x) = x^4 - x^3 - x^2 - 1$. Given that z_1, z_2, z_3, and z_4 are the roots of $Q(x) = 0$, find $P(z_1) + P(z_2) + P(z_3) + P(z_4)$.

7. (IMO 1988/4) Show that the solution set of the inequality

$$\sum_{k=1}^{70} \frac{k}{x-k} \geq \frac{5}{4}$$

is the union of disjoint half-open intervals with sum of lengths 1988.

4 The Fundamental Theorem of Algebra

We give two standard proofs of the following. (Note we've used it implicitly in the last section, when we assumed a polynomial of degree n has n complex roots.)

Theorem 4.1 (Fundamental Theorem of Algebra)**:** Any nonconstant complex polynomial has a zero in $\mathbb{C}$. Hence by induction every complex polynomial splits completely into linear factors $P(x) = c(x-r_1)\dots(x-r_n)$.

By scaling, it suffices to show this for $P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$. The first proof requires a theorem from analysis.

Theorem 4.2: A continuous real-valued function on a compact set attains a maximum and minimum.

In $\mathbb{R}$ or $\mathbb{C}$, a compact set is a closed and bounded set. A subset S of $\mathbb{R}$ or $\mathbb{C}$ is said to be closed if whenever S has elements arbitrarily close to a certain number x, then it contains x. For example, $[a,b]$ is closed in $\mathbb{R}$, but $(a,b]$ is not, because the latter contains points arbitrarily close to a but unequal to a. In fact $\frac{1}{x-a}$ is a function defined on the latter interval that is not bounded. This theorem says that this would not happen on something like $[a,b]$.

Proof. **Main idea**: If P does not have a zero, take x such that it $|P(x)|$ attains minimum. We can move a small amount in one direction to make $|P(x)|$ smaller, a contradiction.

Step 1: $|P|$ attains a minimum.

Note that if x has absolute value at least S, then $|P(x)|$ is at least $S^n - |a_{n-1}|S^{n-1} - \cdots$. This approaches infinity as S approaches infinity. Hence the infimum (greatest lower bound) of $|P|$ is the same as if we restrict it to some sufficiently large ball around 0, $|x| \leq S$ for some S. But this is a compact set, as it is closed and bounded, so $|P|$ attains a minimum here, say at x_0. Suppose that $P(x_0) \neq 0$.

Step 2: Adjust x.

For convenience, set $Q(x) = \frac{P(x_0+x)}{Q(x_0)}$; that is, Q is a shifted and scaled version of P so that $Q(0) = 1$ is the minimum of $|Q|$. Write $Q(x) = 1 + b_k x^k + b_{k+1}x^{k+1} + \cdots$ where $b_k \neq 0$. Then[1]

$$Q(re^{i\theta}) = 1 + b_k r^k e^{i\theta k} + r^{k+1}(b_{k+1}e^{i\theta(k+1)} + \cdots)$$

However,

$$\left|\frac{r^{k+1}(b_{k+1}e^{i\theta(k+1)} + \cdots)}{b_k r^k e^{i\theta k}}\right| \to 0 \text{ as } r \to 0.$$

We can choose the direction θ so that $b_k r^k e^{i\theta k}$ is negative. By the triangle inequality

$$|Q(re^{i\theta})| < 1 - |b_k r^k| + |r^{k+1}(b_{k+1}e^{i\theta(k+1)} + \cdots)|.$$

However, we've shown that the last term is negligible compared to the second term as $r \to 0$, so choosing $r > 0$ small enough we get $|Q(re^{i\theta})| < 1$, contradiction. □

The second proof uses ideas from algebraic topology, as hinted by the first lecture.

Proof. **Main idea**: Let x range over the circles $g(\theta) = re^{2\pi i\theta}, \theta \in [0,1]$ for different r. For $r = 0$, $P(x)$ is just the constant path a_0 and does not go around 0; for large r, the x^n term dominates, and the path resembles $g(\theta)^n$ which goes around 0 n times. Thus for some intermediate r, $P(x)$ passes through 0. We need to make precise what it means for $P(x)$ to "wind" n times around 0, and prove that it is invariant under "deforming" a path (without having it pass through 0).

Suppose that P has no zero. Obviously, $a_0 \neq 0$ as else $x = 0$ is a zero.

Let $P_r(\theta) = P(g_r(\theta))$. We think of this as a family of functions (or paths) $[0,1] \to \mathbb{C}$. For any r, we have that

$$P_0 \equiv a_0 \text{ deforms continuously to } P_r, \tag{1}$$

as $P_r(\theta)$ is continuous in r and θ.

Now, x^n winds n times around 0 as x goes around the circle $g_r(\theta)$, and $|x^n| > |a_{n-1}x^{n-1} + \ldots|$ for sufficiently large r. Thus for such a $r = R$, $P_R(\theta)$ sticks close to x^n as x varies around the circle, following x^n around 0 n times. Indeed,

$$P_R(\theta) \text{ deforms continuously into } r^n e^{2\pi in}. \tag{2}$$

To see this, define $f_t(\theta) = (g_R(\theta))^n + t(a_{n-1}g_R(\theta)^{n-1} + \ldots)$. Then $f_t(x)$ for $0 \leq t \leq 1$ deforms from $f_0(\theta) = r^n e^{2\pi ni\theta}$ to $f_1(\theta) = P_R(\theta)$ in $\mathbb{C} - \{0\}$ (since $|x^n| > |a_{n-1}x^{n-1} + \ldots|$, none of the f_t pass through 0).

(In topology these "deformations" are called **homotopies**.)

From (1) and (2), the point a_0 deforms continuously into the function $r^n e^{2\pi in}$, a circle going through the origin n times, without passing through 0. However this is a contradiction (although to show it rigorously requires some topology), unless $n = 0$, in which case P is a constant polynomial.

□

Example 4.3: Let $f(x)$ be a real polynomial such that $f(x) \geq 0$ for all real x. Then there exist real polynomials $g(x), h(x)$ such that $f(x) = g(x)^2 + h(x)^2$.

[1] $re^{i\theta} = \cos\theta + i\sin\theta$

Proof. By the Fundamental Theorem of Algebra, $f(x)$ splits completely into linear factors $x-r_i$. Since $f(x)$ is real, all its zeros (counted with multiplicity) are either real or come in complex conjugate pairs. Since $f(x) \geq 0$ for all i, all zeros must have even multiplicity—otherwise $f(x)$ would change sign at that zero. Hence the real roots can be paired up (trivially) into complex conjugate pairs as well. Then we can write

$$f(x) = c(x - r_1)(x - \overline{r_1}) \cdots (x - r_n)(x - \overline{r_n})$$

where $c \geq 0$. Let $f_1(x) = \sqrt{c}(x - r_1) \cdots (x - r_n)$ and $f_2(x) = \sqrt{c}(x - \overline{r_1}) \cdots (x - \overline{r_n})$. Then f_1 and f_2 are conjugate, so writing $f_1(x) = g(x) + ih(x)$ for real polynomials g and h, we see that $f_2(x) = g(x) - ih(x)$. Hence

$$f(x) = f_1(x)f_2(x) = [g(x) + ih(x)][g(x) - ih(x)] = g(x)^2 + h(x)^2,$$

as desired. □

4.1 Problem

1. How many ordered pairs of real polynomials $(g(x), h(x))$ are there so that

$$g(x)^2 + h(x)^2 = \frac{x^{20} - 1}{x^2 - 1}?$$