Polynomials

Putnam Notes, Fall 2006 University of Utah

We recall some basic definitions and properties.

Fundamental Theorem of Algebra. Every nonzero polynomial of degree n with complex coefficients has precisely n complex roots $a_1, a_2, \ldots, a_n$ and can be factored as

$$p(x) = c(x - a_1)(x - a_2)\cdots(x - a_n).$$

For example, the complex roots of $x^n - 1 = 0$ (n-th roots of 1) form a regular n-gon in complex plane, and can be written as

$$e^{2\pi ik/n} = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}), \qquad k = 1, \ldots, n.$$

Polynomial Interpolation. For any sequence $a_1, a_2, \ldots, a_n$ of n complex numbers and n distinct points $x_1, x_2, \ldots, x_n$ in $\mathbb{C}$ there exists a unique polynomial of degree at most $n-1$ such that

$$p(x_j) = a_j, \qquad j = 0, 1, \ldots, n.$$

This polynomial is easily constructed using Lagrange's interpolation:

$$P(x) = \sum_{j=0}^{n} a_j \frac{\prod_{i \neq j}(x - x_i)}{\prod_{i \neq j}(x_j - x_i)}.$$

Division Algorithm. If f and $g \neq 0$ are two polynomials with coefficients in a field F, then there exist unique polynomials q and r such that

$$f = qg + r.$$

here either $r = 0$ or $\deg(r) < \deg(g)$. The situation with polynomials with coefficients in a ring is more delicate. However, if f and g have integer coefficients, and g is monic (the first non-zero coefficient is 1), then q and r also have integer coefficients.

One can use the division algorithm to show that $F[x]$ is a unique factorization domain. That is, every polynomial $p(x)$ can be factored into irreducible polynomials $p(x) = q_1(x) \cdot \ldots \cdot q_m(x)$ where $q_i(x)$ are uniquely determined up to a permutation and multiplication of each $q_i(x)$ by a non-zero scalar c_i such that $c_1 \cdot \ldots \cdot c_m = 1$. Once we know that $F[x]$ is a unique factorization domain, it can be shown that $F[x_1, \ldots, x_n]$, the ring of polynomials in n variables is also a unique factorization domain.

Invariant Polynomials. Here we discuss polynomials in n variables $x_1, \ldots, x_n$. A polynomial p is said to be invariant if it does not change under any permutation of n variables. Every invariant polynomial in $x_1, \ldots, x_n$ is a polynomial in elementary symmetric polynomials $c_1, c_2, \ldots, c_n$ which are defined by

$$(x - x_1)(x - x_2) \cdots (x - x_n) = x^n + c_1 x^n + c_2 x^{n-2} + \ldots + c_n.$$

For example, if $n = 3$ then there are three elementary symmetric functions and they are

$$\begin{cases} c_1 = -(x_1 + x_2 + x_3) \\ c_2 = x_1 x_2 + x_1 x_3 + x_2 x_3 \\ c_3 = -x_1 x_2 x_3. \end{cases}$$

The polynomial $S_2 = x_1^2 + x_2^2 + x_3^2$ is symmetric and in terms of c_i's it can be written as

$$S_2 = c_1^2 - 2c_2.$$

This formula is a special case of **Newton's formulas for power sums.** More precisely, let m be a positive integer. The m-th power sum in $x_1, \ldots, x_n$ is

$$S_m = x_1^m + x_2^m + \cdots + x_n^m.$$

Then

$$\begin{array}{rcl} S_1 + c_1 & = & 0 \\ S_2 + c_1 S_1 + 2c_2 & = & 0 \\ S_3 + c_1 S_2 + c_2 S_1 + 3c_3 & = & 0 \\ & \cdots & \\ S_n + c_1 S_{n-1} + \cdots + c_{n-1} S_1 + n c_n & = & 0 \\ S_m + c_1 S_{m-1} + \cdots + c_n S_{m-n} & = & 0 \end{array}$$

where the last equality holds for $m > n$. Notice that the formulas imply not only that S_k can be expressed in terms of c_k but, conversely, that c_k can be expressed in terms of S_k for $k \leq n$. In particular, it follows that any symmetric polynomial in variables $x_1, \ldots, x_n$ can be expresses as a polynomial in S_k for $k \leq n$, as well.

Palindromic polynomials. The equation $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ is called palindromic if $a_j = a_{n-j}$ for all j. If n is even, then by substitution $z := x + 1/x$ reduces to an equation of degree $n/2$. After finding solutions z_j, $j = 1, \ldots z_{n/2}$, the solutions of the original equation are found by solving $x + \frac{1}{x} = z_j$ for all j.

The following is an important observation. If a is a real number then solutions of

$$x + \frac{1}{x} = a$$

are real if $|a| \geq 2$ and complex numbers on the unit circle ($|x| = 1$) if $|a| \leq 2$.

Cubic equation. The equation $x^3 + px + q = 0$ has three solutions which are described as follows: Put

$$R = (q/2)^2 + (p/3)^3$$

and

$$A = \sqrt[3]{-\frac{q}{2} + \sqrt{R}}, \qquad B = \sqrt[3]{-\frac{q}{2} - \sqrt{R}}$$

Then the three solutions are

$$\{A + B, A\rho + B\rho^2, A\rho^2 + B\rho\}$$

where $\rho = e^{2\pi i/3}$ is a cubic root of 1. The number R is essentially the discriminant of the cubic. More precisely,

$$108R = -(x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2$$

where x_1, x_2 and x_3 are three roots of the cubic polynomial. Assume that p and q are real. If all three roots are real then $R < 0$. If one root is real and the other two are complex conjugates of each other, then $R > 0$. Thus calculating the discriminant is a quick way to see whether a cubic has one or three real roots.

Exercises:

1. Find the reminder when $x^{81}+x^{49}+x^{25}+x^9+x$ is divided by a) x^3-x, b) x^2+1, c) x^2+x+1.

2. Let p be a non-constant polynomial with integral coefficients. If $p(k) = 0$ for four distinct integers k, prove that $p(k)$ is composite for every integer k.

3. Factor $(a+b+c)^3 - (a^3+b^3+c^3)$.

4. Find a if a and b are integers such that x^2-x-1 is a factor of $ax^{17}+bx^{16}+1$.

5. Find the unique polynomial of degree n such that
$$p(j) = 2^j$$
for $j = 0, 1, \ldots, n$.

6. Find the unique polynomial $p(x)$ of degree n such that
$$p(j) = \frac{1}{1+j}$$
for $j = 0, 1, \ldots, n$.

7. A polynomial p_n of degree n satisfies $p_n(k) = F_k$ for $k = n+2, n+3, \ldots, 2n+2$, where F_k are Fibonacci numbers. Show that $p_n(2n+3) = F_{2n+3} - 1$.

8. If
$$\begin{array}{ccccccc} x & + & y & + & z & = & 1 \\ x^2 & + & y^2 & + & z^2 & = & 2 \\ x^3 & + & y^3 & + & z^3 & = & 3 \end{array}$$
find $x^4+y^4+z^4$.

9. Complex solutions of $x^n - 1 = 0$ are ζ^k, $k = 1, \ldots n$ where $\zeta = e^{2\pi i/n}$. Show that
$$\sum_{k=1}^{n} \zeta^{dk} = \begin{cases} n \text{ if } d \text{ is a multiple of } n \\ 0 \text{ otherwise} \end{cases}$$

10. Find a cubic equation whose roots are cubes of the roots of $x^3+ax^2+bx+c=0$.

11. Let $x_1, x_2, \ldots, x_n$ be the roots of a polynomial $P(x) = x^n + ax^{n-1} + bx^{n-2} + cx^{n-3} + \cdots$ of degree n. The number

$$\prod_{i \neq j} (x_i - x_j)$$

is called the discriminant of P. It is symmetric in variables x_i, so it can be expressed as a polynomial in the coefficients of P. Do this for $n=2$ and $n=3$. If $n=3$, assume that the polynomial is x^3+px+q.

12. Find all values of the parameter a such that all roots of the equation

$$x^6 + 3x^5 + (6-a)x^4 + (7-2a)x^3 + (6-a)x^2 + 3x + 1 = 0$$

are real.

13. The roots of the fifth degree equation

$$x^5 - 5x^4 - 35x^3 + \ldots$$

form an arithmetic sequence. Find the roots.

14. Let $G_n = x^n \sin nA + y^n \sin nB + z^n \sin nC$ where x, y, z, A, B, C are real numbers such that $A+B+C$ is a multiple of π. Show that if $G_1 = G_2 = 0$ then $G_n = 0$ for all positive n.

15. If

$$\begin{array}{ccccccc} x & + & y & + & z & = & 3 \\ x^2 & + & y^2 & + & z^2 & = & 25 \\ x^4 & + & y^4 & + & z^4 & = & 209 \end{array}$$

find $x^{100} + y^{100} + z^{100}$.

16. (B1 2005) Find a non-zero polynomial $P(x, y)$ such that $P([a], [2a]) = 0$ for all real numbers for all real numbers a. (Note: $[a]$ is the greatest integer less then or equal to a.)

17. (A3 2001) Find values for the integer m such that

$$P_m = x^4 - (2m+4)x^2 + (m-2)^2$$

is a product of two non-constant polynomials with integer coefficients?

Hints and solutions

1. (part c)). The roots of x^2+x+1 are ρ and $\bar{\rho}=\rho^2$, two cubic roots of 1:
$$\rho=-\frac{1}{2}+\frac{\sqrt{-3}}{2}$$
Thus
$$x^{81}+x^{49}+x^{25}+x^9+x=q(x)(x^2+x+1)=ax+b$$
gives
$$1+\rho+\rho+1=a\rho+b$$
which implies that $a=2$ and $b=2$.

2. Hint: Let a,b,c,d be the four integral roots. Then
$$p(x)=(x-a)(x-b)(x-c)(x-d)q(x)$$
where $q(x)$ has integral coefficients. If x is an integer, then $(x-a)(x-b)(x-c)(x-d)$ is composite.

3. Hint: Use formulas for a difference and a sum of two cubes. Then
$$(a+b+c)^3-a^3=(b+c)(\cdots)\text{ and }b^3+c^3=(b+c)(\cdots).$$
It follows that $(b+c)$ divides our polynomial. By symmetry, $a+c$ and $a+b$ also divide our polynomial, as well. Thus
$$(a+b+c)^3-(a^3+b^3+c^3)=k(a+b)(a+c)(b+c)$$
for a constant k. Now put $a=b=c=1$ to find that $k=1$.

4. Solution: The solutions of $x^2-x-1=0$ are
$$\alpha=\frac{1+\sqrt{5}}{2}\text{ and }\bar{\alpha}=\frac{1-\sqrt{5}}{2}.$$
Thus $ax^{17}+bx^{16}+1=q(x)(x^2-x-1)$ gives
$$\begin{aligned}a\alpha^{17}+b\alpha^{16}+1=0\\ a\bar{\alpha}^{17}+b\bar{\alpha}^{16}+1=0\end{aligned}$$

which is a 2×2 system with a and b as unknowns. Since $\alpha\bar{\alpha} = -1$, the determinant of this system is equal to $\alpha - \bar{\alpha} = \sqrt{5}$. Thus, using the Cramer's rule, the solution is

$$a = \frac{(1+\sqrt{5})^{16} - (1-\sqrt{5})^{16}}{2^{16}\sqrt{5}}$$

which we recognize as the 16-th Fibonacci number.

5. Hint: Use the Lagrange's interpolation.

6. Hint: Consider $q(x) = (1+x)p(x) - 1$. Then

$$q(x) = cx(x-1)\dots(x-j)$$

Now pick c so that $q(x)+1$ is divisible by $1+x$.

7. Hint: Notice that for $k = n+1, n+2, \dots, 2n$

$$p_n(k+2) - p_n(k+1) = F_{k+2} - F_{k+1} = F_k$$

so $p_{n-1}(x) = p_n(x+2) - p_n(x+1)$. Use this to do induction.

1) Base of induction: Let $n = 1$. Since $p_1(3) = 2$ and $p_1(4) = 3$ then $p_1(x) = x+1$. Thus

$$p_1(5) = 4 = F_5 - 1.$$

2) Step of induction: Assume that p_{n-1} satisfies $p_{n-1}(2n+1) = F_{2n+1} - 1$. Thus

$$p_n(2n+3) = p_n(2n+2) + p_{n-1}(2n+1) = F_{2n+2} + F_{2n+1} - 1 = F_{2n+3} - 1.$$

8. Elementary exercise in symmetric polynomials.

9. You are asked to compute the power sums for the roots of the polynomial $x^n - 1 = 0$. Note that all $c_i = 0$ except $c_n = 1$.

10. Hint: the coefficients of the desired cubic are also symmetric functions in roots of the original cubic.

11. If $n = 2$, write the polynomial in a more familiar $x^2 + px + q = 0$.

$$(x_1 - x_2)(x_2 - x_1) = 2x_1x_2 - (x_1^2 + x_2^2) = 4x_1x_2 - (x_1 + x_2)^2 = 4q - p^2.$$

Note that this expression appears in the quadratic formula! If $n = 3$, it takes a bit more to do the problem.

12. Hint: The polynomial is palindromic so it can be reduced to the degree 3. Next, the solutions of
$$x + \frac{1}{x} = b$$
are real iff $|b| \geq 2$.

13. Hint: The 5 roots are a, $a+d$, $a+2d$, $a+3d$ and $a+4d$ for two numbers a and b. The first two symmetric polynomials are known. This gives
$$5a + 10d = 5 \text{ and } 10a^2 + 40ad + 35d^2 = -35.$$

14. Solution: Put $X = xe^{iA}$, $Y = ye^{iB}$ and $Z = ze^{iC}$. Then G_n is the imaginary part of the n-th power sum
$$S_n = X^n + Y^n + Z^n.$$
Since $G_1 = G_2 = 0$ the first two elementary symmetric polynomials in X, Y, Z are real. Since
$$XYZ = xyze^{i(A+B+C)} = \pm xyz,$$
(here we are using that $A+B+C$ is a multiple of π) the third elementary symmetric polynomial is also real. Since all S_n can be expressed as polynomials with integer coefficients of the three elementary symmetric polynomials, they have to be real.

15. Hint: (I am not so sure, though.) Note that any symmetric polynomial is a polynomial in S_1, S_2 and S_3. By degree considerations, S_4 must be linear in S_3, so we can certainly figure out S_3, and therefore x, y and z as solutions of a cubic?

16. Hint: This problem is very easy. What is the possible difference $[2a] - 2[a]$?

17. Hint: Find the roots.