

Polynomials

James Bang

January 20, 2020

Polynomials are a simple type of function which are prevalent in Olympiad mathematics problems, coming up in different ways including integer/real/complex functions, their properties and sometimes polynomial functional equations. This handout aims to address certain parts of how polynomials appear in Olympiad problems, and how to solve some of them.

1 Definitions

Simply said, a **polynomial** $P(x)$ of one variable x is any expression that can be created by any string of additions, subtractions and multiplications of real numbers and the pronumeral x . More rigorously, A polynomial $P = P(x)$ of degree n is any expression of the form

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

where the a_0, a_1, \dots, a_n are called the **coefficients** of the polynomial P (with $a_n \neq 0$). For a set A , we denote $A[x]$ as the set of polynomials with coefficients in A : for example, the polynomial $P(x) = x$ is in both $\mathbb{Z}[x]$ as well as $\mathbb{R}[x]$, however $P(x) = \pi x + e \in \mathbb{R}[x]$ but $\notin \mathbb{Z}[x]$.

We also define the following notation:

- The polynomial P is called **monic** if the leading coefficient is 1, i.e. $a_n = 1$.
- A polynomial P is **constant** if $n = 0$, **linear** if $n = 1$, **quadratic** if $n = 2$, **cubic** if $n = 3$, **quartic** if $n = 4$, **quintic** if $n = 5$ and so on.
- The **degree** of a polynomial P is the highest nonzero power of x that exists within its expansion (so it is n in this case). We denote the degree as $\deg(P(x)) = \deg(P)$. For example, $\deg(x^3) = 3$ and $\deg(0x^2 + x + 1) = 1$.

The degree has the following properties:

- The degree is **log-additive**: For any two polynomials $P(x)$ and $Q(x)$, we have

$$\deg(PQ) = \deg(P) + \deg(Q).$$

This is because if $\deg(P) = m$ and $\deg(Q) = n$, then we have $P(x) = Ax^m + \dots$ and $Q(x) = Bx^n + \dots$, and the highest degree term of $P \cdot Q$ can then easily be seen to be x^{m+n} , from which the result follows.

- **The degree of the zero polynomial is defined to be $-\infty$, NOT ZERO.** If it was any real number, then the $\deg(PQ) = \deg(P) + \deg(Q)$ fails:

$$\deg(0) = \deg(P \cdot 0) = \deg(P) + \deg(0).$$

In this case, it makes sense to put $\deg(0) = -\infty$ as otherwise we get $\deg(P) = 0$ for any polynomial P which is a contradiction.

- Given two polynomials $P(x)$ and $Q(x)$ that do not have the same degree, we have

$$\deg(P + Q) = \max\{\deg(P), \deg(Q)\}.$$

If the degrees of P and Q are the same, then $\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\}$. This can be seen by the expansion of $P + Q$.

- Given polynomials $P(x)$ and $Q(x)$, we have

$$\deg(P(Q(x))) = \deg(P) \times \deg(Q).$$

For convenience, we shall denote $P(Q(x)) = P \circ Q$, and hence $\deg(P \circ Q) = \deg(P) \cdot \deg(Q)$.

Any nonzero polynomial P can also be expressed in the form

$$P(x) = A(x - r_1)(x - r_2) \dots (x - r_n)$$

where $A = a_n$ and r_1, r_2, \dots, r_n are the **roots** of the polynomial P , i.e. values for which $P(r_i) = 0$. This is a consequence of the **Fundamental Theorem of Algebra**: we shall discuss this later.

1.1 Basic Properties

- The addition of two polynomials is also a polynomial: more explicitly, if we have $f(x) = \sum_{k=0}^n a_k x^k$ and $g(x) = \sum_{k=0}^m b_k x^k$ for some $n \geq m$, then we have

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \dots + a_n x^n = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k)x^k,$$

where $a_k = 0$ for $k > n$ and similar for b_k .

- The product of two polynomials is also a polynomial: more explicitly, if we have $f(x) = \sum_{k=0}^n a_k x^k$ and $g(x) = \sum_{k=0}^m b_k x^k$ for some $n \geq m$, then we have

$$f(x) \times g(x) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x^k,$$

where $a_k = 0$ for $k > n$ and similar for b_k .

- Dividing two polynomials **will not necessarily give a polynomial**. For instance, if we have $f(x) = x^2 - 1$ and $g(x) = x$, then the quotient

$$\frac{f(x)}{g(x)} = \frac{x^2 - 1}{x} = x - \frac{1}{x}$$

is **not** a polynomial due to the $1/x$ term.

2 Polynomial Division

Given two polynomials P and Q with $\deg(P) \leq \deg(Q)$, we may **divide** the polynomial P by Q and get a **remainder** polynomial B where $\deg(B) < \deg(P)$. Formally, we can find two polynomials $A(x)$ and $B(x)$ such that

$$Q(x) = P(x) \cdot A(x) + B(x).$$

We denote $A(x)$ as the **quotient**, and $B(x)$ as the **remainder** when Q is divided by P .

If we have $B(x) = 0$ for all x , then we say that $P(x)$ **divides** $Q(x)$, and denote $P(x) \mid Q(x)$ or $P \mid Q$.

2.1 Long Division

We all know how to do long-division of base-10 numbers (or hopefully of any base). This same technique can be used to divide one polynomial by another to find its quotient and remainder. For example, let's suppose we wanted to express $x^3 - 4x^2 + 9x - 5$ in the form $(x - 3)A(x) + B(x)$. Then, we can place it in our familiar division box, and divide as follows:

$$\begin{array}{r} x^2 - 1x + 6 \\ x - 3 \overline{) x^3 - 4x^2 + 9x - 5} \\ \underline{x^3 - 3x^2} \\ -x^2 + 9x \\ \underline{-x^2 + 3x} \\ +6x - 5 \\ \underline{+6x - 18} \\ +13 \end{array}$$

Hence, we have $x^3 - 4x^2 + 9x - 5 = (x - 3)(x^2 - x + 6) + 13$. Easy, right?

Note that if the polynomial $Q(x)$ is missing some coefficients (that is, there are numbers k for which the coefficient of x^k is zero), then in the division process, we write it out in full form $\sum_{k=0}^n a_k x^k$ even if some a_k 's are equal to zero. For example, to divide $x^3 - 1$ by $x + 2$, we may need to express $x^3 - 1$ as $x^3 + 0x^2 + 0x - 1$.

Problem 2.1. Use long division to divide $Q(x)$ by $P(x)$ and express $Q(x) = A(x)P(x) + B(x)$, where:

1. $P(x) = x^2 - x + 1$ and $Q(x) = x^6 - 4x^2 + 8$,
2. $P(x) = x^2 - 2x + 2$ and $Q(x) = x^4 - 4$.

2.2 The Remainder Theorem

Suppose we now have the case when $P(x)$ is a monic, linear function, i.e. $P(x) = x - \alpha$ for some $\alpha \in \mathbb{R}$. Then the division algorithm gets that there is some polynomial $A(x)$ and a constant C , such that

$$Q(x) = (x - \alpha)A(x) + C.$$

In fact, we can say much more about this constant C :

Theorem 2.2: The Remainder Theorem / Factor Theorem

Suppose $Q(x)$ is any polynomial with complex coefficients. Then, $\alpha \in \mathbb{C}$ is a root of Q if and only if $x - \alpha \mid Q(x)$.

Proof. By plugging $x = \alpha$ into the equation above, we get $Q(\alpha) = (\alpha - \alpha)A(\alpha) + C$, or so $C = Q(\alpha)$, and so

$$Q(x) - Q(\alpha) = (x - \alpha)A(x).$$

If α is a root of x , then it follows from definition that $Q(\alpha) = 0$, and so there is some polynomial A for which $Q(x) = (x - \alpha)A(x)$.

As for the converse, if there exists a polynomial A for which $Q(x) = (x - \alpha)A(x)$, then from the earlier equation we get $C = Q(\alpha) = 0$, and so α is a root. \square

3 Roots of Polynomials

It follows from the Fundamental Theorem of Algebra that every nonzero polynomial $P(x) \in \mathbb{C}[x]$ has exactly the number of roots as its degree (counting multiplicity). Thus, for $n = \deg(P)$, there exists **roots** $\alpha_1, \alpha_2, \dots, \alpha_n$ (not necessarily distinct) and a nonzero leading coefficient A for which

$$P(x) = A \prod_{k=1}^n (x - \alpha_k).$$

3.1 Why can't polynomials have more than $\deg(P)$ roots?

Obviously, a constant nonzero polynomial $P(x) \equiv c$ cannot have any roots at all, since for any x we have $P(x) = c \neq 0$. Similarly, a linear polynomial $P(x) = ax + b$ cannot have more than one root, since otherwise if $x \neq y$ are roots and $a \neq 0$ then we have

$$0 = 0 - 0 = P(x) - P(y) = (ax + b) - (ay + b) = a(x - y)$$

or so $a = 0$, which is a contradiction. Does this generalise?

Theorem 3.1

A polynomial $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, with $a_n \neq 0$, cannot have more than $n + 1$ roots counted with multiplicity.

It turns out that this theorem is a trivial consequence of the factor theorem: suppose there are roots $\alpha_1, \dots, \alpha_{n+1}$ with multiplicity, then by the factor theorem there exists some polynomial $A(x)$ for which

$$P(x) = A(x) \cdot (x - \alpha_1) \dots (x - \alpha_{n+1}).$$

Comparing the degrees of both sides gives $n = \deg(A) + (n + 1)$, or $\deg(A) = -1$, which is a contradiction.

In particular, the above can address the following problem: does there exist any nonconstant periodic polynomial P (that is, there exists some $t \neq 0$ for which $P(x + t) = P(x)$)? If P is nonconstant, then there exists a root r of P , which means $r + t, r + 2t$, etc are all roots of P . This means P has infinitely many roots, which contradicts the above.

3.2 Vieta's Formulas

Vieta's formulas essentially relate the coefficients of a polynomial its roots. Let's say a polynomial $P(x)$ can be expressed in the form $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, but has the roots r_1, r_2, \dots, r_n . Then we get the equality

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = (x - r_1)(x - r_2) \dots (x - r_n).$$

Comparing the coefficient of x^{n-1} , we get

$$a_{n-1} = -(r_1 + r_2 + \cdots + r_n),$$

i.e. the sum of roots of a monic polynomial P is equal to the negative coefficient of x^{n-1} . By comparing the coefficients of other x^k , we can also get

$$a_{n-2} = r_1r_2 + r_1r_3 + \cdots + r_1r_n + r_2r_3 + \cdots + r_2r_n + \cdots + r_{n-1}r_n = \sum_{1 \leq i < j \leq n} r_i r_j$$

$$a_0 = (-1)^n r_1 r_2 \cdots r_n$$

amongst other such similar formulas. These are collectively called Vieta's Formulas.