Mathematical Olympiad Training
Polynomials

Definition

A polynomial over a ring $R(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$ in x is an expression of the form

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ a_i \in R,\ \text{for } 0 \le i \le n.$$

If $a_n \neq 0$, then $n = \deg p(x)$ is called the degree of $p(x)$. A non-zero element $r \in R$ is a polynomial of degree 0. The zero $0 \in R$ is a polynomial and its degree is negative infinity or undefined. The set of all polynomials over R in x is denoted by $R[x]$. $\Box$

For any $f(x), g(x) \in R[x]$.

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

Many properties of integers have analogues for polynomials.

Properties

1. Sum, difference and product of polynomials are polynomials.
2. Let $f(x), g(x) \in R[x]$, we say that $f(x)$ divides $g(x)$ if there exists non-zero $q(x) \in R[x]$ such that $g(x) = f(x)q(x)$. If $f(x)$ divids $g(x)$, we say that $f(x)$ is a divisor of $g(x)$ and write $f(x)|g(x)$.
3. Let $f(x), g(x) \in R[x]$, then there exists $q(x), r(x) \in R[x]$ such that $f(x) = q(x)g(x) + r(x)$ and $\deg r(x) < \deg g(x)$. (We say that $R[x]$ is a Euclidean domain.)

4. A polynomial $p(x)$ is said to be irreducible if it cannot be factorized into product of polynomials of positive degree. It is said to be reducible if it is not irreducible.

5. A polynomial $p(x)$ is called a prime polynomial if $p(x)|f(x)g(x)$ implies $p(x)|f(x)$ or $p(x)|g(x)$. It is easy to see that a prime polynomial is irreducible and the converse is true, but less obvious, only when R is a UFD.

6. Fix $f(x), g(x) \in R[x]$, the following statements for $d(x) \in R[x]$ are equivalent.

   (a) For any non-zero $p(x) \in R[x]$, $p(x)|f(x)$ and $p(x)|g(x)$ imply $p(x)|d(x)$.

   (b) $d(x)$ is a polynomial of maximal degree satisfying the properties that $d(x)|f(x)$ and $d(x)|g(x)$.

   (c) $d(x)$ is a non-zero polynomial of minimal degree such that there exists $a(x), b(x) \in R[x]$ with $d(x) = p(x)f(x) + q(x)g(x)$.

   If $d(x)$ satisfies one, hence all, of the above properties, we say that $d(x)$ is a greatest common divisor (GCD) of $f(x)$ and $g(x)$ and write $d(x) = (f(x), g(x))$. GCD always exists and is unique up to a unit (an invertible element in R) for every non-zero polynomials $f(x)$ and $g(x)$.

7. Any non-zero $p(x) \in R[x]$ can be factorized uniquely (up to unit and permutation) into product of irreducible polynomials. (We say that $R[x]$ is a unique factorization domain (UFD). To be more precise, $R[x]$ is a UFD if R is a UFD and it is well known that $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all UFD.)

Theorem (**Remainder Theorem**)

When $p(x) \in R[x]$ is divided by $x - a$, the remainder is $p(a)$. In particular $x - a$ divides $p(x)$ if and only if $p(a) = 0$. $\square$

The notion of reducibility of polynomial depends on the ring of coefficients R. For example, $x^2 - 2$ is irreducible over $\mathbb{Z}$ but is reducible over $\mathbb{R}$ and $x^2 + 1$ is irreducible over $\mathbb{R}$ but is reducible over $\mathbb{C}$.

Proposition

1. (**Gauss Lemma**) If a polynomial $f(x) \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}$, i.e. there exists $p(x), q(x) \in \mathbb{Q}[x]$ of positive degree such that $f(x) = p(x)q(x)$, then $f(x)$ is reducible over $\mathbb{Z}$.

2. (**Eisenstein Criterion**) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}$ and p be a prime number. Suppose

   (a) $p \nmid a_n$

   (b) $p | a_k$ for $0 \leq k \leq n - 1$

   (c) $p^2 \nmid a_0$

   Then $f(x)$ is irreducible over $\mathbb{Q}$. $\square$

The most important theorem about polynomials is the following.

Theorem (**Fundamental Theorem of Algebra**)

A polynomial of degree n over $\mathbb{C}$ has n zeros on $\mathbb{C}$ counting multiplicity. $\square$

Another way of stating Fundamental Theorem of Algebra is every complex polynomial $p(x) \in \mathbb{C}[x]$ of degree n can be factorized into product of linear polynomials, i.e. there exists $a, \alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{C}$ such that $p(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$.

Corollary

1. If a polynomial of degree not greater than n has $n+1$ distinct zeros, then it is the zero polynomial.

2. Two polynomials of degree not greater than n are equal if they have the same value at $n+1$ distinct numbers. $\square$

For polynomials with real coefficients $p(x) \in \mathbb{R}[x]$, we have

Propositions

1. Let $p(x) \in \mathbb{R}[x]$ and $\alpha \in \mathbb{C}$. If $p(\alpha) = 0$, then $p(\bar{\alpha}) = 0$, where $\bar{\alpha}$ denotes the complex conjugate of α.

2. Any $p(x) \in \mathbb{R}[x]$ can be factorized into product of quadratic and linear polynomials over $\mathbb{R}$. $\square$

A polynomial $p(x) \in R[x]$ can also be considered as a function $p : R \to R$. One can always find a unique polynomial of degree n with $n+1$ prescribed values.

Lagrange Interpolation Formula

Given any distinct $x_0, x_1, \cdots, x_n \in R$ and any $y_0, y_1, \cdots, y_n \in R$. There exists unique polynomial $p(x) \in R[x]$ of degree n such that $p(x_i) = y_i$ for all $i = 0, 1, \cdots, n$.

In fact we have

$$p(x) = \sum_{i=0}^{n} \frac{(x - x_0)(x - x_1) \cdots \widehat{(x - x_i)} \cdots (x - x_n) y_i}{(x_i - x_0)(x_i - x_1) \cdots \widehat{(x_i - x_i)} \cdots (x_i - x_n)},$$

where the notation $\widehat{(x - x_i)}$ means that $(x - x_i)$ is absent.

Another way of writing the interpolation formula is

$$\begin{vmatrix} y & x^n & \cdots & x^2 & x & 1 \\ y_0 & {x_0}^n & \cdots & {x_0}^2 & x_0 & 1 \\ y_1 & {x_1}^n & \cdots & {x_1}^2 & x_1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ y_n & {x_n}^n & \cdots & {x_n}^2 & x_n & 1 \end{vmatrix} = 0.$$

Proposition

A rational polynomial $p(x) \in \mathbb{Q}[x]$ takes integer values on all integers if and only if

$$p(x) = a_0 \binom{x}{0} + a_1 \binom{x}{1} + a_2 \binom{x}{2} + \cdots + a_n \binom{x}{n}$$

for some $a_0, a_1, a_2, \cdots, a_n \in \mathbb{Z}$, where $\binom{x}{k} = \frac{x(x-1)(x-2)\cdots(x-k+1)}{k!}$, $k \neq 0$ and $\binom{x}{0} = 1$.

Symmetric Polynomials

1. If a polynomial $p(x_1, x_2, \cdots, x_n)$ in n variables satisfies

$$p(x_1, \cdots, x_i, \cdots, x_j, \cdots, x_n) = p(x_1, \cdots, x_j, \cdots, x_i, \cdots, x_n)$$

   for any $i \neq j$, then $p(x_1, x_2, \cdots, x_n)$ is called a symmetric polynomial.

2. The elementary symmetric polynomials of degree k, $k = 0, 1, 2, \cdots, n$, in n variables $x_1, x_2, \cdots, x_n$ is defined by

$$\sigma_k(x_1, x_2, \cdots, x_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

For example $\sigma_0 = 1$, $\sigma_1 = x_1 + x_2 + \cdots + x_n$, $\sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n$, $\cdots$, $\sigma_n = x_1x_2\cdots x_n$.

3. The k-th power sum, $k \geq 0$, of n variables $x_1, x_2, \cdots, x_n$ is defined by

$$S_k(x_1, x_2, \cdots, x_n) = \sum_{1\leq i\leq n} {x_i}^k = {x_1}^k + {x_2}^k + \cdots + {x_n}^k.$$

Fundamental Theorem of Symmetric Polynomials

Any symmetric polynomial can be expressed as a polynomial in elementary symmetric polynomials in (or power sum of) those variables.

Newton-Girard Formulae

Let S_k be the k-th power sum and σ_k be the elementary symmetric polynomials of degree k in $x_1, x_2, \cdots, x_n$. Then for any positive integer m,

$$\sum_{k=0}^{m-1}(-1)^k\sigma_k S_{m-k} + (-1)^m m\sigma_m = 0.$$

Here $\sigma_0 = 1$, $\sigma_k = 0$ when $k > n$.

Example:

For $m = 1, 2, 3, \cdots, n$, we have

$$S_1 - \sigma_1 = 0$$

$$S_2 - \sigma_1 S_1 + 2\sigma_2 = 0$$

$$S_3 - \sigma_1 S_2 + \sigma_2 S_1 - 3\sigma_3 = 0$$

$$\vdots$$

$$S_n - \sigma_1 S_{n-1} + \cdots + (-1)^{n-1}\sigma_{n-1}S_1 + (-1)^n n\sigma_n = 0$$

For $m > n$, we have

$$S_m - \sigma_1 S_{m-1} + \sigma_2 S_{m-2} + \cdots + (-1)^n \sigma_n S_{m-n} = 0$$

Vieta's Formulae

Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}$ be a polynomial over $\mathbb{C}$ of degree n and $\alpha_1, \alpha_2, \cdots, \alpha_n$ be the roots of $p(x) = 0$. Let σ_k be the elementary symmetric polynomials of degree k in $\alpha_1, \alpha_2, \cdots, \alpha_n$. Then we have

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}.$$

Application to recurrence sequences

Combining Vieta's formula with Newton-Girard formula, we get an obvious relation

$$a_n S_m + a_{n-1} S_{m-1} + a_{n-2} S_{m-2} + \cdots + a_0 S_{m-n} = 0.$$

This means that the sequence $S_0, S_1, S_2, \cdots$ satisfies the recurrence relation

$$a_n S_{k+n} + a_{n-1} S_{k+n-1} + a_{n-2} S_{k+n-2} + \cdots + a_0 S_k = 0, \text{ for } k \geq 0.$$

More generally, fix any $A_1, A_2, \cdots, A_n \in \mathbb{C}$, let

$$x_k = A_1 {\alpha_1}^k + A_2 {\alpha_2}^k + \cdots + A_n {\alpha_n}^k. \tag{$*$}$$

Then $x_0, x_1, x_2, \cdots$ satisfies the recurrence relation

$$a_n x_{k+n} + a_{n-1} x_{k+n-1} + a_{n-2} x_{k+n-2} + \cdots + a_0 x_k = 0, \text{ for } k \geq 0. \tag{$**$}$$

Equation $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$ is called the characteristic equation. By solving it, we can find the general solution $(*)$ of the recurrence relation $(**)$.

Example: **Fibonacci sequence**

The Fibonacci sequence $0, 1, 1, 2, 3, 5, 8, 13, \cdots$ is defined by the recurrence equation

$$\begin{cases} F_k = F_{k-1} + F_{k-2}, \text{ for } k > 1 \\ F_0 = 0, \;\; F_1 = 1 \end{cases}.$$

The characteristic equation is $x^2 - x - 1 = 0$ and its roots are $\frac{1 \pm \sqrt{5}}{2}$. Solving

$$\begin{cases} A_1 + A_2 = F_0 = 0 \\ A_1\alpha_1 + A_2\alpha_2 = F_1 = 1 \end{cases},$$

we have $A_1 = \frac{1}{\sqrt{5}}$, $A_2 = -\frac{1}{\sqrt{5}}$ and

$$\begin{aligned} F_k &= \frac{1}{\sqrt{5}}{\alpha_1}^k - \frac{1}{\sqrt{5}}{\alpha_2}^k \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right) \\ &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k + \frac{1}{2}\right] \end{aligned}$$

where the notation $[x]$ means the largest integer not greater than x.

Example 1

Find all rational polynomials $p(x) = x^3 + ax^2 + bx + c$ such that a, b, c are roots of the equation $p(x) = 0$.

Solution

By Vieta's formula

$$\begin{cases} a + b + c = -a \\ ab + bc + ca = b \\ abc = -c \end{cases}$$

From the third equation $(ab + a)c = 0$. Thus $ab = -1$ or $c = 0$.

If $c = 0$, then $a + b = -a$ and $ab = b$. Hence $(a, b, c) = (0, 0, 0)$ or $(1, -2, 0)$.

If $ab = -1$, then $c = -2a - b$ and

$$\begin{aligned}
-1 + b(-2a - b) + (-2a - b)a &= b \\
2a^2 - 2 + b + b^2 &= 0 \\
2a^4 - 2a^2 + a^2 b + a^2 b^2 &= 0 \\
2a^4 - 2a^2 - a + 1 &= 0
\end{aligned}$$

Since a is rational, the only solution is $a = 1$ and $(a, b, c) = (1, -1, -1)$.

Hence the solution of the problem is $(a, b, c) = (0, 0, 0)$, $(1, -2, 0)$ or $(1, -1, -1)$.

Example 2

Given that $p(x)$ is a polynomial of degree n such that $p(k) = 2^k$ for $k = 0, 1, 2, \cdots n$.

Find $p(n + 1)$.

Solution

Take

$$p(x) = \binom{x}{0} + \binom{x}{1} + \binom{x}{2} + \cdots + \binom{x}{n},$$

then $p(x)$ satisfies the condition of the problem and

$$\begin{aligned}
p(n+1) &= \binom{n+1}{0} + \binom{n+1}{1} + \binom{n+1}{2} + \cdots + \binom{n+1}{n} \\
&= \binom{n+1}{0} + \binom{n+1}{1} + \binom{n+1}{2} + \cdots + \binom{n+1}{n} + \binom{n+1}{n+1} - 1 \\
&= 2^{n+1} - 1
\end{aligned}$$

Example 3

Given that $\begin{cases} x + y + z = 1 \\ x^2 + y^2 + z^2 = 3 \\ x^3 + y^3 + z^3 = 7 \end{cases}$. Find the value of $x^5 + y^5 + z^5$.

Solution

Let S_k and σ_k be the k-th power sum and symmetric sum of x, y, z. Then by Newton formula

$$\begin{cases} S_1 - \sigma_1 = 0 \\ S_2 - \sigma_1 S_1 + 2\sigma_2 = 0 \\ S_3 - \sigma_1 S_2 + \sigma_2 S_1 - 3\sigma_3 = 0 \end{cases} \Rightarrow \begin{cases} \sigma_1 = 1 \\ \sigma_2 = -1 \\ \sigma_3 = 1 \end{cases}.$$

Thus x, y, z are roots of the equation $t^3 - t^2 - t - 1 = 0$ and S_k satisfies the recurrence relation $S_{k+3} = S_{k+2} + S_{k+1} + S_k,\ k \geq 0$. Therefore $S_4 = 1 + 3 + 7 = 11$ and $S_5 = 3 + 7 + 11 = 21$.

Example 4

If x, y are non-zero numbers with $x^2 + xy + y^2 = 0$. Find $(\frac{x}{x+y})^{2001} + (\frac{y}{x+y})^{2001}$.

Solution

Observe that $\frac{x}{x+y} + \frac{y}{x+y} = 1$ and $\frac{x}{x+y} \cdot \frac{y}{x+y} = \frac{xy}{x^2+2xy+y^2} = \frac{xy}{xy} = 1$. We know that $\frac{x}{x+y}$, $\frac{y}{x+y}$ are roots of $t^2 - t + 1 = 0$. Thus $S_k = (\frac{x}{x+y})^k + (\frac{y}{x+y})^k$ satisfies the recurrence relation

$$\begin{cases} S_{k+2} = S_{k+1} - S_k,\ k \geq 0 \\ S_0 = 2, S_1 = 1 \end{cases}.$$

Then the sequence $\{S_k\},\ k \geq 0$, is $2, 1, -1, -2, -1, 1, 2, 1, \cdots$ and $S_k = S_l$ if $k \equiv l (\mathrm{mod} 6)$. Therefore $S_{2001} = S_3 = -2$.

Example 5 (IMO 1999)

Let $n \geq 2$ be a fixed integer. Find the least constant C such that the inequality

$$\sum_{1 \leq i < j \leq n} x_i x_j ({x_i}^2 + {x_j}^2) \leq C \left(\sum_{1 \leq i \leq n} x_i \right)^4$$

holds for any $x_1, x_2, x_3, \cdots, x_n \geq 0$. For this constant C, characterize the instances of equality.

Solution

Since the inequality is homogeneous, we may assume that $S_1 = \sigma_1 = 1$. By Newton formula, $S_4 - \sigma_1 S_3 + \sigma_2 S_2 - \sigma_3 S_1 + 4\sigma_4 = 0$. Then

$$\begin{aligned}
\sum_{1\le i<j\le n} x_i x_j ({x_i}^2 + {x_j}^2) &= \sum_{1\le i\le n} \left({x_i}^3 \sum_{j\ne i} x_j \right) \\
&= \sum_{1\le i\le n} {x_i}^3 (1 - x_i) \\
&= S_3 - S_4 \\
&= \sigma_2 S_2 - \sigma_3 S_1 + 4\sigma_4 \\
&= \sigma_2(1 - 2\sigma_2) + 4\sigma_4 - \sigma_3\sigma_1 \\
&\le \frac{1}{8}
\end{aligned}$$

The last inequality holds since

$$\sigma_2(1 - 2\sigma_2) = 2\sigma_2(\frac{1}{2} - \sigma_2) \le \frac{1}{2}(\sigma_2 + (\frac{1}{2} - \sigma_2))^2 = \frac{1}{8}$$

by AM-GM inequality and

$$4\sigma_4 = 4\binom{n}{4} \left(\frac{\sigma_4}{\binom{n}{4}} \right)^{\frac{3}{4}} \left(\frac{\sigma_4}{\binom{n}{4}} \right)^{\frac{1}{4}} \le 4\binom{n}{4} \frac{\sigma_3}{\binom{n}{3}} \frac{\sigma_1}{n} = \frac{n-3}{n}\sigma_3\sigma_1 \le \sigma_3\sigma_1$$

by symmetric mean inequality and the equality holds if and only if $\sigma_2 = \frac{1}{4}$ and $\sigma_3 = \sigma_4 = 0$. Therefore the least value of C is $\frac{1}{8}$ and the equality holds for the original inequality if and only if two x_i are equal and the rest are zero.

Example 6 (IMO 2006)

Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients and let k be a positive integer. Consider the polynomial $Q(x) = P(P(\ldots P(P(x))\ldots))$, where

P occurs k times. Prove that there are at most n integers t such that $Q(t) = t$.

Solution (by Tsoi Yun Pui)

Denote $\underbrace{P(P(\cdots P}_{k}(x))\cdots)$ by $Q_k(x)$. If there is at most one integer t satisfying $Q_k(t) = t$, then we are done. Otherwise, let s, t be integers such that $Q_k(s) = s$, $Q_k(t) = t$. As $P(x)$ is a polynomial with integral coefficients, $u - v \mid P(u) - P(v)$ for any integers u, v. So

$$s - t \mid P(s) - P(t) \mid Q_2(s) - Q_2(t) \mid \cdots \mid Q_k(s) - Q_k(t) = s - t,$$

and hence both $s - t \mid P(s) - P(t)$ and $P(s) - P(t) \mid s - t$. This implies that

$$P(s) - P(t) = s - t \quad \text{or} \quad P(s) - P(t) = t - s.$$

i.e.

$$P(s) - s = P(t) - t \quad \text{or} \quad P(s) + s = P(t) + t \tag{$*$}$$

It is impossible to have $P(s) - P(t) = s - t$ and $P(u) - P(t) = t - u$ for distinct integral roots s, u, t of the equation $Q_k(x) = x$. Otherwise

$$P(s) - P(u) = s - t - (t - u) = s + u - 2t.$$

But $P(s) - P(u) = s - u$ or $u - s$. In either cases, it yields $s = t$ or $u = t$. Contradiction. So only one equation in $(*)$ is true for all the integer roots of $Q_k(x) = x$.

In either cases, let us fix t. Then all integral roots of $Q_k(x) = x$ are also, at the same times, roots of the equation $P(x) - x = 0$ or $P(x) + x = 0$. Note that $P(x) - x$ and $P(x) + x$ are polynomials of degree n. So there is at most n such roots. Hence there are at most n integers t such that $Q(t) = t$.