FOCUS ON...

No. 26

Michel Bataille

Degree and roots of a polynomial

Introduction

In this number, we continue to illustrate some basic results about polynomials, focusing on the links between the degree and the number of roots.

Let $p(x)$ be a polynomial with coefficients in a field F. Recall that if k distinct elements $\alpha_1, \ldots, \alpha_k$ of F satisfy

$$p(\alpha_1) = \cdots = p(\alpha_k) = 0,$$

then $p(x)$ is divisible by

$$(x - \alpha_1) \cdots (x - \alpha_k).$$

A direct consequence is the following: unless $p(x)$ is the zero polynomial, we have $\deg(p(x)) \geq k$ and if $\deg(p(x)) = k$, then $p(x) = \rho(x - \alpha_1) \cdots (x - \alpha_k)$ for some nonzero constant ρ. In particular, a monic polynomial of degree k is completely determined once k distinct roots are identified.

Finding a polynomial through its roots

As an application of the latter, we consider the following nice problem set at the 1998 Vietnamese Olympiad:

> Prove that for each positive odd integer n there is exactly one polynomial $P(x)$ of degree n with real coefficients satisfying
>
> $$P\left(x - \frac{1}{x}\right) = x^n - \frac{1}{x^n} \tag{1}$$
>
> for all real $x \neq 0$.

For a proof by induction, we refer the reader to [2003 : 456]. We propose a solution which, if slightly longer, has the advantage of giving an explicit expression of $P(x)$.

First, suppose that such a polynomial $P(x)$ exists and let us determine its complex roots. If w is any n-th root of unity in $\mathbb{C}$, then (1) gives $P\left(w - \frac{1}{w}\right) = 0$. It follows that the n complex numbers

$$\exp\left(\frac{2k\pi i}{n}\right) - \exp\left(\frac{-2k\pi i}{n}\right) = 2i \sin\frac{2k\pi}{n}, \quad (k = 0, 1, \ldots, n-1)$$

are roots of $P(x)$. Moreover, these numbers are distinct: if w and w' satisfy

$$w^n = w'^n = 1 \quad \text{and} \quad w - \frac{1}{w} = w' - \frac{1}{w'},$$

then

$$(w' - w)(1 + ww') = 0$$

and so $w = w'$ (note that $ww' \neq -1$ since n is odd). In addition, it is easy to see (from (1)) that $P(x)$ must be monic. Thus,

$$P(x) = \prod_{k=0}^{n-1} \left(x - 2i \sin \frac{2k\pi}{n} \right)$$

is the only possible solution.

Conversely, consider this polynomial $P(x)$ and let $n = 2m + 1$. Since

$$\sin \frac{2(m+k)\pi}{2m+1} = -\sin \frac{2(m-k+1)\pi}{2m+1} \quad \text{for} \quad k = 1, 2, \ldots, m,$$

we have

$$P(x) = x \cdot \prod_{k=1}^{m} \left(x^2 + 4 \sin^2 \frac{2k\pi}{2m+1} \right)$$

and therefore $P(x)$ has real coefficients (and degree n). Now, for $x \neq 0$, we readily get

$$P\left(x - \frac{1}{x} \right) = \prod_{k=0}^{n-1} \frac{x^2 - 2ix \sin(2k\pi/n) - 1}{x}.$$

Since the roots of

$$x^2 - 2ix \sin(2k\pi/n) - 1$$

are

$$\exp\left(\frac{2k\pi i}{n} \right) \quad \text{and} \quad -\exp\left(\frac{-2k\pi i}{n} \right),$$

the polynomial $Q(x) = x^n P\left(x - \frac{1}{x}\right)$ is monic, of degree $2n$ and such that $Q(w) = 0$ when either $w^n = 1$ or $w^n = -1$. Since

$$w^{2n} - 1 = (w^n - 1)(w^n + 1),$$

the $2n$-th roots of unity are roots of $Q(x)$ and so $Q(x) = x^{2n} - 1$. It immediately follows that (1) holds.

Proving that a polynomial is the zero polynomial

Another consequence of our introductory result is, roughly speaking: a nonzero polynomial whose degree is not greater than n cannot have more than n roots. We give several examples, showing this result at work in various areas. Let us start with a simple exercise:

> Let n be an integer with $n \geq 2$ and $P_0(x), P_1(x), \ldots, P_{n-2}(x)$ be polynomials of $\mathbb{C}[x]$. If $x^{n-1} + x^{n-2} + \cdots + x + 1$ divides the polynomial $P_0(x^n) + xP_1(x^n) + \cdots + x^{n-2}P_{n-2}(x^n)$, show that $x - 1$ divides each of the polynomials $P_0(x), P_1(x), \ldots, P_{n-2}(x)$.

We observe that the roots of $x^{n-1}+x^{n-2}+\cdots+x+1$ are the numbers

$$w, w^2, \ldots, w^{n-1}, \quad \text{where} \quad w = \exp\left(\frac{2\pi i}{n}\right).$$

From the hypothesis, the polynomial

$$P(x) = P_0(x^n) + xP_1(x^n) + \cdots + x^{n-2}P_{n-2}(x^n)$$

satisfies

$$P(w^k) = 0 \quad \text{for} \quad k = 1, 2, \ldots, n-1.$$

Since $(w^k)^n = 1$, we deduce that

$$P_0(1) + w^k P_1(1) + w^{2k} P_2(1) + \cdots + w^{(n-2)k} P_{n-2}(1) = 0, \quad k = 1, 2, \ldots, n-1$$

so that the $n-1$ complex numbers $w, w^2, \ldots, w^{n-1}$ are distinct roots of the polynomial

$$P_0(1) + xP_1(1) + x^2P_2(1) + \cdots + x^{n-2}P_{n-2}(1).$$

Thus, this polynomial is the zero polynomial, meaning that

$$P_0(1) = P_1(1) = \cdots = P_{n-2}(1) = 0,$$

and these equalities imply the desired conclusion.

We continue with an example from linear algebra:

> Let A be an $n \times n$ matrix with complex entries and distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$. Show that $I_n, A, A^2, \ldots, A^{n-1}$ are independent vectors of $\mathcal{M}_n(\mathbb{C})$.

The hypothesis on A implies that A is similar to the diagonal matrix

$$D = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n),$$

that is, $A = PDP^{-1}$ for some invertible $n \times n$ matrix P.

Now, suppose that a relation

$$\alpha_0 I_n + \alpha_1 A + \cdots + \alpha_{n-1} A^{n-1} = O_n$$

holds for some complex numbers $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$. Since $A^m = PD^mP^{-1}$ for all nonnegative integers m, we deduce that

$$\alpha_0 I_n + \alpha_1 D + \cdots + \alpha_{n-1} D^{n-1} = O_n.$$

As a result,

$$\alpha_0 + \alpha_1\lambda_k + \alpha_2\lambda_k^2 + \cdots + \alpha_{n-1}\lambda_k^{n-1} = 0, \quad k = 1, 2, \ldots, n$$

and consequently $\lambda_1, \lambda_2, \ldots, \lambda_n$ are distinct roots of the polynomial

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{n-1} x^{n-1}.$$

This demands

$$\alpha_0 = \alpha_1 = \alpha_2 = \cdots = \alpha_{n-1} = 0$$

and the result follows.

Our next example is adapted from a problem of the 1996 Swedish competition:

> For every positive integer n, let $p_n(x) = \sum_{k=0}^{n} \binom{2n}{2k} x^{2n-2k}(x^2-1)^k$. If m is a positive integer, prove that $p_m(p_n(x)) = p_{2mn}(x)$.

The key remark is the following one: for any real number $x \geq 1$, we have

$$p_n(x) = \frac{1}{2}\left((x+\sqrt{x^2-1})^{2n} + (x-\sqrt{x^2-1})^{2n}\right),$$

a direct consequence of the Binomial Theorem. Such an expression prompts us to examine what occurs when we substitute $\cosh t$ for x. We obtain that

$$\begin{aligned} p_n(\cosh t) &= \frac{1}{2}\left((\cosh t + \sinh t)^{2n} + (\cosh t - \sinh t)^{2n}\right) \\ &= \frac{1}{2}(e^{2nt} + e^{-2nt}) = \cosh(2nt) \end{aligned}$$

for all $t \in [0, \infty)$ and we may write

$$p_m(p_n(\cosh t)) = p_m(\cosh(2nt)) = \cosh(2m(2nt)) = \cosh(4mnt) = p_{2mn}(\cosh t).$$

Thus, the polynomial $p_m(p_n(x)) - p_{2mn}(x)$ takes the value 0 for infinitely many values of x and, as such, must be the zero polynomial. The desired relation follows.

Our last example is inspired by a problem that appeared in 2004 in *Mathematics Magazine* (problem 1688).

> Let p be an odd prime and let $Q(x)$ be a polynomial of degree $p-1$ with coefficients in $\mathbb{Z}_p$. Show that the mapping $x \mapsto Q(x)$ is not a bijection from $\mathbb{Z}_p$ onto itself.

We propose a solution that makes use of a Lagrange interpolation polynomial. Let us first refresh our memory about this polynomial. Let n be a nonnegative integer and let

$$x_1, x_2, \ldots, x_n, x_{n+1}, y_1, y_2, \ldots, y_n, y_{n+1}$$

be elements of the field F, the x_ks being distinct. Then, there exists a unique element of $F[x]$ of degree less than or equal to n taking the value y_k at x_k for $k = 1, 2, \ldots, n, n+1$.

Indeed, if we define $L_k(x) = \prod_{j=1, j\neq k}^{n+1} (x - x_j)$, then the polynomial

$$L(x) = \sum_{k=1}^{n+1} y_k \cdot \frac{L_k(x)}{L_k(x_k)}$$

is clearly a solution (note that $L_j(x_k) = 0$ if $j \neq k$). In addition, if $P(x)$ is another solution, then $L(x) - P(x)$ is not of degree greater than n and $L(x_k) - P(x_k) = 0$ for $k = 1, 2, \ldots, n+1$; since the x_ks are distinct, we must have $L(x) - P(x) = 0$. Thus, $L(x)$ is the unique solution.

Returning to the problem, let

$$Q(x) = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1},$$

where $a_0, a_1, \ldots, a_{p-1}$ are elements of $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ with $a_{p-1} \neq \overline{0}$ and assume that

$$(Q(\overline{0}), Q(\overline{1}), \ldots, Q(\overline{p-1}))$$

is a permutation of $(\overline{0}, \overline{1}, \ldots, \overline{p-1})$.

The polynomial $Q(x)$ is equal to the Lagrange interpolation polynomial $L(x)$ taking the values $Q(\overline{0}), Q(\overline{1}), \ldots, Q(\overline{p-1})$ at $\overline{0}, \overline{1}, \ldots, \overline{p-1}$, respectively, that is,

$$Q(x) = L(x) = \sum_{k=0}^{p-1} Q(\overline{k}) \cdot \frac{L_k(x)}{L_k(\overline{k})}, \text{ where } L_k(x) = \prod_{j=0, j\neq k}^{p-1} (x - \overline{j}),\ k = 0, 1, \ldots, p-1.$$

Since from Fermat's Little Theorem,

$$x^p - x = x(x-\overline{1})(x-\overline{2})\cdots(x-\overline{p-1}),$$

the polynomial $\sum_{k=0}^{p-1} L_k(x)$ is the derivative of $x^p - x$, which is the constant polynomial $-\overline{1}$; hence, $L_k(\overline{k}) = -\overline{1}$ (recall that $L_j(\overline{k}) = \overline{0}$ if $j \neq k$). As a result,

$$Q(x) = -\sum_{k=0}^{p-1} Q(\overline{k}) L_k(x),$$

and comparing the coefficients of x^{p-1},

$$a_{p-1} = -(Q(\overline{0}) + Q(\overline{1}) + \cdots + Q(\overline{p-1})).$$

Since

$$\{Q(\overline{0}), Q(\overline{1}), \ldots, Q(\overline{p-1})\} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$$

by assumption, we arrive at $a_{p-1} = -(\overline{0} + \overline{1} + \cdots + \overline{p-1})$ and finally at the contradiction $a_{p-1} = \overline{0}$ (since the sum of the roots of $x^p - x$ is $\overline{0}$).

We conclude with two exercises.

Exercises

1. Let $p(x) \in \mathbb{R}[x]$ with $\deg(p(x)) \geq 2$. Prove that the graph of the function p cannot have more than one centre of symmetry.

2. Let n be a positive integer and let $a(x) \in \mathbb{R}[x]$ with $\deg(a(x)) = n$. Find $a(n+1)$ given that $a(k) = \frac{k}{k+1}$ for $k = 0, 1, 2, \ldots, n$,

a) using the polynomial $(x+1)a(x) - x$,

b) using a Lagrange interpolation polynomial.