Polynomials

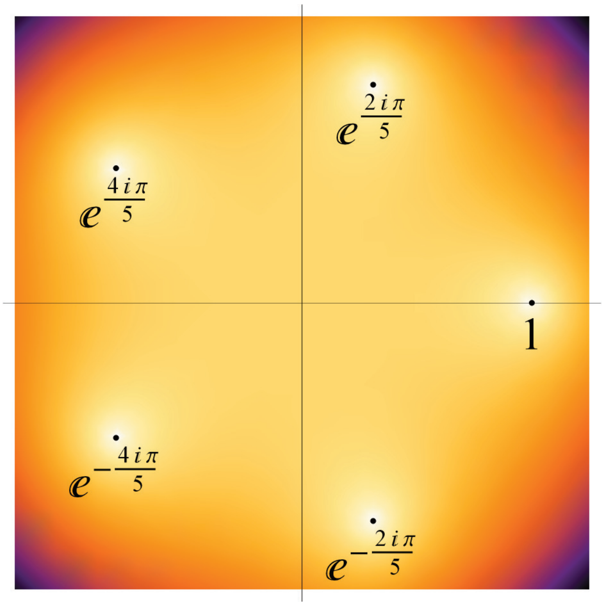
The set of polynomials $\{f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n\}$, where n is a non-negative integer and $\{a_0, a_1, \ldots, a_n\} \subset S$, is denoted $S[x]$ (pronounced 'S adjoin x'). In this chapter, we will explore the cases where S is the set of complex numbers or real numbers.

Complex polynomials, $\mathbb{C}[x]$

Suppose we have a degree-n polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, where $a_0, \ldots, a_n$ are complex constants and a_n is non-zero. According to the *fundamental theorem of algebra*, we can express it as a product of linear factors of the form $x - \alpha_i$, where α_i is a (complex) root of the polynomial.

- If we have a monic polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, where $a_n = 1$, then we can express $f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are (not necessarily distinct) roots of the polynomial. **[Fundamental theorem of algebra]**

For example, the polynomial $x^4 - 1$ can be factorised as $(x - 1)(x + 1)(x + i)(x - i)$, where $i = \sqrt{-1}$ is the imaginary unit. In general, the polynomial $x^n - 1 = (x - 1)(x - \tau)\left(x - \tau^2\right) \ldots \left(x - \tau^{n-1}\right)$, where $\tau = e^{\frac{2\pi i}{n}}$ is a principal nth root of unity. The roots of unity are positioned at the vertices of a regular n-gon with centre 0 and a vertex at 1. The example for $x^5 - 1$ is shown below.



This means that the degree-n curve $y = f(x)$ meets the degree-1 line $y = 0$ in at most n points. There is nothing special about the line $y = 0$, and this also applies to any line. More remarkably, the polynomial curve can be replaced with any algebraic curve (such as the unit circle, $x^2 + y^2 = 1$, which has degree 2). Even more generally, where the line is replaced with another algebraic curve, we have *Bezout's theorem*.

- Suppose P and Q are two curves of degrees m and n, respectively. If they intersect in finitely many points, then they intersect in at most $m\,n$ points. **[Bezout's theorem]**

Equality occurs if we consider intersections on the complex projective plane (instead of the real plane), and count intersections with appropriate multiplicity (*e.g.* twice for tangency, thrice for osculation *et cetera*). The complex projective plane is discussed in later chapters, and it is only necessary at this point to use the weak form of Bezout's theorem.

1. Show that two ellipses intersect in at most four points.

2. Consider the regular n-gon with vertices $A_1, A_2, \ldots, A_n$, where $n \geq 5$. Let P be a variable point on the circumcircle of the n-gon. Show that the value of $f(P) = A_1 P^4 + A_2 P^4 + \ldots + A_n P^4$ remains constant.

Difference of three cubes

A particularly useful polynomial is $x^3 + y^3 + z^3 - 3xyz$. Over the reals, it factorises into $(x+y+z)\left(x^2 + y^2 + z^2 - xy - yz - zx\right)$, and the quadratic term can be further factorised over the complex numbers. This polynomial recurs in many situations, including olympiad problems.

- The polynomial $x^3 + y^3 + z^3 - 3xyz = \det\begin{pmatrix} x & y & z \\ z & x & y \\ y & z & x \end{pmatrix} = (x+y+z)(x+\omega y+\omega^2 z)(x+\omega^2 y+\omega z)$, where ω is a principal cube-root of unity. **[Difference of three cubes]**

This generalises to n variables, instead of merely three. Indeed, the name is derived from the $n = 2$ case, known as the 'difference of two squares', $x^2 - y^2 = \det\begin{pmatrix} x & y \\ y & x \end{pmatrix} = (x+y)(x-y)$.

- $\det\begin{pmatrix} x_0 & x_1 & x_2 & \cdots & x_{n-1} \\ x_{n-1} & x_0 & x_1 & \cdots & x_{n-2} \\ x_{n-2} & x_{n-1} & x_0 & \cdots & x_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & x_3 & \cdots & x_0 \end{pmatrix} = \prod_{r=0}^{n-1}\left(\sum_{r=0}^{n-1}\left(x_r\, e^{2\pi i \frac{k}{n} r}\right)\right).$

The sums in the product on the right-hand side are the terms of the *discrete Fourier transform* of $\{x_0, x_1, \ldots, x_{n-1}\}$. (Continuous) Fourier transforms were originally discovered to explain how the sound of an entire orchestra can be composed of basic sinusoidal waves. Today, this idea is used to analyse electrical circuits. The discrete Fourier transform can be computed quickly using certain algorithms, forming the basis of the fastest known algorithm for multiplying two large integers.

3. Find the minimum value of $x^2 + y^2 + z^2$, where x, y, z are real numbers such that $x^3 + y^3 + z^3 - 3xyz = 1$. **[BMO2 2008, Question 1]**

Cubic equations

For sufficiently small degree, it is possible to solve polynomial equations using *radicals* (nth roots). For the general quadratic equation, the Babylonian technique of 'completing the square' suffices. Solving the cubic equation is a more difficult, multi-step process. If we can immediately find a root α, it is possible to divide by $x - \alpha$ to reduce the equation to a quadratic. Otherwise, more ingenious techniques are required.

4. Suppose we have an equation $a y^3 + b y^2 + c y + d = 0$. Show that this can be converted to an equation of the form $x^3 + px + q = 0$, where x is a linear function of y. **[Reduction to a monic trinomial]**

Hence, it is only necessary to consider the latter case, as all other cubics can be reduced to it.

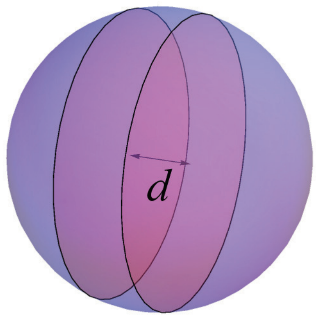
5. Show that $x^3 + px + q = 0$ is equivalent to $x^3 + a^3 + b^3 - 3abx = 0$, where a^3 and b^3 are the roots of the quadratic equation $z^2 - qz - \frac{p^3}{27} = 0$.

6. Hence show that $x^3 + px + q = 0$ has a root

$x = -(a+b) = \sqrt[3]{-\frac{1}{2}q + \sqrt{\frac{1}{4}q^2 + \frac{1}{27}p^3}} + \sqrt[3]{-\frac{1}{2}q - \sqrt{\frac{1}{4}q^2 + \frac{1}{27}p^3}}$. **[General solution to cubic equations]**

The general solution to the cubic equation was the quest of many mediæval mathematicians. After a partial solution by Omar Khayyam, the first complete solution was by Niccolò Tartaglia. However, when the quartic was later solved by Lodovico Ferrari, Tartaglia's solution of the cubic was mistakenly attributed to Gerolamo Cardano, and is thus referred to as *Cardano's formula*. This displeased Tartaglia to a great extent.

Due to the existence of formulae for solving the general quadratic, cubic and quartic equations, people imagined that there might be similar algebraic methods for solving any polynomials using radicals. However, this is not the case. Galois theory demonstrates that it is impossible to solve the general quintic, and of course polynomial equations of higher degree.



7. Two parallel planes cut the sphere of unit radius into three equal volumes. Find a cubic equation in rational coefficients, one root of which is the separation d between the two planes.

Symmetric polynomials

So far, we have mainly considered polynomials in one variable. The difference of three cubes was an exception, as it featured three variables. Indeed, it is what is known as a *symmetric polynomial*, as interchanging any two of the variables leaves the polynomial unchanged. $x^2 - y^2$ is not symmetric, since interchanging x and y negates the value, rather than preserving it. $(x-y)^2$, however, is symmetric.

8. Suppose we have a symmetric polynomial in two variables, x and y. Show that it can be expressed as a polynomial in s and p, where $s = x + y$ and $p = x\,y$.

This is a special case of Newton's theorem of symmetric polynomials:

- Any n-variable symmetric polynomial in $x_1, x_2, \ldots, x_n$ can be expressed as a polynomial in the *elementary symmetric polynomials (ESPs)*, i.e. coefficients of $(x-x_1)(x-x_2)\ldots(x-x_n)$. **[Newton's theorem of symmetric polynomials]**

Proof:

Note that any symmetric polynomial can be multiplied out to yield a sum of terms of the form $k \sum_{\text{sym}} (x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n})$, where the sigma indicates a symmetric sum. We will represent this as $k\,f(a_1, a_2, \ldots, a_n)$.

We assume without loss of generality that $a_1 \geq a_2 \geq \ldots \geq a_n$, and lexicographically order the terms. (Specifically, $f(a_1, a_2, \ldots, a_n)$ precedes $f(b_1, b_2, \ldots, b_n)$ if $a_1 < b_1$, or $a_1 = b_1$ and $a_2 < b_2$, or $a_1 = b_1$ and $a_2 = b_2$ and $a_3 < b_3$, *et* *cetera*.) We then proceed via an inductive argument.

For a given term $k\,f(a_1, a_2, \ldots, a_n)$ of the ordering, assume that all preceding terms can indeed be expressed as polynomials in the ESPs. Suppose that $a_1 = a_2 = \ldots = a_h > a_{h+1}$. We subtract the symmetric polynomial $k\,f(1, 1, \ldots, 1, 0, \ldots, 0)\,f(a_1 - 1, a_2 - 1, \ldots, a_h - 1, a_{h+1}, a_{h+2}, \ldots, a_n)$. Since $f(1, 1, \ldots, 1, 0, \ldots, 0)$ is already an elementary symmetric polynomial, and $f(a_1 - 1, a_2 - 1, \ldots, a_h - 1, a_{h+1}, a_{h+2}, \ldots, a_n)$ is a symmetric polynomial of lower degree than the original expression, the term we have subtracted can be expressed as a polynomial in ESPs. The remainder exclusively contains terms that precede $f(a_1, a_2, \ldots, a_n)$, thus can also be expressed as a polynomial in the ESPs.

9. Given real numbers a, b, c, with $a + b + c = 0$, show that $a^3 + b^3 + c^3 > 0$ if and only if $a^5 + b^5 + c^5 > 0$.
[BMO2 2004, Question 3]

Solutions

1. Ellipses can be represented by quadratic equations in x and y (like all conic sections). As a consequence of Bezout's theorem, they can intersect in no more than $2\times2=4$ points.

2. Consider an arbitrary point Q in general position on the circumcircle of the n-gon, and consider the curve $f(P)=f(Q)$. It is a quartic curve (by definition) and must intersect the circumcircle in $2n$ points (rotations and reflections of Q). Due to Bezout's theorem, a quartic and circle sharing no common component can only intersect in at most 8 points; however, $2n>8$, so the quartic must contain the circle. Hence, all points on the circle satisfy $f(P)=f(Q)$.

3. $x^3+y^3+z^3-3xyz=\det\begin{pmatrix} x & y & z \\ z & x & y \\ y & z & x \end{pmatrix}$ is the volume of the equilateral parallelepiped with vertex $O=(0,0,0)$ and adjacent vertices $A=(x,y,z)$, $B=(y,z,x)$ and $C=(z,x,y)$. Suppose we fix $x^2+y^2+z^2=r^2$, the square of the side length, instead of fixing the volume. If O, A and B are constrained to lie in a plane, then the volume is maximised when $\overrightarrow{OC}$ is a normal to this plane. Hence, the volume is maximised relative to the side length when the parallelepiped is a cube with volume r^3. As such, the minimum value of r^2 for a parallelepiped with unit volume is 1, when $\{x,y,z\}=\{1,0,0\}$.

4. Firstly, we divide by a to obtain $x^3+\frac{b}{a}x^2+\frac{c}{a}x+\frac{d}{a}=0$. Let $y=x+\frac{b}{3a}$. Then, our cubic becomes $\left(y-\frac{b}{3a}\right)^3+\frac{b}{a}\left(y-\frac{b}{3a}\right)^2+y-\frac{b}{3a}+\frac{d}{a}=0$. By using the binomial expansion of the first two terms, the coefficients in y^3 and y^2 are one and zero, respectively.

5. We let $q=a^3+b^3$ and $p=-3ab$. a^3 and b^3 are the roots of $\left(z-a^3\right)\left(z-b^3\right)=0$, which expands to $z^2-\left(a^3+b^3\right)z+a^3b^3=0$. We already have $a^3+b^3=q$, and $a^3b^3=(ab)^3=\left(\frac{-p}{3}\right)^3=-\frac{p^3}{27}$.

6. $x^3+a^3+b^3-3abx=(x+a+b)\left(x+\omega a+\omega^2 b\right)\left(x+\omega^2 a+\omega b\right)=0$ has roots $x=-(a+b)$, $x=-\left(\omega a+\omega^2 b\right)$ and $x=-\left(\omega^2 a+\omega b\right)$. Using the Babylonian formula for solving the quadratic equation gives us the values of a^3 and b^3, whence we can obtain a and b by cube-rooting.

7. The volume enclosed by the two planes is given by $\int_{-\frac{d}{2}}^{\frac{d}{2}}\pi y^2\,dx=\int_{-\frac{d}{2}}^{\frac{d}{2}}\pi\left(1-x^2\right)dx=\pi\left(d-\frac{d^3}{12}\right)$. For this to be $\frac{1}{3}$ of the total volume of the sphere, we have $\pi\left(d-\frac{d^3}{12}\right)=\frac{4}{9}\pi$. This simplifies to $d^3-12d+\frac{16}{3}=0$, one root of which must be the separation between the planes.

8. This is a special case of Newton's theorem of symmetric polynomials, which is proved later in the chapter.

9. We have $a^3+b^3+c^3=3abc$, by the difference of three cubes. Also, $a^2+b^2+c^2=-2ab-2bc-2ca$, since $(a+b+c)^2=0$. We can express $a^5+b^5+c^5$ as $(a+b+c)\left(a^4+b^4+c^4\right)-\sum_{\text{sym}}a^4b$. The first term is zero, so $a^5+b^5+c^5=-\sum_{\text{sym}}a^4b=a^3bc+b^3ca+c^3ab-\left(a^3+b^3+c^3\right)(ab+bc+ca)$. After factorisation, this is then equal to $abc\left(a^2+b^2+c^2\right)-3abc(ab+bc+ca)$, or $\frac{5}{2}abc\left(a^2+b^2+c^2\right)$. Except in the trivial case where all variables are zero, $a^2+b^2+c^2>0$, so $a^3+b^3+c^3$ and $a^5+b^5+c^5$ are positive real multiples of abc, thus both have the same sign.