January 5, 2010

CHAPTER ONE

ROOTS OF POLYNOMIALS

§1. THE CUBIC AND QUARTIC CASES

Polynomials have long been the subject of mathematical investigation. For over a thousand years, linear and quadratic equations have been studied, and by the sixteenth century, there was active interest in solving equations of higher degree. In that century, it was demonstrated that, if one allowed the use of complex numbers, then the solutions of cubic and quartic polynomial equations could be described in terms of square and cube roots of terms involving the coefficients.

Experience with equations of low degree strongly suggested that a polynomial equation $p(z) = 0$ of any positive degree possessed a complex *root*, *i.e.*, a number w that satisfies $p(w) = 0$. Such a number is said to be a *zero* of the polynomial $p(z)$. A natural way to prove this would be to derive general formulas involving radicals and coefficients. For the linear equation $ax + b = 0$, the solution is given by $x = -b/a$, while for the quadratic $ax^2 + bx + c = 0$, the formula for the solution is $x = \frac{1}{2a}(-b \pm \sqrt{b^2 - 4ac})$. More complicated formulae of this type can be derived for equations of degrees 3 and 4.

This proved to be unsuccessful for polynomials of degree exceeding 4, although mathematicians were certain that such polynomial equations had a root. Finally, in the nineteenth century, the situation was clarified. Gauss provided an argument that every polynomial had at least one complex zero and Galois showed that one cannot solve a general polynomial equation by radicals.

In this section, we will look at a couple of interesting approaches to the cubic equation before examining an eighteenth century approach to the quartic that seemed to suggest a route to showing that every polynomial had at least one complex zero.

In the case of both the cubic and the quartic, by making a linear change of variable, one need only consider the forms $x^3 + px + q = 0$ and $x^4 + ax^2 + bx + c = 0$. The cubic case often exploits the interesting identity:

$$(u + v)^3 - 3uv(u + v) - (u^3 + v^3) = 0 \ .$$

If we compare this to the equation $x^3 + px + q = 0$, this suggests the strategy of trying to make $x = u + v$, $p = -3uv$, $q = -(u^3 + v^3)$. Since p and q are given, we have to solve the system

$$u^3 + v^3 = -q \qquad \text{and} \qquad u^3 v^3 = -p^3/27 \ ,$$

for u^3 and v^3. These turn out to be the roots of the quadratic $t^2 + qt - p^3/27 = 0$. Having solved this, we have to match up the cube roots of u^3 and v^3 to satisfy $p = -3uv$, and then $x = u + v$ will satisfy the equation.

Here is another approach that depends on a comparison of forms. Beginning with the equation $x^3 + px + q = 0$, we make the substitution $x = y \cos\theta$ to obtain

$$\cos^3\theta + \frac{p}{y^2}\cos\theta + \frac{q}{y^3} = 0 \ . \tag{1.1}$$

However, we note the identity

$$\cos^3\theta - \frac{3}{4}\cos\theta - \frac{1}{4}\cos 3\theta = 0 \ . \tag{1.2}$$

Hence $p/y^2 = -3/4$ and $q/y^3 = -\cos 3\theta/4$, so that $y^2 = -(4p/3)$ and $\cos 3\theta = -(4q/y^3)$.

Trying this on the example $x^3 - 3x - 1 = 0$ leads to $y = 2$ and $\cos 3\theta = 1/2$, whence $3\theta \equiv \pi/3, 5\pi/3 \pmod{2\pi}$. The solutions are

$$x = 2\cos(\pi/9) = 1.87938\ldots \qquad x = 2\cos(5\pi/9) = -0.34729\ldots \qquad x = 2\cos(7\pi/9) = -1.53209\ldots .$$

The justification of this is a little subtle, as (1.1) is a conditional equation and (1.2) is an identity. However, we first choose y to make $p/y^2 = -3/4$ and then choose θ to satisfy the remaining condition.

As for the quartic, one of the first mathematicians to make a serious assault on the Fundamental Theorem of Algebra, albeit an unsuccessful one, was Leonhard Euler. Around 1750, he published a paper [**4**] in which he sought to obtain the result that every polynomial with real coefficients can be written as the product of real linear and quadratic factors. He pointed out that it is enough to show the result for polynomials of degree 2^m for positive integer m (you can make the initial coefficients vanish to get the other degrees) and tried an induction argument.

Here is how to handle the case of quartics. As noted, we need consider only the type $x^4 + ax^2 + bx + c$. Suppose first that $b = 0$. Then either $a^2 - 4c \geq 0$, in which case we can obtain a real factorization $x^4 + ax^2 + c = (x^2 - h)(x^2 - k)$, or $a^2 - 4c < 0$, in which case $c > 0$ and we can write

$$x^4 + ax^2 + c = (x^2 + \sqrt{c})^2 - (2\sqrt{c} - a)x^2$$

and factor a difference of squares over the reals.

Now suppose that $b \neq 0$. Then we try a factorization with undetermined coefficients:

$$x^4 + ax^2 + bx + c = (x^2 + ux + r)(x^2 - ux + s) = x^4 + (r + s - u^2)x^2 + u(s - r)x + rs \ .$$

Comparing coefficients, we find that $a = r + s - u^2$, $b = u(s - r)$ and $c = rs$, whence $s + r = a + u^2$ and $s - r = b/u$. Thus,

$$4c = 4rs = \left(a + u^2 + \frac{b}{u}\right)\left(a + u^2 - \frac{b}{u}\right)$$

$$\Longrightarrow u^6 + 2au^4 + (a^2 - 4c)u^2 - b^2 = 0 \ .$$

By the Intermediate Value Theorem, this equation in u^2 has a real positive solution, so we can find a real value of u, hence of r and s to get the desired factorization of the quartic.

Note, in passing, that we can settle the case of the quintic polynomial quickly. Being a polynomial of odd degree, it has a real zero and therefore, by the Factor Theorem, a linear factor. Therefore, it has also a quartic factor, which can be factored as a product of linear and quadratic polynomials.

We move to the case of the octic equation where $m = 3$. We look for a factorization

$$x^8 + ax^6 + bx^5 + cx^4 + dx^3 + ex^2 + fx + g = (x^4 + ux^3 + px^2 + qx + r)(x^4 - ux^3 + sx^2 + tx + v) \ .$$

Comparing coefficients promises to lead to a real mess, so let us look back at the quartic for inspiration in cutting through the difficulties.

In the quartic situation, we found that application of the Intermediate Value Theorem turned on recognizing that the constant coefficient of the equation in u^2 was negative from actually determining this coefficient. Is there an alternative way to see its negativity?

Suppose that

$$(x^2 + ux + r)(x^2 - ux + s) = (x - \alpha)(x - \beta)(x - \gamma)(x - \delta) \ ,$$

where $\alpha, \beta, \gamma, \delta$ are zeros of the quartic. Observe that u equals the sum of two of the zeros; the six ways of selecting pairs of zeros of the quartic correspond to the degree of the equation in u. Moreover, since $\alpha + \beta + \gamma + \delta = 0$, the sum of any pair of zeros is equal to the negative of the sum of the other pair, so that the six possible values of u come in opposite sign pairs $\rho_1, -\rho_1, \rho_2, -\rho_2, \rho_3, -\rho_3$. Hence, the equation for u must have the form

$$(u^2 - \rho_1^2)(u^2 - \rho_2^2)(u^2 - \rho_3^2) = 0 \ .$$

Since there are three factors, the constant coefficient is negative. We can apply the Intermediate Value Theorem as before to show that there must be a positive real value of u satisfying this equation.

Turning to the octic, we can take u to be the sum of four of its zeros. There are $\binom{8}{4}$ possible ways of selecting theses zeros, and as the sum of the roots is 0, the choices come in opposite pairs. Hence u turns out to be a root of an equation of the form $\prod(u^2 - r^2) = 0$, where the product is taken over $\frac{1}{2}\binom{8}{4} = 35$ factors. Thus the constant term is negative and we can find a positive value for u and obtain the factorization of the octic into two quartics; each of the quartics can then be factored into quadratic and linear factors.

Assume, as an induction hypothesis, that we can effect a factorization into real linear and quadratic factors for any polynomial of degree 2^i, where $1 \le i \le m-1$. For a given polynomial of degree 2^m whose next-to-leading coefficient is 0, we attempt a factorization

$$x^{2^m} + ax^{2m-2} + bx^{2m-3} + \cdots = (x^{2^{m-1}} + ux^{2^{m-1}-1} + \cdots)(x^{2^{m-1}} - ux^{2^{m-1}-1} + \cdots) \ ,$$

where u is the sum of 2^{m-1} of the zeros. Since the sum of all the zeros is 0, we can argue, as before, that u satisfies an equation of the form $\prod_{1\le j\le k}(u^2 - r_j^2) = 0$ where $k = \frac{1}{2}\binom{2^m}{2^{m-1}}$, this number being odd. Thus, we can, as before, find a value of u to satisfy the equation and then determine the other coefficients of the two factors. By the induction hypothesis, these two factors can be factored as a product of linear and quadratic polynomials.

However, as we know, a proof of the Fundamental Theorem of Algebra, of which this is the real manifestation, had to wait for another half century. There is an error in Euler's argument. Where is it? The difficulty arises in that we do not know whether the roots r that occur in the product are real or nonreal. This did not matter for the quartic, as we could rely on an alternative expression for the constant coefficient. However, if any of the roots r_j were nonreal for the higher degree cases, then we cannot guarantee that the product of the terms $-r_j^2$ is negative, even though there are an odd number of factors.

Note. The attempt to solve equations by radicals has given rise to a lot of ingenuity. It is worth noting one interesting idea, that of expressing the roots in terms of parameters and roots of unity. Suppose that the roots of the cubic equation $x^3 + ax^2 + bx + c = 0$ are of the form $\alpha + \beta + \gamma$, $\alpha + \beta\omega + \gamma\omega^2$ and $\alpha + \beta\omega^2 + \gamma\omega$, where $\omega = \frac{1}{2}(-1 + \sqrt{3}i)$ is an imaginary cube root of unity and α, β, γ are three numbers that satisfy $3\alpha = -a$, $3\alpha^2 - 3\beta\gamma = b$ and $\alpha^3 + \beta^3 + \gamma^3 - 3\alpha\beta\gamma = -c$. From these equations, $\beta^3 + \gamma^3$ and $\beta^3\gamma^3$ can be determined in terms of the coefficients a, b, c and so found by solving a quadratic equation.

A similar procedure can be implemented with the quartic equation. If the roots of the quartic equation $x^4 + ax^3 + bx^2 + cx + d = 0$ are taken to be $\alpha + \beta + \gamma + \delta$, $\alpha + \beta - \gamma - \delta$, $\alpha - \beta + \gamma - \delta$ and $\alpha - \beta - \gamma + \delta$, we find that $4\alpha = -a$, $6\alpha^2 - 2(\beta^2 + \gamma^2 + \delta^2) = b$, $4\alpha^3 - 4\alpha(\beta^2 + \gamma^2 + \delta^2) + 8\beta\gamma\delta = -c$ and $\alpha^4 + (\beta^2 + \gamma^2 + \delta^2)^2 - 2\alpha^2(\beta^2 + \gamma^2 + \delta^2) - 4(\beta^2\gamma^2 + \beta^2\delta^2 + \gamma^2\delta^2) + 8(\alpha\beta\gamma\delta) = d$. These can be solved for the three elementary symmetric polynomials in β^2, γ^2, δ^2 in terms of the coefficients of the quartic, from which β^2, γ^2 and δ^2 can be found as the roots of a cubic equation.

This sort of manoeuvre that reduces the solution of a polynomial equation to the solution of an equation of a lower degree (and the extraction of roots) does not work for degrees exceeding 4, as such attempts lead to polynomial equations of higher degree. In the case of the cubic and quartic, we are led to equations of degree 6. This is masked, because for both the cubic and quartic, we can solve them in two steps, for the cubic, by solving a quadratic for the cubes of the variables, and for the quartic, by solving a cubic for the squares of the variable. The situation for the quintic is spelled out in [**5**, p. 15].

§2. THE FUNDAMENTAL THEOREM OF ALGEBRA

The **Fundamental Theorem of Algebra** states that, *if $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ has complex coefficients a_i, then $p(z)$ has at least one complex zero.*

Before proving this, let us look at an important consequence. Recall that the Remainder Theorem provides that, if $p(z)$ is any polynomial of positive degree over $\mathbf{C}$ (*i.e.*, with complex coefficients) and w is

any complex number, then $p(z) = q(z)(z-w) + p(w)$, for some polynomial $q(z)$. In particular, w is a zero of the polynomial if and only if $z - w$ divides the polynomial. It follows from this and the Fundamental Theorem of Algebra that

$$p(z) = \prod_{i=1}^{k} (z - r_i)^{n_i}$$

where $k \leq n$, $r_1, r_2, \cdots, r_k$ are all the zeros of $p(z)$ and the n_i are positive integers for which $n_1 + n_2 + \cdots + n_k = n$, the degree of $p(z)$. The number n_i is called the *multiplicity* of the zero r_i. By convention, any complex number that is not a zero of $p(z)$ is said to be a zero of multiplicity 0.

Algebraically, the Fundamental Theorem says that each polynomial over $\mathbf{C}$ can be written as a product of linear factors. Call a polynomial *irreducible* if and only if its degree is positive and it cannot be written as a product of more than one polynomial of positive degree; irreducible polynomials are the analogues of primes for integers. Thus, the set of polynomials irreducible over $\mathbf{C}$ coincides with the set of linear polynomials. In the case of polynomials over $\mathbf{R}$, the set of irreducibles consists of all linear polynomials and quadratic polynomials with negative discriminant.

We observe, also, that the Fundamental Theorem implies that for any complex number w, the equation $p(z) = w$ is always solvable, so that any polynomial $p(z)$ maps the complex plane onto itself.

There are many ways of proving the Fundamental Theorem. Two of the shortest proofs rely on deep results from the theory of complex variables [**1**, p. 14-15]. Liouville's Theorem provides that any bounded complex function that is analytic everywhere in the complex plane must be constant. Suppose, if possible, that a polynomial of positive degree fails to have a zero. Then its reciprocal $1/p(z)$ must be defined, bounded and analytic everywhere in the plane, and so be constant. But this is a contradiction.

The second argument relies on Rouché's Theorem: *Suppose that the polynomials p and q satisfy the condition*

$$|p(z) - q(z)| < |q(z)|$$

for z belonging to a closed path in the plane. Then $p(z)$ and $q(z)$ have the same number of zeros counting multiplicity within the region surrounded by the path.

We compare the monic polynomial $p(z)$ to $q(z) = z^n$, a polynomial with a single zero of multiplicity n at the origin. Let $a = \max |a_i|$. Then, on the circle described by $|z| = 1 + a$,

$$\begin{aligned} |p(z) - q(z)| &= |a_{n-1}z^{n-1} + \cdots + a_1 z + a_0| \leq a(|z|^{n-1} + \cdots + |z| + 1) \\ &= a\left(\frac{|z|^n - 1}{|z| - 1}\right) = |z|^n - 1 < |z|^n = |q(z)| \ , \end{aligned}$$

and the desired result follows. In fact, we have the additional information that $p(z)$ has no zeros on or outside of the circle centred at the origin with radius $1 + a$.

A third proof avoids this powerful machinery by exploiting the topology of the plane. Observe that $p(z)$ is a continuous function of z. For each constant M, there is a value of R for which $|p(z)| > M$ when $|z| > R$. Therefore, there is a point w in the complex plane for which $|p(w)| \leq |p(z)|$ for each complex z.

Suppose that v is a complex number for which $|p(v)| > 0$. Then there is a complex number u for which $|p(u)| < |p(v)|$. To see this, write $q(z) = p(v + z)$. We have that $q(z) = b_0 + \sum_{i=1}^{n} b_i z^i$ with $b_0 \neq 0$. We have that

$$|q(z)| \leq |b_0 + b_k z^k| + |z^k||b_{k+1}z + \cdots + b_n z^{n-k}|$$

for every complex z, where k is the smallest positive exponent for which the coefficient b_k of z^k is nonzero. (If $n = k$, there is no second term in the right member.) By continuity, we can select z small enough to make the absolute value of

$$|b_{k+1}z + \cdots + b_n z^{n-k}|$$

less than $\frac{1}{2}|b_k|$ and $|b_k z^k| < |b_0|$. Now choose z so that the complex numbers b_0 and $b_k z^k$ are opposite (*i.e.*, one is a negative real multiple of the other), so that

$$|b_0 + b_k z^k| = |b_0| - |b_k||z^k| \ .$$

Then, for such z, $|q(z)| \leq |b_0| - |b_k||z^k| + \frac{1}{2}|b_k||z^k| < |b_0| = |q(0)|$.

It follows from this that $p(w)$ must vanish and we obtain the result. □

As for many fundamental theorems, there is a variety of approaches and many proofs in the literature, such as [**2**]. . For an interesting topological group theoretic approach, consult [**6**].

§3. PROBLEMS AND INVESTIGATIONS

1. Suppose that a is a parameter not equal to 0 nor 1. Determine all the roots of the equation

$$\frac{x^2 - x + 1)^3}{x^2(x-1)^2} = \frac{a^2 - a + 1)^3}{a^2(a-1)^2} \ .$$

2. Solve the equation

$$x^2 + \left(\frac{x}{x+1}\right)^2 = 1 \ .$$

3. Suppose that $p(x)$ is a polynomial with rational coefficients for which there are r real values of x for which $p(x) = 1$ and s real values of x for which $p(x) = -1$. What is the minimum possible degree of p?

Hints and Comments

1. Let $f(x)$ denote the left side of the equation. What is $f(1-x)$ and $f(1/x)$?

2. Set $u = x + 1$.

3. Without loss of generality, one can assume that $r \geq s$. Then the degree of p must be at least r? Is it possible, for all values of r and s with $r \geq s$ to find a polynomial of degree r that fills the bill? For example, consider the polynomials $\frac{1}{3}(2x^2 - 5)$, $\frac{1}{6}(-x^3 + 7x)$, $1 + \frac{1}{360}(x^2 - 1)(x^2 - 64)$.

References

1. P. Borwein & T. Erdélyi, *Polynlmials and polynomial inequalities.* Springer, 1995
2. Theo de Jong, Lagrange multipliers and the Fundamental Theorem of Algebra. *American Mathematical Monthly* 116:9 (November, 2009), 828-830
3. William Dunham, Euler and the fundamental theorem of algebra. *College Math. J.* 22:4 (September, 1991), 282-293
4. Leonhard Euler, Recherches sur les racines imaginaires des équations. *Mémoires de l'académie des sciences de Berlin* (1749/1751), 222-288 = *Opera Omnia* (1) 6, 78-147 (see especially pp. 93-106)
5. G.V. Milovanović, D.S. Matrinović & Th. M. Rassias, *Topics in polynomials.* Springer, 1994
6. José Carlos de Sousa Oliveira Santos, Another proof of the Fundamental Theorem of Algebra. *American Mathematical Monthly* 112:1 (January, 2005), 76-78