SOLVING POLYNOMIAL EQUATIONS

FRANZ LEMMERMEYER

1. Cubic Equations

Consider $x^3 + ax^2 + bx + c = 0$. Using the same trick as above we can transform this into a cubic equation in which the coefficient of x^2 vanishes: put $x = y - \frac13 a$; then

$$\begin{aligned} 0 &= x^3 + ax^2 + bx + c \\ &= \big(y - \frac{1}{3}a\big)^3 + a\big(y - \frac{1}{3}a\big)^2 + b\big(y - \frac{1}{3}a\big) + c \\ &= y^3 + y\big(b - \frac{1}{3}a^2\big) + c - \frac{ab}{c} + \frac{2}{27}a^3. \end{aligned}$$

If we can solve the cubic equation in y, then $x = y - \frac13 a$ gives the solution of the original equation in x.

Thus assume that

$$y^3 + py + q = 0. \tag{1}$$

Note that $(u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = 3uv(u+v) + (u+v)^3$; if we could find numbers u and v such that $3uv = -p$ and $u^3+v^3 = -q$, then $(u+v)^3 = -p(u+v) - q$, hence $y = u + v$ is a solution of the cubic in question.

From $3uv = -p$ we get $u^3v^3 = -(p/3)^3$. This if we put $r = u^3$ and $s = v^3$, then $rs = (-p/3)^3$ and $r + s = u^3 + v^3 = -q$, showing that r and s are roots of the quadratic equation $z^2 + qz - (p/3)^3 = 0$. Solving this quadratic equation shows that

$$u^3 = -\frac{q}{2} + \sqrt{\big(\frac{q}{2}\big)^2 + \big(\frac{p}{3}\big)^3} \tag{2}$$

$$v^3 = -\frac{q}{2} - \sqrt{\big(\frac{q}{2}\big)^2 + \big(\frac{p}{3}\big)^3} \tag{3}$$

(or the other way around; but since we are interested only in $u + v$, interchanging u and v doesn't change anything).

The equation (2) for u^3 can be solved easily: just as $x^2 = d$ has the two solutions $x = \pm\sqrt{d}$, the cubic $u^3 = d$ has the three solutions $u = \sqrt[3]{d}$, $u = \rho\sqrt[3]{d}$, $u = \rho^2\sqrt[3]{d}$, where $\rho = \frac12(-1 + \sqrt{-3}\,)$ is a primitive third root of unity. Thus we have 9 pairs of numbers (u, v) satisfying (2) and (3). Not all of these combinations give rise to solutions $y = u + v$ of the cubic (1): u and v also have to satisfy $uv = -p/3$. Thus pick any cube root u (there are three possibilities); then v is uniquely determined by $v = -p/3u$ (note that, if $u = 0$, then $p = 0$, and in this case the solution of the cubic is trivial), and for each of the three possibilities for u we get a solution $y = u + v$ of the cubic (1).

Example 1. Take $y^3-3y+2=0$. Then $p=-3$, $q=2$, hence $D=(q/2)^2+(p/3)^3=1-1=0$, hence $u=\sqrt[3]{q/2}=-1$ and $v=-p/3u=-1$ give $y=u+v=-2$ as the first solution; the other two solutions are given by $y=-\rho-\rho^2=1$ and $y=-\rho^2-\rho=1$, and in fact $y^3-3y+2=(y+2)(y-1)^2$.

Example 2. $y^3-6y+4=0$; then $p=-6$, $q=4$, $D=-4$, so we have to solve $u^3=-2+2i$; we find $u=1+i$, hence $v=-p/3u=1-i$, and we find $u+v=2$, $u\rho+v\rho^2=-1-\sqrt{3}$ and $u\rho^2+v\rho=-1+\sqrt{3}$. In fact, $y^3-6y+4=(y-2)(y^2+2y-2)$.

Example 3. Consider the cubic y^3-7y+6; here $p=-7$ and $q=6$, so $u^3=-3+\frac{1}{9}\sqrt{-300}=\frac{1}{27}(-81+30\sqrt{-3}\,)$. Now we have to guess a cube root of the complex number in the brackets. This can be simplified by observing that $3\sqrt{-3}=-(\sqrt{-3}\,)^3$: we find

$$u^3=\frac{3\sqrt{-3}}{27}(10-9\sqrt{-3}\,). \tag{4}$$

Now $10-9\sqrt{-3}=(a+b\sqrt{-3}\,)^3$ gives $10=a^3-9ab^2=a(a^2-9b^2)$ and $-9=b(3a^2-b^2)$. If a and b are integers, then the first equation shows that $a\mid 2$, the second that $b\mid 3$. A little calculation readily gives $a=-2$ and $b=-1$ as a solution. Thus $u=\frac{\sqrt{-3}}{3}(-2-\sqrt{-3}\,)=\frac{1}{3}(3-2\sqrt{-3}\,)$ and $v=\frac{1}{3}(3+2\sqrt{-3}\,)$, hence $y=u+v=2$.

In fact, $y^3-7y+6=(y-1)(y-2)(y+3)$. Where do the other solutions come from? The come from the other solutions of the pure cubic equation (4). Just as $x^2=1$ has the two solutions $x=+\sqrt{1}=1$ and $x=-\sqrt{1}=-1$, the cubic $x^3=1$ has the three solutions $x=1$, $x=\omega$ and $x=\omega^2$, where $\omega=\frac{-1+\sqrt{-3}}{2}$ and $\omega^2=\frac{-1-\sqrt{-3}}{2}$. This is easily seen by solving $x^3-1=(x-1)(x^2+x+1)=0$.

Thus if u is a particular solution of (4), then so are $u\omega$ and $u\omega^2$; in our case, we find

$$u=\frac{3-2\sqrt{-3}}{3},\quad u\omega=\frac{3+5\sqrt{-3}}{6},\quad u\omega^2=\frac{-9-\sqrt{-3}}{6}.$$

In order to compute y, we also need to compute v; since $uv=-p/3$, the value of v is uniquely determined: we cannot just choose any root of (3)! We find

$$v=\frac{7}{3u}=\frac{3+2\sqrt{-3}}{3},\quad v\omega^2=\frac{7}{3u\omega}=\frac{3-5\sqrt{-3}}{6},\quad v\omega=\frac{7}{3u\omega^2}=\frac{-9+\sqrt{-3}}{6}.$$

Thus $u+v=2$, $u\omega+v\omega^2=1$, and $u\omega^2+v\omega=3$.

Note that even if the cubic has three real solutions, the formulas for the roots involve complex numbers! This is fundamentally different from the quadratic case, where real roots occur if and only if there are no complex numbers in the formula.

2. Ferrari's Method

Consider the equation

$$x^4 + ax^3 + bx^2 + cx + d = 0. \tag{5}$$

Ferrari's idea was to add $(ex + f)^2$ on both sides and determine e and f in such a way that the left hand side becomes a square. We find

$$x^4 + ax^3 + (b + e^2)x^2 + (c + 2ef)x + d + f^2 = (ex + f)^2.$$

We want the left hand side to equal

$$(x^2 + px + q)^2 = x^4 + 2px^3 + (p^2 + 2q)x^2 + 2pqx + q^2.$$

Comparing coefficients yields

$$2p = a, \quad p^2 + 2q = b + e^2, \quad 2pq = c + 2ef, \quad q^2 = d + f^2.$$

The first equation determines p. The second and fourth equations give $e^2 = p^2 + 2q - b$ and $f^2 = q^2 - d$; plugging these into the square of the third equation shows

$$(2pq - c)^2 = 4e^2f^2 = 4(p^2 + 2q - b)(q^2 - d),$$

or, after replacing $2p$ by a,

$$(aq - c)^2 = (a^2 + 8q - 4b)(q^2 - d). \tag{6}$$

But this is a cubic equation in q, which can be solved using Cardano's formula. Once we know p and q, the equation

$$(x^2 + px + q)^2 = (ex + f)^2$$

can easily be solved by taking square roots and solving the resulting quadratic equation for x.

The explicit form of the cubic equation (6) is

$$8q^3 - 4bq^2 + 2(ac - 4d)q - (a^2 - 4b)d - c^2 = 0.$$

Substituting $2q = y$ this gives

$$y^3 - by^2 + (ac - 4d)y - (a^2 - 4b)d - c^2 = 0.$$

Example. Consider $x^4+x^3+x^2+x+1 = 0$. The cubic resolvent is $y^3-y^2-3y+2 = (y - 2)(y^2 + y - 1)$. Thus we may take $2q = y = 2$ or $q = 1$, and $p = \frac{1}{2}$. We also find $e^2 = p^2 + 2q - b = \frac{1}{4} + 2 - 1 = \frac{5}{4}$, $f^2 = q^2 - d = 0$, hence we may take $e = \frac{1}{2}\sqrt{5}$ and $f = 0$. This gives

$$(x^2 + \frac{1}{2}x + 1)^2 = \frac{5}{4}x^2,$$

hence $x^2 + \frac{1}{2}x + 1 = \pm\frac{1}{2}\sqrt{5}x$. Thus we have to solve the quadratic

$$x^2 + \frac{1 \mp \sqrt{5}}{2}x + 1 = 0.$$

We find

$$x_{1,2} = \frac{\frac{-1+\sqrt{5}}{2} \pm \sqrt{\frac{-5-\sqrt{5}}{2}}}{2}, \quad x_{3,4} = \frac{\frac{-1-\sqrt{5}}{2} \pm \sqrt{\frac{-5+\sqrt{5}}{2}}}{2}.$$

3. Palindromic Polynomials

A polynomial $x^n + a_{n-1}x^{n-1} + \ldots + a_0$ of even dregree $n = 2m$ is called palindromic if $a_j = a_{n-j}$ for all j. The quartic above is palindromic and therefore can be solved without Ferrari's method. The standard trick is to divide through by x^m and then substitute $y = x + \frac{1}{x}$. For (5) we find $0 = x^2 + x + 1 + x^{-1} + x^{-2} = 1 + y + (y^2 - 2)$ because $y^2 = x^2 + x^{-2} + 2$. The resulting equation $y^2 + y - 1$ has the solutions $y_{1,2} = \frac{-1 \pm \sqrt{5}}{2}$, and plugging these values into $y = x + \frac{1}{x}$ gives two quadratic equations whose roots are the roots of (5).

Similarly, we can solve the equation $\frac{x^7-1}{x-1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$; observe that $y^3 = x^3 + x^{-3} + 3x + 3x^{-1} = x^3 + x^{-3} + 3y$, hence $x^3 + x^{-3} = y^3 - 3y$; thus we find

$$\begin{aligned} 0 &= x^3 + x^2 + x + 1 + x^{-1} + x^{-2} + x^{-3} \\ &= y^3 - 3y + y^2 - 2 + y \\ &= y^3 + y^2 - 3y - 2 \end{aligned}$$

Plugging the three solutions of this cubic into $y = x + \frac{1}{x}$ gives the 6 solution of the original sextic.

Vandermonde used this trick to reduce the equation $\frac{x^{11}-1}{x-1} = 0$ of degree 10 to an equation of degree 5, which he then managed to solve. The general equation $\frac{x^n-1}{x-1} = 0$ was solved by Gauss.

4. Timeline: From Cardano to Galois

1629 Girard claims that equations of degree n have n roots; this is called the fundamental theorem of algebra.

1637 Descartes repeats this claim, distinguishing between real (true roots and false roots, that is, positive and negative roots) and imaginary roots.

1702 Leibniz claims that the quartic polynomial $x^4 + c^4$ cannot be factored into two quadratic polynomials with real coefficients, and therefor is not the product of four linear polynomials with complex coefficients.

1742 Euler shows that Leibniz was wrong by observing

$$x^4 + c^4 = (x^2 + c^2)^2 - 2x^2c^2 = (x^2 + c^2 - \sqrt{2}\,xc)(x^2 + c^2 + \sqrt{2}\,xc),$$

and any quadratic factors into two linear factors over the complex numbers. In particular, this implies that

$$\sqrt{i} = \frac{1+i}{\sqrt{2}}.$$

1746 D'Alembert attempted to prove the fundamental theorem of algebra. 1749, Euler attempts to prove that every real polynomial of degree n has exactly n complex roots. Lagrange observes gaps in Euler's proof and closes some of them in 1772, and in 1795 Laplace attempts a proof.

1770 Vandermonde solves the equation $x^{11} = 1$ using radicals and claims without proof that his method works for all equations $x^n = 1$.

1799 Gauss in his dissertation gives a new proof of the FTA, but even his proof is nowadays not regarded as complete. Gauss gave three more proofs, the last one in 1849.

1799 Ruffini publishes a book in which he tries to proof that, in general, quintics cannot be solved by radicals. In 1801, he sends a copy to Lagrange, but gets no answer. He sends him a second copy and did not get a reply. In 1802, he sends him a third copy. Ruffini publishes improved versions of his proof in 1808 and 1813. Among the first rank mathematicians, only Cauchy accepted the proof.

1821 Abel claims to have solved the quintic and submits an article to Degen. Degen asks for an example, and when Abel started working on it, he realized his error.

1824 Abel proves that the general quintic cannot be solved by radicals. At that time he knew about the work of Cauchy, who knew Ruffini's work. Afterwards, Abel turns to studying elliptic integrals, and at the end of his short life returns to the theory of equations by proving that polynomials with 'abelian Galois group' can be solved by radicals (of course he used neither 'abelian' nor 'Galois' nor 'group').

1832 Galois shows that a polynomial can be solved by radicals if and only if its Galois group is 'solvable'. His results were published later by Liouville and made it into the first textbooks in algebra in the 1860s.