Conference Applications of Mathematics 2015, in honor of the birthday anniversaries of Ivo Babuška (90), Milan Práger (85), and Emil Vitásek (85)
J. Brandts, S. Korotov, M. Křížek, K. Segeth, J. Šístek, T. Vejchodský (Eds.)
Institute of Mathematics CAS, Prague 2015

WHY QUINTIC POLYNOMIAL EQUATIONS ARE NOT SOLVABLE IN RADICALS

Michal Křížek[1], Lawrence Somer[2]

[1] Institute of Mathematics, Academy of Sciences
Žitná 25, CZ – 115 67 Prague 1, Czech Republic
krizek@math.cas.cz

[2] Department of Mathematics, Catholic University of America
Washington, D.C. 20064, USA
somer@cua.edu

Abstract: We illustrate the main idea of Galois theory, by which roots of a polynomial equation of at least fifth degree with rational coefficients cannot general be expressed by radicals, i.e., by the operations $+$, $-$, $\cdot$, $:$, and $\sqrt[n]{\cdot}$. Therefore, higher order polynomial equations are usually solved by approximate methods. They can also be solved algebraically by means of ultraradicals.

Keywords: Galois theory, finite group, permutation, radical

MSC: 20D05, 13B05, 65H05

1. A brief historical survey

A classic problem in mathematics has been to solve polynomial equations with rational coefficients in terms of its coefficients by means of the operations $+$, $-$, $\cdot$, $:$, and $\sqrt[n]{\cdot}$ (this is the radical symbol and involves taking nth roots). For example, we can solve the quadratic equation

$$ax^2 + bx + c = 0, \quad a, b, c \in \mathbb{R},\ a \neq 0,$$

by the well-known quadratic formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{1}$$

In the early to mid-1500s, solutions to the cubic and quartic equations by means of radicals were given by the Italian mathematicians Scipione del Ferro, Niccolo Tartaglia, Antonio Fiore, Gerolamo Cardano, and Lodovico Ferrari. In 1545, Cardano published an account of solutions of cubic and quartic equations by radicals in

Ars Magna [4]. By a suitable linear transfomation any cubic polynomial equation with real coefficients can be reduced to the form

$$x^3 + bx + c = 0,$$

for which Cardano proposed the following solution

$$x = \sqrt[3]{-\frac{c}{2} + \sqrt{\left(\frac{c}{2}\right)^2 + \left(\frac{b}{3}\right)^3}} - \sqrt[3]{\frac{c}{2} + \sqrt{\left(\frac{c}{2}\right)^2 + \left(\frac{b}{3}\right)^3}}.$$

For instance, the equation

$$x^3 + 9x - 26 = 0$$

implies that

$$x = \sqrt[3]{13 + \sqrt{13^2 + 3^3}} - \sqrt[3]{-13 + \sqrt{196}} = \sqrt[3]{27} - \sqrt[3]{1} = 2,$$

and thus this root can be separated:

$$x^3 + 9x - 26 = (x - 2)(x^2 + 2x + 13) = 0.$$

By (1), the remaining two roots are $x = 1 \pm \mathrm{i}2\sqrt{3}$.

Note that by a sophisticated transformation the solution of a quartic polynomial equation can be reduced to the solution of a cubic polynomial equation (see [13, p. 42]).

For centuries, it was an open question whether there existed a solution to the general quintic (fifth degree) equation by radicals. This question was settled in the negative by the Norwegian mathematician Niels Henrik Abel in 1824 (see [1, 2, 3]).

In this paper, we show that the equation

$$f(x) = 2x^5 - 10x + 5 = 0 \tag{2}$$

is not solvable by radicals [8].

We note that the derivative $f'(x) = 10x^4 - 10$ has exactly two real roots ± 1. Moreover, $f''(x) = 40x^3$ and the second derivative test of elementary calculus shows that f has one positive relative maximum at $x = -1$, one negative relative minimum at $x = 1$, and one point of inflection at $x = 0$. It is clear that the polynomial f has exactly three real zeros (cf. Fig. 1). Since its coefficients are real, we also see that f has exactly two imaginary zeros which are complex conjugates of each other.

2. Galois theory

We will show that equation (2) is not solvable by radicals by the use of Galois theory, named after the French mathematician Evariste Galois. In 1830, Galois wrote a groundbreaking paper [5] (see also [6]) that gave a criterion for determining whether any polynomial f of degree n with rational coefficients is solvable by radicals.

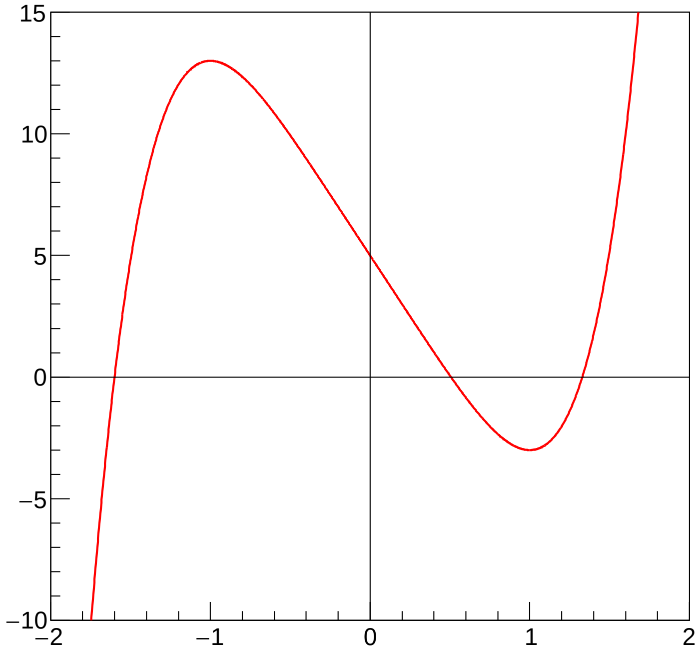

Figure 1: Graph of $y = f(x) = 2x^5 - 10x + 5$.

This criterion involves the Galois group G which is a group of permutations on the n roots of the polynomial f. Recall by the fundamental theorem of algebra that any polynomial of degree n has n roots over the complex numbers $\mathbb{C}$. Each element of the Galois group G transforms any valid polynomial equation with rational coefficients involving the roots of f into another valid equation involving these roots.

Let us take an example. Consider the polynomial equation

$$p(x) = x^4 - 4x - 5 = (x^2 + 1)(x^2 - 5) = 0. \tag{3}$$

There are four zeros: $x \in \{\pm\mathrm{i}, \pm\sqrt{5}\}$. It is clear that they form two natural pairs: i and $-$i go together and so do $\sqrt{5}$ and $-\sqrt{5}$. Indeed, it is impossible to distinguish i from $-$i and $\sqrt{5}$ from $-\sqrt{5}$ in the following sense. Write down any polynomial equation with rational coefficients that is satisfied by some selection from the four zeros. If we let

$$\alpha = \mathrm{i}, \quad \beta = -\mathrm{i}, \quad \gamma = \sqrt{5}, \quad \delta = -\sqrt{5},$$

then such equations include

$$\alpha^2 + 1 = 0, \quad \alpha + \beta = 0, \quad \delta^2 - 5 = 0, \quad \gamma + \delta = 0, \quad \alpha\gamma - \beta\delta = 0, \tag{4}$$

and so on. There are infinitely many valid equations of this kind. If we take any valid equation connecting α, β, γ, and δ and interchange α and β, we again get a valid equation. The same is true if we interchange γ and δ. For example, the above equations lead by this process to

$$\beta^2+1=0, \quad \beta+\alpha=0, \quad \gamma^2-5=0, \quad \delta+\gamma=0, \quad \beta\gamma-\alpha\delta=0,$$
$$\alpha\delta-\beta\gamma=0, \quad \beta\delta-\alpha\gamma=0,$$

and all of these are true. On the other hand, if we interchange α and γ, the second equation in (4) leads to the equation $\gamma+\beta=0$, which is false.

The operations we are using are permutations of the zeros α, β, γ, and δ and thus are elements of S_4, which includes all $4! = 24$ possible permutations of the four symbols α, β, γ, and δ. In fact, in the usual permutation notation, the interchange of α and β is

$$R=\begin{pmatrix}\alpha & \beta & \gamma & \delta\\ \beta & \alpha & \gamma & \delta\end{pmatrix}$$

and that of γ and δ is

$$S=\begin{pmatrix}\alpha & \beta & \gamma & \delta\\ \alpha & \beta & \delta & \gamma\end{pmatrix}.$$

If these two permutations transform valid equations into valid equations, then so does the permutation obtained by performing them both in turn, which is

$$T=\begin{pmatrix}\alpha & \beta & \gamma & \delta\\ \beta & \alpha & \delta & \gamma\end{pmatrix}.$$

There is, of course, one other permutation with this property of preserving all valid equations, namely the identity permutation

$$I=\begin{pmatrix}\alpha & \beta & \gamma & \delta\\ \alpha & \beta & \gamma & \delta\end{pmatrix}.$$

One can check that only these four permutations in S_4 preserve valid equations, while the other twenty permutations in S_4 can turn a valid equation into a false equation. We can write permutations as products of disjoint cycles. Thus, using cycle notation, we can rewrite R, S, T, and I as

$$\begin{aligned} R &= (\alpha\beta)(\gamma)(\delta),\\ S &= (\gamma\delta)(\alpha)(\beta),\\ T &= (\alpha\beta)(\gamma\delta),\\ I &= (\alpha)(\beta)(\gamma)(\delta). \end{aligned}$$

Note that the permutations R, S, T, and I form a subgroup of S_4 under the operation of composition of permutations. Then we call

$$G=\{I, R, S, T\}$$

the Galois group of the equation (3).

3. Application of Galois theory to the quintic polynomials

We use the following facts from Galois theory (see [8, pp. 371–398] or [14]) to show that the equation (2) is not solvable in radicals. Note that the quintic equation (2) has 5 roots in $\mathbb{C}$ and thus its Galois group is a subgroup of S_5 with $5! = 120$ elements.

(A) *A quintic polynomial equation with rational coefficients is not solvable by radicals if its Galois group G is equal to S_5.*

(B) *If a polynomial with rational coefficients has degree n and is irreducible over the rationals, then the order of its Galois group G is divisible by n.*

(C) *By Cauchy's Theorem, if the order of a finite group is divisible by a prime p, then it has an element of order p.*

(D) *Let p be a prime. Then any element of order p in S_p is a p-cycle.*

(E) *By Eisenstein's Criterion, the polynomial*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with integer coefficients is irreducible over the rationals if there exists a prime p such that p does not divide a_n, p divides each of $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$, and p^2 does not divide a_0.

(F) *Let f be a polynomial of degree n with rational coefficients. Suppose that exactly $n-2$ of the roots of f are real and the other two roots are imaginary. Let r_1 and r_2 be the two imaginary roots. Then r_1 and r_2 are complex conjugates of each other and the Galois group G of f contains the two-cycle $(r_1 r_2)(r_3)(r_4)\ldots(r_n)$. This mapping corresponds to complex conjugation which takes imaginary roots into their complex conjugate and leaves real roots fixed.*

(G) *Let f be a polynomial of prime degree p with rational coefficients. If the Galois group G of f contains both a p-cycle and a 2-cycle, then $G = S_p$.*

Theorem. *The polynomial equation* (2) *is not solvable by radicals.*

Proof. Let G be the Galois group of f. We will show that $G = S_5$. It will then follow by (A) that the equation $f(x) = 0$ is not solvable by radicals. By Fig. 1 and our earlier discussion, f has exactly three real roots and two imaginary roots r_1 and r_2 which are complex conjugates of each other. By Eisenstein's Criterion (E) with $p = 5$, we find that f is irreducible over the rationals. It follows by (B) that the order of G is divisible by 5. Since 5 is prime, we see by Cauchy's Theorem (C), that G has an element of order 5. Then by (D), we get that G contains a 5-cycle. By (F), G contains the 2-cycle $(r_1 r_2)(r_3)(r_4)\ldots(r_n)$. It now follows by (G) that the Galois group $G = S_5$. Hence, the equation (2) is not solvable by radicals. $\square$

4. Conclusions

For a popular account of Galois theory, see [11]. It can be shown that for any $n \geq 5$ there exists a polynomial equation of degree n which is not solvable by radicals. This follows from Galois' Theorem which states: *The alternating group A_n is simple for $n \geq 5$* (see [10, p. 311]). Therefore, higher order polynonomial equations are usually solved by approximate methods (numerical, statistical, etc.). For example, the Lehmer-Schur method produces guaranteed error estimates, i.e., we can find arbitrarily small circles in the complex plane containing all roots of any polynomial (see [12]).

Note that the general quintic equation with rational coefficients can also be solved algebraically by other means than the use of radicals. Suppose that for any real number a we define the ultraradical $\sqrt[*]{a}$ to be the real zero of $x^5 + x - a$. It was shown by Erland Samuel Bring in 1796 and by George Birch Jerrard in 1852 (see [9]) that the quintic equation can be solved by the use of radicals and ultraradicals. In 1858, Charles Hermite [7] proved that the quintic equation can be solved in terms of elliptic modular functions.

Acknowledgement

This paper was supported by RVO 67985840.

References

[1] Abel, N. H.: *Mémoire sur les équations algébriques, on l'on démontré l'impossibilité de l'équation générale du cinquiéme degré*, (1824), Oeuvres Complètes de Niels Henrik Abel, vol. 1, Grøndahl, Christiana, 1881.

[2] Abel, N. H.: Beweis der Unmöglichkeit, algebraische Gleichungen von höheren Graden, als dem vierten, allgemein aufzuösen. J. Reine Angew. Math. **1** (1826), 65–84.

[3] Abel, N. H.: Démostration de l'impossibilité de la résolution des équations algébrique générales d'un degré supérieur du quatrième. Bulletin des scinces mathématiques, astronomiques, physiques et chimiques **6** (1826), 347–354.

[4] Cardano, G.: *Ars Magna of the rules of algebra.* T. R. Witmer, trans. and ed., Dover Publications, Mineola, New York, 1993, original edition 1545.

[5] Galois, E.: Mémoire sur les conditions de résolubilité des équations par radicaux. J. Math. Pures Appl. (9) (1830), 417–433.

[6] Galois, E.: Oeuvres mathématiques d'Évariste Galois, J. Math. Pures Appl. (9) **11** (1846), 381–444.

[7] Hermite, C.: Sur la résolution de l'équation du cinquième degré. Comptes Rendus de l'Academie des Sciences **46** (1858), 508–515.

[8] Hungerford, T. W.: *Abstract algebra. An introduction*, 2nd edition. Saunders College Publishing, Orlando, 1997.

[9] Jerrard, G. B.: *An essay on the resolution of equations*. Taylor and Francis, London, 1859.

[10] Křížek, M., Somer, L.: Architects of symmetry in finite nonabelian groups. Symmetry: Culture and Science **21** (2010), 333–344.

[11] Livio, M.: *The equation that couldn't be solved*. Simon and Schuster, New York, 2005.

[12] Ralston, A.: *A first course in numerical analysis*. McGraw-Hill, 1965.

[13] Rektorys, K., et al.: *Survey of applicable mathematics*, vol. I, 2nd edition. Kluwer, Dordrecht, 1994.

[14] Stewart, I.: *Galois theory*, 2nd edition. Chapman and Hall, London, 1989.