A Finite Algorithm for the Solution to an Algebraic Equation

Simon Davis

Research Foundation of Southern California
8837 Villa La Jolla Drive #13595
La Jolla, CA 92039, USA
sbd1000@cam.ac.uk

Abstract. A finite algorithm is developed for the solution of algebraic equations with integer exponents. It is established, by transformation to a matrix equation that a root of the algebraic equation can be determined in $O(n^{\gamma(n)})$ steps, where $n$ is the degree.

Mathematics Subject Classification: 12D10; 65H17

Keywords: algorithm, matrix methods, algebraic number, field extension

1. Introduction

It is possible to map the language of algebraic symbols to another logical system consisting of a propositional calculus and axioms. The solutions to algebraic equations over $\mathbb{Q}$ therefore should be determined by an algorithm consisting of entirely algebraic operations in a finite number of steps, provided that the raising of numbers to rational powers has an image in the system. Otherwise the roots would be transcendental, which can be identified with numbers that can be equated only to the limit point of an infinite sequence of terms defined by rational quantities. The problem of the existence of solutions to algebraic equations with solutions that might have this property shall be discussed in the second section.

The extension of this statement to equations over $\mathbb{Q}(\alpha)$, where $\alpha$ is an algebraic number, only requires the evaluation of expressions containing $\alpha$. The Cauchy completion of $\mathbb{Q}$ into $\mathbb{R}$ provides a convergent sequence of solutions to algebraic equations over $\mathbb{R}$. The exponents in the equations have been taken to be integer. Complex exponents would allow transcendental roots. An example is the equation $x^{i\pi} + 1 = 0$ with the root $e$, even though the coefficients are integers.
If the algebraic equation has integer exponents, it can be transformed to a matrix equation. When the characteristic polynomial of the matrix is identical to the given polynomial, the eigenvalues would be the roots of the polynomial.

The finiteness of an algorithm for determining the roots of an algebraic equation already has been established through expressions for the roots of certain higher-degree equations through hypergeometric functions [15] and closed-form analytical integrals for the zeros [4].

2. Solution to Algebraic Equations by Matrix Methods

Consider a quadratic equation, \(x^2 + bx + c = 0\). The corresponding matrix
\[
\begin{pmatrix}
a_{11} & a_{12} \\
a_{21} & a_{22}
\end{pmatrix}
\]
must satisfy
\[
(a_{11} - \lambda)(a_{22} - \lambda) = \lambda^2 + b\lambda + c \tag{2.1}
\]
and it follows that
\[
b = -(a_{11} + a_{22}) \tag{2.2}
\]
\[
c = a_{11}a_{22} - a_{12}a_{21}.
\]

For the quadratic equation, there are two coefficients and four matrix elements. For the \(n^{th}\) order equation, there are \(n\) coefficients and \(n^2\) matrix elements. A choice of matrix with the given characteristic polynomial can be found in \(O(n)\) steps. It is preferable to have non-zero diagonal elements for the row-echelon procedure to be implemented effectively. The diagonalization procedure would involve \(O(n^{\gamma(n)})\) steps, where \(\gamma(n)\) shall be determined.

The use of linear transformations to eliminate certain terms is consistent with this technique. The Tschirnhaus transformation [31] is used to map a polynomial to another with zero coefficients through \(x \rightarrow \frac{g(x)}{h(x)}\), where \(g, h\) are polynomials over the base field \(K\). This transformation is accompanied by an auxiliary equation with degree less than that of the original polynomial.

Specifically, it has been shown that the general quintic can be mapped to a polynomial without cubic and quartic terms [19][23]
\[
q(x) = x^5 + a_2x^2 + a_1x + a_0. \tag{2.3}
\]
This equation can be further brought to Bring-Jerrard form [6][21][22]
\[
x^5 + b_1x + b_0 = 0 \tag{2.4}
\]
which can be solved through Hermite polynomials. The roots of the quintic equation \(x^5 + px + q = 0\) also equal \((\frac{p}{q})^{\frac{1}{5}} BR \left(-\frac{(\frac{p}{q})^{\frac{1}{5}}}{4}\right)\) and four conjugates through multiplication by fifth roots of unity, where
\[
BR(t) = \sum_{n=0}^{\infty} a_n(t - 57)^n \tag{2.5}
\]
and the analytic continuation, with

\[
(2.6) \quad a_{n+4} = -\frac{185193}{5278000} \frac{2n + 5}{n + 3} a_{n+3} - \frac{9747}{5278000} \frac{10n^2 + 40n + 39}{(n + 4)(n + 3)} a_{n+2} \\
- \frac{52}{5278000} \frac{(2n + 3)(10n^2 + 30n + 17)}{(n + 4)(n + 3)(n + 2)} a_{n+1} \\
- \frac{1}{6597500000} \frac{(5n + 11)(5n + 7)(5n + 3)(5n - 1)}{(n + 4)(n + 3)(n + 2)(n + 1)} a_n.
\]

Although the Bring radical is an algebraic number, it shall be considered whether there exists an equivalent finite expression or algorithm yielding this solution. It is known that the five roots of a quintic equation \[15\] are

\[
(2.7) \quad x_1 = -t^4 F_1(t) \\
x_2 = -F_1(t) + \frac{1}{4} t F_2(t) + \frac{5}{32} t^2 F_3(t) + \frac{5}{32} t^3 F_4(t) \\
x_3 = -F_1(t) + \frac{1}{4} t F_2(t) - \frac{5}{32} t^2 F_3(t) + \frac{5}{32} t^3 F_4(t) \\
x_4 = -i F_1(t) + \frac{1}{4} t F_2(t) - \frac{5}{32} i t^2 F_3(t) - \frac{5}{32} i^3 F_4(t) \\
x_5 = i F_1(t) + \frac{1}{4} t F_2(t) + \frac{5}{32} i t^2 F_3(t) - \frac{5}{32} i^3 F_4(t)
\]

where

\[
F_1(t) = F_2(t) = 4F_3(\frac{1}{5}, \frac{1}{5}, \frac{1}{5}; \frac{1}{5}; 5; \frac{5}{4}; 4; \frac{5}{2}; \frac{5}{4}; 5; \frac{3125}{256}) \\
F_3(t) = 4F_3(\frac{9}{20}, \frac{13}{20}, \frac{17}{20}; \frac{3}{4}; \frac{3}{2}; \frac{3}{4}; \frac{3}{2}; \frac{3}{4}; \frac{3}{2}; \frac{3}{4}; \frac{3125 t^4}{256}) \\
P_4(t) = 4F_3(\frac{7}{10}, \frac{9}{10}, \frac{11}{10}; \frac{7}{4}; \frac{7}{2}; \frac{7}{4}; \frac{7}{2}; \frac{7}{4}; \frac{7}{2}; \frac{7}{4}; \frac{3125 t^4}{256}).
\]
Similarly, for the equation \( x^n - x + t = 0 \), there are \( N - 1 \) solutions of the form [15]

\[
x_k = \omega^{-k} - \frac{t}{(N-1)^2} \sqrt{\frac{N}{2\pi(N-1)}} \sum_{q=0}^{N-2} \left( \frac{\omega t}{N-1} \right)^q \frac{q^N}{n^N}
\]

\[
(2.9)
\]

\[
\frac{\prod_{k=0}^{N-1} \Gamma \left( \frac{Nq + 1 + k}{N} \right)}{\Gamma \left( \frac{q}{N-1} + 1 \right) \prod_{k=0}^{N-2} \Gamma \left( \frac{q+k+2}{N-1} \right)} \]

\[
F_{N+1} \left[ \frac{qN}{N-1} + 1, \ldots, \frac{qN}{N-1} + N, 1; \frac{q+2}{N-1}, \ldots, \frac{q+N}{N-1}, \frac{q}{N-1} + 1; \frac{t\omega}{(N-1)^2} \right]^{N-1}_{N^N}
\]

\[
k = 1, 2, 3, \ldots, N - 1
\]

with \( \omega = \exp \left( \frac{2\pi i}{N-1} \right) \), and the \( N^{th} \) solution is deduced by considering symmetric polynomials of the roots. This expression, however, consists of a finite number of terms. Since the gamma and hypergeometric functions can be identified with contour integrals in the complex plane, it represents an algorithm based on rational numbers and a finite number of operations to determine the roots if there are identities satisfied by the integrals that reduce the computation of the solution to a finite number of steps.

The approach based on matrices then can be used as an algorithm for solving quintic and higher-order equations. For the quintic equation, the matrix must be

\[
(2.10)
\]

\[
A = \begin{pmatrix}
a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\
a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\
a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\
a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\
a_{51} & a_{52} & a_{53} & a_{54} & a_{55}
\end{pmatrix}
\]

where

\[
(2.11)
\]

\[
det(\lambda I - A) = \lambda^5 + p\lambda + q
\]
which implies that

\[(2.12)\]

\[a_{11}a_{22}a_{33}a_{44}a_{55} = -q\]

\[a_{23}(-a_{34}a_{45}a_{52} - a_{35}a_{45}a_{54} + a_{32}a_{45}a_{54}) + a_{22}(a_{34}a_{45}a_{53} + a_{35}a_{45}a_{43})\]

\[-a_{24}(-a_{35}a_{53}a_{42} + a_{35}a_{52}a_{43} + a_{45}a_{53}a_{32}) + a_{25}(-a_{54}a_{43}a_{32} - a_{34}a_{42}a_{53} + a_{34}a_{43}a_{52})\]

\[-a_{11}(a_{34}a_{45}a_{53} + a_{35}a_{45}a_{43})\]

\[+ a_{11}a_{22}[a_{44}a_{55} - a_{45}a_{54} - (a_{34}a_{43} + a_{35}a_{53}) + a_{33}a_{44} + a_{33}a_{55}]\]

\[-a_{11}a_{23}[a_{32}[a_{44} + a_{55}] - a_{35}a_{52} - a_{34}a_{42}]\]

\[+ a_{11}a_{24}[a_{45}a_{52} + a_{43}a_{32} - a_{42}(a_{33} + a_{55})]\]

\[-a_{11}a_{25}[a_{52}(a_{33} + a_{44}) - a_{54}a_{42} - a_{53}a_{32}]\]

\[+ a_{12}\{[a_{31}[a_{44}a_{55} + a_{44}a_{55}] + (a_{34}a_{43} + a_{35}a_{53} + a_{45}a_{54})]\]

\[+ a_{23}[a_{31}(a_{44} + a_{55}) - (a_{35}a_{51} + a_{34}a_{41})]\]

\[-a_{24}[a_{31}a_{43} + a_{45}a_{51} - a_{41}(a_{33} + a_{55})]\]

\[+ a_{25}[a_{51}(a_{33} + a_{44}) - a_{53}a_{31} - a_{54}a_{41}]\}\]

\[-a_{13}\{-a_{21}[a_{32}(a_{44} + a_{55}) - a_{34}a_{42} - a_{35}a_{52}]\]

\[+ a_{31}[a_{22}a_{44} + a_{22}a_{55} + a_{44}a_{55} - a_{24}a_{42} - a_{25}a_{52} - a_{45}a_{54}]\]

\[+ a_{41}[a_{34}(a_{22} + a_{55} - a_{32}a_{24} - a_{35}a_{54})\]

\[+ a_{51}[a_{32}a_{25}a_{44} - a_{35}(a_{22} + a_{44})]\}\]

\[+ a_{14}\{-a_{21}[a_{32}a_{43} + a_{45}a_{52} - a_{42}(a_{33} + a_{55})]\]

\[+ a_{31}[a_{43}(a_{22} + a_{55}) - a_{42}a_{23} - a_{45}a_{53}]\]

\[-a_{41}[a_{22}a_{33} + a_{22}a_{55} + a_{33}a_{55} - a_{23}a_{32} - a_{25}a_{52} - a_{35}a_{53}]\]

\[+ a_{51}[a_{45}(a_{22} + a_{33} - a_{42}a_{25} - a_{43}a_{35})]\}\]

\[-a_{15}\{-a_{21}[a_{52}(a_{33} + a_{44} - a_{53}a_{32} - a_{54}a_{42}]\]

\[+ a_{31}[a_{52}a_{23} + a_{54}a_{43} - a_{53}(a_{22} + a_{44})]\]

\[-a_{41}[a_{54}(a_{22} + a_{33} - a_{52}a_{24} - a_{53}a_{34}]\]

\[+ a_{51}[a_{22}a_{33} + a_{22}a_{44} + a_{33}a_{44} - a_{24}a_{42} - a_{34}a_{43} - a_{23}a_{32}]\}\]

\[= \rho.\]

There are 25 parameters \((a_{ij})\) can be chosen to satisfy these two equations and three other constraints. After selecting the matrix elements such that there are non-zero entries both in the upper and lower triangular parts, the row-echelon procedure can be applied to yield the diagonal elements. The accuracy of this algorithm may be tested by considering the equation \(x^5 - 5x - 228.004 = 0\), since the series for the Bring radical converges rapidly.

The polynomial equation can be translated to a system of linear equations for the variables \((x_1, \ldots, x_n)\). The roots of the algebraic equation can be expressed as algebraic functions of the solutions to the linear system. With
regard to the diagonalization of the matrix defined by rational coefficients, the matrix equation must consist of finite radical expressions because the necessary cancellations cannot be achieved in a finite-term equation with transcendental numbers, unless these can be factored entirely from the relation. A complete factorization splitting the transcendental factor from the rest of the equation would imply the existence of a finite radical solution to the algebraic equation. If the elements of the similarity transformations were chosen such that inverses of transformation matrices included negative powers of transcendental numbers with the effect of nullifying through multiplication other transcendental elements, the eigenvalues would consist of finite radical expressions nevertheless.

Furthermore, given that there does not exist a finite linear relation over \( \mathbb{Q} \) between different algebraic powers of the same transcendental number \( \xi \), following the Hermite-Lindemann theorem [5][20][25], and the extension of this property to fields of the type \( \mathbb{Q}(\xi_1, ..., \xi_k) \), where \( \xi_1, ..., \xi_k \) are transcendental numbers that are algebraically independent of \( \xi \), there remains only the possibility of the inclusion of the same transcendental factor in each term of a linear relation, implying the existence of an algebraic solution. From the algebraic solutions, the constructed root \( x \) would have to be algebraic.

The similarity transformation is known to be a product of orthogonal matrices with trigonometric entries [27]. In the QR algorithm, the matrix is written in upper Hessenberg form and then multiplied by the product \( Q_{n-1,n}Q_{2,n}Q_{1,2} \), where \( Q_{i,j} \) represents the rotation in the plane spanned by the vectors defined by the \( i^{th} \) and \( j^{th} \) rows [28]. Given that the elements of the matrices consist of radicals, the diagonalization must yield algebraic numbers for the eigenvalues. It may be noted that there exists a set of minimum cardinality \( \mathbb{Q}_{n(n-1)/2} \) of rational values of elements and a larger cardinality of algebraic values of entries of the similarity transformations, which can be used to diagonalize matrices based over \( \mathbb{Q} \) to give algebraic eigenvalues. This can be deduced from the systematic solution of the orthogonality conditions. For example, a similarity
transformation of the form

\[
\begin{pmatrix}
0 & \cdots & \cdots & \cdots & 0 \\
0 & \cos \theta_{ij} & -\sin \theta_{ij} & 0 \\
0 & \sin \theta_{ij} & \cos \theta_{ij} & 0 \\
0 & \cdots & \cdots & \cdots & 0
\end{pmatrix}
\begin{pmatrix}
0 & \cdots & \cdots & \cdots & 0 \\
0 & a_{ii} & a_{ij} & 0 \\
0 & a_{ji} & a_{jj} & 0 \\
0 & \cdots & \cdots & \cdots & 0
\end{pmatrix}
= \begin{pmatrix}
0 & \cdots & \cdots & \cdots & 0 \\
0 & \cos \theta_{ij} & \sin \theta_{ij} & 0 \\
0 & -\sin \theta_{ij} & \cos \theta_{ij} & 0 \\
0 & \cdots & \cdots & \cdots & 0
\end{pmatrix}
\]

(2.13)

where

\[
b_{ii} = a_{ii} \cos^2 \theta_{ij} + a_{jj} \sin^2 \theta_{ij} - (a_{ij} + a_{ji}) \sin \theta_{ij} \cos \theta_{ij}
\]

(2.14)

\[
b_{ij} = (a_{ii} - a_{jj}) \sin \theta_{ij} \cos \theta_{ij} + a_{ij} \cos^2 \theta_{ij} - a_{ji} \sin \theta_{ij}
\]

\[
b_{ji} = (a_{ii} - a_{jj}) \sin \theta_{ij} \cos \theta_{ij} - a_{ij} \sin^2 \theta_{ij} + a_{ji} \cos \theta_{ij}
\]

\[
b_{jj} = a_{ii} \sin^2 \theta_{ij} + (a_{ij} + a_{ji}) \sin \theta_{ij} \cos \theta_{ij} + a_{jj} \cos^2 \theta_{ij}
\]

The vanishing of the off-diagonal entries implies

\[
(a_{ii} - a_{ij}) \sin \theta_{ij} \cos \theta_{ij} - a_{ij} \sin^2 \theta_{ij} + a_{ji} \cos^2 \theta_{ij} = 0
\]

(2.15)

\[
(a_{ii} - a_{jj}) \sin \sqrt{1 - \sin^2 \theta_{ij}} - a_{ij} \sin^2 \theta_{ji} + (1 - \sin^2 \theta_{ij}) a_{ji} = 0
\]

\[
(a_{ii} - a_{jj}) \sin \theta_{ij} \sqrt{1 - \sin^2 \theta_{ij}} = (a_{ij} + a_{ji}) \sin^2 \theta_{ij} - a_{ji}
\]

Squaring both sides

\[
\sin^2 \theta_{ij} + (a_{ij} + a_{ji})^2 \sin^4 \theta_{ij}
\]

(2.16)

\[
[(a_{ii} - a_{jj})^2 + (a_{ij} + a_{ji})^2] \sin^4 \theta_{ij} - [2a_{ji}(a_{ij} + a_{ji}) - (a_{ii} - a_{jj})^2] \sin^2 \theta_{ij} + a_{ji}^2 = 0
\]

yielding algebraic values for \(\sin \theta_{ij}\) and \(\cos \theta_{ij}\). The algebraic expression containing the sines and cosines cannot equal a transcendental number at any stage of the calculation.

It may be noted that there exists a set of minimum cardinality \(\mathbb{Q}^{n(n-1)/2}\) of algebraic values of elements of the similarity transformations, which can be used to diagonalize matrices based over \(\mathbb{Q}\) to give algebraic eigenvalues. There are twenty steps in the computation of \(\sin \theta_{ij}\) and \(\cos \theta_{ij}\) for each \(i, j,\)
while the evaluation of the diagonal elements requires another six steps. For each similarity transformation, there are \( 8n \) multiplications, and with \( n(n - 1)/2 \) similarity transformations, the number of steps in the diagonalization procedure is \( O((4n + 13)n(n - 1)) \). When \( n \) is sufficiently large, \( \gamma(n) \approx 3 + \frac{1}{4} \ln n \).

3. Convergence Methods over the Field \( \mathbb{C} \)

By Newton’s method [26], the iteration step is

\[
(3.1) \quad x_n = x_{n-1} - \frac{f(x_{n-1})}{f'(x_{n-1})} \quad n = 1, 2, 3, \ldots
\]

If \( x_{n-1} \) is chosen to be a transcendental number, then a sequence of transcendental numbers results. When \( x_0 \) is a rational number and the polynomial is defined over \( \mathbb{Q} \), \( x_n \) is rational for all finite \( n \), and \( \{x_n\} \) is a convergent sequence to any real root because \( \mathbb{Q} \) is dense in \( \mathbb{R} \). If \( x_0 \) is an algebraic number, the method gives a sequence of numbers that contain rational expressions with radicals in the numerator and denominator, where the latter can be removed through multiplication by the appropriate radical expression, and the sequence consists of terms in \( \mathbb{Q}(\alpha) \) if \( x_0 \in \mathbb{Q}(\alpha) \), which would converge to any value in \( \mathbb{R} \). This technique is known to be quadratically convergent. Generalizations, including Halley’s method, a cubic-order algorithm [16], are known to provide solutions to any real root at different rates of convergence.

In the complex plane, Eq.(3.1) may be used to determine the root if the original value is complex. Since \( \mathbb{Q} \times \mathbb{Q} \) is dense in \( \mathbb{R}^2 \), the convergence to any complex root is established [7].

While the method yields an infinite sequence, it is suggested that there is a finite sequence based on numbers in \( \mathbb{Q} \), \( \mathbb{Q}(\alpha) \),..., giving the real roots of an algebraic equation over \( \mathbb{Q} \), and similarly, a sequence in \( \mathbb{Q} \times \mathbb{Q} \), \( \mathbb{Q}(\alpha_1) \times \mathbb{Q}(\alpha_2) \),..., yielding the complex roots.


An example of an algorithm which is based on a different convergent sequence than that of Newton’s method is given. The iterative technique can be used to determine solutions to higher-order algebraic equations.

When \( n \leq 4 \), the action of \( S_n \) on \( \mathbb{CP}^1 \) may be used to define a map that provides convergence to the corresponding equations. For the quintic, there exists a rational mapping of \( \mathbb{CP}^1 \) that has commutes with a subgroup isomorphic to the solvable group \( A_5 \). The existence of periodic orbits, \( \lim_{k \to \infty} f^k(a) \to a \) for \( a \in \mathbb{CP}^1 \) implies that the iterative method provides a solution to the quintic equation [10].

For the 6\(^{th} \) order equation, the action of \( A_6 \) on \( \mathbb{CP}^2 \) yields a rational map that commutes with the Valentiner group [8]. This technique generates a solution through the successive applications of the rational transformation. It has been noted that there is an \( S_n \) action on \( \mathbb{CP}^2 \) and holomorphic maps of degree \( n + 1 \).
Algebraic equation

[9] which suggests a generalization of the method to \( n^{th} \)-order equations for \( n > 6 \).

5. The Theorem of Abel

The proof of the unsolvability of the quintic equation by Abel proceeded through the following stages. First, the lemma stating that the \( x^p = C \) for prime \( p \) is an irreducible equation in the field of coefficients, where \( C \) is an element of the field [1]. In particular, this field can be chosen to be \( \mathbb{Q} \).

Secondly, an irreducibility theorem on the roots and common factors of rational-coefficient polynomials was used [2]. The statement of this theorem, however, should be qualified by the following remarks. Although, the highest common divisor \( g(x) \) of two arbitrary polynomials \( F(x) \) and \( f(x) \) in \( \mathbb{Q} \) can be derived from a Euclidean algorithm and

\[
F(x) = F_1(x) \cdot g(x) \quad f(x) = f_1(x) \cdot g(x)
\]

it is not possible to isolate one root \( \alpha \) of \( f(x) \), when \( f(x) \) is irreducible, equate it with a root of \( F(x) \) and draw general conclusions about the factorization of \( F(x) \) over \( A \), because the root \( \alpha \) may not belong to \( \mathbb{Q} \). If it did belong to \( \mathbb{Q} \), \( f(x) \) would be reducible and equal to \((x - \alpha)f_2(x)\) for some \( f_2(x) \) with coefficients in \( \mathbb{Q} \).

Thirdly, the proof of Abel requires the fundamental theorem stating that, if an equation is algebraically solvable, a symmetric function of the roots can be given a form, which may be expressed by rational functions of the coefficients of the equation [3][17][18].

Without the general validity of this latter result, the corollaries of the fundamental theorem again can be stated. First, if a root of an irreducible equation \( f(x) = 0 \) in \( A \), where \( f \) satisfies the irreducibility theorem, is also a root of an irreducible equation of lower degree \( F(x) = 0 \), the coefficients of \( F \) vanish. Secondly, given that this property is satisfied, there is no other irreducible equation in \( A \) that has a common root with that of \( f(x) = 0 \). Thirdly, every number of the group \( A(\alpha) \), where \( \alpha \) is a root of an irreducible equation of the \( n^{th} \) degree in \( A \), can be represented by a polynomial of degree \((n - 1)\) in \( \alpha \) with coefficients that are \( A \)-numbers. When the irreducible polynomial \( f(x) \) satisfies the irreducibility theorem, the representation is unique. Fourthly, when the irreducibility theorem can be applied to an irreducible equation of prime degree \( p \) in a group, it can become reducible through the substitution of a root of another irreducible equation in this group only if \( p \) is a divisor of the degree of the latter equation.

The implications for solvability by Ruffini radicals are deduced by attaching sufficiently many radicals such that the polynomial \( f(x) \) becomes reducible [29]. This is achieved by solving the equation \( x^\ell = a \), \( a \in K \) in the field \( L = K(\lambda) \). Including the roots of unity, \( \eta^\ell = 1 \), a set of polynomials of
degree \( n - 1 \) in \( \lambda, \lambda \eta, \lambda \eta^2, \ldots, \lambda \eta^{n-1} \) are constructed. This method is then used to determine the roots as symmetric functions of these variables, and it is concluded that either one of the roots is real and the remainder occur in complex conjugates or all of the roots are real. It follows that an algebraic equation solvable by Ruffini radicals with an odd prime degree, and which is irreducible over \( \mathbb{Q}[x] \) would possess either only one real root or all real roots by Abel’s procedure [24]. However, the equation \( x^5 - ax - b = 0, \ a, b > 0, \ p|a, b, \ p^2 \not|b, \ 4^4a^5 > 5^5b^4 \), would have three real roots and two complex roots [30], and therefore, it should not have a solution in Ruffini radicals.

The proof relies on the solutions to the prime-order equation \( x^p = a \) for some \( a \in K \). For this equation, the irreducibility theorem also may be proven. However, it could be possible to attach factors that arise as solutions of another equation, and then consider the appropriate combinations of the polynomials containing these roots to determine a set of solutions to the original algebraic equation. Furthermore, if another auxiliary equation was used, it would have to be checked that the polynomial satisfied the irreducibility criterion.

6. THE THEOREM OF GALOIS

It is well known that equations of degree greater than 4 are not viewed as solvable by radicals. However, this result does not preclude the possibility of a finite algorithm based on the use of radicals and algebraic numbers yielding the roots of a higher-degree equation.

First, instead of standard expressions with radicals, let us consider more general algorithms, beginning with a truncated continued fraction expansion. Given that the radicals in that formula are the algebraic numbers \( \alpha_1, \ldots, \alpha_{\ell} \), it can be verified that the expression does not belong to \( \mathbb{Q}(\alpha_1, \ldots, \alpha_{\ell}) \) but \( \mathbb{Q}(\alpha_1, \ldots, \alpha_{\ell}, \alpha_1 \alpha_2, \ldots, \alpha_{\ell-1} \alpha_1, \ldots, \alpha_1 \ldots \alpha_{\ell}) \). Consequently, beginning with numbers in the field, \( \mathbb{Q}(\alpha_1, \ldots, \alpha_{\ell}) \), the algorithm yields a value that belongs to a new field extension \( \mathbb{Q}(\alpha_1, \ldots, \alpha_{\ell}, \alpha_1 \alpha_2, \ldots, \alpha_{\ell-1} \alpha_1, \ldots, \alpha_1 \ldots \alpha_{\ell}) \). Starting with a finite extension of \( \mathbb{Q} \) that is postulated to be the splitting field of a polynomial, the algorithm generates a further extension of this field.

The theorem on the solvability of algebraic equations [13] depends on the definition of the splitting field and the solvability of the Galois group of the field extension. The sufficiency may been proven because this property implies that factorizability of the polynomial over the splitting field. Furthermore, given one root, other roots may be derived through the application of transformations in the Galois group [11].

Nevertheless, it is not a necessary condition for all algorithms because the concept of a fixed splitting field can be ill-defined. When an algorithm has an image which yields an extension of the original splitting field, the theorem is not directly applicable.
The normal, separable extension necessary for the existence of the Galois group is linked to a particular method for constructing the root of the algebraic equation. The condition of a normal splitting field is equivalent to the irreducibility criterion of Abel [2]. It follows that there is a restriction again to deriving solutions to the equation consistent with the irreducibility theorem. This can be done, yielding a restriction on the solvability of algebraic equations through Ruffini radicals. In Galois theory, a generalization is apparent then through the variation in the chain of extensions of the base field, which might be achieved, perhaps, through the solution to equations other than \( x^p = a \), where \( a \in K(\alpha_1, \alpha_2, \ldots \alpha_k) \). It follows that the inclusion of algebraic numbers satisfying other auxiliary conditions, which are not necessarily Ruffini radicals, may be sufficient to solve higher-degree equations. This has been verified for the quintic equations with the Bring radical [6][21][22]. The form of these algebraic numbers then may be compared with that derived from the matrix multiplication to establish a finite method for solving algebraic equations of general degree.

**References**


Received: January 30, 2008; in final form September 16, 2009