SOLVING POLYNOMIAL EQUATIONS BY RADICALS

Lee Si Ying[1] and Zhang De-Qi[2]

[1]Raffles Girls' School (Secondary), 20 Anderson Road, Singapore 259978
[2]Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543

ABSTRACT

The aim of this project is to determine the solvability by radicals of polynomials of different degrees. Further, for polynomials which are solvable by radicals, the Galois- theoretic derivation of the general solution to the polynomial is sought. Where a degree $k \geq 5$ polynomial is found to be insolvable, the project aims to prove this, as well as find more specific cases of the polynomial which can be solved.

The solvability by radicals is shown through the use of Galois Theory as well as aspects of Group and Field theory. This solvability is demonstrated through the showing of the solvability of the Galois group of the polynomial.

Polynomials of degree one and two are easily shown to be solvable by radicals due to the presence of a general formula for both. More complex formulas exist for cubic and quartic polynomials, and are thus solvable by radicals. However, general polynomials of degree five are not solvable, and hence no general formulas exist. Rather, more specific cases of polynomials of degree five are solvable, namely polynomials reducible over rational numbers, and cyclotomic polynomials.

Research into the study of polynomials and the solving of its roots is of practical and widespread use in computer aided design and other computer applications in both the fields of physics and engineering.

INTRODUCTION

Polynomials are functions of the type

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

where $a_n \neq 0$. The *root(s)* of a polynomial are the value(s) of x which satisfy $p(x) = 0$.
Being able to solve for polynomial roots using radicals is not about finding a root, as this is known by the fundamental theorem of algebra that any polynomial of degree n has n complex roots, which need not be distinct. Solving a polynomial by radicals is the expression of all roots of a polynomial using only the four basic operations: addition, subtraction, multiplication and division, as well as the taking of radicals, on the arithmetical combinations of coefficients of any given polynomial.

Solving for polynomial roots by radicals, involves finding the general solution to the general form of a polynomial of some specific degree.

The purpose of this research is thus to find out if all polynomials can be solved by radicals and to prove the resultant findings about the solvability of polynomials.

RESULTS

1. Cubic Functions

Solving Cubic functions can be done using Cardano's method, which transforms the general cubic equation into a depressed cubic without the x^2 term.

The method is as follows.

We begin with the general form of a polynomial of degree three.

$$ax^3 + bx^2 + cx + d = 0. \qquad --(1)$$

Since it is easier to work with a polynomial of leading coefficient one, we can divide a out of the entire equation to obtain

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0.$$

Substitute the following equation into (2)

$$x = y - \frac{b}{3a}.$$

The polynomial becomes

$$\left(y - \frac{b}{3a}\right)^3 + \frac{b}{a}\left(y - \frac{b}{3a}\right)^2 + \frac{c}{a}\left(y - \frac{b}{3a}\right) + \frac{d}{a}$$
$$= y^3 + y\left(\frac{b^2}{3a^2} - \frac{2b^2}{3a^2} + \frac{c}{a}\right) + \left(-\frac{b^3}{27a^3} + \frac{b^3}{9a^3} - \frac{cb}{3a^2} + \frac{d}{a}\right) = 0.$$

Thus we are reduced to the cubic polynomial of the form

$$y^3 + py + q = 0. \qquad --(2)$$

Here

$$p = \frac{b^2}{3a^2} - \frac{2b^2}{3a^2} + \frac{c}{a}, q = -\frac{b^3}{27a^3} + \frac{b^3}{9a^3} - \frac{cb}{3a^2} + \frac{d}{a},$$

and observe that

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

Equation (2) corresponds to equation (3) since we can let

$$(u+v) = y, 3uv = -p, u^3+v^3 = -q.$$

Thus we can solve equation (3) for y as follows:

$$y = w_i\left(\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}\right),$$

where $i \in \{1,2,3\}$ and w_i is one of the 3rd roots of unity.

Thus the general solutions for the equation (4) are

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

We will consider the Galois group of the irreducible depressed cubic equation.

The Galois group of the splitting field of a general cubic equation is S_3 .
Thus we see that the possible Galois group of any cubic is isomorphic to either S_3 or A_3.

Let $f(x) = x^3 + px + q$ be an irreducible cubic in the polynomial ring F[x] over a field F of characteristic zero (e.g. F = Q, R), with roots y_1, y_2, y_3.

We have the relations $y_1 + y_2 + y_3 = 0$,

$$y_1y_2 + y_2y_3 + y_3y_1 = p,$$

$$y_1y_2y_3 = -q.$$

Hence we have the chain of fields $F \subset F(y_1) \subseteq K$, where $K = F(y_1, y_2) = F(y_1, y_2, y_3)$. This is because if two roots are in the field, the third automatically is.

We know that either $F(y_1) = K$, or $F(y_1) < K$.

Case I: $F(y_1) = K$. Thus we know $K = F(y_i)$ for any $i = \{1,2,3\}$, or $[K{:}F] = 3$. Hence $Gal(K/F) = A_3$.

The composition series of $Gal(K/F)$ is thus $A_3 \rhd 1$.

Case II: $F(y_1) < K$.

We know that $G = Gal(K/F)$ is a subgroup of S_3.

Since we know that $f(x)$ factors over K, and $F(y_1)$ does not contain y_2, consider $h(x) = (x - y_2)(x - y_3)$. We know that $h(x)$ is irreducible over $F(y_1)$, hence $[K{:}\,F] = 6$.

Since $[K{:}\,F] = 6, G = S_3$. S_3 has only one degree 3 subgroup, A_3. This implies that there exists a field L such that $[K{:}\,L] = |A_3| = 3$, and $[L{:}\,F] = 2$. L is thus obtained by adjoining a square root, that of the discriminant, D, where

$$D = \prod_{1 \le i < j \le 3} \left(y_j - y_i\right)^2.$$

We realise that $\sqrt{D}$ is fixed by any even permutation of the roots , but that $\sigma(\sqrt{D}) = -\sqrt{D}$ for any odd permutation σ, where σ acts naturally on the subscripts in the above expression of D. Thus we see that D is fixed by all of S_4 , so if D is not a square, $\sqrt{D} \notin F$, hence $\left[F\left(\sqrt{D}\right){:}\,F\right] = 2$, or is a radical extension. Since $Gal(K/F) = S_3$, one can show that $L \;=\; F(\sqrt{D})$.

Thus $K = F(y_1, y_2) = F\left(\sqrt{D}, y_1\right)$, and we have the composition series of $Gal(K/F)$:

$$S_3 \rhd A_3 \rhd 1.$$

We also realise that this is so because we find that

$$\begin{aligned}\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 &= \left(-\frac{b^3}{27a^3} + \frac{b^3}{9a^3} - \frac{cb}{3a^2} + \frac{d}{a}\right)^2 + \left(\frac{b^2}{9a^2} - \frac{2b^2}{9a^2} + \frac{c}{3a}\right)^3 \\ &= -\frac{1}{108}\left(b^2c^2 - 4db^3 - 4ac^3 + 18abcd - 27d^2a^2\right) \\ &= -\frac{1}{108}(y_1 - y_2)^2(y_2 - y_3)^2(y_1 - y_3)^2.\end{aligned}$$

Thus we see that the adjoining of the square root of the discriminant gives rise to the field L which contains the term

$$\sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}.$$

2. Quartic Functions

Solving Quartic polynomials can be done using Ferrari's method, which transforms a quartic polynomial into a depressed quartic which has no x^3 term.

We begin with the general form of a quartic equation.

$$x^4 + ax^3 + bx^2 + cx + d = 0. \qquad --(4)$$

Indeed, we can reduce all quartic polynomials to the above monic polynomials by dividing throughout by the leading coefficient, and replacing the coefficients of the other terms with a, b, c, d.

Substitute the following into (5)

$$x = y - \frac{a}{4} \qquad --(5)$$

to get an equation of the form

$$y^4 + py^2 + qy + r = 0. \qquad --(6)$$

We can add $2zy^2 + z^2$ to the above equation, to obtain

$$y^4 + 2zy^2 + z^2 = (2z - p)y^2 - qy + (z^2 - r).$$

Since we want the right hand side to be a square as well, we should let the discriminant of the quadratic on the RHS be 0. Namely, we assume that

$$q^2 - 4(z^2 - r)(2z - p) = 0. \qquad -- (7)$$

Rearranging the terms we get a cubic in z,

$$8z^3 - 4pz^2 - 8rz + 4rp - q^2 = 0. \qquad --- (8)$$

We can thus find the root z of this equation, and solve for y by substituting that value into (6) to get a quadratic in y^2

Solving the resultant quadratic in y^2 gives the roots of the depressed quartic, from which we can derive x.

Thus we get the solutions for the quartic equation (4). One root of (8) is fixed in this formula.

$$x = \frac{1}{2}\sqrt{2z - p} \pm \sqrt{\frac{1}{2}z - \frac{1}{4}p \pm \sqrt{z^2 - r}} - \frac{a}{4}.$$

The Galois theoretic derivation of the formula is as follows.

Solving for the roots of a quartic involves the solving of the cubic equation (8) in z:

$$8x^3 - 4pz^2 - 8rz + 4rp - q^2 = 0.$$

We know that for a $general\ irreducible$ quartic equation f in $F[x]$ the Galois group $G = Gal(E/F)$ is S_4.

$G = S_4$ has the composition series:

$$1 \lhd < \sigma > \lhd V \lhd A_4 \lhd S_4,$$

where V is the Klein 4-group. σ is any of the 3 order 2 involutions in V .

The corresponding field extension is:

$$E \supset E_\sigma \supset E_V \supset E_{A_4} \supset F.$$

The part $E_{A_4} \supset F$ (corresponding to $A_4 \lhd S_4$) is of degree two, and corresponds to the degree two extension in solving z. The element z is solved through the taking of a degree two extension i.e., square root of the discriminant, and followed by a cubic root (as stated above for cubic equations). We note that $Gal(E/F) = S_4/V$, which is isomorphic to S_3 . Indeed, $S_4 = VS_3 = gh\ |g$ in V, h in $S_3\}$. The group V acts on E_v trivially and hence S_4/V (identified with S_3) acts on E_v which fixes exactly elements in F.

The extension $E_\sigma \supset E_v$ is of degree 2, and corresponds to the taking of either $\sqrt{2z-p}$ or $\sqrt{z^2-r}$. These are equivalent since from equation (7) we have that $(2z-p)(z^2-r) = \frac{q^2}{4}$, which is a square.

There are 3 possible groups $< \sigma >$, which correspond to the adjoining of the 3 possible values of z as solutions of the equation (8).

The last radical extension ($E \supset E_\sigma$) corresponds to the taking of

$$\sqrt{-\frac{1}{2}z - \frac{1}{4}p + \sqrt{z^2-r}} \text{ or } \sqrt{-\frac{1}{2}z - \frac{1}{4}p - \sqrt{z^2-r}} \ .$$

Adjoining either of these two to E_σ will give rise to the same field E since the degree $[E: E_\sigma] = 2$.

3. Quintic Functions

Generally, quintic polynomials are insolvable by radicals. This proof makes use of group theory and Galois Theory, and is unlike Abel's 1819 paper. We will use the result below:

Theorem 1. An irreducible polynomial $f(x)$ defined over a field F of characteristic zero (e.g. $F = Q, R$) is solvable by radicals if and only if the *Galois group* $Gal(E/F)$ of the *splitting field* E of the polynomial z is a solvable group.[1],[2] Let $y_1, \dots y_5$ be independent transcendental elements over the field $\mathbb{Q}$ of rational numbers. Consider

$$f(x) = (x - y_1) \dots (x - y_5) = x^5 - s_1 x^4 + s_2 x^3 - s_3 x^2 + s_4 x - s_5.$$

By Vieta's formula, we know that

$s_1 = y_1 + \dots + y_5, s_2 = y_1 y_2 + \dots + y_4 y_5, \dots, s_5 = y_1 y_2 y_3 y_4 y_5,$

are elementary symmetrical functions in y_i . Thus $f(x)$ is a polynomial defined over the field $F = Q(s_1, \dots, s_5)$ .We now show that this $f(x)$ is not solvable by taking radicals.

Set $E = Q(y_1, \dots, y_5)$. Then the polynomial $f(x)$ in $F[x]$ has E as its splitting field.
Suppose on the contrary that $G = Gal(E/F)$ is solvable for the above polynomial $f(x)$ of degree five.

Consider the composition series of subgroups from $G = G_0$ to $G_r = 1$:

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd G_r.$$

This corresponds to the following extension of fields:

$$F = F_0 \subset F_1 \subset \cdots \subset F_{r-1} \subset F_r.$$

Each extension is cyclic and Galois.

We know that $S_5 = Gal(E/F)$ the commutator group $[S_5, S_5] = A_5$ and that A_5 has no nontrivial normal subgroup. Indeed, the composition series of S_5 is as follows:

$$S_5 \rhd A_5 \rhd 1.$$

Thus $Gal(E/F)$ is not solvable. Hence $f(x)$ is not solvable by radicals by Theorem 1.■

Special Solvable Cases

By the proof above, we know that it is impossible to solve all quintics by radicals, and thus no general solution can be found. However, there are many cases of quintics which are solvable by radicals. A case will be discussed below.

a. Cyclotomic Polynomials

Consider the cyclotomic polynomial $x^5 - 1 = 0$.

By Theorem 1, we know that a polynomial is solvable if and only if its Galois group is solvable. This equation is solvable in radicals as its splitting field is generated by the 5th roots of unity, so the resultant Galois group is also solvable.

The roots of this equation are simply the 5th roots of unity,

$$w_k = e^{\frac{2\pi ik}{5}},$$

where $k \in \{0,1,2,3,4\}$.

These roots of unity can be expressed by radicals.

Similarly, all equations of the form$x^5 - m = 0$, where m is a constant, are solvable by radicals, since the roots are simply

$$w_k = e^{\frac{2\pi ik}{5}} \sqrt[5]{m}\,.$$

Polynomials and the solving of its roots have practical and widespread use in computer applications, the foremost of which is cryptography, or the encryption of sensitive data for sending over the internet. This is especially useful in banking transactions where secrecy and privacy of the individual customer is paramount. Polynomials can be used in public key encryption, as a means to encrypt information. The decryption of a polynomial is hence directly linked to the solvability of this polynomial. Only those with the required decryption key will get to know the real message behind the encrypted message. Being able to solve for a polynomials roots will enable one to create a decryption key, and hence solvability or the lack thereof of such a polynomial, is important in choosing a polynomial as a possible encryption key so that it cannot be hacked.

DISCUSSION

In general, polynomials of degree 5 or greater than 5 cannot be solved using radicals. Polynomials of degree 0,1,2,3 and 4 all can be solved generally by radicals, as there is the quadratic formula for polynomials of degree 2, Cardano's method for polynomials of degree 3, and Ferrari's method for polynomials of degree 4.

While polynomials of degree five or larger cannot be solved by radicals generally, there are many more specific types of polynomials $f(x)$ that can be solved by radicals.

Polynomials of the form $x^5 - m$ for some real number m are solvable, as the Galois group of its splitting field is solvable.

ACKNOWLEDGEMENTS

I sincerely thank my mentor Assoc Professor Zhang De-Qi, for his patient and constant guidance throughout this project. My thanks also to Ms Carmen Hoo, my teacher- mentor for her support.

REFERENCES

[1] Artin, M., Algebra, Prentice-Hall Inc, 1991, Singapore.

[2] Fraleigh, J.B., A First Course in Abstract Algebra. Addison- Wesley, 1997, United States of America.