“Solving Solvable Sextics Using Polynomial Decomposition”

Titus Piezas III

ABSTRACT: Using basic results established by Etienne Bezout (1730-1783) and Niels Henrik Abel (1802-1829), we devise a general method to solve the solvable sextic in radicals by deriving two kinds of resolvents, one kind of the 15th degree and the other of the 10th degree, that factors when the sextic is solvable and thus enabling us to decompose the solvable sextic either as: a) three quadratics whose coefficients are determined by a cubic or b) two cubics whose coefficients are determined by a quadratic.

Mathematics Subject Classification. Primary: 12E12.

Brescia, Italy, 1512

The sound of people shouting and screaming, and the metallic clang of clashing swords, was becoming louder, and the boy hid inside his small room, terrified. His father had gone out to fight the French invaders and it was only days later that the boy would know he would never come back again.

Suddenly, to the boy’s horror, he heard the door of their cottage slam open and the sound of men speaking loudly in a strange language he could not understand. Tables and chairs were being overturned and there were heavy footsteps getting closer to his room.

One of the men entered the room and the boy saw that his clothes were dirty and bloody. The man also saw him, raised his sword and walked towards him.

“*Per favore, no, signore,*” the boy pleaded.

The next thing the boy felt was a horrible pain in his face and warm blood got into his eyes. But before the French soldier could draw his sword a second time, there was a commotion outside the house and the boy could hear Italian voices. The man left him and he blacked out.

The boy would eventually recover from his wounds and become a mathematician. But his injuries damaged his jaw and he could only speak with difficulty. Because of this, he gave himself the nickname, “*Tartaglia*”, or the Stammerer…

I. Introduction

The quest to find formulas to solve equations in one unknown extends as far back in time to the ancient Babylonians of c. 2000 BC, who had knowledge of a version of the quadratic formula. The cubic and quartic formulas in turn were discovered during the Renaissance (the former by Scipione del Ferro and, independently, Niccolo “Tartaglia” Fontana and the latter by Ludovico Ferrari).

The formula to solve the general quintic in radicals obviously was next in the list. A *lot* of mathematicians tried to find the formula and to name some, we have Count Ehrenfried Walter von Tschirnhaus who in the course of trying to solve equations of the *nth* degree found an important transformation that now bears his name, as well as Leonard Euler, Etienne Bezout, Joseph-Louis Lagrange, and Carl Gustav Jacobi.

Erland Bring and, independently, George Jerrard later found a transformation that could eliminate the three terms x^4, x^3, x^2 from the general quintic and thus bring it tantalizingly close to the solvable binomial form. We also have George Young and Arthur Cayley though by this time it was known that one had to solve a sextic in order to solve the quintic. Even the intuitive genius Srinivasa Ramanujan (1887-1920), isolated from the mainstream mathematical community early in his career and perhaps not knowing that Galois theory had already proven it was impossible, tried his hand at solving the quintic and naturally failed.

However, there were also mathematicians who had an inkling that perhaps the general quintic was *not* solvable in radicals. One of the first to try to come up with an argument to prove its impossibility was Paolo Ruffini (1765-1822). Niels Henrik Abel (1802-1829) initially thought he found a solution but when asked to give a numerical example, discovered a mistake in his paper. Eventually he came to the conclusion that it was impossible to solve and later gave a convincing proof, as did Evariste Galois (1811-1832). Charles Hermite (1822-1901), perhaps unaware of the earlier work, also tried to prove its impossibility though it can be said that the last nail on the coffin of solving the general quintic in radicals was already hammered down years before by Abel and Galois.

Before we go to the sextic, perhaps we can be excruciatingly precise on what we mean by "there is no formula in radicals to solve the general quintic". To say that there is *no formula in radicals* is not the same as there is *no formula whatsoever*. The former restricts itself to a "finite number of arithmetic operations and root extractions". The latter has no such restrictions and can go beyond radicals.

Indeed *there are formulas to solve the general quintic with symbolic coefficients*. One, given by Hermite, solves the Bring-Jerrard quintic using *elliptic functions*. Another, by Felix Klein (1849-1925), solves the principal quintic (a quintic on which a Tschirnhausen transformation has been applied to eliminate two terms) using *hypergeometric functions*. So the attempt to solve the quintic in radicals, while futile, has not been totally a waste of effort and is an illustration of how something can be inadvertently useful.

While Galois theory has established that general equations of degree greater than four are not solvable in radicals, there are particular equations that can be solvable as such, which aptly enough are called *solvable equations*. It may be desired to find a general method to solve solvable equations of a certain degree greater than four and find the exact expressions for its roots. We have discussed the case of solvable quintics in previous papers. Perhaps it is now time to tackle solvable equations of the next degree in line, namely, the sextic.

While the quintic degree has five transitive groups, three of which are solvable (the cyclic group of order 5, dihedral group of order 10, and Frobenius group of order 20), the sextic degree has sixteen transitive groups, twelve of which are solvable:

GAP/Magma #	Order	Solvability
6T1	(2)(3)	Y
6T2	(2)(3)	Y
6T3	$(2^2)(3)$	Y
6T4	$(2^2)(3)$	Y
6T5	$(2)(3^2)$	Y
6T6	$(2^3)(3)$	Y
6T7	$(2^3)(3)$	Y
6T8	$(2^3)(3)$	Y
6T9	$(2^2)(3^2)$	Y
6T10	$(2^2)(3^2)$	Y
6T11	$(2^4)(3)$	Y
6T12	$(2^2)(3)(5)$	N
6T13	$(2^3)(3^2)$	Y
6T14	$(2^3)(3)(5)$	N
6T15	$(2^3)(3^2)(5)$	N
6T16	$(2^4)(3^2)(5)$	N

Table 1.

The transitive groups are numbered according to the convention set by GAP or Magma. For the precise names of the groups, the interested reader is referred to the database of number fields by Klueners and Malle cited in the References.

If the quintic is somehow "special" being the first degree that is not generally solvable in radicals, the sextic is also special in its own way. For one, important for the method that we are using, is that the factorization of the degree of the sextic involves only the primes less than five.

Another, it is the first degree m that is the auxiliary resolvent of one degree, the quintic, and the Lagrange resolvent of another, namely, the septic or septemic. Degrees m that can be both auxiliary and Lagrange resolvents are factorials $m = (n-2)!$ such that both n and $(n-2)!+1$ are prime, the latter being called a factorial prime which are quite rare, only twenty of the positive form known so far. The next such degree is the humongous $m = 11! = 39{,}916{,}800^{th}$, such that m is the auxiliary and Lagrange resolvent of the 13th and 39,916,801th degree, respectively.

Since the sextic is a composite degree, it seems the most efficient method to solve it would be different than the one used to solve the quintic which is a prime degree. The importance of primes and its significance in various mathematical contexts perhaps cannot be understated. The general approach to prime degrees, using results established by Lagrange, was discussed in a previous paper, "*An Easy Way To Solve The Solvable Quintic Using Two Sextics*" by the same author.

For composite degrees *pq* it seems an efficient method, using results established by Bezout and Abel, would be *to decompose it as a number q equations of degree p whose coefficients are determined by an equation of degree q*. For distinct primes *p* and *q*, as they can be interchanged, its decomposition then can be in two ways.

Let us give as an example of this method of decomposition, for the particular case of the sextic, a "natural" solvable sextic, a class polynomial associated with an elliptic function of period $\sqrt{-35}$,

$$x^6 - 2x^5 - 2x^4 + 4x^3 - 4x + 4 = 0$$

As a side note, we can mention that class polynomials have an interesting connection to transcendental numbers of the form e^{pp}, especially for p as a quadratic irrational. For example, a numerical root of the above sextic is given by x = 2.169318… while the value of $(e^{p\sqrt{35}} + 24)^{1/24}$ is 2.169318… which starts to differ from *x* only in the 14th decimal place. However, if we want the exact representation of *x*, we can do it in two ways:

a) Expressed as three quadratics in the variable *x*, we have,

$$x^2 + mx + (m^2 + 2m - 2) = 0$$

where *m* is any root of the cubic,

$$m^3 + 2m^2 - 4m + 2 = 0$$

b) Or expressed as two cubics, we have

$$x^3 + mx^2 - mx - 2 = 0$$

where *m* is any root of the quadratic,

$$m^2 + 2m - 4 = 0$$

The resulting quadratic or cubic in the variable *x* and *m* can then be solved by known methods. Obviously, the problem is how to find the decomposition of the solvable sextic. That is what this paper aims to solve.

II. The Method

The basis for the method that we will use here primarily comes from two well-established results. First, the one from Bezout. In his paper, "*Sur plusieurs classes d'equations de tous les degrees qui admettent une solution algebrique*", he discusses how a single equation in a single unknown can be approached as two equations in two unknowns. To quote,

"It is known that a determinate equation can always be viewed as the result of two equations in two unknowns, when one of the unknowns is eliminated."

That is precisely what we did in the above example. We reduced the problem of solving that sextic to solving either a cubic or a quadratic, which can then be easily solved. And to know whether the two equations in the two unknowns share roots in common with the sextic, by eliminating *m* between the two equations, one can see that indeed it will give us back the original sextic in the unknown x.

The second is from Abel. In his paper, *"Memoire sur une classe particuliere d'equations resolubles algebriquement"* (1829), he wrote,

Theorem 8.1 "The equation under consideration $fx = 0$ (of degree pq) can thus be decomposed into a number q of equations of degree p in which the coefficients are rational functions of a fixed root of a single equation of degree q, respectively."

Note that Abel made no mention of the rationality of the coefficients of the equation of degree *q*. While we may expect this equation to have rational coefficients, as indeed may be case, we shall see that with certain higher degree equations, this is not always the case.

Using these two results, the obvious conclusion, for the particular case of the solvable sextic, is that we can express it either as: a) three quadratics with coefficients determined by a cubic, or b) two cubics with coefficients determined by a quadratic. Let us explore the first case.

Given the sextic,

$$x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0 \qquad (1)$$

we can express it as,

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5)(x - x_6) = 0 \qquad (2)$$

or as three quadratics,

$$\left(x^2 - (x_1 + x_2)x + x_1x_2\right)\left(x^2 - (x_3 + x_4)x + x_3x_4\right)\left(x^2 - (x_5 + x_6)x + x_5x_6\right) = 0 \qquad (3)$$

or simply,

$$x^2 - (x_i + x_j)x + x_i x_j = 0$$

The objective then is find the polynomials, say, in the variables *y* and *z*, formed by taking a) the sum of two roots of the sextic at a time, and b) the product of two roots at a time,

a) $\prod_{i<j} y - (x_i + x_j) = 0$

b) $\prod_{i<j} z - (x_i x_j) = 0$

The degree *k* of the polynomial in *y* or *z* is a simple combinatorial question of *n* objects taken *r* at a time and is given by,

$$k = \frac{n!}{r!(n-r)!} = \frac{6!}{2!4!} = 15$$

So we have two 15th degree polynomials. Since these are formed from elementary symmetric polynomials, we know that their coefficients would be expressible in terms of the coefficients of the sextic. The problem now is how then to find the explicit expressions of the coefficients of the 15th degree polynomials. We can use Newton's relations or variations of power sums but since we are talking about a 15th degree polynomial, it might tax the capabilities of a rather slow computer.

There is a clever way to find the polynomial in *y* or *z*. We simply express (2) as the product of a quartic and a quadratic:

$$\left(x^4 + r_1 x^3 + r_2 x^2 + r_3 x + r_4\right)\left(x^2 + mx + n\right) = 0 \qquad (4)$$

where one can see that $m = -(x_i + x_j)$ and $n = (x_i x_j)$. By expanding (4) and comparing coefficients with (1), we have a system of six equations in six unknowns, namely,

$$m + r_1 = a$$
$$n + mr_1 + r_2 = b$$
$$nr_1 + mr_2 + r_3 = c$$
$$nr_2 + mr_3 + r_4 = d$$
$$nr_3 + mr_4 = e$$
$$nr_4 = f$$

By eliminating the r_i, we will be left with two equations in the two desired unknowns *m* and *n*, and by eliminating either one, we will have our 15th degree polynomials. Solving for the r_i in the first four equations, we get,

$$r_1 = a - m$$
$$r_2 = b - am + m^2 - n$$
$$r_3 = c - bm + am^2 - m^3 - an + 2mn$$
$$r_4 = d - cm + bm^2 - am^3 + m^4 - bn + 2amn - 3m^2n + n^2$$

And substituting these into the last two, we end up with two equations in the unknowns *m* and *n*,

$$(3m - a)n^2 - (4m^3 - 3am^2 + 2bm - c)n + m^5 - am^4 + bm^3 - cm^2 + dm - e = 0 \quad (5)$$

and,

$$n^3 - (3m^2 - 2am + b)n^2 + (m^4 - am^3 + bm^2 - cm + d)n - f = 0 \quad (6)$$

Eliminating *n* in (5) and (6) by getting their resultant, and assuming a reduced sextic with *a = 0* so that our symbolic 15th degree will not be so unwieldy, we get,

$$\begin{aligned} &m^{15} + 4bm^{13} - 2cm^{12} + 2(3b^2 - d)m^{11} - 2(3bc - 5e)m^{10} + 2(2b^3 - bd - 13f)m^9 \\ &- 6(b^2c - cd - 2be)m^8 + (b^4 + 2b^2d - 7d^2 - 3ce - 24bf)m^7 \\ &- 2(b^3c - c^3 - 2bcd - b^2e - 5de + 15cf)m^6 + 2(b^3d - 3c^2d - 3bd^2 + 3bce \\ &- 6e^2 - 9b^2f + 27df)m^5 - 2(-bc^3 + b^2cd - 4cd^2 + 3c^2e - bde + 3bcf + 9ef)m^4 \\ &+ (-c^4 - 2bc^2d + b^2d^2 - 4d^3 + b^2ce + 7cde - 5be^2 - 4b^3f + 3c^2f + 18bdf - 27f^2)m^3 \\ &+ 2c(c^2d - 3e^2)m^2 + (-c^2d^2 - c^3e + bcde - b^2e^2 + 3de^2 + 3bc^2f - 9cef)m \\ &+ c^2de - bce^2 + e^3 - c^3f = 0 \end{aligned} \quad (7)$$

then eliminating *m*,

$$\begin{aligned} &n^{15} - bn^{14} - dn^{13} + (-c^2 + 2bd - f)n^{12} + (-d^2 + ce + 2bf)n^{11} \\ &(-bd^2 + 2bce - 2e^2 - 2b^2f + 2df)n^{10} + (d^3 - 3cde + be^2 + 3c^2f - 2f^2)n^9 \\ &+ (-b^2e^2 + de^2 + 2b^2df - d^2f - 3cef)n^8 + (bde^2 - 2bd^2f - bcef + e^2f + b^2f^2)n^7 \\ &+ (-ce^3 + 3cdef + be^2f - b^3f^2 - 3c^2f^2 + 2f^3)n^6 + (e^4 - 4de^2f + b^2df^2 + 2d^2f^2 \\ &+ 3cef^2 - 2bf^3)n^5 + f^2(-bce + e^2 + b^2f - 2df)n^4 + f^2(be^2 + c^2f - 2bdf + f^2)n^3 \\ &- f^3(ce - bf)n^2 + df^4n - f^5 = 0 \end{aligned} \quad (8)$$

and we have our 15th degree resolvents! While reducing the sextic is easy to do, in actual use one can just substitute the numerical values into (5) and (6) and a good computer algebra system can easily find its resultant without one having to set $a = 0$.

Theorem 1. If the irreducible sextic $P(x) = x^6 + bx^4 + cx^3 + dx^2 + ex + f = 0$ with rational coefficients is solvable in radicals, then (7) and (8) factors into lower degrees also with rational coefficients, with the degree evenly divisible only by a number less than or equal to three.

We can easily prove the above statement. It is known that a transitive subgroup of the symmetric group S_6 is solvable if and only if it is imprimitive. For the sextic degree, there are only two possibilities: two blocks of size three or three blocks of size two. One can see from Table 1 that only twelve groups can be solvable.

Tthe number field generated by the roots of an irreducible but solvable sextic has a subfield, of degree less than a sextic, *only as a quadratic or cubic subfield*. *It does not have a quintic subfield.* If (7) or (8) was irreducible for solvable P(x), and we know that they were formed from the roots x_i of P(x) as sums or products taken two at a time, then we would have the peculiar situation *of an irreducible but solvable 15th degree equation expressible in terms of a cubic or quadratic subfield that does not need a quintic subfield, which is absurd*.

Thus, (7) or (8) must be factorable for solvable P(x). And for the same reasons cited above, it cannot have an irreducible factor of some degree r where r has a prime factor k greater than three, otherwise we would have a solvable equation of degree *r* that does not need a *kth* subfield. So, its possible factorizations would be of degrees (3,12) and (6,9) with the factor of the higher degree possibly factorizing further. If the factorization is (3,12), then we have reached our goal, namely, to decompose the sextic into a quadratic with coefficients determined by a cubic.

If the factorization is (6,9), it seems our sextic just gave birth to another sextic. We cannot assume that it will factorize further. However, we did say that decomposition for distinct *p* and *q* can be done *in two ways* so we can explore that other avenue, namely to decompose the sextic into a cubic with coefficients determined by a quadratic. In other words, we are simply factoring the sextic over a square root extension.

This time, we can express (2) as a product of two cubics,

$$\left(x^3 + r_1 x^2 + r_2 x + r_3\right)\left(x^3 + mx^2 + nx + r_4\right) = 0 \tag{9}$$

where $m = -(x_i + x_j + x_k)$, $n = (x_i x_j + x_i x_k + x_j x_k)$, and $r_4 = -(x_i x_j x_k)$. The degree *h* of the polynomial formed by the sum of roots of the sextic taken three at a time, would be,

$$h = \frac{n!}{r!(n-r)!} = \frac{6!}{3!3!} = 20$$

which we shall see later can be reduced to a 10th degree equation. By expanding (9) and comparing terms with (1), we have,

$$\begin{aligned}
&m + r_1 = a \\
&n + mr_1 + r_2 = b \\
&nr_1 + mr_2 + r_3 + r_4 = c \\
&nr_2 + mr_3 + r_1 r_4 = d \\
&nr_3 + r_2 r_4 = e \\
&r_3 r_4 = f
\end{aligned}$$

Solving for the r_i in the first four equations we get,

$$\begin{aligned}
r_1 &= a - m \\
r_2 &= b - am + m^2 - n \\
r_3 &= \frac{-ac + d + (ab + c)m - (a^2 + b)m^2 + 2am^3 - m^4 + (a^2 - b - 2am + m^2)n + n^2}{-a + 2m} \\
r_4 &= \frac{d - cm + bm^2 - am^3 + m^4 - (b - 2am + 3m^2)n + n^2}{a - 2m}
\end{aligned}$$

and substituting the r_i into the last two, the fifth becomes a cubic in n,

$$\begin{aligned}
&bd - ae - (bc + ad - 2e)m + (b^2 + ac + d)m^2 - (2ab + c)m^3 + (a^2 + 2b)m^4 - 2am^5 + m^6 \\
&+ (-b^2 + ac - 2d + 2abm - a^2m^2 - 4bm^2 + 4am^3 - 3m^4)n \\
&+ (-a^2 + 3b - am + 3m^2)n^2 - 2n^3 = 0
\end{aligned} \tag{10}$$

and the sixth a quartic in n,

$$\begin{aligned}
&acd - d^2 - a^2 f - a(c^2 + bd - 4f)m + (2abc + c^2 + a^2 d - 4f)m^2 \\
&- (ab^2 + 2a^2 c + 2bc + ad)m^3 + (2a^2 b + b^2 + 4ac)m^4 - (a^3 + 4ab + 2c)m^5 \\
&+ (3a^2 + 2b)m^6 - 3am^7 + m^8 \\
&+ \begin{pmatrix} -abc - a^2 d + 2bd + a(b^2 + 3ac)m + (-4a^2 b - 7ac + 2d)m^2 \\ + (3a^3 + 8ab + 4c)m^3 - 2(5a^2 + 2b)m^4 + 11am^5 - 4m^6 \end{pmatrix} n \\
&+ \left(a^2 b - b^2 + ac - 2d - a(2a^2 + b)m + 2(4a^2 - b)m^2 - 9am^3 + 3m^4\right) n^2 \\
&+ \left(-a^2 + 2b + 2m^2\right) n^3 - n^4 = 0
\end{aligned} \tag{11}$$

Eliminating n between (10) and (11) we get a 24th degree equation in the variable m with the spurious factor $(a - 2m)^4$. So we really just have a 20th degree equation, as expected.

However, as mentioned earlier, we can still reduce this to a 10th degree equation. The coefficient *a* of the x^5 term of the sextic is $a = -(x_1 + x_2 + x_3 + x_4 + x_5 + x_6)$ and by depressing the sextic by setting *a = 0*, then $(x_1 + x_2 + x_3) = -(x_4 + x_5 + x_6)$. Since our equation in *m* is formed by the sum of the roots taken three at a time, one can see that of the twenty possible values, the last ten will just be the negation of the first ten. So for the depressed sextic (a = 0), our equation in *m* has just even degrees. By letting $m = \sqrt{t}$, it will become a 10th degree equation, call it *Q(t)*, in the variable *t*.

In actual practice, if one has access to a computer algebra system, it is preferable to use (10) and (11) as it is cumbersome to have this 10th degree equation in symbolic form. However, for purposes of demonstration, we can write it down with the further assumption *b = 0*, with no loss of generality, so that its coefficients will not be too unwieldly.

$$\begin{aligned}
Q(t) &= t^{10} - 6dt^8 - 3(c^2 - 22f)t^7 + (d^2 + 36ce)t^6 + 3(4c^2d - 41e^2 + 38df)t^5 \\
&+ 3(c^4 + 8d^3 - 46cde + 46c^2f + 43f^2)t^4 - 2(c^2d^2 + 18c^3e - 47de^2 - 40d^2f + 171cef)t^3 \\
&+ (-6c^4d + 16d^4 - 24cd^2e + 51c^2e^2 - 6c^2df + 66e^2f + 120df^2)t^2 \\
&+ (-c^6 + 8c^2d^3 - 6c^3de - 8d^2e^2 - 14ce^3 + 12c^4f + 32d^3f + 24cdef - 48c^2f^2 + 64f^3)t \\
&+ (c^2d + e^2 - 4df)^2 = 0
\end{aligned}$$

Theorem 2. If the irreducible sextic $P(x) = x^6 + bx^4 + cx^3 + dx^2 + ex + f = 0$ with rational coefficients is solvable in radicals, by eliminating *n* between (10) and (11), disregarding the spurious factor $(a\text{-}2m)^4$, and letting $m = \sqrt{t}$, then the 10th degree equation *Q(t)* will factor into lower degrees also with rational coefficients, with the degree evenly divisible only by a number less than or equal to three.

The proof is basically the same as for Theorem 1. Since *Q(t)* is expressible in terms of the sum of the roots of the sextic, if it were irreducible for solvable *P(x)* then we would have an irreducible but solvable 10th degree equation that does not need a quintic subfield, which is impossible. So *Q(t)* must be factorable for solvable *P(x)*.

In the same manner, we know that its factors must not be of degree *r* where *r* has a prime factor greater than three. So the permissible factorizations of *Q(t)* would be of degrees (1,9), (2,8), and (4,6), with the factor of the larger degree possibly still reducible. However, its further factorization is not that relevant. What is important is the result that if *P(x)* is solvable, then Q(t) has factors either of degree 1, 2, 4 (and possibly also 3 if the factor with the larger degree is reducible), all of which obviously are solvable in radicals.

If its factor is of degree 1, then we have reached our aim, namely, to decompose the solvable sextic into a cubic whose coefficients are determined by a quadratic since we are after the original variable *m* and $m = \sqrt{t}$. The reduced sextic would factor into 2 cubics over the extension $\sqrt{t}$. Or, if the sextic was not reduced, would factor over the square root of the discriminant of the quadratic factor in the variable *m*.

If the factor of *Q(t)* is of degree 2, 3, or 4, obviously we can still use it to find all the unknowns of our cubic, namely, m, n, and r_4. After finding m, to find n, one need only substitute the value of m into (10) or (11) to have either a cubic or a quartic in n, which again would be solvable in radicals. Then substitute the value of m and n into the expression for r_4 and we have all our unknowns.

Our second approach then, modified such that it seeks to decompose the reduced solvable sextic into a cubic whose coefficients are determined by an equation of degree not greater than four, *seems to be the general formula to solve irreducible but solvable sextics*.

However, while it would suffice to solve all solvable sextics, the obvious problem in exclusively using that approach is that it may unnecessarily complicate matters. If in a particular case the first method yields a cubic, while the second yields a quartic, then the former can give a simpler expression for the roots of the sextic. If we are to be guided by aesthetic principles, then the two methods should complement each other: whichever yields a simpler expression for a specific case, then that should be the preferred method to use.

III. Examples

Before we go to the examples, we can point out one drawback of the two approaches, as well as its solution. Using the first approach, we seek to decompose the solvable sextic into a quadratic determined by a cubic (two, in fact). Given the sextic,

$$x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

we wish to find the quadratic,

$$x^2 + mx + n = 0$$

with roots in common with the sextic and where m and n are roots of the cubics,

$$m^3 + pm^2 + qm + r = 0$$

and,

$$n^3 + s_1 n^2 + s_2 n + s_3 = 0$$

The obvious problem is: which root of one cubic goes with which root of the other? There is a similar problem with the second approach, though if the resolvent yields a linear factor t, (for the reduced sextic) that is all that is needed as the sextic would factor into two cubics over the extension $\sqrt{t}$ which computer algebra systems can easily do.

The solution has already been implied in Abel's theorem when he said, *"…the coefficients are rational functions of a fixed root of a single equation"*. Thus, we need to express the roots of the one cubic with respect to the other. In other words, we seek to find a transformation that will transform one equation into the other. In a previous paper, "*Solving The Solvable Quintic Using One Fifth Root Extraction*" by the same author, we established the theorem (Theorem 2) that,

"Any solvable equation Q(x), with no repeated roots, can be transformed into any solvable form P(y) of the same degree in radicals using a Tschirnhausen transformation of degree n-1."

Given,

$$Q(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

we transform it into,

$$P(y) = y^n + c_{n-1}y^{n-1} + \ldots + c_1 y + c_0 = 0$$

for known a_i and c_i using the *n-1* degree Tschirnhausen transformation,

$$y = b_n x^{n-1} + b_{n-1}x^{n-2} + \ldots + b_1 x + b_0$$

where the b_i are unknown and have to be solved for.

Thus, to transform our *m* cubic,

$$m^3 + pm^2 + qm + r = 0$$

into the *n* cubic,

$$n^3 + s_1 n^2 + s_2 n + s_3 = 0$$

we need the quadratic Tschirnhausen transformation,

$$n = um^2 + vm + w$$

with the unknowns *u, v, w*. Forming the cubic, we have,

$$(n - (um_1^2 + vm_1 + w))(n - (um_2^2 + vm_2 + w))(n - (um_3^2 + vm_3 + w)) = 0$$

Collecting the variable *n* and expressing the m_i in terms of the coefficients of the *m* cubic, we have,

$$n^3 + P(a)_1 n^2 + P(a)_2 n + P(a)_3 = 0$$

where the $P(a)_i$ are polynomials in the unknowns *u, v, w*. Equating with the coefficients s_i of the *n* cubic, we have,

$$P(a)_1 = s_1 = -p^2u + 2qu + pv - 3w$$
$$P(a)_2 = s_2 = q^2u^2 - 2pru^2 - pquv + 3ruv + qv^2 + 2p^2uw - 4quw - 2pvw + 3w^2$$
$$P(a)_3 = s_3 = -r^2u^3 + qru^2v - pruv^2 + rv^3 - q^2u^2w + 2pru^2w + pquvw$$
$$- 3ruvw - qv^2w - p^2uw^2 + 2quw^2 + pvw^2 - w^3$$

Since we have three equations in three unknowns, we can resolve this into a single equation in a single unknown, and hence this system has a definite set of solutions. A system of equations with degrees 1, 2, 3 will yield, from a theorem established by Bezout, a final equation of degree n! = 3! = 6. While we end up with a sextic, we know from Theorem 2 of the previous paper cited earlier that this sextic will always be solvable in radicals even if it is not generally reducible.

However, we are not transforming a random cubic into another random one. Our *m* and *n* cubics are somehow "related" and we can generate additional information about our system of equations to simplify it. Perhaps then our final equation will be of smaller degree. In fact, we can prove that indeed this is the case and that *u, v, w* are just rational numbers.

Since our sextic is given by,

$$(x^2 + m_1x + n_1)(x^2 + m_2x + n_2)(x^2 + m_3x + n_3) = 0$$

Using the Tschirnhausen transformation defined for the n_i, it is equivalent to,

$$(x^2 + m_1x + um_1{}^2 + vm_1 + w)(x^2 + m_2x + um_2{}^2 + vm_2 + w)(x^2 + m_3x + um_3{}^2 + vm_3 + w) = 0$$

Collecting the variable *x* and again expressing the m_i in terms of the coefficients of the *m* cubic, we have,

$$x^6 + P(b)_1x^5 + P(b)_2x^4 + P(b)_3x^3 + P(b)_4x^2 + P(b)_5x + P(b)_6 = 0$$

where the $P(b)_i$ are *alternative polynomials* in the unknowns *u, v, w*. Equating with the coefficients of the sextic,

$$P(b)_1 = a = -p$$

$$P(b)_2 = b = q + p^2u - 2qu - pv + 3w$$
$$P(b)_3 = c = -r - pqu + 3ru + 2qv - 2pw$$
$$P(b)_4 = d = pru + q^2u^2 - 2pru^2 - 3rv - pquv + 3ruv + qv^2 + qw + 2p^2uw - 4quw - 2pvw + 3w^2$$
$$P(b)_5 = e$$
$$P(b)_6 = f$$

where the explicit expressions for the last two polynomials are not needed. Since we already have established that the unknowns *u, v, w* have a definite set of solutions, then it is valid to solve the system of equations involving $P(b)_2$, $P(b)_3$, and $P(b)_4$. It has degrees *1, 1, 2* so the final equation of this system is only a quadratic, with one root in common with the previous system. However, inspecting $P(b)_4$, one can see that it can be expressed in terms of $P(a)_3$ of the previous set. So our final system of equations would be,

$$\begin{aligned} b &= q + p^2u - 2qu - pv + 3w \\ c &= -r - pqu + 3ru + 2qv - 2pw \\ d &= pru - 3rv + qw + s_2 \end{aligned} \tag{12}$$

and (12) is *just a linear system in the unknowns u, v, w*. If the known variables *b, c, d, p, q, r,* s_2 are rational then the unknown ones are also rational and we have proven our assertion.

Example 1.

The author has observed that it seems that the first method is preferable for the five transitive groups 6T4, 6T6, 6T7, 6T8, and 6T11.

Given the solvable sextic with transitive group 6T8,

$$x^6 + x^4 - 4x^3 + 7x^2 - 2x - 5 = 0$$

Using the first method, by eliminating *n* in (5) and (6), our 15th degree equation in *m* factors into,

$$(m^3 - 4m - 2)\big(P(m)\big) = 0$$

and eliminating *m*, our 15th degree equation in *n* has factors,

$$(n^3 - 5n^2 + 3n + 5)\big(P(n)\big) = 0$$

where *P(m)* and *P(n)* are irreducible 12th degree polynomials.

Using the second method, by eliminating n in (10) and (11), we get the 20th degree equation in m which factors, disregarding the spurious linear factor of multiplicity four, into,

$$(81 - 40m^2 + 54m^4 + 12m^6 + m^8)(729 - 486m^2 - 81m^4 - 40m^6 - 9m^8 - 6m^{10} + m^{12}) = 0$$

By setting $m = \sqrt{t}$, we have quartic and sextic factors in the variable t. Since the first method yields a factor with a smaller degree, it is preferable to use it.

We transform the m cubic into the n cubic, or equivalently, express the roots of the latter in terms of the former. The m cubic gives us $p = 0$, $q = -4$, $r = -2$, the n cubic gives us $s_2 = 3$, and the sextic gives us $b = 1$, $c = -4$, $d = 7$. Substituting these values into the linear system (12), we get,

$$\begin{aligned} -4 + 8u + 3w &= 1 \\ 2 - 6u - 8v &= -4 \\ 3 + 6v - 4w &= 7 \end{aligned}$$

then solving for the unknowns u, v, w, we have,

$$u = 1,\ v = 0,\ w = -1$$

So the solution of the sextic,

$$x^6 + x^4 - 4x^3 + 7x^2 - 2x - 5 = 0$$

is given by the quadratic in x,

$$x^2 + mx + (m^2 - 1) = 0$$

with coefficients determined by the cubic,

$$m^3 - 4m - 2 = 0$$

Example 2.

For some groups, 6T1, 6T2, and 6T3 (the cyclic and dihedral groups), it seems it does not matter which method is used. If the first is used, the resolvent has a cubic factor. If the second, it has a quadratic factor. Just like the sextic class polynomial given as an example in the introduction.

Furthermore, if the first method is used, either or both of the 15th degree resolvents in the variables m and n may have several cubic factors, thus adding the complication of which cubic factor of one variable goes with which cubic factor of the other. One can easily resort to the second method but we can give a solution to this complication. Let us give as an example, a sextic of group 6T2,

$$x^6 - 3x^5 - 2x^4 + 9x^3 - 5x + 1 = 0$$

By eliminating *n* in (5) and (6), our 15th degree equation in *m* factors as,

$$(1+m)^3(-5-m+3m^2+m^3)(-1-m+3m^2+m^3)\big(P(m)\big)=0$$

and eliminating *m*, our 15th degree equation in *n* factors as,

$$(-1-5n+n^2+n^3)(-1-3n+n^2+n^3)(-1+5n+5n^2+n^3)\big(P(n)\big)=0$$

where *P(m)* and *P(n)* are irreducible 6th degree polynomials. We have three cubic factors. The first method can then solve this particular sextic in three ways though we have to first figure out which are the correct cubic pairs in *m* and *n*.

The solution is simply to choose one cubic in *m* and using (5) or (6), eliminate *m* yielding a sextic or nonic in *n*, which should factor and indicate the proper partner. Selecting $-5-m+3m^2+m^3$ and eliminating *m* in (5), the sextic in *n* factors as,

$$(-1-3n+n^2+n^3)(5+9n-45n^2+27n^3)=0$$

and we know the first factor is the proper partner. Doing the same to the others, we find the correct pairings are,

$$-1-m+3m^2+m^3 \qquad \& \qquad -1-5n+n^2+n^3$$

and,

$$(1+m)^3 \qquad \& \qquad -1+5n+5n^2+n^3$$

Transforming the first *m* cubic into its partner *n* cubic, we have $p = 3, q = -1, r = -5, s_2 = -3, b = -2, c = 9, d = 0$. Solving our system of equations (12) for the unknowns *u, v, w*, we get,

u = 1, v = 1, w = -3

Transforming the second *m* cubic, we have $p = 3, q = -1, r = -1, s_2 = -5, b = -2, c = 9, d = 0$. Solving (12) a second time we have,

u = 1, v = 2, w = -2

Since the third m cubic has repeated roots, we cannot transform it. But there is no need anyway as there is only one root m that goes with the three roots n_i.

Thus, the solution of our sextic,

$$x^6 - 3x^5 - 2x^4 + 9x^3 - 5x + 1 = 0$$

as a decomposition into a quadratic in x can be done in three ways, namely,

$$x^2 + mx + (m^2 + m - 3) = 0 \qquad [1]$$
$$x^2 + mx + (m^2 + 2m - 2) = 0 \qquad [2]$$
$$x^2 - x + n = 0 \qquad [3]$$

where the coefficients are determined by the cubics,

$$-5 - m + 3m^2 + m^3 \qquad [1]$$
$$-1 - m + 3m^2 + m^3 \qquad [2]$$
$$-1 + 5n + 5n^2 + n^3 \qquad [3]$$

applied respectively.

The other way to solve this sextic is to use the second method. Our sextic is in unreduced form. But since the general result of our Theorem 2 (that the resultant of (10) and (11) will have no irreducible factor of degree r such that r has a prime factor greater than three) will hold whether we reduce it or not, then there really is no need to reduce it.

Eliminating n in (10) and (11), our 20th degree equation factors as,

$$(-7 + 3m + m^2)(P(m)_1)(P(m)_2)(P(m)_3) = 0$$

disregarding the spurious factor $(3+2m)^4$ and where the $P(m)_i$ are irreducible sextic equations. Solving the quadratic, we have,

$$m = \frac{-3 \pm \sqrt{37}}{2}$$

We can go through the tedious process of deriving the other unknowns, namely n and r_4. However, since m determines a coefficient of the cubic, we know that the sextic factors over the extension $\sqrt{37}$, something which any good computer algebra system (CAS) can do, though it can be mentioned that for most CAS, factoring over an extension is not automatic and one has to be first specify to the system under what particular extension it has to work with.

Telling the computer to factor over $\sqrt{37}$ we then get,

$$\left(2-(5+\sqrt{37})x+(3+\sqrt{37})x^2-2x^3\right)\left(-2+(5-\sqrt{37})x-(3-\sqrt{37})x^2+2x^3\right)=0$$

Example 3.

For the remaining solvable transitive groups, 6T5, 6T9, 6T10, 6T13, it seems the preferred method is the second one, since using the first method just gives another sextic. Given the solvable sextic with group 6T5,

$$x^6-x^5-6x^4+7x^3+4x^2-5x+1=0$$

Using the first method, eliminating *n* in (5) and (6), our resultant factors as,

$$(-4+8m+8m^2-10m^3-6m^4+2m^5+m^6)\left(P(m)\right)=0$$

then eliminating *m* in (5) and (6),

$$(1+n-6n^2-7n^3+4n^4+5n^5+n^6)\left(P(n)\right)=0$$

where *P(m)* and *P(n)* are irreducible 9^{th} degree polynomials. Since the smallest factor is just another sextic, we are no better off than when we started. Fortunately, there is the second method.

Eliminating *n* in (10) and (11), our 20^{th} degree equation factors as,

$$(-1+m+m^2)\left(P(m)\right)=0$$

disregarding the spurious factor $(1+2m)^4$ and where P(m) is an irreducible 18^{th} degree equation. Solving the quadratic, we get,

$$m=\frac{-1\pm\sqrt{5}}{2}$$

and we know our sextic factors over the extension $\sqrt{5}$, given by,

$$\left(-2+(5-\sqrt{5})x+(1+\sqrt{5})x^2-2x^3\right)\left(2-(5+\sqrt{5})x-(1-\sqrt{5})x^2+2x^3\right)=0$$

Example 4.

While we have focused on sextics with coefficients in the rational field, our results are also valid for other fields. Consider the solvable sextic with coefficients in the quadratic field,

$$x^6-(3-\sqrt{3})x^5-(9+5\sqrt{3})x^4+6(3+\sqrt{3})x^3+6(7+4\sqrt{3})x^2-6(21+11\sqrt{3})x+18(1+\sqrt{3})=0$$

Using the first method, our 15th degree resolvent factors over $\sqrt{3}$ into a sextic and a nonic. But with the second, our 20th degree resolvent factors into,

$$(21+15\sqrt{3}-(3-\sqrt{3})m-m^2)\big(P(m)\big)=0$$

where P(m) is an irreducible 18th degree equation. Solving for *m*, we have,

$$m=\frac{-3+\sqrt{3}\pm\sqrt{96+54\sqrt{3}}}{2}$$

and we know our sextic factors over the quartic extension $\sqrt{96+54\sqrt{3}}$. Letting the computer do the leg work, we find one cubic factor is given by,

$$2x^3+\left(-3+\sqrt{3}-\sqrt{96+54\sqrt{3}}\right)x^2+2\left(6+5\sqrt{3}+\sqrt{15+6\sqrt{3}}\right)x-6\left(2+\sqrt{3}+\sqrt{5+2\sqrt{3}}\right)=0$$

IV. Conclusion: Beyond The Sextic

So we now have the answer to our question on how to decompose the sextic and, consequently, a method to solve the solvable sextic. It is only fitting to ask if the method can be extended to other composite *pq*.

It certainly can, with some disclaimers. First, we were exploiting the fact mentioned early in the paper that, conveniently for us, for the particular case of the sextic, *p* and *q* are both less than five. When we decompose it as an equation of degree *p* with coefficients determined by an equation of degree *q*, regardless of what factor is set as *p* or *q*, we are guaranteed that it will always be solvable. Obviously, it will not always be the case for other composite degrees. For the decic, since one factor of the degree is greater than four, there is no guarantee that the decomposition will yield a solvable equation.

One can easily construct a decic, say, from a quadratic whose coefficients are rational functions of the roots of an unsolvable quintic. Factoring the 45th degree resolvent polynomial formed by taking the sum of the roots of this decic two at a time, one can recover this quintic. But the decic will still be unsolvable. If the decic was solvable to begin with, then our method can certainly apply.

Second, even if the factors of the degree will be less than five, like for the octic or nonic, there are certain complications. For one, something which was also alluded to earlier, is that it was never maintained that for solvable equations of composite degree *pq*, the equation of degree *q* that determines the coefficients will have rational coefficients, even if the original equation of degree *pq* was such.

For the sextic, it was true enough. However, it is not necessarily the case for *certain* solvable groups of the octic or nonic. One might think that for the nonic degree, since $p = q$, then the solvable nonic has no alternative but a cubic determined by a cubic with rational coefficients.

However, there are solvable nonics such that it can be decomposed into a cubic with coefficients determined by a *sextic*. In other words, its 84th degree resolvent polynomial formed by taking the sum of its roots three at a time has a sextic as the smallest factor. An example is the nonic,

$$x^9 - 2x^8 + 8x^7 - 8x^6 + 20x^5 - 8x^4 + 4x^3 - 24x^2 + 23x - 6 = 0$$

whose solution is given by,

$$x^3 + F(m)_1 x^2 + F(m)_2 x + F(m)_3 = 0$$

where the coefficients $F(m)_i$ are rational functions of a root of the sextic,

$$m^6 + 4m^5 + 2m^4 - 4m^3 + m^2 - 8 = 0$$

which is one of two sextics that are the smallest factors of the 84th degree resolvent. However, this sextic factors over $\sqrt{2}$, so we actually have the solution of this nonic as,

$$x^3 + mx^2 + \left((2-\sqrt{2})m^2 - 1 + 2\sqrt{2}\right)x - \left((2-\sqrt{2})m^2 + m - 2 + 2\sqrt{2}\right) = 0$$

where,

$$m^3 + 2m^2 - m + 2\sqrt{2} = 0$$

so indeed it is a cubic determined by another cubic, though with irrational coefficients.

For certain octics and other nonics, the solution is not so easy, though perhaps we can reserve more discussion on octics and nonics for another time. Thus, one can say that this is another way that the sextic degree is "special". Of the composite degrees generally not solvable in radicals, since it is the smallest, it is also the simplest one.

Last, since the method depends on forming polynomials of the *r*-tuples of roots of equations of composite degree *n*, polynomials with degree determined by $\frac{n!}{r!(n-r)!}$, then it yields resolvents of increasingly high degree the higher you go. This is a similar problem to the general method of solving solvable equations of prime degree *n*, which needs an auxiliary resolvent of *(n-2)!* degree.

Now that we know how to solve the solvable sextic, it should help us solve the solvable septic (rather unfortunate name!) since its Lagrange resolvent is a sextic. But its auxiliary resolvent is of degree (7-2)!=5!=120th.

However, for certain septics, there may be a way around that though…

--End--

Author's Note:

There is this Chinese curse, "May you live in interesting times". And the people whose names we come across in the early part in the history of the theory of equations certainly did.

The years 1494-1559 span the Italian Wars, when the country which we now call Italy was divided into numerous city-states and thus invited invasion from emerging national states like France and Spain. So mathematicians like del Ferro (1465-1526), Tartaglia (1499-1557), Cardano (1501-1576), and Ferrari (1522-1565), while having the privilege of living in that crucial moment in human history which is the Renaissance, also had to do their mathematics and their day-to-day living in the milieu of war.

Nicolo Fontana, aka Tartaglia, not only became fatherless and was left with a disability that became his name, but also had to survive the socio-economic conditions engendered by war. He was self-taught in mathematics and book-keeping, and was said to have been too poor to buy paper that he had to use tombstones as slates.

Del Ferro, Tartaglia, and Cardano did work on cubics, with the last two having a bitter dispute over credit reminiscent of the Newton-Leibniz controversy. Since the sextic relies heavily on solving a cubic, I thought it was only proper that I start it with a dramatization of Tartaglia's life, though Cardano's life was similarly dramatic.

by Titus Piezas III
Nov. 13, 2004
tpiezas@uap.edu.ph

References:

1. Jurgen Klueners and Gunter Malle, “A Database For Number Fields”, http://www.mathematik.uni-kassel.de/~klueners/minimum/minimum.html
2. The MacTutor History Of Mathematics Archive, http://www-gap.dcs.st-and.ac.uk/~history/index.html
3. Henrik Kragh Sorensen, The Mathematics Of Niels Henrik Abel: Continuation and New Approaches in Mathematics During the 1820s (PhD Dissertation, March 2002), http://www.henrikkragh.dk/phd/
4. Jean-Pierre Tignol, Galois’ Theory of Algebraic Equations, World Scientific, 2001
5. Eric W. Weisstein, CRC Concise Encyclopedia of Mathematics, Chapman & Hall/CRC, 1999. or http://mathworld.wolfram.com/