CHAPTER VI

The discovery of the polynomial wheel

6.1. Introduction.

The objective in this chapter is to provide an account of polynomial wheel theory, which gives solutions by radicals for polynomial equations of arbitrary degree, documented further by aspects of polynomial comparison theory, the concrete results of which violate the Galois solvability model. The point of view we presented in [Ad15], Volume II, is that Galois theory fails in the case of dependent roots and matrix roots, and the group automorphism model does not generally leave other complex roots fixed when two roots are swapped, this multiplicative theory does not describe solvability of polynomials, since a polynomial in multiplicative form is already solved, and when the automorphism model is extended to ring automorphisms, with + and ×, then for complex roots these inner automorphisms are involutions which cannot in general be represented by permutation groups, as is claimed to happen in Galois solvability theory. Ring automorphism theory is also defective because it does not incorporate linear maps, used of necessity in the standard solutions of polynomial equations up to the quartic.

We have shown that under the additional condition that zeros of polynomial equations are obtained by killing central terms in a method of descent, that a theory of degrees of freedom, in other words an independency result not contingent on group theory, shows that solutions of polynomial equations in radicals are absent when the degree of the equation is more than 4.

When killing central terms our methods contain examples of a more sophisticated treatment of Galois theory concerned with ring automorphisms. These are not necessarily multiplicative automorphisms which are written in the form $H = \sigma H \sigma^{-1}$, but can be outer automorphisms not of this type. An account of this theory is given in J. S. Milne's website. The existence of this theory which is more general than the usual might explain the persistence with which the teaching of the Galois solvability model is held in mathematics departments at universities.

Nevertheless, we are able to show the falsity of the Galois model in respect of the absence of solutions by radicals which bypass these assumptions by using comparison methods and do not even assume that a solution of an equation of degree n is limited to considering equations starting from degree n. As will be shown explicitly, these give rise to solutions in radicals of polynomial wheel equations of general degree. It is natural to ask whether there exist abstract reasons for solutions of polynomial equations using these methods. We begin in section 3 a sketch, close to a formal proof, which we call Birkby's theorem, that general solutions in radicals of polynomial equations of degree n greater than 4 always exist and are computable.

In section 4 we discuss the comparison technique for a cubic variety, where there is an interesting geometric realisation available in violation of Galois solvability theory. The process of assembling these solutions has been arduous. Some failed calculations are given in the archive section of the mathematics website [AdWeb]. We investigate the quintic with adjoined roots in comparison with a quartic variety in quadratic variables in section 6, which relates the quintic to an elliptic curve. A proof in section 7 solving the sextic from the quintic, is part of a general algorithm deriving the solution of a polynomial in even degree n, when the equation for (n – 1) is known. We provide solutions of degree > 4 by polynomial wheel methods. Birkby's theorem indicates these may involve equations of high degree. Such solutions reduce to independent quadratic equations, solving the P/NP problem. Section 9 extends solutions to incorporate polynomial degrees expressed in Gaussian integers.

6.2. Galois representation theory, Galois solvability and proofs.

On one level of description Galois *representation* theory connects the theory of groups with the binomial theorem. Not only are the coefficients of the expansion of the binomial theorem in integer powers numbers of combinations, and combinations form abelian groups, but also Fermat's little theorem is a consequence of the binomial theorem, and this theorem connects directly with many features of finite arithmetic, called congruence theory. An alternative terminology for Fermat's little theorem uses the phrase Frobenius automorphism. Essentially, the theory of Galois representations is correct in its programme and outline. We will need Galois representation theory to prove the Weil conjectures and the modularity theorem.

The issue with Galois *solvability* theory, which goes in additive format beyond the binomial theorem to encompass polynomials of arbitrary degree and arbitrary complex coefficients, as we have mentioned in [Ad15] Volume II and in polynomial wheel theory in section 8, is that the model it provides for the solvability, or the zeros, of a polynomial equation is erroneous in the general case. This creates multiple issues in mathematics which are currently unresolved. These issues may be divided into the social communication of mathematics, what it teaches, what it admits as the truth, and how this knowledge is passed from one generation to another, including through the examination system, and then the body of mathematical knowledge and its consequences, because we are saying that proofs in other areas which depend on this theory are false, and need re-examination.

The historical background to Jerrard theory is that in a failed attempt to solve the quintic, Tschirnhaus introduced his transformation in the journal *Acta Eruditorum* [Ts1683]. In 1786 the mathematician E. S. Bring showed that a general quintic equation can be reduced to what is now called Bring-Jerrard form

$$x^5 + px + q = 0.$$

In 1834 George B. Jerrard, who studied at Trinity College Dublin 1821–1827, showed that a Tschirnhaus transformation can be used to eliminate the x^{n-1}, x^{n-2} and x^{n-3} terms for every general polynomial of degree $n > 4$. In 1859 he wrote *An essay on the resolution of equations* [Je1859]. One version contains an epilogue by James Cockle stating that Jerrard's insistence that the quintic was solvable by radicals was incorrect. As mentioned by G. B. Mathews [Ma30], Jerrard was 'the last disputant'.

In the 1920's and early 1930's the high point of mathematical development was situated in Germany. The abstract school of mathematics begun by David Hilbert, and developed further in conjunction with him by Emmy Noether, gave rise to the programme, as an extension of Galois theory, to replace all of mathematics with group theory. This programme was begun in topology by P. Alexandroff in the Soviet Union and H. Hopf in Germany [AH35], and was enthusiastically continued in the Soviet Union under the school of mathematics headed by S. Pontrjagin. An abstract extension of mathematics was later developed further in France, most notably by A. Grothendieck and co-workers in an attempt to prove the Weil conjectures, a subcase of the Riemann hypothesis. The Weil conjectures were fully proved by P. Deligne in a paper of 1974.

The phrase iron curtain as a metaphor for strict separation goes back to the early 19th century, originally referring to fireproof curtains in theatres. In reference to this, G. N. Watson, who edited Ramanujan's notebooks and had a lifelong interest in the quintic equation, described research into solutions of the quintic as surrounded by an iron curtain.

That this situation has arisen is a tragedy for mathematical culture, but it is not an isolated feature of accepted but false mathematics. We need therefore to examine the social structures for the communication of mathematics. It is my contention that the journal system dominated by Reed Elsevier has been in a state of corruption, this is obvious and a scandal, and that the peer review process, the language which the system insists is necessary and other forms of acceptance are also lacking sometimes in what is desirable. Mathematics and other sciences need to reach out in plain language to the general scholar so that its features can be inspected in full and knowledgeable detail, and so that the doors to this knowledge are not guarded by a clique restricting inspection of its contents and creating barriers to communication through the excessive use of jargon and results only explained in an interminable trail of references, or with no explanation at all.

As a separate issue, I wish to raise again here the work of Nathan Jacobson (1910 – 1999, who taught at Yale from 1947 and was president of the AMS 1971 – 1973). It follows from the work of Gentzen that all proofs may be put in the form of a tree, where the top of the tree contains the assumptions of the proof, and the root contains the conclusion. So far as I can gather, all proofs by Jacobson contain internal loops, that is, they cannot be reduced to tree form. It may happen that a proof branches off into other proofs which themselves contain circuits, or nodes which are ambiguous or absent. It is difficult to prove motivation here. I would make the suggestion that all proofs by Jacobson cannot be modified to axiomatic form. Thus it appears that whereas Jacobson's work contains many true theorems (and a few false ones), the proofs are invalid. For instance, by these means he proves that all functions are associative. But a nonassociative function can be defined by multiplication of an octionian by another octonian to form an octonion function, and octonions are nonassociative. This is significant, because there is only one purported theorem on the correctness of the Galois model, and this is provided by Jacobson, which he calls the Jacobson-Bourbaki theorem, although it does not appear in Bourbaki.

6.3. The incorrectness of the Galois hypothesis.

It is the often case that mathematical theorems are misattributed, and sometimes deliberately so. The present section gives birth to a new subject in mathematics, and since my niece Katy Birkby gave birth to her son Jack whilst the solution of the quintic was being substantially developed, and this general theorem arose at that time as a consequence of trying to understand the foundations of such a result and whether it was possible, the author asks the indulgence of the mathematical community that it be called Birkby's theorem.

In the case of killing central terms, the Galois hypothesis that there are no general solutions by radicals for polynomial equations degree $n > 4$ was confirmed in [Ad15] by dependency theory. It can be expressed in the language of categories. Where central terms are not killed, a question arises as to whether counterexamples to the Galois hypothesis are feasible. In order to give an indication of an answer, we need to ask what is meant by a solution and what is meant by an algorithm.

The problem we face may be described as finding a mapping

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 \overset{g}{\to} (x + b_1)(x + b_2)\cdots(x + b_n) \qquad (1)$$

where the left hand side is a polynomial function in additive format and the right hand side is in multiplicative format. The mapping may also be described in terms of the two sides in the form of equations, perhaps not in the same variable x, which equal zero.

This is clearly a problem where the algorithm, or method of solution, not only depends on polynomial ring theory, but is a problem about maps in ring theory. Relatively these maps, as pointed out by J. S. Milne, may not be inner ring automorphisms satisfying multiplicatively

$$H = \sigma H \sigma^{-1}$$

but possibly exclude this type – outer ring automorphisms (or maybe not be multiplicative).

We first note that by the distributive axioms of a ring

$$(c + d)e = ce + de$$

the mapping g^{-1} is injective and surjective over its elements in the complex field, since this mapping contains no singularities for complex numbers, and we are dealing with a ring here with no division, including by zero, and therefore g^{-1} is a bijection. In the case we are considering, this bijection is an equality for its equations which have value zero. This is often stated as Gauss's theorem, that a polynomial in additive format of degree $n \geq 1$ has at most n zeros and at least one. It is clear that if the field is finite, the b_m are finite, the zeros of x are finite and thus by the distributive axiom and solving simultaneous equations the a_m are finite. This also happens when the a_m and b_m are considered not as collections of values in a field, but as symbols representing sets (the symbol terminology in category theory is a *universal*, and category theory, being about associative collections of mappings, applies to rings).

An algorithm is a set of maps from one set of absolute states to another. It may be defined inductively, by a repetitive process on finite states where the algorithm is specified finitely, or otherwise the algorithm does not range over a finite set of states, but an infinite set.

If there is no algorithm, its existence is inconsistent, and is equivalent to the statement 1 = 0, which is excluded in the axioms for a field. The transformation g^{-1} exists and is consistent (we prove elsewhere, extending the methods of Gentzen, that fields are consistent provided the choice function is restricted to exclude the choice 1 = 0), g^{-1} is bijective and so g is consistent. A question is whether the algorithm or specification for g is finite or infinite.

The right hand side of (1) is invariant under permutations of the b_m. It is not invariant under other transformations of the symbols b_m which exclude permutations. The number of states which this correspond to is n! If the number of states of g acting on x, a_m and b_m were infinite this contradicts the statement that the number of transformations of g is at most the number of mappings of n! states to n! states, which is finite.

Thus algorithms acting on symbols are defined finitely for this problem, as a set of states

$$(n! \to n!) \to \big((n + 1)! \to (n + 1)!\big),$$

and is definable by a finite algorithm in n, where the number of mappings from a set with A members to a set with B members is B^A. This indicates that what we have called the Galois hypothesis is false, so that by a finite search an algorithm can be found, and the issue is not one of the computability of solutions by radicals, but their discovery and efficiency. □

6.4. A geometric realisation of the cubic.

Our theories have deconstructed Galois solvability theory, where we have replaced a theory of group symmetries by a theory of dependencies, and obtained the unsolvability of the quintic by techniques of killing central terms which are independent of group theory. We now explore a case of comparison theory in which there is no killing of central terms, but a polynomial with appended roots is equated to a comparison equation which is a nested

polynomial within another, and this polynomial is solvable. We are able to extend the type of comparison equation essentially to a nested variety, and this will allow us to express a cubic equation with an appended root in terms of an extended comparison equation. As pointed out by Doly García, this has implications for the representation of a cube root of a number in terms of square roots which are geometrically realisable. This is the complete negation of the classical result on the impossibility of such a construction and some other no-go results which are also derived from Galois theory.

We will show that the equation

$$x^3 + Kx + L = 0 \quad (1)$$

is solvable by only using square roots. The method does not involve 'killing central terms' but uses a type of comparison method where the comparison equation is written not in the form of a polynomial, but a variety with two variables. Let

$$(x^3 + Kx + L)(x + m) = 0 \quad (2)$$

so

$$x^4 + mx^3 + Kx^2 + (Km + L)x + Lm = 0. \quad (3)$$

We now consider a comparison equation, where detailed work shows $(x + c)$ is not feasible as the second variable, so we substitute $(x^2 + c)$ instead

$$(x^2 + ax + b)^2 + p(x^2 + ax + b)(x^2 + c) + q(x^2 + c)^2 = 0, \quad (4)$$

which can be expressed as the solvable quadratic equation

$$y^2 + pyz + qz^2 = 0$$

with

$$y = x^2 + ax + b$$
$$z = x^2 + c,$$

with solution that of

$$(x^2 + ax + b) = \left[\frac{-p \pm \sqrt{p^2 - 4q}}{2}\right](x^2 + c), \quad (5)$$

giving

$$\left[1 + \frac{p \mp \sqrt{p^2 - 4q}}{2}\right]x^2 + ax + b + \left[\frac{p \mp \sqrt{p^2 - 4q}}{2}\right]c = 0,$$

which using

$$G = 1 + \frac{p \mp \sqrt{p^2 - 4q}}{2} \quad (6)$$

$$H = b + \frac{p \mp \sqrt{p^2 - 4q}}{2}c \quad (7)$$

has solution

$$x = \frac{-a \pm \sqrt{a^2 - 4GH}}{2G}. \quad (8)$$

Expanding out (4) gives

$$(1 + p + q)x^4 + (2a + pa)x^3 + (2b + a^2 + p(c + b) + 2qc)x^2 + (2ab + pac)x + b^2 + pbc + qc^2 = 0, \quad (9)$$

comparing with equation (3)

$$m = a(2 + p)/(1 + p + q) \quad (10)$$
$$K(1 + p + q) = 2b + a^2 + p(c + b) + 2qc \quad (11)$$
$$Km + L = (2ab + pac)/(1 + p + q)$$
$$Lm = (b^2 + pbc + qc^2)/(1 + p + q),$$

and on eliminating m from (10)

$$Ka(2 + p) + L(1 + p + q) = 2ab + pac \quad (12)$$
$$La(2 + p) = b^2 + pbc + qc^2. \quad (13)$$

We will put for convenience c = 1, giving

$$K(1 + p + q) = 2b + a^2 + p(1 + b) + 2q \quad (14)$$

$$Ka(2 + p) + L(1 + p + q) = 2ab + pa \quad (15)$$

$$La(2 + p) = b^2 + pb + q, \quad (16)$$

and eliminate q from, say, (14) to give

$$q = [–K(1 + p) + 2b + a^2 + p(1 + b)]/(K – 2) \quad (17)$$

$$Ka(2 + p) + L(1 + p) + L[–K(1 + p) + 2b + a^2 + p(1 + b)]/(K – 2) = a(2b + p) \quad (18)$$

$$La(2 + p) = b^2 + pb + [–K(1 + p) + 2b + a^2 + p(1 + b)]/(K – 2). \quad (19)$$

We will use (18) and (19) to give two expressions for p.

$$\{Ka – a + L + L[–K + 1 + b]/(K – 2)\}p = \{–2Ka – L – L[–K + 2b + a^2]/(K – 2) + 2ab\} \quad (20)$$

$$\{La – b – [–K + (1 + b)]/(K – 2)\}p = \{–2La + b^2 + [–K + 2b + a^2]/(K – 2)\}, \quad (21)$$

and then set, for the number D

$$\{Ka – a + L + L[–K + 1 + b]/(K – 2)\} = D\{La – b – [–K + 1 + b]/(K – 2)\},$$

giving a linear relationship between a and b, for, say, D = 1

$$[K – 1 – L]a = [(–L – K + 1)b + (L + K – 1)]/(K – 2) \quad (22)$$

giving for a^2

$$[K – 1 – L]^2a^2 = (–L – K + 1)^2[b – 1]^2/(K – 2)^2 \quad (23)$$

whereas equations (20) and (21) combine to give

$$–2Ka – L – L[–K + 2b + a^2]/(K – 2) + 2ab = –2La + b^2 + [–K + 2b + a^2]/(K – 2),$$

$$2[–K + L + b]a – L – [L – 1][–K + 2b + a^2]/(K – 2) = b^2, \quad (24)$$

which means for instance that the term in b^2 is nontrivially

$$\{–(L – 1)(–L – K + 1)^2/[(K – L – 1)^2(K – 2)^3] + 2(–L – K + 1)/[(K – L – 1)(K – 2)] – 1\}b^2,$$

so that substituting for a in (22) and a^2 in (23) into (24) gives a solvable quadratic for b, where the full equation is

$$\left[2(-L-K+1) - \frac{(L-1)(-L-K+1)^2}{(K-2)^2(K-L-1)} - (K-2)(K-L-1)\right]b^2 + 2[(-K+L)(-L-K+1) + (L+K-1) - (L-1)(K-L-1)]b - 2\left[\frac{(L-1)(-L-K+1)^2}{(K-2)^2(K-L-1)}\right]b + [2(-K+L)(L+K-1) - L(K-2)(K-L-1) - (L-1)(-K)(K-L-1)] + \frac{(L-1)(-L-K+1)^2}{(K-2)^2(K-L-1)} = 0. \quad (25)$$

which allows further simplification. It then determines a in (22), thus p in (20), q in (16), m from (10) and we have set c = 1. We conclude that we can solve for x in (8). □

Doly García remarks that the final equation is not expressed explicitly. Our intention here is to give the method by which a human can understand the process by which a solution is found. This expression can be found in a small number of steps, all of which are given in the text of this work or *Superexponential algebra* [Ad15]. The equation we have given is not intended to be used directly on pen and paper in human computation. The formulas can all be checked by programs such as Mathematica, and their logical correctness deduced by many examples in the same way. This method, and others we have developed, can be implemented in computer software. My point of view is that the reader will be confronted with a sea of symbols throughout this chapter, and an objective should be to minimise this.

An Argand diagram for complex numbers containing a real and imaginary axis represents these numbers geometrically. So a Pythagoras theorem representation of a right-angled triangle can be used to represent a square root. This arises because it is possible geometrically to bisect a line, and if $\sqrt{q}$ is a number we wish to represent geometrically, then

$$(q - 1)^2 + 4q = (q + 1)^2$$
$$(q - 1)^2 + (2\sqrt{q})^2 = (q + 1)^2,$$

so that if q can be constructed in terms of the number 1, so can $\sqrt{q}$.

If we choose K = 0 and L = –2 in (2) so

$$x^3 = 2, \tag{26}$$

then we find from (25) for example that

$$b = \frac{51 \pm \sqrt{2306}}{59},$$

with similar evaluations for other variables, and we find that the cube root of 2 given by (1) is geometrically realisable, because we have provided the solution of essentially the cubic (1) entirely in terms of square roots. □

The quartic was solved in [Ad15] volume II, chapter VIII, section 5, needing an intermediate cubic to solve it. Since the cubic is geometrically realisable, this means the quartic is too. □

6.5. Discriminants, the Sylvester determinant and Bring-Jerrard form.

A polynomial equation in complex variables and coefficients if written as

$$x^n + Tx^{n-1} + Ux^{n-2} + \ldots + W = 0, \tag{1}$$

reduces to the equations

$$A + B + \ldots + D = T \tag{2}$$
$$AB + AC + ... + BA + BC + \ldots = U$$
$$ABC\ldots D = W,$$

which are invariant under permutations of A and B, A and C, B and C etc., that is, of n objects. Galois theory states there is no equation to convert A, B, C etc. for these symmetric polynomials (2) in terms of combinations of T, U, … W for n > 4.

For the general polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \tag{3}$$

the discriminant, denoted by Δ, is given in terms of the roots by

$$\Delta = a_n^{2n-2} \prod_{j<k} (u_j - u_k)^2$$
$$= (-1)^{\frac{n(n-1)}{2}} a_n^{2n-2} \prod_{j \neq k} (u_j - u_k), \tag{4}$$

where a_n is the leading coefficient and u_1, ... u_n are the roots of the polynomial. Δ is the square of the Vandermonde polynomial multiplied by a_n^{2n-2}.

Since the discriminant is a symmetric function of its roots, it can also be expressed in terms of the coefficients of the polynomial. These coefficients are called the elementary symmetric polynomials in the roots.

Expressing the discriminant in terms of the roots makes its key property clear, namely that it vanishes if and only if there is a repeated root, but this only enables it to be calculated by factoring the polynomial. Hence a formula in terms of the coefficients allows the nature of the roots to be determined without factoring.

For a, b and c in the quadratic equation

$$ax^2 + bx + c = 0 \quad (5)$$

the discriminant satisfies

$$\Delta = b^2 - 4ac, \quad (6)$$

where if $\Delta > 0$ the quadratic has two real roots, if $\Delta = 0$ it has real duplicate roots, whereas for $\Delta < 0$ both roots of the polynomial equation are complex conjugates.

The discriminant of the cubic polynomial equation

$$ax^3 + bx^2 + cx + d = 0 \quad (7)$$

is

$$\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd, \quad (8)$$

so that for the monic (a = 1) cubic polynomial without quadratic term, $x^3 + cx + d = 0$, this is

$$\Delta = -4c^3 - 27d^2,$$

and for the quartic

$$ax^4 + bx^3 + cx^2 + dx + e = 0, \quad (9)$$

its discriminant is

$$\begin{aligned}\Delta = {} & 256a^3e^3 - 192a^2bde^2 - 128a^2c^2e^2 + 144a^2cd^2e - 27a^2d^4 + 144\,ab^2ce^2 \\ & - 6ab^2d^2e - 80abc^2de + 18abcd^3 + 16ac^4e - 4ac^3d^2 - 27b^4e^2 + 18b^3cde \\ & - 4b^3d^3 - 4b^2c^3e + b^2c^2d^2. \end{aligned} \quad (10)$$

In a homogeneous polynomial all nonzero terms have the same degree. The discriminants above are homogenous polynomials in the coefficients, respectively of degree 2, 4 and 6, and are also homogeneous in term of the roots, of respective degrees 2, 6 and 12.

For a polynomial of degree n in real coefficients, we have

- $\Delta > 0$: for some integer k such that $0 \le k \le \frac{n}{4}$, there are 2k pairs of complex conjugate roots and n – 4k real roots, all different.
- $\Delta < 0$: for some integer k such that $0 \le k \le \frac{n-2}{4}$, , there are 2k + 1 pairs of complex conjugate roots and n – 4k – 2 real roots, all different.
- $\Delta = 0$: at least 2 roots coincide, which may be either real or not real. □

For the polynomial (1), if we consider from the coefficients the two row vectors

$$\begin{bmatrix} a_n & a_{n-1} & \dots & a_0 & 0 \\ 0 & a_n & \dots & a_1 & a_0 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}, \quad (11)$$

then these are linearly independent, since no nonzero combination of one row with the other will give zero; the first element is $a_n \neq 0$ for the first row and 0 for the second, so if a linear combination $bv_1 + cv_2 = 0$, then b = c = 0, which defines linear independence.

Now consider the formal derivative of (3), which we introduced in chapter VIII section 11 of [Ad15], and will write here as

$$f'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + a_1, \quad (12)$$

where we saw that if f(x) = 0 contains duplicate roots $(x + u)^2$, then f′(x) = 0 contains a copy of one of them. We have seen that if (3) contains the duplicate roots $(x + a)^2$ then (12) contains the root (x + a).

Since (12) has (n – 1) terms at maximum with no a_0 value, but where (11) contains a_0, for the same reason the vectors

$$\begin{bmatrix} a_n & a_{n-1} & \dots & a_0 & 0 \\ 0 & \dots & na_{n-1} & \dots & a_1 \end{bmatrix} = \begin{bmatrix} v_1 \\ u_1 \end{bmatrix}, \quad (13)$$

are linearly independent when f′(x) has no roots in common with f(x).

Thus the (2n – 1) × (2n – 1) *Sylvester matrix*, shown below for n = 4

$$\begin{bmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_4 & a_3 & a_2 & a_1 & 0 \\ 0 & 0 & 0 & a_4 & a_3 & a_2 & a_1 \\ 4a_4 & 3a_3 & 2a_2 & a_1 & 0 & 0 & 0 \\ 0 & 4a_4 & 3a_3 & 2a_2 & a_1 & 0 & 0 \\ 0 & 0 & 4a_4 & 3a_3 & 2a_2 & a_1 & 0 \\ 0 & 0 & 0 & 4a_4 & 3a_3 & 2a_2 & a_1 \end{bmatrix}$$

contains linearly independent rows if and only if there are no duplicate roots in f(x).

A determinant is zero if and only if it contains linearly dependent rows. Thus the Sylvester matrix has zero determinant if and only if the polynomial f(x) has duplicate roots. This determinant is known as the *resultant*, denoted by R(f, f′). Since the resultant vanishes if and only if the discriminant is zero, that is, when a term $(u_1 - u_1)$ exists in the discriminant, and the degree of the resultant is one more than the degree of the discriminant, the two differ only by a factor, and the two are equal up to a factor of degree one.

$$\Delta(f) = (-1)^{\frac{1}{2}n(n-1)} \frac{1}{a_n} R(f, f'). \square$$

To reduce the general quintic

$$y^5 + Ay^4 + By^3 + Cy^2 + Dy + E = 0 \qquad (14)$$

to Bring-Jerrard form, we will transform (14) to principal quintic form, which zeroises the coefficients of the y^4 and y^3 terms, using a quadratic Tschirnhaus transformation

$$-z + y^2 + my + n = 0 \qquad (15)$$

and eliminate y between (14) and (15) using resultants, so that (14) and (15) have duplicate roots and we can calculate from their zero Sylvester determinant a z with

$$z^5 + c_1z^4 + c_2z^3 + c_3z^2 + c_4z + c_5 = 0. \qquad (16)$$

This can be done in *Mathematica* or *Mapl*e. In Wolframalpha.com, the command is

```
Collect[Resultant[y^5+ay^4+by^3+cy^2+dy+e, z-(y^2+my+n), y],z]
```

and gives

$$c_1 = -A^2 + 2B + Am - 5n$$

$$c_2 = B^2 - 2AC + 2D - ABm + 3Cm + Bm^2 + 4A^2n - 8Bn - 4Amn + 10n^2, \text{ etc.}$$

For two unknowns m and n this allows us to eliminate two of the c_i. Thus (14) becomes the principal quintic form

$$z^5 + Uz^2 + Vz + W = 0. \qquad (17)$$

To transform this equation to Bring-Jerrard form the impulse is to use a cubic Tschirnhaus transformation. But this involves a computation of first, second and third degree equations which result in a sextic. Bring and Jerrard found a rather clever way around this using a quartic Tschirnhaus transformation, where the extra parameter prevents raising the degree.

This transformation is

$$v = z^4 + Pz^3 + Qz^2 + Rz + T, \qquad (18)$$

so that on eliminating z between (10) and (11) we get

$$v^5 + d_1v^4 + d_2v^3 + d_3v^2 + d_4v + d_5 = 0, \qquad (19)$$

where

$$d_1 = -5T + 3PU + 4V$$

$$d_2 = 10T^2 - 12PTU + 3P^2U^2 - 3QU^2 + 2Q^2V - 16TV + 5PU + 6V^2 + 5PQW - 4UW + R(3QU + 4PV + 5W), \text{ etc.}$$

In a similar way to the first step, solving $d_1 = d_2 = 0$ will only need a quadratic.

We now use the three variables P, Q and T to solve the three equations

$$3QU + 4PV + 5W = 0 \tag{20}$$

$$d_1 = d_2 = 0. \tag{21}$$

Because the third term of (8) has the form

$$d_3 = e_3R^3 + e_2R^2 + e_1R + e_0, \tag{22}$$

where the e_i are polynomials in the other variables, we can use R to solve $d_3 = 0$ merely as a cubic. This is much easier to calculate when the general quintic is reduced to its principal form first. □

6.6. The comparison method for the quintic and its elliptic curve.

This section is the result of collaboration between Jim Hamilton and me. The insight we are trying to apply in this section is that, as we discovered first in section 7, a sextic with bogus roots is bijective to a solvable quintic equation in a quadratic variable, and correspondingly a quintic equation with bogus roots might be mapped bijectively to a quartic, which we know is solvable, provided we choose this quartic as a variety in a specific form of variables which are quadratics. The conclusion we reach is that the solution of the quintic can be made to depend on the solution of an elliptic curve, a result first obtained by Felix Klein [Kl56]. But if the Galois hypothesis holds that there are no solutions by radicals of a general polynomial equation of degree $n > 4$, then the demonstration of a solution by radicals of a general quintic polynomial equation is inconsistent, which is equivalent to $1 = 0$.

Theorem 6.6.1. *For symbols* (*also called universals*) K *and* L *in a field of variables of zero characteristic, the quintic polynomial equation with variable* x *in Bring-Jerrard form*

$$x^5 + Kx + L = 0 \tag{1}$$

has a solution dependent on the elliptic equation (24) *to follow.*

The solution is fairly long and appears to reach a hitch which is not straightforward to solve.

Proof. We will start by appending the spurious roots $(x^3 + fx^2 + gx + h)$ to obtain

$$(x^5 + Kx + L)(x^3 + fx^2 + gx + h) = 0, \tag{2}$$

$$x^8 + fx^5 + gx^6 + hx^5 + Kx^4 + (L + Kf)x^3 + (Kg + Lf)x^2 + (Kh + Lg)x + Lh = 0. \tag{3}$$

Then if we try to force the situation and compare this with a variety we know is solvable

$$(x^2 + ax + b)^4 + p(x^2 + ax + b)^3(x^2 + c) + q(x^2 + ax + b)^2(x^2 + c)^2 + r(x^2 + ax + b)(x^2 + c)^3 + t(x^2 + c)^4 = 0, \tag{4}$$

we will see that equations (3) and (4) are mutually compatible.

Equation (4) is

$$\begin{aligned} &x^8 + 4(ax + b)x^6 + 6(ax + b)^2x^4 + 4(ax + b)^3x^2 + (ax + b)^4 \\ &+ p(x^6 + 3(ax + b)x^4 + 3(ax + b)^2x^2 + (ax + b)^3)(x^2 + c) \\ &+ q(x^4 + 2(ax + b)x^2 + (ax + b)^2)(x^4 + 2cx^2 + c^2) \\ &+ r(x^2 + ax + b)(x^6 + 3cx^4 + 3c^2x^2 + c^3) \\ &+ t(x^8 + 4cx^6 + 6c^2x^4 + 4c^3x^2 + c^4) = 0. \end{aligned}$$

Thus

$$(1 + p + q + r + t)x^8 + (4a + 3pa + 2qa + ra)x^7$$
$$+ (4b + 6a^2 + p(c + 3b + 3a^2) + q(2c + 2b + a^2) + r(3c + b) + 4tc)x^6$$
$$+ (12ab + 4a^3 + p(3ac + 6ab + a^3) + q(4ac + 2ab) + 3rac)x^5$$
$$+ (a^4 + 6b^2 + 12a^2b + p(3bc + 3a^2c + 3b^2 + 3a^2b) + q(c^2 + 4bc + 2a^2c + b^2)$$
$$+ r(3c^2 + 3bc) + 6tc^2)x^4$$
$$+ (12ab^2 + 4a^2b + p(6abc + a^3c + 3ab^2) + q(2ac^2 + 4abc) + 3rac^2)x^3$$
$$+ (4b^3 + 6a^2b^2 + p(b^3 + 3b^2c + 3a^2bc) + q(2bc^2 + a^2c^2 + 2b^2c)$$
$$+ r(c^3 + 3bc^2) + 4tc^3)x^2$$
$$+ (4ab^3 + 3pab^2c + 2qabc^2 + rac^3)x + b^4 + pb^3c + qb^2c^2 + rbc^3 + tc^4 = 0. \quad (5)$$

To compare this with equation (3), put (3) in the form

$$(1 + p + q + r + t)x^8 + f(1 + p + q + r + t)x^7 + g(1 + p + q + r + t)x^6$$
$$+ h(1 + p + q + r + t)x^5 + K(1 + p + q + r + t)x^4 + (L + Kf)(1 + p + q + r + t)x^3$$
$$+ (Kg + Lf)(1 + p + q + r + t)x^2 + (Kh + Lg)(1 + p + q + r + t)x$$
$$+ Lh(1 + p + q + r + t) = 0. \quad (6)$$

Comparing terms

$$f(1 + p + q + r + t) = 4a + 3pa + 2qa + ra \quad (7)$$
$$g(1 + p + q + r + t) = 4b + 6a^2 + p(c + 3b + 3a^2) + q(2c + 2b + a^2)$$
$$+ r(3c + b) + 4tc \quad (8)$$
$$h(1 + p + q + r + t) = 12ab + 4a^3 + p(3ac + 6ab + a^3) + q(4ac + 2ab) + 3rac \quad (9)$$
$$K(1 + p + q + r + t) = a^4 + 6b^2 + 12a^2b + p(3bc + 3a^2c + 3b^2 + 3a^2b)$$
$$+ q(c^2 + 4bc + 2a^2c + b^2) + r(3c^2 + 3bc) + 6tc^2 \quad (10)$$
$$(L + Kf)(1 + p + q + r + t) = 12ab^2 + 4a^3b + p(6abc + a^3c + 3ab^2) + q(2ac^2 + 4abc)$$
$$+ 3rac^2 \quad (11)$$
$$(Kg + Lf)(1 + p + q + r + t) = 4b^3 + 6a^2b^2 + p(b^3 + 3b^2c + 3a^2bc)$$
$$+ q(2bc^2 + a^2c^2 + 2b^2c) + r(c^3 + 3bc^2) + 4tc^3 \quad (12)$$
$$(Kh + Lg)(1 + p + q + r + t) = 4ab^3 + 3pab^2c + 2qabc^2 + rac^3 \quad (13)$$
$$Lh(1 + p + q + r + t) = b^4 + pb^3c + qb^2c^2 + rbc^3 + tc^4. \quad (14)$$

Let is prepare to solve these 8 simultaneous equations. We wish to determine the 10 variables f, g, h, p, q, r, t, a, b and c in terms of K and L. We have two constraints which we can satisfy. At first it looks desirable to set the coefficient c = 1, but an alternative presents itself: b = c.

We will use the symmetries in the list (7) to (14). Setting b = c, equation (14) is now in a particularly simple form

$$h = b^4/L \quad (15)$$

so we will choose this. Comparing (8) and (13)

$$Kh + Lg = fb^3. \quad (16)$$

Comparing (9) and (12) we obtain

$$Kg + Lf = gb^2, \quad (17)$$

and on comparing (10) and (11)

$$L + Kf = hb. \quad (18)$$

Using (15), (16) and (17) these equations may be represented by

$$\begin{bmatrix} -b^3 & L & K \\ L & K - b^2 & 0 \\ 0 & 0 & L \end{bmatrix} \begin{bmatrix} f \\ g \\ h \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ b^4 \end{bmatrix} \quad (19)$$

plus (18).

The solutions for f, g and h are

$$\begin{bmatrix} f \\ g \\ h \end{bmatrix} = \frac{b^4}{(L^2 - b^5 + Kb^3)} \begin{bmatrix} -\frac{(Kb^2 - K^2)}{L} \\ -K \\ \frac{(L^2 - b^5 + Kb^3)}{L} \end{bmatrix}, \tag{20}$$

so all terms on the second factor in (2) have been found.

Combining equations (18) and (20) together gives

$$L\frac{(L^2 - b^5 + Kb^3)}{b^4} + K\left[-\frac{(Kb^2 - K^2)}{L}\right] - \frac{(L^2 - b^5 + Kb^3)}{L} b = 0$$

$$b^{10} - Kb^8 - K^2b^6 - 2L^2b^5 + K^3b^4 + KL^2b^3 + L^4 = 0, \tag{21}$$

which appears at first sight to be unsolvable.

We wish to introduce here no constraints, but relate K and L to b. For general variables v and w if we put

$$K = vb^2 \tag{22}$$

$$L^2 = wb^5, \tag{23}$$

then equation (21) becomes

$$b^{10}(1 - v - v^2 - 2w + v^3 + vw + w^2) = 0$$

and since $b \neq 0$ this is the elliptic equation

$$v^3 - v^2 - v + 1 + w^2 + vw - 2w = 0. \tag{24}$$

Thus we see that in this instance the comparison method reduces to finding a solution of an elliptic curve. □

We will investigate the current method a little further. If we introduced a second constraint relating a in terms of b, then the solution of the four simultaneous equations (7) to (14) linear in p, q, r and t leads to (7) as a polynomial equation in a, equation (15) in a^2, (16) in a^3 and (17) in a^4.

But the value of b is determined from (22) and (23). If we combine these equations as

$$K^5/L^4 = v^5/w^2 \tag{25}$$

it can be seen that the problem of determining b depends on determining K and L in terms of v and w. Thus we set aside the problem of determining b, as being dependent on finding firstly a solution of (24).

It is clear that if two equations are solvable by comparison methods, then so is their product. However, if we look at the form of equation (24) expressed instead as a general elliptic curve

$$w^2 - p(av^3 + bv^2 + cv + d) = 0, \tag{26}$$

then we see if we put w = 1, this gives a solvable cubic curve, and if v = w the curve

$$w^2 - q(av^3 + bv^2 + cv + d) = 0, \tag{27}$$

is a solvable quartic. Nevertheless, we have found no effective method using this idea either for the quintic, or a product of a cubic and a quartic.

6.7. The solution of the sextic given the solution of the quintic.

Our objective here is to document comparison methods that can be used, assuming the quintic is solvable, to solve the polynomial equation of degree six, the sextic. We find a solution dependent on a decic polynomial equation, which has degree ten, reducing to a quintic, thus solving the sextic when the quintic solution is known. This solution is indicative of the complexity of the problem when applied without thorough theoretical analysis.

Consider the polynomial in form

$$x^6 + Gx^5 + Hx^4 + Kx^3 + Lx^2 + Mx + N = 0. \quad (1)$$

We will append by multiplication to this sextic polynomial the polynomial equation

$$x^4 + m_1x^3 + m_2x^2 + m_3x + m_4 = 0, \quad (2)$$

so that when multiplied together equations (1) and (2) result in

$$\begin{aligned} x^{10} &+ (G + m_1)x^9 + (H + Gm_1 + m_2)x^8 + (K + Hm_1 + Gm_2 + m_3)x^7 \\ &+ (L + Km_1 + Hm_2 + Gm_3 + m_4)x^6 + (M + Lm_1 + Km_2 + Hm_3 + Gm_4)x^5 \\ &+ (N + Mm_1 + Lm_2 + Km_3 + Hm_4)x^4 + (Nm_1 + Mm_2 + Lm_3 + Km_4)x^3 \\ &+ (Nm_2 + Mm_3 + Lm_4)x^2 + (Nm_3 + Mm_4)x + Nm_4 = 0. \end{aligned} \quad (3)$$

Proceeding in a more elementary way than the method for the quintic, we compare this polynomial with the decic (degree 10) polynomial equation

$$\begin{aligned} &(x^2 + px + q)^5 + a(x^2 + px + q)^4 + b(x^2 + px + q)^3 + c(x^2 + px + q)^2 \\ &\quad + d(x^2 + px + q) + e = 0, \end{aligned} \quad (4)$$

with seven free coefficients, which expanded out becomes

$$\begin{aligned} &x^{10} + 5(px + q)x^8 + 10(px + q)^2x^6 + 10(px + q)^3x^4 + 5(px + q)^4x^2 + (px + q)^5 \\ &\quad + a(x^8 + 4(px + q)x^6 + 6(px + q)^2x^4 + 4(px + q)^3x^2 + (px + q)^4) \\ &\quad + b(x^6 + 3(px + q)x^4 + 3(px + q)^2x^2 + (px + q)^3) \\ &\quad + c(x^4 + 2(px + q)x^2 + (px + q)^2) + d(x^2 + px + q) + e = 0, \\ &x^{10} + 5px^9 + (5q + 10p^2 + a)x^8 + (20pq + 10p^3 + 4ap)x^7 \\ &\quad + (10q^2 + 30p^2q + 5p^4 + a(4q + 6p^2) + b)x^6 \\ &\quad + (30pq^2 + 20p^3q + p^5 + a(12pq + 4p^3) + 3bp)x^5 \\ &\quad + (10q^3 + 30p^2q^2 + 5p^4 + a(6q^2 + 12p^2q + p^4) + b(3q + 3p^2) + c)x^4 \\ &\quad + (20pq^3 + 10p^3q^2 + a(12pq^2 + 4p^3q) + b(6pq + p^3) + 2cp)x^3 \\ &\quad + (5q^4 + 10p^2q^3 + a(4q^3 + 6p^2q^2) + b(3q^2 + 3p^2q) + c(2q + p^2) + d)x^2 \\ &\quad + (5pq^4 + 4apq^3 + 3bpq^2 + 2cpq + dp)x \\ &\quad + q^5 + aq^4 + bq^3 + cq^2 + dq + e = 0. \end{aligned} \quad (5)$$

Hence, on comparing coefficients between (3) and (5) we find

$$G + m_1 = 5p \quad (6)$$

$$H + Gm_1 + m_2 = 5q + 10p^2 + a \quad (7)$$

$$K + Hm_1 + Gm_2 + m_3 = 20pq + 10p^3 + 4ap \quad (8)$$

$$L + Km_1 + Hm_2 + Gm_3 + m_4 = 10q^2 + 30p^2q + 5p^4 + a(4q + 6p^2) + b \quad (9)$$

$$M + Lm_1 + Km_2 + Hm_3 + Gm_4 = 30pq^2 + 20p^3q + p^5 + a(12pq + 4p^3) + 3bp \quad (10)$$

$$\begin{aligned} N + Mm_1 + Lm_2 + Km_3 + Hm_4 &= 10q^3 + 30p^2q^2 + 5p^4 \\ &+ a(6q^2 + 12p^2q + p^4) + b(3q + 3p^2) + c \end{aligned} \quad (11)$$

$$\begin{aligned} Nm_1 + Mm_2 + Lm_3 + Km_4 &= 20pq^3 + 10p^3q^2 + a(12pq^2 + 4p^3q) \\ &+ b(6pq + p^3) + 2cp \end{aligned} \quad (12)$$

$$\begin{aligned} Nm_2 + Mm_3 + Lm_4 &= 5q^4 + 10p^2q^3 + a(4q^3 + 6p^2q^2) \\ &+ b(3q^2 + 3p^2q) + c(2q + p^2) + d \end{aligned} \quad (13)$$

$$Nm_3 + Mm_4 = 5pq^4 + 4apq^3 + 3bpq^2 + 2cpq + dp \quad (14)$$

$$Nm_4 = q^5 + aq^4 + bq^3 + cq^2 + dq + e. \quad (15)$$

Of the seven variables p, q, a, b, c, d and e, and the four bogus roots m_1, m_2, m_3 and m_4 making 11 variables in all, we have 10 equations satisfying them, which gives us the freedom to set in the case of the sextic the now suitable p = 1. This is all we need to find a solution of equation (4), and its comparable equation (3) and hence (1). Putting p = 1 in equations (6) to (15) gives

$$G + m_1 = 5 \quad (16)$$

$$H + Gm_1 + m_2 = 5q + 10 + a \quad (17)$$

$$K + Hm_1 + Gm_2 + m_3 = 20q + 10 + 4a \tag{18}$$
$$L + Km_1 + Hm_2 + Gm_3 + m_4 = 10q^2 + 30q + 5 + a(4q + 6) + b \tag{19}$$
$$M + Lm_1 + Km_2 + Hm_3 + Gm_4 = 30q^2 + 20q + 1 + a(12q + 4) + 3b \tag{20}$$
$$N + Mm_1 + Lm_2 + Km_3 + Hm_4 = 10q^3 + 30q^2 + 5 + a(6q^2 + 12q + 1) + b(3q + 3) + c \tag{21}$$
$$Nm_1 + Mm_2 + Lm_3 + Km_4 = 20q^3 + 10q^2 + a(12q^2 + 4q) + b(6q + 1) + 2c \tag{22}$$
$$Nm_2 + Mm_3 + Lm_4 = 5q^4 + 10q^3 + a(4q^3 + 6q^2) + b(3q^2 + 3q) + c(2q + 1) + d \tag{23}$$
$$Nm_3 + Mm_4 = 5q^4 + 4aq^3 + 3bq^2 + 2cq + d \tag{24}$$
$$Nm_4 = q^5 + aq^4 + bq^3 + cq^2 + dq + e. \tag{25}$$

Then from (16) to (19) we are able to determine m_1 to m_4 directly

$$m_1 = 5 - G \tag{26}$$
$$m_2 = 5q + 10 + a - (5 - G)G - H \tag{27}$$
$$m_3 = 20q + 10 + 4a - (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K \tag{28}$$
$$\begin{aligned} m_4 = {} & 10q^2 + 30q + 5 + a(4q + 6) + b \\ & - (20q + 10 + 4a - (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K)G \\ & - (5q + 10 + a - (5 - G)G - H)H - (5 - G)K - L. \end{aligned} \tag{29}$$

Using these values we can express (20) to (25) so that they are eliminated. For instance, for equation (20)

$$\begin{aligned} & M + L[5 - G] + K[5q + 10 + a - (5 - G)G - H] \\ & \quad + H[20q + 10 + 4a - (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K] \\ & \quad + G[10q^2 + 30q + 5 + a(4q + 6) + b \\ & \quad - (20q + 10 + 4a - (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K)G \\ & \quad - (5q + 10 + a - (5 - G)G - H)H - (5 - G)K - L] \\ & \quad = 30q^2 + 20q + 1 + a(12q + 4) + 3b \end{aligned}$$

$$\begin{aligned} (G - 3)b = {} & -M - L[5 - G] - K[5q + 10 - (5 - G)G - H] \\ & - H[20q + 10 - (5q + 10 - (5 - G)G - H)G - (5 - G)H - K] \\ & - G[10q^2 + 30q + 5 \\ & - (20q + 10 - (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K)G \\ & - (5q + 10 - (5 - G)G - H)H - (5 - G)K - L] \\ & + 30q^2 + 20q + 1 \\ & + a(-K - 5H - G(4q + 2) + 12q + 4). \end{aligned} \tag{30}$$

From (21) and (22) we can eliminate c

$$\begin{aligned} & 2N + (2M - N)m_1 + (2L - M)m_2 + (2K - L)m_3 + (2H - K)m_4 = \\ & \quad 50q^2 + 10 + a(20q + 2) + 5b, \end{aligned}$$

$$\begin{aligned} 5b = {} & 2N + (2M - N)(5 - G) + (2L - M)(5q + 10 + a - (5 - G)G - H) \\ & + (2K - L)(20q + 10 + 4a - (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K) \\ & + (2H - K)(10q^2 + 30q + 5 + a(4q + 6) + b \\ & - (20q + 10 + 4a - (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K)G \\ & - (5q + 10 + a - (5 - G)G - H)H - (5 - G)K - L) \\ & + (-50q^2 - 10 - a(20q + 2)), \end{aligned}$$

$$\begin{aligned} (5 - 2H + K)b = {} & 2N + (2M - N)(5 - G) + (2L - M)(5q + 10 - (5 - G)G - H) \\ & + (2K - L)(20q + 10 - (5q + 10 - (5 - G)G - H)G - (5 - G)H - K) \\ & + (2H - K)(10q^2 + 30q + 5 \\ & - (20q + 10 - (5q + 10 - (5 - G)G - H)G - (5 - G)H - K)G \\ & - (5q + 10 - (5 - G)G - H)H - (5 - G)K - L) - 50q^2 - 10 \\ & + a((2L - M) + 3(2K - L) + (2H - K)(4q + 2) - (20q + 2)). \end{aligned} \tag{31}$$

Then using (30)

$$(5 - 2H + K)[-M - L[5 - G] - K[5q + 10 - (5 - G)G - H]$$
$$- H[20q + 10 - (5q + 10 - (5 - G)G - H)G - (5 - G)H - K]$$
$$- G[10q^2 + 30q + 5$$
$$- (20q + 10 - (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K)G$$
$$- (5q + 10 - (5 - G)G - H)H - (5 - G)K - L]$$
$$+ 30q^2 + 20q + 1$$
$$+ a(-K - 5H - G(4q + 2) + 12q + 4)] =$$
$$(G - 3)[2N + (2M - N)(5 - G) + (2L - M)(5q + 10 - (5 - G)G - H)$$
$$+ (2K - L)(20q + 10 - (5q + 10 - (5 - G)G - H)G - (5 - G)H - K)$$
$$+ (2H - K)(10q^2 + 30q + 5$$
$$- (20q + 10 - (5q + 10 - (5 - G)G - H)G - (5 - G)H - K)G$$
$$- (5q + 10 - (5 - G)G - H)H - (5 - G)K - L) - 50q^2 - 10$$
$$+ a((2L - M) + 3(2K - L) + (2H - K)(4q + 2) - (20q + 2))]. \quad (32)$$

From (23) and (24) we can eliminate d

$$Nm_2 + (M - N)m_3 + (L - M)m_4 = 10q^3 + a(6q^2) + b(3q) + c,$$

using (21) for c we get

$$-N - Mm_1 + (N - L)m_2 + (M - N - K)m_3 + (L - M - H)m_4 =$$
$$-30q^2 - 5 - a(12q + 1) - 3b,$$

giving

$$-N - M[5 - G] + (N - L)[5q + 10 + a - (5 - G)G - H]$$
$$+ (M - N - K)[20q + 10 + 4a$$
$$- (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K]$$
$$+ (L - M - H)[10q^2 + 30q + 5 + a(4q + 6) + b$$
$$- (20q + 10 + 4a - (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K)G$$
$$- (5q + 10 + a - (5 - G)G - H)H - (5 - G)K - L]$$
$$= -30q^2 - 5 - a(12q + 1) - 3b \quad (33)$$

and then not sparing the graphic details, on substituting (30) for b in (33)

$$(G - 3)\{ -N - M[5 - G] + (N - L)[5q + 10 + a - (5 - G)G - H]$$
$$+ (M - N - K)[20q + 10 + 4a$$
$$- (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K]$$
$$+ (L - M - H)[10q^2 + 30q + 5 + a(4q + 6)$$
$$- (20q + 10 + 4a - (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K)G$$
$$- (5q + 10 + a - (5 - G)G - H)H - (5 - G)K - L]$$
$$+ 30q^2 + 5 + a(12q + 1)\} =$$
$$(-3 - L + M + H)\{-M - L[5 - G] - K[5q + 10 - (5 - G)G - H]$$
$$- H[20q + 10 - (5q + 10 - (5 - G)G - H)G - (5 - G)H - K]$$
$$- G[10q^2 + 30q + 5$$
$$- (20q + 10 - (5q + 10 + a - (5 - G)G - H)G - (5 - G)H - K)G$$
$$- (5q + 10 - (5 - G)G - H)H - (5 - G)K - L]$$
$$+ 30q^2 + 20q + 1 + a(-K - 5H - G(4q + 2) + 12q + 4)\},$$

which can be collected together in a as

$$(G - 3)\{ -N - M[5 - G] + (N - L)[5q + 10 - (5 - G)G - H]$$
$$+ (M - N - K)[20q + 10 - (5q + 10 - (5 - G)G - H)G - (5 - G)H - K]$$
$$+ (L - M - H)[10q^2 + 30q + 5$$
$$- (20q + 10 - (5q + 10 - (5 - G)G - H)G - (5 - G)H - K)G$$
$$- (5q + 10 - (5 - G)G - H)H - (5 - G)K - L]$$
$$+ 30q^2 + 5 + a[(12q + 1) + (N - L) + (M - N - K)(4 + G)$$
$$+ (L - M - H)(4q + 6 - 4G + G^2 - 1)]\} =$$

$$
\begin{aligned}
&(-3-L+M+H)\{-M-L[5-G]-K[5q+10-(5-G)G-H]\\
&-H[20q+10-(5q+10-(5-G)G-H)G-(5-G)H-K]\\
&-G[10q^2+30q+5\\
&-(20q+10-(5q+10+a-(5-G)G-H)G-(5-G)H-K)G\\
&-(5q+10-(5-G)G-H)H-(5-G)K-L]\\
&+30q^2+20q+1\\
&+a(-K-5H-G(4q+2)+12q+4)\}. \qquad (34)
\end{aligned}
$$

Thus we have two equations under suitable substitutions, from (32)

$$(sq^2+tq+u)=a(vq+w) \qquad (35)$$

and from (34)

$$(s'q^2+t'q+u')=a(v'q+w'), \qquad (36)$$

where by inspection the a terms do not become identically zero. This means

$$(v'q+w')(sq^2+tq+u)=(vq+w)(s'q^2+t'q+u'), \qquad (37)$$

which is nontrivial since (34) contains qN but (32) does not, this is solvable as a cubic in q, and this almost concludes the calculation. Having found q from (37), knowing p = 1, a from (32), b from (31), c from (21), with m_1 to m_4 from (26) to (29) respectively, d from (24) and e from (25) we have obtained all coefficients of this decic given by the quintic equation (4). □

This result is part of a more general one, that when the degree n of a solvable polynomial is odd, so all polynomials of degree < n are solvable, then the polynomial of degree (n + 1) is solvable.

We saw that for n = 3 the comparison method can be used to create a solution by radicals of a polynomial equation of degree 2n from a solvable equation of degree 2n – 1. This is part of a more general theorem holding for an arbitrary natural number n. We then continue by appending to the first equation 2n – 2 spurious roots, so that the resulting degree is 4n – 2. The solution is dependent on a comparison polynomial equation of degree 4n – 2, which reduces to a polynomial in 2n – 1 variables, each variable of which is a quadratic, so that in total for this polynomial the number of independent variables is 2n + 1. The total number of comparison variables minus the number of spurious roots is (2n + 1) – (2n – 2) = 3, which on the face of it looks very manageable. The main difficulty arises in designing a notation in which an induction can be followed for a large number of variables. □

6.8. Polynomial wheel methods solving general polynomials in radicals.

A question arises as to whether there exist practical solutions by these methods beyond the quartic. Birkby's theorem indicates there are solutions. An observation that can be made is that hitherto there has been no theory of algorithms, though such a theory is quite natural, because such a theory would be in conflict with standard incomputability and undecidability results which we maintain are false.

The theorem indicates that to solve the quintic may require calculations with polynomials of quite high degree. J.L. Lagrange in *Réflexions sur la résolution algébrique des équations*, Oeuvres vol. 3, p 305, whose work on the quintic gave rise to some aspects of Galois solvability theory, says: "To apply, for example, the Tschirnhaus method to the fifth degree, we have to resolve four equations comprising four unknowns, of which the first is a first degree equation, the second of the second degree, etc., so that the first equation results in the elimination of three of these unknowns which display, in general, a degree of the form 1.2.3.4, that is, the twenty-fourth degree.

Thus, independently of the enormous work which would be necessary to obtain this equation, it is clear that when we have found it, we are hardly further forward, in that we have at least to reduce it to a degree less than the fifth, a reduction, if it is possible, which would be none other than the fruit of a new endeavour considerably more than the first.

Also we see that the same developers of these techniques have been satisfied with applying them only to the third and fourth degree, and no-one else has displayed sufficient capacity to push forward this work any further".

We have not accepted the analysis of Lagrange that solutions of polynomial equations are obtained by killing central terms (but Lagrange does not say this is the only method, but that it was a review of methods then currently known), and indeed if these methods are applied, then Galois solvability results are obtained.

We could ask, by analogy, what methods if applied to the quintic would give rise to a solution by new methods? The cubic, by conventional methods, gives rise to a polynomial of degree 3! = 6 reducible to a quadratic by known methods. The quartic gives rise to the same type of sextic, reducible to a cubic and thus solvable by killing central terms. We might think that a quintic gives rise to a polynomial of, say, degree 4! = 24, reducible to a quartic. By the techniques already developed, the cubic is reducible by comparison methods to a nested quadratic, a result unobtainable by killing central terms, and the quartic, being solvable via a cubic, is susceptible to the same methods.

Then, if the degree needed to solve a polynomial is high, we can apply modern computation methods and computer software. Now that the conceptual blockage to attempt a solution has been removed, we will be able to resolve the general solvability issue.

For polynomials, we may wish to construct an independent basis. Numbers p^n, where the absolute value of $p \neq 0$ or 1 and $n \in \mathbb{N}_{U0}$ provide such a basis. For example $p = \pm 2$ gives a basis, and we will use $p = 2$, which generates the sequence

$$1, 2, 4, 8, \ldots \qquad (1)$$

in what follows. Additively two independent numbers taken from the sequence (1) cannot generate another member of the sequence. The reader is invited to construct the definition when p is complex.

Let us consider the case of a quadratic variety. Consider two linear polynomials in this basis,

$$(x + 1) \text{ and } (x + 2),$$

and the variety

$$(x + 1)^2 + p(x + 1)(x + 2) + q(x + 2)^2 = 0, \qquad (2)$$

which by the binomial theorem is

$$(1 + p + q)x^2 + (2 + 3p + 4q)x + (1 + 2p + 4q) = 0. \qquad (3)$$

This is in two variables and can easily be linearly transformed to the equation

$$x^2 + Ax + B = 0, \qquad (4)$$

and from this solution we can back-transform to equation (2).

By the solution of the quadratic equation, (2) gives

$$(x + 1) = \left[\frac{-p \pm \sqrt{p^2 - 4q}}{2}\right](x + 2) \qquad (5)$$

or

$$\left[\frac{2 + p \mp \sqrt{p^2 - 4q}}{2}\right] x = \left(-p - 1 \pm \sqrt{p^2 - 4q}\right),$$

and thus multiplicatively

$$\left[x + \frac{2\left(p + 1 - \sqrt{p^2-4q}\right)}{\left(2 + p - \sqrt{p^2-4q}\right)}\right]\left[x + \frac{2\left(p + 1 + \sqrt{p^2-4q}\right)}{\left(2 + p + \sqrt{p^2-4q}\right)}\right] = 0. \quad (6)$$

Now consider the two varieties equivalent to

$$x^2 + Ax + B = 0 \quad (7)$$

and

$$x^2 + Cx + D = 0, \quad (8)$$

where (7) is equivalent to (4) and (8) is now expressed in the basis

(x + 4) and (x + 8).

By analogy with what went previously, consider the variety

$$(x^2 + Ax + B)^2 + t(x^2 + Ax + B)(x^2 + Cx + D) + u(x^2 + Cx + D)^2. \quad (9)$$

Again, since we have sufficient variables at our disposal, this can be linearly expressed as a quartic equation

$$x^4 + Ex^3 + Fx^2 + Gx + H = 0. \quad (10)$$

Indeed, since $x^2 + Ax + B$ is expressed in terms of two parameters, and so is $x^2 + Cx + D$, and these are independent parameters, we can construct a solution to (10) under an explicit choice of t and u, and still have 4 independent variables.

By classical techniques, or those introduced in sections 4 and a lower degree case of section 7, the cubic and quartic equations are solvable.

If we wish to solve the quintic, for instance, then we can use the cubic to solve the quintic equation.

Consider the variety

$$(x^3 + Fx^2 + Gx + H)^2 - (x^3 + Kx^2 + Lx + M)^2 = 0. \quad (11)$$

$$2(F - K)x^5 + (F^2 - K^2 + 2(G - L))x^4 + 2(FG - KL + H - M)x^3 + (G^2 - L^2 + 2(FH - KM))x^2 + 2(GH - LM)x + H^2 - M^2 = 0,$$

$$x^5 + \left(\frac{F + K}{2} - \left(\frac{G - L}{F - K}\right)\right)x^4 + \left(\frac{FG - KL + H - M}{F - K}\right)x^3 + \left(\frac{G^2 - L^2}{2(F - K)} + \frac{FH - KM}{F - K}\right)x^2 + \left(\frac{GH - LM}{F - K}\right)x + \frac{H^2 - M^2}{2(F - K)} = 0. \quad (12)$$

Since we have one free parameter, we can put

$$L = 0. \quad (13)$$

Introduce variables v and w so that

$$v(F - K) = H - M, \quad (14)$$

giving

$$H = v(F - K) + M,$$

and

$$w(F - K) = G. \quad (15)$$

Under these substitutions, equation (13) is

$$x^5 + \left(\frac{F + K}{2} - w\right)x^4 + (Fw + v)x^3 + \left(\frac{Gw}{2} + Fv + M\right)x^2 + (Gv + Mw)x + \frac{v^2(F - K)}{2} + vM = 0. \quad (16)$$

We will now compare this quintic polynomial equation with the quintic

$$x^5 + Qx^4 + Rx^3 + Sx^2 + Tx + U = 0. \quad (17)$$

On equating coefficients between (17) and (16) we obtain

$$\frac{F+K}{2} - w = Q \tag{18}$$

$$Fw + v = R \tag{19}$$

$$\frac{Gw}{2} + Fv + M = S \tag{20}$$

$$Gv + Mw = T \tag{21}$$

$$v^2(F - K) + 2vM = 2U. \tag{22}$$

Various choices are available to us. If equation (17) were in Bring-Jerrard form with

$$Q = R = S = 0 \tag{23}$$

then

$$w = \frac{F+K}{2}, \tag{24}$$

$$v = -\frac{F(F+K)}{2}, \tag{25}$$

giving

$$M = \frac{F+K}{2}\left(F^2 - \frac{G}{2}\right). \tag{26}$$

Using (21), (22), and (26) to eliminate M gives for (21)

$$T = \frac{(F+K)}{2}\left(-GF + \frac{F+K}{2}\left(F^2 - \frac{G}{2}\right)\right) \tag{27}$$

and for (22)

$$2U = -F\left(\frac{F+K}{2}\right)^2 (2F^2 - G - F(F - K)). \tag{28}$$

Various stratagems may be used to invert these two remaining equations. Since in (27) and (28) we now have two variables T and U expressed in terms of three, F, K and G, we could set

$$w = \frac{(F+K)}{2} = 1, \tag{29}$$

so that

$$T = -GF + \left(F^2 - \frac{G}{2}\right) \tag{30}$$

$$2U = +GF - 2F^2 \tag{31}$$

Thus the solution to the Bring-Jerrard quintic is given by

$$F^3 + F^2 + (2U + T)F + U = 0 \tag{32}$$

$$G = -2F^2 - 4U - 2T \tag{33}$$

$$H = 2F + 2U + T \tag{34}$$

$$K = 2 - F \tag{35}$$

$$M = 2F^2 + 2U + T, \tag{36}$$

where

$$(F - K)x^2 + Gx + H - M = 0 \tag{37}$$

or

$$x^3 + \left(\frac{F+K}{2}\right)x^2 + \frac{G}{2}x + \frac{H+M}{2} = 0. \tag{38}$$

Now consider the octic variety generated by the polynomials

$x^4 + Ex^3 + Fx^2 + Gx + H$

and

$x^4 + Kx^3 + Lx^2 + Mx + N.$

Then the same method generates, from simultaneous linear equations, the solution to the general septic equation.

Further, any equation of lower degree than this can be solved by adjoining bogus roots.

This is the general polynomial wheel method solving polynomial equations of arbitrary large degree. □

The P/NP problem includes the decryption problem of resolving the factorisation of two large primes, and in general seeks to relate the complexity of the factorisation problem and its solution time to the simplicity of the algorithm need to solve it.

The polynomial wheel method indicates that polynomial problems are directly equivalent to the solution of simultaneous quadratic equations, which reduce to the simplest type.

We have seen in section 6 that the quintic is related to an elliptic curve, and we have now solved this problem. Thus there is a connection between elliptic curves, and their higher dimensional analogues, and polynomial wheel methods, so we can use polynomial wheels to give answers to problems formed in terms of higher dimensional elliptic curves. □

6.9. Solutions for Gaussian integer degrees.

Any root $(x^{a + bi} + c) = 0$ may be multiplied by $(x^{a - bi} - c)$ to give a root of real degree. Thus by appending such roots to a polynomial in Gaussian integer degree in either additive or multiplicative format, a polynomial in integer degree can be obtained, and the reversible algorithm of section 6.7 can be applied to obtain a bijection in radicals between additive and multiplicative format polynomials in this case. This method can also be extended to Heegner number degrees, and indeed any general polynomial with degree surds in their real and complex parts. □