CHAPTER 9

The discovery of the polynomial wheel

9.1. 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 derived from group theory, shows that solutions of polynomial equations in radicals are absent when the degree of the equation is more than 4. For killing central terms we show by considering independence of solutions that Galois solvability restrictions hold.

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 and do not even assume that a solution of an equation of degree n is limited to considering equations starting from degree n.

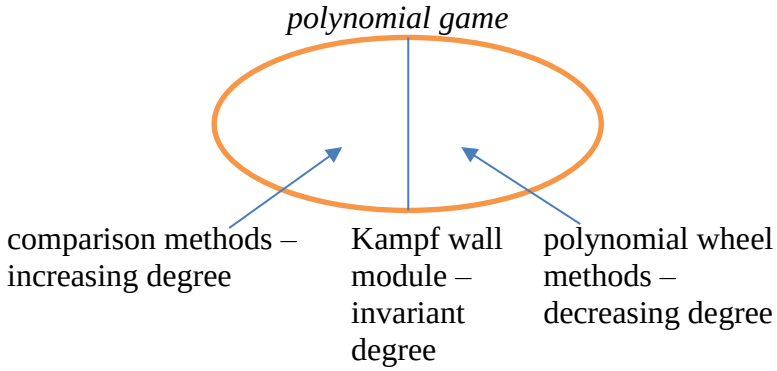
Comparison methods increase the degree of a polynomial equation by appending bogus roots and comparing this with a solvable variety. Polynomial wheel methods decrement the degree of a polynomial equation by equating it to the difference of two powers of polynomials with the same leading coefficients.

In section 5 we discuss the comparison technique for a cubic variety, where there is an interesting geometric realisation available violating 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]. As will be shown explicitly, these methods give rise to more 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. This relates naturally to the theory of algorithms, to which Galois solvability theory provides an obstruction. In section 7, close to a formal proof, we sketch

Birkby's theorem, that solutions in radicals of polynomial equations of degree n greater than 4 always exist and are computable. Birkby's theorem indicates these may involve equations of high degree.

The key to solving the quintic by polynomial wheel methods is given in section 8. In section 9 we expand the discussion to consider polynomial games.



All games are in reason, that is, they are consistent mathematics. The Kampf wall boundary describes Galois solvability theory and dependent solvability. A polynomial wheel game is distinct from module theory. Solutions by this method are either inconsistent – we are in unreason – or they provide a solvable solution for instance to the quintic, and indirectly for higher degree polynomial equations.

Polynomial wheels which decrease the degree are also distinct from comparison methods which increase it, say on the right of (1) below. If the polynomial equation is given by

$$0 = (x^3 + px^2 + qx + r)(x^2 + tx + u)$$
$$= (x^3 + Ax^2 + Bx + C)^2 - (k = 1)(x^3 + Dx^2 + Ex + F)^2 \qquad (1)$$

it is a variety in two variables, each a cubic.

When $k \neq 1$ equation (1) is a sextic and its two factors are both cubics. Under such a stable degree if there are no dependent roots this reduces to Galois solvability theory, so there is no algorithm in radicals.

If one of the factors on the left is say a quintic, then if the other factor is known and the right hand side is a quartic variety in say two quadratic variables, we find the quintic can be solved. In section 12 we show this quintic reduces to an elliptic curve, a result first obtained by Felix Klein.

If a polynomial wheel solution is available, then on lowering the Kampf wall to zero, which has a height representing a perfect obstruction at 1 – so polynomial wheel methods obtrude into comparison methods – then the solution of the right hand polynomial wheel can be shared with – we say it 'overwhelms' – the left hand comparison game. This builds up new forms of solutions. The asymmetry arises because only polynomial wheels can donate new solutions.

9.2. A history of Galois solvability and Galois representation ideas.

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 can introduce, as an extension of the abelian case, noncommutative groups into this type of discussion, including the study of normal subgroups.

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.

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.

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 attempted by P. Deligne in a paper of 1974.

The phrase iron curtain as a metaphor for strict separation goes back to the early 19^{th} 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 octonian 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.

9.3. Deconstructions of Galois solvability theory.

The method we develop now, using duplicate and antiduplicate roots, is the most practical for obtaining iterated roots of polynomial equations. However, the approach using dependent root techniques was first developed using polynomials of degree ≤ 6 with duplicate zeros. It was

conjectured from the book by Netto [Ne1892] that non degree conserving techniques allowed an escape clause from Galois theory.

We will first take the case of the sextic and study the equation with roots $(x + a)(x – a) = 0$:

$$(x^2 – a^2)(x^4 + bx^3 + cx^2 + dx + e) = 0. \quad (1)$$

If this is put in the form

$$x^6 + Px^5 + Qx^4 + Rx^3 + Tx^2 + Ux + V = 0, \quad (2)$$

then there is a computable mapping between (2) and (1).

Indeed, we have

$$P = b \quad (3)$$
$$Q = -a^2 + c$$
$$R = -a^2b + d$$
$$T = -a^2c + e$$
$$U = -a^2d$$
$$V = -a^2e,$$

and the equations given by (3) can be directly inverted:

$$b = P \quad (4)$$
$$a^4P + Ra^2 + U = 0$$

with the constraint

$$T = -a^2(Q + a^2) – V/a^2$$

and so

$$a^2 = \frac{-R \pm \sqrt{R^2 - 4UP}}{2P}$$
$$b = P$$
$$c = Q + \frac{-R \pm \sqrt{R^2 - 4UP}}{2P}$$
$$d = \frac{3R \pm \sqrt{R^2 - 4UP}}{2}$$
$$e = V/[\frac{R \pm \sqrt{R^2 - 4UP}}{2P}].$$

We may now directly solve (1), knowing the classical solution of the quartic. □

According to Galois theory, if we then consider the Tschirnhaus substitution

$$x = y + h, \quad (5)$$

so that in effect the polynomial is a completely general one, the equation

$$y^6 + P'y^5 + Q'y^4 + R'y^3 + T'y^2 + U'y + V' = 0, \quad (6)$$

is then unsolvable directly by the common method, that is, the mapping

$$(h, a, b, c, d, e) \rightarrow (P', Q', R', T', U', V')$$

cannot be inverted by usual Galois techniques of steady descent to equations of lower degree.

In the case of duplicate roots, which follows in the next section, the duplicate roots maintain their status under Tschirnhaus substitutions. □

We will next take the case of the sextic and study the equation with duplicate roots

$$(x + a)^2(x^4 + bx^3 + cx^2 + dx + e) = 0. \quad (7)$$

If this is put in the form

$$x^6 + Px^5 + Qx^4 + Rx^3 + Tx^2 + Ux + V = 0, \quad (8)$$

then again there is a computable mapping between (8) and (7).

This time we have

$$P = 2a + b \quad (9)$$

$$Q = 2ab + a^2 + c$$
$$R = 2ac + a^2b + d$$
$$T = 2ad + a^2c + e$$
$$U = 2ae + a^2d$$
$$V = a^2e.$$

The value of a in terms of P, Q, R, T, U and V can be obtained, and so b, c, d and e can be determined.

We may now directly solve (7), knowing the classical solution of the quartic. □

We can consider the Tschirnhaus substitution

$$x = y + h', \tag{10}$$

when (10) retains duplicate roots in y and the modified equation (8)

$$x^6 + P'x^5 + Q'x^4 + R'x^3 + T'x^2 + U'x + V' = 0, \tag{11}$$

is then solvable by the same method, that is, the mapping

$$(h', a, b, c, d, e) \to (P', Q', R', T', U', V')$$

may be inverted. □

We obtain a differential condition for the detection of duplicate roots.

Theorem 9.3.1. *Select a quadratic factor* $g(x) = 0$ *of a polynomial equation* $F(x) = 0$. *There exists a unique transformation* $x \to x + h$, *such that either*

$g(x)$ *represents* $(x + a)^2 = 0$ *or* $g(x)$ *represents* $x^2 - a^2 = 0$.

Proof. Consider the product $(x + b)(x + c) = 0$. If $b = c$, then this is the first case, and if $b \neq c$, $h = -(b + c)/2$. □

Definition 9.3.2. Let x be real or complex, then $\Delta x^m = mx^{m-1}$ if $m \geq 1$, otherwise $\Delta x^m = 0$.

Remark 9.3.3. We are not employing Cauchy-Riemann complex differentiation.

Theorem 9.3.4. *If*

$$F(x) = \sum_{m=0}^{n} a_m x^m = 0 \tag{12}$$

has duplicate roots, then at this root

$$\Delta F(x) = 0. \tag{13}$$

Proof.

$$\Delta[f(x)g(x)] = f(x)\Delta g(x) + g(x)\Delta f(x).$$

Thus if $f(x)$ corresponds to an arbitrary polynomial and $g(x)$ to the duplicate zero $(x + a)^2$, then

$$\Delta g(x) = 2(x + a),$$

so that

$$\Delta[f(x)g(x)] = (x + a)\times(\text{a polynomial}). \square$$

Equation (13) is of the form

$$\Delta F(x) = \sum_{m=1}^{n} ma_m x^{m-1} = 0, \tag{14}$$

so that multiplying the above equation by x and subtracting $mF(x)$ we get a distinct equation in the power x^{m-1}. Combining this equation with (14), we get an equation in x^{m-2}, so that we have obtained a further descent of the degree, and this process may be iterated. At each stage we retain the root $(x + a) = 0$, thus at the penultimate resolution we obtain a linear equation in x, which must be the root, and finally we obtain an equation in x^0 which corresponds to a constraint on the coefficients of (12).

By this technique the zero (x + a) may be obtained, and we may proceed by methods already introduced. □

We discuss polynomial equations of degree ≤ 6 with roots $(x + a)(x + ha) = 0$.

If we know a relationship between two zeros of the sextic, say if one zero is a then the other zero is ha, then from the observation that a polynomial containing these zeros satisfies

$$(x + a)(x + ha) = K(x + da)^2 + (1 - K)(x^2 - d^2a^2), \tag{15}$$

with

$$2Kd = h + 1 \tag{16}$$

and

$$(2K - 1)d^2 = h, \tag{17}$$

there are two solutions to (16) and (17), corresponding to d = 1 and d = h. Choosing d = 1 gives

$$(x + a)(x + ha) = \left(\frac{1 + h}{2}\right)(x + a)^2 + \left(\frac{1 - h}{2}\right)(x^2 - a^2), \tag{18}$$

so that the sextic equation can be split into two parts, one with duplicate roots, and one with antiduplicate roots, both parts of which we have previously solved, represented by

$$\left(\frac{1 + h}{2}\right)(x^6 + Px^5 + Qx^4 + Rx^3 + Tx^2 + Ux + V) + \left(\frac{1 - h}{2}\right)(x^6 + P'x^5 + Q'x^4 + R'x^3 + T'x^2 + U'x + V') = 0. \tag{19}$$

If Galois theory were to hold then the splitting of solutions for unknown h cannot be obtained algorithmically by radicals, since this corresponds to independent roots, but if h is known then the methods already found for polynomial equations work for factorisation not just equated to zero, and (19) can be obtained. □

A question concerning the solvability of polynomial equations is: how do we treat dependent roots of polynomial equations? It is a reduction procedure, followed by solvability algorithms if available.

As accountancy we can consider root symbols all different, but possibly with related values.

When identical elements occur, the usual terminology is to say the polynomial is *inseparable*, and if this does not occur, to call the polynomial *separable*. For my part, when there is a function h_{ab} which is known or can be found so that

$$u_b = h_{ab}(u_a)$$

then we say the roots $(x - u_a)$ and $(x - u_b)$ are *dependent*, and if there is no such known function, that the roots are *independent*. Thus an inseparable polynomial is a special case of a polynomial with dependent roots.

General dependencies may be subdivided into the absolute case, where we know a specific set of roots, in which case the remaining equation is obtained by dividing out these roots, so this is fairly trivial, and the relative case, where with respect to a set of roots we specify dependencies between them.

Let a general polynomial be of the form

$$x^n + Px^{n-1} + ... + V = 0. \tag{20}$$

To consider the relative case, we select a root if there is one for which a dependency is to be specified. If this root is a, then if there is a binary dependency so that a further root is ha, then we will find that there is an extension of the argument, so that

$$(x + a)(x + ha) = \left(\frac{1 + h}{2}\right)(x + a)^2 + \left(\frac{1 - h}{2}\right)(x^2 - a^2), \tag{21}$$

where the polynomial equation can be split into two parts, one with duplicate roots, and one with antiduplicate roots, both parts of which we must ensure we can solve in the general case, representing (18) by (19) multiplied by a common polynomial as

$$\left(\frac{1+h}{2}\right)(x^n + P'x^{n-1} + ... + V') + \left(\frac{1-h}{2}\right)(x^n + P''x^{n-1} + ... + V'') = 0, \quad (22)$$

where

$$\left(\frac{1+h}{2}\right)(P') + \left(\frac{1-h}{2}\right)(P'') = P \quad (23)$$

is uniquely expressed with h known and likewise for the other coefficients.

We have already indicated the method of solution for the $(x + a)^2$ roots which occupy the $\left(\frac{1+h}{2}\right)$ term in (22), explained as a method by descent.

Now consider the $\left(\frac{1-h}{2}\right)$ term in (22), which contains $(x + a)(x – a)$. We will look at the monic function

$$x^n + p_1x^{n-1} + p_2x^{n-3} + ... + p_{n-1}x + p_n, \quad (24)$$

which contains this $(x^2 – a^2)$ term. Writing this as

$$(x^2 – a^2)(x^{n-2} + b_3x^{n-3} + b_4x^{n-4} + ... + b_{n-2}x^2 + b_{n-1}x + b_n), \quad (25)$$

expanding out and comparing with (24) gives

$$\begin{aligned}
p_1 &= b_3 \\
p_2 &= b_4 – a^2 \\
p_3 &= b_5 – a^2b_3 \\
&... \\
p_{n-r} &= b_{n-r-2} – a^2b_{n-r} \\
&... \\
p_{n-2} &= b_n – a^2b_{n-2} \\
p_{n-1} &= -a^2b_{n-1} \\
p_n &= -a^2b_n. \quad (26)
\end{aligned}$$

These terms may be split into two sets of equations in p_k, with k even or odd. For instance we have $p_1 = b_3$ and $p_3 = b_5 – a^2b_3$ give $p_3 = b_5 – a^2p_1$, and then $p_5 = b_7 – a^2b_5$ determines the value of b_7 in $p_5 = b_7 – a^2(p_3 – a^2p_1)$, etc.

By these means we obtain two equations in powers of a^2, one in values p_k with k odd, and another in p_k with k even. By a method perfectly analogous to that of descent for $(x + a)^2$, we may solve these two equations in a^2 when $(x + a)(x – a)$ are the roots.

Having done this, we can extract out the roots a and ha, so that the degree of the resulting equation is decremented by two. If this is the only dependency, we can amalgamate the left and right terms before zero in (22) as the same equation, which is now subject to standard solvability criterions.

If there are further dependencies related to the root a, and they are all of a binary form, we can reintroduce the root a and now its dependency with another root, say h′a. Since we have reintroduced a, the result on repeating this method is now only to reduce the degree by one, and we can continue in this fashion until we are finished.

If further dependencies are not related in any way to the root a, we can introduce roots b and h″b, and proceed as before, the first time decrementing the degree by two, and subsequently by one.

These dependencies we have assumed so far are linear, and can be manipulated and solved by linear algebra, but the involution (19) is not inherently linear. In general dependencies will be polynomial dependencies between roots, so that the problem has to be solved recursively, if that is possible. □

9.4. Ring automorphisms.

After defining ring automorphisms, we develop their concrete representation and then show some of their properties. We show that ring automorphisms are linear reflections, they are not linear transformations except in a trivial case, they are involutions of roots, that is, the application of a ring automorphism twice is the identity transformation, and that the ring automorphism of a root is another root, but when the same automorphism is applied to a different root not equal to these two, in the general case it does not leave the different root fixed. We introduce the idea of discriminants, which can be incorporated within the ring automorphism theory. We provide a geometric picture of the application of automorphisms as rigid transformations of the roots.

We show that in general ring automorphisms, which attach to specific roots, are not described by permutations on roots. From this it follows that ring automorphisms do not bijectively describe the Galois group theory on roots, since multiplicative inner group automorphisms between roots and their images are not in general inner ring root automorphisms, which include addition. The idea of a normal extension, describing the insertion of a new root to a polynomial by an inner group automorphism leaving other roots fixed does not relate directly to polynomial solvability.

The allowable operations on complex roots in a field we will consider are addition, which displaces a root $u + iv$ by $a + ib$ to form $(u + a) + i(v + b)$, subtraction, which can be considered as addition of the additive inverse $(-a) + i(-b)$, multiplication for which

$$(u + iv)(c + id) = (uc – vd) + i(ud + vc),$$

division by a nonzero complex number as multiplication by the multiplicative inverse

$$(c – id)/(c^2 + d^2),$$

where of course, division is always defined for zero algebras, and complex conjugation

$$u + iv \rightarrow u – iv.$$

Complex conjugation is an involution: applied twice it is the identity transformation

$$u + iv \rightarrow u + iv.$$

We can also consider multiplication using complex polar coordinates $u + iv = \rho e^{i\theta}$, where we have used the Euler relation $e^{i\theta} = \cos\theta + i \sin\theta$.

A particular type of transformation applies to rigid mappings, where there is no change of the norm, ρ^2.

The theorems that we wish to develop concern the solutions of polynomial equations, and polynomials generate examples of rings.

Definition 9.4.1. *A ring is a field, except multiplication may be noncommutative and it may not have division.*

Fields are described in chapter I, section 12, by rules for addition and multiplication. Division by zero is not defined and is excluded for fields, because $(1 \times 0) = (n \times 0)$, so dividing by zero is not unique.

Consider a finite commutative polynomial in additive format

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

Definition 9.4.2. *If a number,* c, *can be represented by* $f(x) = 0$ *in* (1), *where the coefficients* a_r *are integers and* $x = c$, *it is called algebraic, otherwise it is called transcendental*.

So the roots, $u_1, u_2, \ldots u_s$ of a polynomial equation may be partitioned into two equivalence classes: those which are algebraic, and those which are transcendental. By the results of chapter VII of [Ad15], these may be encoded in the multiplicative form of a polynomial equation

$$(x - u_1)(x - u_2) \ldots (x - u_s) = 0. \quad (2)$$

Equation (1) looks very like a finite vector space with vectors $x^n, x^{n-1}, \ldots x, x^0$, and satisfies the axioms of a vector space. The ideas of linear dependence and independence can be applied to such a polynomial.

When $f(x) = 0$ and the coefficients a_r belong to a field, so they are algebraic or transcendental, the values of x for which this equation holds are called the zeros of the polynomial, or the roots of the polynomial equation. The vectors $a_n x^n, a_{n-1}x^{n-1}, \ldots a_1 x, a_0 x^0$ are then linearly dependent, by definition.

When $a_n = 1$ in equation (1) the polynomial is called *monic*. The commutative polynomials of non-negative degree generate a ring $\mathbb{P}$ by addition, subtraction and multiplication. These polynomials are members of $\mathbb{P}$. Not all divisions by polynomials of non-negative degree give a product of polynomials with zero remainder, the interpretation being that there is no complete division, so the polynomial ring $\mathbb{P}$ does not form a field.

We note that this is the case only under the rules we have provided for it. If we were to consider polynomials as in (1) under the condition that terms of arbitrary finite integer degree – positive, negative or zero – are allowed, then finite division is indeed possible. Such polynomials where $(x + a)^{-n}$ is allowed form a field.

A type of Euclidean algorithm for division with remainder also holds. Consider the division

$$\frac{(x-2)(x-1)}{(x-3)} = \frac{x^2 - 3x + 2}{(x-3)} = x + \frac{2}{(x-3)},$$

so we could say

$$x^2 - 3x + 2 = 2 \pmod{(x-3)}. \quad (3)$$

Multiplication can be formed using a polynomial congruence class, say $(x - 3)$, as in (3), so we keep dividing by, say, $(x - 3)$ until we get a remainder, which could be zero, of degree less than $(x - 3)$.

Example 9.4.3. When we take the complex conjugate of a complex number $(a + ic)$, then we are applying a map $a + ic \rightarrow S(a + ic) = a - ic$. This preserves addition

$$S(a + ic + b + id) = a - ic + b - id$$
$$= S(a + ic) + S(b + id)$$

and also preserves multiplication

$$S[(a + ic)(b + id)] = S[(ab - cd) + i(ad + bc)]$$

$= (ab - cd) - i(ad + bc)$
$= (a - ic)(b - id)$
$= S(a + ic)S(b + id).$

It is an example of a ring automorphism.

Definition 9.4.4. *A ring automorphism* T *of a polynomial is a bijective mapping of its roots*, a, b: a ↔ T(a) *so that sums and products are preserved*

$T(a + b) = T(a) + T(b)$ (4)

$T(ab) = T(a)T(b),$ (5)

(*the bijection implies* T(a) = T(0) *if and only if* a = 0). (6)

Example 9.4.5. We see from the definition that the identity map $a + ic \to S'(a + ic) = a + ic$ is also a ring automorphism.

Theorem 9.4.6. *All ring automorphisms of a polynomial ring* $\mathbb{P}$ *form a ring*.

Proof. By (4), the sum of two ring automorphisms is also a ring automorphism, and the zero element of the automorphism ring is T(0), since

$T(0 + 0) = T(0) + T(0),$

and from the properties of a ring, negative ring automorphisms exist.

From (5) the product of two ring automorphisms is a ring automorphism, where the identity is

$T(1) = T(1)T(1).$

That the distributive laws hold follows from the corresponding statements for a ring:

$a(b + c) = ab + ac,$

so

$T(a(b + c)) = T(a)T(b + c)$
$= T(ab) + T(ac)$
$= T(a)T(b) + T(a)T(c).$ □

Remark 9.4.7. If T could act on inverse elements, not generally existing in a polynomial, then inverse ring automorphisms would be present and these would form a field:

$T(1) = T(a)T(a^{-1})$
$= T(a)[T(a)]^{-1}.$

Theorem 9.4.8. *If two roots* u_1 *and* u_2 *differ*, *then so too do their ring automorphisms*.

Proof. If $u_1 \neq u_2$ then $(u_1 - u_2) \neq (u_1 - u_1) = 0$, so from (6)

$T(u_1) - T(u_2) \neq T(0) = 0.$ □

Theorem 9.4.9. *If* u *is a root of a polynomial equation in* x, *so is* T(u).

Proof. If $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$, then x is a variable and T applies to it, whilst a_r is a complex coefficient and we will assume in this chapter can be chosen fixed with $T(a_r) = a_r$, so

$T(0) = 0$
$= T(u^n + a_{n-1}u^{n-1} + \ldots + a_0)$
$= T(u)^n + a_{n-1}T(u)^{n-1} + \ldots + a_1T(u) + a_0.$ □

If firstly we consider linear ring automorphisms, for a linear map

$U(a + ic) \to ga + ihc + m,$

then for this to be a ring automorphism, the definition of U implies

$$U(a + ic) + U(b + id) = U((a + b) + i(c + d)) + m, \quad (7)$$

so the additive condition for a ring automorphism, (4), gives

$$m = 0. \quad (8)$$

Also, from equation (5) the multiplicative ring automorphism

$$(ga + ihc)(gb + ihd) = g(ab – cd) + ih(cb + ad)$$

thus

$$g^2ab – h^2cd = g(ab – cd) \quad (9)$$

and

$$g(cb + ad) = cb + ad, \quad (10)$$

so that g = 1, which implies from (9) that $h^2 = 1$, that is, $h = \pm 1$. □

In general, if a polynomial ring automorphism were of the form

$$U'(a + ic) = \sum_{j+k=0}^{r} g_{jk}a^j(ic)^k, \quad (11)$$

the definition of U′ and (4), imply for the same reasons as equation (8) that

$$g_{00} = 0, \quad (12)$$

thus the summation can start from 1

$$U'(a + ic) = \sum_{j+k=1}^{r} g_{jk}a^j(ic)^k. \quad (13)$$

From the additive ring automorphism equation (4)

$$U'(2a + i2c) = 2U'(a + ic), \quad (14)$$

so

$$\sum_{j+k=1}^{r} g_{jk}(2a)^j(i2c)^k = 2\sum_{j+k=1}^{r} g_{jk}a^j(ic)^k, \quad (15)$$

and since this holds for arbitrary a and c, if we assume (15) for r, then for r + 1

$$\sum_{j+k=r+1} g_{jk}(2a)^j(i2c)^k = \sum_{j+k=r+1} 2^{r+1}\, a^j(ic)^k$$

$$= 2\sum_{j+k=r+1} g_{jk}a^j(ic)^k,$$

$$\sum_{j+k=r+1} g_{jk}(2^{r+1} - 2)\, a^j(ic)^k = 0. \quad (16)$$

If g_{jk} does not depend on a or c, this means r + 1 = 1, which is the linear automorphism already encountered. □

We have seen in the previous section that a ring automorphism is of the form

$$U(a + ic) = a + ihc, \quad (17)$$

where $h = \pm 1$. Therefore defining U^2 by

$$U^2(a + ic) = U[U(a + ic)]$$

$$= U[a + ihc]$$

$$= a + ic, \quad (18)$$

we find that ring automorphisms are involutions; U^2 is the identity. □

Since theorem 9.4.9 shows that if u is a root then so is the ring automorphism T(u), this only swaps roots, since T^2 is the identity. As we will show, there must be ring automorphisms with many instances.

We can introduce an equivalence class of automorphisms by defining the maps

$$a \to e + if$$

$$c \to s + it$$

so that where by implication we had previously assumed a and c real, these are now complex.

Thus we can form, say, continuous maps

$$a + ic \to (e – t) + i(s + f)$$

We can now treat the automorphism U(a + ic) as the automorphism

$$U''[(e - t) + i(s + f)] = (e - t) + ih(s + f), \quad (19)$$

where U and U″ are identical if f = 0 and t = 0, and are defined distinct otherwise.

We can put U ≡ U″ in the same equivalence class if there is a continuous map with end points U = [e, is] and U″ = [-t, if]. □

We can prove that a linear substitution of the variable x, called a Tschirnhaus transformation, which we will denote by T′, does not usually form a ring automorphism. Let

$$T': x \to gx + m,$$

where g and m belong to a field, be a linear transformation.

Theorem 9.4.10. T′ *is not a ring automorphism unless* g = 1 *and* m = 0.

Proof.

$$T'(x + x) = g(2x) + m \neq T'(x) + T'(x)$$

and

$$T'(xx) = g(x^2) + m \neq (gx + m)(gx + m) = T'(x)T'(x). \square$$

We can extend theorem 8.4.10 to consider the map

$$a + ic \to g(a + ihc) + m. \square$$

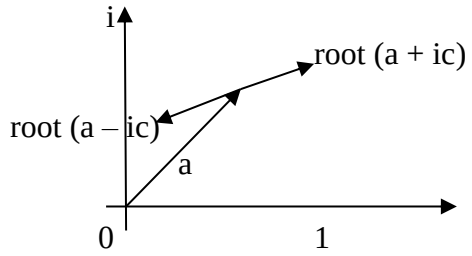
Since a ring automorphism is a symmetry operation, we are justified in calling a Tschirnhaus transformation a symmetry breaking operation.

For monic polynomials, the products factorise as terms like (x – u). Here u is a fixed element of a field and x is a variable, of which there is only one type. Thus if we apply the linear substitution x = y + m with m fixed (this would hold when the transformation is non-linear) we can view this two ways, firstly as a re-labeling of the variable x where the automorphism idea applies, and secondly as a transformation of u, which is no longer a fixed element. In the first interpretation we allow ring automorphisms, and in the second, we do not.

The second way, the transformation (x – u) → (x – u + m), makes available a method for solution of polynomial equations. We will see in section 7, that solutions of complex polynomials exist, so if the solution is accessible there exists a state as well as a transformation where the roots are detected by an automorphism under re-labeling of x. Conversely, a solution by radicals is inaccessible if and only if no ring automorphism can describe it.

Since we have found that the Tschirnhaus substitution is a trivial ring automorphism, it follows that polynomial recursion on adding further linear transformations to a polynomial in x so that y = x + h and z = y + h′ does not alter the solvability question if it is determined by automorphisms. Related questions will be studied in volume 3 chapter 1, where we discuss varieties.

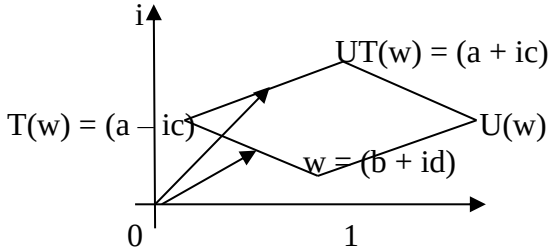
We have described a ring automorphism as a map U: a + ic → a – ic, where a and c are complex in the general case, and U^2 is the identity. The pair of roots this describes can be pictured in an Argand diagram. Any pair of roots can be pictured in this way. For two roots in the Argand diagram, draw the connecting lines between them. Then the value a is the complex vector between 0 and the midpoint of the two roots and the value ±ic is the vector from the tip of a to one of the roots.



For three roots, define one of the previous roots, say a – ic, and the new root b + id. Then the construction proceeds as before, this time on the vector [(a + b) + i(d – c)]/2. If T is this new ring automorphism, then we can define for the root w at b + id, the ring automorphism T(w) = a – ic, and then form UT(w) = a + ic.

A ring automorphism T(w) of a root w transfers the root to another root, but does not in general keep roots outside of this pair fixed. If we apply an automorphism U distinct from T to the root T(w), then UT(w) is a ring automorphism, but U acts on T(w) and not w, so that U(w) is not a root automorphism.

Note that, although in general U(w) = U(b + id) is not a root, we can define U(b + id) from the following parallelogram:



Then from the properties of the parallelogram, we have

$$UT(w) = TU(w),$$

and so

$$U^{-1}UT(w) = T(w)$$
$$= U^{-1}TU(w).$$

The ring automorphism $U^{-1}TU$ is known as an inner ring automorphism. □

Definition 9.4.11. An *isolated ring automorphism* acts on a pair of roots

$$(x + a)(x + b) = 0 \qquad (20)$$

maintaining their invariance under the automorphism. It is thus equivalent to a permutation of two roots in multiplicative format.

Definition 9.4.12. A generally complex symbol has *real* (respectively *imaginary*) *status* if it has the same properties under a ring automorphism as a real (respectively imaginary) symbol.

Writing x as y + iz, and treating a and b as symbols with real status, we have

$$y + iz + a = 0 \qquad (21)$$

under the automorophism

$$y + iz \rightarrow y – iz \qquad (22)$$

is the same as

$$y – iz + b = 0, \qquad (23)$$

that is on adding (21) and (23)

$$y = (a + b)/2 \qquad (24)$$

and

$$iz = (a - b)/2. \tag{25}$$

Alternatively, we can treat x as a symbol with real status and introduce the roots

$$(x + c + id)(x + e + if) = 0 \tag{26}$$

so that under an isolated automorphism, this is the same as

$$(x + c - id)(x + e - if) = 0. \tag{27}$$

Another way of putting this is that under the permutation of roots, (26) and (27) imply

$$x + c + id = x + e - if, \tag{28}$$

so that on identifying parts with real and imaginary status

$$(e - c) = i(d + f) = 0. \ \square \tag{29}$$

For isolated transformations, we now relate these ideas to the theory of varieties. Note that if we can solve (1) we can also solve

$$(x + wa)(x + wb) = 0, \tag{30}$$

and since the two solutions are linear in x, a and b, any root which is valid for (20), say

$$x = -a,$$

is also valid in (30) for

$$x = -wa,$$

and to generalise, for any expression involving a and b combined, say in the function f(a, b) satisfying

$$x = f(a, b)$$

from the analogue of (20), it has the solution

$$x = wf(a, b)$$

under a transformation to the analogue of (30). $\square$

Let us consider the expression (20) under the linear substitutions

$$x = u + p \tag{31}$$

$$a = gu + q \tag{32}$$

$$b = hu + r, \tag{33}$$

then one of the roots is

$$(u + p) + gu + q = 0, \tag{34}$$

satisfying

$$u = -(p + q)/(1 + g). \tag{35}$$

For p = 0, g = h = 1, (1) becomes

$$u = -q/2 \text{ or } -r/2, \tag{36}$$

since using expressions like (34)

$$(2u + q)(2u + r) = 0.$$

Then as an automorphism (24) and (25) become under

$$u = y + iz, \tag{37}$$

the allocations

$$y = (u + q + u + r)/2 = u + (q + r)/2, \tag{38}$$

$$iz = (u + q - u - r)/2 = (q - r)/2, \tag{39}$$

and this is the form for a linear transformation of an isolated ring automorphism. $\square$

Definition 9.4.13. A *combined ring automorphism* is a multiplicative sequence of isolated ring automorphisms, each isolated isomorphism of which is independent of the others.

Notation 9.4.14. We use the symbol i for the first imaginary part of a variable occurring in the first isolated ring automorphism in the sequence, and i', i'' etc. for later ones.

Thus in our notation

$$i^2 = i'^2 = \ldots \text{ etc.}, = -1 \tag{40}$$

and

$$ii' = -1 \tag{41}$$

for all combinations. This notation allows us to keep track of the independent automorphisms occurring in a combined ring automorphism.

We wish to consider combined automorphisms in a simple case. We will first consider the quartic polynomial equation, and we will compare the same quartic polynomial written in standard form, and expanded out as containing terms in combined format.

Consider the complex polynomial equation

$$x^n + p_{n-1}x^{n-1} + \ldots + p_1x + p_0 = 0, \tag{42}$$

As an example, we will choose n = 4 and put (42) in combined automorphism form

$$(z + a + ib)(z + c + id)(z + e + i'f)(z + g + i'h) = 0. \tag{43}$$

On expanding out, the z^3 coefficient is

$$(a + c + e + g + i(b + d) + i'(f + h)) = p_3 = 0, \tag{44}$$

where we have chosen to make a Tschirnhaus substitution so that $p_3 = 0$. Thus equating real and imaginary status parts

$$g = -a - c - e \tag{45}$$

$$d = -b \tag{46}$$

$$h = -f. \tag{47}$$

We will resubstitute these values in (43), to obtain

$$(z + a + ib)(z + c - ib)(z + e + i'f)(z - a - c - e - i'f) = 0, \tag{48}$$

so

$$(z^2 + (a + c)z + ac - b^2 + ib(c - a)) \times(z^2 - (a + c)z - e^2 - e(a + c) - f^2 - i'f(a + c + 2e)) = 0, \tag{49}$$

and equation (30) may be split into two similar results, the first being

$$z^2 + (a + c)z + ac - b^2 + ib(c - a) = 0. \tag{50}$$

Now if this remains invariant under the automporphism $i \rightarrow -i$ on (50), then we obtain

$$z^2 + (a + c)z + ac - b^2 = 0, \tag{51}$$

$$b(c - a) = 0. \tag{52}$$

which gives with c = a or b = 0, the standard quadratic equation in real status symbols, in a form which is solvable for coefficients in (42) under substitutions.

Hence, applying this to a general polynomial of degree 2n, in which a polynomial of degree 2n – 1 can be embedded

Theorem 9.4.15. *Transformations available under multiplicative representations of roots are not enhanced by the incorporation of combined ring automorphisms*. □

For groups, the isomorphism $G \rightarrow G$, $x \leftrightarrow g^{-1}xg = h(x)$ is called an *inner automorphism*, since it satisfies the group automorphism axiom

$$h(xy) = h(x)h(y). \ \square$$

A group automorphism which is not inner is *outer*. As pointed out by J.S. Milne [Mi14], the group automorphism model can be extended to include outer automorphisms.

Concerning the representation of a polynomial in multiplicative format, this is always solvable, the group of permutations of these roots is called the symmetric group, and the polynomial remains solvable on introducing new roots, which can be represented by features of the symmetric group. Thus under this model, a 'solvable group' or its transformations does not represent a 'solvable polynomial', since they can also be represented by 'unsolvable groups'. Thus the Galois model of the solvability mapping from groups to polynomials requires justification from elsewhere.

We have seen that ring automorphisms are commutative, and thus in the general case cannot be represented by permutations. Further, the group automorphism idea must extend to that of ring automorphisms, otherwise if addition is irrelevant to the group structure, a polynomial in multiplicative format cannot be transformed to a polynomial in additive format.

We cannot claim in general that if we add the extra distributive axioms

$$a(b + c) = ab + ac$$

to the axioms for a multiplicative group, even if that group describes some of the properties of a polynomial in multiplicative format, then unsolvability criterions derived in that way are unaffected by the introduction of the distributive rules, since there is the possibility that the theory augmented with addition might alter these criterions.

If we say the permutation structure of a group automorphism has nothing to do with addition or multiplication, are we to assume that the roots of a quintic equation permute the formulas expressed with the variable x as each of the roots? Then the permutation of formulas gives no method for obtaining solutions, nor does this change when we consider that a property of the alternating group on five letters is that it has no nontrivial normal subgroups.

Theorem 9.4.16. *There exist successive ring automorphisms which do not correspond to any permutation of roots*.

These successive ring automorphisms are not combined ring automorphisms in the sense we have used these terms, since combined automorphisms act on isolated pairs which permute independently of one another, but successive ring automorphisms may not.

Proof. Consider four roots, A, B, C and D. Apply a ring automorphism to A and B, so that A becomes B and B becomes A. Now apply a ring automorphism between B and C, then A is displaced in general to a non-root A′. Then applying the same process with D replacing A, then D is displaced to a non-root D′. Apply the ring automorphism to A′ and D′, then all roots are displaced in general to non-roots. □

The deconstruction of Galois theory, which contains within it a theory of groups based on the permutation of roots, has now taken place in this chapter. This analysis has depended on the theoretical understanding of automorphisms begun by E. Artin [Ar59], and a further account given by Birkhoff and Mac Lane [BM69]. Our point of view is this. Viewed as a theory of groups, Galois theory is correct. Viewed as a theory of rings, in particular as a solvability model for polynomial rings, it fails; we have proved formally that a complex polynomial equation remains commutative under ring automorphisms, and further that the only instances of such automorphisms are themselves commutative.

This insight is similar to the observation, as we have proved in chapter III of [Ad15], that Wedderburn's little theorem states that all finite division rings are commutative, and thus noncommutative algebra has no part to play in the implementation of such rings.

Galois *representation* theory is used in a number of important areas of mathematics: the proof of Fermat's last theorem, the proof of the Weil conjectures, and in the classification of finite groups, but it can be made independent of the Galois *solvability* theory discussed here.

Features of the various models of solutions by radicals are itemised below.

	Variety	**Ring automorphism**	**Galois**
Transformation type	all	ring automorphism (a) isolated (b) combined	group automorphism
Solution method	(1) polynomial wheel (2) comparison (3) killing central terms	ring automorphism	false
Polynomial solvability	(1) unlimited (2) unlimited (3) restricted to degree ≤ 4	known for degree 2	restricted to degree ≤ 4
Dependent roots	incorporated	duplicate roots are identity involutions	defective (inseparable extensions)
Linear transformations	allowed	usually violated	usually violated

Table 9.4.17. *Theories of complex polynomial equations*.

9.5. Dependency theory restrictions.

Although explicit coefficients may have dependencies giving rise to solvable equations, we now show that an end result of Galois theory holds: by 'killing central terms' there are no solutions by radicals for general complex polynomials of degree > 4.

We will divide the proof into two parts. In the first part we will show that for varieties in two variables written in additive format, the only possible linear substitution of variables that kills central terms occurs for equations of degree ≤ 4.

We then show that for varieties in more than two variables, when these are represented by a common variable plus another term, then this reduces to the case of two variables.

Theorem 9.5.1. *Let* R[y, z] *be a ring of polynomials in two variables*. *The only linear substitutions* $y = sx' + u$, $z = tx' + v$ *that kill central terms in all cases occur for degrees in* $x' \leq 4$.

Proof. Consider the quadratic variety in which dependencies have been removed

$$y^2 + ayz + bz^2 = 0. \quad (1)$$

If we make the substitutions

$$y = sx' + u, \quad (2)$$

$$z = tx' + v, \quad (3)$$

then under the further linear substitution

$$x' = [(q - p)x + (vp - uq)]/(sq - pt) \quad (4)$$

we get

$$y = x + p, \tag{5}$$

$$z = x + q, \tag{6}$$

which maintains the relative proportions of y and z, and we will keep these. If the relative proportions of y and z change, we have $y = rz$, with $r \neq 0$. Putting $r = 1$, this gives

$$(1 + a + b)x^2 + [2p + a(p + q) + 2bq]x + [p^2 + apq + q^2] = 0, \tag{7}$$

and we can 'kill the central term' in x, by a choice of p, for instance. Then equation (7) is solvable. The solution is

$$x = \pm\sqrt{\frac{p^2 + apq + bq^2}{(1 + a + b)}}. \tag{8}$$

Consider the cubic variety

$$y'^3 + a'y'^2z' + b'y'z'^2 + c'z'^3 = 0. \tag{9}$$

Put

$$y' = Py + Qz$$

$$z' = Ty + Uz$$

then there exists a solution of

$$y^3 + ay^2z + byz^2 + cz^3 = 0,$$

in which primed variables are expressed in terms of the unprimed variables. This follows because there are sufficient degrees of freedom to give a solution (fixing the coefficients 1, a, b and c in terms of the coefficients 1, a′, b′ and c′, there are four variables, P, Q, T and U to do this). We will not attempt to find this explicitly, and we will not assume this is given by a solvable formula.

We will make the same substitutions for y and z as before, so that

$$\begin{aligned}(1 + a + b + c)x^3 &+ [3p + a(2p + q) + 2b(p + 2q) + 3cq]x^2 \\ &+ [3p^2 + a(2pq + p^2) + b(2pq + q^2) + 3cq^2]x \\ &+ [p^3 + ap^2q + bpq^2 + cq^3] = 0.\end{aligned} \tag{10}$$

We will now set the coefficient of x^2 to zero, and this is linear in p, q, and a, b and c, and also the coefficient in x to zero, which gives a quadratic equation on substitution from the first zeroised coefficient equation, for example on substituting for 3cq. The resulting equation expresses p in terms of q, and the coefficients a and b, but this means we have a constraint on the variable c. We have seen a solution with $a = a'$, $b = b'$ and the variable c reset to its original value exists. We also know a solution of the cubic by a formula exists, but we have only shown in this section that such a solution may be possible, as a solution already derived by these methods for the quadratic equation.

Consider the quartic variety

$$y^4 + ay^3z + by^2z^2 + cyz^3 + dz^4 = 0. \tag{11}$$

Then by the same substitution

$$y = x + p,$$

$$z = x + q,$$

we can kill the x^3 and x coefficients. The first is a linear equation again, and the x coefficient term is a cubic, so that by a similar method to the one before, it may be possible to solve a cubic equation for p and q. This may now be reduced to an equation essentially of the form suitably defined of

$$x^4 + ex^2 + f = 0, \tag{12}$$

which we can solve as a quadratic in x^2. Thus the quartic equation may be solvable.

Now consider the quintic variety

$$y^5 + ay^4z + by^3z^2 + cy^2z^3 + dyz^4 + ez^5 = 0. \tag{13}$$

We have three free variables, p, q and r, $r \neq 0$, in the substitution for x. But we must set the coefficients of the four variables x^4, x^3, x^2 and x to zero, and this is impossible to solve independently of x. Thus the solution of the quintic is impossible by this method. The degree is prime, so the number of variables needed is this prime number minus one.

Further, for the sextic

$$y^6 + ay^5z + by^4z^2 + cy^3z^3 + dy^2z^4 + eyz^5 + fz^6 = 0, \tag{14}$$

we must set the coefficients of x^5, x^3 and x to zero, and this is impossible independently of x for three variables p, q and r, if we have to solve a quintic. Thus the solution of the sextic is impossible by this method. We also show polynomials are unsolvable this way for degree a product of primes.

All higher degree equations than the sextic need more variables than three, p, q and r, to solve them, hence there is no general solution independent of x by this method. □

Theorem 9.5.2. *The polynomial* $R[y_1, ..., y_m]$ *in* m *variables of degree* n *can be reduced to a polynomial* R[y, z] *in two variables*.

Proof. We now consider the case of introducing more than two variables in a variety. For example for the sextic, with degree a product of more than one prime, we could have

$$(u^3 + au^2v + buv^2 + cu^3)^2 + g(u^3 + au^2v + buv^2 + cu^3)(y^3 + ay^2z + byz^2 + cz^3) + h(y^3 + ay^2z + byz^2 + cz^3)^2 = 0, \tag{15}$$

where

$$\begin{aligned} u &= x + r, \\ v &= x + t, \\ y &= x + p, \\ z &= x + q. \end{aligned} \tag{16}$$

Let us restrict ourselves to three of these equations. Then if $t \neq p \neq q$ we may put

$$v = jy + kz, \tag{17}$$

$$x + t = (j + k)x + (jp + kq), \tag{18}$$

so

$$\begin{aligned} j + k &= 1, \\ jp + kq &= jp + (1 - j)q = t \\ &= j(p - q) + q, \end{aligned}$$

and

$$j = (t - q)/(p - q) \tag{19}$$

can always be chosen so that v is a linear combination of y and z. The same can be said of other variables.

Thus equation (15) must be equivalent to two variables, y and z, and we have already proved that this is impossible to solve independently of x. The general case is similar. □

The following example is included in the conditions for the previous two theorems, on multiplying out the factors.

Example 9.5.3. *Equation* (20) *expanded out contains a constraint on the coefficients, so the additive form* (22) *is not the most general.*

Proof. Let

$$(x^3 + py^3)(x^2 + qxy + ry^2) = 0. \tag{20}$$

We know the left hand term can always be rearranged in this form from an arbitrary cubic.

Then expanding out

$$x^5 + qx^4y + rx^3y^2 + px^2y^3 + pqxy^4 + pry^5 = 0, \quad (21)$$

and if this is equated to

$$x^5 + Hx^4y + Ix^3y^2 + Jx^2y^3 + Kxy^4 + Ly^5 = 0, \quad (22)$$

then there are constraints on the coefficients

$$L = IJ,\ K = HJ, \quad (23)$$

so there is a constraint

$$HL = KI, \quad (24)$$

and this cannot be removed in a way that is independent of x and y, say by boosting x or y by a factor. But if x or y are shifted by a term, then the previous theorems apply. □

We have seen that isolated automorphisms are equivalent to equating real and imaginary parts of symbols (which may be complex) with $i = i'$. Combined automorphisms also allow $i = -i'$. To distinguish between combined ring automorphisms we will sometimes write $x \pm_u iu$ for a ring automorphism with values $x + iu$ and $x - iu$.

Lemma 9.5.4. *If* $x \pm_u iu$ *and* $x \pm_v iv$ *are distinct combined ring automorphisms, then if* $x \pm_w iw$ *is another ring automorphism,* w *is a linear combination of* u *and* v.

Proof. A linear combination of ring automorphisms is also a ring automorphism. Consider the ring automorphisms $\beta(x \pm_u iu)$ and $(1-\beta)(x \pm_v iv)$. Provided $u \mp_v v \neq 0$, their linear combination

$$(x \pm_w iw) = \beta(x \pm_u iu) + (1-\beta)(x \pm_v iv)$$

is satisfied by

$$\beta = \frac{\pm_w w \mp_v v}{u \mp_v v}. \ \square$$

Corollary 9.5.5. *A polynomial in multiplicative combined ring automorphism form may be written as*

$$(x + a \pm_u iu)(x + a \mp_u iu)(x + b \pm_v iv)(x + b \mp_v iv) \cdots$$
$$(x + c \pm_w iw)(x + c \mp_w iw) = 0,$$

where c *is a linear combination of* a *and* b, *and* w *is a linear combination of* u *and* v. Its additive form is therefore of the type we will use next. □

Lemma 9.5.6. *Let*

$$(x + p + ia)^n + a_{n-1}(x + p + ia)^{n-1}(x + q + i'b) + \ldots + a_0(x + q + i'b)^n = 0. \quad (25)$$

Then combined automorphisms constrain the coefficients, but isolated automorphisms give equivalent results to linear transformations, where

$$p + ia \to p$$
$$q + ib \to q. \quad (26)$$

Proof. Applying isolated automorphisms $i \to i$ and $i' \to i'$, and equating real and imaginary parts, by the binomial theorem for the coefficient a_{n-1}

$$np + a_{n-1}((n-1)p + q) + \ldots + a_0 q = c \quad (27)$$

for some c and

$$na + a_{n-1}((n-1)a + b) + \ldots + na_0 b = 0. \quad (28)$$

Applying the further combined automorphism $i \to -i'$ gives

$$na + a_{n-1}((n-1)a - b) + \ldots - na_0 b = 0. \quad (29)$$

Thus (28) and (29) constrain the coefficients $a_{n-1}, \ldots a_0$, but add no further information. □

Transformations of variables may be classified in various ways. There is the linear transformation

$$x \to px + q, \tag{30}$$

where we have seen that if

$$y = x^n + a_{n-1}x^{n-1} + ... + a_0, \tag{31}$$

and the zeros of y are solvable, then on putting

$$y = w + g, \tag{32}$$

$$x = w + h, \tag{33}$$

the equation in w is also solvable, and thus the nonlinear allocation reduces to a linear one.

We have also seen in lemma 8.5.4 that for a ring automorphism acting on symbols a and b, so that

$$a + ib \to a - ib, \tag{34}$$

then combined ring automorphisms, the most general type of ring automorphism available to polynomials, have no other effect than constraining coefficients when i and i′ are present, so we now discount this type of solution.

Thus linear transformations are the only transformations we have not discounted.

Theorem 9.5.7. *The solution by radicals of any polynomial with independent roots in* x *of degree* n > 4 *which includes a killed solution of the quintic must be dependent on* x.

Proof. We have already proved the theorem when each central term is killed individually. Now consider the case where not all central terms are zeroised. This means the polynomial equation is split into at least two separate polynomial equations, say an outer polynomial containing x^n and a_0, and an inner polynomial containing central terms. But if these polynomial equations are independent, there must exist coefficients of these polynomials for which the polynomial equations have no dependent solutions between them, a contradiction.

Conversely, if a polynomial of degree n > 4 has a solution by multiplication of n independent roots, a relation between two non-intersecting polynomials containing the central terms will have different solutions. Thus no pair of such polynomials exists. Hence if a solution by radicals exists, all central terms for n prime are zeroised. For n = 5 we have seen that no independent variables can satisfy this condition, and the solution for n > 5 may involve the case for n = 5. Hence under these conditions any other method to find a solution by radicals reduces to the solvability case of killing central terms. □

9.6. 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

$$x^3 + Kx + L = 0 \tag{1}$$

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

$$x^3 = 2, \quad (26)$$

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. □

A polynomial is a ring, which has additive and multiplicative operations. Galois solvability theory says we may for the purpose of solving a cubic equation, assume that only the group multiplicative structure of the ring is important. Further, it says that the group structure embedded in the ring provides a solution. Indeed it does. What we have found here, but not proved, is that by appending a bogus root to the polynomial so that it becomes a quartic polynomial equation and not a cubic, we have found an illegal solution. By Galois solvability theory the solution of a cubic using only square roots and no cubic roots is impossible. But we have found such an impossible solution. □

9.7. Abstract underpinnings of polynomial wheels. First example.

At the end of chapter 6 we said that we would not always use an abstract approach because we wanted to explain and be understood.

This section may, and perhaps will, be converted to an abstract discussion, and the theorems derived from many abstractly viewed results can be linked so that they end up with the result that any polynomial equation of degree n is solvable 'by radicals'. This means there exist universal symbols in which these polynomials are expressed and these may be converted to polynomial equations which can be expressed in the same universals. A polynomial equation of degree n has n solutions, each of which may be represented by combinations of the universal symbols using addition, subtraction, multiplication, division and the use of mth roots of these symbols.

I wish to give an analogy of our approach to the historical development of the proof of the Pythagoras theorem. The reader may not be aware of this history (nor in many ways are we), and may not even, given a modern approach of replacing geometry by vectors, and the Pythagoras theorem as a result on vector scalar products, know of the proof introduced by the Greeks to prove it using very general simple rules called axioms expressing geometry.

The earliest evidence of man thinking about numbers comes from Africa 35,000 years ago. The Ishago bone from Africa between Congo and Rwanda is about 20,000 years old. It is possible this example was in use before the invention of writing. It probably shows sequences of prime numbers. Detective work indicates it uses number systems to bases 10 and 12, and is a calculator for multiplication. This would indicate an African civilisation 15,000 before that in Egypt.

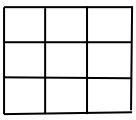
The Sumerian civilisation of 3000 BCE, covering modern-day Iraq, had a zero and a modern place system but no place marker for decimal points. Multiplication and division with numerals to the base 60 was used by them. The Moscow mathematical papyrus from Egypt dated 1890 BC contains Pythagorean triples, and the Babylonian tablet Plimton 322, dated 1822 – 1784 BC, probably from a teacher setting problems to students, gives 11 of them. In China the

Pythagoras theorem, known as the Gougu theorem, developed around 1000 BC. Pythagoras went to Egypt around 535 BC.

In modern notation the simplest example is

$$3^2 + 4^2 = 25 = 5^2. \qquad (1)$$

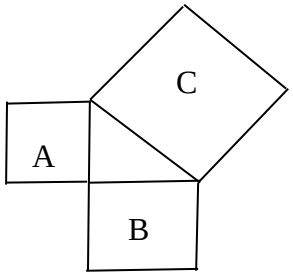
The square of a number, say 3, may be represented by a geometrical figure, a square, so that its area is $3^2 = 9$ squared units.



A problem was that you can give a very large number (in fact an infinite number) of examples of whole number Pythagorean triples like (1), but you have not proved it in the general case.

The Greeks also knew that you cannot represent some numbers, like $\sqrt{2}$, as a whole number n divided by a whole number m in lowest terms, so that common factors are divided out.

So they came up with the idea of representing any number, like $\sqrt{2}$, and numbers like π, where the area of a circle of unit radius is π, geometrically. The problem of proving the Pythagoras theorem then reduces to proving in a 'right angled triangle'



where A, B and C are areas, that

$$A + B = C.$$

You have to prove what you mean by a right angle, and then discover basic building blocks for a proof, assumptions or axioms, that you use to prove the result. But the approach is clear.

A problem is, when you turn this reasoning upside down, and start with axioms, and then go through a series of theorems where you always apply these rules mechanically, and you end up with the final result, the Pythagoras theorem

(i) The sequence of the applications of rules to obtain the Pythagoras theorem is long.

(ii) If you do not explain where you are going, you end up with a series of (possibly boring) intermediate results, and then when the surprising result, the Pythagoras theorem, comes at the end, you have to scramble through the intervening results to understand them, because you have come to the revelation that you have acquired knowledge that is important.

I want to prove that any polynomial equation is solvable by radicals. The general theory we can describe did not arise from the application of abstract principles, just as the proof of the Pythagoras theorem by the Greeks did not originate from abstract principles. The method was founded on the existence of concrete examples. Rigour came afterwards.

Archimedes could solve the cubic.

http://www.hellenicaworld.com/Greece/Science/en/ArchimedesEquations.html

The burning of books and burying of scholars occurred in China 213 – 210 BC. Wang Xietang in the Tang Dynasty (618 – 907) could solve the cubic.

https://en.wikipedia.org/wiki/Chinese_mathematics

Ceyuan heijing or *Sea Mirror of the Circle Measurements* is a collection of 692 formulas and 170 problems written by Li Zhi (1192 – 1272 AD). He used Horner's method to solve equations of degree as high as six.

Here is a fundamental result, like a Pythagoras theorem example. For some coefficient symbols Q, R, S, T and U there exists a variable x with coefficients F, G, H, K, L and M satisfying

$$x^5 + Qx^4 + Rx^3 + Sx^2 + Tx + U$$
$$= (x^3 + Fx^2 + Gx + H)^2 - (x^3 + Kx^2 + Lx + M)^2 = 0.$$

What is the theoretical underpinning of this simple result?

I wish to relate this to the theory of rings which we have extensively discussed. These have operations + and ×.

For the operation +, when variables are complex numbers, then addition of complex numbers is a complex number, and we can add the negative of a complex number to the complex number to form zero. These features with the abelian and associative nature of addition, define complex numbers under + as a group.

Multiplication for rings has in general no inverse, so they are not groups, although for complex numbers, × is again closed under multiplication and is abelian and associative.

When we combine these operations together, which is related to a similar discussion in chapter V, section 2, because for $n \neq m$, $n \times 0 \neq m \times 0$, multiplication is not unique. Thus, if we want generally to have unique results, we cannot include 0 in a multiplicative structure. This means we must consider + and × separately.

But if we include 0 in the additive side for a set and exclude it for elements under multiplication, if a variable $y = x^n + a$, where a has degree in x less than n, and a variable $y' = x^n + b$, where b has degree in x less than n, additively we can form $y - y'$, and this has degree less than n.

It follows that two polynomials C and of degree n, each squared, may be combined together under subtraction to form a polynomial of degree $2n - 1$.

Consequently, if we can solve a general equation of degree n by radicals, there is the possibility, for which we must provide an implementation, of solving a general equation of degree $2n - 1$. If that were the case, we could solve a general equation of degree $2n - 2$, since on applying a known bogus root to this, we obtain an equation of degree $2n - 1$.

Thus whether n is even or odd, by induction there would be a general method of solving polynomial equations by radicals for all n. □

We have now an indication of why Galois solvability theory is defective in the general case, not just the cubic of section 6. If we were able to find a solution of the quintic directly using the above technique, this would dynamite Galois solvability theory which states directly that such a solution in the general case is never possible. Further, this would give an underlying

reason why Galois solvability theory is false: the zeros of polynomial rings have solutions dependent on higher degrees which are solvable and reduce backwards to solutions by radicals which are impossible by Galois solvability theory. □

9.8. Second example. An additive and multiplicative ring game.

For the case we will study here, we will consider two ring algebras operating simultaneously. On the 'left' hand side we have an additive structure (mod p) where p is prime, so this contains the number zero. On the right we have two multiplicative structures. The first is zero under multiplication but we will also consider is a ring and the second is a multiplicative structure (mod q) where zero does not occur. The latter is a group, but we are not interested in division properties here, only multiplication. Say q and p differ. This means for the structure on the 'right' the zero multiplication object can combine with the nonzero multiplicative structure on the right, and everything is consistently within a ring (mod q), where the zero object has special properties, but is still consistent outside the (mod q) structure.

To put it another way, the consistent bijective group map addition → multiplication

$$(0, a > 0) \rightarrow a > 0$$

maintains additive and group structures. In general, when the left hand side may not be zero, the mapping is confused and in unreason. However, murder of murder

$$(a > 0, b > 0) \rightarrow a.b > 0$$

is consistent and not confused.

We proclaim an inequivalence between rings and groups, which should be in a sense obvious, but also the restriction of this fact to solvability is wrong too. All we have to do is find an example solution, and then we have a direct counterexample, or disproof, of Galois solvability theory. □

We now consider a too abstract discussion which is intended as an 'immersion' technique to allow us to study game theory in a subsequent work whilst being intuitively aware of what will be going on before we eventually reach that stage.

Both the left and the right structures are consistent within their worlds. We will say there is a wall or boundary between these two worlds, which separates them. It is normal to designate a *zero* as a distinguished object belonging to the height of the Kampf wall for a totally interpenetrated 2-game. For another object homotopically reached in its algebra from zero, this may be taken as a Kampf height as a totally blocked and impenetrable Kampf height in a 3-game. Murder is described not ethically but by overwhelming. In the totally interpenetrated instance, the need currency of the ethical system accepts all exchanges of the death currency of the murder component and death wins everywhere.

We like a bit of jargon here. Kant wrote three books all saying the same thing, reality exists. The massive work Critique of Pure Reason says this just as the slim semi-pamphlet the same size as Perpetual Peace, which everyone throws away. Misplacing Descartes Cogito ergo sum as a Kogito think, or mathematical game, and Fizyk as a cleansed reality, we have a {Kogito, Fizyk} object which is injective to Fizyk. An idea is that this inclusion is in truth. We think [Ethics, T, Murder] (T is the control tribble) is antisymmetric representing true to false, where T = X is determinate/blocked, and T = 0 is free when murder overwhelms ethics. For *Jesus forgiveness* the ethicality roles are reversed. Love loves Love, Hate loves Love, Love forgives Hate and Hate forgives Hate. Love is the murder game and overwhelms Hate!

In the example we started with which is in Kogito, an exchange of 0 at the tribble wall keeps all structures in reason, which is the ethics ascent logic to truth. The structure is stable. If we exchange another object, say 2, say from '+' on the left to 'x' on the right, then the 0 coset 'x' form which originally had no effect now becomes a disruptive 2 coset operator, and the murder ring has no consistent algebra – we are in unreason. □

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

A polynomial equation in complex variables and coefficients if written as

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

reduces to the equations

$$A + B + \ldots + D = T \quad (2)$$
$$AB + AC + ... + BA + BC + \ldots = U$$
$$ABC\ldots D = W,$$

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

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

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

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

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 Δ > 0 the quadratic has two real roots, if Δ = 0 it has real duplicate roots, whereas for Δ < 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

$$ax^4 + bx^3 + cx^2 + dx + e = 0, \tag{9}$$

its discriminant is

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

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

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

then these are linearly independent, since no nonzero combination of one row with the other will give zero; the first element is $a_n \ne 0$ 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

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

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

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

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.

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

As was proved separately by Bring and Jerrard, the general quintic equation may be put in the Bring-Jerrard form

$$y^5 + My + N = 0, \qquad (14)$$

which with M = -6 and N = 3 is the Abel-Ruffini equation. Under the transformation y = w/t this may be given in reduced Bring-Jerrard form

$$w^5 + w + G = 0. \qquad (15)$$

To reduce the general quintic

$$y^5 + Ay^4 + By^3 + Cy^2 + Dy + E = 0 \qquad (16)$$

to Bring-Jerrard form, we will transform (16) to principal quintic form, which zeroises the coefficients of the y^4 and y^3 terms, using a quadratic Tschirnhaus transformation

$$-z + y^2 + my + n = 0 \qquad (17)$$

and eliminate y between (16) and (17) using resultants, so that (16) and (17) have duplicate roots and we can calculate from their zero Sylvester determinant a z with

$$z^5 + c_1z^4 + c_2z^3 + c_3z^2 + c_4z + c_5 = 0. \qquad (18)$$

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 (16) becomes the principal quintic form

$$z^5 + Uz^2 + Vz + W = 0. \qquad (18)$$

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

$$v = z^4 + Pz^3 + Qz^2 + Rz + T, \qquad (19)$$

so that on eliminating z between (18) and (19) we get

$$v^5 + d_1v^4 + d_2v^3 + d_3v^2 + d_4v + d_5 = 0, \qquad (20)$$

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

$$3QU + 4PV + 5W = 0 \qquad (21)$$

$d_1 = d_2 = 0.$ (22)

Because the third term of (20) has the form

$d_3 = e_3R^3 + e_2R^2 + e_1R + e_0,$ (23)

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. □

9.10. A polynomial wheel method solving the quintic polynomial 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 may indicate that to solve the quintic requires calculations with polynomials of quite high degree. 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 or complexity needed to solve a polynomial is high, we could 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 solution of the quintic polynomial by surprisingly direct and simple methods and so the general solvability issue.

By classical techniques, or those introduced in section 6, the cubic and quartic equations are solvable.

The book *Substitutiontheorie und ihre Anwendung auf die Algebra* by Eugen Netto (1882, Teubner) claims that symmetries act on polynomial equations and transformations of them, which do not change their degree. The explicit method we introduce bypasses this restriction. If we wish to solve the quintic, for instance, then we can use the cubic to solve the quintic equation.

Consider the variety

$$(x^3 + Ax^2 + Bx + C)^2 - (x^3 + Dx^2 + Ex + F)^2 = 0. \quad (1)$$

$$2(A - D)x^5 + (A^2 - D^2 + 2B - 2E)x^4 + 2(AB - DE + C - F)x^3 + (B^2 - E^2 + 2AC - 2DF)x^2 + (2BC - 2EF)x + C^2 - F^2 = 0,$$

$$x^5 + \left(\frac{A+D}{2} + \left(\frac{B-E}{A-D}\right)\right)x^4 + \left(\frac{C-F}{A-D} + \frac{AB-DE}{A-D}\right)x^3 + \left(\frac{B^2-E^2}{2(A-D)} + \frac{AC-DF}{A-D}\right)x^2 + \left(\frac{BC-EF}{A-D}\right)x + \frac{C^2-F^2}{2(A-D)} = 0. \quad (2)$$

Put

$C - F = A - D = k.$ (3)

This is not a homogenous constraint in that A and D are associated with x^4 whereas C and F are pure coefficients of no degree in x. Netto indicates but in no way properly proves that homogenous substitutions reduce to Galois theory.

Equation (2) becomes

$$x^5 + \left(\frac{k+2D}{2} + \left(\frac{B-E}{k}\right)\right)x^4 + \left(1 + \frac{(D+k)B - DE}{k}\right)x^3 + \left(\frac{B^2-E^2}{2k} + \frac{(D+k)(F+k) - DF}{k}\right)x^2$$

$$+\left(\frac{B(F+k)-EF}{k}\right)x+\frac{(k+2F)}{2}=0. \quad (4)$$

Let us see what happens when this quintic equation is represented in Bring-Jerrard form, which is equivalent to a general quintic.

$$x^5+Tx+U=0. \quad (6)$$

Equating coefficients

$$0=\frac{k+2D}{2}+\left(\frac{B-E}{k}\right) \quad (7)$$

$$0=1+\frac{(D+k)B-DE}{k} \quad (8)$$

$$0=\frac{B^2-E^2}{2k}+\frac{(D+k)(F+k)-DF}{k} \quad (9)$$

$$T=\frac{B(F+k)-EF}{k} \quad (10)$$

$$U=\frac{(k+2F)}{2} \quad (11)$$

Thus

$$\left(\frac{B-E}{k}\right)=-\frac{k+2D}{2}$$

$$0=-D(\frac{k+2D}{2})+B+1, \quad (12)$$

giving

$$\frac{k+2D}{2}=(\frac{B+1}{D}),$$

$$k=2(\frac{B+1}{D})-2D, \quad (13)$$

$$F=\frac{B+1}{D}\left(2(\frac{B+1}{D})-2D\right)\left(\frac{B+1}{D}-2(\frac{B+1}{D})D+2\right)+D-2(\frac{B+1}{D}), \quad (14)$$

$$U=\frac{B+1}{D}-D+F \quad (15)$$

$$T=F\frac{B+1}{D}+1. \quad (16)$$

We will use (15) and (16) to solve (14) for F in terms of T and U. Equation (16) will then give $\frac{B+1}{D}$ in terms of T and U, and consequently (15) for D.

$$0=\frac{T-1}{F}(2U-2F)\left(-\left(\frac{T-1}{F}\right)^2+\frac{T-1}{F}(1+2U-2F)+2\right)-U+\frac{T-1}{F},$$

$$0=(T-1)(2U-2F)(-(T-1)^2+F(T-1)(1+2U-2F)+2F^2)$$
$$+F^3(-U+\frac{T-1}{F}). \quad (17)$$

We thus obtain B and D, since from (15)

$$\frac{B+1}{D}=D-F+U, \quad (18)$$

and from (16)

$$D=\frac{T-1}{F}+F-U. \quad (19)$$

From (16)

$$B=\left[\frac{T-1}{F}+F-U\right]\frac{T-1}{F}-1. \quad (20)$$

From (13) with (19) and (20)

$$k=2U-2F. \quad (21)$$

From (21) and (3) we obtain C and A

$$C=2U-F \quad (22)$$

and

$$A=U-F+\frac{T-1}{F}. \quad (23)$$

From (7) we finally obtain E

$$E = B + k\left(\frac{k}{2} + D\right),$$

$$E = \left(\frac{T-1}{F}\right)\left[\frac{T-1}{F} + U - F\right] - 1. \quad (24)$$

Doly García does not accept abstract methods unless they are backed up by specific examples. Perhaps this attitude should be more widely accepted by mathematicians. Our task is now to solve the Abel-Ruffini equation

$$x^5 - 6x + 3 = 0, \quad (25)$$

for which the group theory model was used by Abel to claim there is no solution by radicals. We note that this is in Bring-Jerrard form and thus the solution by radicals we propose is direct.

9.11. 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 given in chapter 8, 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. We again refute this hypothesis.

Theorem 9.11.1. *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*

$$x^5 + Kx + L = 0 \quad (1)$$

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

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

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

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

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

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

Equation (4) is

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

Thus

$$\begin{aligned} &(1 + p + q + r + t)x^8 + (4a + 3pa + 2qa + ra)x^7 \\ &\quad + (4b + 6a^2 + p(c + 3b + 3a^2) + q(2c + 2b + a^2) + r(3c + b) + 4tc)x^6 \\ &\quad + (12ab + 4a^3 + p(3ac + 6ab + a^3) + q(4ac + 2ab) + 3rac)x^5 \end{aligned}$$

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

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

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

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

Combining equations (18) and (20) together gives

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

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

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

$$K = vb^2 \quad (22)$$

$$L^2 = wb^5, \quad (23)$$

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

$$v^3 - v^2 - v + 1 + w^2 + vw - 2w = 0. \quad (24)$$

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^2.

$$f(1 + p + q + r + t) = (4 + 3p + 2q + r)a \quad (25)$$

$$b^4(4 + 3p + 2q + r)/fL = 12b + 4a^2 + p(3c + 6b + a^2) + q(4c + 2b) + 3rc \quad (26)$$

$$Kab^4/L + Laf\,(4b + 6a^2 + p(c + 3b + 3a^2) + q(2c + 2b + a^2) + r(3c + b) + 4tc)/(4 + 3p + 2q + r) = fab^3. \quad (27)$$

$$La = (b^2 - K)(4b + 6a^2 + p(c + 3b + 3a^2) + q(2c + 2b + a^2) + r(3c + b) + 4tc)/(4 + 3p + 2q + r), \quad (28)$$

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

$$K^5/L^4 = v^5/w^2 \quad (29)$$

it can be seen that the problem of determining b depends on determining K and L in terms of v and w. Thus we might 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. If we look at the form of equation (24) expressed instead as a general elliptic curve

$$w^2 - p(av^3 + bv^2 + cv + d) = 0, \quad (30)$$

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

$$w^2 - q(av^3 + bv^2 + cv + d) = 0, \quad (31)$$

is a solvable cubic.

However, a judicious choice of a in equation (7) which we have not so far used, resolves our problem of the solution of the quintic. Equation (7) involves f, which we have solved in (20). Combining these

$$\frac{(L^2 - b^5 + Kb^3)}{b^4}\left[\frac{-Kb^2 + K^2}{L}\right] = b^4L\frac{4 + 3p + 2q + r}{1 + p + q + r + t}(a). \quad (32)$$

Put

$$a = \frac{(1 + p + q + r + t)}{L(4 + 3p + 2q + r)}(Kb^3 - (K + K^2)b), \quad (33)$$

then provided K is not zero

$$K^2b^3 - L^2b^2 + KL^2 = 0, \quad (34)$$

which provides b as a function b(K, L) of K and L. Equations (7) to (10) now step up the degree in p, q, r and t from one to four. Equation (33) can be used to eliminate t. We have f, g and h as functions f(K, L), g(K, L) and h(K, L) respectively given by equation (20) in which b(K, L) is substituted.

Then (7) can be used to express

(1 + p + q + r + t) as (4 + 3p + 2q + r)a/f(K, L)

and this value, which is an expression in a that is linear in p, q and r can be substituted in (8), (9) and (10). Since b = c = b(K, L) and we know t is linear in p, q and r from (33), equation (8) can be used to determine r as a function linear in p and q and quadratic in a.

Then equations (8), (9) and (10) can be used to eliminate a^2 and a terms in q, leaving us able to express one of these equations, say (9) as a quartic equation in a with coefficients functions of K and L. This solves for a, and hence p, q, r and t are determined as functions of K and L. This solves (1) as the solution to (4), which is a solvable variety. □

9.12. Investigating a comparison method for the quintic using a nonic.