CHAPTER XI

Solvability of complex varieties

11.1. Introduction.

We introduce the theory of complex varieties – complex polynomial equations in more than one variable, with a discussion of standard theory, first in the case of polynomials in two variables. We introduce new solutions of the quadratic equation from this point of view. Since we have shown Galois theory for group automorphisms does not extend to ring automorphisms, we develop a theory of polynomial equations naturally embedded within the theory of varieties, containing Galois end results in the special case of ‘killing central terms’ by linear transformations but outside of its framework.

We investigate algorithms for the solution of polynomial equations both by radicals (this is the descending unsolvability theorem obtained as an extension of the killing central terms theorem) and we investigate a solution of the sextic in radicals by comparison methods, also in [Ad18], and the polynomial equations by the convergent matrix eigenvalue QR algorithm, which provides an algorithm for real solutions, which we extend to the complex case.

There is an interesting feature of the solutions we are presenting in this chapter, namely that classical solutions of polynomial equations of degree n have only at most n! representable solutions, a maximum n of which are different, but we find some polynomial solutions are valid over a spectrum determined by a complex variable, and again at most n are different.

11.2. Sylvester’s law of inertia. [BM69]

Conic sections are described by quadratic forms in two variables

$$ax^2 + bxy + cy^2, \tag{1}$$

where a process similar to “completing the square” of a quadratic equation reduces (1) to

$$a(x + (b/2a)y)^2 + (c – (b^2/4a))y^2,$$

so that in new variables

$$a'x'^2 + c'y'^2$$

and the middle term in (1) has been eliminated. If $a = 0$ and $c \neq 0$ a similar method works. Finally, if also $c = 0$ then $bxy = 1$ represents a hyperbola given by

$$b(x'' + y'')(x'' – y'') = b(x''^2 – y''^2). \ \square$$

Theorem 11.2.1. *Any nonzero quadratic form* $\sum x_j a_{jk} x_k$ *can be converted to one with leading coefficient* $a_{11} \neq 0$ *by a nonsingular linear transformation, and to the diagonal quadratic form*

$$d_{11}z_1^2 + d_{22}z_2^2 + ... + d_{nn}z_n^2, \tag{2}$$

where each $d_{jj} \neq 0$.

Proof. We assume numbers are not contained within a finite field. Since at least one $a_{jk} \neq 0$, if necessary promote this to being the first. Choose the first three terms as in (1), so the method above applies, where the inverse transformations $x' \to x$, $y' \to y$ and $x'' \to x$, $y'' \to y$ exist so that the transformation is nonsingular.

To complete the square of any quadratic form, we write it as $a_{11}\sum x_j b_{jk} x_k$, where $b_{11} = 1$. For a quadratic form, the matrix b_{jk} is symmetric: $b_{jk} = b_{kj}$. Because of the symmetry of b_{jk}, terms in x_1 are

$$x_1^{\,2} + 2\sum_{k=2}^{n} x_1 b_{1k} x_k$$
$$= (x_1 + \sum_{k=2}^{n} b_{1k} x_k)^2 - (\sum_{k=2}^{n} b_{1k} x_k)^2,$$
so if we set
$$z_1 = x_1 + \sum_{k=2}^{n} b_{1k} x_k$$
and
$$z_2 = x_2, \ldots z_n = x_n,$$
then z_1 will appear in (2) as $z_1^{\,2}$, and
$$-(\sum_{k=2}^{n} b_{1k} x_k)^2 + \sum_{j,k=2}^{n} x_{j1} b_{jk} x_k$$
is a quadratic form in (n – 1) variables, so we can complete the induction by applying these types of substitution to the remaining (n – 1) cases. ☐

We see in the new basis that the d_{jj} are eigenvalues, λ, of the symmetric matrix $D = d_{jk}$, given by $(d_{11} - \lambda)(d_{22} - \lambda) \ldots (d_{nn} - \lambda) = 0$. Hence, by chapter II, section 11, they are described by a similarity transformation PAP^{-1} of the matrix $A = a_{jk}$.

A matrix P is called orthogonal when $PP^T = I$. Thus for an orthogonal matrix $P^T = P^{-1}$. The basis d_{jk} is orthogonal in the case $d_{jj} = \pm 1$, with $d_{jk} = 0$, $j \neq k$, found under the transformation $z_j \to z_j\sqrt{(\pm d_{jj})}$ with z_j real and $\sqrt{(\pm d_{jj})}$ positive. The number of positive values of these d_{jj} is called the signature of a real quadratic form, and is an invariant of it, since if it were not, there would be two common values d_{jj} and d'_{jj} describing the same eigenvalue with opposite signs, which cannot be obtained by a similarity transformation. ☐

11.3. The complex quadratic as a variety.

Let R be a ring that is commutative unless we say otherwise and R[x] represent the ring with polynomials in a single variable x with coefficients from R. The ring of polynomials R[y, z] can be thought of as a ring of polynomials in a single variable x under the linear substitution
$$y = x + a$$
$$z = x + b.$$

If the quadratic equation
$$Kx^2 + Lx + M = 0, \qquad (1)$$
corresponds to the equation
$$p(x + a)^2 + q(x + a)(x + b) + r(x + b)^2 = 0, \qquad (2)$$
the solution of (2) is
$$(x + a) = \frac{-q \pm \sqrt{q^2 - 4rp}}{2p}(x + b). \qquad (3)$$
But (2) is of the form
$$(p + q + r)x^2 + (2ap + (a + b)q + 2br)x + pa^2 + qab + rb^2 = 0, \qquad (4)$$
so if this is compared with (1) then
$$K = p + q + r, \qquad (5)$$
$$L = 2ap + (a + b)q + 2br, \qquad (6)$$
$$M = pa^2 + qab + rb^2. \qquad (7)$$

On eliminating r
$$L = 2ap + (a + b)q + 2b(K - p - q),$$
$$L = 2ap + aq + b(2K - 2p - q), \qquad (8)$$
$$M = pa^2 + qab + (K - p - q)b^2. \qquad (9)$$

Now eliminate p
$$L - aq + b(q - 2K) = 2(a - b)p \qquad (10)$$

so

$$M = \frac{[L - aq + b(q - 2K)](a^2 - b^2)}{2(a - b)} + abq + (K - q)b^2. \qquad (11)$$

This gives

$$M - \frac{[L + b(-2K)](a + b)}{2} - Kb^2 = \frac{(b^2 - a^2)q}{2} + abq + qb^2 = (a + b)\left(\frac{b - a}{2} + b\right)q,$$

$$q = \frac{(L - 2bK)}{(3b - a)} + \frac{2(M - Kb^2)}{(a + b)(3b - a)}, \qquad (12)$$

and hence from (10) we obtain p, and then from (5), r. Thus the general solution for the quadratic for arbitrary a and b is obtained, provided $a \neq \pm b$ and $3b \neq a$. □

11.4. The complex cubic as a variety.

Let

$$Hx^3 + Jx^2 + Kx + L = 0 \qquad (1)$$

correspond to the equation

$$m(x + a)^3 + n(x + a)^2(x + b) + p(x + a)(x + b)^2 + q(x + b)^3 = 0, \qquad (2)$$

where (2) can be expanded out as

$$\begin{aligned}&(m + n + p + q)x^3 + (3am + (2a + b)n + (a + 2b)p + 3bq)x^2\\ &\quad + (3a^2m + (a^2 + 2ab)n + (2ab + b^2)p + 3b^2q)x\\ &\quad + a^3m + a^2bn + ab^2p + b^3q = 0, \qquad (3)\end{aligned}$$

so if this is compared with (1) then

$$H = m + n + p + q, \qquad (4)$$
$$J = 3am + (2a + b)n + (a + 2b)p + 3bq, \qquad (5)$$
$$K = 3a^2m + (a^2 + 2ab)n + (2ab + b^2)p + 3b^2q, \qquad (6)$$
$$L = a^3m + a^2bn + ab^2p + b^3q. \qquad (7)$$

By section 4 of chapter VIII, if we zeroise n, then since

$$(x + a)^3 + \left(\frac{p}{m}\right)(x + a)(x + b)^2 + \left(\frac{q}{m}\right)(x + b)^3 = 0, \qquad (8)$$

the solution of (2) is

$$(x + a) = -(B + C)(x + b),\ -(\omega B + \omega^2C)(x + b) \text{ or } -(\omega^2B + \omega C)(x + b),$$

where

$$B = \left[\frac{q}{m}\left(1 \pm \sqrt{1 + \frac{4p^3}{27mq^2}}\right)\right]^{1/3}$$

and

$$C = \left[\frac{q}{m}\left(1 \mp \sqrt{1 + \frac{4p^3}{27mq^2}}\right)\right]^{1/3}.$$

If we now eliminate q, then on setting n = 0

$$q = H - m - p, \qquad (9)$$
$$J = 3(a - b)am + (a - b)p + 3bH, \qquad (10)$$
$$K = 3(a^2 - b^2)m + 2b(a - b)p + 3b^2H, \qquad (11)$$
$$L = (a^3 - b^3)m + b^2(a - b) + b^3H. \qquad (12)$$

Similarly, on eliminating p:

$$J = (a - b)[3m + p] + 3bH,$$

$$p = \frac{J - 3bH}{(a - b)} - 3m, \qquad (13)$$

$$K = (a - b)[3(a - b)m] + 2b(J - 3bH) + 3b^2H, \qquad (14)$$

$$L = (a - b)^2[(a + b)m] + b^2(J - 3bH) + b^3H. \tag{15}$$

Thus both

$$m = \frac{K - 2b(J - 3bH) - 3b^2H}{3(a - b)}, \tag{16}$$

and

$$m = \frac{L - b^2(J - 3bH) - b^3H}{(a - b)^2(a + b)}. \tag{17}$$

Hence

$$(K - 2b(J - 3bH) - 3b^2H)(a^2 - b^2) = 3(L - b^2(J - 3bH) - b^3H), \tag{18}$$

and so

$$a^2 = \frac{3(L - b^2(J - 3bH) - b^3H)}{(K - 2b(J - 3bH) - 3b^2H)} + b^2, \tag{19}$$

and we have solved (1) by a more general formula than the usual.

11.5. Constraints on polynomial solutions by killing terms.

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. See exercise F for polynomial substitutions.

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 11.5.1. *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' ≤ 4.

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

$$y^2 + ayz + bz^2 = 0. \tag{1}$$

If we make the substitutions

$$y = sx' + u, \tag{2}$$

$$z = tx' + v, \tag{3}$$

then under the further linear substitution

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

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

$$y'^3 + a'y'^2z' + b'y'z'^2 + c'z'^3 = 0. \qquad (9)$$

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

$$(1 + a + b + c)x^3 + [3p + a(2p + q) + 2b(p + 2q) + 3cq]x^2$$
$$+ [3p^2 +a(2pq + p^2) + b(2pq + q^2) + 3cq^2]x$$
$$+ [p^3 +ap^2q + bpq^2 + cq^3] = 0. \qquad (10)$$

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

$$y^4 + ay^3z + by^2z^2 + cyz^3 + dz^4 = 0. \qquad (11)$$

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

$$x^4 + ex^2 + f = 0, \qquad (12)$$

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

Now consider the quintic variety

$$y^5 + ay^4z + by^3z^2 + cy^2z^3 + dyz^4 + ez^5 = 0. \qquad (13)$$

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

$$y^6 + ay^5z + by^4z^2 + cy^3z^3 + dy^2z^4 + eyz^5 + fz^6 = 0, \qquad (14)$$

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 11.5.2. *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

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

where

$$u = x + r,$$
$$v = x + t,$$
$$y = x + p,$$
$$z = x + q. \quad (16)$$

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

$$v = jy + kz, \quad (17)$$
$$x + t = (j + k)x + (jp + kq), \quad (18)$$

so

$$j + k = 1,$$
$$jp + kq = jp + (1 – j)q = t = j(p – q) + q,$$

and

$$j = (t – q)/(p – q) \quad (19)$$

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

Proof. Let

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

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. □

11.6. The descending unsolvability theorem.

We have seen in exercise 10.14(B) 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 11.6.1. *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 11.6.2. *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. $\square$

Lemma 11.6.3. *Let*

$$(x + p + ia)^n + a_{n-1}(x + p + ia)^{n-1}(x + q + i'b) + ... + a_0(x + q + i'b)^n = 0. \quad (5)$$

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

$$p + ia \to p$$
$$q + ib \to q. \quad (6)$$

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}

$$np + a_{n-1}((n - 1)p + q) + ... + a_0 q = c \quad (7)$$

for some c and

$$na + a_{n-1}((n - 1)a + b) + ... + na_0 b = 0. \quad (8)$$

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

$$na + a_{n-1}((n - 1)a - b) + ... - na_0 b = 0. \quad (9)$$

Thus (8) and (9) constrain the coefficients $a_{n-1}, ... a_0$, but add no further information. $\square$

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

$$x \to px + q, \quad (10)$$

where we have seen in exercise 11.11(A) that if

$$y = x^n + a_{n-1}x^{n-1} + ... + a_0, \quad (11)$$

and the zeros of y are solvable, then on putting

$$y = w + g, \quad (12)$$
$$x = w + h, \quad (13)$$

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

We have also seen in lemma 11.6.4 that for a ring automorphism acting on symbols a and b, so that

$$a + ib \rightarrow a - ib, \qquad (14)$$

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 11.6.4. *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. ☐

11.7. Solvable representability of varieties.

We will investigate in this section solvable representations of varieties, and will find some bounds on solutions in general when multiplicative varieties of two types, those similar to equation (2) and those similar to equation (4), are reconstructed from varieties in additive form, given by example type (3). As in the case of polynomial equations in one variable, these are solvability results which are independent of the variables and are results on algorithms, and not existence statements. For the case of polynomial equations we have already shown in chapter VII that these solutions exist, even when having now proved that there is no descending algorithm for their solution by radicals for degree > 4.

We will take the case of the solvable cubic variety entity

$$(x'^3 - a^3)(y'^2 - b^2)(z' - c) = 0,$$

which is determinable from its additive form

$$x'^3y'^2z' - cx'^3y'^2 - b^2x'^3z' + (-a^3y'^2z' + b^2cx'^3) + a^3cy'^2 + a^3b^2z' - a^3b^2c = 0. \qquad (1)$$

We can solve this when

$$x' = p_1x + q_1y + r_1z,$$
$$y' = p_2x + q_2y + r_2z,$$
$$z' = p_3x + q_3y + r_3z,$$

by starting from the rightmost term of equation (1) and working to the front. This is because z' and y'^2 are detectable, and therefore their coefficients. Hence for the last three terms a^3c, a^3b^2 and $-a^3b^2c$ can be found, and so a^3, b^2 and c. This means $(-a^3y'^2z' + b^2cx'^3)$ can be obtained, from which x'^3 can also be found.

Within this solvable variety entity is embedded the variety

$$(p_1x + q_1y + r_1z - a)(p_2x + q_2y + r_2z - b)(p_3x + q_3y + r_3z - c) = 0. \qquad (2)$$

A general variety of the third degree in additive format

$$ax^3 + by^3 + cz^3 + dx^2y + exy^2 + fx^2z + gxz^2 + hy^2z + jyz^2 + kxyz$$
$$+ mx^2 + ny^2 + pz^2 + qxy + rxz + syz$$
$$+ tx + uy + vz + w = 0, \qquad (3)$$

has 20 coefficients, whereas equation (2) has 12. However, we can substitute for x in (3) the sum of four variables, x'', y'', z'' and a constant, and similarly for y and z. This modifies (3) by the introduction of 12 new variables, so 20 coefficients minus 12 new variables is less than the number of variables in (2) now represented by x'', y'', z'' and constants.

Further, a variety in the format

$$(p_1x + q_1y + r_1z - a)(p_2x + q_2y + r_2z - b)(p_3x + q_3y + r_3z - c) =$$
$$(p_1'x + q_1'y + r_1'z - a')(p_2'x + q_2'y + r_2'z - b')(p_3'x + q_3'y + r_3'z - c'), \qquad (4)$$

which has 24 coefficients, can directly represent (3). Indeed, we can pick solutions of (4). For each factor on the left, equate this to a factor on the right. This gives six sets of three linear equations, but these solutions are not the most general. These solutions can be generalised, so that we can select, say,

$$(p_1x + q_1y + r_1z - a) = D(p_1'x + q_1'y + r_1'z - a')$$
$$(p_2x + q_2y + r_2z - b) = E(p_2'x + q_2'y + r_2'z - b')$$
$$DE(p_3x + q_3y + r_3z - c) = (p_3'x + q_3'y + r_3'z - c'), \qquad (5)$$

for arbitrary D and E. These are simultaneous solutions with two degrees of freedom given by D and E for fixed p_k, p'_k, q_k, q'_k, r_k, r'_k, a, a′, b, b′, c and c′.

A variety of degree n with k variables x_1, x_2, ... x_k in multiplicative format (2) has (k + 1)n coefficients and in format (4) has 2(k + 1)n coefficients.

If we look at the number of coefficients in additive format (3), on putting k = 3, n = 3, these coefficients exist for variables

x^3 y^3 z^3	for k items, in one variable
x^2y xy^2	for (n – 1)k(k – 1)/2 items, in paired variables
x^2z xz^2	
y^2z yz^2	
xyz	for (n – 2)k(k – 1)(k – 2)/3! items, in triple variables
x^2 y^2 z^2	for k items, in one variable
xy	for (n – 2)k(k – 1)/2 items, in paired variables
xz	
yz	
x y z	for k items, in one variable
1	a coefficient in no variables.

The general expression for the number of coefficients in additive format is

$$M = 1 + nk + \sum_{t=1}^{n-1}\sum_{r=1}^{t}\frac{k(k-1)\cdots(k-r)}{r!}(n-t), \qquad (6)$$
$$= 1 + nk + \Sigma\Sigma.$$

If, as for example equation (3), we substitute for each of k variables the sums of k other variables and a constant, this modifies k(k + 1) variables in the corresponding equation. We therefore see that for k = 5 and degree n = 3, the number of coefficients in multiplicative format given by example equation (2) can become at most

$$(k + 1)n < M – k(k + 1),$$
and in the explicit case considered
$$18 < 1 + 15 + 20 + 10 + 10 – 30 = 26,$$
so there is no solution in multiplicative format (2) from additive format by these means. ☐

We now wish to show that also in multiplicative format (4), if
$$2(k + 1)n > M – k(k + 1),$$
that is, if there were a solution in multiplicative format (4) from additive format by these means, that this is a contradiction. Then we would have
$$k^2 + k(n + 1) + 2n – 1 > \Sigma\Sigma,$$
which up to t = 3 gives a selected term
$$k^2 + k(n + 1) + 2n – 1 > k(k – 1)(k – 3)(n – 3)/6,$$
or
$$(k^3 – 4k^2 + 3k)(n – 3) < 6[k^2 + k(n + 1) + 2n – 1].$$
But it is obvious, given the k^3 term, that this is violated for sufficiently high k and n > 3. ☐

11.8. Bring-Jerrard form. [Stack exchange], [Ki96]

As was proved separately by Bring and Jerrard, the general quintic equation may be put in the Bring-Jerrard form
$$y^5 + My + N = 0, \tag{1}$$
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
$$w^5 + w + G = 0. \tag{2}$$

Theorem 11.8.1. *Every complex polynomial of the* n*th degree can be reduced by a determinate linear transformation so that the coefficient of either degree* (n – 1) *or* 1 *is zero.*

Proof. Let
$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0. \tag{3}$$
Then by the substitution
$$x = y + p$$
using the binomial expansion of $(y + p)^n$, the coefficient of y^{n-1} is $(np + a_{n-1})$. Thus this coefficient may be set to zero if
$$p = -\frac{a_{n-1}}{n}. \tag{4}$$
Then this polynomial becomes
$$y^n + a'_{n-1}y^{n-1} + ... + a'_1y + a'_0 = 0. \tag{5}$$
Put
$$y = \frac{1}{z}. \tag{6}$$
Multiply by $\left(\frac{z^n}{a'_0}\right)$, which is the required form with the coefficient of degree 1 set to zero. ☐

The techniques to put a polynomial in this form can be extended to a general polynomial of degree n in a form in which the y^{n-1}, y^{n-2} and y^{n-3} coefficients are zero, or our preferred form in which the y^{n-2}, y^{n-3} and y^{n-4} coefficients are zero.

To reduce the general quintic
$$y^5 + Ay^4 + By^3 + Cy^2 + Dy + E = 0 \tag{7}$$
to reduced Bring-Jerrard form, we will transform (3) to principal quintic form, which zeroises

the coefficients of the y^4 and y^3 terms, using a quadratic Tschirnhaus transformation

$$-z + y^2 + my + n = 0 \tag{8}$$

and eliminate y between (7) and (8) using the resultants of chapter X section 7, so that (7) and (8) have duplicate roots and we can calculate from their zero Sylvester determinant a z with

$$z^5 + c_1z^4 + c_2z^3 + c_3z^2 + c_4z + c_5 = 0. \tag{9}$$

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 (7) becomes the principal quintic form

$$z^5 + Uz^2 + Vz + W = 0. \tag{10}$$

Remark 11.8.2. To transform this to reduced 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

$$v = z^4 + Pz^3 + Qz^2 + Rz + T, \tag{11}$$

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

$$v^5 + d_1v^4 + d_2v^3 + d_3v^2 + d_4v + d_5 = 0, \tag{12}$$

where

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

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

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

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

$$3QU + 4PV + 5W = 0 \tag{13}$$

$$d_1 = d_2 = 0. \tag{14}$$

Because the third term of (8) has the form

$$d_3 = e_3R^3 + e_2R^2 + e_1R + e_0, \tag{15}$$

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.

Equation (15) is now in Bring-Jerrard form (1), which we have seen can be transformed to reduced Bring-Jerrard form (2). □

If we could find a solution of the quintic, and inductively higher order polynomial equations, then this method could be usefully extended.

For instance, as a variation on a theme, we will present a method for a reduction of a general septic to a form in which two of the coefficients are set to zero, which we have just used for the quintic using resultants.

Let

$$t^7 + j_6t^6 + j_5t^5 + j_4t^4 + j_3t^3 + j_2t^2 + j_1t + j_0 = 0 \quad (16)$$

if and only if there is a solution to

$$t^7 + j_6t^6u + j_5t^5u^2 + j_4t^4u^3 + j_3t^3u^4 + j_2t^2u^5 + j_1tu^6 + j_0u^7 = 0. \quad (17)$$

Now set

$$u = t + v. \quad (18)$$

Then we have an equation

$$t^7 + j'_6t^6 + j'_5t^5 + j'_4t^4 + j'_3t^3 + j'_2t^2 + j'_1t + j'_0 = 0. \quad (19)$$

Setting

$$t = 1/w \quad (20)$$

we get

$$w^7 + j''_6w^6 + j''_5w^5 + j''_4w^4 + j''_3w^3 + j''_2w^2 + j''_1w + j''_0 = 0. \quad (21)$$

Making a substitution

$$w = y + z \quad (22)$$

gives

$$y^7 + j'''_6y^6 + j'''_5y^5 + j'''_4y^4 + j'''_3y^3 + j'''_2y^2 + j'''_1y + j'''_0 = 0. \quad (23)$$

We now have enough solvable degrees of freedom in v and z to set simultaneously

$$j'''_2 = 0, j'''_3 = 0. \quad (24)$$

Then this is the form of the equation we could use to further develop the theory in which we have obtained three coefficients equal to zero. □

11.9. Comparison method examples for the quintic and cubic equations.

We give an indication of why a general polynomial equation of the fifth degree is unsolvable by some descending comparison methods, using the method of transforming this polynomial in a variable y in Bring-Jerrard form to a polynomial in the variable $x = y^{-1}$, appending bogus roots and comparing this with a polynomial in direct format. For now we are unable to supply an explicit solution of the quintic polynomial equation using this ‘reciprocal Bring-Jerrard comparison’ method, which is the same result as is obtained by ‘killing central terms’. By the Schreier replacement theorem of Galois theory, the solution of the quintic would be impossible via an octic. The example we use is dependent on the coefficient term of the fourth degree being present.

It is first of all instructive to look at comparison methods which reduce to a sextic. We will invert the Bring-Jerrard equation in form 11.8.(1) under the substitution

$$y = 1/x \quad (1)$$

to put it in reciprocal Bring-Jerrard form

$$x^5 + Kx^4 + L = 0. \quad (2)$$

This means we have divided out the coefficient of x^5. We adjoin a root to (2) to form

$$(x^5 + Kx^4 + L)(x + m) = x^6 + (K + m)x^5 + Kmx^4 + Lx + Lm = 0, \quad (3)$$

and compare this with the cubic polynomial equation

$$(x^2 + px + q)^3 + a(x^2 + px + q)^2 + b(x^2 + px + q) + c = 0, \quad (4)$$

which is solvable, since from the definition of a function, the polynomial of a polynomial is a polynomial, and by chapter VIII, section 4, the cubic of a solvable function is solvable.

Then equation (4) becomes

$$x^6 + 3(px + q)x^4 + 3(px + q)^2x^2 + (px + q)^3$$
$$+ a(x^4 + 2(px + q)x^2 + (px + q)^2) + b(x^2 + (px + q)) + c = 0,$$

or expanded out

$$x^6 + 3px^5 + 3qx^4 + 3p^2x^4 + 6pqx^3 + 3q^2x^2 + p^3x^3 + 3p^2qx^2 + 3pq^2x + q^3$$
$$+ a(x^4 + 2px^3 + 2qx^2 + p^2x^2 + 2pqx + q^2)$$
$$+ b(x^2 + px + q) + c = 0,$$

giving

$$x^6 + 3px^5 + [3q + 3p^2 + a]x^4 + [6pq + p^3 + 2ap]x^3$$
$$+ [3q^2 + 3p^2q + a(2q + p^2) + b]x^2 + [3pq^2 + 2apq + bp]x$$
$$+ q^3 + aq^2 + bq + c = 0. \quad (5)$$

By a result of chapter VII, section 7, complex polynomials are uniquely expressed, so we can compare the coefficients of (3) and (5) to obtain

$$K + m = 3p \quad (6)$$
$$Km = 3q + 3p^2 + a \quad (7)$$
$$0 = 6pq + p^3 + 2ap \quad (8)$$
$$0 = 3q^2 + 3p^2q + a(2q + p^2) + b \quad (9)$$
$$L = 3pq^2 + 2apq + bp \quad (10)$$
$$Lm = q^3 + aq^2 + bq + c. \quad (11)$$

In equation (8), since $p \neq 0$, we can divide by it to get

$$0 = 6q + p^2 + 2a, \quad (12)$$

so that

$$a = -3q - (p^2/2). \quad (13)$$

We will substitute (13) in the remaining (7) to (11)

$$Km = 3q + 3p^2 - 3q - (p^2/2) = 5p^2/2. \quad (14)$$
$$0 = 3q^2 + 3p^2q - [3q + (p^2/2)](2q + p^2) + b$$
$$0 = -3q^2 - p^2q - (p^4/2) + b. \quad (15)$$
$$L = 3pq^2 - 2[3q + (p^2/2)]pq + bp$$
$$L = -3pq^2 - p^3q + bp \quad (16)$$
$$Lm = q^3 - [3q + (p^2/2)]q^2 + bq + c$$
$$Lm = -2q^3 - (p^2q^2/2) + bq + c. \quad (17)$$

We now use (6) to eliminate m

$$m = 3p - K. \quad (18)$$

Equation (14) becomes

$$(3p - K)K = 5p^2/2$$
$$5p^2 - 6Kp + 2K^2 = 0 \quad (19)$$

and by the standard solution of a quadratic equation

$$p = \frac{6 \pm \sqrt{36 - 40}}{10}K = \frac{3 \pm i}{5}K, \quad (20)$$

which we will abbreviate to

$$p = \gamma K. \quad (21)$$

Using (21) equation (15) is

$$0 = 6q^2 + 2\gamma^2K^2q + \gamma^4K^4 - 2b, \quad (22)$$

and inserting this value of b in (16) gives

$$L = -3\gamma Kq^2 - (\gamma K)^3q + (3q^2 + \gamma^2K^2q + \gamma^4K^4/2)\gamma K$$
$$\gamma^5K^5 = 2L, \quad (23)$$

so there appears to be no general solution of the quintic by this method. □

We will now extend the discussion, retain (2) and append the cubic

$$x^3 + m_1x^2 + m_2x + m_3 = 0, \tag{24}$$

to get

$$(x^5 + Kx^4 + L)(x^3 + m_1x^2 + m_2x + m_3) = 0,$$

which on expanding out is the octic polynomial equation

$$\begin{aligned} &x^8 + (K + m_1)x^7 + (Km_1 + m_2)x^6 + (Km_2 + m_3)x^5 + Km_3x^4 \\ &\qquad + Lx^3 + Lm_1x^2 + Lm_2x + Lm_3 = 0. \end{aligned} \tag{25}$$

We now compare this with the solvable octic

$$(x^2 + px + q)^4 + a(x^2 + px + q)^3 + b(x^2 + px + q)^2 + c(x^2 + px + q) + d = 0. \tag{26}$$

Equation (26) has six coefficients p, q, a, b, c and d. This octic equation leads to eight comparison equations with (25). A quintic has five coefficients, which means equation (26) may be constrained. We will delay an implementation of this. Indeed a specific constraint is strictly speaking unnecessary, and we can obtain more general equations. However, it is the case that p cannot be solved by an induction method in terms of the other coefficients, since its degree is too high, and although in the final result p may be set to a value we choose, we will find some values are too restricting. In particular, we will see that $p = 0$ and $p = 1$ are ruled out.

Then (26) becomes

$$\begin{aligned} &x^8 + 4(px + q)x^6 + 6(px + q)^2x^4 + 4(px + q)^3x^2 + (px + q)^4 \\ &\qquad + a(x^6 + 3(px + q)x^4 + 3(px + q)^2x^2 + (px + q)^3) \\ &\qquad + b(x^4 + 2(px + q)x^2 + (px + q)^2) + c(x^2 + (px + q)) + d = 0, \end{aligned}$$

or expanded out

$$\begin{aligned} &x^8 + 4px^7 + (4q + 6p^2)x^6 + (12pq + 4p^3)x^5 + (6q^2 + 12p^2q + p^4)x^4 \\ &\qquad + (12pq^2 + 4p^3q)x^3 + (4q^3 + 6p^2q^2)x^2 + 4pq^3x + q^4 \\ &\qquad + a(x^6 + 3px^5 + (3q + 3p^2)x^4 + (6pq + p^3)x^3 + (3q^2 + 3p^2q)x^2 + 3pq^2x + q^3) \\ &\qquad + b(x^4 + 2px^3 + (2q + p^2)x^2 + 2pqx + q^2) + c(x^2 + px + q) + d = 0, \end{aligned}$$

giving

$$\begin{aligned} &x^8 + 4px^7 + (4q + 6p^2 + a)x^6 + (12pq + 4p^3 + 3ap)x^5 \\ &\qquad + (6q^2 + 12p^2q + p^4 + a(3q + 3p^2) + b)x^4 \\ &\qquad + (12pq^2 + 4p^3q + a(6pq + p^3) + 2bp)x^3 \\ &\qquad + (4q^3 + 6p^2q^2 + a(3q^2 + 3p^2q) + b(2q + p^2) + c)x^2 \\ &\qquad + (4pq^3 + 3apq^2 + 2bpq + cp)x + q^4 + aq^3 + bq^2 + cq + d = 0. \end{aligned} \tag{27}$$

Thus

$$K + m_1 = 4p \tag{28}$$

$$Km_1 + m_2 = 4q + 6p^2 + a \tag{29}$$

$$Km_2 + m_3 = 12pq + 4p^3 + 3ap \tag{30}$$

$$Km_3 = 6q^2 + 12p^2q + p^4 + a(3q + 3p^2) + b \tag{31}$$

$$L = 12pq^2 + 4p^3q + a(6pq + p^3) + 2bp \tag{32}$$

$$Lm_1 = 4q^3 + 6p^2q^2 + a(3q^2 + 3p^2q) + b(2q + p^2) + c \tag{33}$$

$$Lm_2 = 4pq^3 + 3apq^2 + 2bpq + cp \tag{34}$$

$$Lm_3 = q^4 + aq^3 + bq^2 + cq + d. \tag{35}$$

From (28)

$$m_1 = 4p – K, \tag{36}$$

from (29)

$$m_2 = 4q + 6p^2 + a – K(4p – K), \tag{37}$$

from (30)

$$m_3 = 12pq + 4p^3 + 3ap – K(4q + 6p^2 + a – K(4p – K)), \quad (38)$$

from (31)

$$K[12pq + 4p^3 + 3ap – K(4q + 6p^2 + a – K(4p – K))] =$$
$$6q^2 + 12p^2q + p^4 + a(3q + 3p^2) + b, \quad (39)$$

from (33)

$$L(4p – K) = 4q^3 + 6p^2q^2 + a(3q^2 + 3p^2q) + b(2q + p^2) + c, \quad (40)$$

from (34)

$$L(4q + 6p^2 + a – K(4p – K)) = 4pq^3 + 3apq^2 + 2bpq + cp, \quad (41)$$

and from (35)

$$L[12pq + 4p^3 + 3ap – K(4q + 6p^2 + a – K(4p – K))] = q^4 + aq^3 + bq^2 + cq + d. \quad (42)$$

We now have equations (32), (39), (40), (41) and (42) with m_1, m_2 and m_3 eliminated.

Equation (42) determines d. We will begin by eliminating c from (40) in (41). This gives

$$L(4q + 6p^2 + a – K(4p – K)) = 4pq^3 + 3apq^2 + 2bpq +$$
$$+ [L(4p – K) – 4q^3 – 6p^2q^2 – a(3q^2 + 3p^2q) – b(2q + p^2)]p,$$
$$6p^3q^2 + (4L + 3ap^3)q + (6p^2 + a – (K + p)(4p – K))L + bp^3 = 0. \quad (43)$$

The equations in b excluding (42) are now (32), (39) and (43). Equation (32) becomes

$$bp = ½[L – 12pq^2 – 4p^3q – a(6pq + p^3)],$$

and substituted in (39) this gives

$$K[12pq + 4p^3 + 3ap – K(4q + 6p^2 + a – K(4p – K))] = 6q^2 + 12p^2q + p^4 + a(3q + 3p^2)$$
$$+ ½[(L/p) – 12q^2 – 4p^2q – a(6q + p^2)],$$

or

$$K[12pq + 4p^3 + 3ap – K(4q + 6p^2 + a – K(4p – K))] =$$
$$10p^2q + p^4 + ½(5ap^2) + (L/2p), \quad (44)$$

whereas (32) substituted in (43) gives

$$6p^3q^2 + (4L + 3ap^3)q + (6p^2 + a – (K + p)(4p – K))L$$
$$+ ½[L – 12pq^2 – 4p^3q – a(6pq + p^3)]p^2 = 0,$$

or

$$(4L – 2p^5)q + ½(13p^2 + (p – K)(4p – K))L + a(L – ½p^5) = 0. \quad (45)$$

Using (44) and (45) we can now eliminate a. (44) gives

$$(K^2 – 3Kp + 5p^2/2)a =$$
$$K[12pq + 4p^3 – K(4q + 6p^2 – K(4p – K))] – 10p^2q – p^4 – (L/2p). \quad (46)$$

Therefore (45) becomes

$$(K^2 – 3K + 5p^2/2)(4L – 2p^5)q + (L – ½p^5)(12Kpq – 4K^2q – 10p^2q) +$$
$$(K^2 – 3K + 5p^2/2)(13p^2/2 – (p + K)(4p – K))L$$
$$+ (L – ½p^5)\{K[4p^3 – K(6p^2 – K(4p – K))] – p^4 – (L/2p)\} = 0, \quad (47)$$

thus on collecting the terms in q, these are

$$[4LK^2 – 2p^5K^2 – 12KLp + 6Kp^6 + 10Lp^2 – 5p^7$$
$$12KLp – 4K^2L – 10p^2L – 6Kp^6 + 2K^2p^5 + 5p^7]q, \quad (48)$$

which is zero. This means dependencies are determined by p and not q, and inductively the degree is too high to solve for them. □

Our theories have deconstructed Galois solvability theory, where for a solution of the quintic equation, 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 have now explored 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, but we were not able to be effective in solving the quintic by such techniques.

What will now happen is that we are able to extend the comparison equation essentially to a nested variety, and this will allow us to express a cubic equation with 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

$$x^3 + Kx + L = 0 \tag{49}$$

is solvable by only using square roots. The method does not involve 'killing central terms' but uses a type of comparison method. We call this method *extended comparison*, because the comparison equations like (51) or (73) are written not in the form of a polynomial, but a variety with two variables. We chose two methods. As we will see, the first method has to be modified to yield a solution.

Let

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

so

$$x^4 + mx^3 + Kx^2 + (Km + L)x + Lm = 0. \tag{50}$$

Now consider the extended comparison equation

$$(x^2 + ax + b)^2 + p(x^2 + ax + b)(x + c) + q(x + c)^2 = 0, \tag{51}$$

which can be expressed as the solvable quadratic equation

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

with

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

with solution

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

giving

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

which using

$$A = a + \frac{p \mp\sqrt{p^2 - 4q}}{2} \tag{52}$$

$$B = b + \frac{p \mp\sqrt{p^2 - 4q}}{2} \tag{53}$$

has solution

$$x = \frac{-A \mp\sqrt{A^2 - 4B}}{2}. \tag{54}$$

Expanded out, equation (51) is

$$x^4 + (2a + p)x^3 + (2b + a^2 + pc + ap + q)x^2 + (2ab + pac + pb + 2qc)x$$
$$+ b^2 + pbc + qc^2 = 0, \tag{55}$$

so that on comparing (50) and (55) the equated coefficients satisfy

$$m = 2a + p \tag{56}$$

$$K = 2b + a^2 + pc + ap + q \tag{57}$$
$$Km + L = 2ab + pac + pb + 2qc$$
$$Lm = b^2 + pbc + qc^2,$$
and on eliminating m from (56)
$$K(2a + p) + L = 2ab + pac + pb + 2qc \tag{58}$$
$$L(2a + p) = b^2 + pbc + qc^2. \tag{59}$$

If we now eliminate q from (57) in (58) and (59) we obtain
$$q = K - 2b - a^2 - pa - pc, \tag{60}$$
$$K(2a + p) + L = 2ab + pac + pb + 2c(K - 2b - a^2 - pa - pc) \tag{61}$$
$$L(2a + p) = b^2 + pbc + c^2(K - 2b - a^2 - pa - pc). \tag{62}$$

We could retain the value of c as an arbitrary parameter, but we will simplify these equations by putting
$$c = 1. \tag{63}$$
Then on collecting together the terms in p, equation (61) with c = 1 becomes
$$K(2a + p) + L = 2ab + pa + pb + 2(K - 2b - a^2 - pa - p) \tag{64}$$
and likewise equation (62) becomes
$$L(2a + p) = b^2 + pb + (K - 2b - a^2 - pa - p). \tag{65}$$

We will now eliminate p from these two equations
$$(L - b + a + 1)\frac{(2K + 2ab - 4b - 2a^2 - 2Ka - L)}{(K + a - b + 2)} = b^2 + (K - 2b - a^2 - 2La). \tag{66}$$

Equation (66) when expanded out gives a cubic in b and a, so in order to keep (66) as a solvable quadratic we set
$$\frac{(L - b + a + 1)}{(K + a - b + 2)} = D \tag{67}$$
where D is a number. We do not wish to have D = 1 because then L = K + 1, so that L is not independent of K, but otherwise we are free to choose any value. In order to simplify the discussion further, we will choose
$$D = 2, \tag{68}$$
but the reader could investigate the full result for arbitrary D.

Then for D = 2 equation (67) becomes
$$a = b + L - 2K - 3. \tag{69}$$
We will need the expression for a^2
$$a^2 = b^2 + 2(L - 2K - 3)b + (L - 2K - 3)^2. \tag{70}$$
When equation (67) for D = 2 holds, equation (66) is
$$4K + 4ab - 8b - 4a^2 - 4Ka - 2L = b^2 + (K - 2b - a^2) - 2La$$
or
$$b^2 + (-4a + 6)b - 3K + 3a^2 + 4Ka - 2La + 2L = 0. \tag{71}$$
Then from (69), (70) and (71) we obtain the equation to find b
$$b^2 + (-4b - 4(L - 2K - 3) + 6)b - 3K + 3(b^2 + 2(L - 2K - 3)b + (L - 2K - 3)^2$$
$$+ (4K - 2L)(b + L - 2K - 3) + 2L = 0,$$
which is the equation
$$(L - 2K - 3)(- L + 2K - 3) - 3K + 2L = 0, \tag{72}$$
an unacceptable constraint for which the parameter b is absent. ☐

We will continue to use equation (50) but now consider the extended comparison equation
$$(x^2 + ax + b)^2 + p(x^2 + ax + b)(x^2 + c) + q(x^2 + c)^2 = 0, \tag{73}$$

with solution that of

$$(x^2 + ax + b) = \left[\frac{-p \pm\sqrt{p^2 - 4q}}{2}\right](x^2 + c). \qquad (74)$$

Expanding out (73) gives

$$(1 + p + q)x^4 + (2a + pa)x^3 + (2b + a^2 + p(c + b) + 2qc)x^2$$
$$+ (2ab + pac)x + b^2 + pbc + qc^2 = 0, \qquad (75)$$

comparing with equation (50)

$$m = a(2 + p)/(1 + p + q) \qquad (76)$$
$$K(1 + p + q) = 2b + a^2 + p(c + b) + 2qc \qquad (77)$$
$$Km + L = (2ab + pac)/(1 + p + q)$$
$$Lm = (b^2 + pbc + qc^2)/(1 + p + q),$$

and on eliminating m from (76)

$$Ka(2 + p) + L(1 + p + q) = 2ab + pac \qquad (78)$$
$$La(2 + p) = b^2 + pbc + qc^2. \qquad (79)$$

We will put for convenience c = 1, giving

$$K(1 + p + q) = 2b + a^2 + p(1 + b) + 2q \qquad (80)$$
$$Ka(2 + p) + L(1 + p + q) = 2ab + pa \qquad (81)$$
$$La(2 + p) = b^2 + pb + q, \qquad (82)$$

and eliminate q from, say, (80) to give

$$q = [-K(1 + p) + 2b + a^2 + p(1 + b)]/(K - 2) \qquad (83)$$
$$Ka(2 + p) + L(1 + p) + L[-K(1 + p) + 2b + a^2 + p(1 + b)]/(K - 2) =$$
$$a(2b + p) \qquad (84)$$
$$La(2 + p) = b^2 + pb + [-K(1 + p) + 2b + a^2 + p(1 + b)]/(K - 2). \qquad (85)$$

We will use (84) and (85) to give two expressions for p.

$$\{Ka - a + L + L[-K + 1 + b]/(K - 2)\}p =$$
$$\{-2Ka - L - L[-K + 2b + a^2]/(K - 2) + 2ab\} \qquad (86)$$
$$\{La - b - [-K + (1 + b)]/(K - 2)\}p =$$
$$\{-2La + b^2 + [-K + 2b + a^2]/(K - 2)\}, \qquad (87)$$

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

$$[K - 1 - L]a = [(-L - K + 1)b + (L + K - 1)]/(K - 2) \qquad (88)$$

giving for a^2

$$[K - 1 - L]^2a^2 = (-L - K + 1)^2[b - 1]^2/(K - 2)^2 \qquad (89)$$

whereas equations (86) and (87) combine to give

$$-2Ka - L - L[-K + 2b + a^2]/(K - 2) + 2ab =$$
$$-2La + b^2 + [-K + 2b + a^2]/(K - 2),$$
$$2[-K + L + b]a - L - [L - 1][-K + 2b + a^2]/(K - 2) = b^2, \qquad (90)$$

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 (88) and a^2 in (89) into (90) gives a solvable quadratic for b, where the full equation is

$$\left[2(-L - K + 1) - \frac{(L - 1)(-L - K + 1)^2}{(K - 2)^2(K - L - 1)} - (K - 2)(K - L - 1)\right]b^2$$
$$+ 2[(-K + L)(-L - K + 1) + (L + K - 1) - (L - 1)(K - L - 1)]b$$
$$- 2\left[\frac{(L-1)(-L-K+1)^2}{(K-2)^2(K-L-1)}\right]b$$

$$+ [2(-K + L)(L + K - 1) - L(K - 2)(K - L - 1) - (L - 1)(-K)(K - L - 1)]$$
$$+ \frac{(L-1)(-L-K+1)^2}{(K-2)^2(K-L-1)} = 0. \qquad (91)$$

which allows further simplification. It then determines a in (88), thus p in (86), q in (83), m from (76) and we have set c = 1. We conclude that we can solve for x in (74), providing the solution of essentially the cubic (50). ☐

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 (49) so

$$x^3 = 2, \qquad (92)$$

then we find from (91) 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 (92) is geometrically realisable. ☐

By these means we are able to solve for x in (74), providing the solution of the cubic (49) entirely in terms of square roots. ☐

11.10. Obstructions to solutions in radicals of the sextic.

Although we have shown that there is no solution of the sextic by killing central terms, our theory of dependencies does not extend to comparison methods where the degree does not descend. Thus we have no overarching theory in this case, and the author has been reduced to looking at specific cases. Our methods do not work. The second method uses a small change in the structure of the comparison equation to try to find a solution to the sextic by radicals.

If we look at the quintic

$$x^5 + Hx^4 + Kx^3 + Lx^2 + Mx + N = 0 \qquad (1)$$

this is a special case of the general sextic equation

$$x^6 + Hx^5 + Kx^4 + Lx^3 + Mx^2 + Nx + R = 0, \qquad (2)$$

with R = 0. If we compare (2) with the solvable polynomial in six variables

$$(x^3 + ax^2 + bx + c)^2 + p(x^3 + ax^2 + bx + c)(x + d) + q(x + d)^2. \qquad (3)$$

The solution of (3) is the solution of

$$x^3 + ax^2 + bx + c = \left[\frac{-p \pm \sqrt{p^2 - 4q}}{2}\right](x + d), \qquad (4)$$

which is a solvable cubic.

Expanded out, (3) is

$$x^6 + 2(ax^2 + bx + c)x^3 + (ax^2 + bx + c)^2$$
$$+ p(x^4 + (a + d)x^3 + (b + ad)x^2 + (c + bd)x + cd)$$
$$+ q(x^2 + 2dx + d^2) = 0$$

or

$$x^6 + 2ax^5 + (2b + a^2 + p)x^4 + (2c + 2ab + p(a + d))x^3 + (b^2 + 2ac + p(b + ad) + q)x^2 + (2bc + p(c + bd) + 2qd)x + (c^2 + pcd + qd^2) = 0. \tag{5}$$

Comparing (2) and (5)

$$H = 2a \tag{6}$$
$$K = 2b + a^2 + p \tag{7}$$
$$L = 2c + 2ab + p(a + d) \tag{8}$$
$$M = b^2 + 2ac + p(b + ad) + q \tag{9}$$
$$N = 2bc + p(c + bd) + 2qd \tag{10}$$
$$R = c^2 + pcd + qd^2. \tag{11}$$

Eliminating a in (6) from (7) to (9)

$$a = \frac{H}{2} \tag{12}$$
$$K = 2b + \frac{H^2}{4} + p \tag{13}$$
$$L = 2c + Hb + p\left(\frac{H}{2} + d\right) \tag{14}$$
$$M = b^2 + Hc + p\left(b + \frac{Hd}{2}\right) + q. \tag{15}$$

Eliminating b from (13) in (14), (15) and (10)

$$b = \frac{K}{2} - \frac{H^2}{8} - \frac{p}{2} \tag{16}$$
$$L = 2c + \frac{HK}{2} - \frac{H^3}{8} - \frac{Hp}{2} + \frac{Hp}{2} + pd$$
$$c = L - \frac{HK}{2} + \frac{H^3}{16} - \frac{pd}{2} \tag{17}$$
$$M = \left(\frac{K^2}{4} + \frac{H^4}{64} + \frac{p^2}{4} - \frac{H^2K}{8} - \frac{Kp}{2} + \frac{H^2p}{8}\right) + Hc + p\left(\frac{K}{2} - \frac{H^2}{8} - \frac{p}{2} + \frac{Hd}{2}\right) + q$$

$$M = \frac{K^2}{4} + \frac{H^4}{64} - \frac{p^2}{4} - \frac{H^2K}{8} + Hc + \frac{Hdp}{2} + q$$

and using (17)

$$M = \frac{K^2}{4} + \frac{H^4}{64} - \frac{p^2}{4} - \frac{H^2K}{8} + HL - \frac{H^2K}{2} + \frac{H^4}{16} + q$$

so

$$q = M - \frac{K^2}{4} - \frac{5H^4}{64} + \frac{p^2}{4} - HL + \frac{5H^2K}{8}. \tag{18}$$
$$N = \left(K - \frac{H^2}{4} - p\right)\left(L - \frac{HK}{2} + \frac{H^3}{16} - \frac{pd}{2}\right) + p\left(L - \frac{HK}{2} + \frac{H^3}{16} - \frac{pd}{2}\right) + p\left(\frac{K}{2} - \frac{H^2}{8} - \frac{p}{2}\right)d + 2qd$$
$$N = KL - \frac{HK^2}{2} + \frac{H^3K}{16} - \frac{pdK}{2} + \frac{H^3K}{8} - \frac{H^5}{64} + \frac{H^2pd}{8} - pL + \frac{HKp}{2} - \frac{H^3p}{16} + \frac{p^2d}{2} + pL - \frac{HKp}{2} + \frac{H^3p}{16} - \frac{p^2d}{2} + \frac{Kpd}{2} - \frac{H^2pd}{8} - \frac{p^2d^2}{2} + 2Md - \frac{K^2d}{2} - \frac{5H^4d}{32} + \frac{p^2d}{2} - 2HLd + \frac{5H^2Kd}{4}$$
$$N = KL - \frac{HK^2}{2} + \frac{3H^3K}{16} - \frac{H^5}{64} + 2Md - \frac{K^2d}{2} - \frac{5H^4d}{32} - 2HLd + \frac{5H^2Kd}{4} \tag{19}$$

giving

$$d = \frac{64N - 64KL + 32HK^2 - 12H^3K + H^5}{128M - 32K^2 - 10H^4 - 128HL + 80H^2K}. \tag{20}$$

From equation (11)

$$R = \left(L - \frac{HK}{2} + \frac{H^3}{16} - \frac{pd}{2}\right)^2 + p\left(L - \frac{HK}{2} + \frac{H^3}{16} - \frac{pd}{2}\right)d$$
$$+ \left(M - \frac{K^2}{4} - \frac{5H^4}{64} + \frac{p^2}{4} - HL + \frac{5H^2K}{8}\right)d^2$$
$$R = \left(L - \frac{HK}{2} + \frac{H^3}{16}\right)^2 + \left(M - \frac{K^2}{4} - \frac{5H^4}{64} - HL + \frac{5H^2K}{8}\right)d^2. \quad (21)$$

Thus there is a constraint between R and H, K, L M and N. Basically, the variable p is not available in the solution. ☐

We now resort to 'plan B' and introduce the general sextic equation

$$x^6 + Gx^5 + Hx^4 + Kx^3 + Lx^2 + Mx + N = 0, \quad (22)$$

but our comparison equation is now modified to

$$(x^3 + ax^2 + bx + c)^2 + p(x^3 + ax^2 + bx + c)(x^2 + d) + q(x^2 + d)^2. \quad (23)$$

The solution of (23) this time is the solution of

$$x^3 + ax^2 + bx + c = \left[\frac{-p \pm \sqrt{p^2 - 4q}}{2}\right](x^2 + d), \quad (24)$$

which is again a solvable cubic.

Expanded out, (23) is

$$x^6 + 2(ax^2 + bx + c)x^3 + (ax^2 + bx + c)^2$$
$$+ p(x^5 + ax^4 + (b + d)x^3 + (c + ad)x^2 + bdx + cd)$$
$$+ q(x^4 + 2dx^2 + d^2) = 0$$

or

$$x^6 + (2a + p)x^5 + (2b + a^2 + pa + q)x^4 + (2ab + 2c + p(b + d))x^3$$
$$+ (b^2 + 2ac + p(c + ad) + 2qd)x^2 + (2bc + pbd)x$$
$$+ (c^2 + pcd + qd^2) = 0. \quad (25)$$

Comparing (22) and (25)

$$G = 2a + p \quad (26)$$
$$H = 2b + a^2 + pa + q \quad (27)$$
$$K = 2c + 2ab + p(b + d) \quad (28)$$
$$L = b^2 + 2ac + p(c + ad) + 2qd \quad (29)$$
$$M = b(2c + pd) \quad (30)$$
$$N = c^2 + pcd + qd^2. \quad (31)$$

We now make the observation that M factorises, so that if M = 0, then if b ≠ 0, we can divide by it and reduce in effect the degree of equation (30). But this is possible by the result of theorem 11.8.1, since a linear substitution in y of the equation

$$y^6 + ry^5 + sy^4 + ty^3 + uy^2 + vy + w = 0$$

can reduce the coefficient of y^5 to zero, and on substitution of y = 1/x, we obtain effectively equation (22) with M = 0, and bypass a solution of the quintic.

Using equation (26)

$$p = G – 2a, \quad (32)$$

which enables us to obtain q from equation (27), namely

$$H = a^2 + 2b + Ga – 2a^2 + q$$

or

$$q = H + a^2 – Ga – 2b. \quad (33)$$

Then equation (28) becomes

$$K = 2ab + 2c + (G – 2a)(d + b)$$
$$K = 2c + Gd + Gb – 2ad, \quad (34)$$

whereas (32) and (33) in (29) gives

$$L = 2ac + b^2 + (G - 2a)(ad + c) + 2d(H + a^2 - Ga - 2b)$$

$$L = b^2 - Gad + Gc + 2Hd - 4db. \tag{35}$$

From (30) using M = 0 and b ≠ 0

$$c = \left(a - \frac{G}{2}\right)d, \tag{36}$$

$$c^2 = \frac{G^2d^2}{4} - Gad^2 + a^2d^2. \tag{37}$$

Equation (31) now becomes

$$N = c^2 + (G - 2a)cd + (H + a^2 - Ga - 2b)d^2$$

$$N = c^2 + Gcd - 2acd + Hd^2 + a^2d^2 - Gad^2 - 2bd^2. \tag{38}$$

Using (36) and (37) in (34), (35) and (38)

$$K = Gb, \tag{39}$$

$$L = b^2 - Gad + G\left(a - \frac{G}{2}\right)d + 2Hd - 4db$$

$$L = b^2 - \frac{G^2d}{2} + 2Hd - 4db, \tag{40}$$

$$N = \frac{G^2d^2}{4} - Gad^2 + a^2d^2 + (G - 2a)\left(a - \frac{G}{2}\right)d^2 + Hd^2 + a^2d^2 - Gad^2 - 2bd^2$$

$$N = -\frac{G^2d^2}{4} + Hd^2 - 2bd^2. \tag{41}$$

Now substituting

$$b = \frac{K}{G} \tag{42}$$

from (39) in (40) gives

$$L = \left(\frac{K}{G}\right)^2 - \frac{G^2d}{2} + 2Hd - \frac{4Kd}{G}$$

$$d\left(-\frac{G^2}{2} + 2H - \frac{4K}{G}\right) = L - \left(\frac{K}{G}\right)^2$$

$$d = \frac{L - \left(\frac{K}{G}\right)^2}{\left(-\frac{G^2}{2} + 2H - \frac{4K}{G}\right)} \tag{43}$$

and in (41)

$$N = -\frac{G^2d^2}{4} + Hd^2 - \frac{2K}{G}d^2,$$

so that on substituting d in (43) we have an unacceptable constraint derived from the fact that the ‘a’ term has disappeared from (41).

However, we will find in [Ad18] that a quintic with bogus roots can be set equal to a quartic variety in quadratic variables, leading an elliptic curve, and that the quintic is solvable. ☐

11.11. QR algorithms.

The QR algorithm is a method giving a stable progressive computation of the eigenvalues of a real matrix, which we will discuss and is extended here to complex matrices. We will introduce a number of ideas used by the QR algorithm. This will allow us to find the roots of a polynomial of arbitrary degree with complex or quaternionic coefficients by approximation methods.

Our point of view is that complex matrices may be represented by real matrices using the intricate representation of chapter I, section 6. A more general setting includes a discussion of quaternions, which can be represented by the real matrices of chapter III, section 7.

Indeed if we look at the matrix

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

which we know is the matrix representation of the complex number a1 + bi, the determinant

$$\det \begin{bmatrix} a - x & b \\ -b & a - x \end{bmatrix} = 0$$

is $(x^2 - 2ax + a^2 + b^2) = 0$, with solution

$$x = a1 \pm bi,$$

so we retrieve this complex number as an eigenvalue of its matrix representation. Further, any of these two choices is appropriate for the matrix, provided it is applied consistently (and the two types of solution are representable in terms of the automorphisms of chapter X). ☐

We know the transpose A^T of a matrix A interchanges rows and columns. The *complex conjugate* A* of a complex n × n matrix A converts each element $a_{jk} + ib_{jk}$ of the matrix to its complex conjugate $a_{jk} - ib_{jk}$.

Since we have just seen that an n × n matrix A of complex numbers can be represented by a 2n × 2n matrix A′ of real numbers, the *conjugate transpose* of A, also called the *Hermitian conjugate* or *Hermitian transpose* of A, which we will denote by A^{*T}, is the result of transposing the real matrix representation A′ to A'^T. ☐

In chapter II we gave the example of a 4 × 4 *companion matrix*

$$C = \begin{bmatrix} 0 & 0 & 0 & -a_0 \\ 1 & 0 & 0 & -a_1 \\ 0 & 1 & 0 & -a_2 \\ 0 & 0 & 1 & -a_3 \end{bmatrix},$$

where the determinant of C with eigenvalues x

$$\det(C - xI) = \det \begin{bmatrix} -x & 0 & 0 & -a_0 \\ 1 & -x & 0 & -a_1 \\ 0 & 1 & -x & -a_2 \\ 0 & 0 & 1 & -x - a_3 \end{bmatrix}$$

is given by

$$g(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + x^4,$$

with an obvious extension to the more general case given by n × n companion matrices. ☐

For a square matrix, the *main* or *principal diagonal* is the diagonal line of entries running from the top left hand corner to the bottom right hand corner. An *upper triangular matrix* R has all zero entries below the main diagonal. A *superdiagonal* entry is one that is directly above and to the right of the main diagonal. A *subdiagonal* entry is one that is directly below and to the left of the main diagonal.

The companion matrix is an example of an *upper Hessenberg matrix*, which is defined as having zero entries below the first subdiagonal.

Many linear algebra algorithms require significantly less computational effort when applied to triangular matrices, and this improvement often carries over to Hessenberg matrices. If the constraints of a linear algebra problem forbid a general matrix to be reduced conveniently to a triangular one, reduction to Hessenberg form is often the next best approach. In fact, reduction of any matrix to a Hessenberg form can be achieved in a finite number of steps, for example by using the Householder algorithm of unitary similarity transforms. Subsequent reduction of a Hessenberg matrix to a triangular matrix can be achieved through iterative procedures, known as shifted QR-factorisation. In eigenvalue algorithms, the Hessenberg matrix can be further reduced to a triangular matrix through shifted QR-factorisation combined with *deflation* steps, to be described. Reducing a general matrix to a Hessenberg matrix and then reducing further to a triangular matrix, instead of directly reducing a general matrix to a triangular matrix, often economises the arithmetic involved in the QR algorithm for eigenvalue problems.

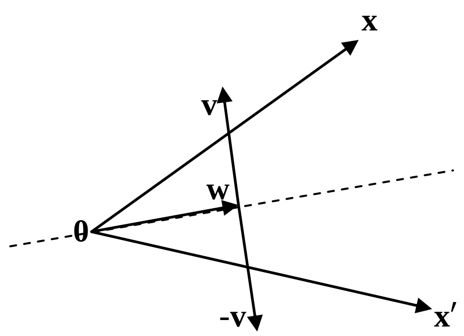
The product of a Hessenberg matrix with a triangular matrix is again Hessenberg. If A is upper Hessenberg and R is upper triangular, then AR and RA are upper Hessenberg. ☐

Let I be the identity matrix. We can factor a complex $n \times n$ matrix A as the product of a *unitary matrix* Q (so $Q^{*T}Q = I$) and an $n \times n$ upper triangular matrix R. ☐

A *Householder transformation,* otherwise known as a *Householder reflection* or *elementary reflector,* is a linear transformation that describes a reflection about a hyperplane containing the origin. The reflection hyperplane can be defined by a column vector **v** with length 1 which is orthogonal (at right angles) to the hyperplane. Let $\langle\mathbf{x}, \mathbf{v}\rangle$ be the scalar product of the vector **v** and a point column vector **x** anywhere with respect to the origin **0**, extending the idea from chapter II, section 10, so that the Hermitian transpose of **v** is combined in the scalar product with the complex vector **x** forming $\mathbf{v}^{*T}\mathbf{x}$.

The reflection of the point **x** to **x′** about this hyperplane is then

$$\mathbf{x} - 2\langle\mathbf{x}, \mathbf{v}\rangle\mathbf{v} = \mathbf{x} - 2\mathbf{v}(\mathbf{v}^{*T}\mathbf{x}).$$



A Householder reflection about the dotted hyperplane bisecting the angle between **x** and **x′**.

With I the identity matrix, a *Householder matrix* is defined as

$$P = I - 2\mathbf{v}\mathbf{v}^{*T}.$$

The Householder matrix has the following properties

(1) It is Hermitian, $P = P^{*T}$.
(2) It is unitary, the inverse $P^{-1} = P^{*T}$.
(3) It satisfies the involution $P^2 = I$; applied twice, the transformation returns to itself.

A Householder matrix has eigenvalues ±1, because in the n-dimensional space if **w** is in the hyperplane orthogonal to **v** then $P\mathbf{w} = \mathbf{w}$, also $P\mathbf{v} = -\mathbf{v}$. The determinant of a Householder reflector is –1, since the determinant of a matrix is the product of its eigenvalues, and there are (n – 1) independent vectors orthogonal to **w** with eigenvalues +1 and one instance of the vector **v**, with eigenvalue –1. ☐

The description of this transformation given by Stoer and Bulirsch, *Introduction to Numerical Analysis* (3rd ed.), Springer, 2002, p. 225, is in error for the complex case. Note that for two complex numbers, in general

$$(a - ib)(x + iy) \neq (a + ib)(x - iy)$$

so if we define the scalar product as the real number

$$\tfrac{1}{2}(\mathbf{v}^{*T}\mathbf{x} + \mathbf{x}^{*T}\mathbf{v}),$$

as these authors do, then the reflection of the point $\mathbf{x}$ about this hyperplane is then

$$\mathbf{x} - 2\langle\mathbf{x}, \mathbf{v}\rangle\mathbf{v} = \mathbf{x} - (1 + t)\mathbf{v}(\mathbf{v}^{*T}\mathbf{x})$$

where

$$t = \mathbf{x}^{*T}\mathbf{v}/\mathbf{v}^{*T}\mathbf{x}$$

is real, and in general is not 1.

This means the Householder matrix would be defined as

$$P = I - (1 + t)\mathbf{v}\mathbf{v}^{*T},$$

but then

$$P^2 = I - 2(1 + t)\mathbf{v}\mathbf{v}^{*T} + (1 + t)^2(\mathbf{v}\mathbf{v}^{*T})(\mathbf{v}\mathbf{v}^{*T}),$$

where since $\mathbf{v}^{*T}\mathbf{v} = 1$,

$$(\mathbf{v}\mathbf{v}^{*T})(\mathbf{v}\mathbf{v}^{*T}) = \mathbf{v}(\mathbf{v}^{*T}\mathbf{v})\mathbf{v}^{*T} = \mathbf{v}\mathbf{v}^{*T},$$

which means that this P^2 is not usually an involution. But a reflection applied twice returns to itself, a contradiction. □

We will consider as an example the case where A is a real matrix for which we want to compute the eigenvalues, and start with $A_{k=0} = A_0 = A$. At the k-th step we compute the QR decomposition $A_k = Q_kR_k$, where in this instance Q_k is an *orthogonal matrix* (so $Q^T = Q^{-1}$ and there is no complex conjugate to bother about) and R_k is an upper triangular matrix. We then form the product in reverse order $A_{k+1} = R_kQ_k$.

Note that

$$A_{k+1} = R_kQ_k = Q_k^{-1}Q_kR_kQ_k = Q_k^{-1}A_kQ_k = Q_k^{*T}A_kQ_k,$$

so as defined in chapter II, section 8, all the A_k are *similar*, and hence from section 12 of the same chapter, they have the same eigenvalues. The algorithm is *numerically stable* because it proceeds by orthogonal, or in the more general case unitary, similarity transforms.

Under certain conditions, the matrices A_k converge to a triangular matrix, the *Schur form* of A. The eigenvalues of a triangular matrix are listed on the diagonal, and the eigenvalue problem is solved. In testing for convergence it is impractical to require exact zeros, but the *Gershgorin circle theorem* provides a bound on the error.

Consider the example matrix

$$A = \begin{bmatrix} 12 & -51 & 4 \\ 6 & 167 & -68 \\ -4 & 24 & -41 \end{bmatrix}.$$

We will find a Householder reflection that transforms the first column of the matrix A, represented by the column vector $\mathbf{x} = (12, 6, -4)^T$, so that its last two rows are zero.

The norm of $(12, 6, -4)^T$ is

$$\|\mathbf{x}\| = 2\sqrt{6^2 + 3^2 + 2^2} = 14.$$

Let $\mathbf{e}_1$ be the column vector $(1, 0, 0)^T$. We form

$$\mathbf{u} = \mathbf{x} - \|\mathbf{x}\|\mathbf{e}_1$$

and

$$\mathbf{v} = \frac{\mathbf{u}}{\|\mathbf{u}\|},$$

so

$$\mathbf{u} = (12, 6, -4)^T - (14, 0, 0)^T$$
$$= 2(-1, 3, -2)^T$$

and

$$\mathbf{v} = \frac{(-1, 3, -2)^T}{\sqrt{14}}.$$

Then

$$Q_1 = I - \frac{2}{\sqrt{14}\sqrt{14}}\begin{bmatrix}-1\\3\\-2\end{bmatrix}\begin{bmatrix}-1 & 3 & -2\end{bmatrix}$$

$$= I - \frac{1}{7}\begin{bmatrix}1 & -3 & 2\\-3 & 9 & -6\\2 & -6 & 4\end{bmatrix} = \begin{bmatrix}\frac{6}{7} & \frac{3}{7} & \frac{-2}{7}\\ \frac{3}{7} & \frac{-2}{7} & \frac{6}{7}\\ \frac{-2}{7} & \frac{6}{7} & \frac{3}{7}\end{bmatrix}.$$

We now see that

$$Q_1A = \begin{bmatrix}14 & 21 & -14\\0 & -49 & -14\\0 & 168 & -77\end{bmatrix},$$

so that the first column is already in the form of a triangular matrix. We will now perform deflation, which amounts to reducing our considerations to the submatrix M_{11}, where

$$M_{11} = \begin{bmatrix}-49 & -14\\168 & -77\end{bmatrix}.$$

By the same method as above, we obtain the matrix of the Householder transformation

$$Q_2 = \begin{bmatrix}1 & 0 & 0\\0 & \frac{-7}{25} & \frac{24}{25}\\0 & \frac{24}{25} & \frac{7}{25}\end{bmatrix}.$$

We find

$$Q = Q_1^T Q_2^T = \begin{bmatrix}\frac{6}{7} & \frac{-69}{175} & \frac{-58}{175}\\ \frac{3}{7} & \frac{158}{175} & \frac{-6}{175}\\ \frac{-2}{7} & \frac{6}{35} & \frac{33}{35}\end{bmatrix}.$$

Then

$$R = Q_2Q_1A = Q^TA$$
$$= \begin{bmatrix}14 & 21 & -14\\0 & 175 & -70\\0 & 0 & -35\end{bmatrix}.$$

The matrix Q is orthogonal and R is upper triangular, so

$$A = QR$$

is the required QR-decomposition. □

The use of Householder transformations is inherently the most simple of the numerically stable QR decomposition algorithms due to the use of reflections as the mechanism for producing zeroes in the R matrix. However, the Householder reflection algorithm is bandwidth heavy and not parallelisable, as every reflection that produces a new zero element changes the entirety of both Q and R matrices. In modern computational practice the QR algorithm is performed in an implicit version which makes the use of multiple shifts easier to introduce. □

Similarly, for one of the many representations of a quaternion, usually denoted by the letter H after W.R. Hamilton who discovered them

$$H = a + bi + cj + dk,$$

taken now from the example of the matrices of chapter II, section 2, when its four basis elements 1, i, j and k are multiplied by a, b, c and d respectively this gives rise to the corresponding eigenvalue equation

$$\det\begin{bmatrix} a-x & b & c & d \\ -b & a-x & -d & c \\ -c & d & a-x & -b \\ -d & -c & b & a-x \end{bmatrix} = 0,$$

with complex solutions. On expanding out the determinant by subdeterminants starting from the top row we get

$$\begin{aligned}&(a-x)[(a-x)((a-x)^2 + b^2) + d(d(a-x) + bc) + c(db + (a-x)c)]\\ &\quad - b[-b((a-x)^2 + b^2) + d(-c(a-x) + b(-d)) + c(-cb - (a-x)(-d))]\\ &\quad + c[-b(d(a-x) - bc) - (a-x)((-c)(a-x) - bd) + c(c^2 + d^2)]\\ &\quad - d[-b(db + (a-x)(c)) - (a-x)(-cb + (a-x)d) - d(c^2 + d^2)]\\ &\quad = 0.\end{aligned}$$

We have also seen from an exercise of chapter III, this has solutions

$$[(a-x)^2 + b^2 + c^2 + d^2]^2 = 0,$$

which we can write in the equivalent form

$$[(H-x)(H-x)^*]^2 = [(a-x) + bi + cj + dk)((a-x) - bi - cj - dk)]^2 = 0.$$

From these solutions we see that the surjective mapping

$$(a-x) + bi + cj + dk \to (a-x) \pm \sqrt{b^2 + c^2 + d^2}\, i$$

allows a mapping from quaternionic to complex solutions.

Further the complex conjugate has an analogue for a quaternion. If we put

$$H^* = (a + bi + cj + dk)^* = a - bi - cj - dk,$$

then we can consider quaternion solutions in the same way as we have already done for complex ones. □

11.12. Exercises.

(A) In equation 11.5.(13) for the quintic variety, we have so far only considered linear substitutions of variables. For the nonlinear allocation

$$y = x^4 + rx^3 + sx^2 + tx + u,$$

on putting the linear substitutions

$$y = w + g,$$
$$x = w + h,$$

show that this is solvable, and thus in this case the nonlinear allocation reduces to a linear one.

(B) Let

$$x^3 + Kx^2 + Lx + M = 0, \tag{1}$$

adjoin by multiplication the root

$$(x + n) = 0. \tag{2}$$

Show by equating coefficients that there is no general such quartic polynomial equation with the result available by an inductive procedure equivalent to the solvable equation

$$(x^2 + px + q)^2 + a(x^2 + px + q) + b = 0. \tag{3}$$

(C) Show any quartic polynomial equation may be put in the form

$$y^4 + K'y^2 + L'y + M' = 0. \tag{1}$$

Hence under the substitution

$$y = 1/x \tag{2}$$

show this may be represented in the form

$$x^4 + Jx^3 + Kx^2 + M = 0. \tag{3}$$

Adjoin by multiplication the quadratic

$$x^2 + n_1x + n_2 = 0. \tag{4}$$

Show the resulting equation is

$$x^6 + (J + n_1)x^5 + (K + Jn_1 + n_2)x^4 + (Kn_1 + Jn_2)x^3$$
$$+ (M + Kn_2)x^2 + Mn_1x + Mn_2 = 0. \tag{5}$$

Compare this with the solvable sextic

$$(x^2 + px + q)^3 + a(x^2 + px + q)^2 + b(x^2 + px + q) + c = 0, \tag{6}$$

which you should find gives

$$x^6 + 3(px + q)x^4 + 3(px + q)^2x^2 + (px + q)^3 +$$
$$ax^4 + 2a(px + q)x^2 + a(px + q)^2$$
$$+ bx^2 + b(px + q) + c = 0,$$
$$x^6 + 3px^5 + (3q + 3p^2 + a)x^4 + (6pq + p^3 + 2ap)x^3 + (3q^2 + 3p^2q + 2aq + ap^2 + b)x^2$$
$$+ (3pq^2 + 2apq + bp)x + (q^3 + aq^2 + bq + c) = 0. \tag{7}$$

Then compare coefficients between (5) and (7). Find that

$$J + n_1 = 3p,$$
$$K + Jn_1 + n_2 = 3q + 3p^2 + a,$$
$$Kn_1 + Jn_2 = 6pq + p^3 + 2ap,$$
$$M + Kn_2 = 3q^2 + 3p^2q + 2aq + ap^2 + b,$$
$$Mn_1 = 3pq^2 + 2apq + bp,$$
$$Mn_2 = q^3 + aq^2 + bq + c.$$

If you then evaluate n_1 and n_2 you should get

$$n_1 = 3p – J, \tag{8}$$
$$n_2 = 3q + 3p^2 + a – K – J(3p – J)), \tag{9}$$

and then eliminating n_1 and n_2 from the comparison equations you have generated you should get

$$K(3p – J) + J(3q + 3p^2 + a – K – J(3p – J)) = 6pq + p^3 + 2ap, \tag{10}$$
$$M + K(3q + 3p^2 + a – K – J(3p – J)) = 3q^2 + 3p^2q + 2aq + ap^2 + b, \tag{11}$$
$$M(3p – J) = 3pq^2 + 2apq + bp, \tag{12}$$
$$M(3q + 3p^2 + a – K – J(3p – J)) = q^3 +aq^2 + bq + c. \tag{13}$$

Eliminate b. You should find

$$M(3p – J) = 3pq^2 + 2apq$$
$$+ (M + K(3q + 3p^2 + a – K – J(3p – J)) – 3q^2 – 3p^2q – 2aq – ap^2)p,$$

$$M(3p - J) = (M + K(3q + 3p^2 - K - J(3p - J)))p - 3p^3q + ap(-p^2 + K). \qquad (14)$$

Now eliminate a from the combination of equations (10) and (14). Do you get

$$\begin{aligned} &p(K - p^2)[K(3p - J) + J(3p^2 - K - J(3p - J)) - p^3] \\ &\quad + (J - 2p)[M(2p - J) - K(3p^2 - K - J(3p - J))p] \\ &\quad = (2p - J)[-3Kqp + 3p^3q] - p(K - p^2)[3Jq - 6pq]? \qquad (15) \end{aligned}$$

Show that the terms in q to the right of the equal sign = 0, and thus J, K and M are given by an inductively unsolvable quintic in p. ☐

(D) The comparison method has not created a solution by radicals of the quintic from a solvable quartic. More generally from a solvable general polynomial equation of degree g by the same methods we might wish to find whether there exist solutions by induction of a polynomial equation of degree g + 1. Our objective could be to extend the method for the quintic to the polynomial equation of degree six, the sextic. We will find in [Ad18] a solution dependent on a decic equation, of degree ten which reduces to a quintic. So this solves the sextic if the quintic solution is known.

This might lead us to consider in the general case to an equation of the form

$$y^g + Fy^{g-1} + Gy^h + Hy^{h-1} + ... + L = 0. \qquad (1)$$

Thus inductively we will need to find a method for this equation of degree g for any g.

For the general method we could employ a polynomial in a general Bring-Jerrard form like (1). In order that the analogue of equations for the quintic can be used, it might be desirable to set at least three of the coefficients equal to zero in the new polynomial, which can be obtained by the methods of section 7. ☐

For these types of solution, we are confronted with a problem in mathematics. On the one hand we might feel that these equations, although complicated, can be followed, and that their unusual complexity is not a barrier to understanding. On the other, we might say that the equations are so complicated that eventually the computation has to be done by machine, but to understand the process by which a solution is obtained a machine equation solver has to be used to follow the calculation.