The composition heresies

Maurice Craig

1 Introduction

First published in 1202 [16, p. 167–170], the "two–squares" identity

$$(x^2 + y^2)(x'^2 + y'^2) = (xx' - yy')^2 + (xy' + x'y)^2$$

was possibly known still earlier [13, p. 60]. Writing sums of squares as products of complex conjugates reduces it to expanding the product $(x + y\sqrt{-1})(x' + y'\sqrt{-1})$. Many such "composition identities" are similarly explained by decomposing the homogeneous forms into products of linear forms with suitable algebraic numbers as coefficients. But unfortunately for theoretical simplicity, the identities for sums of four or eight squares differ, the forms being indecomposable.

The 1840s saw attempts to incorporate these exceptions via a subtle analogy. New algebras constructed *ad hoc* [14, p. 178] permit linear factorisation. However, one disturbing thought overshadows this early experiment in "abstract" algebra. Namely, the treatment of $x^2 + y^2$ employs well known tools developed for quite different ends [15], so explains the identity in the popular sense of making the unknown familiar. By contrast, derivations of the four or eight squares identities that merely "exhibit" a composition algebra (e.g. [11, p. 159]) risk the same logical circularity as the traditional "Chicken–and–Egg" paradox, a mathematical felony censured in a celebrated remark by Russell [17, p.71].

Bakker [1, p. 457] advanced a non–circular theory of chicken origins. The present paper advances a new paradigm for composition formulae. I exploit the idea that complex conjugation of $x + y\sqrt{-1}$ leaves $x^2 + y^2$ *invariant* – a word rich in algebraic associations! Besides its success in "rounding up the usual suspects" (forms of small degree and dimension known to have composition properties), noteworthy features of the method are as follows.

(a) The decomposability distinction mentioned above is entirely absent.

(b) The product of one application is not one identity, but a family of identities corresponding to different parameter values.

(c) Along with the forms themselves we recover both their composition formulae and associated "composition algebras" (such as $\mathbb{Q}(\sqrt{-1})$ for $x^2 + y^2$).

(d) The algebras are not formal systems introduced *ad hoc*, but algebraic number fields equipped with a synthetic "product", this being a specific bilinear function of the conjugates of the numbers to be "multiplied".

The significance of (c) is that, as neither the identity nor the algebra is used in deriving the other, we avoid explanations which themselves lack explanation. Item (d) means that all properties of the composition algebras reduce to properties of algebraic number fields. Small wonder then (*cf.* [2, p. 395]), should the product prove anti–commutative or non–associative. For so too, under the binary operation of subtraction, are even the ordinary integers.

Though not universally applicable, a convenient summary for many identities is as follows. Suppose the *associative* algebra A has a finite basis B and matrix representation R [10, p. 25-49]. By the multiplicative property of determinants $\det R(\alpha)$, a form in the coordinates

of $\alpha \in A$ relative to B, has a composition formula. The eight-square identity is excluded, obstructed by the associativity of matrix multiplication. The four-square identity passes, albeit subject to due caution against mistaking an implication for an explication.

When A is a number field the determinant is a so–called norm form [10, p. 127–133]. Two explicit examples involving group algebras will be convenient for reference later. First, the cyclic matrices (written row–sequentially for brevity)

$$\Gamma(x,y,z) = (x \quad z \quad y \quad | \quad y \quad x \quad z \quad | \quad z \quad y \quad x)$$

form a closed system. Hence follows a composition identity for the ternary cubic $\Delta(x,y,z) = \det \Gamma(x,y,z) = x^3 + y^3 + z^3 - 3xyz$, often called a cyclic determinant or circulant. In this instance R is the regular matrix representation [10, p. 32–34] of the group algebra for $\mathbf{C}_3$, the cyclic group of order 3. The system of matrices $(x+y \quad z+t \quad | \quad z-t \quad x-y)$ is likewise closed, so $x^2 - y^2 - z^2 + t^2$ has a composition formula too. The matrix cofactors of x, y, z, t comprise a representation of the (commutative) Klein four–group $\mathbf{C}_2 \times \mathbf{C}_2$. However, as some coefficient pairs anti–commute, it is merely a *projective* representation [10, p. 348].

The second section introduces the group–theoretic tools. Section 3 applies them to binary quadratic composition. Although trivial, this case makes an ideal starting point, being quite typical and because novelties are best met in a familiar setting. Later sections treat quaternary and octonary forms. I mention also a problem of Dickson that seems amenable now to a computational attack.

2   Group invariants

A linear transformation group G on a set of indeterminates permutes the homogeneous polynomials of each degree. Invariants may outnumber forms expressible by elementary symmetric functions. For example, when the dihedral group $< (12), (1324) >$ permutes x_1, x_2, x_3, x_4 according to its effect on the subscripts, $x_1 x_2 + x_3 x_4$ is a quadratic invariant independent of Σx_i and Σx_i^2.

The Molien series [4, p. 300] is a formal power series (in the indeterminate λ, say) whose coefficients forecast the number of basic invariants for each degree. For the dihedral example it reads

$$(1/8)[1/(1-\lambda)^4 + 3/(1-\lambda^2)^2 + 2/(1-\lambda^2)(1-\lambda)^2 + 2/(1-\lambda^4)]$$
$$= 1 + \lambda + 3\lambda^2 + 4\lambda^3 + 8\lambda^4 + \ldots$$

In fact, as the other two basis elements thus predicted for quadratic invariants, we may choose $(u+v)^2$ and uv, where $u = x_1 + x_2, v = x_3 + x_4$.

In the right–regular (permutation) representation, G acts on indeterminates, indexed by the N elements of G itself, according to the rule $(\xi^g)^h = \xi^{gh}$. Invariants are simplest to compute when G is abelian. In that situation there are N homomorphisms $\chi : G \to \mathbb{C}$, the characters of G [3, p. 415], producing N independent linear forms $J = \Sigma \chi(g) \xi^g$. We have $J^h = \chi(h^{-1})J$, whence J is unchanged except for multiplication by a certain N–th root of unity. We can then construct absolute invariants as judiciously chosen products of these relative invariants. Non–abelian groups lack this handy aid. In the example above, we still have $J = u \pm v$, but the two second–degree invariants J^2 prove insufficient.

The first two Molien coefficients are always unity. Table 1 shows the next few, for the regular representations of some groups of interest to us.

Group	λ^2	λ^3	λ^4	λ^5
$\mathbf{C}_2$	2	2	3	3
$\mathbf{C}_3$	2	4	5	7
$\mathbf{C}_4$	3	5	10	14
$\mathbf{C}_2 \times \mathbf{C}_2$	4	5	11	14
$\mathbf{C}_5$	3	7	14	26
$\mathbf{C}_2 \times \mathbf{C}_2 \times \mathbf{C}_2$	8	15	50	99

Table 1. Coefficients in Molien series for small abelian groups.

Number fields are the final prerequisite. Let K, the base-field, be a finite extension of $\mathbb{Q}$, L a finite normal extension of the K, and $G = Aut(L/K)$. Thus L is the root–field of some polynomial whose roots, being permuted transitively, conveniently may be indexed by the elements of G. In this setting it helps to reinterpret the indeterminates ξ^g as a generic element $\xi \in L$, together with its algebraic conjugates. Restricting ξ to a sub–field reduces form dimension in a proposed identity, whence prior results may suffice to evaluate some parameters.

3   Binary forms

Here $G = \mathbf{C}_2 = \langle \rho \rangle$, the first-degree relative invariants α, β being given by

$$2 \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \xi \\ \xi^\rho \end{bmatrix}.$$

The coefficient matrix, H say, is a Hadamard matrix [18, p. 104-107], and will recur. Noting that $\alpha^\rho = \alpha, \beta^\rho = -\beta$, with use of Table 1 we conclude that bases for the absolute invariants of the first few degrees are as follows.

Degree 1: α	Degree 2: α^2, β^2
Degree 3: $\alpha^3, \alpha\beta^2$	Degree 4: $\alpha^4, \alpha^2\beta^2, \beta^4$

Next let η and ζ be two further field elements with respective relative invariants α', β' and α'', β'', and suppose that ζ is a bilinear function of the conjugates of ξ and η. However, instead of writing ζ in terms of the four products $\xi^g\eta^h$, express α'', β'' as bilinear functions of the singly primed and the unaccented variables. Because ρ fixes the alphas while reversing the betas, the only consistent arrangement, still with four unknown coefficients (elements of K), is:

$$\begin{bmatrix} \alpha'' \\ \beta'' \end{bmatrix} = \begin{bmatrix} a_1\alpha & b_1\beta \\ a_2\beta & b_2\alpha \end{bmatrix} \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix}.$$

Assume additionally that $\zeta = \xi$ when $\eta = 1$ and $\zeta = \eta$ when $\xi = 1$. In the former case $(\alpha', \beta') = (1, 0)$ so $\zeta = \alpha'' + \beta'' = a_1\alpha + a_2\beta$, whereas $\xi = \alpha + \beta$. Thus $a_1 = a_2 = 1$. Similarly $a_1 = b_2 = 1$, leaving only b_1 still to find. The composition identities themselves now make their entrance. They will be equations of the type $\mathcal{F}(\xi)\mathcal{F}(\eta) = \mathcal{F}(\zeta)$, where $\mathcal{F}(\xi)$ is an invariant form homogeneous in the conjugates of ξ with the restriction that $\mathcal{F}(1) = 1$. (Although more general identities exist [13], those involving just these "principal" forms are enough for a start. The crucial point to avoid obscuring is the *invariance* of $\mathcal{F}$.)
(a) Quadratic composition.
By invariance $\mathcal{F}(\xi) = \alpha^2 + B\beta^2$ for $B \in K$ so the identity reads

$$(\alpha^2 + B\beta^2)(\alpha'^2 + B\beta'^2) = (\alpha\alpha' + b_1\beta\beta')^2 + B(\alpha\beta' + \beta\alpha')^2.$$

Comparison of the $\alpha\alpha'\beta\beta'$ terms shows that $b_1 = -B$, this necessary condition proving also sufficient. Note that $\zeta = \alpha'' + \beta''$ is

$$(\alpha + \beta)(\alpha' + \beta') - (1 + B)\beta\beta' = \xi\eta - (1/4)(1 + B)(\xi - \xi^\rho)(\eta - \eta^\rho).$$

When $B = -1$ we recover the orthodox formulae $\mathcal{F}(\xi) = \xi^{1+\rho}$ and $\zeta = \xi\eta$. To illustrate how heterodox values $B \neq -1$ fulminate heresies, write $\xi = x + y\sqrt{d}$, so that $\xi^\rho = x - y\sqrt{d}, \alpha = x, \beta = y\sqrt{d}$ and $\mathcal{F}(\xi) = x^2 + Bdy^2$. (Here, B and d are parameters, as adumbrated in the Introduction (b).) Consequently, by taking $(B, d) = (2, -1)$ we can apply $\mathbb{Q}(\sqrt{-1})$ to produce a composition identity for $x^2 - 2y^2$ (the traditional norm–form of $\mathbb{Q}(\sqrt{2})$) while, with $(B, d) = (1/2, 2)$, from $\mathbb{Q}(\sqrt{2})$ we derive a two–squares identity.

(b) Cubic composition

Now $\mathcal{F}(\xi) = \alpha^3 + B\alpha\beta^2$ for $B \in K$, but the only allowed values are $B = b_1 = 0$. To accommodate sections 4 and 5 I must omit verification.

(c) Quartic composition

We have $\mathcal{F}(\xi) = \alpha^4 + 2B\alpha^2\beta^2 + C\beta^4$. The solutions are all of the type $\mathcal{F}(\xi) = (\alpha^2 + B\beta^2)^2$. Again the proof must be left to the interested reader.

SectionQuaternary non–cyclic forms

For the Klein four–group $G = \langle \rho, \sigma \rangle$ the coefficient matrix of the linear relative–invariant system is the direct (Kronecker) product $H \otimes H$. Thus

$$4 \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} \xi \\ \xi^\rho \\ \xi^\sigma \\ \xi^{\rho\sigma} \end{bmatrix},$$

for which $(\alpha, \beta, \gamma, \delta)^\rho = (\alpha, -\beta, \gamma, -\delta), (\alpha, \beta, \gamma, \delta)^\sigma = (\alpha, \beta, -\gamma, -\delta)$. Hence with constants $b_1, \ldots, d_3$,

$$\begin{bmatrix} \alpha'' \\ \beta'' \\ \gamma'' \\ \delta'' \end{bmatrix} = \begin{bmatrix} \alpha & b_1\beta & c_1\gamma & d_1\delta \\ \beta & \alpha & c_2\delta & d_2\gamma \\ \gamma & b_3\delta & \alpha & d_3\beta \\ \delta & b_4\gamma & c_4\beta & \alpha \end{bmatrix} \begin{bmatrix} \alpha' \\ \beta' \\ \gamma' \\ \delta' \end{bmatrix},$$

while basic invariants (omitting degree 1) are as follows.

Degree 2: $\alpha^2, \beta^2, \gamma^2, \delta^2$

Degree 3: $\alpha^3, \alpha\beta^2, \alpha\gamma^2, \alpha\delta^2, \beta\gamma\delta$

Degree 4: $\alpha^4, \beta^4, \gamma^4, \delta^4, \alpha^2\beta^2, \alpha^2\gamma^2, \alpha^2\delta^2, \beta^2\gamma^2, \beta^2\delta^2, \gamma^2\delta^2, \alpha\beta\gamma\delta$.

(a) Quadratic composition

We have $\mathcal{F}(\xi) = \alpha^2 + B\beta^2 + C\gamma^2 + D\delta^2$. In the proposed identity $\mathcal{F}(\xi)\mathcal{F}(\eta) = \mathcal{F}(\zeta)$ the cross–products $\alpha'\beta', \ldots, \gamma'\delta'$ do not appear on the left side. Equating to zero their coefficients on the right, we obtain identities in the unaccented variables whose coefficients likewise must vanish. The full system reads $(b_1, c_1, d_1) = (-B, -C, -D)$, together with the relations

$$Bc_2 = Cd_3 = Db_4 = -Bd_2 = -Cb_3 = -Dc_4, \tag{1}$$

$$Bc_2d_2 + CD = CDd_3b_2 + DB = Db_4c_4 + BC = 0. \tag{2}$$

To solve it, rewrite equations (1) as

$$Bc_2 = Cd_3 = Db_4 = \lambda c_2d_3b_4, B(c_2 + d_2) = C(d_3 + b_3) = D(b_4 + c_4) = 0,$$

let $(p, q, r) = (d_2, b_3, c_4)$, and suppose $BCD \neq 0$. We have firstly $(c_2, d_3, b_4) = (-p, -q, -r)$. Second, from equations (2) we see that $pqr \neq 0$ so $(B, C, D) = \lambda(qr, rp, pq)$. Substitution in equations (2) shows now that $\lambda = 1$ and we get $\mathcal{F}(\xi) = \alpha^2 + qr\beta^2 + rp\gamma^2 + pq\delta^2$. For example, if $(p, q, r) = (-1, -1, 1)$ then

$$\mathcal{F}(\xi) = (1/2)(\xi^{1+\rho\sigma} + \xi^{\rho+\sigma}), \zeta = \xi\eta - (1/2)(\xi - \xi^\rho)(\eta - \eta^\sigma). \tag{3}$$

The composition algebra is the K–vector space L newly equipped with this bilinear function of conjugates as "product". The formula for ζ shows at a glance why "multiplication" must be non–commutative. That it should be associative might cause surprise, but our earlier $x^2 - y^2 - z^2 + t^2$ example dampens the effect. An interesting property of the second formula in (3), equivalent to orthogonality of a certain 16-rowed matrix, is its persistence for interchange of synthetic with "natural" multiplication.

As a further specialisation let $K = \mathbb{Q}, L = K(\theta)$ where $\theta^4 = -1$, and define ρ, σ as the automorphisms for which $\theta^\rho = \theta^3, \theta^\sigma = \theta^5$. Then with $\xi = x + y\theta + z\theta^2 + t\theta^3$ we find that $\mathcal{F}(\xi) = x^2 + y^2 + z^2 + t^2$. So our composition formula includes one for sums of four squares. From the second of equations (3) one may verify that the elements $\theta, \theta^2, \theta^3$ multiply synthetically by the rules for Hamilton's quaternions i, j, k, as mysteriously revealed to him in his epiphany of 16 October, 1843 [2, p. 395; 19].

(b) Cubic composition is necessarily trivial, of the type $\alpha''^3 = \alpha^3 \alpha'^3$.

(c) Quartic composition

Just two form types have composition, namely the square of the quadratic type above, and a determinantal type $\mathcal{F}(\xi) = \Lambda(\alpha, qr\beta, rp\gamma, pq\delta)$, with $p^2, q^2, r^2 \in K$ and $\Lambda(x, y, z, t)$ the determinant for the regular matrix representation of KG.

4   Octonary forms

I consider here only the elementary abelian group $G = \langle \rho, \sigma, \tau \rangle$ and $K = \mathbb{Q}$. The equation for relative invariants takes the form $8\vec{\alpha} = (H \otimes H \otimes H)\vec{\xi}$, where (say)

$$\vec{\alpha}^T = (\alpha, \beta, \gamma, \delta, \kappa, \lambda, \mu, \nu), \vec{\xi}^T = (\xi, \xi^\rho, \xi^\sigma, \xi^{\rho\sigma}, \xi^\tau, \xi^{\rho\tau}, \xi^{\sigma\tau}, \xi^{\rho\sigma\tau}).$$

The entries in ξ are so ordered as to make the character, for each relative invariant except α, unity on just one of the seven bicyclic subgroups. Thus, entries 2, 3 and 5 can use any three generators of G, but the others are then determined.

(a) Quadratic composition

Table 1 counsels moderation, so I consider only this case. We have

$$\mathcal{F}(\xi) = \alpha^2 + B\beta^2 + C\gamma^2 + D\delta^2 + K\kappa^2 + L\lambda^2 + M\mu^2 + N\nu^2.$$

The bilinear relations take the form $\vec{\alpha}'' = T\vec{\alpha}'$ with T the matrix displayed as Table 2. Though it appears formidable, the work needed to construct it has already been done. Thus if $\xi^\tau = \xi$ then $\kappa, \lambda, \mu, \nu$ are all zero. By restricting ξ, η to the fixed field of τ, we reduce the equation to one determined by just the first four rows and columns of T, which must therefore take the form found above for quaternary quadratic composition. Transcription of the 4–by–4 matrices for all seven biquadratic subfields fills out T completely. It remains to determine compatibility conditions for the 21 parameters $p_1, q_1, \ldots, r_7$ thus introduced.

$$\begin{bmatrix}
\alpha & -B\beta & -C\gamma & -D\delta & -K\kappa & -L\lambda & -M\mu & -N\nu \\
\beta & \alpha & -p_1\delta & p_1\gamma & -p_2\lambda & p_2\kappa & -p_3\nu & p_3\mu \\
\gamma & q_1\delta & \alpha & -q_1\beta & -p_4\mu & -p_5\nu & p_4\kappa & p_5\lambda \\
\delta & -r_1\gamma & r_1\beta & \alpha & -p_6\nu & -p_7\mu & p_7\lambda & p_6\kappa \\
\kappa & q_2\lambda & q_4\mu & q_6\nu & \alpha & -q_2\beta & -q_4\gamma & -q_6\delta \\
\lambda & -r_2\kappa & q_5\nu & q_7\mu & r_2\beta & \alpha & -q_7\delta & -q_5\gamma \\
\mu & q_3\nu & -r_4\kappa & -r_7\lambda & r_4\gamma & r_7\delta & \alpha & -q_3\beta \\
\nu & -r_3\mu & -r_5\lambda & -r_6\kappa & r_6\delta & r_5\gamma & r_3\beta & \alpha
\end{bmatrix}$$

Table 2. The matrix T for the equation $\vec{\alpha}'' = T\vec{\alpha}'$.

Assume $BCDKLMN \neq 0$ and solve in terms of the products $A_i = p_i q_i r_i$ as parameters. We need also are certain auxiliary products z_i and put $B^* = Bz_1, \ldots, N^* = Nz_7$ where (with my shorthand obscuring actual symmetry)

$$(z_1, \ldots, z_7) = (p_1 p_2 p_3, -p_4 p_5 q_1, p_6 p_7 r_1, -q_2 q_4 q_6, q_5 q_7 r_2, -q_3 q_4 r_7, r_3 r_5 r_6).$$

Lastly, let such an ordered triple as (B, C, D) be compressed to $\overline{BCD}$, and a product like $A_1 A_2 A_3$ to A_{123}.

Lemma. *Necessary and sufficient conditions for $\mathcal{F}(\xi)\mathcal{F}(\eta) = \mathcal{F}(\zeta)$ are*

$$A_i = Up_i = Vq_i = Wr_i, \tag{4}$$
$$U^*/p_i = V^*/q_i = W^*/r_i. \tag{5}$$

where, for $i = 1, \ldots, 7$, the respective triples $\overline{UVW}$ are $\overline{BCD}$, $\overline{BKL}$, $\overline{BMN}$, $\overline{CKM}$, $\overline{CLN}$, $\overline{DKN}$, $\overline{DLM}$ (form coefficient sets for the biquadratic subfields).

Proof. These are the conditions for the cross–product terms in $\mathcal{F}(\xi)\mathcal{F}(\eta)$ to vanish. The products $\alpha'\beta', \alpha'\gamma', \ldots, \alpha'\nu'$ give equations (4). After reductions that they allow, the remaining terms $\beta'\gamma', \ldots, \mu'\nu'$ not involving α' give (5). $\square$

From equations (4) follow $A_i^3 = p_i q_i r_i UVW$ and hence $UVW = A_i^2$, a square, in accordance with a theorem of Brandt (see [13, p. 232]). Multiply corresponding sides of all seven of these equations. The common value is both a square and a cube, so we can write $A_{1234567} = Z^3$, $BCDKLMN = Z^2$, where $Z \in \mathbb{Q}$ and Z^2 is the determinant of $\mathcal{F}(\xi)$, regarded as a diagonal form in $\alpha, \beta, \ldots, \nu$.

Proposition. *The unknowns are expressed in terms of the eight (algebraically dependent) rational quantities A_i and Z by means of the formulae*:

$$\begin{array}{llll}
B = -A_{123}/Z, & p_1 = -Z/A_{23}, & q_1 = Z/A_{45}, & r_1 = -Z/A_{67}, \\
C = A_{145}/Z, & p_2 = -Z/A_{13}, & q_2 = Z/A_{46}, & r_2 = -Z/A_{57}, \\
D = -A_{167}/Z, & p_3 = -Z/A_{12}, & q_3 = Z/A_{47}, & r_3 = -Z/A_{56}, \\
K = A_{246}/Z, & p_4 = Z/A_{15}, & q_4 = Z/A_{26}, & r_4 = Z/A_{37}, \\
L = -A_{257}/Z, & p_5 = Z/A_{14}, & q_5 = -Z/A_{27}, & r_5 = -Z/A_{36}, \\
M = A_{347}/Z, & p_6 = -Z/A_{17}, & q_6 = Z/A_{24}, & r_6 = -Z/A_{35}, \\
N = -A_{356}/Z, & p_7 = -Z/A_{16}, & q_7 = -Z/A_{25}, & r_7 = Z/A_{34}.
\end{array}$$

Proof. We have $A_1 = Bp_1$ etc., so all results will follow from those for $B, \ldots, N$. They, in turn, depend on solving the equations $UVW = A_i^2$, which entail linear equations for the logarithms of $B, \ldots, N$. Hindsight lets me shorten the work by computing, for example, $(A_{123}/Z)^2 = (BCD)(BKL)(BMN)/(BCDKLMN) = B^2$. To permit root extraction, sign information must next be sought.

Thus, let $\mathrm{sgn}(B) = \epsilon_B = (-1)^b$ and so on. From $A_1^2 = BCD$ we find the linear congruence $b + c + d \equiv 0 \pmod{2}$. The system of all seven congruences has rank 3, its simultaneous solution being expressible as

$$(d, l, m, n) \equiv (b + c, b + k, c + k, b + c + k) \pmod{2}.$$

Hence $(\epsilon_D, \epsilon_L, \epsilon_M, \epsilon_N) = (\epsilon_{BC}, \epsilon_{BK}, \epsilon_{CK}, \epsilon_{BCK})$, where ϵ_{BC} means $\epsilon_B \epsilon_C$ etc.

Next, write $\mathrm{sgn}(A_i) = \epsilon_i$ and observe that ϵ_Z is the product of the ϵ_i. Extracting positive square roots we have therefore $\epsilon_B B = \epsilon_{4567} A_{123}/Z$. Now, by equations (5), $B^*/p_1 = C^*/q_1 = D^*/r_1$ or $Bp_2p_3 = -Cp_4p_5 = Dp_6p_7$. Also $A_2 = Bp_2$ so $\mathrm{sgn}(p_2) = \epsilon_2 \epsilon_B$ and so on. We conclude that $\epsilon_B \epsilon_2 \epsilon_3 = -\epsilon_C \epsilon_4 \epsilon_5 = \epsilon_B \epsilon_C \epsilon_6 \epsilon_7$. In particular, $\epsilon_B = -\epsilon_{4567}$ whence $B = -A_{123}/Z$. Of course, we have also $\epsilon_C = \epsilon_{2367}$. The value of ϵ_K follows by use of $B^*/p_2 = K^*/q_2 = L^*/r_2$ (equation (5) for $i = 2$), whereupon all the unknowns can be evaluated. $\square$

Remarks: Checking sufficiency of these necessary conditions needs more work, but not further guidance. All numerical constants are rational if the A_i are so, but succinct conditions, in terms of $B, \ldots, N$, for integer coefficients seem elusive.

As to particular results, I mention here only the special form [6]

$$\mathcal{F}(\xi) = (1/4)(\xi^{1+\rho\sigma\tau} + \xi^{\rho+\sigma\tau} + \xi^{\sigma+\rho\tau} + \xi^{\tau+\rho\sigma}),$$

for which $\mathcal{F}(\xi)\mathcal{F}(\eta) = \mathcal{F}(\zeta)$ if $\zeta = \xi\eta - (1/4)\Sigma[(\xi - \xi^\rho)(\eta - \eta^\sigma + \eta^\tau - \eta^{\sigma\tau})]$. Sum over three terms by cyclically permuting ρ, σ, τ. To match the formulae in [11], choose $L = \mathbb{Q}(\varphi)$ where $\varphi = exp(2\pi\sqrt{-1}/24)$. Let $\varphi^{\rho,\sigma,\tau} = \varphi^{11,5,17}$ and $\psi = (1 + \varphi^3 + \varphi^9)/(\varphi^4 + \varphi^8) = (1 + \sqrt{-2})/\sqrt{-3}$. We can take $\theta = \varphi^3$ (*cf.* Section 5). The elements $1, \theta, \theta^2, \theta^3, \psi, \psi\theta, \psi\theta^2, \psi\theta^3$ correspond to Dickson's $1, i, j, k, e, ie, je, ke$ respectively [7]. Particular triples of these "octonions" multiply non–associatively so L, in its role as composition algebra, cannot be replaced by an algebra of matrices.

5 A challenge

Characters of $\mathbf{C}_3$ include cube roots of unity, making the cyclotomic field K_3 best for K in treating ternary forms. I found only trivial identities with forms of degree at most five, except cubic circulants $\mathcal{F}(\xi) = \Delta(\alpha, b^2 c\beta, bc^2\gamma)$. Here $b^3, c^3 \in K_3$ but, by choosing them to be conjugates, we can deduce rational composition identities. Pure cubic extensions of K_3 are cyclic, so examples abound. For cyclic quaternary forms ($G = \mathbf{C}_4$), $K = K_4$ is best. Quadratic forms with composition are special cases of $\mathcal{F}(\xi) = \alpha^2 + C\gamma^2$. Cubic composition is trivial. The quartic identities are of circulant type, with $\mathcal{F}(\xi) = \Delta(\alpha, p\beta, q\gamma, pq\delta)$ for $p^2, q^2/p \in K$.

These findings agree with [12] [13, p. 268]. Dickson [12] characterised ternary and quaternary forms (of arbitrary degree) with composition and noted some decomposable quinary types. However, to decide the existence of non-degenerate indecomposable quinary quintics with composition remained beyond his reach [12, p. 608]. Though too labor-intensive for manual computation (Table 1 indicates 26 basic invariants), the method of this paper looks capable in principle of finding such forms if they exist. In cases I treated, manual solution

of equations was comparatively easy, the main work being to set them up. As that step reduces to expanding a product and collecting like terms, can it perhaps be automated?

6   Conclusion

As remarked in [5, p. 77], the composition algebras are "equivalent" to the identities. But so, for that matter, were Ptolemy's epicycles "equivalent" to the planetary observations that they purported to explain. Mathematical models generally contain parameters, adjusted to fit the data. In the four-squares identity $\Sigma x_i^2 \Sigma y_i^2 = \Sigma z_i^2$ the data are the 64 constants implied by the four bilinear functions z_i of the x and y variables. This being also the number of structure constants for a four-dimensional algebra, the fitting exhausts the data. So that model – the classical theory – is *ad hoc* in the sense of [14, p. 178]. With only 16 parameters, a bilinear function of conjugates of $\xi, \eta \in K_8$ evades this judgment.

Hamilton's i, j, k remain useful as always. But they should be seen as umbral symbols for derived quantities, part of ordinary, commutative algebra, not a separate reality. Long live quaternions – and Occam's razor!

References

[1] R. Bakker, *The Dinosaur Heresies* (Penguin 1986).

[2] E.T. Bell, *Men of Mathematics*, Vol. 2 (Penguin 1965).

[3] Z.I. Borevich and I.R. Shafarevich, *Number Theory* (Academic Press New York 1966).

[4] W. Burnside, *Theory of groups of finite order*, 2nd ed. (Dover New York 1955).

[5] J.H. Conway and D.A. Smith, *On quaternions and octonions: their geometry, arithmetic, and symmetry* (A.K. Peters Natick (Mass.) 2003); (See also http://www.akpeters.com/QANDO).

[6] M. Craig, *What are quaternions?*, Math. Student **50** (1982), 289–292.

[7] M. Craig, *Analytic signals for multivariate data*, Math. Geology **28** (1996), 315–329.

[8] C.W. Curtis, *Linear Algebra*, 3rd ed. (Allyn and Bacon Boston).

[9] C.W. Curtis, *The four and eight square problem and division algebras*, in: *Studies in Modern Algebra* (Ed. A.A. Albert) (Mathematical Assoc. of America 1963).

[10] C.W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras* (John Wiley New York 1962).

[11] L.E. Dickson, *On quaternions and their generalization and the history of the eight square theorem*, Ann. Math. **20** (1919), 155–171 and 297.

[12] L.E. Dickson, *Homogeneous polynomials with a multiplication theorem*, in: *The collected mathematical papers of Leonard Eugene Dickson*, (Ed: A.A. Albert) Vol. II (Chelsea New York 1975).

[13] L.E. Dickson, *History of the theory of numbers*, Vol. 3 (Chelsea New York).

[14] H. Jeffreys, *Scientific Inference*, 2nd ed. (C.U.P. Cambridge 1957).

[15] P.J. Nahin, *An imaginary tale: the story of $\sqrt{-1}$* (P.U.P. Princeton 1998).

[16] W.W. Rouse Ball, *History of Mathematics* (Dover New York 1960).

[17] B. Russell, *Introduction to Mathematical Philosophy*, 9th ed. (Allen and Unwin London 1956).

[18] H.J. Ryser, *Combinatorial Mathematics* (Mathematical Assoc. of America 1963).

[19] B.L. van der Waerden, *Hamilton's discovery of quaternions*, Math. Mag. **49** (1976), 227–234.

E-mail: towenaar@optusnet.com.au