Nonexistence of a Composition Law

ŞABAN ALACA
Carleton University
Ottawa, Ontario, Canada K1S 5B6
salaca@math.carleton.ca

KENNETH S. WILLIAMS*
Carleton University
Ottawa, Ontario, Canada K1S 5B6
kwilliam@connect.carleton.ca

It was known to the ancient Greeks that sums of two squares satisfy the composition law

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = z_1^2 + z_2^2$$

with

$$z_1 = x_1y_1 + x_2y_2,\ z_2 = x_1y_2 - x_2y_1,$$

and to Euler in 1770 that sums of four squares satisfy the composition law

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

with

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4,\ z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3,$$
$$z_3 = x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2,\ z_4 = x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1.$$

Degen in 1822 and Cayley in 1845 gave the corresponding identity for eight squares, see for example [**6**, p. 2]. Sums of three squares however cannot possess an analogous composition law as $3 = 1^2 + 1^2 + 1^2$, $5 = 0^2 + 1^2 + 2^2$ but $15 = 3 \cdot 5 \neq x^2 + y^2 + z^2$ for integers x, y, z. Hurwitz proved in 1898 that there is an identity of the type

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2,$$

where the z_k are bilinear functions of the x_i and y_i, if and only if $n = 1, 2, 4, 8$. Dickson [**2**] gave a detailed, amplified form of Hurwitz's proof in four pages. Rajwade [**6**] gave an amplified version of Dickson's proof in six pages. A proof using normed algebras is given in [**1**]. For more on such laws see for example [**6**].

As $2 = 1^2 + 1^2 + 2 \cdot 0^2$, $7 = 1^2 + 2^2 + 2 \cdot 1^2$, and $14 = 2 \cdot 7 \neq x^2 + y^2 + 2z^2$ for integers x, y, z there cannot exist a composition law of the type

$$(x_1^2 + x_2^2 + 2x_3^2)(y_1^2 + y_2^2 + 2y_3^2) = z_1^2 + z_2^2 + 2z_3^2$$

with z_1, z_2, z_3 bilinear functions of x_1, x_2, x_3 and y_1, y_2, y_3 with integer coefficients. However every odd positive integer can always be expressed in the form $x^2 + y^2 + 2z^2$ for some integers x, y, z, see for example [**3**, Theorem 86, p. 96], [**4**], [**5**, Theorem 1].

*Research of the second author was supported by National Sciences and Engineering Research Council of Canada grant A-7233.

Moreover one of x and y is odd and one is even. Thus every positive odd integer is of the form

$$(2x_1+1)^2+2x_2^2+4x_3^2$$

for some integers x_1, x_2, x_3. Let m and n be odd positive integers. Then mn is also an odd positive integer and there exist integers x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2 and z_3 such that

$$\begin{aligned} m &= (2x_1+1)^2+2x_2^2+4x_3^2, \\ n &= (2y_1+1)^2+2y_2^2+4y_3^2, \\ mn &= (2z_1+1)^2+2z_2^2+4z_3^2. \end{aligned}$$

Hence

$$\begin{aligned} &((2x_1+1)^2+2x_2^2+4x_3^2)((2y_1+1)^2+2y_2^2+4y_3^2) \\ &\quad = (2z_1+1)^2+2z_2^2+4z_3^2. \end{aligned}$$

The question naturally arises: Is this equality a consequence of some underlying composition law for the polynomial $(2x_1+1)^2+2x_2^2+4x_3^2$? In fact it is not, as can be deduced from Hurwitz's theorem. We show this directly from first principles without recourse to Hurwitz's theorem.

Suppose that there exist integers

$$a_1, a_2, \ldots, a_{16}, b_1, b_2, \ldots, b_{16}, c_1, c_2, \ldots, c_{16}$$

such that

$$\begin{aligned} &((2x_1+1)^2+2x_2^2+4x_3^2)((2y_1+1)^2+2y_2^2+4y_3^2) \\ &\quad = (2z_1+1)^2+2z_2^2+4z_3^2 \end{aligned} \tag{1}$$

is an identity in $\mathbb{Z}[x_1, x_2, x_3, y_1, y_2, y_3]$ with

$$\begin{aligned} z_1 = {} & a_1x_1y_1+a_2x_1y_2+a_3x_1y_3+a_4x_2y_1+a_5x_2y_2+a_6x_2y_3 \\ & +a_7x_3y_1+a_8x_3y_2+a_9x_3y_3+a_{10}x_1+a_{11}x_2+a_{12}x_3 \\ & +a_{13}y_1+a_{14}y_2+a_{15}y_3+a_{16}, \end{aligned} \tag{2}$$

$$\begin{aligned} z_2 = {} & b_1x_1y_1+b_2x_1y_2+b_3x_1y_3+b_4x_2y_1+b_5x_2y_2+b_6x_2y_3 \\ & +b_7x_3y_1+b_8x_3y_2+b_9x_3y_3+b_{10}x_1+b_{11}x_2+b_{12}x_3 \\ & +b_{13}y_1+b_{14}y_2+b_{15}y_3+b_{16}, \end{aligned} \tag{3}$$

$$\begin{aligned} z_3 = {} & c_1x_1y_1+c_2x_1y_2+c_3x_1y_3+c_4x_2y_1+c_5x_2y_2+c_6x_2y_3 \\ & +c_7x_3y_1+c_8x_3y_2+c_9x_3y_3+c_{10}x_1+c_{11}x_2+c_{12}x_3 \\ & +c_{13}y_1+c_{14}y_2+c_{15}y_3+c_{16}. \end{aligned} \tag{4}$$

We equate the coefficients of y_3^2, y_3, $x_2y_3^2$, x_2^2, $x_2^2y_3$, and $x_2^2y_3^2$ in (1) (with z_1, z_2, z_3 given by (2), (3), (4) respectively) to obtain the required contradiction. We have

$$[y_3^2] \;\; 4a_{15}^2+2b_{15}^2+4c_{15}^2=4$$

so

$$b_{15}=0,\;\; (a_{15}, c_{15}) = (\pm 1, 0) \text{ or } (0, \pm 1); \tag{5}$$

$[y_3]$ $4a_{15}(2a_{16}+1)+4b_{15}b_{16}+8c_{15}c_{16}=0$

so by (5) and division by 4 we have

$$a_{15}(2a_{16}+1)+2c_{15}c_{16}=0,$$

which forces a_{15} to be even and thus, by (5) again

$$a_{15}=0,\ c_{15}=\pm 1; \tag{6}$$

$[x_2y_3^2]$ $8a_6a_{15}+4b_6b_{15}+8c_6c_{15}=0$

so by (5) and (6)

$$c_6=0; \tag{7}$$

$[x_2^2]$ $4a_{11}^2+2b_{11}^2+4c_{11}^2=2$

so

$$a_{11}=c_{11}=0,\ b_{11}=\pm 1; \tag{8}$$

$[x_2^2y_3]$ $8a_6a_{11}+4b_6b_{11}+8c_6c_{11}=0$

so by (8)

$$b_6=0. \tag{9}$$

Finally we consider the coefficient of $x_2^2y_3^2$ in (1). We have

$$4a_6^2+2b_6^2+4c_6^2=8.$$

Appealing to (7) and (9) we obtain the required contradiction $a_6^2=2$.

Panaitopol [**5**] has shown that the only diagonal ternary quadratic forms $ax^2+by^2+cz^2$ ($1\le a\le b\le c$), which represent every odd positive integer are the forms $x^2+y^2+2z^2$, $x^2+2y^2+3z^2$, and $x^2+2y^2+4z^2$. Our proof shows that the representability of odd integers by $x^2+y^2+2z^2$ and $x^2+2y^2+4z^2$ does not arise from an underlying composition law. We leave it to the reader to show also that $x^2+2y^2+3z^2$ does not possess such a composition law.

REFERENCES

1. A. A. Albert (editor), *Studies in Modern Algebra*, Vol. 2, MAA Studies in Mathematics, 1963.
2. L. E. Dickson, On quaternions and their generalizations and the history of the 8-square theorem, *Annals of Math.* **20** (1919) 155–171.
3. L. E. Dickson, *Modern Elementary Theory of Numbers,* The University of Chicago Press, Chicago, Illinois, 1947.
4. I. Kaplansky, Ternary positive quadratic forms that represent all odd positive integers, *Acta Arith.* **70** (1995) 209–214.
5. L. Panaitopol, On the representation of natural numbers as sums of squares, *Amer. Math. Monthly* **112** (2005) 168–171.
6. A. R. Rajwade, *Squares*, London Mathematical Lecture Note Series 171, Cambridge University Press, 1993.