PRODUCTS OF SUMS OF SQUARES

There are several delightful formulas that write the product of sums of squares as other sums of squares. We prove the two most important examples here by simple complex number arguments.

_Sums of two squares_ For any real numbers $a, b, c, d$ we have

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$  

Of course it is trivial to check this by algebra, but note how it arises by complex numbers. Let $\alpha = a + ib, \gamma = c + id$. Recall that complex conjugation is given by $(x + iy)^* = x - iy$ and that $zz^* = |z|^2$. We now have

$$(a^2 + b^2)(c^2 + d^2) = \alpha\gamma\gamma^* = (\alpha\gamma^*)(\alpha\gamma)^*.$$  

But $\alpha\gamma^* = (ac + bd) + i(bc - ad)$. The required formula is immediate.

_Sums of four squares_ For any real numbers $a, b, c, d, e, f, g, h$ we have

$$(a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) = (ae - bf + cg - dh)^2 + (af + be + ch + dg)^2 + (ag + bh - ce - df)^2 + (-ah + bg + cf - de)^2.$$  

It is less trivial to check this by algebra — or to discover it! To derive it by complex numbers, we write

$$\alpha = a + ib, \quad \gamma = c + id, \quad \epsilon = e + if, \quad \zeta = g + ih.$$  

We now have

$$(a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) = (\alpha\epsilon^* + \gamma\zeta^*)(\epsilon\epsilon^* + \zeta\zeta^*) = \alpha\epsilon\epsilon^* + \gamma\zeta^* \zeta^* + \alpha\zeta\epsilon^* + \gamma\epsilon\epsilon^* = (\alpha\epsilon + \gamma\zeta)(\alpha\epsilon + \gamma\zeta)^* + (\alpha\epsilon^* - \gamma\epsilon^*)(\alpha\epsilon^* - \gamma\epsilon^*)^*$$  

But

$$\alpha\epsilon + \gamma\zeta = (ae - bf + cg - dh) + i(af + be + ch + dg)$$  

and

$$\alpha\epsilon^* - \gamma\epsilon^* = (ag + bh - ce - df) + i(-ah + bg + cf - de).$$
The result is immediate.

**Remarks** The usual proof for the case of four squares occurs in the context of the algebra of *quaternions*, discovered by the Irish mathematician Hamilton, and denoted by $\mathbb{H}$. The quaternions form a four-dimensional real vector space with a (non-commutative) multiplication for which every non-zero vector has a multiplicative inverse. The basis elements are usually denoted by $1, i, j, k$ and the multiplication is determined from:

\[
i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j.
\]

Note that it follows from the above rules that

\[
ji = -k, \quad kj = -i, \quad ik = -j
\]

and this indicates the non-commutativity of the multiplication.

We may ask more generally whether we can get an equation of the form

\[
(x_1^2 + x_2^2 + \cdots + x_n^2)(y_1^2 + y_2^2 + \cdots + y_n^2) = (z_1^2 + z_2^2 + \cdots + z_n^2)
\]

where each $z_k$ is a bilinear function of the $x_i$ and $y_j$. A remarkable theorem of the German mathematician Hurwitz (1898) proves that such a formula holds if and only if $n = 1, 2, 4, 8$. The case $n = 8$ arises from the context of the Cayley numbers, where the multiplication fails to satisfy the associative law! Hurwitz’s proof is a *tour de force* of linear algebra.