PFISTER'S THEOREM ON SUMS OF SQUARES

KEITH CONRAD

1. Introduction

A classical identity in algebra is the 2-square identity:

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2. \tag{1.1}$$

This expresses a sum of two squares times a sum of two squares as another sum of two squares. It was known to Brahmagupta in the 7th century and rediscovered 1000 years later by Fermat. For example, since $5^2 = 1^2 + 2^2$ and $13 = 2^2 + 3^2$, we get

$$65 = 5 \cdot 13 = (1^2 + 2^2)(2^2 + 3^2) = (1 \cdot 2 - 2 \cdot 3)^2 + (1 \cdot 3 + 2 \cdot 2)^2 = 4^2 + 7^2.$$

A similar 4-square identity was discovered by Euler in 1748:

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \quad = \quad & (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + \\ & (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ & (x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2)^2 + \\ & (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)^2.\end{aligned}$$

This was rediscovered by Hamilton (1843) in his work on quaternions. Soon thereafter, Graves (1843) and Cayley (1845) independently found an 8-square identity: the product $(x_1^2 + \cdots + x_8^2)(y_1^2 + \cdots + y_8^2)$ equals

$$\begin{aligned}&(x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7 - x_8y_8)^2 + \\ &(x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 + x_5y_6 - x_6y_5 - x_7y_8 + x_8y_7)^2 + \\ &(x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 + x_5y_7 + x_6y_8 - x_7y_5 - x_8y_6)^2 + \\ &(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1 + x_5y_8 - x_6y_7 + x_7y_6 - x_8y_5)^2 + \\ &(x_1y_5 - x_2y_6 - x_3y_7 - x_4y_8 + x_5y_1 + x_6y_2 + x_7y_3 + x_8y_4)^2 + \\ &(x_1y_6 + x_2y_5 - x_3y_8 + x_4y_7 - x_5y_2 + x_6y_1 - x_7y_4 + x_8y_3)^2 + \\ &(x_1y_7 + x_2y_8 + x_3y_5 - x_4y_6 - x_5y_3 + x_6y_4 + x_7y_1 - x_8y_2)^2 + \\ &(x_1y_8 - x_2y_7 + x_3y_6 + x_4y_5 - x_5y_4 - x_6y_3 + x_7y_2 + x_8y_1)^2.\end{aligned}$$

This formula had been discovered about 35 years earlier, by Degen, but that was unknown to Hamilton, Cayley, and Graves. Mathematicians began searching next for a 16-square identity but results were inconclusive for a long time.

The general question we ask is: for which n is there any identity

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2 \tag{1.2}$$

where the z's are polynomials in the x's and y's? The 2-square and 4-square identities (as well as the 8-square identity of Cayley and Graves) describe the z's as simple polynomial functions of the x's and y's. More precisely, each z_i is a bilinear function of $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ in these identities for $n = 2, 4,$ and 8. In 1898, Hurwitz proved a theorem that killed this subject: if an identity of the form (1.2) holds in a field of characteristic 0, where each z_i is a bilinear function of the x's and the y's, then $n = 1, 2, 4$, or 8. (The trivial 1-square identity is $x_1^2 y_1^2 = z_1^2$ where $z_1 = x_1 y_1$.) This is called Hurwitz's 1, 2, 4, 8 theorem. Moreover, it turns out for these four values of n that the identity must be the known one up to a linear change of variables.

Hurwitz's 1, 2, 4, 8 theorem should not have ended the search for a 16-square identity. Hurwitz proved that there is no hope for an identity like (1.2) for $n = 16$ when the z's are bilinear functions of the x's and y's. But perhaps there is a 16-square identity without the z's being bilinear in the x's and y's.

In the 1960s, a 16-square identity was finally discovered [6]. This identity did not violate Hurwitz's theorem (with bilinear z's) since it involved variables in denominators. Even more generally, and without knowing about [6], Pfister [3, 4] proved that an identity like (1.2) holds when n is any power of 2, with the z's being rational functions of the x's and y's. His method was so simple that everyone was taken by surprise. A few years later, Pfister found an even easier approach to his result, and this is what we describe here (based on [5, pp. 22–24]).

2. Pfister's Theorem

The heart of Pfister's argument is the following lemma. We write $M^\top$ for the transpose of a matrix M.

Lemma 2.1. *Let F be a field. Suppose $c = c_1^2 + \cdots + c_n^2$, where n is a power of 2 and $c_i \in F$. Then there is an $n \times n$ matrix C with entries in F and first row*

$$(c_1, \ldots, c_n)$$

such that $CC^\top = C^\top C = cI_n$.

The $(1,1)$ entry of $CC^\top$ is $c_1^2 + \cdots + c_n^2 = c$. That is how the lemma will get used.

Proof. Writing $n = 2^k$, we induct on k. The case $k = 0$ is easy. For the case $k = 1$, we want to find $u, v \in F$ such that the 2×2 matrix

$$C = \begin{pmatrix} c_1 & c_2 \\ u & v \end{pmatrix}$$

satisfies

$$CC^\top = C^\top C = \begin{pmatrix} c_1^2 + c_2^2 & 0 \\ 0 & c_1^2 + c_2^2 \end{pmatrix}.$$

Well,

$$\begin{aligned} CC^\top &= \begin{pmatrix} c_1 & c_2 \\ u & v \end{pmatrix} \begin{pmatrix} c_1 & u \\ c_2 & v \end{pmatrix} \\ &= \begin{pmatrix} c_1^2 + c_2^2 & c_1 u + c_2 v \\ c_1 u + c_2 v & u^2 + v^2 \end{pmatrix}. \end{aligned}$$

Setting $u = c_2$ and $v = -c_1$ (or $u = -c_2$ and $v = c_1$) we get $CC^\top = cI_2$. The reader can check $C^\top C$ also equals cI_2.

Now suppose $k \geq 2$ and the result is true for $k - 1$. Setting $a = c_1^2 + \cdots + c_{n/2}^2$ and $b = c_{n/2+1}^2 + \cdots + c_n^2$, which are both sums of $n/2$ squares, $c = a + b$ and by induction there are $2^{k-1} \times 2^{k-1}$ matrices A and B with entries in F and respective first rows $(c_1, \ldots, c_{n/2})$ and $(c_{n/2+1}, \ldots, c_n)$ such that

$$AA^\top = A^\top A = aI_{n/2} \quad\text{and}\quad BB^\top = B^\top B = bI_{n/2}.$$

We seek a $2^k \times 2^k$ matrix C such that $CC^\top = C^\top C = cI_n = (a+b)I_n$. Generalizing the case $k = 1$, let's try to get C in the form

$$C = \begin{pmatrix} A & B \\ U & V \end{pmatrix} \tag{2.1}$$

for some $2^{k-1} \times 2^{k-1}$ matrices U and V with entries in F. What could U and V be?

When matrices are decomposed into square blocks of the same size, as in (2.1), addition and multiplication of such matrices can be carried out by working with the blocks as the "entries," taking care to remember the order of multiplication of those blocks. Therefore

$$\begin{aligned} CC^\top &= \begin{pmatrix} A & B \\ U & V \end{pmatrix}\begin{pmatrix} A^\top & U^\top \\ B^\top & V^\top \end{pmatrix} \\ &= \begin{pmatrix} AA^\top + BB^\top & AU^\top + BV^\top \\ UA^\top + VB^\top & UU^\top + VV^\top \end{pmatrix} \\ &= \begin{pmatrix} (a+b)I_{n/2} & AU^\top + BV^\top \\ UA^\top + VB^\top & UU^\top + VV^\top \end{pmatrix}. \end{aligned}$$

The off-diagonal blocks are transposes of each other, so we have $CC^\top = cI_n$ provided

$$AU^\top + BV^\top = O \quad\text{and}\quad UU^\top + VV^\top = cI_{n/2}. \tag{2.2}$$

As in the 2×2 case, take $U = B$. Then the first equation implies $V = -BA^\top(B^{-1})^\top$ if B is invertible. Is B invertible? Since $BB^\top = bI_{n/2}$ if $b \neq 0$ then B is invertible. Could $b = 0$? If $c \neq 0$ then the equation $c = a + b$ shows at least one of a or b is nonzero, so we can suppose $b \neq 0$ by swapping the roles of a and b (and thus also A and B) at the beginning if necessary. If $c = 0$ then it could happen that $b = 0$ and we'll address this case later.

When $c \neq 0$, so we can choose $b \neq 0$ and thus make B invertible, let's check the above choices for U and V work:

$$\begin{aligned} UU^\top + VV^\top &= BB^\top + (-BA^\top(B^{-1})^\top)(-B^{-1}AB^\top) \\ &= BB^\top + BA^\top(B^\top)^{-1}B^{-1}AB^\top \\ &= bI_{n/2} + BA^\top(BB^\top)^{-1}AB^\top \\ &= bI_{n/2} + BA^\top(bI_{n/2})^{-1}AB^\top \\ &= bI_{n/2} + (1/b)BA^\top AB^\top \\ &= bI_{n/2} + (1/b)B(aI_{n/2})B^\top \\ &= bI_{n/2} + (a/b)BB^\top \\ &= bI_{n/2} + aI_{n/2} \\ &= cI_{n/2}. \end{aligned}$$

Therefore $CC^\top = cI_n$. Since $c \neq 0$, C is invertible, so the equation $C^\top C = cI_n$ follows automatically (a matrix C and its inverse, in this case $(1/c)C^\top$, always commute).

Showing C exists if $c = 0$ is almost wholly a technicality. It is possible in this case that both a and b vanish. Consider $F = \mathbf{C}$ and $0 = (1^2 + i^2) + (1^2 + i^2)$. However, in this example there is a rearranged half-sum decomposition with nonzero b (and a), namely $0 = (1^2 + 1^2) + (i^2 + i^2)$. More generally, if

$$0 = c_1^2 + c_2^2 + \cdots + c_n^2$$

where n is a power of 2 (or n is any positive even integer), then either some half-sum of terms is nonzero or the numbers $c_1^2, \ldots, c_n^2$ are all equal. Indeed, if every half-sum of terms is zero then the sum of the first $n/2$ squares is 0 and the sum of the first $n/2 - 1$ squares added to $c_{n/2+1}^2$ is 0, so after subtraction we get $c_{n/2}^2 = c_{n/2+1}^2$. By a similar argument all c_j^2 are equal.

When $c = 0$ and one of the half-sums is nonzero, take such a half-sum to be b and run through the above argument with U and V as defined before. (Now, since C is not invertible, you really have to check directly that $C^\top C = cI_n$ rather than deduce it from $CC^\top = cI_n$. This is left to the reader.)

When $c = 0$ and all c_j^2 are equal, we get $0 = c_1^2 + \cdots + c_n^2 = nc_1^2$. Recall $n = 2^k$ is a power of 2. Therefore when F does not have characteristic 2, $c_1 = 0$ (so each c_j is 0) and we can take for C the zero matrix. When F has characteristic 2, let C be the matrix whose rows all equal $(c_1, \ldots, c_n)$. Then each entry of $CC^\top$ is $\sum c_j^2 = 0$, so $CC^\top = O = cI_n$. Multiplying out $C^\top C$, its (i, j) entry is nc_ic_j, which vanishes since $n = 0$ in F. Thus $C^\top C = O = cI_n$ too. □

Theorem 2.2 (Pfister)**.** *In any field, the set of sums of n squares is closed under multiplication when n is a power of 2.*

Proof. Let the field be F. Suppose x and y in F can be written as sums of n squares:

$$x = x_1^2 + \cdots + x_n^2 \quad \text{and} \quad y = y_1^2 + \cdots + y_n^2$$

with $x_i, y_i \in F$. In Lemma 2.1, choose $n \times n$ matrices X and Y with entries in F such that

$$XX^\top = X^\top X = xI_n \quad \text{and} \quad YY^\top = Y^\top Y = yI_n,$$

with the first row of X being $(x_1, \ldots, x_n)$ and the first row of Y being $(y_1, \ldots, y_n)$. Then

$$(XY)(XY)^\top = XYY^\top X^\top = yXX^\top = xyI_n.$$

Let the first row of XY be denoted $(z_1, \ldots, z_n)$. Then $(XY)(XY)^\top$ has $(1, 1)$ entry

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

□

In the proof of Pfister's theorem, the main point was to compute the $(1, 1)$ entry, but *we needed the full matrix machinery to get it.* Using $XY^\top$ in place of XY, we can take

$$z_1 = x_1y_1 + \cdots + x_ny_n$$

but we are not assured that the other z_i's will be bilinear functions of the x's and y's. Since $(z_1, \ldots, z_n)$ can be taken as the first row of XY or $XY^\top$, we can always make each z_i linear in the x's since the first row of XY (or $XY^\top$) only involves X through its first row. Usually z_i is not linear in the y's.

Corollary 2.3. *If n is a power of 2 and $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ are independent variables over a field K, there is an algebraic identity of the form*

$$(X_1^2 + \cdots + X_n^2)(Y_1^2 + \cdots + Y_n^2) = Z_1^2 + \cdots + Z_n^2,$$

where $Z_i \in K(X_1, \ldots, X_n, Y_1, \ldots, Y_n)$.

Proof. Apply Pfister's theorem to the field $F = K(X_1, \ldots, X_n, Y_1, \ldots, Y_n)$ with $x_i = X_i$ and $y_i = Y_i$. $\square$

Corollary 2.4. *When n is any power of 2, the set of nonzero sums of n squares in any field F is a subgroup of $F^\times$.*

Proof. Pfister's theorem tells us this set is closed under multiplication. Closure under inversion follows by a simple trick: for nonzero s,

$$s = a_1^2 + \cdots + a_n^2 \Longrightarrow \frac{1}{s} = \frac{s}{s^2} = \left(\frac{a_1}{s}\right)^2 + \cdots + \left(\frac{a_n}{s}\right)^2.$$

$\square$

If we make the proof of Pfister's theorem explicit, then we see denominators are introduced from the term $-BA^\top(B^{-1})^\top$ in Lemma 2.1. Specifically, $\det B$ will be a denominator. Let's go through the proof of the theorem in early cases to see what sum of squares formulas Pfister's theorem gives us if $n = 2$ and $n = 4$.

Suppose $n > 1$ is a power of 2 and $x = \sum_{i=1}^n x_i^2$ and $y = \sum_{i=1}^n y_i^2$. The proof of Pfister's theorem says xy is a sum of squares of the entries in the first row of XY (or $XY^\top$) where X and Y are $n \times n$ matrices of the form

$$X = \begin{pmatrix} A & B \\ B & -BA^\top(B^{-1})^\top \end{pmatrix} \text{ and } Y = \begin{pmatrix} C & D \\ D & -DC^\top(D^{-1})^\top \end{pmatrix}, \tag{2.3}$$

with A being the $n/2 \times n/2$ matrix from Lemma 2.1 that corresponds to $\sum_{i=1}^{n/2} x_i^2$, B being the $n/2 \times n/2$ matrix from Lemma 2.1 that corresponds to $\sum_{i=n/2+1}^{n} x_i^2$, and likewise for C and C with $\sum_{i=1}^n y_i^2$. (Here, for simplicity, we assume the half-sums in their initial order are nonzero, which is certainly the case if the x_i's and y_i's are independent indeterminates.)

Take $n = 2$, with $x = x_1^2 + y_1^2$ and $y = y_1^2 + y_2^2$. Matrices of size $n/2 \times n/2$ are just numbers, so they commute and equal their transposes. Then (2.3) becomes

$$X = \begin{pmatrix} x_1 & x_2 \\ x_2 & -x_1 \end{pmatrix} \text{ and } Y = \begin{pmatrix} y_1 & y_2 \\ y_2 & -y_1 \end{pmatrix},$$

and the sum of squares formula for xy using XY is $(x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2$. This is just a slight variation on the classical identity (1.1).

Now let $n = 4$, $x = \sum_{i=1}^4 x_i^2$, and $y = \sum_{i=1}^4 y_i^2$. Using the case $n = 2$ to build 2×2 matrices corresponding to the half-sums $x_1^2 + x_2^2$ and $x_3^2 + x_4^2$, Lemma 2.1 gives us a 4×4 matrix X that has first row (x_1, x_2, x_3, x_4) and satisfies $XX^\top = X^\top X = xI_4$:

$$X = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & -x_1 & x_4 & -x_3 \\ x_3 & x_4 & w_1/d & w_2/d \\ x_4 & -x_3 & w_2/d & -w_1/d \end{pmatrix},$$

where $w_1 = x_1(-x_3^2 + x_4^2) - 2x_2x_3x_4$, $w_2 = x_2(x_3^2 - x_4^2) - 2x_1x_3x_4$, and $d = x_3^2 + x_4^2$. An analogous 4×4 matrix Y is built from $\sum_{i=1}^4 y_i^2$. Then $(\sum_{i=1}^4 x_i^2)(\sum_{i=1}^4 y_i^2) = \sum_{i=1}^4 z_i^2$, where (z_1, z_2, z_3, z_4) is the first row of the matrix product XY. Explicitly,

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4, \quad z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3,$$

$$\begin{aligned} z_3 &= x_1y_3 + x_2y_4 + x_3\frac{y_1(-y_3^2+y_4^2) - 2y_2y_3y_4}{y_3^2+y_4^2} + x_4\frac{y_2(y_3^2-y_4^2) - 2y_1y_3yy_4}{y_3^2+y_4^2} \\ z_4 &= x_1y_4 - x_2y_3 + x_3\frac{y_2(y_3^2-y_4^2) - 2y_1y_3y_4}{y_3^2+y_4^2} + x_4\frac{y_1(y_3^2-y_4^2) + 2y_2y_3y_4}{y_3^2+y_4^2}. \end{aligned}$$

(As a reality check, compute $(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)-(z_1^2+z_2^2+z_3^2+z_4^2)$ with the above definitions of z_1, z_2, z_3, z_4 on a computer algebra system and check the answer is 0; watch out for sign errors.) Unlike Euler's 4-square identity, Pfister's 4-square identity has denominators in z_3 and z_4.

3. A Converse to Pfister's Theorem

When n is a power of 2, Pfister's theorem shows the nonzero sums of n squares in every field form a group under multiplication. What if n is not a power of 2? Of course in *some* fields the nonzero sums of n squares will be a group under multiplication for any $n \geq 1$, such as in $\mathbf{R}$, where the nonzero sums of n squares are the same thing as the positive real numbers. It turns out, though, that for any $n \geq 1$ that is not a power of 2 there is some field in which the nonzero sums of n squares are not a group. In fact, there is a field that settles this problem for all such n.

Theorem 3.1 (Pfister)**.** *In the field $\mathbf{R}(X_1, X_2, X_3, \dots)$, for every positive integer n that is not a power of 2 the nonzero sums of n squares are not closed under multiplication.*

Proof. For any field K, let $S_K(n)$ be the set of nonzero sums of n squares. Pfister [3] showed that $S_K(\ell)S_K(m) = S_K(\ell \circ m)$ where

$$\ell \circ m = \min\{k \geq 1 : (x+y)^k = 0 \text{ in } \mathbf{F}_2[x,y]/(x^\ell, y^m)\}$$

Since each monomial in the expansion of $(x+y)^{\ell+m-1}$ is divisible by x^ℓ or y^m, we have $\ell \circ m \leq \ell + m - 1$. As examples, $3 \circ 3 = 4$ and $3 \circ 5 = 7$. When n is a power of 2 we have $n \circ n = n$, which implies as a special case that nonzero sums of n squares are closed under multiplication when n is a power of 2. When n is not a power of 2, some intermediate binomial coefficient $\binom{n}{i}$ for $0 < i < n$ is odd, so $(x+y)^n \neq 0$ in $\mathbf{F}_2[x,y]/(x^n, y^n)$. Therefore $n \circ n > n$.

Generalizing a result of Cassels [1], Pfister [3] showed that if -1 is not a sum of squares in a field K then $X_1^2 + \cdots + X_n^2$ is not a sum of $n-1$ squares in $K(X_1, \dots, X_n)$. Since -1 is not a sum of squares in $\mathbf{R}(X_{n+1}, X_{n+2}, \dots)$, it follows that $X_1^2 + \cdots + X_n^2$ is not a sum of $n-1$ squares in $\mathbf{R}(X_{n+1}, X_{n+2}, \dots)(X_1, \dots, X_n) = \mathbf{R}(X_1, X_2, X_3, \dots)$. Call this field F, so $S_F(n-1) \subsetneq S_F(n)$ for all $n \geq 2$ by the example of $X_1^2 + \cdots + X_n^2$. Therefore

$$S_F(1) \subsetneq S_F(2) \subsetneq \cdots \subsetneq S_F(n-1) \subsetneq S_F(n) \subsetneq \cdots,$$

so if $m < n$ then $S_F(m) \subsetneq S_F(n)$. When n is not a power of 2, so $n < n \circ n$, we have $S_F(n) \subsetneq S_F(n \circ n)$. Therefore $S_F(n) \subsetneq S_F(n)S_F(n)$, which says there is a product of two sums of n squares in F that is not a sum of n squares in F. □

What can be said about sums of n squares being closed under multiplication in rings, not just fields?

Theorem 3.2. *If the sums of n squares in every commutative ring are closed under multiplication then $n = 1, 2, 4,$ or 8.*

Proof. Our argument is taken from [2, pp. 278–279].

We will work in the particular ring $A = \mathbf{R}[X_1, \dots, X_n, Y_1, \dots, Y_n]$. Set $u = X_1^2 + \cdots + X_n^2$ and $v = Y_1^2 + \cdots + Y_n^2$. Assuming sums of n squares in A are closed under multiplication, uv is a sum of n squares in A, so there is an algebraic identity

$$(X_1^2 + \cdots + X_n^2)(Y_1^2 + \cdots + Y_n^2) = f_1^2 + \cdots + f_n^2 \tag{3.1}$$

for some polynomials $f_1, \dots, f_n \in \mathbf{R}[X_1, \dots, X_n, Y_1, \dots, Y_n]$.

We will show $f_1, \dots, f_n$ are each bilinear in the X_i's and Y_j's, so $n = 1, 2, 4$, or 8 by the Hurwitz 1, 2, 4, 8 theorem.

First note that by setting all variables equal to 0 in (3.1) we see that $f_1, \dots, f_n$ all have constant term 0. (This uses a special feature of $\mathbf{R}$: a sum of squares is 0 only when each term is 0.) Writing each of $f_1, \dots, f_n$ as a sum of homogeneous polynomials in $X_1, \dots, X_n$ (with coefficients in $\mathbf{R}[Y_1, \dots, Y_n]$), let d be the largest degree of such a term, so $d \geq 1$. Write $f_{i,d}$ for the homogeneous X-term in f_i of degree d, so $f_{i,d} \neq 0$ for some i. If $d > 1$ then equating the homogeneous X-terms of degree $2d$ on both sides of (3.1) implies $0 = \sum_{i=1}^{n} f_{i,d}^2$, so each $f_{i,d}$ is 0, which is a contradiction. Therefore $d = 1$, so each f_i is linear in $X_1, \dots, X_n$ with coefficients in $\mathbf{R}[Y_1, \dots, Y_n]$. By symmetry, each f_i is also linear in $Y_1, \dots, Y_n$ with coefficients in $\mathbf{R}[X_1, \dots, X_n]$. Thus each f_i is bilinear in the X_i's and Y_j's, so we are done by the $1, 2, 4$, 8 theorem.

□

It we look instead at the *units* in a ring that are sums of n squares (not necessarily of other units), then such units being closed under multiplication also implies n is 1, 2, 4, or 8. This is a theorem of Dai, Lam, and Milgram and uses algebraic topology. See [2] or [7, Prop. A.2].

References

[1] J. W. S. Cassels, "On the representation of rational functions as sums of squares," *Acta Arith.* **9** (1964), 79–82.

[2] Z. D. Dai, T. Y. Lam, and R. J. Milgram, "Application of Topology to Problems on Sums of Squares," *L'Enseign. Math.* **27** (1981), 277–283.

[3] A. Pfister, "Zur Darstellung von −1 als Summe von Quadraten in einem Körper," *J. London Math. Soc.* **40** (1965), 159–165.

[4] A. Pfsiter, "Multiplikative quadratische Formen," *Arch. Math.* **16** (1965), 363–370.

[5] A. R. Rajwade, *Squares*, Cambridge Univ. Press, Cambridge, 1993.

[6] H. Zassenhaus and W. Eichhorn, "Herleitung von Acht- und Sechzehn-Quadrate-Identitäten mit Hilfe von Eigenschaften der verallgemeinerten Quaternionen und der Cayley–Dicksonchen Zahlen," *Arch. Math.* **17** (1966), 492–496.

[7] D. B. Shapiro, *Compositions of Quadratic Forms*, W. de Gruyter, Berlin, 2000.