J. Eur. Math. Soc. 18, 1495–1513 © European Mathematical Society 2016

DOI 10.4171/JEMS/620

Claus Scheiderer

Sums of squares of polynomials with rational coefficients

Received July 25, 2013 and in revised form May 4, 2014

Abstract. We construct families of explicit (homogeneous) polynomials f over $\mathbb{Q}$ that are sums of squares of polynomials over $\mathbb{R}$, but not over $\mathbb{Q}$. Whether or not such examples exist was an open question originally raised by Sturmfels. In the case of ternary quartics we prove that our construction yields all possible examples. We also study representations of the f we construct as sums of squares of rational functions over $\mathbb{Q}$, proving lower bounds for the possible degrees of denominators. For $\deg(f) = 4$, or for ternary sextics, we obtain explicit such representations with the minimum degree of the denominators.

Keywords. Sums of squares, rational coefficients, Hilbert's 17th problem, real plane quartics, exact positivity certificates, semidefinite programming

Introduction

Let $f(x_1, \ldots, x_n)$ be a polynomial with rational coefficients, and assume that f is a sum of squares of polynomials with real coefficients. A few years ago, Sturmfels raised the question whether f is necessarily a sum of squares of polynomials with rational coefficients. The main result of this paper gives a negative answer.

The background for the question comes from semidefinite programming (see e.g. [22], [7], [15], [1]) and more specifically, from polynomial optimization. Lasserre's method of moment relaxation [13] gives, in principle, positivity certificates for real polynomials based on sum-of-squares decompositions. However, even if the initial data is exact, e.g. given by polynomials with rational coefficients, the algorithm produces floating point solutions, and therefore the output is not necessarily reliable. One would like to understand to what extent one can expect exact certificates (see for instance [17], [12]). The question by Sturmfels addresses this issue in its most basic form.

From general facts, it is clear that f has a sum-of-squares representation over some real number field K. So far, it was known by work of Hillar [11] that the question has a positive answer when K is totally real. Under this assumption, Hillar also gave a bound

C. Scheiderer: Fachbereich Mathematik and Statistik, Universität Konstanz, D-78457 Konstanz, Germany;
e-mail: claus.scheiderer@uni-konstanz.de, URL: http://www.math.uni-konstanz.de/˜scheider

Mathematics Subject Classification (2010): Primary 14G05; Secondary 11E25, 14J70, 14P99, 90C22

for the number of squares needed over $\mathbb{Q}$, in terms of the number needed over K and of the degree of the Galois closure of K over $\mathbb{Q}$. Quarez [16] later gave a different proof to the same result and improved Hillar's bound significantly. Both proofs are constructive. In Section 1 we revisit the result and show that it is essentially an immediate consequence of well-known properties of the trace form of $K/\mathbb{Q}$. This argument is completely constructive as well. In addition it gives various new information, for instance a slight improvement of the bound found by Quarez, and the fact that these bounds hold in the non-Galois case as well. The generalization to weighted sums of squares (Proposition 1.6) is new.

In Section 2 we present a general and explicit construction that gives a negative answer to the question by Sturmfels. Working with homogeneous polynomials (forms) we construct, for any integer $n \geq 2$ and any even number $d \geq 4$, a family of forms $f \in \mathbb{Q}[x_0, \dots, x_n]$ of degree d that are sums of two squares of forms over $\mathbb{R}$, but not sums of squares of forms over $\mathbb{Q}$ (Theorem 2.1). The forms we construct are the $K/\mathbb{Q}$-norms of linear forms defined over suitable number fields K of degree d. As a by-product, we show for any real number field k that there is no analogue of Hilbert's theorem on nonnegative ternary quartics (the qualitative part): There always exists a nonnegative ternary quartic form with coefficients in $\mathbb{Q}$ that is not a sum of squares of forms over k (Corollary 2.11).

Any nonnegative form $f \in \mathbb{Q}[x_0, \dots, x_n]$ is a sum of squares of rational functions over $\mathbb{Q}$, according to Artin. In Section 3 we study such representations for the family of examples constructed in Section 2. If f is such a form with $\deg(f) = d$, we prove (Theorem 3.3) that there always exists a nonzero form h over $\mathbb{Q}$ of degree $d-2$, but not of any smaller degree, for which fh is a sum of squares over $\mathbb{Q}$. In fact, we explicitly construct all such forms h of degree $d-2$ (Proposition 3.4). The form f can be chosen to be strictly positive (Corollary 3.6). In particular, for $d = 4$ or $(n, d) = (2, 6)$, we get an explicit representation of f as a sum of squares of rational functions over $\mathbb{Q}$ à la Artin.

In Section 4 we prove a partial converse to the construction from Section 2. In the case $(n, d) = (2, 4)$ of ternary quartics, we show that every nonnegative form f over $\mathbb{Q}$ that fails to be a sum of squares over $\mathbb{Q}$ arises from our construction (Theorem 4.1). For this we relate the set of sum-of-squares decompositions of f over $\mathbb{R}$ to the real singularities of the curve $f = 0$. At the end of the paper we collect a few open questions.

1. Descending sum-of-squares representations in totally real extensions

Let $f \in \mathbb{Q}[x_1, \dots, x_n] = \mathbb{Q}[\mathrm{x}]$ be a polynomial, and assume that f is a sum of squares of polynomials in $K[\mathrm{x}]$ where K is a real number field. In this section we review the result of Hillar [11] according to which f is a sum of squares in $\mathbb{Q}[\mathrm{x}]$. We will show that it is a simple consequence of properties of the trace form of $K/\mathbb{Q}$. As a consequence, we will generalize the bound of Quarez [16] to the case where $K/\mathbb{Q}$ is not necessarily Galois.

1.1. Before giving the actual proof, which is very short, we need to recall a few facts about trace quadratic forms. Let K/k be a finite separable field extension of degree $d := [K : k]$, and consider the quadratic form

$$\tau \colon K \to k, \quad y \mapsto \mathrm{tr}_{K/k}(y^2),$$

over k, where $\mathrm{tr}_{K/k}$ denotes the trace of K over k. The trace form τ has the following well-known property: For any ordering P of k, the Sylvester signature of τ with respect to P is equal to the number of extensions of the ordering P to K (see [18, Theorem 3.4.5]).

Assume that k is real and that every ordering of k has $d = [K : k]$ different extensions to K, or equivalently, every ordering of k extends to the Galois hull of K over k. Then τ is positive definite with respect to every ordering of k. Diagonalizing τ therefore gives sums of squares $a_1, \dots, a_d$ in k^* together with a k-linear basis $y_1, \dots, y_d$ of K such that $\mathrm{tr}_{K/k}(y_i y_j) = \delta_{ij} a_i$ for $1 \le i, j \le d$. Note that we can choose $a_1 = d$ here by starting the diagonalization with $y_1 = 1$. Therefore, if A is an arbitrary (commutative) k-algebra and $A_K = A \otimes_k K$, then

$$\mathrm{tr}_{A_K/A}\Big(\Big(\sum_{i=1}^{d} x_i \otimes y_i\Big)^2\Big) = \sum_{i=1}^{d} a_i x_i^2$$

for all $x_1, \dots, x_n \in A$.

The following theorem is now a simple observation. It sharpens the results of Hillar [11] and Quarez [16]:

Theorem 1.2. *Let K/k be an extension of real fields of degree $d = [K : k] < \infty$, and assume that every ordering of k extends to d different orderings of K. Then there exist sums of squares $c_1, \dots, c_d$ in k with $c_1 = 1$ and with the following property:*

For every k-algebra A, every $m \ge 1$ and every $f \in A$ which is a sum of m squares in $A_K = A \otimes_k K$, there exist $f_1, \dots, f_d \in A$ such that each f_i is a sum of m squares in A, and

$$f = \sum_{i=1}^{d} c_i f_i .$$

In particular, f is a sum of $dm \cdot p(k)$ squares in A. (*This number can be improved, see Remarks 1.4 below.*)

Here $p(k)$ denotes the Pythagoras number of k, i.e., the smallest number p such that every sum of squares in k is a sum of p squares in k. (If no such number p exists one sets $p(k) = \infty$.)

Proof of Theorem 1.2. Choose sums of squares a_i in k and elements $y_i \in K$ ($i = 1, \dots, d$) as in 1.1. It suffices to take $c_i = a_i/d$ for $i = 1, \dots, d$. Indeed, assuming $f = g_1^2 + \cdots + g_m^2$ with $g_1, \dots, g_m \in A_K$, we get

$$d \cdot f = \mathrm{tr}_{A_K/A}(f) = \sum_{j=1}^{m} \mathrm{tr}_{A_K/A}(g_j^2) = \sum_{j=1}^{m} \sum_{i=1}^{d} a_i x_{ij}^2,$$

where the $x_{ij} \in A$ are determined by $g_j = \sum_{i=1}^{d} x_{ij} \otimes y_i$ ($j = 1, \dots, m$). So the assertion of the theorem holds with $f_i = \sum_{j=1}^{m} x_{ij}^2$ ($i = 1, \dots, d$). □

Example 1.3. The proof of Theorem 1.2 is completely constructive. We get $c_1, \dots, c_d$ from diagonalizing the trace form of K/k. From a sum-of-squares decomposition of f in A_K, we explicitly find $f_1, \dots, f_d$ together with corresponding sum-of-squares decompositions in A.

To illustrate this by an example, let $p(t) = t^4 - 7t^2 + 11$, and let $K = \mathbb{Q}(\alpha)$ where α is a root of $p(t)$. Since $p(t)$ is irreducible over $\mathbb{Q}$ and all its roots are real, Theorem 1.2 applies to the extension $K/\mathbb{Q}$ (which is not Galois). By linear algebra we find that $y_1 = 1$, $y_2 = \alpha$, $y_3 = 2\alpha^2 - 7$, $y_4 = 27\alpha - 7\alpha^3$ is a $\mathbb{Q}$-basis of K satisfying $\mathrm{tr}_{K/\mathbb{Q}}(y_i y_j) = a_i \delta_{ij}$ $(1 \le i, j \le 4)$, where $(a_1, a_2, a_3, a_4) = (4, 14, 20, 770)$. Therefore

$$\mathrm{tr}_{K/\mathbb{Q}}\big((a_1 y_1 + a_2 y_2 + a_3 y_3 + a_4 y_4)^2\big) = 4a_1^2 + 14a_2^2 + 20a_3^2 + 770a_4^2$$

for $a_1, \dots, a_4 \in \mathbb{Q}$. Let A be a ring containing $\mathbb{Q}$, and let $g_i = \sum_{j=0}^3 \alpha^j g_{ij} \in A_K$ with $g_{ij} \in A$ $(1 \le i \le m, 0 \le j \le 3)$. If $f = \sum_{i=1}^m g_i^2$ lies in A then $f = \frac{1}{4}\mathrm{tr}_{K/\mathbb{Q}}(f) = \frac{1}{4}\sum_{i=1}^m \mathrm{tr}_{K/\mathbb{Q}}(g_i^2)$. Expressing the α^j in terms of $y_1, \dots, y_4$ we find that

$$f = \frac{1}{4}\sum_{i=1}^m \Big((2g_{i0} + 7g_{i2})^2 + \frac{2}{7}(7g_{i1} + 27g_{i3})^2 + 5g_{i2}^2 + \frac{110}{7}g_{i3}^2\Big)$$

is an explicit representation of f as a sum of squares in A.

Remarks 1.4. 1. The *length* $l(k)$ of a field k with $\mathrm{char}(k) \ne 2$ is the smallest number r such that for all sums of squares $0 \ne a_1, \dots, a_r, b$ in k there exist $x_1, \dots, x_r \in k$ with $b = \sum_{i=1}^n a_i x_i^2$. (If no such r exists one sets $l(k) = \infty$.) See [4] for properties of this notion. In particular, it is proved there (Proposition 2.10) that any quadratic form in n variables over k which is a sum of squares of linear forms is in fact a sum of $n + l(k) - 1$ squares of linear forms. From the proof of Theorem 1.2 we therefore see that, in the general situation of this theorem, f is in fact a sum of $dm + l(k) - 1$ squares in A. When k is a number field, it follows from the Hasse–Minkowski theorem that $l(k) = 4$. Hence, in this case, f in 1.2 is a sum of $dm + 3$ squares in A.

2. Assume that k in Theorem 1.2 is a number field, so $p(k) = 4$. Using the well-known composition formula for sums of four squares, we can improve the upper bound $4dm$ in 1.2 in a different way. Indeed, $c_i f_i$ is a sum of $4\lceil m/4\rceil$ squares for every i, and is a sum of m squares for $i = 1$. So altogether f is a sum of

$$m + 4(d-1)\cdot\lceil m/4\rceil$$

squares in A. This is precisely the bound found by Quarez [16] in the case where $k = \mathbb{Q}$ and $K/\mathbb{Q}$ is Galois. Note that this bound lies between dm and $dm + 3(d-1)$. When $m \equiv 0 \pmod 4$, or for small d, this bound is a little better than the bound $dm + 3$ from item 1. In the other cases, the bound from item 1 is better.

3. Similar to the previous remark, we can use composition for sums of eight squares to obtain the general bound

$$8d\cdot\lceil p(k)/8\rceil\cdot\lceil m/8\rceil \tag{1.1}$$

for the number of squares needed to express f in A in Theorem 1.2. This number is roughly 1/8 of the bound mentioned in 1.2. When $p(k) \le 8$ and $m \equiv 0 \pmod 8$, or for small values of d (depending on k), the bound (1.1) is better than the bound in item 1.

1.5. The qualitative part of the above result extends immediately to the following more general situation. For any commutative ring B, let ΣB^2 denote the set of sums of squares in B. Let K/k be a field extension, and let A be a (commutative) k-algebra. Fix elements $h_1, \dots, h_r \in A$, and consider the so-called (pseudo) quadratic module

$$M := \left\{ \sum_{i=1}^{r} s_i h_i : s_1, \dots, s_r \in \Sigma A^2 \right\}$$

generated in A by the h_i. Similarly, let

$$M_K := \left\{ \sum_{i=1}^{r} t_i h_i : t_1, \dots, t_r \in \Sigma A_K^2 \right\}$$

be the (pseudo) quadratic module generated by M in $A_K = A \otimes_k K$. Then we have:

Proposition 1.6. *In the above situation, if K/k is a finite extension of real fields such that every ordering of k extends to $[K : k]$ different orderings of K, we have $A \cap M_K = M$.*

Proof. Let $t_1, \dots, t_r \in \Sigma A_K^2$ be such that $f := \sum_{i=1}^{r} t_i h_i$ lies in A. Taking the trace of f gives

$$f = \frac{1}{d} \sum_{i=1}^{r} \mathrm{tr}_{A_K/A}(t_i) h_i.$$

For any $i = 1, \dots, r$, the trace $\mathrm{tr}_{A_K/A}(t_i)$ lies in ΣA^2 (see 1.1), so $f \in M$. □

2. Main construction

We construct a class of forms with rational coefficients which are sums of squares over $\mathbb{R}$, but not over $\mathbb{Q}$:

Theorem 2.1. *Let $n \geq 2$, and let $d \geq 4$ be an even number. There exists a form $f \in \mathbb{Q}[x_0, \dots, x_n]$ of degree d with the following properties:*

(1) *f is irreducible over $\mathbb{Q}$, and decomposes into a product of d linear forms over $\mathbb{C}$;*
(2) *f is a sum of two squares in $\mathbb{R}[x_0, \dots, x_n]$;*
(3) *f is not a sum of any number of squares in $\mathbb{Q}[x_0, \dots, x_n]$.*

For example,

$$f = x_0^4 + x_0 x_1^3 + x_1^4 - 3x_0^2 x_1 x_2 - 4x_0 x_1^2 x_2 + 2x_0^2 x_2^2 + x_0 x_2^3 + x_1 x_2^3 + x_2^4$$

is such a form.

The idea of proof is very simple. We start with a suitable field extension $K/\mathbb{Q}$ of degree d, and take for f the $K/\mathbb{Q}$-norm of a sufficiently general linear form $l = l(x_0, \dots, x_n)$ over K. If the Galois group of the Galois hull of $K/\mathbb{Q}$ is "sufficiently large", we show that there exists no nonzero form of degree $d/2$ that vanishes at all the real zeros of f, together with their Galois conjugates over $\mathbb{Q}$. Clearly, this implies that f cannot be a sum of squares of forms over $\mathbb{Q}$.

2.2. Here are the precise details. Let K be a totally imaginary number field of degree $d = 2m$, let E be the Galois hull of $K/\mathbb{Q}$, and let $G = \mathrm{Gal}(E/\mathbb{Q})$ (resp. $H = \mathrm{Gal}(E/K)$) be the Galois group of E over $\mathbb{Q}$ (resp. of E over K). The group G acts transitively on the set $\mathrm{Hom}(K, E)$ of embeddings $K \to E$ by

$$({}^{\sigma}\varphi)(\alpha) = \sigma(\varphi(\alpha)) \quad (\alpha \in K)$$

($\sigma \in G$, $\varphi \in \mathrm{Hom}(K, E)$), thereby identifying the G-set $\mathrm{Hom}(K, E)$ with G/H. Note that $|G/H| = d$. We fix an embedding $E \subseteq \mathbb{C}$ and denote by $\tau \in G$ the restriction of complex conjugation to E. Since K is totally imaginary, τ acts on G/H without fixpoint.

2.3. We extend the G-action on E to an action on $E[\mathrm{x}] = E[x_0, \dots, x_n]$ by letting G act on the coefficients. Let $l \in K[\mathrm{x}]$ be a linear form, and let $L \subseteq \mathbb{P}^n$ be the hyperplane $l = 0$. We assume that the d Galois conjugates of L are in general position, that is, the intersection of any $r \le n+1$ of them has codimension r in $\mathbb{P}^n$ (the empty set is assigned codimension $n+1$). For example, this condition is satisfied when α is a primitive element for $K/\mathbb{Q}$ and

$$l = \sum_{i=0}^{n} \alpha^i x_i,$$

as one sees by a Vandermonde argument. We consider the form

$$f := \prod_{\sigma H \in G/H} {}^{\sigma}l = N_{K/\mathbb{Q}}(l) \tag{2.1}$$

of degree d. Clearly, f has rational coefficients and is irreducible over $\mathbb{Q}$. Moreover, since τ acts on G/H without fixpoint, we can write $G/H = \{\sigma_1 H, \dots, \sigma_d H\}$ in such a way that $\tau\sigma_i H = \sigma_{j+m} H$ for $1 \le j \le m = d/2$. Writing $l_j := {}^{\sigma_j}l$ $(j = 1, \dots, d)$ we therefore have

$$f = \prod_{i=1}^{d} l_i = \prod_{i=1}^{m} l_i \overline{l_i}$$

where bar denotes coefficientwise complex conjugation. This shows that f is a product of m quadratic forms over $\mathbb{R}$, each of which is a sum of two squares over $\mathbb{R}$. In particular, f itself is a sum of two squares in $\mathbb{R}[\mathrm{x}]$.

2.4. For $1 \le i \le d$, let L_i denote the hyperplane $l_i = 0$ in $\mathbb{P}^n$. By our assumption of general position, the $\binom{d}{2}$ pairwise intersections $M_{ij} = L_i \cap L_j$ $(1 \le i < j \le d)$ are all distinct, and are linear subspaces of $\mathbb{P}^n$ of codimension two. Exactly m of the M_{ij} are invariant under complex conjugation, namely $M_{i,m+i} = L_i \cap \overline{L}_i$ for $i = 1, \dots, m$. We say that M_{ij} is *real* if it is conjugation-invariant.

We now assume that the action of G on G/H is 2-transitive. Then G acts transitively on the set $\{M_{ij} \colon 1 \le i < j \le d\}$. We claim that f cannot be a sum of squares of forms with rational coefficients. To see this, suppose

$$f = p_1^2 + \cdots + p_r^2$$

where $p_1, \ldots, p_r \in \mathbb{Q}[\mathtt{x}]$ are forms of degree m. Each p_ν vanishes identically on the real intersections $M_{i,i+m} = L_i \cap \overline{L}_i$ $(i = 1, \ldots, m)$. By the transitivity assumption, the p_ν vanish identically on all $\binom{d}{2}$ intersections M_{ij}. But there is no nonzero form of degree m with this property. In fact, we have $m \le d-2$ since $d = 2m \ge 4$, and there is not even any nonzero such form of degree $d-2$. This follows from the next lemma, which we state in a stronger version with a view to later applications:

Lemma 2.5. *Let k be a field and $\mathtt{x} = (x_0, \ldots, x_n)$ with $n \ge 2$, and let $l_1, \ldots, l_d \in k[\mathtt{x}]$ be linear forms such that the hyperplanes $L_i = \{l_i = 0\}$ $(i = 1, \ldots, d)$ are in general position. Let I be the vanishing ideal of $\bigcup_{1 \le i < j \le d} L_i \cap L_j$ in $k[\mathtt{x}]$. Then I is generated by the d forms*

$$p_i := \frac{l_1 \cdots l_d}{l_i} \qquad (i = 1, \ldots, d)$$

of degree $d-1$.

In particular, for $d \ge 3$ there is no hypersurface of degree $d-2$ containing $L_i \cap L_j$ for all $1 \le i < j \le d$.

Proof of Lemma 2.5. The assertion is obviously true for $d \le 2$, so we can assume that $d \ge 3$ and the assertion is proved for smaller values of d. Clearly $p_1, \ldots, p_d \in I$. Let $g \in I$ be a form. Since $L_1 \cap L_2, \ldots, L_1 \cap L_d$ are distinct hypersurfaces in L_1, and since g vanishes on all of them, we see that g is a multiple of $l_2 \cdots l_d = p_1$ modulo l_1, that is, $g = g_1 p_1 + l_1 h$ with suitable forms g_1 and h. The form h vanishes on the pairwise intersections of the hypersurfaces $L_2, \ldots, L_d$. Writing $q_i := (l_2 \cdots l_d)/l_i$ for $i = 2, \ldots, d$, it follows from the inductive hypothesis that $h \in (q_2, \ldots, q_d)$. Since $l_1 q_i = p_i$ for $i = 2, \ldots, d$, we conclude $g \in (p_1, \ldots, p_d)$, as desired. □

Summarizing, we have proved:

Theorem 2.6. *Let $n \ge 2$, let $K/\mathbb{Q}$ be a totally imaginary number field of degree $d \ge 4$, and let $l \in K[x_0, \ldots, x_n]$ be a linear form whose d Galois conjugates over $\mathbb{Q}$ are in general position. If the Galois action on* $\mathrm{Hom}(K, \mathbb{C})$ *is 2-transitive, then*

$$f := N_{K/\mathbb{Q}}(l)$$

is a form of degree d with rational coefficients that is irreducible over $\mathbb{Q}$ and a sum of two squares over $\mathbb{R}$, but not a sum of any number of squares over $\mathbb{Q}$. □

2.7. Clearly, this implies the statement of Theorem 2.1: We may start with any totally imaginary number field K of degree $d \ge 4$ for which the Galois action on $\mathrm{Hom}(K, \mathbb{C})$ is 2-transitive. For example, the Galois group may act as the alternating or full symmetric group on d letters. If we pick any primitive element α of $K/\mathbb{Q}$, the form f constructed as in 2.3 has all the properties of 2.1. For the explicit form mentioned in 2.1, see the example below.

Example 2.8. To produce an explicit example, take $K = \mathbb{Q}(\alpha)$ where $\alpha^4 - \alpha + 1 = 0$. In this case the Galois group acts as the full symmetric group on the roots of $t^4 - t + 1$, as one sees by reducing modulo 2 and modulo 3. Starting with $l = x_0 + \alpha x_1 + \alpha^2 x_2$, one obtains the form f displayed after Theorem 2.1.

To see explicitly a sum-of-squares representation of f over $\mathbb{R}$, let β be a root of $t^3 - 4t - 1 = 0$ (the cubic resolvent of $t^4 - t + 1$). Then the following decomposition holds:

$$4f = \left(2x_0^2 + \beta x_1^2 - x_1x_2 + \left(2 + \frac{1}{\beta}\right)x_2^2\right)^2 - \beta\left(2x_0x_1 - \frac{x_1^2}{\beta} + \frac{2x_0x_2}{\beta} + \beta x_1x_2 - x_2^2\right)^2.$$

The cubic field $\mathbb{Q}(\beta)$ is totally real, but not Galois over $\mathbb{Q}$. Its three places send β to real numbers approximately equal to

$$-1.860805854, \quad -0.2541016885, \quad 2.114907542,$$

respectively. Therefore, the first two embeddings $\mathbb{Q}(\beta) \to \mathbb{R}$ give each a representation of f as a sum of two squares of quadratic forms over $\mathbb{R}$. These representations are defined over the real field $F = \mathbb{Q}(\sqrt{-\beta})$ of degree six. Up to equivalence, these are the only two representations of f over $\mathbb{R}$ as a sum of two squares. It can be shown that every other sum-of-squares representation of f over $\mathbb{R}$ is (equivalent to) a sum of four squares, and arises as a convex combination of the two extremal representations.

Remark 2.9. For the conclusion of Theorem 2.6, it is not necessary that G acts 2-transitively on G/H, or equivalently, that G acts transitively on the set $\{M_{ij} : 1 \le i < j \le d\}$ (see 2.4). It suffices that any G-orbit in this set contains at least one space M_{ij} which is real, i.e., invariant under complex conjugation τ. In terms of the G-action on G/H, this means the following condition (we use the notation from 2.2–2.4):

(∗) *For any x, $y \in G/H$ with $x \neq y$ there exist $z \in G/H$ and $\sigma \in G$ such that $x = \sigma z$ and $y = \sigma\tau z$.*

For $d = |G/H| = 4$, condition (∗) implies 2-transitivity of G on G/H. But for $d \ge 6$ there are examples where G satisfies (∗) without being 2-transitive. The simplest such example is given by the group G of rotations of a regular cube P, acting on the set F of (two-dimensional) faces. (So G is isomorphic to S_4, the symmetric group on four letters, and H corresponds to the cyclic subgroup generated by a 4-cycle in S_4.) A pair $\{f, f'\}$ of different faces of P consists either of two faces with a common edge, or of two opposite faces. Hence there are exactly two G-orbits in the set $\binom{F}{2}$ of pairs of faces. The involution τ is the rotation of order two around an axis that joins the midpoints of two opposite edges. Among the three pairs $\{f, \tau f\}$ $(f \in F)$ of faces, one consists of opposite faces, while the other two consist of adjacent faces. So each pair of faces is G-conjugate to a pair of the form $\{f, \tau f\}$.

An example of a (totally imaginary) number field which realizes this Galois action on its set of places is $k = \mathbb{Q}(\alpha)$ with

$$\alpha^6 - \alpha^5 + 2\alpha^4 + \alpha^3 + 2\alpha^2 + 3\alpha + 1 = 0.$$

The example was found by consulting the Bordeaux number field tables [5].

Remark 2.10. We can easily extend Theorem 2.1 to real number fields other than $\mathbb{Q}$. Indeed, let K, E, l, f etc. be as in 2.3, and assume that $G = \mathrm{Gal}(E/\mathbb{Q})$ acts 2-transitively on $\mathrm{Hom}(K, E)$. Let k be any number field with at least one real place, and consider the natural embedding ϕ from $\mathrm{Gal}(kE/k)$ into G, induced by restriction of automorphisms. Then ϕ is surjective if (and only if) $E \cap k = \mathbb{Q}$, that is, if E and k are linearly disjoint over $\mathbb{Q}$. Assuming that this is the case, we claim that f is not a sum of squares over k. Indeed, by the argument in 2.4, the $\binom{d}{2}$ intersections $M_{ij} = L_i \cap L_j$ are all Galois conjugate to each other over k. If there were an identity $f = p_1^2 + \cdots + p_r^2$ with forms $p_\nu \in k[\mathrm{x}]$, the p_ν would have to vanish on the union of the M_{ij}, which is again impossible by Proposition 2.5.

Using this way of reasoning, we conclude:

Corollary 2.11. *Let k be any fixed number field with at least one real place, let $n \geq 2$ and $d \geq 4$ be even. Then there exists a form $f \in \mathbb{Q}[x_0, \dots, x_n]$ of degree d which is a sum of two squares of forms over $\mathbb{R}$, but not a sum of squares of forms over k.*

In particular, over a real number field there is no analogue of Hilbert's theorem [9] over $\mathbb{R}$, according to which every nonnegative ternary quartic form is a sum of squares of quadratic forms.

Proof of Corollary 2.11. Given k, it suffices by 2.10 to find a totally imaginary extension $K/\mathbb{Q}$ with Galois hull $E/\mathbb{Q}$ for which $G = \mathrm{Gal}(E/\mathbb{Q})$ acts 2-transitively on $\mathrm{Hom}(K, E)$, and such that E and k are linearly disjoint. The latter will certainly be the case if the discriminants of E and k are relatively prime. So the assertion follows from the next lemma. ◻

Lemma 2.12. *For any finite set S of primes and any even number d, there exists a totally imaginary number field $K/\mathbb{Q}$ of degree d with Galois hull $E/\mathbb{Q}$ such that the discriminant of E is not divisible by any prime in S, and $\mathrm{Gal}(E/\mathbb{Q})$ is 2-transitive on $\mathrm{Hom}(K, E)$.*

Proof. We claim that it suffices to find a monic polynomial $g(t)$ over $\mathbb{Z}$ of degree d with the following properties: (1) g is positive definite; (2) the discriminant of g is not divisible by any prime in S; (3) there exist primes p, q such that g mod p is irreducible and g mod q is a linear factor times an irreducible polynomial. Indeed, given such a g, let $K = \mathbb{Q}(\alpha)$ where α is a root of g, and let E be the Galois hull of K. Then K has the required properties. In particular, the action of $G = \mathrm{Gal}(E/\mathbb{Q})$ on the roots of g is 2-transitive since G contains a $(d-1)$-cycle. To show the existence of such a g, observe that properties (2) and (3) can be guaranteed by arranging a particular factor decomposition of g modulo p, for finitely many primes p. Positivity can be forced by adding mt^2 for large $m > 0$, divisible by the finitely many primes involved. So it is clear that (many) polynomials g as above can be found. ◻

3. Rational denominators

3.1. Let $\mathrm{x} = (x_0, \dots, x_n)$ with $n \geq 2$, and let $f \in \mathbb{Q}[\mathrm{x}]$ be a form of degree d as constructed in Theorem 2.1. In particular, f is a sum of squares over $\mathbb{R}$, but not over $\mathbb{Q}$. By Artin's solution [3] to Hilbert's 17th problem, f is a sum of squares of rational functions over $\mathbb{Q}$. In other words, there exists a form $h \neq 0$ in $\mathbb{Q}[\mathrm{x}]$ such that both h and fh are sums of squares of forms over $\mathbb{Q}$. What can be said about the degree of such h? Is it possible to give explicit constructions for h?

These questions were raised by M.-F. Roy. We will give a complete answer for $d = 4$, and a partial answer for $d \geq 6$ (see Theorem 3.3 and Proposition 3.4).

3.2. For the following we assume the setup of Theorem 2.6. Hence $K/\mathbb{Q}$ will be a totally imaginary number field of degree $d \geq 4$, with Galois hull $E/\mathbb{Q}$. Letting $G = \mathrm{Gal}(E/\mathbb{Q})$ and $H = \mathrm{Gal}(E/H)$, we assume that the action of G on G/H is 2-transitive. (In fact, it will suffice for the following to have the weaker condition $(*)$ of 2.9 satisfied.) For convenience we fix an embedding $E \subseteq \mathbb{C}$. Let $l \in K[\mathrm{x}]$ be a linear form such that the d Galois conjugates $l = l_1, l_2, \ldots, l_d$ of l are in general position. The form

$$f = l_1 \cdots l_d = \prod_{\sigma H \in G/H} {}^{\sigma}l = N_{K/\mathbb{Q}}(l)$$

in $\mathbb{Q}[\mathrm{x}]$ satisfies the conclusions of Theorem 2.6.

Theorem 3.3. *Let f be as in 3.2.*

(a) *There exists a nonzero form $h \in \mathbb{Q}[\mathrm{x}]$ of degree $d - 2$, but not of smaller degree, for which fh is a sum of squares of forms in $\mathbb{Q}[\mathrm{x}]$.*
(b) *When $d = 4$, or when $n = 2$ and $d = 6$, the form h in* (a) *can be chosen to be a sum of squares of forms in $\mathbb{Q}[\mathrm{x}]$.*

Proof. Let $0 \neq h \in \mathbb{Q}[\mathrm{x}]$ be a form for which fh is a sum of squares of forms over $\mathbb{Q}$, say $fh = g_1^2 + \cdots + g_r^2$ with forms $g_1, \ldots, g_r \in \mathbb{Q}[\mathrm{x}]$. Let $L_i \subseteq \mathbb{P}^n$ be the hyperplane $l_i = 0$ $(i = 1, \ldots, d)$. By the same argument as in 2.4, the g_ν vanish identically on $\bigcup_{i<j}(L_i \cap L_j)$. The vanishing ideal I of this union (inside $E[\mathrm{x}]$) is generated by the forms $p_i := f/l_i$ $(i = 1, \ldots, d)$ of degree $d - 1$, by Lemma 2.5. We conclude that $\deg(g_\nu) \geq d - 1$, and hence $\deg(h) \geq d - 2$.

To prove (a), it remains to construct a form h of degree $d - 2$ for which fh is a sum of squares over $\mathbb{Q}$. This will be done in Proposition 3.4. The $d = 4$ case in assertion (b) is clear: Any h from (a), being a nonnegative quadratic form over $\mathbb{Q}$, is automatically a sum of squares of linear forms over $\mathbb{Q}$. The $(n, d) = (2, 6)$ case needs a finer argument and will be proved in 3.7 below. □

The next proposition gives a fully explicit rendering of the theorem:

Proposition 3.4. *Let f be as in 3.2. For a form $g \in \mathbb{Q}[\mathrm{x}]$ of degree $2d - 2$, the following conditions are equivalent:*

(i) *g is divisible by f and is a sum of squares of forms in $\mathbb{Q}[\mathrm{x}]$;*
(ii) *there exist $r \geq 1$ and elements $a_1, \ldots, a_r \in K$ with $a_1^2 + \cdots + a_r^2 = 0$ such that*

$$g = \sum_{\nu=1}^{r} \left(\mathrm{tr}_{K/\mathbb{Q}} \left(\frac{a_\nu f}{l} \right) \right)^2.$$

If (i) *and* (ii) *hold, then conversely every sum-of-squares representation of g in $\mathbb{Q}[\mathrm{x}]$ has the form given in* (ii)*, for suitable $a_\nu \in K$ with $\sum_\nu a_\nu^2 = 0$.*

Proof. Assume $g = g_1^2 + \cdots + g_r^2$ where $g_1, \dots, g_r \in \mathbb{Q}[x]$ are forms of degree $d-1$, and assume that g is divisible by f. As before, let $I \subseteq E[x]$ be the vanishing ideal of $\bigcup_{i<j}(L_i \cap L_j)$. By Lemma 2.5, $g_1, \dots, g_r$ are E-linear combinations of $f/l_1, \dots, f/l_d$.

Let $\mathrm{tr} = \mathrm{tr}_{K/\mathbb{Q}}$ be the trace of K over $\mathbb{Q}$. We claim that a form $g \in I$ of degree $d-1$ has $\mathbb{Q}$-coefficients if and only if $g = \mathrm{tr}(af/l)$ for some $a \in K$. Indeed, let

$$g = a_1 f/l_1 + \cdots + a_d f/l_d$$

with $a_i \in E$. Let us label the elements of G/H as $\sigma_1 H, \dots, \sigma_d H$ in such a way that $\sigma_1 = 1$ and $l_i = {}^{\sigma_i} l$ for $i = 1, \dots, d$. The forms $f/l_1, \dots, f/l_d$ are linearly independent. Therefore g lies in $\mathbb{Q}[x]$ if and only if $a_1 \in K$ and $a_i = \sigma_i(a_1)$ for $i = 1, \dots, d$, or in other words, if and only if $g = \mathrm{tr}(a_1 f/l)$ with $a_1 \in K$.

It remains to characterize when a sum of squares

$$g = \sum_{\nu=1}^{r} (\mathrm{tr}(a_\nu f/l))^2$$

with $a_1, \dots, a_r \in K$ is divisible by $f = l_1 \cdots l_d$, or equivalently, by $l = l_1$. Since

$$g = \sum_{\nu=1}^{r} \bigl(\sigma_1(a_\nu) f/l_1 + \cdots + \sigma_d(a_\nu) f/l_d\bigr)^2,$$

we see that g is divisible by l_1 if and only if $\sum_\nu a_\nu^2 = 0$. This completes the proof. □

We now show that the multiplier form h in Theorem 3.3(a) can be chosen to be strictly positive. The essential part of the argument is contained in the next lemma:

Lemma 3.5. *Under the assumptions of 3.2, assume that $a_1, \dots, a_r \in K$ span K linearly over $\mathbb{Q}$ and satisfy $\sum_{\nu=1}^{r} a_\nu^2 = 0$. Then the form*

$$h = f \sum_{\nu=1}^{r} \mathrm{tr}_{K/\mathbb{Q}} \left(\frac{a_\nu}{l}\right)^2$$

is stricly positive on $\mathbb{R}^{n+1} \setminus \{0\}$.

Proof. Since h is always nonnegative, we have to show that h has no nontrivial real zeros. We keep the notation from 3.2, and let again $G/H = \{\sigma_1 H, \dots, \sigma_d H\}$ with $\sigma_1 = 1$. Write $\mathrm{tr} = \mathrm{tr}_{K/\mathbb{Q}}$. Recall (3.4) that $h \in \mathbb{Q}[x]$ is a form of degree $d-2$, and that $fh = \sum_{\nu=1}^{r} g_\nu^2$ where $g_\nu = \mathrm{tr}(a_\nu f/l) \in \mathbb{Q}[x]$ $(\nu = 1, \dots, r)$. Let $\xi \in \mathbb{R}^{n+1}$ with $h(\xi) = 0$. Then $g_\nu(\xi) = 0$ for every $\nu = 1, \dots, r$, which means

$$\sum_{i=1}^{d} \sigma_i(a_\nu) \cdot \frac{f}{l_i}(\xi) = 0$$

for every $\nu = 1, \dots, r$. The vector $\bigl(\frac{f}{l_i}(\xi)\bigr)_{i=1,\dots,d} \in \mathbb{C}^d$ therefore lies in the kernel of the $r \times d$-matrix

$$\begin{pmatrix} \varphi_1(a_1) & \cdots & \varphi_d(a_1) \\ \vdots & & \vdots \\ \varphi_1(a_r) & \cdots & \varphi_d(a_r) \end{pmatrix}.$$

Since $a_1, \dots, a_r$ span K, this matrix has full rank d, and so $\frac{f}{l_i}(\xi) = 0$ for $i = 1, \dots, d$. Clearly, this implies $f(\xi) = 0$.

It remains to show for $0 \neq \xi \in \mathbb{R}^{n+1}$ with $f(\xi) = 0$ that $h(\xi) \neq 0$. There is an index $i \in \{1, \dots, m\}$ such that l_i and $l_{m+i} = \bar{l}_i$ vanish at ξ, and no other l_j does. So the multiplicity of f at ξ is 2. We show that fh has multiplicity 2 at ξ as well, which will imply $h(\xi) \neq 0$. Since $fh = \sum_\nu g_\nu^2$, we have to show that g_ν is nonsingular at ξ for at least one index ν. Clearly we can assume $i = 1$, so $l_i = l$. Writing $\tilde{f} = f/(l\bar{l})$, we have $\tilde{f}(\xi) \neq 0$ and $g_\nu = (a_\nu \bar{l} + \bar{a}_\nu l)\tilde{f} +$ (terms of multiplicity ≥ 2 at ξ). So we have to show $\mathrm{Re}(a_\nu \bar{l}) \neq 0$ for at least one index ν. But this follows again from the assumption $K = \sum_\nu \mathbb{Q}a_\nu$, and the proof of the lemma is complete. □

Corollary 3.6. *In Theorem 3.3, the form h in* (a) *can be chosen to be strictly positive on* $\mathbb{R}^{n+1} \smallsetminus \{0\}$.

Proof. In view of 3.5, it suffices to remark that there exist finitely many elements $a_1, \dots, a_r \in K$ with $\sum_{\nu=1}^r a_\nu^2 = 0$ which span K linearly over $\mathbb{Q}$. (This is obvious since every element of K is a sum of squares in K.) □

3.7. It remains to supply the proof of the case $(n, d) = (2, 6)$ in 3.3(b). By 3.6, there exists a strictly positive form $h \in \mathbb{Q}[\mathrm{x}]$ of degree 4 such that fh is a sum of squares over $\mathbb{Q}$. The main result of Section 4 (Theorem 4.1) implies that such an h is a sum of squares of quadratic forms over $\mathbb{Q}$. (To be sure, the results of this section are nowhere used in Section 4.)

Remark 3.8. In (a) of Theorem 3.3, we can always find a multiplier form $h \in \mathbb{Q}[\mathrm{x}]$ of degree $d - 2$ such that fh is a sum of five squares in $\mathbb{Q}[\mathrm{x}]$. This follows from 3.4, since -1 is a sum of four squares in K. If K happens to have level 2, i.e., if -1 is a sum of two squares in K, then fh can be made a sum of three squares in $\mathbb{Q}[\mathrm{x}]$. (Note that $\sqrt{-1} \notin K$ since G acts primitively on G/H, and so fh can never be made a sum of two squares in $\mathbb{Q}[\mathrm{x}]$, with $\deg(h) = d - 2$.)

Example 3.9. To illustrate the construction of 3.4, let us review the example of a ternary quartic $f \in \mathbb{Q}[x_0, x_1, x_2]$ given in Theorem 2.1 (cf. also Example 2.8). In this case, the number field $K = \mathbb{Q}(\alpha)$ with $\alpha^4 - \alpha + 1 = 0$ has level 2, as one can conclude from general facts since the prime 2 is inert in K. Explicitly, it is confirmed by the identity

$$(\alpha^2 + \alpha - 1)^2 + (\alpha^2 - \alpha)^2 + 1 = 0$$

valid in K. Writing

$$g_1 = \mathrm{tr}\left(\frac{f}{l}\right), \quad g_2 = \mathrm{tr}\left(\frac{(\alpha^2 + \alpha - 1)f}{l}\right), \quad g_3 = \mathrm{tr}\left(\frac{(\alpha^2 - \alpha)f}{l}\right)$$

(with $l = x_0 + \alpha x_1 + \alpha^2 x_2$ and $\mathrm{tr} = \mathrm{tr}_{K/\mathbb{Q}}$) we find

$$g_1 = 4x_0^3 + x_1^3 + x_2^3 + 4x_0x_2^2 - 4x_1^2x_2 - 6x_0x_1x_2,$$
$$g_2 = -4x_0^3 + 3x_1^3 + 4x_2^3 - 3x_0^2x_1 - x_0x_1^2 + x_0^2x_2 - x_0x_2^2 + 4x_1^2x_2 + 3x_1x_2^2 - 2x_0x_1x_2,$$
$$g_3 = -4x_1^3 + 3x_2^3 - 3x_0^2x_1 - 7x_0x_1^2 + 7x_0^2x_2 + 3x_0x_2^2 + 3x_1x_2^2 + 8x_0x_1x_2.$$

Expanding the sum of squares, we obtain

$$fh = g_1^2 + g_2^2 + g_3^2$$

where

$$h = 32x_0^2 + 24x_0x_1 - 8x_0x_2 + 26x_1^2 + 16x_1x_2 + 26x_2^2.$$

To write h as a sum of squares in an explicit way, we may observe

$$86h = 43(8x_0 + 3x_1 - x_2)^2 + (43x_1 + 19x_2)^2 + 1832x_2^2.$$

Remarks 3.10. 1. For $d \geq 6$, unless $(n, d) = (2, 6)$, Theorem 3.3 does not solve the question of writing f as a sum of squares of rational functions over $\mathbb{Q}$. Rather, it only gives a lower bound for the degree of the denominator in such a representation. Indeed, the multiplier form h constructed in 3.3 may not be a sum of squares of forms over $\mathbb{Q}$ (and not even over $\mathbb{R}$).

2. Even when working with real coefficients, it is very hard to estimate the degrees involved when writing a nonnegative form as a sums of squares of rational functions. Consider nonnegative forms $f \in \mathbb{R}[x_0, \dots, x_n]$ of fixed degree d. From general arguments using the Tarski–Seidenberg theorem, it is clear that there exists a number $N = N(n, d)$ such that for any such f there exists a form $h \neq 0$ with $\deg(h) \leq N$ for which h and fh are both sums of squares of forms. However, the true nature of N is a mystery. Schmid [21] proved an upper bound for $N(n, d)$ that is $(n + 1)$-fold exponential. Recent work by Lombardi–Perrucci–Roy [14] gives a uniform upper bound that is 5-fold exponential. For $n = 2$, much better upper bounds come from Hilbert's paper [10]. Lower bounds for $N(n, 4)$ were found very recently by Blekherman–Gouveia–Pfeiffer [6].

4. Ternary quartics

In this section we restrict to ternary forms of degree four. It was proved by Hilbert [9] in 1888 that every nonnegative quartic form $f \in \mathbb{R}[x_0, x_1, x_2]$ is a sum of squares of quadratic forms (and, in fact, of three squares). In Theorem 2.1 we constructed a family of quartic forms $f \in \mathbb{Q}[x_0, x_1, x_2]$ that are sums of squares over $\mathbb{R}$, but not over $\mathbb{Q}$. Now we will show that conversely every nonnegative ternary quartic $f \in \mathbb{Q}[x_0, x_1, x_2]$ that fails to be a sum of squares over $\mathbb{Q}$ arises from the construction in 2.1. More precisely, we will prove:

Theorem 4.1. *Let $f \in \mathbb{Q}[x_0, x_1, x_2]$ be a nonnegative form of degree 4 which is not a sum of squares over $\mathbb{Q}$. Then f is a product $f = l_1l_2l_3l_4$ of linear forms in $\mathbb{C}[x_0, x_1, x_2]$, the four lines $l_i = 0$ are in general position, and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set of these lines as the symmetric or alternating group on four letters.*

Remark 4.2. Before starting the proof we explain its overall strategy. Let $f \in \mathbb{Q}[x_0, x_1, x_2]$ be a nonnegative quartic form. By Hilbert's celebrated result [9], f is a sum of squares of forms over $\mathbb{R}$. The main tool of our proof is to introduce and study the linear subspace U_f of $\mathbb{R}[\mathrm{x}]$ spanned by the forms p occurring in a sum-of-squares representation $f = p^2 + p'^2 + \cdots$ of f. If the subspace U_f happens to be defined over $\mathbb{Q}$, it is easy to see that f is a sum of squares over $\mathbb{Q}$ (Lemma 4.5). By Hilbert's theorem, U_f is spanned by the p for which $f - p^2 \geq 0$. This latter formulation allows us to describe U_f by local geometric conditions around the real zeros (singularities) of f (Lemma 4.7). Working these out for isolated singularities, we show that they are conditions on the local intersection numbers of f and p (Proposition 4.10). Therefore, if f has isolated singularities, it will be a sum of squares over $\mathbb{Q}$ if the set of *real* singularities is stable under the Galois action. We apply this argument to the case where f is irreducible over $\mathbb{C}$ (4.13). It turns out that the condition on the real singularities is always satisfied with only one possible exception, namely curves with three nodes. This trinodal case can be dealt with using a different argument. It then remains to study those f that are reducible over $\mathbb{C}$. Here the essential cases are those where f is a norm from a quadratic or quartic extension of $\mathbb{Q}$. These cases are analyzed directly in 4.15 and 4.16.

In what follows, let $\mathrm{x} = (x_0, \ldots, x_n)$ with arbitrary $n \geq 1$, and denote by Σ the cone of sums of squares in $\mathbb{R}[\mathrm{x}]$. As indicated in the previous remark, the following notion will play a key role in the proof.

Definition 4.3. Given a sum of squares $f \in \Sigma$, the set

$$U_f := \{p \in \mathbb{R}[\mathrm{x}]\colon\ f - \varepsilon p^2 \in \Sigma \text{ for some } \varepsilon > 0\}$$

will be called the *characteristic subspace* for f.

Lemma 4.4. *Let* $f \in \Sigma$.

(a) *The set* $\{p \in \mathbb{R}[\mathrm{x}]\colon\ f - p^2 \in \Sigma\}$ *is convex. Hence* U_f *is a linear subspace of* $\mathbb{R}[\mathrm{x}]$.
(b) *There is a representation* $f = p_1^2 + \cdots + p_r^2$ *of* f *in which* $p_1, \ldots, p_r$ *is a linear basis of* U_f.

Proof. If $f - p_j^2 \in \Sigma$ for $j = 1, 2$, then

$$f - ((1-t)p_1 + tp_2)^2 = (1-t)(f - p_1^2) + t(f - p_2^2) + t(1-t)(p_1 - p_2)^2 \in \Sigma$$

for $0 \leq t \leq 1$, proving (a). As for (b), there is a basis $q_1, \ldots, q_r$ of U_f such that $f - q_i^2 \in \Sigma$ for $i = 1, \ldots, r$. By averaging over corresponding sum-of-squares expressions we find a representation $f = g_1^2 + \cdots + g_k^2$ in which $g_1, \ldots, g_k$ span U_f. Now diagonalizing the symmetric tensor $\sum_{i=1}^k g_i \otimes g_i \in U_f \otimes U_f$ gives the assertion. □

The reason why the characteristic subspaces will be useful here is the following lemma (which generalizes [11, Theorem 1.2]):

Lemma 4.5. *Let* $f \in \mathbb{Q}[\mathrm{x}] \cap \Sigma$, *i.e.,* f *is a polynomial with rational coefficients and is a sum of squares in* $\mathbb{R}[\mathrm{x}]$. *If the subspace* U_f *of* $\mathbb{R}[\mathrm{x}]$ *is defined over* $\mathbb{Q}$, *then* f *is a sum of squares in* $\mathbb{Q}[\mathrm{x}]$.

(If V is a $\mathbb{Q}$-vector space, a linear subspace L of $V \otimes_{\mathbb{Q}} \mathbb{R}$ is said to be *defined over* $\mathbb{Q}$ if it is spanned by $L \cap V$. Similarly for affine-linear subspaces.)

Proof. Let $U_f \subseteq \mathbb{R}[\mathrm{x}]$ be the characteristic subspace of f, let $\mathsf{S}^2 U_f$ be its second symmetric power, and let $\gamma \colon \mathsf{S}^2 U_f \to \mathbb{R}[\mathrm{x}]$ be the natural linear (product) map. Since U_f is defined over $\mathbb{Q}$, so is $\Gamma_f := \gamma^{-1}(f)$, an affine-linear subspace of $\mathsf{S}^2 U_f$. By Lemma 4.4(b), Γ_f contains an element of $\mathsf{S}^2 U_f$ that is positive definite. From density of $\mathbb{Q}$ in $\mathbb{R}$ we conclude that Γ_f also contains a positive definite element defined over $\mathbb{Q}$. In particular, f is a sum of squares over $\mathbb{Q}$. □

In the case of ternary quartics, Hilbert's theorem [9] turns the characteristic subspaces into a geometric notion:

Corollary 4.6. *Let $f \in \mathbb{R}[x_0, x_1, x_2]$ be a nonnegative form of degree 4. Then U_f is the space of quadratic forms p with $f - \varepsilon p^2 \geq 0$ for some $\varepsilon > 0$.* □

These forms are in fact characterized by local properties, according to the next lemma:

Lemma 4.7. *Let $f, g \in \mathbb{R}[\mathrm{x}] = \mathbb{R}[x_0, \ldots, x_n]$ be nonnegative forms of the same degree. Assume that for every $0 \neq \eta \in \mathbb{R}^{n+1}$ there exists $\varepsilon > 0$ for which $f - \varepsilon g$ is nonnegative in a neighborhood of η. Then there exists $\varepsilon > 0$ such that $f - \varepsilon g$ is nonnegative on $\mathbb{R}^{n+1}$.*

Proof. This follows from compactness of projective space: For any $\xi \in \mathbb{P}^n(\mathbb{R})$ there exists $\varepsilon_\xi > 0$ and a neighborhood $W_\xi \subseteq \mathbb{P}^n(\mathbb{R})$ of ξ such that $f - \varepsilon_\xi g$ is nonnegative on W_ξ. Choose finitely many points $\xi_1, \ldots, \xi_r \in \mathbb{P}^n(\mathbb{R})$ such that $\mathbb{P}^n(\mathbb{R}) = \bigcup_{i=1}^r W_{\xi_i}$, and set $\varepsilon = \min\{\varepsilon_{\xi_i} : i = 1, \ldots, r\}$. Then $f - \varepsilon g$ is everywhere nonnegative. □

4.8. From now on let $\mathrm{x} = (x_0, x_1, x_2)$, and let $\mathbb{R}[\mathrm{x}]_2$ denote the space of quadratic forms in $\mathbb{R}[\mathrm{x}]$. For a nonnegative ternary quartic $f \in \mathbb{R}[\mathrm{x}]$ with isolated real zeros we will determine the characteristic subspace U_f explicitly. (The case where the real zeros are not isolated is even easier, since it reduces to nonnegative quadratic forms.) By Lemma 4.7, it suffices to do this locally, namely to determine the subspace

$$U_{f,\xi} := \{p \in \mathbb{R}[\mathrm{x}]_2 \colon \exists \varepsilon > 0 \;\; f - \varepsilon p^2 \geq 0 \text{ around } \xi\}$$

for every $\xi \in \mathbb{P}^2(\mathbb{R})$ with $f(\xi) = 0$. Note that $U_{f,\xi}$ is also the space of all $p \in \mathbb{R}[\mathrm{x}]_2$ for which p^2/f is locally bounded around ξ in $\mathbb{P}^2(\mathbb{R})$.

4.9. Assume that ξ is an isolated real zero of a quartic form $f \in \mathbb{R}[\mathrm{x}]$. Then ξ is a singularity of the curve $f = 0$ of real type A_1^*, A_3^*, A_5^*, A_7^* or X_9^{**} (see [8]). The last two can occur only when f is reducible over $\mathbb{C}$. Here, by a (plane) A_k^* *singularity* (for $k \geq 1$ odd) we mean a real analytic singularity of type A_k whose two analytic branches are complex conjugate. See 4.11 for X_9^{**}.

Proposition 4.10. *Let $f(x, y)$, $p(x, y)$ be real analytic function germs in $(\mathbb{R}^2, 0)$, and assume that the singularity $f = 0$ is of type A_{2r-1}^* with $r \geq 1$. Then the germ p^2/f is locally bounded in $\mathbb{R}^2$ around $(0, 0)$ if and only if $i(f, p) \geq 2r$, where i denotes the local intersection number at $0 \in \mathbb{R}^2$.*

Proof. We may assume $f = y^2 + x^{2r}$, and we will show that both properties are equivalent to $\omega(p(x,0)) \ge r$, where ω is the vanishing order at $x = 0$. It is clear that p^2/f locally bounded implies $\omega(p(x,0)) \ge r$. Conversely, if $\omega(p(x,0)) \ge r$, we can write $p = yg + x^r h$ with analytic germs g, h. Then a simple calculation shows that p^2/f is locally bounded around $0 \in \mathbb{R}^2$. On the other hand, from $f = (y+ix^r)(y-ix^r)$ we can directly deduce that $\omega(p(x,0)) \ge r$ if and only if $i(f,p) \ge 2r$. □

Remark 4.11. For completeness, we add a similar characterization for X_9^{**} singularities. These facts will not be used in the arguments below. A plane real singularity of type X_9^{**} corresponds to the union of four nonreal lines through a real point (two pairs of complex conjugate lines; see [2, p. 185]). A normal form is given by $f = x^4 + y^4 + ax^2y^2$ with $a > 0$, $a \ne 2$. For a real analytic germ $p(x,y)$, the quotient p^2/f is locally bounded iff $\omega(p(x,y)) \ge 2$ iff $i(f,p) \ge 8$.

Corollary 4.12. *Let $f \in \mathbb{Q}[\mathrm{x}]$ be a nonnegative ternary quartic over $\mathbb{Q}$, let $\xi_1, \dots, \xi_r$ be isolated real zeros of f in $\mathbb{P}^2$, and assume that the set $\{\xi_1, \dots, \xi_r\}$ is invariant under the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on $\mathbb{P}^2(\overline{\mathbb{Q}})$. Then the subspace $\bigcap_{j=1}^r U_{f,\xi_j}$ of $\mathbb{R}[\mathrm{x}]_2$ is defined over $\mathbb{Q}$.*

Note that $\xi_1, \dots, \xi_r$ have coordinates in $\overline{\mathbb{Q}}$, so the Galois group acts on these points.

Proof of Corollary 4.12. By 4.10 and 4.11 (see also 4.9), there exist numbers $n_j \ge 0$ $(j = 1, \dots, r)$ such that

$$\bigcap_{j=1}^r U_{f,\xi_j} = \{p \in \mathbb{R}[\mathrm{x}]_2 \colon i_{\xi_j}(f,p) \ge n_j\},$$

and $n_j = n_k$ whenever ξ_j and ξ_k are Galois conjugate over $\mathbb{Q}$. From this the assertion is obvious. □

4.13. We now give the proof of Theorem 4.1. Let $\mathrm{x} = (x_0, x_1, x_2)$, and let $f \in \mathbb{Q}[\mathrm{x}]$ be a nonnegative form of degree 4. Let $U_f \subseteq \mathbb{R}[\mathrm{x}]_2$ be the characteristic subspace of f (see 4.3). By a case distinction we will show that f is a sum of squares over $\mathbb{Q}$ unless it meets the conditions of Theorem 4.1.

Whenever U_f is defined over $\mathbb{Q}$, f is a sum of squares over $\mathbb{Q}$ by Lemma 4.5. In particular, this is the case when f is strictly positive definite, since then $U_f = \mathbb{R}[\mathrm{x}]_2$. So we assume that f has at least one real zero. We first consider the case where f is irreducible over $\mathbb{C}$. The real zeros of f are precisely the real singular points of the curve $f = 0$. The configuration of all (real or nonreal) singularities of this curve is one of the following (see [19, 7.3]):

$$A_1^*,\ 2A_1^*,\ 3A_1^*,\ A_3^*,\ A_1^* + A_3^*,\ A_5^*,\ A_1^* + 2A_1^i,\ A_1^* + 2A_2^i.$$

(Here $2A_k^i$ denotes a pair $P \ne \overline{P}$ of complex conjugate A_k-singularities.) The singularities are permuted by the Galois action. In all cases except the last two, every singularity of f is real. By Corollary 4.12 (combined with Corollary 4.6 and Lemma 4.7), the subspace U_f is defined over $\mathbb{Q}$ in these cases, and we are done. In the case of $A_1^* + 2A_2^i$, the same is true since the unique real singularity is Galois invariant, hence defined over $\mathbb{Q}$.

It remains to consider the case where f has three nodes, one of which is real (with a pair of nonreal tangents) and the other two are complex conjugate. Here U_f consists of the quadratic forms with a zero at the real node. Unless the real node is $\mathbb{Q}$-rational, the space U_f fails to be defined over $\mathbb{Q}$. Instead we can argue as follows. For such an f, there exists a unique (up to orthogonal equivalence) representation $f = p_1^2 + p_2^2 + p_3^2$ in $\mathbb{C}[\mathrm{x}]$ for which p_1, p_2, p_3 vanish at all three nodes. Moreover, the symmetric tensor $t := \sum_{j=1}^3 p_j \otimes p_j$ is defined over $\mathbb{R}$ and is positive semidefinite. This follows from the analysis in [19] (for more details see [20, pp. 4 and 6]). Since the set of all three nodes is Galois invariant, the tensor t is defined over $\mathbb{Q}$, and hence f is a sum of squares over $\mathbb{Q}$. We have thus shown that f is a sum of squares over $\mathbb{Q}$ when f is irreducible over $\mathbb{C}$.

4.14. An explicit example of the case just discussed is the nonnegative quartic

$$f = x_0^4 + x_1^4 + x_2^4 - 2x_0^3x_1 + 2x_0x_2^3 + 2x_0^2x_1^2 + 2x_0^2x_2^2 + x_1^2x_2^2 - 4x_0^2x_1x_2 - 2x_0x_1x_2^2.$$

It has the three nodes $(1 : \alpha : \alpha^2)$ where $\alpha^3 + \alpha - 1 = 0$. These nodes are Galois conjugate to each other, and precisely one of them is real. The unique sum-of-three-squares decomposition of f vanishing at all three nodes is given by

$$f = (x_1^2 - x_0x_2)^2 + (x_1x_2 + x_0x_1 - x_0^2)^2 + (x_2^2 - x_0x_1 + x_0x_2)^2.$$

4.15. It is very easy to see that f is a sum of squares over $\mathbb{Q}$ whenever f is reducible over $\mathbb{Q}$. Hence we can assume that f is irreducible over $\mathbb{Q}$, but reducible over $\mathbb{C}$. So f is either the $K/\mathbb{Q}$-norm of a quadratic form $p \in K[\mathrm{x}]$ defined over a quadratic number field K, or the $K/\mathbb{Q}$-norm of a linear form $l \in K[\mathrm{x}]$ defined over a quartic number field K. In either case, K is generated by the coefficients of p resp. l, since otherwise f would be reducible over $\mathbb{Q}$. First consider the case $[K : \mathbb{Q}] = 2$. It is clear that f is a sum of squares over $\mathbb{Q}$ when K is imaginary. When K is real, both p and its $K/\mathbb{Q}$-conjugate p' must be nonnegative, since $f = pp'$ is nonnegative. Hence p is nonnegative with respect to every (real) place of K, and therefore p is a sum of squares over K, being a quadratic form. Now Hillar's result [11] implies that f is a sum of squares over $\mathbb{Q}$.

4.16. It remains to consider the case when $f = N_{K/\mathbb{Q}}(l)$ where $[K : \mathbb{Q}] = 4$ and $l \in K[\mathrm{x}]$ is a linear form whose coefficients generate K. When $K/\mathbb{Q}$ has a quadratic subfield $L/\mathbb{Q}$, we can write $f = N_{L/\mathbb{Q}}(N_{K/L}(l))$ and conclude that f is a sum of squares over $\mathbb{Q}$, by the argument in 4.15. So we can assume that $K/\mathbb{Q}$ has no proper intermediate field. This means that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\mathrm{Hom}(K, \overline{\mathbb{Q}})$ as the alternating or symmetric group. Let $l_i = 0$ $(i = 1, 2, 3, 4)$ be the four Galois conjugates of the line $l = 0$. When $l_1, \ldots, l_4$ fail to be in general position, all four meet in a common $\mathbb{Q}$-point. After a suitable coordinate change we are then in the case of binary forms, in which it is clear that f is a sum of squares over $\mathbb{Q}$. The proof of Theorem 4.1 is complete. □

5. Some open questions

Here are several natural questions that arise in connection with the results of this paper. Let always $\mathrm{x} = (x_0, \ldots, x_n)$.

5.1. In Theorem 2.1 we constructed forms in $\mathbb{Q}[\mathtt{x}]$ that are sums of squares of forms over $\mathbb{R}$, but not over $\mathbb{Q}$. All our examples split over $\mathbb{C}$ as products of linear forms. Are there examples that are irreducible over $\mathbb{C}$? Are there examples that are strictly positive definite, i.e., have no nontrivial real zeros? Are there examples that define a nonsingular projective hypersurface? (The last question is a common sharpening of the former two.)

Note added in proof: The first question has an easy positive answer when the number $n+1$ of homogeneous variables is at least 4. This observation is due to Fernando Galve Mauricio. With his kind permission I include his argument here:

Let $n \geq 2$, and take any form $f \in \mathbb{Q}[\mathtt{x}] = \mathbb{Q}[x_0, \dots, x_n]$ with $\deg(f) = 2m$ that splits into distinct linear forms in $\mathbb{C}[\mathtt{x}]$, and that is a sum of squares in $\mathbb{R}[\mathtt{x}]$ but not in $\mathbb{Q}[\mathtt{x}]$. Then the form $y^{2m} + f(\mathtt{x})$ in $n+2$ homogeneous variables $(\mathtt{x}, y)$ is irreducible over $\mathbb{C}$ by Eisenstein's criterion. Evidently, it is a sum of squares in $\mathbb{R}[\mathtt{x}, y]$ but not in $\mathbb{Q}[\mathtt{x}, y]$.

5.2. Let K be a real number field, and let f be a form in $\mathbb{Q}[\mathtt{x}]$ that is a sum of squares of forms over K. When K is totally real, it follows that f is a sum of squares over $\mathbb{Q}$ (Hillar [11], cf. also Section 1). Are there other sufficient conditions on K that allow the same conclusion?

5.3. More specifically, let K be a number field of odd degree, and assume that a form f over $\mathbb{Q}$ is a sum of squares over K. Is then f a sum of squares over $\mathbb{Q}$?

5.4. We may generalize the last question to arbitrary linear matrix inequalities. Thus, let $A_0, \dots, A_r$ be symmetric matrices of some size with rational entries, and assume that there exists $x = (x_1, \dots, x_r) \in K^r$ such that the matrix $A(x) := A_0 + \sum_{i=1}^r x_i A_i$ is positive semidefinite with respect to every real place of K. If $[K : \mathbb{Q}]$ is odd, does there exist $x \in \mathbb{Q}^r$ such that $A(x)$ is positive semidefinite? For $r = 1$, the answer is yes.

5.5. When $f \in \mathbb{Q}[\mathtt{x}]$ is any nonnegative form, there exists a sum of squares $h \neq 0$ of forms in $\mathbb{Q}[\mathtt{x}]$ such that fh is a sum of squares of forms in $\mathbb{Q}[\mathtt{x}]$. Assuming that f is a sum of squares of forms over $\mathbb{R}$, can we give an upper bound on $\deg(h)$, for example in terms of n and $d = \deg(f)$? Other than over $\mathbb{R}$ (3.10), there seems to be no a priori reason why a uniform such bound only in terms of n and d should exist.

Note that there is one case in which the results of this paper give an answer to this question, namely $(n, d) = (2, 4)$. Here $\deg(h) = 2$ suffices by 4.1 and 3.3.

Acknowledgments. I would like to thank Marie-Françoise Roy and Ronan Quarez for stimulating discussions. In particular, the results of Section 3 were prompted by a question of Roy. I am also grateful to Fernando Galve Mauricio for his nice argument partially answering Question 5.1.

References

[1] Anjos, M. F., Lasserre, J. B. (eds.): Handbook on Semidefinite, Conic and Polynomial Optimization. Springer (2012) Zbl 1235.90002 MR 2894661

[2] Arnol'd, V. I., Guseĭn-Zade, S. M., Varchenko, A. N.: Singularities of Differentiable Maps, Volume 1. Monogr. Math. 82, Birkhäuser, Boston (1985) Zbl 0554.58001 MR 0777682

[3] Artin, E.: Über die Zerlegung definiter Funktionen in Quadrate. Abh. Math. Sem. Univ. Hamburg **5**, 100–115 (1927) JFM 52.0122.01 MR 3069468

[4] Baeza, R., Leep, D., O'Ryan, M., Prieto, J. P.: Sums of squares of linear forms. Math. Z. **193**, 297–306 (1986) Zbl 0598.10032 MR 0856157

[5] Belabas, K.: Number field tables, generated by the Bordeaux computational number theory group (H. Cohen et al.) around 1995. Corrected version (2007). Available from pari.math.u-bordeaux1.fr/pub/pari/packages/nftables

[6] Blekherman, G., Gouveia, J., Pfeiffer, M.: Sums of squares on the hypercube. J. Amer. Math. Soc. **29**, 893–913 (2016) MR 3486176

[7] Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge Univ. Press, Cambridge (2004) Zbl 1058.90049 MR 2061575

[8] Gudkov, D. A.: On the topology of real projective algebraic varieties. Uspekhi Mat. Nauk **29**, no. 4, 3–79 (1974) (in Russian); English transl.: Russian Math. Surveys **29**, no. 4, 1–79 (1974) Zbl 0316.14018 MR 0399085

[9] Hilbert, D.: Über die Darstellung definiter Formen als Summe von Formenquadraten. Math. Ann. **32**, 342–350 (1888) JFM 20.0198.02 MR 1510517

[10] Hilbert, D.: Über ternäre definite Formen. Acta Math. **17**, 169–197 (1893) JFM 25.0319.01 MR 1554835

[11] Hillar, Ch.: Sums of squares over totally real fields are rational sums of squares. Proc. Amer. Math. Soc. **137**, 921–930 (2009) Zbl 1163.12005 MR 2457431

[12] Kaltofen, E. L., Li, B., Yang, Z., Zhi, L.: Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients. J. Symbolic Comput. **47**, 1–15 (2012) Zbl 1229.90115 MR 2854844

[13] Lasserre, J. B.: Moments, Positive Polynomials and Their Applications. Imperial College Press, London (2010) Zbl 1211.90007 MR 2589247

[14] Lombardi, H., Perrucci, D., Roy, M.-F.: An elementary recursive bound for effective Positivstellensatz and Hilbert 17-th problem. arXiv:1404.2338 (2014)

[15] Nemirovski, A.: Advances in convex optimization: conic programming. In: Int. Congress Math. (Madrid, 2006), Vol. I, Eur. Math. Soc., Zürich, 413–444 (2007) Zbl 1135.90379 MR 2334199

[16] Quarez, R.: Tight bounds for rational sums of squares over totally real fields. Rend. Circ. Mat. Palermo **59**, 377–388 (2010) Zbl 1247.12003 MR 2745518

[17] Safey El Din, M., Zhi, L.: Computing rational points in convex semialgebraic sets and sum of squares decompositions. SIAM J. Optim. **20**, 2876–2889 (2010) Zbl 1279.90127 MR 2735935

[18] Scharlau, W.: Quadratic and Hermitian Forms. Grundlehren Math. Wiss. 270, Springer, Berlin (1985) Zbl 0584.10010 MR 0770063

[19] Scheiderer, C.: Hilbert's theorem on positive ternary quartics: A refined analysis. J. Algebraic Geom. **19**, 285–333 (2010) Zbl 05702780 MR 2580677

[20] Scheiderer, C.: In how many ways is a quartic a conic of conics? Data over $\mathbb{C}$ and over $\mathbb{R}$. www.math.uni-konstanz.de/~scheider/notes/TQ.details.pdf

[21] Schmid, J.: On the degree complexity of Hilbert's 17th problem and the Real Nullstellensatz. Habilitationsschrift, Univ. Dortmund (1998)

[22] Wolkowicz, H., Saigal, R., Vandenberghe, L. (eds.): Handbook of Semidefinite Programming. Theory, Algorithms, and Applications. Kluwer, Boston (2000) Zbl 0951.90001 MR 1778223