Expository notes on sum of square of polynomials with rational coefficients

Jose Capco, Claus Scheiderer

Notation.

- $\underline{x} := x_1, \ldots, x_n$ for some $n \in \mathbb{N}$
- For a square matrix $A \in \mathbb{R}^{n\times n}$ by $A \succ 0$ and $A \succcurlyeq 0$ we mean that A is a positive definite resp. positive semidefinite symmetric matrix.
- $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$
- Let K be a field and $f \in L[\underline{x}]$ for any subfield $L \leq K$ then we write $Z_K(f)$ (or simply $Z(f)$ if K is clear) to mean the set of zeros of f that is in K^n.
- for any polynomial $f \in \mathbb{C}[\underline{x}]$ by $\bar{f}$ we mean the polynomial in $\mathbb{C}[\underline{x}]$ obtained by replacing the coefficients of f with their complex conjugates.
- Let $k \in \mathbb{N}$. We denote the cyclic group of order k by C_k i.e. $C_k \cong (\mathbb{Z}/k\mathbb{Z}, +)$. By S_k we mean the symmetric group of all permutations of $\{1, \ldots, k\}$.

Let $\underline{x} = x_1, \ldots, x_n$ with $n \geq 2$. Here we are interested in finding a multivariate polynomial $f \in (\mathbb{Q}[\underline{x}] \cap \sum \mathbb{R}[\underline{x}]^2) \setminus \sum \mathbb{Q}[\underline{x}]^2$. We call polynomials satisfying this property as polynomials satisfying *Sturmfel's condition*. We may replace $\mathbb{R}$ by any real subfield K of $\mathbb{R}$ and call it *Sturmfel's condition for* K. For $\mathbb{R}$, the problem was solved a few years ago by Claus Scheiderer in [CS]. We recall the construction discussed by Scheiderer in [CS]. It suffices to show these for forms so for the sake of simplicity we take $n = 2$ and let $\underline{x} = x_0, x_1, x_2 \ldots$

We also want to remark that all the field extension we consider are finite algebraic field extension over $\mathbb{Q}$.

Construction 1.

1. Find a non-real number field $L \geq \mathbb{Q}$ that is the splitting field of an irreducible quartic polynomial $f(t) \in \mathbb{Q}[t]$ and such that the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$ is 2-transitive (acting on the four roots) and such that its maximum real subfield is not Galois over $\mathbb{Q}$. One easy way to do this is to take the splitting field of polynomial of degree $2d$ over $\mathbb{Q}$ with non-real zeros, L, that is the Galois closure of its maximum real subfield and such that the Galois group G is isomorphic to S_{2d} (the symmetric group on $1, 2, \ldots, 2d$). The example provided in [CS] is taking L to be the splitting field of $t^4 - t + 1$.
2. Take a root α of f and consider the linear form in $L[x_0, x_1, x_2]$ defined by
$$l : x_0 + \alpha x_1 + \alpha^2 x_2$$
or in general if $n > 2$
$$l : x_0 + \alpha x_1 + \cdots + \alpha^n x_n$$
3. Find the norm of l with respect to the field extension $\mathbb{Q} \hookrightarrow L$, i.e. compute for $N_{L/\mathbb{Q}}(l)$, we shall remove the subscript of N if the field extension is clear (this will be a homogeneous polynomial of degree 4). For the particular example we had, we compute the norm to be
$$N(l) = x_0^4 + 2x_0^2x_2^2 - 3x_0^2x_2x_1 + x_0x_2^3 - 4x_0x_2x_1^2 + x_0x_1^3 + x_2^4 + x_2^3x_1 + x_1^4$$
By [Flan] the above is an irreducible polynomial in $\mathbb{Q}[x_0, x_1, x_2]$.

The construction above has the following premise that we shall use and refer very often ...

Premise 2. Let L be the splitting field of an irreducible $f \in \mathbb{Q}[t]$ with only non-real zeros $\alpha_1, \ldots, \alpha_{2d}$ for some $d \in \mathbb{N}$ with $d \geq 2$. We assume that these roots are ordered in such a way that (we use *overline* to mean complex-conjugate)

$$\alpha_{2i-1} = \overline{\alpha}_{2i} \qquad i = 1, \ldots, d$$

Furthermore, suppose that the maximum real subfield of L is not Galois over $\mathbb{Q}$. For $\underline{x} = x_0, \ldots, x_n$ we define hyperplanes in $\mathbb{P}^n(L)$ by the equations

$$l_i(\underline{x}) := x_0 + \alpha_i x_1 + \cdots + \alpha_i^n x_n$$

Finally, we also denote $G := \mathrm{Gal}(L/\mathbb{Q})$ and think of it acting on $\{1, \ldots, 2d\}$ (corresponding to the same order as the roots).

There were several open questions left by Scheiderer in the end of his paper and we intend to answer some of them.

Question 1. Can we find a polynomial $f \in (\mathbb{Q}[\underline{x}] \cap \sum \mathbb{R}[\underline{x}]^2) \setminus \sum \mathbb{Q}[\underline{x}]^2$ that do not factor into linear forms over $\mathbb{C}$? Can we find an example that is irreducible over $\mathbb{C}$?

Answer. This can be done by modifying the construction above. This can be done with any choice of imaginary number field L leading to a Galois group described above. To illustrate better we pick the result of the example given in the above construction. Above we obtained a

$$g = x_0^4 + 2x_0^2x_2^2 - 3x_0^2x_2x_1 + x_0x_2^3 - 4x_0x_2x_1^2 + x_0x_1^3 + x_2^4 + x_2^3x_1 + x_1^4$$

which is a ternary quartic with coefficients in $\mathbb{Q}$ satisfying Sturmfel's condition. Now consider the sextic form

$$f = g(x_0x_3, x_1x_4, x_2x_5) \in \mathbb{Q}[x_0, x_1, \ldots, x_5]$$

By the construction above, this is factored into irreducible quadratic forms over $\mathbb{C}$ of the form

$$x_0x_3 + \alpha x_1x_4 + \alpha^2 x_2x_5$$

This answers the first question and this can be imitated for any polynomial obtained by the above construction. In other words, we conclude that if $g = g(x_0, \ldots, x_{n-1})$ is obtained from the above construction (for any number of variables and any field extension satisfied in the construction) then the polynomial

$$f = g(x_0x_n, x_1x_{n+1}, \ldots, x_{n-1}x_{2n-1})$$

will be an answer to the first question.

For the second question. In Scheiderer's published paper he gives an elegant answer modifying a polynomial from his construction and using Eisenstein's criterion. We recall his answer: If $g(\underline{x})$ is any polynomial obtained by the above construction then one quickly sees that $g(\underline{x}) + y^{2n}$ is a polynomial that is irreducible over $\mathbb{C}$ and this can be checked using Eisenstein's criterion on polynomials (y as indeterminate) over the domain $\mathbb{C}[\underline{x}]$ with prime ideal $\langle x_0, x_1, \ldots, x_n \rangle$. Another, maybe less elegant, possibility is to specifically consider the polynomial $g(x_0, x_1, x_2)$ as above, i.e.

$$g(x_0, x_1, x_2) = x_0^4 + 2x_0^2x_2^2 - 3x_0^2x_2x_1 + x_0x_2^3 - 4x_0x_2x_1^2 + x_0x_1^3 + x_2^4 + x_2^3x_1 + x_1^4$$

and then define

$$f_1(x_0, x_1, x_2) := g(x_0, x_1, x_2)$$
$$f_2(x_3, x_4, x_5) := g(x_3, x_4, x_5)$$

for indeterminates $x_0, x_1, \ldots, x_5$. Then one checks (e.g. with computer algebra) that the 6-variable quartic form $f_1 + f_2 \in \mathbb{Q}[x_0, \ldots, x_5]$.

Lemma 1. Let K be a number field Galois over $\mathbb{Q}$ such that its maximum real subfield $L := K \cap \mathbb{R}$ is not Galois over $\mathbb{Q}$ and such that K is the Galois closure of L. Let $\alpha \in K$ is a primitive element of K, i.e. such that $K = \mathbb{Q}(\alpha)$, and suppose $f \in \mathbb{Q}[x]$ is the minimal polynomial of α. There exists an element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and a $z \in Z_K(f)$ such that $\sigma(\bar{z}) \neq \overline{\sigma(z)}$

Proof. Suppose by contradiction that the result of this lemma does not hold and denote $G := \mathrm{Gal}(K/\mathbb{Q})$. If we further denote $\tau : K \to K$ as the complex conjugate automorphism, we see that $\tau\sigma = \sigma\tau$ for any $\sigma \in G$ and so $H := \{\mathrm{id}, \tau\}$ is a normal subgroup of G. Hence, by the Fundamental Theory of Galois Theory, the field fixed by H,

$$\{a \in K \,:\, \sigma(a) = a \quad \forall \sigma \in H\}$$

is Galois over $\mathbb{Q}$. But this field is L and we initially assumed that it is not Galois over $\mathbb{Q}$. □

From the above the following corollary follows immediately

Corollary 2. Suppose that $K = \mathbb{Q}(\alpha)$ and L are the fields in the proposition above. Set $G := \mathrm{Gal}(K/\mathbb{Q})$ and let us order the underlying set of this group as

$$\{\sigma_1, \sigma_2, \ldots, \sigma_{2d}\} \qquad \sigma_1 := \mathrm{id}$$

Let $d \geq 2$ and define linear forms in $K[x, y, z]$

$$l_i := x + \sigma_i(\alpha)y + \sigma_i(\alpha^2)z \qquad i = 1, \ldots, 2d$$

We abuse notation and sometimes write $\sigma_i(l_1)$ instead of l_i. Then there exists $i \in \{1, \ldots, 2d\}$ such that $\overline{\sigma_i(l_1)} \neq \sigma_i(\overline{l_1})$

A condition (*) was given in [CS] Remark 2.9 (weaker than 2-transitive of the Galois group) for which we can construct a polynomial satisfying Strumfel's condition. We restate this condition of Scheiderer in the case of homogeneous polynomials with three variables. Consider Construction 1 (for three variables l is just a line in the projective plane) and define $f := N(l)$. $Z(f)$ has exactly d real points, say $P_1, P_2, \ldots, P_d$. Then condition $(*)$ can be compactly restated as follows

(*) The union of orbits of the real points, namely $\bigcup_{i=1}^{d} GP_i$, has cardinality $\binom{2d}{2}$

If the above is satisfied then G need not be 2-transitive and we can still find a polynomial satisfying the Sturmfel's condition. Our claim is that we can even have a relatively weaker condition. We need to only satisfy a condition for which we can use degree argument and vanishing polynomials (similar argument to the proof of the crucial Lemma 2.5 of [CS]). We illustrate this by an example

Example 1. Consider the splitting field L of $f := x^8 + x^4 + x^2 + 1 \in \mathbb{Q}[x]$. The Galois group, G, of this field is solvable and has a normal subgroup isomorphic to S_4 (permutation of roots of $x^4 + x^2 + x + 1$) and it also has a subgroup isomorphic to C_2^3. Specifically, G is a transitive group (identified as 8T39 in [GAP]) isomorphic to $C_3^3 \rtimes S_4$ and has order 192. Moreover, the maximum real subfield of L is not a Galois extension of $\mathbb{Q}$ (obtained from [DNF]). Let us order the roots of f as follows (to be consistent with Magma Online Calculator [Magma]):

$$\begin{aligned}
\alpha_1 &\approx -0.9473207447 - 0.5916018921\,\mathrm{i} \\
\alpha_2 &\approx -0.9473207447 + 0.5916018921\,\mathrm{i} \\
\alpha_3 &\approx 0.9473207447 - 0.5916018921\,\mathrm{i} \\
\alpha_4 &\approx 0.9473207447 + 0.5916018921\,\mathrm{i} \\
\alpha_5 &\approx -0.3565372616 - 0.8213054325\,\mathrm{i} \\
\alpha_6 &\approx -0.3565372616 + 0.8213054325\,\mathrm{i} \\
\alpha_7 &\approx 0.3565372616 - 0.8213054325\,\mathrm{i} \\
\alpha_8 &\approx 0.3565372616 + 0.8213054325\,\mathrm{i}
\end{aligned}$$

With the above ordering of the roots of f, the Galois group (using Magma Online Calculator [Magma]) G is generated by the following permutations in S_8:

$$\begin{aligned}(1,2,5,6)(3,8,7,4)\\(1,2)(3,4)\\(1,3)(2,4)\\(1,3,8,7)(2,5,6,4)\end{aligned}$$

We used the above with [GAP] to compute the orbits of the complex conjugate pairs of the roots i.e.

$$\begin{aligned}G\{1,2\}\cup G\{3,4\}\cup G\{5,6\}\cup G\{7,8\} \quad &= \\ &\{\{1,2\},\{1,3\},\{1,5\},\{1,6\},\{1,7\},\{1,8\},\{2,4\},\{2,5\},\\ &\{2,6\},\{2,7\},\{2,8\},\{3,4\},\{3,5\},\{3,6\},\{3,7\},\{3,8\},\\ &\{4,5\},\{4,6\},\{4,7\},\{4,8\},\{5,6\},\{5,7\},\{6,8\},\{7,8\}\}\end{aligned}$$

From the lines

$$l_i := x + \alpha_i y + \alpha_i^2 z \qquad i = 1,\dots,8$$

we get four real points $P_1, P_2, P_3, P_4 \in \mathbb{P}^2(\mathbb{C})$ (namely the unique points in $Z_{\mathbb{C}}(l_1,l_2), Z_{\mathbb{C}}(l_3,l_4)$, $Z_{\mathbb{C}}(l_5,l_6)$ and $Z_{\mathbb{C}}(l_7,l_8)$). So there are 24 points in $\mathbb{P}^2(\mathbb{C})$ that are in the union of the orbits of these four points. Using [Giac, GiacPy] we were able to determine the minimum degree needed for a homogenous polynomial to vanish at these 24 points. The computed minimum degree is 6. If the form $F(x,y,z) := N_{L/\mathbb{Q}}(l_1)$ is a sum of squares over $\mathbb{Q}$ then there are homogeneous polynomials $p_1,\dots,p_k \in \mathbb{Q}[x,y,z]$ of degree 4 such that

$$F = p_1^2 + p_2^2 + \dots p_k^2$$

The p_i's should vanish at the real points for which F vanishes and at all the conjugates of these points. But we know that such a form must have a degree at least 6 in order to vanish at all the 24 points we computed. Thus, F cannot be a sum of squares over $\mathbb{Q}$. Moreover, the union of the orbits of the points are less than $\binom{8}{2} = 28$ (so they do not satisfy (*) in Remark 2.9 of [CS]).

The above example suggests that we may find a stronger condition than (*) in Remark 2.9 [CS]. Indeed, we can describe a necessary condition for which there are polynomials satisfying Sturmfel's condition.

Proposition 3. Suppose Premise 2 and let

$$\mathcal{P} := \{\{1,2\},\dots,\{2d-1,2d\}\}$$

and define S to be the union of the G-orbits of pairs in $\mathcal{P}$. For a fixed $i \in \{1,\dots,2d\}$ if

$$|S \cap \{\{i,j\} \,:\, j = 1,\dots,2d\}| \geq d+1$$

then we can find polynomials satisfying Sturmfel's condition for $L \cap \mathbb{R}$.

Proof. (with C. Scheiderer) Denote

$$S(i) := \{j \,:\, 1 \leq j \leq n, \{i,j\} \in S\} \qquad i = 1,\dots,n$$

We easily see that for any $\sigma \in G$ we have $S(\sigma(i)) = \sigma S(i)$. Thus, so for any i,j we have $\#S(i) = \#S(j)$.

For now let us fix an $i = 1,\dots,2d$. Observe that this proposition claims that if $\#S(i) \geq d+1$ then we can find polynomials satisfying Sturfel's condition for $L \cap \mathbb{R}$. In particular, we will

show that the constructed $F := N(l)$ in Construction 1 will yield such a polynomial. As in the construction, we set

$$l_j = x + \alpha_j y + \alpha_j^2 z \qquad j = 1, \ldots, 2d$$

We now identify $1, \ldots, 2d$ with $l_1, \ldots, l_{2d}$ (so G acts on these linear forms), so we a pair in $\mathcal{P}$ with the real points

$$\{l_j \cap \overline{l_j} \, : \, i = 1, 3, \ldots, 2d-1\}$$

Assuming that $\#S(i) \geq d+1$ implies that l_i contains $d+1$ distinct points that are G-conjugates to a real point in S. If, by contradiction, F is a sum squares of finite homogeneous forms in $\mathbb{Q}[x, y, z]$ then these polynomials must have degree d and vanish at all points in $\mathcal{P}$. For any one of the polynomial, say p, the curve defined by p has $d+1$ common (real) point with the line l_i. But p has degree d which is a contradiction. □

We can extend this to any n-ary form with $n \geq 2$. The proof is very similar and is left to the reader

Corollary 4. Suppose Premise 2, let

$$\mathcal{P} := \{\{1, 2\}, \ldots, \{2d-1, 2d\}\}$$

and define S to be the union of the G-orbits of pairs in $\mathcal{P}$. For a fixed $i \in \{1, \ldots, 2d\}$ let

$$|S \cap \{\{i, j\} \, : \, j = 1, \ldots, 2d\}| \geq d+1$$

Then, Construction 1 with n-indeterminates ($n \geq 3$) yields an n-ary F with degree $2d$ that satisfies Sturmfel's condition for $L \cap \mathbb{R}$.

However, if we consider $d = 3$, we cannot find an example of such a polynomial using Construction 1 such that Condition $(*)$ in [CS] does not hold (unlike when $d = 4$ as shown in Example 1). This fact is demonstrated in the following Example.

Example 2. Suppose now that $f \in \mathbb{Q}[x]$ with $\deg(f) = 6$ and let L be its splitting field and $G = \mathrm{Gal}(L/\mathbb{Q})$ satisfying Premise 2. We claim that if we can use the above data in Construction 1 then G must satisfy Condition $(*)$ in [CS].

We know the complex conjugation in G above must be a permutation consisting of 3 disjoint transpositions (i.e. permutation with cycle type $2, 2, 2$). Furthermore G must be one of the 16 transitive subgroups of S_6 (the groups, up to isomorphism, are given by the names 6T1,6T2,..., 6T16 in [GAP, DNF]). One of the $2, 2, 2$ permutation in these transitive groups will correspond with the complex conjugation, we can check all of them by brute force. We did the following with each of the 16 groups

1. Get a list of all $2, 2, 2$ permutations in the group
2. Convert each of the permutation into a list of 3 sets with 2 elements.
3. For each list find the union of the G-orbits of the unordered pairs in the list, and name it S
4. For S from each permutation check if it satisfies $9 < |S| < 15$

Because of Premise 2 we can rule out 6T1 (cyclic group) and groups that do not have a $2, 2, 2$ permutations. With [GAP] we computed which groups do not have $2, 2, 2$ permutations, they are 6T4, 6T7, 6T10, 6T12 and 6T15. In fact, we can also show with [GAP] that if the computed S for any $2, 2, 2$ permutation in a transitive subgroup of S_6 consists of more than 9 pairs, then it has exactly 15 pairs. For the degree argument (see Example 1) to work one must have at least $S \geq 11$. We can thus conclude that all such G will satisfy $(*)$ in [CS]. Here is a sample computation with G isomorphic to 6T9:

In [GAP] 6T9 is represented by a group G' with the following generators

$$\begin{aligned}(2,4,6)\\(1,5)(2,4)\\(1,4)(2,5)(3,6)\end{aligned}$$

Furthermore G' is centerless and has the following $2,2,2$ permutations

$$(1,4)(2,5)(3,6),(1,5)(2,4)(3,6),(1,2)(3,6)(4,5),(1,3)(2,5)(4,6),$$
$$(1,6)(2,5)(3,4),(1,4)(2,6)(3,5),(1,4)(2,3)(5,6)$$

Let us look at the first $2,2,2$ permutation, we get the set $\{1,4\},\{2,5\},\{3,6\}$ and we compute the union of G'-orbits of the pairs:

$$S := \{\{1,2\},\{1,4\},\{1,6\},\{2,3\},\{2,5\},\{3,4\},\{3,6\},\{4,5\},\{5,6\}\}$$

One computes the union of G'-orbits of the pairs corresponding to the other $2,2,2$ permutations and sees that it consists of 9 pairs.

Observation 3. Consider the givens in Premise 2 with indeterminates $x_0, x_1, x_2 = x, y, z$. Suppose futhermore that $d = 4$, then by Construction 1 we can create a positive polynomial $F(x,y,z)$ over $\mathbb{Q}$ sos over $\mathbb{R}$ but not sos over $\mathbb{Q}$, namely

$$4F(x,y,z) = p_1(x,y,z)^2 - p_2(x,y,z)^2$$

where p_1, $\mathrm{i}\,p_2 \in K[x,y,z]$ for $i = 1,2$ specifically computed to be as shown in Table 1. Notice that the coefficients of p_2 are all purely imaginary.

Coefficients of _____ for p_1:

x^2:	2
y^2:	$\alpha_1\alpha_4 + \alpha_2\alpha_3$
z^2:	$\alpha_1^2\alpha_4^2 + \alpha_2^2\alpha_3^2$
xy:	$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$
xz:	$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$
yz:	$\alpha_1^2\alpha_4 + \alpha_1\alpha_4^2 + \alpha_2^2\alpha_3 + \alpha_2\alpha_3^2$

Coefficients of _____ for p_2:

x^2:	0
y^2:	$\alpha_1\alpha_4 - \alpha_2\alpha_3$
z^2:	$\alpha_1^2\alpha_4^2 - \alpha_2^2\alpha_3^2$
xy:	$\alpha_1 - \alpha_2 - \alpha_3 + \alpha_4$
xz:	$\alpha_1^2 - \alpha_2^2 - \alpha_3^2 + \alpha_4^2$
yz:	$\alpha_1^2\alpha_4 + \alpha_1\alpha_4^2 - \alpha_2^2\alpha_3 - \alpha_2\alpha_3^2$

Table 1: Coefficients of p_1 and p_2

We want to argue that any real number field whose polynomial ring contains both p_1 and $\mathrm{i}\,p_2$ is an even degree extension of $\mathbb{Q}$. We note that the only two possibilities for G such that Construction 1 yields a polynomial satisfying Sturmfel's condition is when $G \cong A_4$ or $G \cong S_4$ so we will only consider these two possibilities. We now make the following claims

1. The stabilizer of p_1 as a subgroup of G (acting on the polynomials by acting on the coefficients) contains a subgroup H of A_4 of order 4 and generated by $(1,2)(3,4)$ and $(1,3)(2,4)$. We claim that the stabilizer is exactly this subgroup of A_4. If there were other permutations, then from the coefficient of y^2 in p_1 we would get

$$\alpha_1\alpha_3 + \alpha_2\alpha_4 = \alpha_1\alpha_4 + \alpha_2\alpha_3 \quad (\text{or } \alpha_1\alpha_2 + \alpha_3\alpha_4 = \alpha_1\alpha_4 + \alpha_2\alpha_3)$$

and this is a contradiction because $\alpha_3 \neq \alpha_4$ ($\alpha_2 \neq \alpha_4$) implies that $\alpha_1 = \alpha_2$ ($\alpha_1 = \alpha_3$). So, by Galois correspondence, if $G \cong S_4$ then any real number field whose polynomial ring contains p_1 is an extension of $\mathbb{Q}$ of even degree since $[L^H : \mathbb{Q}] = (S_4 : H) = 6$.

What concerns us more now is if $G \cong A_4$ and the stabilizer of $\mathrm{i}\,p_2$, in this case p_1 could lie in the polynomial ring over a real number field K_1 such that $[K_1 : \mathbb{Q}] = 3$. We thus assume henceforth that $G \cong A_4$.

2. The imaginary unit i is not in L, because any Galois number field with Galois group isomorphic to A_4 will not contain a quadratic field. Thus, we know that $L < L[\mathrm{i}]$ and $|\operatorname{Gal}(L[\mathrm{i}]/\mathbb{Q})| = 24$

3. Let $G' = \operatorname{Gal}(L[\mathrm{i}]/\mathbb{Q})$, then any automorphism σ in the stabilizer of $\mathrm{i}\,p_2$ in G' restricts to an automorphism in the stabilizer of p_1 in G. But an automorophism in G that stabilizes p_1 completely determines the automorphism in G' that stabilizes $\mathrm{i}\,p_2$ i.e. it completely determines the image of i (for this, it suffices again to look at the coefficient of y^2 in $\mathrm{i}\,p_2$). Thus, the group $H := \operatorname{Stab}(p_1, G') \cap \operatorname{Stab}(\mathrm{i}\,p_2, G')$ has order 4 and so, by Galois correspondence, any real number field whose polynomial ring contains $\mathrm{i}\,p_2$ must be an even degree field extension of $\mathbb{Q}$ since $[L[\mathrm{i}]^H : \mathbb{Q}] = (G' : H) = 6$.

From the above observation we can conclude following Theorem

Theorem 5. Let K be a real number field and suppose $F \in \mathbb{Q}[x,y,z]$ be such that $F \notin \sum \mathbb{Q}^2[x,y,z]$ and that $F = f_1^2 + f_2^2$ for $f_1, f_2 \in K[x,y,z]$ then $[K : \mathbb{Q}]$ is even.

Proof. By Theorem 4.1 in [CS], F is the product of four linear forms l_1, l_2, l_3, l_4 with $l_1 = \bar{l}_3$ (complex conjugate) and $l_2 = \bar{l}_4$. We can assume furthermore that l_1 and l_2 has a monomial with coefficient 1 (otherwise we simply divide by the non-zero coefficients), thus F also has a monomial that has coefficient 1. Then F is in a natural way the sum of two squares of ternary quadratic forms p_1, p_2 defined over a real number field that is an even extension of $\mathbb{Q}$: this is proven similar to the above observation, where we choose the product of monomials with coefficient 1, instead of coefficient of x^2, and another product of monomial with non-zero coefficients, instead of y^2, to make most of our argument. This argument also shows us that one of the quadratic forms, say p_1, has a monomial with coefficient 2 while p_2 will not have this monomial at all (in the above observation this was x^2). We thus have

$$F = p_1^2 + p_2^2 = f_1^2 + f_2^2 = (p_1 + \mathrm{i}\,p_2)(p_1 - \mathrm{i}\,p_2)$$

This implies that there is a k-th root of unity $\zeta \in \bar{\mathbb{Q}}$ such that

$$f_1 = \operatorname{Re}(\zeta)p_1 - \operatorname{Im}(\zeta)p_2$$
$$f_2 = \operatorname{Im}(\zeta)p_1 + \operatorname{Re}(\zeta)p_2$$

Since p_1 has a monomial (with rational coefficient) that p_2 does not have, we can at once conclude $\operatorname{Re}(\zeta), \operatorname{Im}(\zeta) \in K$ and this implies that $\operatorname{Re}(\zeta^{-1}), \operatorname{Im}(\zeta^{-1}) \in K$. We can now write p_1 and p_2 in terms of f_1 and f_2 to obtain

$$p_1 = \operatorname{Re}(\zeta^{-1})f_1 - \operatorname{Im}(\zeta^{-1})f_2$$
$$p_2 = \operatorname{Im}(\zeta^{-1})f_1 + \operatorname{Re}(\zeta^{-1})f_2$$

Thus p_1 and p_2 should be in $K[x,y,z]$, but they are defined over a real number field that is an even extension of $\mathbb{Q}$. Thus $[K : \mathbb{Q}]$ is even. □

References

[Magma] **W. Bosma, J. Cannon, C. Playoust**, *The Magma algebra system. I. The user language*, Journal of Symbolic Computation 1997, Vol. 24, p.235–265. Online Calculator: http://magma.maths.usyd.edu.au/calc/

[CLO] **D. Cox, J. Little, D. O'Shea**, *Ideals, Varieties and Algorithms*, 3rd Edition, Springer 2007.

[Flan] **H. Flanders**, *The Norm Function of an Algebraic Field Extension*, Pacific Journal of Mathematics 1953, Vol. 3, p.103-113

[GAP] **The GAP Group**, *GAP – Groups, Algorithms, and Programming, Version 4.9.1*, Online: https://www.gap-system.org, Accessed: 06.2018

[Giac] **B. Parisse, R. De Graeve**, *Giac/Xcas*. Online: https://www-fourier.ujf-grenoble.fr/~parisse/giac.html, Accessed: 01.2017

[GiacPy] **F. Han**, *giacpy*. Online: https://gitlab.math.univ-paris-diderot.fr/han/giacpy, Accessed: 06.2017

[Hillar] **C.J. Hillar**, *Sums of squares over totally real fields are rational sums of squares*, Proceedings of the American Mathematical Society 2009, Vol. 137, No. 3, p.921-930

[Milne] **J.S. Milne**, *Fields and Galois Theory*, Version 4.21 Sept. 28, 2008. Online: www.jmilne.org/math/. Accessed: 04.2009.

[PW] **V. Powers, T. Wörmann**, *An algorithm for sums of squares of real polynomials*, Journal of Pure and Applied Algebra 1998, Vol. 127, p.99-104

[CS] **C. Scheiderer**, *Sums of squares of polynomials with rational coefficients*, Journal of European Mathematical Society 2016, Vol. 18, p.1495-1513

[DNF] **J. Klüners, G. Malle**, *Database of Number Fields*. Online: http://galoisdb.math.upb.de/. Accessed: 06.2018