ACTA ARITHMETICA
225.2 (2026)

Anisotropy of quadratic forms over global fields of characteristic $\neq 2$ is diophantine

by

Guang Hu

Abstract. We prove that the set of anisotropic quadratic forms over global fields of characteristic different from 2 is a diophantine set. Our proof builds upon and extends the method of Koenigsmann, using tools from class field theory, the local-global principle, and advances on the diophantine definability of nonnorm sets over global fields.

1. Introduction. Let K be a global field. Roughly speaking, a diophantine set is a set that can be described by the solvability of a family of polynomial equations. Equivalently, we give the following definition.

Definition 1.1. A subset $S \subset K^n$ is called a *diophantine set* over K if there exists a polynomial

$$f(a_1, \ldots, a_n; x_1, \ldots, x_m) \in K[a_1, \ldots, a_n; x_1, \ldots, x_m]$$

such that for each $(a_1, \ldots, a_n) \in K^n$ we have

$$(a_1, \ldots, a_n) \in S \iff \exists (x_1, \ldots, x_m) \in K^m \text{ such that } f(a_1, \ldots, a_n; x_1, \ldots, x_m) = 0.$$

The study of diophantine sets is closely connected with Hilbert's Tenth Problem. Matiyasevich [Mat70] proved that the problem has a negative answer over $\mathbb{Z}$. Furthermore, if $\mathbb{Z}$ is diophantine over $\mathbb{Q}$, then Hilbert's Tenth Problem over $\mathbb{Q}$ would also have a negative answer. However, this remains an open problem.

Besides the connection to foundational questions in logic and number theory, the study of diophantine sets is of intrinsic interest as an inverse to the problem of solving polynomial equations. While the classical problem asks for the solutions of given polynomial equations, the study of diophantine

2020 *Mathematics Subject Classification*: Primary 11U05; Secondary 11R37.
Key words and phrases: diophantine sets, global fields, class field theory.
Received 24 July 2024; revised 11 August 2026.
Published online 13 October 2026 in Open Access (under CC-BY license).

DOI: 10.4064/aa240724-7-9 © Instytut Matematyczny PAN, 2026

sets addresses the reverse question: which subsets of K^n can arise as the set of parameter values for which a polynomial system has a solution?

A significant advance in this direction was achieved by Poonen [Poo09], who proved, using the Brauer–Manin obstruction, that the set of nonsquares in number fields is diophantine. This provided one of the first nontrivial examples of such sets.

This result has been generalized to various situations in recent years. Colliot-Thélène and Jan Van Geel [CTG15] extended Poonen's result to the complements of n-th powers over number fields. Koenigsmann [Koe16] introduced powerful new methods for constructing diophantine sets over $\mathbb{Q}$, notably the set of nonnorms for quadratic extensions.

More generally, for a quadratic extension L/K of a global field K of characteristic different from 2, the set of nonnorms

$$\{x \in K^\times \mid x \notin N_{L/K}(L^\times)\}$$

is diophantine. In fact, a stronger statement holds:

$$\{(x, y) \in (K^\times)^2 \mid x \notin N_{K(\sqrt{y})/K}(K(\sqrt{y})^\times)\}$$

is diophantine. Park [Par13] extended Koenigsmann's method to number fields, and Eisenträger and Morrison [EM18] later applied it to global function fields of odd characteristic. Morrison [Mor19] further generalized the result to cyclic extensions of degree prime to the characteristic.

Another result was obtained by Philip Dittmann [Dit18]. He generalized the method uniformly to apply to any global field and proved that the set of coefficients of univariate polynomials that have no solutions in a global field is diophantine. As a corollary, he showed that the set of coefficients of irreducible multivariate polynomials is diophantine.

In this paper, we study diophantine sets defined by quadratic forms. We begin by recalling the notions of isotropy and anisotropy of quadratic forms.

Definition 1.2. Let F be a field and let f be a quadratic form in m variables over F. We say that f is *isotropic over* F if there exists a tuple $(x_1, \ldots, x_m) \in F^m$, not all zero, such that

$$f(x_1, \ldots, x_m) = 0.$$

Otherwise, we say that f is *anisotropic over* F.

Our goal is to show that the set of coefficients of anisotropic quadratic forms over a global field of characteristic not equal to 2 is a diophantine set. In any case, the set of coefficients of isotropic quadratic forms is obviously diophantine. So, the set we deal with here is the complement of this obvious diophantine set, just like the works we mentioned above. Our main theorem is the following.

THEOREM 1.3. *Let K be a global field with* $\mathrm{char}(K) \neq 2$, *and let* $m \in \mathbb{N}$. *Then the set*

$$\Big\{(a_i) \in (K^\times)^m \;\Big|\; \sum_{i=1}^{m} a_i x_i^2 \text{ is anisotropic over } K\Big\}$$

is diophantine over K.

REMARK 1.4. In the notation $(K^\times)^m$ we mean the Cartesian product of m copies of $K^\times$, i.e. the set of m-tuples of elements of $K^\times$, and not the set of mth powers in $K^\times$, which we denote by $K^{\times m}$.

As a corollary of Theorem 1.3, we obtain the following.

COROLLARY 1.5. *Let K be a global field with* $\mathrm{char}(K) \neq 2$, *and let* $m \in \mathbb{N}$. *Then the set*

$$\Big\{(a_{ij}) \in (K)^{m^2} \;\Big|\; \sum_{1\le i,j\le m} a_{ij} x_i x_j \text{ is anisotropic over } K\Big\}$$

is diophantine over K.

To prove Theorem 1.3, we distinguish cases according to the value of m. For $m \geq 5$, the result follows from the local-global principle. For $m = 1, 2$, or 3, the result is already known, in the context of "nonsquares" and "nonnorms". The only genuinely new case is $m = 4$, for which we employ generalizations of Koenigsmann's method developed in [Dit18, Par13, EM18].

2. Preliminaries. From now on, we denote by S_K the set of primes of K, including both finite and infinite primes. By a prime of K we mean an equivalence class of nontrivial absolute values on K.

If K is a number field, we write S_K^∞ for the set of infinite primes of K. For $\mathfrak{p} \in S_K^\infty$, if the corresponding completion $K_\mathfrak{p}$ is isomorphic to the real field $\mathbb{R}$, we call $\mathfrak{p}$ a *real infinite prime*; if $K_\mathfrak{p} \simeq \mathbb{C}$, then $\mathfrak{p}$ is called a *complex infinite prime*. If $\mathfrak{p}$ is finite, we also use $\mathfrak{p}$ to denote the corresponding prime ideal, and we write $v_\mathfrak{p}$ for the associated normalized discrete valuation on K. Let

$$S_K^f := S_K \setminus S_K^\infty$$

denote the set of finite primes of K.

For $a, b \in K_\mathfrak{p}^\times$, the notation $(a, b)_\mathfrak{p}$ denotes the Hilbert symbol at $\mathfrak{p}$. Note that the Hilbert symbol $(a, b)_\mathfrak{p}$ defines a nondegenerate bilinear pairing on $K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2}$.

For $a \in K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2}$, we define the group homomorphism

$$T_a \colon K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2} \to \{\pm 1\}, \qquad x \mapsto (x, a)_\mathfrak{p},$$

where we regard $\{\pm 1\}$ as a multiplicative group. Let f be a quadratic form in m variables over K, and let $a \in K^\times$. We say that f *represents* a over K

if there exists a tuple $(x_1, \ldots, x_m) \in K^m$ such that

$$f(x_1, \ldots, x_m) = a.$$

We say that f is *isotropic* (or *anisotropic*) over $\mathfrak{p}$ if it is isotropic (or anisotropic) over the completion $K_\mathfrak{p}$.

LEMMA 2.1. *With the notations above, let $\epsilon, \epsilon' \in \{\pm 1\}$ and let $a, a' \in K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2}$ be nontrivial. Then*

$$T_a^{-1}(\epsilon) \cap T_{a'}^{-1}(\epsilon') = \emptyset \iff a = a' \text{ and } \epsilon = -\epsilon'.$$

Proof. $\Leftarrow$: This is obvious.

$\Rightarrow$: By [O'M00, 63:9], the index $[K_\mathfrak{p}^\times : K_\mathfrak{p}^{\times 2}]$ is finite. Since $a \neq 1$ and the Hilbert symbol is nondegenerate, T_a is nontrivial. Hence, the cardinalities of $T_a^{-1}(1)$ and $T_a^{-1}(-1)$ are both equal to half of $[K_\mathfrak{p}^\times : K_\mathfrak{p}^{\times 2}]$.

For $\epsilon, \epsilon' \in \{\pm 1\}$ and nontrivial $a, a' \in K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2}$, we have

$$T_a^{-1}(\epsilon) \cap T_{a'}^{-1}(\epsilon') = \emptyset \iff T_a^{-1}(\epsilon) \sqcup T_{a'}^{-1}(\epsilon') = K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2},$$

by a cardinality argument.

The complement of $T_a^{-1}(1)$ in $K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2}$ is $T_a^{-1}(-1)$. Hence,

$$T_a^{-1}(\epsilon) \sqcup T_{a'}^{-1}(\epsilon') = K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2}$$

is equivalent to

$$T_a^{-1}(1) = T_{a'}^{-1}(1) \text{ or } T_a^{-1}(1) = T_{a'}^{-1}(-1).$$

However, $T_a^{-1}(1) = T_{a'}^{-1}(-1)$ is impossible, since this would imply

$$(x, aa')_\mathfrak{p} = (x, a)_\mathfrak{p}(x, a')_\mathfrak{p} = -1 \quad \forall x \in K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2},$$

which cannot happen.

Also, it is easy to verify that

$$\begin{aligned} T_a^{-1}(1) = T_{a'}^{-1}(1) &\iff (x, a)_\mathfrak{p} = (x, a')_\mathfrak{p} \quad \forall x \in K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2} \\ &\iff (x, aa')_\mathfrak{p} = 1 \quad \forall x \in K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2} \\ &\iff T_{aa'} \text{ is trivial} \\ &\iff aa' = 1 \\ &\iff a = a'. \end{aligned}$$

In conclusion, we have

$$T_a^{-1}(\epsilon) \cap T_{a'}^{-1}(\epsilon') = \emptyset \iff a = a' \text{ and } \epsilon = -\epsilon'. \blacksquare$$

2.1. Quadratic forms. The arithmetic of quadratic forms over a global field is well understood. The local-global principle for isotropy applies to quadratic forms, and while the theory becomes more subtle in characteristic 2, the situation for our purposes is particularly transparent.

To prove Theorem 2.3 below, we will need the following lemma:

LEMMA 2.2. *For* $(a_1, a_2, a_3, a_4) \in (K_\mathfrak{p}^\times)^4$, *the following two conditions are equivalent:*

(1) *There exists* $(x_1, x_2, x_3, x_4) \in (K_\mathfrak{p})^4 \setminus \{(0,0,0,0)\}$ *such that* $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = 0$.

(2) *There exist nonzero* $x' \in K_\mathfrak{p}$ *and* $(x_1, x_2, x_3, x_4) \in (K_\mathfrak{p})^4 \setminus \{(0,0,0,0)\}$ *such that*

$$a_1x_1^2 + a_2x_2^2 = -a_3x_3^2 - a_4x_4^2 = x'.$$

Proof. (2)⇒(1) is obvious.

For (1)⇒(2), suppose there exists

$$(x_1, x_2, x_3, x_4) \in (K_\mathfrak{p})^4 \setminus \{(0,0,0,0)\}$$

such that

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = 0.$$

If $a_1x_1^2 + a_2x_2^2 \neq 0$, take $x' = a_1x_1^2 + a_2x_2^2$, and we are done. If $a_1x_1^2 + a_2x_2^2 = 0$, then the quadratic form $a_1x_1^2 + a_2x_2^2$ is isotropic, and hence universal by [O'M00, 42:10]. In this case, we can take $x' = -a_3x_3^2 - a_4x_4^2$ for any $(x_3, x_4) \in (K_\mathfrak{p})^2$ such that $x' \neq 0$. ∎

THEOREM 2.3. *Let* K *be a global field with* $\mathrm{char}(K) \neq 2$, *and let* f *be a nondegenerate quadratic form in* m *variables over* K. *Then the following statements hold:*

(1) f *is isotropic over* K *if and only if* f *is isotropic over* $K_\mathfrak{p}$ *for every prime* $\mathfrak{p} \in S_K$.

(2) *If* $m \geq 5$ *and* $\mathfrak{p} \in S_K$ *is a nonarchimedean place, then* f *is isotropic over* $K_\mathfrak{p}$.

(3) *If* $m = 4$, $\mathfrak{p} \in S_K$ *is nonarchimedean, and*

$$f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2,$$

then f *is anisotropic over* $K_\mathfrak{p}$ *if and only if*

$$a_1a_2a_3a_4 \in K_\mathfrak{p}^{\times 2} \quad \textit{and} \quad (a_1, a_2)_\mathfrak{p} = -(-a_3, -a_4)_\mathfrak{p}.$$

Proof. The first item follows from [O'M00, Theorem 66:1], and the second item from [O'M00, Theorem 63:19]. The third item is stated in [Ser73, Theorem 6, Chapter IV] for $K = \mathbb{Q}$, and the same proof naturally generalizes to arbitrary global fields. We provide a detailed proof of this generalization below, following the method of [Ser73].

By Lemma 2.2, the form $f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$ is isotropic over $K_\mathfrak{p}$ if and only if there exists a nonzero $x' \in K_\mathfrak{p}$ such that the two forms $a_1x_1^2 + a_2x_2^2$ and $-a_3x_3^2 - a_4x_4^2$ both represent x'. Let x denote the coset of x' in $K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2}$.

The statement that $a_1x_1^2 + a_2x_2^2$ represents x' is equivalent to

$$(xa_1, xa_2)_\mathfrak{p} = 1.$$

After a calculation using the properties of the Hilbert symbol, we get

$$\begin{aligned}(xa_1, xa_2)_{\mathfrak{p}} &= (xa_1, x)_{\mathfrak{p}} \cdot (xa_1, a_2)_{\mathfrak{p}} \\ &= (x, x)_{\mathfrak{p}} \cdot (a_1, x)_{\mathfrak{p}} \cdot (x, a_2)_{\mathfrak{p}} \cdot (a_1, a_2)_{\mathfrak{p}} \\ &= (x, -1)_{\mathfrak{p}} \cdot (x, a_1)_{\mathfrak{p}} \cdot (x, a_2)_{\mathfrak{p}} \cdot (a_1, a_2)_{\mathfrak{p}} \\ &= (x, -a_1a_2)_{\mathfrak{p}} \cdot (a_1, a_2)_{\mathfrak{p}}.\end{aligned}$$

Hence, $a_1x_1^2 + a_2x_2^2$ represents x' if and only if

$$(x, -a_1a_2)_{\mathfrak{p}} = (a_1, a_2)_{\mathfrak{p}},$$

which is equivalent to

$$x \in T^{-1}_{-a_1a_2}((a_1, a_2)_{\mathfrak{p}}).$$

Similarly, $-a_3x_3^2 - a_4x_4^2$ represents x' if and only if

$$(x, -a_3a_4)_{\mathfrak{p}} = (-a_3, -a_4)_{\mathfrak{p}},$$

which is equivalent to

$$x \in T^{-1}_{-a_3a_4}((-a_3, -a_4)_{\mathfrak{p}}).$$

Therefore, the absence of such an x is equivalent to

$$T^{-1}_{-a_1a_2}((a_1, a_2)_{\mathfrak{p}}) \cap T^{-1}_{-a_3a_4}((-a_3, -a_4)_{\mathfrak{p}}) = \emptyset.$$

By Lemma 2.1, this is in turn equivalent to

$$a_1a_2 = a_3a_4 \text{ up to a square in } K_{\mathfrak{p}}^{\times} \quad \text{and} \quad (a_1, a_2)_{\mathfrak{p}} = -(-a_3, -a_4)_{\mathfrak{p}},$$

as claimed. ∎

2.2. Global class field theory. In this section, we recall some standard results from global class field theory. We begin by introducing the notion of a modulus, which generalizes the role of an integer m in classical modular arithmetic.

Definition 2.4. Let K be a global field and $\mathcal{O}_K$ its ring of integers. A *modulus* of K is a formal product of primes of K

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})},$$

where each exponent $\mathfrak{m}(\mathfrak{p}) \geq 0$, and the following conditions are satisfied:

- $\mathfrak{m}(\mathfrak{p}) = 0$ for all but finitely many primes $\mathfrak{p}$;
- $\mathfrak{m}(\mathfrak{p}) = 0$ for every infinite complex prime $\mathfrak{p}$;
- $\mathfrak{m}(\mathfrak{p}) \in \{0, 1\}$ for every infinite real prime $\mathfrak{p}$.

In the number field case, a modulus can be written as

$$\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty,$$

where $\mathfrak{m}_0$ denotes the finite part and $\mathfrak{m}_\infty$ the infinite part. The notion of congruence extends naturally to this setting.

Definition 2.5. Let $a, b \in K^\times$, and let $\mathfrak{m}$ be a modulus of K. For a finite or real infinite prime $\mathfrak{p}$, we define

$$a \equiv^* b \pmod{\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}}$$

as follows:

- If $\mathfrak{p}$ is finite, then
$$a \equiv^* b \pmod{\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}} \iff v_{\mathfrak{p}}(a/b - 1) \geq \mathfrak{m}(\mathfrak{p}).$$
- If $\mathfrak{p}$ is real, then
$$a \equiv^* b \pmod{\mathfrak{p}} \iff \frac{a}{b} > 0$$
under the real embedding associated with $\mathfrak{p}$.

Moreover, we write

$$a \equiv^* b \pmod{\mathfrak{m}}$$

if the above holds for every $\mathfrak{p}$ with $\mathfrak{m}(\mathfrak{p}) > 0$.

Let I_K denote the group of fractional ideals of K, and let

$$I_{\mathfrak{m}} := \langle \mathfrak{p} \subseteq \mathcal{O}_K : \mathfrak{m}(\mathfrak{p}) = 0 \rangle$$

be the subgroup of I_K generated by all prime ideals $\mathfrak{p}$ of K that do not divide $\mathfrak{m}$.

Definition 2.6. The *ray modulo* $\mathfrak{m}$ is

$$K_{\mathfrak{m},1} = \{a \in K^\times : a \equiv^* 1 \pmod{\mathfrak{m}}\}.$$

Every $\alpha \in K^\times$ defines a principal fractional ideal

$$(\alpha) := \alpha \mathcal{O}_K \in I_K.$$

If $\alpha \in K_{\mathfrak{m},1}$, then $(\alpha) \in I_{\mathfrak{m}}$, so we obtain a well-defined homomorphism

$$i : K_{\mathfrak{m},1} \to I_{\mathfrak{m}}, \qquad \alpha \mapsto (\alpha).$$

Definition 2.7. Let

$$P_{\mathfrak{m}} := i(K_{\mathfrak{m},1}) \leq I_{\mathfrak{m}}.$$

The *ray class group modulo* $\mathfrak{m}$ is defined by

$$C_{\mathfrak{m}} := I_{\mathfrak{m}}/P_{\mathfrak{m}}.$$

Let L/K be a finite abelian extension. For a prime ideal $\mathfrak{p}$ of K unramified in L, denote by

$$(\mathfrak{p}, L/K) \in \mathrm{Gal}(L/K)$$

the associated Frobenius automorphism.

If $\mathfrak{m}$ is a modulus of K divisible by all primes that ramify in L, the *global Artin map* is the homomorphism

$$\psi_{L/K} : I_{\mathfrak{m}} \to \mathrm{Gal}(L/K),$$

defined on a fractional ideal $\mathfrak{a} = \prod \mathfrak{p}_i^{e_i} \in I_{\mathfrak{m}}$ by $\psi_{L/K}(\mathfrak{a}) := \prod (\mathfrak{p}_i, L/K)^{e_i}$.

THEOREM 2.8 (Artin reciprocity). *Let L/K be a finite abelian extension. There exists a modulus $\mathfrak{m}$ of K, containing all primes of K that ramify in L, such that the global Artin map*

$$\psi_{L/K} : I_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$

is surjective, with kernel

$$\ker(\psi_{L/K}) = P_{\mathfrak{m}} \cdot N_{L/K}(I_L(\mathfrak{m}')),$$

where $\mathfrak{m}'$ is the modulus of L associated to $\mathfrak{m}$, defined as follows.

If

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}} \cdot \prod_{\omega \text{ real}} \omega^{n_\omega}, \qquad n_\omega \in \{0,1\},$$

then

$$\mathfrak{m}' = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{n_{\mathfrak{p}}} \cdot \prod_{\Omega|\omega \text{ real}} \Omega^{n_\omega},$$

where the first product runs over all finite primes $\mathfrak{P}$ of L above $\mathfrak{p}$, and the second product runs over all real embeddings Ω of L extending the real embedding ω of K.

We call a modulus $\mathfrak{m}$ as in Theorem 2.8 an *admissible modulus* for the extension L/K.

Theorem 2.8 is stated for number fields and function fields in various standard references. For instance, it appears in [EM18, Theorem 2.1] in the case of global function fields, and in [Par13, Theorem 3.3] in the case of number fields. For a standard exposition of the Artin symbol, we refer to [Lan86], where a proof of Artin reciprocity is given in Theorems 1–3.

3. Main method. In this section, we recall the methods used in [Koe16, Par13, EM18, Dit18] to construct diophantine sets. These methods will serve as the main ingredients in the proof of our main result.

3.1. Notations and some examples. Let K be a field, and let A be a finite-dimensional central simple algebra over K. We define

$$S(A/K) \coloneqq \{\mathrm{Trd}(x) : x \in A,\ \mathrm{Nrd}(x) = 1\},$$
$$T(A/K) \coloneqq S(A/K) + S(A/K),$$

where Trd and Nrd denote the reduced trace and norm, respectively.

From now on, let K be a global field with $\mathrm{char}(K) \neq 2$, and let A be the quaternion algebra $H_{a,b}$ for $a, b \in K^\times$ defined by

$$H_{a,b} \coloneqq K \oplus \alpha K \oplus \beta K \oplus \alpha\beta K,$$

where $\alpha^2 = a$, $\beta^2 = b$, $\alpha\beta = -\beta\alpha$.

Note that for the quaternion algebra $H_{a,b}$ over a global field K, we have

$$T(A/K) \coloneqq S(A/K) + S(A/K) = S(A/K) - S(A/K),$$

since for any $x \in A$ with $\mathrm{Nrd}(x) = 1$, we have $-x \in A$ and $\mathrm{Nrd}(-x) = \mathrm{Nrd}(x) = 1$, and moreover $\mathrm{Trd}(-x) = -\mathrm{Trd}(x)$. Hence $x \in S(A/K)$ implies $-x \in S(A/K)$, which ensures that $S(A/K)+S(A/K) = S(A/K)-S(A/K)$.

For $\mathfrak{p} \in S_K^f$, let $R_\mathfrak{p}$ be its valuation ring in $K_\mathfrak{p}$, and define

$$\mathcal{O}_\mathfrak{p} \coloneqq (\mathcal{O}_K)_\mathfrak{p} = R_\mathfrak{p} \cap K$$

as the local ring of $\mathfrak{p}$ in K. For simplicity, we write $S(A/K)$ as $S_{a,b}$ and $T(A/K)$ as $T_{a,b}$, since A is the quaternion algebra as stated.

Lemma 3.1. *If A/K splits at all real places of K (this holds if K is a global function field, or if K is a number field and $a, b \in K^\times$ are totally positive), then*

$$T_{a,b} = \bigcap_{\mathfrak{q} \in \Delta_{a,b}} \mathcal{O}_\mathfrak{q},$$

where $\Delta_{a,b}$ is the finite set of places of K at which A does not split.

Proof. This is a special case of [Dit18, Proposition 2.9]. ∎

Remark 3.2. $T_{a,b}$ is a diophantine set over K by definition. This fact forms the basis for proving that many other sets are diophantine in [EM18, Dit18, Par13]. Moreover, $T_{a,b}$ is uniformly existentially defined in a and b, since we have the following formula for $S_{a,b}$:

$$S_{a,b} = \{2x_1 \in K : \exists x_2, x_3, x_4 \text{ with } x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1\},$$

together with the definition $T_{a,b} = S_{a,b} + S_{a,b}$.

The following definition appears in [Koe16, Definition 9] for $K = \mathbb{Q}$, and is also given after the proof of [Par13, Lemma 3.8] as well as after the proof of [EM18, Lemma 3.3].

Definition 3.3. Let $L \coloneqq K(\sqrt{a}, \sqrt{b})/K$ be an abelian extension with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, and let $\psi_{L/K} : I_\mathfrak{m} \to \mathrm{Gal}(L/K)$ be the global Artin map with admissible modulus $\mathfrak{m}$. We define the following notations:

- For $(i, j) \in \mathrm{Gal}(L/K)$, $i, j \in \{\pm 1\}$, we define
$$\mathbb{P}^{(i,j)} \coloneqq \{\mathfrak{p} \in S_K^f : \mathfrak{p} \in I_\mathfrak{m} \text{ and } \psi_{L/K}(\mathfrak{p}) = (i, j)\}.$$
- For $p \in K$ we define
$$\mathbb{P}(p) \coloneqq \{\mathfrak{p} \in S_K^f : v_\mathfrak{p}(p) \text{ is odd}\}, \qquad \mathbb{P}^{(i,j)}(p) \coloneqq \mathbb{P}(p) \cap \mathbb{P}^{(i,j)}.$$

Here, $(1, 1)$ is the identity in the Galois group; $(-1, 1)$ is the element which sends $\sqrt{a}$ to $-\sqrt{a}$ and fixes $\sqrt{b}$; $(1, -1)$ is the element which sends $\sqrt{b}$

to $-\sqrt{b}$ and fixes $\sqrt{a}$; and finally $(-1,-1)$ is the element which sends $\sqrt{a}$ to $-\sqrt{a}$ and $\sqrt{b}$ to $-\sqrt{b}$.

The following lemma is a summary of some results in [Par13] and [EM18].

LEMMA 3.4.

(1) *If K is a number field, then there exist $a, b \in K^\times$ with disjoint supports and* $\mathrm{Gal}(K(\sqrt{a},\sqrt{b})/K) \cong (\mathbb{Z}/2\mathbb{Z})^2$ *such that for any $p \in K^\times$ coprime to the admissible modulus $\mathfrak{m}$, we have*

- $\mathbb{P}^{(-1,-1)}(p) = \Delta_{a,p} \cap \Delta_{b,p}$,
- $\mathbb{P}^{(-1,1)}(p) = \Delta_{a,p} \cap \Delta_{ab,p}$,
- $\mathbb{P}^{(1,-1)}(p) = \Delta_{b,p} \cap \Delta_{ab,p}$.

(2) *If K is a global function field with* $\mathrm{char}(K) \neq 2$, *there exist $a, b, c, d \in K^\times$ such that a and b have disjoint supports and* $\mathrm{Gal}(K(\sqrt{a},\sqrt{b})/K) \cong (\mathbb{Z}/2\mathbb{Z})^2$. *For any $p \in K^\times$ coprime to the admissible modulus $\mathfrak{m}$, we have*

- $\mathbb{P}^{(-1,-1)}(p) = \Delta_{a,p} \cap \Delta_{b,p}$,
- $\mathbb{P}^{(-1,1)}(p) = \Delta_{a,p} \cap \Delta_{ab,p} \cap \Delta_{a,cp}$,
- $\mathbb{P}^{(1,-1)}(p) = \Delta_{b,p} \cap \Delta_{ab,p} \cap \Delta_{b,dp}$.

Proof. We first address (1), which was proved in [Par13]. By [Par13, Lemma 3.9], for any p coprime to $\mathfrak{m}$, the sets on the left- and right-hand sides of each equation differ at most by the primes dividing the modulus. Then, [Par13, Lemmas 3.19 and 3.20] provide a careful choice of a and b such that these sets are equal.

Part (2) follows from [EM18, Corollary 3.11].

The fact that a and b have disjoint supports is guaranteed by [Par13, Lemma 3.19(4)] and [EM18, Lemma 3.8(4)]. ∎

From now on, unless otherwise stated, the parameters a, b (or a, b, c, d) are as fixed in Lemma 3.4, and L denotes the field $K(\sqrt{a},\sqrt{b})$, depending on whether K is a number field or a function field. We also fix the admissible modulus $\mathfrak{m}$ for the field extension L/K as in Lemma 3.4.

DEFINITION 3.5. Let K be a global field with $\mathrm{char}(K) \neq 2$, and keep the constants a, b, c, d as above. For each $\sigma \in \mathrm{Gal}(L/K)$, we define the ring R_p^σ as follows:

(a) If K is a number field, then

$$R_p^{(-1,-1)} := \bigcap_{\mathfrak{p}\in\Delta_{a,p}\cap\Delta_{b,p}} \mathcal{O}_\mathfrak{p}, \qquad R_p^{(1,-1)} := \bigcap_{\mathfrak{p}\in\Delta_{ab,p}\cap\Delta_{b,p}} \mathcal{O}_\mathfrak{p},$$

$$R_p^{(-1,1)} := \bigcap_{\mathfrak{p}\in\Delta_{a,p}\cap\Delta_{ab,p}} \mathcal{O}_\mathfrak{p}, \qquad R_{p,q}^{(1,1)} := \bigcap_{\mathfrak{p}\in\Delta_{ap,q}\cap\Delta_{bp,q}} \mathcal{O}_\mathfrak{p}.$$

(b) If K is a global function field, then

$$R_p^{(-1,-1)} := \bigcap_{\mathfrak{p}\in\Delta_{a,p}\cap\Delta_{b,p}} \mathcal{O}_\mathfrak{p}, \qquad R_p^{(1,-1)} := \bigcap_{\mathfrak{p}\in\Delta_{b,p}\cap\Delta_{ab,p}\cap\Delta_{b,dp}} \mathcal{O}_\mathfrak{p},$$

$$R_p^{(-1,1)} := \bigcap_{\mathfrak{p}\in\Delta_{ab,p}\cap\Delta_{a,p}\cap\Delta_{a,cp}} \mathcal{O}_\mathfrak{p}, \qquad R_{p,q}^{(1,1)} := \bigcap_{\mathfrak{p}\in\Delta_{ap,q}\cap\Delta_{bp,q}} \mathcal{O}_\mathfrak{p}.$$

For $K = \mathbb{Q}$, the definitions of R_p^σ and $R_{p,q}^{(1,1)}$ above coincide with [Koe16, Definition 7]. Their generalizations to number fields and global fields are given in [Par13, Definition 3.10] and [EM18, Definition 3.12], respectively.

The following lemma is well known (see [EP05, Lemma 3.2.6 and Theorem 3.2.7]).

LEMMA 3.6. *Let Δ be a finite subset of S_K^f. Recall that $J(R)$ denotes the Jacobson radical of a ring R. If*

$$R = \bigcap_{\mathfrak{p}\in\Delta} \mathcal{O}_\mathfrak{p},$$

then

$$J(R) = \bigcap_{\mathfrak{p}\in\Delta} \mathfrak{p}\mathcal{O}_\mathfrak{p}.$$

The following lemma describes the behavior of addition for finite intersections of valuation rings and their Jacobson radicals.

LEMMA 3.7. *Let Δ_1, Δ_2 be two finite subsets of S_K^f. Then*

$$\bigcap_{\mathfrak{p}\in\Delta_1} \mathcal{O}_\mathfrak{p} + \bigcap_{\mathfrak{p}\in\Delta_2} \mathcal{O}_\mathfrak{p} = \bigcap_{\mathfrak{p}\in\Delta_1\cap\Delta_2} \mathcal{O}_\mathfrak{p}, \tag{1}$$

$$\bigcap_{\mathfrak{p}\in\Delta_1} \mathfrak{p}\mathcal{O}_\mathfrak{p} + \bigcap_{\mathfrak{p}\in\Delta_2} \mathfrak{p}\mathcal{O}_\mathfrak{p} = \bigcap_{\mathfrak{p}\in\Delta_1\cap\Delta_2} \mathfrak{p}\mathcal{O}_\mathfrak{p}. \tag{2}$$

Proof. For both (1) and (2), the left-hand sides are obviously contained in the right-hand sides. For the reverse inclusion, let $t \in \{0,1\}$ and $x \in K$ be such that $v_\mathfrak{p}(x) \geq t$ for all $\mathfrak{p} \in \Delta_1 \cap \Delta_2$.

By weak approximation, there exists $x_1 \in K$ such that

$$v_\mathfrak{p}(x_1) \geq t \quad \text{for all } \mathfrak{p} \in \Delta_1,$$

and

$$v_\mathfrak{p}(x_1 - x) \geq t \quad \text{for all } \mathfrak{p} \in \Delta_2 \setminus \Delta_1.$$

Set $x_2 = x - x_1$. Then, for all $\mathfrak{p} \in \Delta_1 \cap \Delta_2$, we have

$$v_\mathfrak{p}(x_2) = v_\mathfrak{p}(x - x_1) \geq \min\{v_\mathfrak{p}(x), v_\mathfrak{p}(x_1)\} \geq t.$$

Thus $x = x_1 + x_2$, which is of the form appearing on the left-hand side. ∎

The following definition summarizes [Par13, Definitions 3.21 and 3.24], which also appears in [EM18, Definitions 3.13 and 3.16].

Definition 3.8. For each $\sigma \in \mathrm{Gal}(L/K)$, define

$$\begin{aligned}
&\Phi_\sigma := \{p \in K^\times : (p) \in I_{\mathfrak{m}},\ \psi_{L/K}((p)) = \sigma, \text{ and } \mathbb{P}(p) \subset \mathbb{P}^{(1,1)} \cup \mathbb{P}^\sigma\},\\
&\widetilde{\Phi_\sigma} := K^{\times 2} \cdot \Phi_\sigma,\\
&\Psi_K := \Big\{(p,q) \in \widetilde{\Phi_{(1,1)}} \times \widetilde{\Phi_{(-1,-1)}} \;\Big|\; \prod_{\mathfrak{p}|\mathfrak{m}} (ap,q)_{\mathfrak{p}} = -1,\\
&\qquad\qquad p \in a \cdot K^{\times 2} \cdot (1 + J(R_q^{(-1,-1)}))\Big\}.
\end{aligned}$$

For later use, we summarize several results from [EM18] and [Par13].

Proposition 3.9. *Let K be a global field with* $\mathrm{char}(K) \neq 2$, *and keep the notations introduced above. Then the following statements hold:*

(1) *The sets Φ_σ, Ψ_K, R_p^σ, $J(R_p^\sigma)$, $R_{p,q}^{(1,1)}$, and $J(R_{p,q}^{(1,1)})$ are all diophantine over K.*
(2) *For any $p \in \Phi_\sigma$ and any $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma \neq (1,1)$, the set $\mathbb{P}^\sigma(p)$ is nonempty.*
(3) *Let $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma \neq (1,1)$, and let $\mathfrak{p} \nmid \mathfrak{m}$ be a prime of K satisfying $\psi_{L/K}(\mathfrak{p}) = \sigma$. Then there exists $p \in \Phi_\sigma$ such that*

$$\mathbb{P}^\sigma(p) = \{\mathfrak{p}\}.$$

(4) *For any $(p,q) \in \Psi_K$, we have*

$$\emptyset \neq \Delta_{ap,q} \cap \Delta_{bp,q} \subset I_{\mathfrak{m}}.$$

(5) *For each prime ideal $\mathfrak{p}_0$ satisfying $\mathfrak{p}_0 \nmid \mathfrak{m}$ and $\psi_{L/K}(\mathfrak{p}_0) = (1,1)$, there exists $(p,q) \in \Psi_K$ such that*

$$\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}_0\}.$$

Moreover, we may require that $v_{\mathfrak{p}_0}(p) = 1$, $v_{\mathfrak{p}_0}(q) = 0$, and that q is not a square modulo $\mathfrak{p}_0$.

Proof. This proposition follows from [EM18, Lemmas 3.14 and 3.17] for global function fields, and from [Par13, Lemmas 3.22 and 3.25] for number fields. Only the last assertion in (5) requires additional justification, which we provide below.

Number field case. The proof of [Par13, Lemma 3.25(c)] is based on an explicit construction of the pair (p,q). In the choice of $p,q \in K$, condition (B) for q requires that the Legendre symbol $\left(\frac{q}{\mathfrak{p}_0}\right)$ is equal to -1. This implies that $v_{\mathfrak{p}_0}(q) = 0$ and that q is not a square modulo $\mathfrak{p}_0$.

Condition (4) for p is $(q,p)_{\mathfrak{p}_0} = -1$. Using the explicit formula for the Hilbert symbol, we compute

$$-1 = (q,p)_{\mathfrak{p}_0} = (-1)^{v_{\mathfrak{p}_0}(q)v_{\mathfrak{p}_0}(p)\frac{|\mathbb{F}_{\mathfrak{p}_0}|-1}{2}} \left(\frac{q}{\mathfrak{p}_0}\right)^{v_{\mathfrak{p}_0}(p)} \left(\frac{p}{\mathfrak{p}_0}\right)^{v_{\mathfrak{p}_0}(q)} = \left(\frac{q}{\mathfrak{p}_0}\right)^{v_{\mathfrak{p}_0}(p)},$$

since $v_{\mathfrak{p}_0}(q) = 0$. As $\left(\frac{q}{\mathfrak{p}_0}\right) = -1$, this implies that $v_{\mathfrak{p}_0}(p)$ is odd. By multiplying p by a square in $K^\times$, we may further assume that $v_{\mathfrak{p}_0}(p) = 1$.

Global function field case. This is addressed in the proof of Lemma 3.17(3) in [EM18]. In the construction, the element q again satisfies $\left(\frac{q}{\mathfrak{p}_0}\right) = -1$. Since $\mathfrak{p}_0 \in \Delta_{ap,q}$, we have $(ap,q)_{\mathfrak{p}_0} = -1$. By computing the Hilbert symbol and using the fact that $\mathfrak{p}_0 \nmid a$, we conclude that $v_{\mathfrak{p}_0}(p)$ is odd. This is stated explicitly in the third-to-last line of the proof of [EM18, Theorem 1.3]. ∎

Remark 3.10. In fact, the sets R_p^σ, $J(R_p^\sigma)$, $R_{p,q}^{(1,1)}$, and $J(R_{p,q}^{(1,1)})$ are not only diophantine, but are defined uniformly in the parameters p and q. More precisely, the following sets are diophantine:

$$\{(p,x) \in K^\times \times K \mid x \in R_p^\sigma\},$$
$$\{(p,x) \in K^\times \times K \mid x \in J(R_p^\sigma)\},$$
$$\{(p,q,x) \in K^\times \times K^\times \times K \mid x \in R_{p,q}^{(1,1)}\},$$
$$\{(p,q,x) \in K^\times \times K^\times \times K \mid x \in J(R_{p,q}^{(1,1)})\}.$$

For the rings R_p^σ and $R_{p,q}^{(1,1)}$, this uniformity follows from the uniform definability of $T_{a,b}$ (see Remark 3.2), together with Lemmas 3.1 and 3.7(1). For the corresponding Jacobson radicals, the uniformity follows from [Par13, Lemma 3.17], Lemma 3.6, and Lemma 3.7(2).

3.2. Diagonalization of quadratic forms. Since we always work over a global field K with characteristic not equal to 2, we obtain the following proposition concerning the diagonalization of quadratic forms by congruence.

Proposition 3.11. *Let*

$$f = \sum_{1 \le i,j \le m} a_{ij} x_i x_j$$

be a quadratic form in m variables over K. Define the symmetric matrix $A = [A_{ij}]_{1 \le i,j \le m}$ by setting $A_{ii} = a_{ii}$ and $A_{ij} = \frac{a_{ij}+a_{ji}}{2}$ for $i \ne j$. Then there exist m^2 polynomials

$$(h_{kl})_{1 \le k,l \le m} \subset \mathbb{Z}[\overline{t_{ij}}, \overline{u_{rs}}],$$

depending only on m, where $\overline{t_{ij}}$ denotes the m^2 variables $(t_{ij})_{1 \le i,j \le m}$ and $\overline{u_{rs}}$ denotes the m^2 variables $(u_{rs})_{1 \le r,s \le m}$, such that the following statements are equivalent:

(1) *The quadratic form f is anisotropic over K.*
(2) *There exist $b_1, \ldots, b_m \in K^\times$ such that the diagonal quadratic form*

$$\sum_{i=1}^{m} b_i x_i^2$$

is anisotropic over K, and there exist $(u_{rs})_{1\le r,s\le m} \in (K)^{m^2}$ satisfying

$$\begin{cases} h_{kl}(\overline{A_{ij}}, \overline{u_{rs}}) = 0, & 1 \le k \ne l \le m, \\ h_{kk}(\overline{A_{ij}}, \overline{u_{rs}}) = b_k, & 1 \le k \le m. \end{cases}$$

Proof. Consider the ring $M_{m\times m}(\mathbb{Z}[\overline{t_{ij}}, \overline{u_{rs}}])$ of $m \times m$ matrices with entries in $\mathbb{Z}[\overline{t_{ij}}, \overline{u_{rs}}]$. Define two matrices

$$T := [t_{ij}]_{1\le i,j\le m} \in M_{m\times m}(\mathbb{Z}[\overline{t_{ij}}]) \subset M_{m\times m}(\mathbb{Z}[\overline{t_{ij}}, \overline{u_{rs}}]),$$
$$U := [u_{rs}]_{1\le r,s\le m} \in M_{m\times m}(\mathbb{Z}[\overline{u_{rs}}]) \subset M_{m\times m}(\mathbb{Z}[\overline{t_{ij}}, \overline{u_{rs}}]).$$

Then

$$U^t T U \in M_{m\times m}(\mathbb{Z}[\overline{t_{ij}}, \overline{u_{rs}}]),$$

and the (k,l)th entry of $U^t T U$ is a polynomial

$$h_{kl} \in \mathbb{Z}[\overline{t_{ij}}, \overline{u_{rs}}].$$

By construction, the polynomials h_{kl} depend only on the number m of variables.

For matrices

$$A := [A_{ij}]_{1\le i,j\le m} \in M_{m\times m}(K), \qquad C := [C_{rs}]_{1\le r,s\le m} \in M_{m\times m}(K),$$

we define the evaluation of $H = (h_{kl})$ at A and C by

$$H(A, C)_{kl} := h_{kl}(\overline{A_{ij}}, \overline{C_{rs}}) \in K.$$

This is well-defined since if $\mathrm{char}(K) = 0$, then $\mathbb{Z} \subset K$, and if $\mathrm{char}(K) = p > 0$, we interpret the polynomials modulo p.

Let $B = \mathrm{diag}(b_1, \ldots, b_m)$ be a diagonal matrix. Then the matrix equation

$$C^t A C = B$$

is equivalent to

$$\begin{cases} h_{kl}(\overline{A_{ij}}, \overline{C_{rs}}) = 0, & 1 \le k \ne l \le m, \\ h_{kk}(\overline{A_{ij}}, \overline{C_{rs}}) = b_k, & 1 \le k \le m. \end{cases}$$

If f has full rank m, the existence of $b_1, \ldots, b_m \in K^\times$ and $C \in (K)^{m^2}$ satisfying this system is equivalent to the diagonalization of f as

$$\sum_{i=1}^{m} b_i x_i^2.$$

The diagonal form $\sum_{i=1}^{m} b_i x_i^2$ is isotropic over K if and only if there is a nonzero vector $x = (x_1, \ldots, x_m) \in (K)^m$ such that

$$\sum_{i=1}^{m} b_i x_i^2 = x^t B x = x^t C^t A C x = 0,$$

which is equivalent to $f(Cx) = 0$. The matrix C is invertible, since $B = \mathrm{diag}(b_1, \ldots, b_m)$ is invertible. The vector Cx is nonzero since C is invertible. So Cx is an isotropic vector of f. Conversely, if $y = (y_1, \ldots, y_m)$ is an isotropic vector of f over K, then $C^{-1}y$ is an isotropic vector of the diagonal form $\sum_{i=1}^{m} b_i x_i^2$. Therefore, f is isotropic over K if and only if the diagonal form $\sum_{i=1}^{m} b_i x_i^2$ is isotropic over K.

If the rank of f is less than m, then f is always isotropic, and the equivalence holds trivially.

In conclusion, condition (2) implies (1) by the above discussion, and (1) implies (2) since the symmetric matrix A is congruent to a diagonal matrix over K. ∎

Under the assumption that our main theorem (Theorem 1.3) holds, Corollary 1.5 follows immediately from the diagonalization process in Proposition 3.11. We now give a precise derivation.

Proof of Corollary 1.5. Let $f = \sum_{1 \le i,j \le m} a_{ij} x_i x_j$ be a quadratic form defined over K. Let $A = [A_{ij}]_{1 \le i,j \le m} \in M_{m \times m}(K)$ be the matrix defined in Proposition 3.11. By Proposition 3.11, f is anisotropic over K if and only if there exist $b_1, \ldots, b_m \in K^\times$ and $C_{rs} \in K$ $(1 \le r, s \le m)$ such that

$$h_{kl}(\overline{A_{ij}}, \overline{C_{rs}}) = 0, \qquad 1 \le k \ne l \le m,$$
$$h_{kk}(\overline{A_{ij}}, \overline{C_{rs}}) = b_k, \qquad 1 \le k \le m,$$

and the diagonal quadratic form $\sum_{i=1}^{m} b_i x_i^2$ is anisotropic over K.

By Theorem 1.3, the condition that the diagonal form $\sum_{i=1}^{m} b_i x_i^2$ is anisotropic over K is diophantine. Therefore, the set of coefficients $(a_{ij})_{1 \le i,j \le m}$ for which f is anisotropic is diophantine, proving Corollary 1.5. ∎

4. Proof of the main results

4.1. Dealing with a single prime. Our strategy consists in partitioning the set of primes into finitely many classes and handling the primes in each class in a uniform manner. As a preliminary step, we consider the local case for a single prime.

The following lemma, which is a slightly different version of [EM18, Lemma 4.4], is restated here for completeness, as it constitutes a key ingredient in our proof.

LEMMA 4.1. *Let $\mathfrak{p}$ be a finite prime of K such that the residue field $\mathbb{F}_\mathfrak{p}$ has odd characteristic. Fix $p, s \in K^\times$ such that $v_\mathfrak{p}(p)$ is odd, $v_\mathfrak{p}(s) = 0$ and the reduction $\mathrm{red}_\mathfrak{p}(s)$ is not a square in $\mathbb{F}_\mathfrak{p}$. Then for $x, y \in K^\times$, $(x, y)_\mathfrak{p} = -1$ if and only if*

$$((x \in p \cdot K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times) \wedge (y \text{ or } -xy \text{ is in } s \cdot K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p}))) \\ \vee ((y \in p \cdot K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times) \wedge (x \text{ or } -xy \text{ is in } s \cdot K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p}))).$$

Proof. We modify the condition $v_\mathfrak{p}(p) = 1$ used in [EM18, Lemma 4.4] to the more general condition that $v_\mathfrak{p}(p)$ is odd. This modification does not alter the set $p \cdot K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times$. ∎

Moreover, we need the following elementary observation to obtain an equivalent form of Lemma 4.1, which is Lemma 4.3.

LEMMA 4.2. *Let $\mathfrak{p}$ be a finite prime of K such that $|\mathbb{F}_\mathfrak{p}|$ is odd. Fix $p, s \in K^\times$ such that $v_\mathfrak{p}(p) = 1$ and $v_\mathfrak{p}(s) = 0$, with $\mathrm{red}_\mathfrak{p}(s)$ being a nonsquare in the residue field $\mathbb{F}_\mathfrak{p}$. Then for $x \in K^\times$, the following hold:*

(1) *$v_\mathfrak{p}(x)$ is even if and only if $x \in K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times$.*
(2) *$v_\mathfrak{p}(x)$ is odd if and only if $x \in p \cdot K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times$.*
(3) *$x \in K_\mathfrak{p}^{\times 2}$ if and only if $x \in K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p})$.*
(4) *$x \notin K_\mathfrak{p}^{\times 2}$ if and only if $x \in s \cdot K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p}) \vee x \in p \cdot K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times$.*

Consequently, we have the following two partitions of $K^\times$:

$$\begin{aligned} K^\times &= (K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times) \sqcup (p \cdot K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times) \\ &= (K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p})) \sqcup (s \cdot K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p})) \sqcup (p \cdot K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times). \end{aligned}$$

Proof. (1) The valuation $v_\mathfrak{p}(x)$ is even if and only if it can be reduced to 0 by multiplication by a square in $K^\times$, which is equivalent to $x \in K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times$.

(2) $v_\mathfrak{p}(x)$ is odd if and only if $v_\mathfrak{p}(p^{-1}x)$ is even, which is equivalent to $p^{-1}x \in K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times$ by (1), hence also equivalent to $x \in p \cdot K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times$.

(3) First, if $u \in 1 + \mathfrak{p}\mathcal{O}_\mathfrak{p}$, then $u \in K_\mathfrak{p}^{\times 2}$ by the local square theorem (see [O'M00, 63:1]). Conversely, suppose $u \in K_\mathfrak{p}^{\times 2}$. By multiplying by a suitable square in $K^\times$, we may assume $v_\mathfrak{p}(u) = 0$. Let $t \in K_\mathfrak{p}^\times$ be such that $u = t^2$. Since K is dense in the local field $K_\mathfrak{p}$, there exists $\eta \in K$ such that $v_\mathfrak{p}(\eta - t) \geq 1$. Given that $v_\mathfrak{p}(t) = 0$, we have $v_\mathfrak{p}(\eta) = \min\{v_\mathfrak{p}(\eta - t), v_\mathfrak{p}(t)\} = 0$, which implies $\eta \in \mathcal{O}_\mathfrak{p}^\times$. It follows that

$$u - \eta^2 = (t - \eta)(t + \eta) \in \mathfrak{p}\mathcal{O}_\mathfrak{p},$$

and therefore $u \in \eta^2 + \mathfrak{p}\mathcal{O}_\mathfrak{p} = \eta^2(1 + \mathfrak{p}\mathcal{O}_\mathfrak{p})$. This shows $u \in K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p})$.

(4) For $x \notin K_\mathfrak{p}^{\times 2}$, we consider two cases based on the parity of the valuation:

- If $v_{\mathfrak{p}}(x)$ is odd, then $x \in p \cdot K^{\times 2} \cdot \mathcal{O}_{\mathfrak{p}}^{\times}$ follows immediately from (2).
- If $v_{\mathfrak{p}}(x)$ is even, we can write $x = p^{2k}u$ with $v_{\mathfrak{p}}(u) = 0$ and $u \notin K_{\mathfrak{p}}^{\times 2}$. According to [O'M00, 63:9], the index $[\mathcal{O}_{\mathfrak{p}}^{\times} : \mathcal{O}_{\mathfrak{p}}^{\times 2}]$ is 2. Since $\mathrm{red}_{\mathfrak{p}}(s)$ is not a square in the residue field, us must be a square in $K_{\mathfrak{p}}^{\times}$. By the result in (3), this implies $sx \in K^{\times 2} \cdot (1+\mathfrak{p}\mathcal{O}_{\mathfrak{p}})$, or equivalently $x \in s \cdot K^{\times 2} \cdot (1+\mathfrak{p}\mathcal{O}_{\mathfrak{p}})$. ∎

LEMMA 4.3. *With the same notation as in Lemma* 4.1*, for* $x, y \in K^{\times}$*,* $(x, y)_{\mathfrak{p}} = 1$ *if and only if*

$$((x \in K^{\times 2} \cdot \mathcal{O}_{\mathfrak{p}}^{\times}) \vee (y, -xy \in (K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}})) \cup (p \cdot K^{\times 2} \cdot \mathcal{O}_{\mathfrak{p}}^{\times})))$$
$$\wedge ((y \in K^{\times 2} \cdot \mathcal{O}_{\mathfrak{p}}^{\times}) \vee (x, -xy \in (K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}})) \cup (p \cdot K^{\times 2} \cdot \mathcal{O}_{\mathfrak{p}}^{\times}))).$$

Proof. By Lemma 4.1, $(x, y)_{\mathfrak{p}} = -1$ if and only if

$$((x \in p \cdot K^{\times 2} \cdot \mathcal{O}_{\mathfrak{p}}^{\times}) \wedge (y \text{ or } -xy \text{ is in } s \cdot K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}})))$$
$$\vee ((y \in p \cdot K^{\times 2} \cdot \mathcal{O}_{\mathfrak{p}}^{\times}) \wedge (x \text{ or } -xy \text{ is in } s \cdot K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}}))).$$

To get $(x, y)_{\mathfrak{p}} = 1$, we take the negation of this condition. By the partitions established in Lemma 4.2, the complement of the set $p \cdot K^{\times 2} \cdot \mathcal{O}_{\mathfrak{p}}^{\times}$ in $K^{\times}$ is $K^{\times 2} \cdot \mathcal{O}_{\mathfrak{p}}^{\times}$. Similarly, the complement of $s \cdot K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}})$ in the union of the two nonsquare classes is given by

$$x \in (K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}})) \cup (p \cdot K^{\times 2} \cdot \mathcal{O}_{\mathfrak{p}}^{\times}).$$

Applying De Morgan's laws and substituting these complements yields the desired characterization. ∎

In the dyadic case (which means $\mathfrak{p} \mid 2$), one obtains a characterization of local squares similar to the one presented in Lemma 4.2 (3). However, due to the requirements of the stronger version of Hensel's Lemma for even primes, a higher power of the prime ideal $\mathfrak{p}$ is necessary. Specifically, we have the following result:

LEMMA 4.4. *Let* K *be a number field and* $\mathfrak{p}$ *a prime dividing* 2*. Let* e *be the absolute ramification index. Then*

$$K^{\times 2} \cdot (1 + \mathfrak{p}^{2e+1}\mathcal{O}_{\mathfrak{p}}) = K \cap K_{\mathfrak{p}}^{\times 2}.$$

Proof. Suppose that $u \in 1 + \mathfrak{p}^{2e+1}\mathcal{O}_{\mathfrak{p}}$. By [O'M00, 63:1], u is a local square, so $u \in K_{\mathfrak{p}}^{\times 2}$. Since $u \in K$ by assumption, it follows that $u \in K \cap K_{\mathfrak{p}}^{\times 2}$. This establishes the inclusion $K^{\times 2} \cdot (1 + \mathfrak{p}^{2e+1}\mathcal{O}_{\mathfrak{p}}) \subseteq K \cap K_{\mathfrak{p}}^{\times 2}$.

Conversely, let $x \in K \cap K_{\mathfrak{p}}^{\times 2}$. We can write $x = \pi^{2k}u$, where $v_{\mathfrak{p}}(\pi) = 1$ and $u \in \mathcal{O}_{\mathfrak{p}}^{\times} \cap K_{\mathfrak{p}}^{\times 2}$. Let $s \in \mathcal{O}_{\mathfrak{p}}^{\times}$ be such that $u = s^2$. If $s \in K$, the result is trivial. If $s \notin K$, then by the density of K in $K_{\mathfrak{p}}$, there exists $\eta \in K$ such that

$$v_{\mathfrak{p}}(\eta - s) \geq 2e + 1.$$

Since $v_{\mathfrak{p}}(s) = 0$ and $2e + 1 > 0$, the properties of valuations imply $v_{\mathfrak{p}}(\eta) = v_{\mathfrak{p}}(\eta - s + s) = \min\{v_{\mathfrak{p}}(\eta - s), v_{\mathfrak{p}}(s)\} = 0$, hence $\eta \in \mathcal{O}_{\mathfrak{p}}^{\times}$.

To show that $u\eta^{-2} \in 1 + \mathfrak{p}^{2e+1}\mathcal{O}_{\mathfrak{p}}$, we consider the difference

$$u - \eta^2 = (s - \eta)(s + \eta).$$

By our choice of η, we have $v_{\mathfrak{p}}(s - \eta) \geq 2e + 1$. For the second factor, since $s + \eta = (s - \eta) + 2\eta$, and noting that $v_{\mathfrak{p}}(s - \eta) \geq 2e + 1 > e = v_{\mathfrak{p}}(2\eta)$, we have

$$v_{\mathfrak{p}}(s + \eta) = v_{\mathfrak{p}}(2\eta) = e.$$

Therefore, $v_{\mathfrak{p}}(u - \eta^2) = v_{\mathfrak{p}}(s - \eta) + v_{\mathfrak{p}}(s + \eta) \geq (2e + 1) + e = 3e + 1$. In particular, this implies $v_{\mathfrak{p}}(u - \eta^2) \geq 2e + 1$. Since $v_{\mathfrak{p}}(\eta^2) = 0$, we conclude that

$$u \in \eta^2(1 + \mathfrak{p}^{2e+1}\mathcal{O}_{\mathfrak{p}}),$$

so $x \in K^{\times 2} \cdot (1 + \mathfrak{p}^{2e+1}\mathcal{O}_{\mathfrak{p}})$. This proves the reverse inclusion $K \cap K_{\mathfrak{p}}^{\times 2} \subseteq K^{\times 2} \cdot (1 + \mathfrak{p}^{2e+1}\mathcal{O}_{\mathfrak{p}})$. ∎

THEOREM 4.5. *Let $\mathfrak{p}$ be a finite or real infinite prime of K. The set*

$$\{(a_1, a_2, a_3, a_4) \in (K^{\times})^4 \mid f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \text{ is anisotropic over } K_{\mathfrak{p}}\}$$

is diophantine over K.

Proof. If $\mathfrak{p} \in S_K^f$, then by Theorem 2.3(3), f is anisotropic over $K_{\mathfrak{p}}$ if and only if $a_1a_2a_3a_4 \in K_{\mathfrak{p}}^{\times 2}$ and $(a_1, a_2)_{\mathfrak{p}} = -(-a_3, -a_4)_{\mathfrak{p}}$. To establish that this condition defines a diophantine set, it suffices to verify that the following three types of sets are diophantine:

(1) $\{x \in K^{\times} \mid x \in K_{\mathfrak{p}}^{\times 2}\}$,
(2) $\{(x, y) \in K^{\times} \times K^{\times} \mid (x, y)_{\mathfrak{p}} = 1\}$,
(3) $\{(x, y) \in K^{\times} \times K^{\times} \mid (x, y)_{\mathfrak{p}} = -1\}$.

Based on the first three chapters of [Rum80], the valuation ring $\mathcal{O}_{\mathfrak{p}}$ is diophantine over K. Consequently, the maximal ideal $\mathfrak{p}\mathcal{O}_{\mathfrak{p}} = \pi\mathcal{O}_{\mathfrak{p}}$ (where $v_{\mathfrak{p}}(\pi) = 1$) is also diophantine. More precisely, [Rum80, Theorem 1] implies that $\mathcal{O}_{\mathfrak{p}}$ is definable, and since the predicate $S_l(x, \vec{c})$ is given by an existential positive formula, it is diophantine.

If $|\mathbb{F}_{\mathfrak{p}}|$ is odd, the diophantine nature of (2) and (3) follows from Lemma 4.1 and Lemma 4.3, as these sets are constructed from $\mathcal{O}_{\mathfrak{p}}$ and $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ using field operations and logical disjunction/conjunction. Additionally, Lemma 4.2(3) ensures that the set in (1) is diophantine.

If K is a number field and $\mathfrak{p} \mid 2$, the index $[K_{\mathfrak{p}}^{\times} : K_{\mathfrak{p}}^{\times 2}]$ is finite (see [O'M00, 63:9]). Let $s_1, \ldots, s_n \in K^{\times}$ be a set of representatives for the cosets of $K_{\mathfrak{p}}^{\times 2}$ in $K_{\mathfrak{p}}^{\times}$. Such representatives can be chosen in $K^{\times}$ because K is dense

in $K_\mathfrak{p}$ and the cosets are open in the local topology. Let e be the absolute ramification index. We define the sets

$$S_i := s_i \cdot K^{\times 2} \cdot (1 + \mathfrak{p}^{2e+1}\mathcal{O}_\mathfrak{p}) \quad \text{for } i = 1, \ldots, n.$$

The sets $S_1, \ldots, S_n$ form a partition of $K^\times \cap K_\mathfrak{p}^\times$. This follows from two facts:

- The sets are disjoint: if $i \neq j$, then $s_i s_j^{-1} \notin K_\mathfrak{p}^{\times 2}$. By Lemma 4.4, the set $K^{\times 2} \cdot (1 + \mathfrak{p}^{2e+1}\mathcal{O}_\mathfrak{p})$, being a subset of $K_\mathfrak{p}^{\times 2}$, cannot contain $s_i s_j^{-1}$.
- They cover the relevant elements: if $x \in K \cap s_i K_\mathfrak{p}^{\times 2}$, then $s_i^{-1} x \in K \cap K_\mathfrak{p}^{\times 2}$. By Lemma 4.4, we have $s_i^{-1} x \in K^{\times 2} \cdot (1 + \mathfrak{p}^{2e+1}\mathcal{O}_\mathfrak{p})$, which implies $x \in S_i$.

Under this partition, $x \in K_\mathfrak{p}^{\times 2}$ if and only if $x \in S_i$ for $s_i \in K_\mathfrak{p}^{\times 2}$. Furthermore, the Hilbert symbol conditions satisfy

$$(x, y)_\mathfrak{p} = 1 \iff (x, y) \in \bigcup_{(s_i, s_j)_\mathfrak{p} = 1} (S_i \times S_j),$$

$$(x, y)_\mathfrak{p} = -1 \iff (x, y) \in \bigcup_{(s_i, s_j)_\mathfrak{p} = -1} (S_i \times S_j).$$

Since $\mathfrak{p}^{2e+1}\mathcal{O}_\mathfrak{p}$ is diophantine, each S_i is diophantine, and so are their finite unions.

For a real infinite prime $\mathfrak{p}$, let $\omega\colon K \hookrightarrow \mathbb{R}$ be the corresponding embedding. Then [EM18, Lemma 4.1] states that the set $P_\omega := \{x \in K^\times \mid \omega(x) > 0\}$ is diophantine over K. The form f is anisotropic over $K_\mathfrak{p} \cong \mathbb{R}$ if and only if it is definite, i.e.,

$$\Big(\bigwedge_{i=1}^{4} a_i \in P_\omega\Big) \vee \Big(\bigwedge_{i=1}^{4} -a_i \in P_\omega\Big).$$

Since P_ω is diophantine, this condition defines a diophantine set. ∎

4.2. The proof of main theorem. Now we prove our main result, Theorem 1.3.

LEMMA 4.6. *Let $f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$ denote the quadratic form with coefficients a_1, a_2, a_3, a_4. The set*

$$\{(a_1, a_2, a_3, a_4) \in (K^\times)^4 \mid f \text{ is anisotropic over some } \mathfrak{p} \in S_K\}$$

is diophantine.

Proof. Recall that the elements a, b (or a, b, c, d) in $K^\times$ and the admissible modulus $\mathfrak{m}$ are defined as in Lemma 3.4 and the rings R_p^σ for $\sigma \in \mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K)$ are defined as in Definition 3.5.

For $\sigma \in \mathrm{Gal}(K(\sqrt{a},\sqrt{b})/K)$ with $\sigma \neq (1,1)$, define

$$s_\sigma := \begin{cases} a & \text{if } \sigma = (-1,\pm 1), \\ b & \text{if } \sigma = (1,-1). \end{cases}$$

We claim that the quadratic form

$$f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$$

is anisotropic over some $\mathfrak{p} \in S_K$ if and only if *one of the following three conditions holds.*

(i) There exists a prime $\mathfrak{p} \mid \mathfrak{m}$ such that f is anisotropic over $K_\mathfrak{p}$.

(ii) There exists $\sigma \neq (1,1)$ and an element $p \in \Phi_\sigma$ such that

$$\big((\dagger^+_{a_1,a_2} \wedge \dagger^-_{-a_3,-a_4}) \vee (\dagger^-_{a_1,a_2} \wedge \dagger^+_{-a_3,-a_4})\big) \wedge \mathfrak{e},$$

where

$$\mathfrak{e}\colon \quad a_1a_2a_3a_4 \in K^{\times 2} \cdot (1 + J(R_p^\sigma)).$$

Here the formulas $\dagger^\pm_{x,y}$ are defined as follows:

$$\begin{aligned} \dagger^-_{x,y} := \big(&x \in p \cdot K^{\times 2} \cdot (R_p^\sigma)^\times \\ &\wedge (y \text{ or } -xy \text{ is in } s_\sigma \cdot K^{\times 2} \cdot (1 + J(R_p^\sigma)))\big) \\ \vee \big(&y \in p \cdot K^{\times 2} \cdot (R_p^\sigma)^\times \\ &\wedge (x \text{ or } -xy \text{ is in } s_\sigma \cdot K^{\times 2} \cdot (1 + J(R_p^\sigma)))\big), \end{aligned}$$

$$\begin{aligned} \dagger^+_{x,y} := \big(&x \in K^{\times 2} \cdot (R_p^\sigma)^\times \\ &\vee (y, -xy \in p \cdot K^{\times 2} \cdot (R_p^\sigma)^\times \cup K^{\times 2} \cdot (1 + J(R_p^\sigma)))\big) \\ \wedge \big(&y \in K^{\times 2} \cdot (R_p^\sigma)^\times \\ &\vee (x, -yx \in p \cdot K^{\times 2} \cdot (R_p^\sigma)^\times \cup K^{\times 2} \cdot (1 + J(R_p^\sigma)))\big). \end{aligned}$$

(iii) There exists $(p,q) \in \Psi_K$ such that $q \in (R_{p,q}^{(1,1)})^\times$ and

$$\big((\ddagger^+_{a_1,a_2} \wedge \ddagger^-_{-a_3,-a_4}) \vee (\ddagger^-_{a_1,a_2} \wedge \ddagger^+_{-a_3,-a_4})\big) \wedge \mathfrak{e}',$$

where $\mathfrak{e}'$ is defined analogously to $\mathfrak{e}$, with R_p^σ replaced by $R_{p,q}^{(1,1)}$. The formulas $\ddagger^\pm_{x,y}$ are given by

$$\begin{aligned} \ddagger^-_{x,y} := \big(&x \in p \cdot K^{\times 2} \cdot (R_{p,q}^{(1,1)})^\times \\ &\wedge (y \text{ or } -xy \text{ is in } q \cdot K^{\times 2} \cdot (1 + J(R_{p,q}^{(1,1)})))\big) \\ \vee \big(&y \in p \cdot K^{\times 2} \cdot (R_{p,q}^{(1,1)})^\times \\ &\wedge (x \text{ or } -yx \text{ is in } q \cdot K^{\times 2} \cdot (1 + J(R_{p,q}^{(1,1)})))\big), \end{aligned}$$

$$\begin{aligned}\ddagger^{+}_{x,y} := \big(&x \in K^{\times 2}\cdot(R^{(1,1)}_{p,q})^{\times}\\ &\vee (y, -xy \in p\cdot K^{\times 2}\cdot(R^{(1,1)}_{p,q})^{\times} \cup K^{\times 2}\cdot(1+J(R^{(1,1)}_{p,q})))\big)\\ \wedge \big(&y \in K^{\times 2}\cdot(R^{(1,1)}_{p,q})^{\times}\\ &\vee (x, -yx \in p\cdot K^{\times 2}\cdot(R^{(1,1)}_{p,q})^{\times} \cup K^{\times 2}\cdot(1+J(R^{(1,1)}_{p,q})))\big).\end{aligned}$$

The first condition defines a diophantine set, since only finitely many primes divide $\mathfrak{m}$ and by Theorem 4.5. The second and third conditions also define diophantine sets by Proposition 3.9(1) together with Remark 3.10. Consequently, the set

$$\{(a_1,a_2,a_3,a_4) \in (K^{\times})^4 \mid f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \text{ is anisotropic over some } \mathfrak{p} \in S_K\}$$

is diophantine, being a finite union of the three sets defined above. It remains to verify that the claim holds. For brevity, we write

$$\begin{aligned}\dagger &:= (\dagger^{+}_{a_1,a_2} \wedge \dagger^{-}_{-a_3,-a_4}) \vee (\dagger^{-}_{a_1,a_2} \wedge \dagger^{+}_{-a_3,-a_4}),\\ \ddagger &:= (\ddagger^{+}_{a_1,a_2} \wedge \ddagger^{-}_{-a_3,-a_4}) \vee (\ddagger^{-}_{a_1,a_2} \wedge \ddagger^{+}_{-a_3,-a_4}).\end{aligned}$$

The primes $\mathfrak{p} \nmid \mathfrak{m}$ can be classified according to $\sigma \in \mathrm{Gal}(K(\sqrt{a},\sqrt{b})/K)$. By Theorem 2.3(3), the condition that f is anisotropic over $\mathfrak{p} \nmid \mathfrak{m}$ is equivalent to

$$(a_1,a_2)_{\mathfrak{p}} = -(-a_3,-a_4)_{\mathfrak{p}} \quad \text{and} \quad a_1a_2a_3a_4 \in K_{\mathfrak{p}}^{\times 2}.$$

Hence, it suffices to establish the following two equivalences between the statements in our claim and this local condition for the different types of primes $\mathfrak{p}$.

- For $\sigma \neq (1,1)$, the sentence

  $$\exists p \in \Phi_\sigma \text{ such that } \dagger \wedge \mathfrak{e}$$

  is equivalent to the existence of a prime $\mathfrak{p}$ with $\psi_{L/K}(\mathfrak{p}) = \sigma$ such that

  $$(a_1,a_2)_{\mathfrak{p}} = -(-a_3,-a_4)_{\mathfrak{p}} \quad \text{and} \quad a_1a_2a_3a_4 \in K_{\mathfrak{p}}^{\times 2}.$$

- The sentence

  $$\exists (p,q) \in \Psi_K \text{ such that } q \in (R^{(1,1)}_{p,q})^{\times} \text{ and } \ddagger \wedge \mathfrak{e}'$$

  is equivalent to the existence of a prime $\mathfrak{p}$ with $\psi_{L/K}(\mathfrak{p}) = (1,1)$ such that

  $$(a_1,a_2)_{\mathfrak{p}} = -(-a_3,-a_4)_{\mathfrak{p}} \quad \text{and} \quad a_1a_2a_3a_4 \in K_{\mathfrak{p}}^{\times 2}.$$

For $\sigma \neq (1,1)$, suppose there exists $p \in \Phi_\sigma$ such that $\dagger$ holds. Then, by Proposition 3.9(2), the set $\mathbb{P}^{\sigma}(p)$ is nonempty.

Let $\mathfrak{p} \in \mathbb{P}^\sigma(p)$. Recall that the formula $\dagger^-_{x,y}$ is given by

$$\big((x \in p \cdot K^{\times 2} \cdot (R_p^\sigma)^\times) \wedge (y \text{ or } -xy \text{ is in } s_\sigma \cdot K^{\times 2} \cdot (1 + J(R_p^\sigma)))\big)$$
$$\vee \big((y \in p \cdot K^{\times 2} \cdot (R_p^\sigma)^\times) \wedge (x \text{ or } -yx \text{ is in } s_\sigma \cdot K^{\times 2} \cdot (1 + J(R_p^\sigma)))\big).$$

By Lemma 3.4 and the definition of R_p^σ, we have $R_p^\sigma \subset \mathcal{O}_\mathfrak{p}$. Moreover, by Lemma 3.6, $J(R_p^\sigma) \subset \mathfrak{p}\mathcal{O}_\mathfrak{p}$.

Hence, $\dagger^-_{x,y}$ implies $(x,y)_\mathfrak{p} = -1$, because $v_\mathfrak{p}(p)$ is odd, by Lemma 4.1, and since s_σ is a $\mathfrak{p}$-adic unit which is not a square (by the construction of s_σ and the definition of the Artin map). For example, if $\sigma = (1,-1)$, then b is not a square modulo $\mathfrak{p}$ since $\psi_{L/K}(\mathfrak{p}) = (1,-1)$.

By Lemma 4.3 and a similar argument, $\dagger^+_{x,y}$ implies $(x,y)_\mathfrak{p} = 1$.

Finally, the formula $\mathfrak{e}$ implies

$$a_1a_2a_3a_4 \in K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p}),$$

which means that $a_1a_2a_3a_4$ is a square in $K_\mathfrak{p}$ by Lemma 4.2(3).

Therefore, $\dagger \wedge \mathfrak{e}$ implies

$$(a_1,a_2)_\mathfrak{p} = -(-a_3,-a_4)_\mathfrak{p} \quad \text{and} \quad a_1a_2a_3a_4 \in K_\mathfrak{p}^{\times 2}.$$

Conversely, suppose there exists a prime $\mathfrak{p} \nmid \mathfrak{m}$ with $\psi_{L/K}(\mathfrak{p}) = \sigma$ such that

$$(a_1,a_2)_\mathfrak{p} = -(-a_3,-a_4)_\mathfrak{p} \quad \text{and} \quad a_1a_2a_3a_4 \in K_\mathfrak{p}^{\times 2}.$$

Then, by Proposition 3.9(3), we can find $p \in \Phi_\sigma$ such that $\mathbb{P}^\sigma(p) = \{\mathfrak{p}\}$. In this situation, for $\sigma \neq (1,1)$, we have

$$R_p^\sigma = \mathcal{O}_\mathfrak{p}.$$

Therefore, the formula $\dagger^\pm_{x,y}$ can be deduced directly from $(x,y)_\mathfrak{p} = \pm 1$, and the formula $\mathfrak{e}$ can be deduced from

$$a_1a_2a_3a_4 \in K_\mathfrak{p}^{\times 2}.$$

Hence, we conclude that $\dagger \wedge \mathfrak{e}$ follows from

$$(a_1,a_2)_\mathfrak{p} = -(-a_3,-a_4)_\mathfrak{p} \quad \text{and} \quad a_1a_2a_3a_4 \in K_\mathfrak{p}^{\times 2}.$$

A similar argument establishes the second equivalence, using Proposition 3.9(4), (5). We now handle the case $\psi_{L/K}(\mathfrak{p}) = (1,1)$.

Assume $\mathfrak{p}_0 \in I_\mathfrak{m}$ with $\psi_{L/K}(\mathfrak{p}_0) = (1,1)$. Then by Proposition 3.9, we can find $(p,q) \in \Psi_K$ such that

$$\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}_0\}.$$

Moreover,

$$v_{\mathfrak{p}_0}(p) = 1, \quad v_{\mathfrak{p}_0}(q) = 0,$$

and q is not a square modulo $\mathfrak{p}_0$. Then, by Lemmas 4.1–4.3, the condition

$$(a_1,a_2)_{\mathfrak{p}_0} = -(-a_3,-a_4)_{\mathfrak{p}_0} \quad \text{and} \quad a_1a_2a_3a_4 \in K_{\mathfrak{p}_0}^{\times 2}$$

implies $\ddagger \wedge \mathfrak{e}'$, since $R_{p,q}^{(1,1)} = \mathcal{O}_{\mathfrak{p}_0}$ and $J(R_{p,q}^{(1,1)}) = \mathfrak{p}_0\mathcal{O}_{\mathfrak{p}_0}$.

Conversely, suppose $(p,q) \in \Psi_K$; then by Proposition 3.9, we have $\Delta_{ap,q} \cap \Delta_{bp,q} \neq \emptyset$. For any $\mathfrak{p} \in \Delta_{ap,q} \cap \Delta_{bp,q}$, since $q \in (R_{p,q}^{(1,1)})^\times$ and

$$(ap,q)_\mathfrak{p} = (bp,q)_\mathfrak{p} = -1,$$

we obtain

$$\left(\frac{q}{\mathfrak{p}}\right)^{v_\mathfrak{p}(bp)} = \left(\frac{q}{\mathfrak{p}}\right)^{v_\mathfrak{p}(ap)} = -1.$$

Hence q is not a square modulo $\mathfrak{p}$, and $v_\mathfrak{p}(ap), v_\mathfrak{p}(bp)$ are odd. Since the supports of a and b are disjoint (Lemma 3.4), it follows that $v_\mathfrak{p}(p)$ is odd.

Again, by Lemmas 4.1–4.3, we conclude that

$$\ddagger \wedge \mathfrak{e}' \implies (a_1,a_2)_\mathfrak{p} = -(-a_3,-a_4)_\mathfrak{p} \text{ and } a_1a_2a_3a_4 \in K_\mathfrak{p}^{\times 2},$$

since $R_{p,q}^{(1,1)} \subset \mathcal{O}_\mathfrak{p}$ and $J(R_{p,q}^{(1,1)}) \subset \mathfrak{p}\mathcal{O}_\mathfrak{p}$. ∎

Proof of Theorem 1.3. We proceed by considering each possible number of variables m separately.

- $m = 1$. For all $a_1 \neq 0$, we have $f = a_1x_1^2$ is anisotropic, and the set $K^\times$ is obviously diophantine.
- $m = 2$. For all $a_1, a_2 \neq 0$, $f = a_1x_1^2 + a_2x_2^2$ is isotropic if and only if $-a_1a_2 \in K^{\times 2}$, and the set

  $$\{(a_1,a_2) \in K^\times \times K^\times \mid -a_1a_2 \notin K^{\times 2}\}$$

  is diophantine over K by [EM18, Theorem 1.4].
- $m = 3$. In this case $f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$. Then $-a_1a_2 \in K^{\times 2}$ means exactly $f = 0$ has a nontrivial solution for $x_3 = 0$. The condition $f = 0$ has a nontrivial solution for $x_3 \neq 0$ is equivalent to the solubility of the equation $-a_3 = a_1x_1^2 + a_2x_2^2$, which means exactly

  $$-a_3 = a_1\left(x_1^2 + a_1a_2\left(\frac{x_2}{a_1}\right)^2\right) \in a_1\mathrm{N}_{K(\sqrt{-a_1a_2})/K}(K(\sqrt{-a_1a_2})^\times).$$

  Hence for all $a_1, a_2, a_3 \neq 0$, $f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ is isotropic if and only if $-a_1a_2 \in K^{\times 2}$ or $-a_3 \in a_1 \cdot \mathrm{N}_{K(\sqrt{-a_1a_2})/K}(K(\sqrt{-a_1a_2})^\times)$. The sets

  $$\{(a_1,a_2,a_3) \in K^\times \times K^\times \times K^\times \mid -a_1a_2 \notin K^{\times 2})\}$$

  and

  $$\{(a_1,a_2,a_3) \in K^\times \times K^\times \times K^\times \mid -a_3 \notin a_1 \cdot \mathrm{N}_{K(\sqrt{-a_1a_2})/K}(K(\sqrt{-a_1a_2})^\times)\}$$

  are all diophantine by [EM18, Theorem 1.4] and [EM18, Theorem 1.3]. Their intersection is therefore diophantine.
- $m = 4$. This follows from Lemma 4.6 and Theorem 2.3(1).
- $m \geq 5$. By Theorem 2.3(1)(2), in this situation f is anisotropic over K if and only if f is anisotropic over some real infinite primes since f is

always isotropic over complex primes and finite primes [O'M00, 63:19]. For a single real infinite prime ω, f is anisotropic over ω if and only if

$$\Big(\bigwedge_{i=1}^{m} \omega(a_i) > 0\Big) \vee \Big(\bigwedge_{i=1}^{m} \omega(-a_i) > 0\Big),$$

which gives a diophantine set by [EM18, Lemma 4.1]. Since there are only finitely many real primes, the set

$$\Big\{(a_1, \ldots, a_m) \in (K^\times)^m \;\Big|\; \sum_{i=1}^{m} a_i x_i^2 \text{ is anisotropic over } K\Big\}$$

is diophantine. ∎

Acknowledgements. I am grateful to my PhD advisor Yongqi Liang for leading me to the question studied in this paper and for many helpful suggestions. I would like to express my sincere thanks to Arno Fehm, my host supervisor during the Sino-German (CSC-DAAD) Postdoc Scholarship Program, who spent a great deal of time carefully reading the manuscript and provided extensive and insightful advice on both the mathematics and the exposition. I would also like to thank Yang Cao and Yongqi Liang for their valuable help and support throughout the application process for the Sino-German (CSC-DAAD) Postdoc Scholarship Program.

Funding. This work was carried out during a research visit to TU Dresden supported by the Sino-German (CSC-DAAD) Postdoc Scholarship Program and was also supported by the Shandong Provincial Natural Science Foundation (Project No. ZR2024QA184).

References

[CTG15] J.-L. Colliot-Thélène et J. Van Geel, *Le complémentaire des puissances n-ièmes dans un corps de nombres est un ensemble diophantien*, Compos. Math. 151 (2015), 1965–1980.

[Dit18] P. Dittmann, *Irreducibility of polynomials over global fields is diophantine*, Compos. Math. 154 (2018), 761–772.

[EM18] K. Eisenträger and T. Morrison, *Universally and existentially definable subsets of global fields*, Math. Res. Lett. 25 (2018), 1173–1204.

[EP05] A. J. Engler and A. Prestel, *Valued Fields*, Springer Monogr. Math., Springer, Berlin, 2005.

[Koe16] J. Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Ann. of Math. 183 (2016), 73–93.

[Lan86] S. Lang, *The Artin symbol, reciprocity law, and class field theory*, Springer, New York, 1986, 197–212.

[Mat70] Y. Matiyasevich, *The diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR 191 (1970), 279–282 (in Russian).

[Mor19] T. Morrison, *Diophantine definability of nonnorms of cyclic extensions of global fields*, Trans. Amer. Math. Soc. 372 (2019), 5825–5850.

[O'M00] O. T. O'Meara, *Introduction to Quadratic Forms*, Classics Math., Springer, Berlin, 2000 (reprint of the 1973 ed.).

[Par13] J. Park, *A universal first-order formula defining the ring of integers in a number field*, Math. Res. Lett. 20 (2013), 961–980.

[Poo09] B. Poonen, *The set of nonsquares in a number field is diophantine*, Math. Res. Lett. 16 (2009), 165–170.

[Rum80] R. Rumely, *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. 262 (1980), 195–217.

[Ser73] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, New York, 1973.

Guang Hu
School of Mathematics
Shandong University
250100 Jinan, China
and
Institute of Algebra
Technische Universität Dresden
01062 Dresden, Germany
E-mail: huguang@mail.ustc.edu.cn