Math. Res. Lett.
Volume 25, Number 4, 1173–1204, 2018

Universally and existentially definable subsets of global fields

Kirsten Eisenträger and Travis Morrison

We show that rings of S-integers of a global function field K of odd characteristic are first-order universally definable in K. This extends work of Koenigsmann and Park who showed the same for $\mathbb{Z}$ in $\mathbb{Q}$ and the ring of integers in a number field, respectively. We also give another proof of a theorem of Poonen and show that the set of non-squares in a global field of characteristic $\neq 2$ is diophantine. Finally, we show that the set of pairs $(x, y) \in K^\times \times K^\times$ such that x is not a norm in $K(\sqrt{y})$ is diophantine over K for any global field K of characteristic $\neq 2$.

1. Introduction

Hilbert's Tenth Problem asks whether there exists an algorithm that decides, given an arbitrary polynomial equation with integer coefficients, whether it has a solution in the integers. Matiyasevich answered this in the negative in [9] using work by Davis, Putnam, and J. Robinson [3]. We say that Hilbert's

Tenth Problem is undecidable. The same question can be asked for polynomial equations with coefficients and solutions in other commutative rings R. We refer to this as Hilbert's Tenth Problem over R. Hilbert's Tenth Problem over $\mathbb{Q}$, and over number fields in general, is still open. The function field analogue is much better understood, and Hilbert's Tenth Problem is known to be undecidable for global function fields ([13], [26], [23], [7]).

One approach to proving that Hilbert's Tenth Problem for $\mathbb{Q}$ is undecidable is to show that $\mathbb{Z}$ is *diophantine* over $\mathbb{Q}$:

Definition 1.1. Let R be a ring. We say that $A \subseteq R^m$ is diophantine over R if there exists a polynomial

$$g(x_1, \ldots, x_m, y_1, \ldots, y_n) \in R[x_1, \ldots, x_m, y_1, \ldots, y_n]$$

such that

$$(a_1, \ldots, a_m) \in A \iff \exists r_1, \ldots, r_n \in R \text{ s.t. } g(a_1, \ldots, a_m, r_1, \ldots, r_n) = 0.$$

If one had a diophantine, i.e. a positive existential definition of $\mathbb{Z}$ in $\mathbb{Q}$, then a reduction argument, together with Matiyasevich's theorem for Hilbert's Tenth Problem over $\mathbb{Z}$, would imply that Hilbert's Tenth Problem for $\mathbb{Q}$ is undecidable. But it is still open whether $\mathbb{Z}$ is positive existentially definable in $\mathbb{Q}$. In fact, if Mazur's conjecture holds, then $\mathbb{Z}$ is not existentially definable in $\mathbb{Q}$ [10].

It is, however, possible to define the integers inside the rationals with a first-order formula. This is due to J. Robinson [16] who gave a $\forall\exists\forall\exists$ definition of $\mathbb{Z}$ in $\mathbb{Q}$. Her result was improved by Poonen [14] who gave a $\forall\exists$ definition of $\mathbb{Z}$ in $\mathbb{Q}$. Koenigsmann [8] further improved on Poonen's result and gave a definition of the integers inside $\mathbb{Q}$ that uses only universal quantifiers.

Park generalized this and showed that for any number field K, the ring of integers $\mathcal{O}_K$ is universally definable in K [12].

Similar definability questions can be asked for subrings of global function fields. Let q be a power of a prime. While Hilbert's Tenth Problem for both $\mathbb{F}_q[t]$ and $\mathbb{F}_q(t)$ is undecidable ([4], [13], [26]), it is not known whether $\mathbb{F}_q[t]$ is diophantine over $\mathbb{F}_q(t)$. Showing this still seems out of reach, but it is possible to give a universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ which we do in this paper for odd q. More generally, we prove the natural generalization of Park's result for defining rings of integers to global function fields K.

This is the first of three main theorems in this paper, and we prove it in Section 3:

Theorem 1.2. *Let K be a global function field of odd characteristic and let S be a finite, nonempty set of primes of K. Then $\mathcal{O}_S$ is first-order universally definable in K. Equivalently, $K \setminus \mathcal{O}_S$ is diophantine over K.*

Here, for a finite set S of primes of K we denote by $\mathcal{O}_S$ the ring

$$\mathcal{O}_S := \{x \in K : v_{\mathfrak{p}}(x) \geq 0 \quad \forall \text{ primes } \mathfrak{p} \notin S\}.$$

Our theorem generalizes a result by Rumely [19] who gave a first-order definition of a polynomial ring inside a global function field K. It also improves one of the results in [24], where it was shown how to define the S-integers in a global function field using a first-order formula that involves one change in quantifiers.

One of the main ideas in proving Theorem 1.2 is to use certain diophantine rings, parametrized by $K^\times$, to encode integrality at finite sets of primes; this is based on ideas of Poonen in [14] and Koenigsmann in [8]. Park replaces the congruence classes that Koenigsmann used for $\mathbb{Z}$ in $\mathbb{Q}$ with ray classes of a fixed modulus of K for a fixed biquadratic extension of K.

Some parts of Park's arguments do not extend to the function field setting and require a different approach; in [12], a biquadratic extension of K is chosen so that it is linearly disjoint from the Hilbert class field of K. Since the Hilbert class field of a global function field is an infinite extension, we cannot use it in our arguments, but there is another natural finite extension of the global function field K that we can use instead. We use a finite extension of K whose Galois group is the ideal class group of the Dedekind domain $\mathcal{O}_{S'}$ for some carefully chosen set of primes S'. Another crucial ingredient in the proof of Theorem 1.2 is showing that any class in the ray class group of a Dedekind domain A contained in K contains infinitely many primes of A.

We also show that other arithmetic subsets of a global field K are diophantine over K, extending the results in [8]. Given $y \in K^\times \setminus K^{\times 2}$, consider the norm map

$$\begin{aligned} N_y : K(\sqrt{y}) &\to K \\ a + b\sqrt{y} &\mapsto a^2 - yb^2. \end{aligned}$$

In Section 4.2 we show the following new result:

Theorem 1.3. *Let K be a global field with* $\mathrm{char}(K) \neq 2$. *Then*

$$\{(x, y) \in K^\times \times K^\times | x \notin N_y(K(\sqrt{y}))\}$$

is diophantine over K.

This generalizes a result of [8] from $K = \mathbb{Q}$ to global fields.
We also give a new proof of the following theorem:

Theorem 1.4. *Let K be a global field with* $\mathrm{char}(K) \neq 2$. *Then $K^\times \setminus K^{\times 2}$ is diophantine over K.*

This was established by Poonen in [15], using results on the Brauer-Manin obstruction. For number fields, this was extended to non-nth powers in [2] and further in [6]. In [8], Koenigsmann gave a more elementary proof for $K = \mathbb{Q}$. Using results in [12] and their extensions in this paper, together with Artin Reciprocity and the Chebotarev Density Theorem, we give a different proof of Poonen's result.

2. S-integers and class field theory of global function fields

Let K be a global function field. In this section we recall some facts about rings of S-integers and their class groups.

2.1. Background and definitions

Let K be a global function field, and let S_K denote the set of all primes of K. By a prime of K we mean an equivalence class of nontrivial absolute values of K. In a global function field, all such absolute values are non-archimedean and we can represent a prime as a pair $(\mathfrak{p}, \mathcal{O}_\mathfrak{p})$ where $\mathcal{O}_\mathfrak{p}$ is a local ring of K and $\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{p}$ is its maximal ideal. We will often refer only to the ideal $\mathfrak{p}$ as a prime of K. We denote by $v_\mathfrak{p}$ the associated normalized discrete valuation on K. We now recall some facts about the ring of S-integers $\mathcal{O}_S$ in K where $S \subset S_K$ is a finite set of primes of K. The ring $\mathcal{O}_S$ is a Dedekind domain and its prime ideals are in one-to-one correspondence with the primes of K not in S; this correspondence is given by

$$\mathfrak{p} \mapsto \mathfrak{p} \cap \mathcal{O}_S.$$

See [18, Theorem 14.5]. So given $q \in \mathcal{O}_S$, we can factor $q\mathcal{O}_S$ uniquely into a product of prime ideals of $\mathcal{O}_S$. The support of the divisor of q contains the primes in this factorization and some primes of S.

A modulus $\mathfrak{m}$ of K is a formal product of primes of K, $\mathfrak{m} = \prod \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$, such that $\mathfrak{m}(\mathfrak{p}) \geq 0$ for all $\mathfrak{p}$ and $\mathfrak{m}(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p}$. The group of fractional ideals I of K is the free abelian group generated by the primes of K. We define $I_{\mathfrak{m}}$ to be the subgroup generated by the primes which do not appear in $\mathfrak{m}$. Given $\alpha \in K^{\times}$, it defines a fractional ideal

$$(\alpha) := \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}.$$

Define

$$K_{\mathfrak{m},1} = \{x \in K^{\times} : v_{\mathfrak{p}}(x-1) \geq \mathfrak{m}(\mathfrak{p}) \text{ for all } \mathfrak{p} \text{ dividing } \mathfrak{m}\}.$$

We have a well-defined map $i : K_{\mathfrak{m},1} \to I_{\mathfrak{m}}$, sending α to the fractional ideal (α). Define $P_{\mathfrak{m}}$ to be the subgroup $i(K_{\mathfrak{m},1})$ of $I_{\mathfrak{m}}$. The ray class group modulo $\mathfrak{m}$, $C_{\mathfrak{m}}$, is defined to be the quotient $I_{\mathfrak{m}}/P_{\mathfrak{m}}$. This group is not finite, but the degree map (which we can define by viewing these formal products as divisors) induces an exact sequence

$$0 \to C^0_{\mathfrak{m}} \to C_{\mathfrak{m}} \to \mathbb{Z} \to 0.$$

The subgroup $C^0_{\mathfrak{m}}$ of degree-zero divisor classes can be shown to be finite.

Let L be a finite abelian extension of K. Suppose $\mathfrak{p} \in S_K$ is unramified in L. Then we define $(\mathfrak{p}, L/K) \in \mathrm{Gal}(L/K)$ to be its associated Frobenius automorphism. If $\mathfrak{m}$ is a modulus of K divisible by those primes which ramify in L, we have the global Artin map

$$\begin{aligned} \psi_{L/K} : I_{\mathfrak{m}} &\to \mathrm{Gal}(L/K) \\ \prod \mathfrak{p}_i^{e_i} &\mapsto \prod (\mathfrak{p}_i, L/K)^{e_i}. \end{aligned}$$

Theorem 2.1. *(Artin Reciprocity) The Artin map is surjective and there exists a modulus $\mathfrak{m}$ containing all the primes of K which ramify in L such that the kernel is $P_{\mathfrak{m}} N_{L/K}(I_L(\mathfrak{m}'))$; here $N_{L/K}$ is the norm map on fractional ideals and $\mathfrak{m}'$ is the modulus of L consisting of primes of L lying above those of K contained in $\mathfrak{m}$.*

Remark 2.2. We call any $\mathfrak{m}$ as in Theorem 2.1 an *admissible* modulus for the extension L over K.

We will need the existence theorem of class field theory for function fields, so we introduce the idele group. We define the idele group of K to be

the restricted product of $K_{\mathfrak{p}}^{\times}$ for $\mathfrak{p} \in S_K$ with respect to the compact groups $R_{\mathfrak{p}}^{\times}$, where $R_{\mathfrak{p}}$ is the ring of integers in the completion $K_{\mathfrak{p}}$ of K at $\mathfrak{p}$. We denote the idele group of K by $\mathbb{I}$. Denote the diagonal embedding of $K^{\times}$ in $\mathbb{I}$ again by $K^{\times}$ and the idele class group by $C_K := \mathbb{I}/K^{\times}$, which we endow with the quotient topology.

An idele of K determines a fractional ideal of K via the surjective map

$$\begin{aligned} \mathrm{id} : \mathbb{I} &\to I \\ (x_{\mathfrak{p}}) &\mapsto \prod_{\mathfrak{p} \in S_K} \mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})}. \end{aligned}$$

Again let L/K be a finite abelian extension and let S_{ram} be the set of primes of K ramifying in L. Define

$$\mathbb{I}_{S_{ram}} := \{(x_{\mathfrak{p}}) \in \mathbb{I} : x_{\mathfrak{p}} = 1 \text{ for all } \mathfrak{p} \in S_{ram}\}.$$

There is a unique function $\phi_{L/K} : \mathbb{I} \to \mathrm{Gal}(L/K)$ which is continuous, trivial on $K^{\times}$, and satisfies $\phi_{L/K}((x_{\mathfrak{p}})) = \psi_{L/K}(\mathrm{id}((x_{\mathfrak{p}})))$ for all $(x_{\mathfrak{p}}) \in \mathbb{I}_{S_{ram}}$; see [25]. Hence $\phi_{L/K}$ induces a map on the idele class group C_K, which we again denote by $\phi_{L/K}$. This is the idelic Artin map. The idelic Artin reciprocity law states that the kernel of $\phi_{L/K}$ is $N(C_L)$ where N is the norm map on ideles.

Now we state the existence theorem of class field theory; see Theorem 1 of Chapter 8 in [1].

Theorem 2.3 (Existence Theorem). *Let K be any global field. Fix an algebraic closure $\overline{K}$ of K. Given a finite index open subgroup $H \subset C_K$, there is a unique finite abelian extension L of K in $\overline{K}$ such that $H = N(C_L)$.*

2.2. Ray class groups of rings of S-integers

Let $S_\infty := \{\infty_1, \ldots, \infty_n\} \subseteq S_K$, and $A := \mathcal{O}_{S_\infty}$. The ideal class group $\mathrm{Cl}(A)$ of the Dedekind domain A is finite. Denote by K^A the maximal abelian unramified extension of K in which each prime of S_∞ splits completely. Then $\mathrm{Cl}(A) \cong \mathrm{Gal}(K^A/K)$ via the Artin map (see [17]), and we will use K^A and $\mathrm{Cl}(A)$ in Section 3.2. Set $\infty := \infty_1 \cdots \infty_n$. For the rest of this section, let $\mathfrak{m}$ be another modulus of K coprime to ∞; we can then view $\mathfrak{m}$ as an ideal of A. Below we define $\mathrm{Cl}_{\mathfrak{m}}(A)$, the ray class group of A for the modulus $\mathfrak{m}$. One crucial ingredient to the universal definition of S-integers is Lemma 3.15, where we need that a given class of $\mathrm{Cl}_{\mathfrak{m}}(A)$ contains infinitely

many primes of A. This is Theorem 2.9 at the end of this section, whose proof uses idelic class field theory. The remainder of this section is devoted to proving Theorem 2.9. One can think of this as a function field analogue of Dirichlet's theorem.

Definition 2.4. Let $I_{\mathfrak{m}}(A)$ be the group of fractional ideals of A which are coprime to $\mathfrak{m}$. We have a natural injection $j : K_{\mathfrak{m},1} \to I_{\mathfrak{m}}(A)$ whose image we denote by $P_{\mathfrak{m}}(A)$. This image consists of principal fractional ideals αA with $v_{\mathfrak{p}}(\alpha - 1) \geq \mathfrak{m}(\mathfrak{p})$. Define

$$\mathrm{Cl}_{\mathfrak{m}}(A) := I_{\mathfrak{m}}(A)/P_{\mathfrak{m}}(A).$$

We need the following lemma:

Lemma 2.5 (Kernel-Cokernel sequence). *Given a pair of maps between abelian groups*

$$A \xrightarrow{f} B \xrightarrow{g} C$$

there is an exact sequence

$$0 \to \ker f \to \ker g \circ f \to \ker g \to \mathrm{coker}\, f \to \mathrm{coker}\, g \circ f \to \mathrm{coker}\, g \to 0.$$

Proof. This is Proposition 0.24 in [11]. □

Define

$$\begin{aligned} U_{\mathfrak{m},\mathfrak{p}} &:= \{x \in K_{\mathfrak{p}}^{\times} : v_{\mathfrak{p}}(x-1) \geq \mathfrak{m}(\mathfrak{p})\}, \\ \mathbb{I}_{\mathfrak{m}} &:= \prod_{\mathfrak{p} \nmid \mathfrak{m}} K_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p} \mid \mathfrak{m}} U_{\mathfrak{m},\mathfrak{p}} \cap \mathbb{I}, \\ W_{\mathfrak{m}} &:= \prod_{\mathfrak{p} \mid \infty} K_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p} \nmid \mathfrak{m} \cdot \infty} \mathcal{O}_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p} \mid \mathfrak{m}} U_{\mathfrak{m},\mathfrak{p}}. \end{aligned}$$

Proposition 2.6. *Let $\mathfrak{m}$ be a modulus of K coprime to ∞.*

1) *The ideal map $id : \mathbb{I}_{\mathfrak{m}} \to I_{\mathfrak{m}}(A)$ induces an isomorphism $\mathbb{I}_{\mathfrak{m}}/(K_{\mathfrak{m},1} W_{\mathfrak{m}}) \cong \mathrm{Cl}_{\mathfrak{m}}(A)$.*
2) *The inclusion map $\mathbb{I}_{\mathfrak{m}} \to \mathbb{I}$ induces an isomorphism $\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \cong C_K$.*

Proof. (1) We have maps

$$K_{\mathfrak{m},1} \to \mathbb{I}_{\mathfrak{m}} \to I_{\mathfrak{m}}(A),$$

where the first map is the diagonal embedding and the second is the ideal map. Applying the kernel-cokernel sequence gives us the exact sequence

$$W_{\mathfrak{m}} \to \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to \mathrm{Cl}_{\mathfrak{m}}(A) \to 0.$$

This follows because by definition, $\mathrm{Cl}_{\mathfrak{m}}(A) = I_{\mathfrak{m}}(A)/P_{\mathfrak{m}}(A)$, $P_{\mathfrak{m}}(A) = j(K_{\mathfrak{m},1})$, and the kernel of the ideal map restricted to $\mathbb{I}_{\mathfrak{m}}$ is $W_{\mathfrak{m}}$. Thus $\mathrm{Cl}_{\mathfrak{m}}(A)$ is isomorphic to $\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}$ modulo the image of $W_{\mathfrak{m}}$. Since the first map in the above sequence is reduction modulo the image of $K_{\mathfrak{m},1}$ in $W_{\mathfrak{m}}$, we get that

$$\mathrm{Cl}_{\mathfrak{m}}(A) \cong (\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1})/(W_{\mathfrak{m}}K_{\mathfrak{m},1}/K_{\mathfrak{m},1}) \cong \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}W_{\mathfrak{m}}.$$

(2) The injection $\mathbb{I}_{\mathfrak{m}} \to \mathbb{I}$ gives us an injection $\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_K$. Denote the maximal ideal of $R_{\mathfrak{p}}$ by $\hat{\mathfrak{p}}$. Let $(x_{\mathfrak{p}}) \in \mathbb{I}$ and choose, using weak approximation, $b \in K^{\times}$ such that $v_{\mathfrak{p}}(x_{\mathfrak{p}} - b) > \mathfrak{m}(\mathfrak{p}) + v_{\mathfrak{p}}(x_{\mathfrak{p}})$ for each $\mathfrak{p}|\mathfrak{m}$. Because $v_{\mathfrak{p}}(x_{\mathfrak{p}} - b) > v_{\mathfrak{p}}(x_{\mathfrak{p}})$, we must have that $v_{\mathfrak{p}}(x_{\mathfrak{p}}) = v_{\mathfrak{p}}(b)$. Then

$$v_{\mathfrak{p}}(x_{\mathfrak{p}}/b - 1) = v_{\mathfrak{p}}(x_{\mathfrak{p}} - b) - v_{\mathfrak{p}}(b) > \mathfrak{m}(\mathfrak{p}),$$

implying that $x_{\mathfrak{p}}/b \in U_{\mathfrak{m},\mathfrak{p}}$ for each $\mathfrak{p}|\mathfrak{m}$. Then $(x_{\mathfrak{p}}/b) \in \mathbb{I}_{\mathfrak{m}}$ maps to the image of $(x_{\mathfrak{p}})$ in C_K and we see that the map is surjective. □

Proposition 2.7. *The group* $\mathrm{Cl}_{\mathfrak{m}}(A)$ *is finite.*

Proof. In any ideal class of A, we can find an ideal in it coprime to $\mathfrak{m}$, so we have a surjection $\mathrm{Cl}_{\mathfrak{m}}(A) \to \mathrm{Cl}(A)$. The kernel of this map is the subgroup of $\mathrm{Cl}_{\mathfrak{m}}(A)$ consisting of the principal ideal classes of the form $\overline{xA}$ where $v_{\mathfrak{p}}(x) = 0$ for $\mathfrak{p}|\mathfrak{m}$. These classes can be viewed as elements in $C^0_{\mathfrak{m}}$. Since $C^0_{\mathfrak{m}}$ is finite, we see that $\mathrm{Cl}_{\mathfrak{m}}(A)$ is an extension of finite groups and is itself finite. □

Corollary 2.8. *There is a finite abelian extension* $K^A_{\mathfrak{m}}$ *of* K *whose Galois group is isomorphic to* $\mathrm{Cl}_{\mathfrak{m}}(A)$ *via the Artin map.*

Proof. The injection $\mathbb{I}_{\mathfrak{m}} \to \mathbb{I}$, when restricted to $K_{\mathfrak{m},1}W_{\mathfrak{m}}$, induces an isomorphism

$$(K_{\mathfrak{m},1}W_{\mathfrak{m}})/K_{\mathfrak{m},1} \simeq (K^{\times}W_{\mathfrak{m}})/K^{\times}.$$

Indeed, given $c \in K^{\times}$ and $(x_{\mathfrak{p}}) \in W_{\mathfrak{m}}$ we can use weak approximation to find $c' \in K^{\times}$ such that $c/c' \in K_{\mathfrak{m},1}$ as in the proof of part (2) of Theorem 2.6. Then $\frac{c}{c'}(x_{\mathfrak{p}}) \in K_{\mathfrak{m},1}W_{\mathfrak{m}}$ maps to the image of $c \cdot (x_{\mathfrak{p}})$ in $(K^{\times}W_{\mathfrak{m}})/K^{\times}$. Thus $\mathrm{Cl}_{\mathfrak{m}}(A)$ is a quotient of C_K by an open subgroup subgroup, whose index is finite by Proposition 2.7. The Existence Theorem then guarantees such an extension $K_{\mathfrak{m}}^A/K$ as desired. □

Together with an application of the Chebotarev Density Theorem, the above discussion gives us the following theorem:

Theorem 2.9. *Let A and $\mathfrak{m}$ be as above. Any ideal class in $\mathrm{Cl}_{\mathfrak{m}}(A)$ contains infinitely many prime ideals of A.*

3. *S*-integers are universally definable in global function fields

In Sections 3.1 and 3.2 we will review facts and results from [12]. The rest of Park's argument does not extend to the function field setting, so we use results of Section 2 on idelic class field theory to finish the proof in Section 3.3 and Section 3.4.

3.1. Notation and facts about quaternion algebras

Throughout this section, let K be a global function field of odd characteristic. Let $a, b \in K^{\times}$. We recall the following notation from [12]:

1) Given a prime $\mathfrak{p} \in S_K$, let $v := v_{\mathfrak{p}}$ be its associated valuation, normalized so that it takes values in $\mathbb{Z} \cup \{\infty\}$. Define $K_{\mathfrak{p}}$ to be the completion of K at $\mathfrak{p}$, $R_{\mathfrak{p}}$ the ring of integers in $K_{\mathfrak{p}}$, the maximal ideal of $R_{\mathfrak{p}}$ by $\hat{\mathfrak{p}}$, and $\mathbb{F}_{\mathfrak{p}}$ the residue field of $\mathfrak{p}$. Set $U_{\mathfrak{p}} := \{s \in \mathbb{F}_{\mathfrak{p}} : x^2 - sx + 1$ is irreducible over $\mathbb{F}_{\mathfrak{p}}\}$ and let $\mathrm{red}_{\mathfrak{p}} : R_{\mathfrak{p}} \to \mathbb{F}_{\mathfrak{p}}$ be the reduction map. Let $\mathcal{O}_{\mathfrak{p}} := R_{\mathfrak{p}} \cap K$; this is the local ring of the prime $\mathfrak{p}$ in K.

2) $H_{a,b} = K \oplus \alpha K \oplus \beta K \oplus \alpha\beta K$, the quaternion algebra over K with multiplication given by $\alpha^2 = a, \beta^2 = b, \alpha\beta = -\beta\alpha$.

3) Given $x := x_1 + x_2\alpha + x_3\beta + x_4\alpha\beta$, define $\overline{x} := x_1 - x_2\alpha - x_3\beta - x_4\alpha\beta$. This is the standard involution on $H_{a,b}$. Define the (reduced) trace

of x to be $x + \overline{x} = 2x_1$ and the (reduced) norm of x to be $x \cdot \overline{x} = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2$.

4) $\Delta_{a,b} = \{\mathfrak{p} \in S_K : H_{a,b} \otimes_K K_\mathfrak{p} \ncong M_2(K_\mathfrak{p})\}$, that is, the set of primes where $H_{a,b}$ ramifies.

5) $(a,b)_\mathfrak{p} = \begin{cases} 1 & : \mathfrak{p} \notin \Delta_{a,b} \\ -1 & : \mathfrak{p} \in \Delta_{a,b} \end{cases}$, the Hilbert symbol of $K_\mathfrak{p}$.

6) $S_{a,b} = \{2x_1 \in K : \exists x_2, x_3, x_4 \text{ such that } x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1\}$. This is the set of traces of norm one elements of $H_{a,b}$.

7) $T_{a,b} = S_{a,b} + S_{a,b}$.

Given a prime $\mathfrak{p} \in S_K$, we similarly define $S_{a,b}(K_\mathfrak{p})$ and $T_{a,b}(K_\mathfrak{p})$ just by replacing K with $K_\mathfrak{p}$ in the above definitions.

Lemma 3.1.

1) If $\mathfrak{p} \notin \Delta_{a,b}$, then $S_{a,b}(K_\mathfrak{p}) = K_\mathfrak{p}$.

2) If $\mathfrak{p} \in \Delta_{a,b}$ then $\mathrm{red}_\mathfrak{p}^{-1}(U_\mathfrak{p}) \subseteq S_{a,b}(K_\mathfrak{p}) \subseteq \mathcal{O}_\mathfrak{p}$.

3) For any $\mathfrak{p}$ with $|\mathbb{F}_\mathfrak{p}| > 11$, we have $\mathbb{F}_\mathfrak{p} = U_\mathfrak{p} + U_\mathfrak{p}$.

4) For each $a, b \in K^\times$,

$$S_{a,b} = K \cap \bigcap_{\mathfrak{p} \in \Delta_{a,b}} S_{a,b}(K_\mathfrak{p}).$$

Proof. See [12], Lemma 2.2; the arguments work when K is any global field. □

Proposition 3.2. *For any $a, b \in K^\times$, we have*

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

Proof. See [12, Proposition 2.3]. □

In our setting, we also have the following formula for the Hilbert symbol from [21, XIV.3.8]:,

$$(a,b)_\mathfrak{p} = \left[(-1)^{v_\mathfrak{p}(a)v_\mathfrak{p}(b)} \left(\frac{a^{v_\mathfrak{p}(b)}}{b^{v_\mathfrak{p}(a)}}\right)\right]^{(|\mathbb{F}_\mathfrak{p}|-1)/2}. \tag{1}$$

Hence for a $\mathfrak{p}$-adic unit a, $(a,p)_{\mathfrak{p}} = -1$ if and only if $v_{\mathfrak{p}}(p)$ is odd and $\mathrm{red}_{\mathfrak{p}}(a)$ is not a square in $\mathbb{F}_{\mathfrak{p}}$.

3.2. Partitioning the primes of K

Suppose a is not a square in K. Then if $\mathfrak{p}$ is unramified in $K(\sqrt{a})$, after possibly multiplying by a square of $K^\times$, a is a $\mathfrak{p}$-adic unit. We can then identify $\psi_{K(\sqrt{a})/K}(\mathfrak{p})$ with the power residue symbol $\left(\frac{a}{\mathfrak{p}}\right)_2$ (see Proposition 10.5 and 10.6 in [18]). If the images of a, b are distinct in $K^\times/K^{\times 2}$, we can use the splitting of $\mathfrak{p}$ in $\mathrm{Gal}(K(\sqrt{a},\sqrt{b})/K)$ to study the Hilbert symbols $(a,p)_{\mathfrak{p}}$ and $(b,p)_{\mathfrak{p}}$, since if $v_{\mathfrak{p}}(p)$ is odd, $(a,p)_{\mathfrak{p}} = \left(\frac{a}{\mathfrak{p}}\right)_2$. We have the following lemma:

Lemma 3.3. *Take $a, b \in K^\times$ whose images in $K^\times/K^{\times 2}$ are distinct and let $\mathfrak{m}$ be an admissible modulus for the extension $L := K(\sqrt{a},\sqrt{b})/K$ and let*

$$\psi_{L/K} : I_{\mathfrak{m}} \to \{\pm 1\} \times \{\pm 1\}$$

be the Artin map. Suppose that $\mathfrak{m}$ is divisible also by all primes dividing (ab). For a prime $\mathfrak{p} \in S_K$ such that $\mathfrak{p} \nmid \mathfrak{m}$, $\mathfrak{p} \in \Delta_{a,p} \cap \Delta_{b,p}$ if and only if $v_{\mathfrak{p}}(p)$ is odd and $\psi_{L/K}(\mathfrak{p}) = (-1,-1)$.

Proof. See [12], Lemma 3.8. The only change in the argument is that we do not to worry about total positivity conditions defining $K_{\mathfrak{m},1}$ since there are no archimedean primes of a global function field. □

As in [12], we partition primes of K coprime to $\mathfrak{m}$ based on their image under $\psi_{L/K}$. Choose $a, b \in K^\times$ and L as in Lemma 3.3 and set

$$\mathbb{P}(p) := \{\mathfrak{p} \in S_K : v_{\mathfrak{p}}(p) \text{ is odd.}\}.$$

Also, for $(i,j) \in \mathrm{Gal}(L/K)$, $i, j \in \{\pm 1\}$, set

$$\mathbb{P}^{(i,j)} = \{\mathfrak{p} \in S_K : \mathfrak{p} \in I_{\mathfrak{m}} \text{ and } \psi_{L/K}(\mathfrak{p}) = (i,j)\}$$

and set

$$\mathbb{P}^{(i,j)}(p) = \mathbb{P}(p) \cap \mathbb{P}^{(i,j)}.$$

Lemma 3.4. *Suppose $p \in K^\times$ and let $\mathfrak{m}$ be a modulus as in Lemma 3.3. Additionally, suppose (p) and $\mathfrak{m}$ are coprime. Then we have the following*

identification of sets of primes, where the two sets differ at most by primes dividing the modulus.

$$\begin{aligned}\mathbb{P}^{(-1,-1)}(p) &\leftrightarrow \Delta_{a,p} \cap \Delta_{b,p},\\ \mathbb{P}^{(-1,1)}(p) &\leftrightarrow \Delta_{a,p} \cap \Delta_{ab,p},\\ \mathbb{P}^{(1,-1)}(p) &\leftrightarrow \Delta_{b,p} \cap \Delta_{ab,p}.\end{aligned}$$

Proof. See [12, Lemma 3.9]. □

Lemma 3.5. *Let $\mathfrak{p} \in S_K$ with $\mathfrak{p} \nmid \mathfrak{m}$ and suppose that $\psi_{L/K}(\mathfrak{p}) = (i,j)$ with $(i,j) \neq (1,1)$. Then $\mathfrak{p} \in \mathbb{P}^{(i,j)}(p)$ for some $p \in K^\times$. Hence there exist $c, d \in K^\times$ such that $\mathfrak{p} \in \Delta_{c,p} \cap \Delta_{d,p}$. If $\psi_{L/K}(\mathfrak{p}) = (1,1)$ then there exist $p, q \in K^\times$ so that $\mathfrak{p} \in \Delta_{ap,q} \cap \Delta_{bp,q}$.*

Proof. See [12, Lemmas 3.11, 3.12]. □

Definition 3.6. Let $a, b \in K^\times$. Let

$$J_{a,b} := \bigcap_{\mathfrak{p} \in \Delta_{a,b} \cap (\mathbb{P}(a) \cup \mathbb{P}(b))} \mathfrak{p}\mathcal{O}_{\mathfrak{p}}.$$

Proposition 3.7. *$J_{a,b}$ is diophantine over K.*

Proof. See [12, Lemmas 3.14, 3.15, 3.17]. □

3.3. Controlling integrality with diophantine sets

The remainder of the argument used to give a universal definition of the S-integers in K requires a different approach than the one in [12]. In order to make our proof work, we need to find infinitely many $q \in K^\times$ with prescribed image under $\psi_{L/K}$ and which generate prime ideals in a certain Dedekind domain contained in K in order to control the poles of q.

Lemma 3.8. *Let S be a finite set of primes in S_K. We can choose $a, b \in K^\times$ so that the following hold:*

1) *The images of a and b in $K^\times/K^{\times 2}$ are distinct.*
2) *Any admissible modulus $\mathfrak{m}$ for $L := K(\sqrt{a}, \sqrt{b})/K$ is divisible by the primes of S.*

3) Given a finite set of primes $S' \subseteq S_K$ disjoint from S, an ideal class $\overline{I}$ in $\mathrm{Cl}(\mathcal{O}_{S'})$, and an element $\sigma \in \mathrm{Gal}(L/K)$, there exists a prime $\mathfrak{q}$ of K such that $\mathfrak{q} \cap \mathcal{O}_{S'}$ is in the ideal class $\overline{I}$, $\mathfrak{q} \in I_{\mathfrak{m}}$, and $\psi_{L/K}(\mathfrak{q}) = \sigma$.

4) As fractional ideals, (a) and (b) are coprime, meaning their supports are disjoint.

Proof. Set $A = \mathcal{O}_{S'}$. Let $\mathfrak{p}_1 \in S_K \setminus S$ and choose $a \in K^\times$ with $v_{\mathfrak{p}_1}(a) = 0$ and $v_{\mathfrak{p}}(a) = 1$ for $\mathfrak{p} \in S$; this is possible by weak approximation.

Now we choose $b \in K^\times$ with $v_{\mathfrak{p}_1}(b) = 1$ and $v_{\mathfrak{p}}(b) = 0$ for any $\mathfrak{p}$ in the support of (a). Then (a) and (b) have disjoint support. They have distinct images in $K^\times/K^{\times 2}$ as the primes at which a has odd valuation differ from the primes where b has odd valuation. Thus we have established (1) and (4). Since the primes in S ramify in $K(\sqrt{a})$, they also ramify in L and hence will be contained in any admissible modulus for L/K.

We are left with showing that (3) holds. Recall that K^A/K is the maximal abelian unramified extension of K in which every prime of S' splits completely and for which $\mathrm{Gal}(K^A/K) \simeq \mathrm{Cl}(A)$. We claim that K^A and L are linearly disjoint; this will follow if we can show that none of $\sqrt{a}$, $\sqrt{b}$, and $\sqrt{ab}$ are in K^A. Since the primes in S ramify in $K(\sqrt{a})$, $\sqrt{a} \notin K^A$. As $\mathfrak{p}_1$ ramifies in $K(\sqrt{b})$ and the primes of S along with $\mathfrak{p}_1$ all ramify in $K(\sqrt{ab})$, we have that $\sqrt{b}$, and $\sqrt{ab}$ are not in K^A, and the claim follows.

We conclude

$$\mathrm{Gal}(LK^A/K) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(K^A/K) \cong \{(\pm 1, \pm 1)\} \times \mathrm{Cl}(A).$$

We then apply the Chebotarev density theorem to find a prime $\mathfrak{q}$ such that $(\mathfrak{q}, LK^A/K) = (\sigma, \overline{I}) \in \mathrm{Gal}(L/K) \times \mathrm{Gal}(K^A/K)$. This yields part (c):

$$\begin{aligned} \sigma &= (\mathfrak{q}, LK^A/K)|_L = (\mathfrak{q}, L/K) = \psi_{L/K}(\mathfrak{q}) \quad \text{and} \\ \overline{I} &= (\mathfrak{q}, LK^A/K)|_{K^A} = (\mathfrak{q}, K^A/K). \end{aligned}$$

□

For the rest of this section, fix $a, b \in K^\times$ as in Lemma 3.8 along with an admissible modulus $\mathfrak{m}$ of K for $L := K(\sqrt{a}, \sqrt{b})$.

For the rest of this section, fix $a, b \in K^\times$ as in Lemma 3.8 and set $L := K(\sqrt{a}, \sqrt{b})$. Next, we must fix two additional elements of $K^\times$. To construct them, we need Theorem 3.7 of [12], which we restate below for convenience. This theorem lets us construct an element of $K^\times$ with prescribed Hilbert symbols against finitely many elements of $K^\times$.

Theorem 3.9. *[12, Theorem 3.7] Let K be a global field,* $\mathrm{char}(K) \neq 2$*. Let Σ denote the set of primes of K, and let Λ be a finite set of indices. Let $(a_i)_{i\in\Lambda}$ be a finite sequence of elements of K^* and suppose that $(\varepsilon_{i,\mathfrak{p}})_{i\in\Lambda,\mathfrak{p}\in\Sigma}$ is a family of elements of $\{1,-1\}$. There exists $x \in K^*$ satisfying $(a_i, x)_\mathfrak{p} = \varepsilon_{i,\mathfrak{p}}$ for all $i \in \Lambda$ and $\mathfrak{p} \in \Sigma$ if and only if the following conditions hold:*

1) *All but finitely many of the $\varepsilon_{i,\mathfrak{p}}$ are equal to 1.*
2) *For all $i \in \Lambda$, we have $\prod_{\mathfrak{p}\in\Sigma} \varepsilon_{i,\mathfrak{p}} = 1$.*
3) *For every $\mathfrak{p} \in \Sigma$, there exists $x_\mathfrak{p} \in K^*$ such that $(a_i, x_\mathfrak{p})_\mathfrak{p} = \varepsilon_{i,\mathfrak{p}}$.*

Lemma 3.10. *There exist $c, d \in K^\times$ such that $\Delta_{a,c} = \mathbb{P}(a)$ or $\Delta_{a,c} = \mathbb{P}(a) \cup \{\mathfrak{p}_a\}$ where $\mathfrak{p}_a$ is coprime to (a) and (b), and $\Delta_{b,d} = \mathbb{P}(b)$ or $\Delta_{b,d} \cup \{\mathfrak{p}_b\}$ where $\mathfrak{p}_b$ is coprime to (a), (b), and $\mathfrak{p}_a$.*

Proof. Assume $\mathbb{P}(a)$ has even cardinality. Then by Theorem 3.9, there exists c in K such that $(a, c)_\mathfrak{p} = -1$ for each $\mathfrak{p} \in \mathbb{P}(a)$, and $(a, c)_\mathfrak{q} = 1$ if $\mathfrak{q}$ is not in $\mathbb{P}(a)$. Indeed, there are an even number of primes in $\mathbb{P}(a)$, and for a local element we can take any $c_\mathfrak{p} \in K^\times$ such that $\left(\frac{c_\mathfrak{p}}{\mathfrak{p}}\right) = -1$. Then $(a, c_\mathfrak{p})_\mathfrak{p} = -1$, since $v_\mathfrak{p}(a)$ is odd. The proof in the case that $\mathbb{P}(a)$ has odd cardinality is the same by choosing $\mathfrak{p}_a$ coprime to (a) and (b) such that $\left(\frac{a}{\mathfrak{p}_a}\right) = -1$ and considering the set $\mathbb{P}(a) \cup \mathfrak{p}_a$. The local element for $\mathfrak{p}_a$ can be taken to be any element $c_{\mathfrak{p}_a} \in \mathfrak{p}_a \setminus \mathfrak{p}_a^2$. The proof for the existence of d is a similar argument. □

We now also fix $c, d \in K^\times$ as in Lemma 3.10, along with a modulus $\mathfrak{m}$ of K for L such that $\mathfrak{m}$ contains all the primes dividing $(a), (b), (c)$, and (d) and any other primes $\mathfrak{p}$ such that $(a, c)_\mathfrak{p} = -1$ or $(b, d)_\mathfrak{p} = -1$.

Corollary 3.11. *Let $p \in K^\times$ such that (p) and $\mathfrak{m}$ are coprime. We have*

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

Proof. For the first equality, see [12, Corollary 3.20]. We will prove the second equality. We have

$$\Delta_{a,p} \cap \Delta_{ab,p} = \mathbb{P}^{(-1,1)}(p) \cup \left\{\mathfrak{p} \in \mathbb{P}(a) : \left(\frac{a}{\mathfrak{p}}\right) = -1\right\},$$

by Lemma 3.4. Also, $\mathbb{P}^{(-1,1)}(p) \subseteq \Delta_{a,cp}$, since $(a,c)_{\mathfrak{p}} = 1$ for any $\mathfrak{p}$ coprime to $\mathfrak{m}$. Thus we need to compute the intersection $\Delta_{a,cp} \cap \{\mathfrak{p}|\mathfrak{m}\}$. Suppose $\mathfrak{p} \in \mathbb{P}(a)$. Then $(a,c)_{\mathfrak{p}} = -1$ by our choice of c, so $(a,cp)_{\mathfrak{p}} = -1$ if and only if $\left(\frac{p}{\mathfrak{p}}\right) = 1$. If $\mathfrak{p}|\mathfrak{m}$ but $\mathfrak{p} \notin \mathbb{P}(a)$, then $(a,p)_{\mathfrak{p}} = 1$ by Equation 1, so $(a,cp)_{\mathfrak{p}} = -1$ if and only if $(a,c)_{\mathfrak{p}} = -1$. In any case, we conclude that

$$\Delta_{a,p} \cap \Delta_{a,cp} \cap \{\mathfrak{p}|\mathfrak{m}\} = \emptyset,$$

because whenever $(a,p)_{\mathfrak{p}} = -1$ for $\mathfrak{p}|\mathfrak{m}$, we have $(a,c)_{\mathfrak{p}} = -1$ as well. Thus the second equality holds. The proof of the third equality goes the same way by calculating

$$\Delta_{b,dp} \cap \{\mathfrak{p}|\mathfrak{m}\}.$$

□

Definition 3.12. For $p, q \in K^\times$, let

$$\begin{aligned} R_p^{(-1,-1)} &= \bigcap_{\mathfrak{p} \in \Delta_{a,p} \cap \Delta_{b,p}} \mathcal{O}_{\mathfrak{p}}, \\ R_p^{(1,-1)} &= \bigcap_{\mathfrak{p} \in \Delta_{ab,p} \cap \Delta_{b,p} \cap \Delta_{a,cp}} \mathcal{O}_{\mathfrak{p}}, \\ R_p^{(-1,1)} &= \bigcap_{\mathfrak{p} \in \Delta_{a,p} \cap \Delta_{ab,p} \cap \Delta_{b,dp}} \mathcal{O}_{\mathfrak{p}}, \\ R_{p,q}^{(1,1)} &= \bigcap_{\mathfrak{p} \in \Delta_{ap,q} \cap \Delta_{bp,q}} \mathcal{O}_{\mathfrak{p}}. \end{aligned}$$

Given a finite set of primes $S \subset S_K$, in Section 3 we will express the S-integers $\mathcal{O}_S$ in terms of the rings R_p^σ for $\sigma = (-1,-1), (-1,1)$, and $(1,-1)$ and $R_{p,q}^{(1,1)}$ defined above.

Definition 3.13. For each $\sigma \in \mathrm{Gal}(L/K)$, let

$$\Phi_\sigma = \{p \in K^\times : (p) \in I_{\mathfrak{m}}, \psi_{L/K}((p)) = \sigma, \text{ and } \mathbb{P}(p) \subseteq \mathbb{P}^{(1,1)} \cup \mathbb{P}^\sigma\}.$$

Lemma 3.14.

1) *For each $\sigma \in \mathrm{Gal}(L/K)$, Φ_σ is diophantine over K.*
2) *For any $p \in \Phi_\sigma$ and $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma \neq (1,1)$, we have that $\mathbb{P}^{(\sigma)}(p)$ is nonempty. Furthermore, the Jacobson radical of R_p^σ, denoted $J(R_p^\sigma)$, is diophantine over K.*

3) Let $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma \neq (1,1)$, and let $\mathfrak{p}_0 \nmid \mathfrak{m}$ be a prime of K satisfying $\psi_{L/K}(\mathfrak{p}_0) = \sigma$. Then there is an element $p \in \Phi_\sigma$ such that $\mathfrak{p}_0 \in \mathbb{P}^\sigma(p)$. In fact, p can be chosen so that $\mathbb{P}^\sigma(p) = \{\mathfrak{p}_0\}$.

Proof. To prove (1), we first establish that $K_{\mathfrak{m},1}$ is diophantine over K: this follows from the fact that $K_{\mathfrak{m},1}$ is defined by the finitely many local conditions $v_\mathfrak{p}(a-1) \geq \mathfrak{m}(\mathfrak{p})$ for $\mathfrak{p}|\mathfrak{m}$ and that the local rings $\mathcal{O}_\mathfrak{p}$ are diophantine over K for any prime $\mathfrak{p}$ by [22, Lemma 3.22]. Because a class of principal ideals in $C_\mathfrak{m}$ lies in $C_\mathfrak{m}^0$ which is finite, we see there are only finitely many inequivalent classes of the form $(p)P_\mathfrak{m}$ for $p \in K^\times$. Thus $\{p \in K^\times : (p) \in I_\mathfrak{m}\}$ is diophantine over K as it is a finite union of translates of $K_\mathfrak{m}$. Observe that $\mathbb{P}(p) \subseteq \mathbb{P}^{(1,1)} \cup \mathbb{P}^\sigma$ is equivalent to one of the following:

- $\mathbb{P}^{(1,-1)}(p) = \mathbb{P}^{(-1,1)}(p) = \emptyset$, if $\sigma = (-1,-1)$;
- $\mathbb{P}^{(-1,-1)}(p) = \mathbb{P}^{(-1,1)}(p) = \emptyset$, if $\sigma = (1,-1)$;
- $\mathbb{P}^{(-1,-1)}(p) = \mathbb{P}^{(1,-1)}(p) = \emptyset$, if $\sigma = (-1,1)$;
- $\mathbb{P}^{(1,-1)}(p) = \mathbb{P}^{(-1,1)}(p) = \mathbb{P}^{(-1,-1)}(p) = \emptyset$, if $\sigma = (1,1)$.

For $\tau \neq (1,1)$, we have that $\mathbb{P}^\tau(p) = \emptyset$ if and only if $p \in K^{\times 2} \cdot (R_p^\tau)^\times$, and this is a diophantine subset of K. Thus for any σ, Φ_σ is the intersection of finitely many diophantine sets and is thus diophantine over K.

Now we prove (2). Suppose $\sigma \neq (1,1)$ and that $p \in \Phi_\sigma$. Then because $\psi_{L/K}((p)) = \sigma$ and $\mathbb{P}(p) \subseteq \mathbb{P}^{(1,1)} \cup \mathbb{P}^\sigma$, there must be some prime $\mathfrak{p} \in \mathbb{P}^\sigma(p)$, because otherwise we would have $\psi((p)) = (1,1)$. If $\sigma = (-1,-1)$, then we observe that $J(R_p^{(-1,-1)}) = J_{a,p} + J_{b,p}$ is diophantine over K by Definition 3.6 and Lemma 3.7. Similarly, $J(R_p^{(-1,1)}) = J_{a,p} + J_{ab,p} + J_{a,cp}$ and $J(R_p^{(1,-1)}) = J_{b,p} + J_{ab,p} + J_{b,dp}$ are diophantine over K.

We move on to (3). Suppose that $\sigma \in \mathrm{Gal}(K(\sqrt{a},\sqrt{b})/K)$ with $\sigma \neq (1,1)$ and $\mathfrak{p}_0 \nmid \mathfrak{m}$ is a prime of K satisfying $\psi_{L/K}(\mathfrak{p}_0) = \sigma$. Let $\mathfrak{q}' \nmid \mathfrak{m}$ be a prime of K with $\psi_{L/K}(\mathfrak{q}') = (1,1)$ and let $S' = \{\mathfrak{q}'\}$. By Lemma 3.8 we can choose a prime $\mathfrak{q}$ of K such that it represents the class of $(\mathfrak{p}_0 \cap \mathcal{O}_{S'})^{-1}$ in $\mathrm{Cl}(\mathcal{O}_{S'})$ and $\psi_{L/K}(\mathfrak{q}) = (1,1)$. Then there is an element $p \in \mathcal{O}_{S'}$ such that $(\mathfrak{p}_0 \cap \mathcal{O}_{S'})(\mathfrak{q} \cap \mathcal{O}_{S'}) = p\mathcal{O}_{S'}$.

We claim that $p \in \Phi_\sigma$. Since $v_\mathfrak{p}(p) = 0$ if $\mathfrak{p} \neq \mathfrak{p}_0, \mathfrak{q}, \mathfrak{q}'$, it follows that $(p) \in I_\mathfrak{m}$ and

$$\psi_{L/K}((p)) = \psi_{L/K}(\mathfrak{p}_0)\psi_{L/K}(\mathfrak{q})\psi_{L/K}(\mathfrak{q}') = \sigma.$$

Additionally, the only primes $\mathfrak{p}$ with $v_\mathfrak{p}(p)$ odd are $\mathfrak{p}_0$, $\mathfrak{q}$, and possibly $\mathfrak{q}'$. Hence $\mathbb{P}(p) \subseteq \mathbb{P}^{(1,1)} \cup \mathbb{P}^\sigma$ and $p \in \Phi_\sigma$. Finally, we observe that $\mathbb{P}^\sigma(p) = \{\mathfrak{p}_0\}$. □

Lemma 3.15. *Let $\mathfrak{p}_0, \mathfrak{q}_0$ be primes of K not dividing $\mathfrak{m}$ with $\psi_{L/K}(\mathfrak{q}_0) = (1,1)$. Let $A := \mathcal{O}_{\{\mathfrak{q}_0\}}$. Then there exists infinitely many $q \in K^\times$ satisfying*

1) $\psi_{L/K}((q)) = (-1,-1)$;
2) $\left(\frac{q}{\mathfrak{p}_0}\right) = -1$;
3) *qA is a prime ideal of A, so there exists a prime $\mathfrak{q}$ of K such that $\mathfrak{q} \cap A = qA$.*

Proof. Set

$$K_{\mathfrak{m}} := \{\alpha \in K^\times : v_{\mathfrak{p}}(\alpha) = 0 \quad \forall \mathfrak{p} | \mathfrak{m}\}.$$

For a prime $\mathfrak{p} \neq \mathfrak{q}_0$ of K, let $I_{\mathfrak{p}} := A \cap \mathfrak{p}$ be the associated prime ideal in A. Given $x \in K_{\mathfrak{m}}$, we can find $y, z \in A \cap K_{\mathfrak{m}}$ such that $x = y/z$. Then y and z are $\mathfrak{p}$-adic units for each $\mathfrak{p}|\mathfrak{m}$ and thus we can map $x = y/z$ to the image of y/z modulo $\prod_{\mathfrak{p}|\mathfrak{m}} I_{\mathfrak{p}}^{\mathfrak{m}(\mathfrak{p})}$. The kernel of this map is $K_{\mathfrak{m},1}$ so there is a well-defined isomorphism

$$K_{\mathfrak{m}}/K_{\mathfrak{m},1} \simeq \left(A \Big/ \prod_{\mathfrak{p}|\mathfrak{m}} I_{\mathfrak{p}}^{\mathfrak{m}(\mathfrak{p})}\right)^\times.$$

By the Chinese Remainder Theorem,

$$K_{\mathfrak{p}_0\mathfrak{m}}/K_{\mathfrak{p}_0\mathfrak{m},1} \cong K_{\mathfrak{m}}/K_{\mathfrak{m},1} \times (A/I_{\mathfrak{p}_0})^\times.$$

The group $K_{\mathfrak{m}}/K_{\mathfrak{m},1}$ surjects onto the ray classes in $C_{\mathfrak{m}}$ consisting of principal fractional ideals by the map

$$xK_{\mathfrak{m},1} \mapsto (x)P_{\mathfrak{m}}.$$

Now we apply Lemma 3.8 part (3) to find a prime $\mathfrak{q}'$ of K in the principal ideal class of $\mathrm{Cl}(A)$ such that $\psi_{L/K}(\mathfrak{q}') = (-1,-1)$. Then there exists $x_1 \in K^\times$ such that $\psi_{L/K}((x_1)) = (-1,-1)$ and $x_1 A = \mathfrak{q}' \cap A$ is a prime ideal of A. Let s be a non-square of $(A/I_{\mathfrak{p}_0})^\times$. By the Chinese Remainder Theorem, the element $(x_1 K_{\mathfrak{m},1}, s)$ in $K_{\mathfrak{m}}/K_{\mathfrak{m},1} \times (A/I_{\mathfrak{p}_0})^\times$ corresponds to an element $x_2 K_{\mathfrak{p}_0\mathfrak{m},1} \in K_{\mathfrak{p}_0\mathfrak{m}}/K_{\mathfrak{p}_0\mathfrak{m},1}$. By construction, $\left(\frac{x_2}{\mathfrak{p}_0}\right) = -1$. The ideal $x_2 A$ need not be a prime ideal of A, but by Theorem 2.9, we can find infinitely many prime ideals of A in the class generated by x_2 in $\mathrm{Cl}_{\mathfrak{m}\mathfrak{p}_0}(A)$; such a prime ideal is of the form $qA = \mathfrak{q} \cap A$. Both qA and $x_2 A$ generate the same class in $\mathrm{Cl}_{\mathfrak{m}\mathfrak{p}_0}(A)$ and hence $q = x_2 t$ for some $t \in K_{\mathfrak{m}\mathfrak{p}_0,1}$. Thus

$\psi_{L/K}((q)) = \psi_{L/K}((x_2))$ and since q and x_2, as elements of A, are congruent modulo the ideal $I_{\mathfrak{p}_0}$ of A,

$$\left(\frac{q}{\mathfrak{p}_0}\right) = \left(\frac{x_2}{\mathfrak{p}_0}\right) = -1.$$

Thus the element q satisfies the three requirements of the lemma. □

We now need more definitions from [12].

Definition 3.16. For $\sigma \in \mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K)$, and $S \subseteq S_K$ the fixed set of primes from above, define

$$\widetilde{\Phi_\sigma} := K^{\times 2} \cdot \Phi_\sigma;$$

$$\Psi_K := \left\{ (p,q) \in \widetilde{\Phi_{(1,1)}} \times \widetilde{\Phi_{(-1,-1)}} \;\middle|\; \prod_{\mathfrak{p}|\mathfrak{m}} (ap,q)_{\mathfrak{p}} = -1 \right.$$
$$\left. \text{and } p \in a \cdot K^{\times 2} \cdot (1 + J(R_q^{(-1,-1)})) \right\}.$$

Lemma 3.17.

1) *The set Ψ_K is diophantine over K.*
2) *For $(p,q) \in \psi_{L/K}$, we have $\emptyset \neq \Delta_{ap,q} \cap \Delta_{bp,q} \subseteq I_{\mathfrak{m}}$, and $J(R_{p,q}^{(1,1)})$ is diophantine over K.*
3) *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 $\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}_0\}$.*

Proof. By Lemma 3.14 part (1), $\widetilde{\Phi_{(1,1)}} \times \widetilde{\Phi_{(-1,-1)}}$ is diophantine over K, and by Lemma 3.14 part (2), $J(R_q^{(-1,-1)})$ is diophantine over K. By Theorem 4.5, for any prime $\mathfrak{p}$ of K,

$$\{(x,y) : (x,y)_{\mathfrak{p}} = -1\} \subseteq K^\times \times K^\times$$

is diophantine over K. Here, $(\cdot,\cdot)_{\mathfrak{p}}$ denotes the Hilbert symbol of K at $\mathfrak{p}$. Since only finitely many $\mathfrak{p}$ divide $\mathfrak{m}$, the set Ψ_K is the intersection of finitely many sets diophantine over K.

For (2), the proof in [12] of Lemma 3.25 part (2) shows that for $(p,q) \in \Psi_K$, if $\mathfrak{p} \nmid \mathfrak{m}$ then $\Delta_{ap,q} \cap \Delta_{bp,q} \cap I_{\mathfrak{m}}$ is nonempty. We only need to show that if $\mathfrak{p}|\mathfrak{m}$, $\mathfrak{p} \notin \Delta_{ap,q} \cap \Delta_{bp,q}$. Suppose that $\mathfrak{p} \in \Delta_{ap,q}$. Then $(ap,q)_{\mathfrak{p}} = -1$. Since

$p \in \widetilde{\Phi_{(1,1)}}$ and $q \in \widetilde{\Phi_{(-1,-1)}}$ we can assume that, possibly after multiplying by a square of $K^\times$, $v_\mathfrak{p}(p) = v_\mathfrak{p}(q) = 0$. Then $(ap, q)_\mathfrak{p} = -1$ implies that $v_\mathfrak{p}(ap) = v_\mathfrak{p}(a)$ is odd, which implies $v_\mathfrak{p}(b)$ must be 0 since the fractional ideals (a) and (b) have disjoint support. Thus $(bp, q)_\mathfrak{p} = 1$ and $\mathfrak{p} \notin \Delta_{ap,q} \cap \Delta_{bp,q}$.

Now we prove (3). Let $\mathfrak{p}_0$ satisfy $\mathfrak{p}_0 \nmid \mathfrak{m}$ and $\psi_{L/K}(\mathfrak{p}_0) = (1,1)$; we wish to construct a pair $(p,q) \in \Psi_K$ such that $\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}_0\}$. We begin by constructing our candidate for q. Choose a different prime $\mathfrak{q}_0$ of K not dividing $\mathfrak{m}$ with $\psi_{L/K}(\mathfrak{q}_0) = (1,1)$. Using Lemma 3.15, choose $q \in K^\times$ such that $\psi_{L/K}((q)) = (-1,-1)$, $\left(\frac{q}{\mathfrak{p}_0}\right) = -1$, and q generates a prime ideal of $A := \mathcal{O}_{\{\mathfrak{q}_0\}}$. Thus there exists a prime $\mathfrak{q}$ of K with $qA = \mathfrak{q} \cap A$. Observe that this implies that the support of (q) is $\{\mathfrak{q}, \mathfrak{q}_0\}$. We claim that

$$\Delta_{a,q} \cap \Delta_{b,q} = \{\mathfrak{q}\}.$$

We begin by showing that $(a,q)_\mathfrak{q} = (b,q)_\mathfrak{q} = -1$. The support of (a) and (b) is contained in $\mathfrak{m}$, so $v_\mathfrak{q}(a) = v_\mathfrak{q}(b) = 0$. We have that $v_\mathfrak{q}(q)$ is odd, so we need to show a and b are non-squares in the completion of K at $\mathfrak{q}$. This follows immediately from $\psi_{L/K}(\mathfrak{q}) = (-1,-1)$. From $\psi_{L/K}(\mathfrak{q}_0) = (1,1)$ we get that $\mathfrak{q}_0 \notin \Delta_{a,q} \cap \Delta_{b,q}$. No other prime $\mathfrak{p}$ in $I_\mathfrak{m}$ can appear in this set since we have $v_\mathfrak{p}(q) = v_\mathfrak{p}(a) = v_\mathfrak{p}(b) = 0$. Finally, no prime $\mathfrak{p}|\mathfrak{m}$ can occur in $\Delta_{a,q} \cap \Delta_{b,q}$ since we cannot have that $v_\mathfrak{p}(a)$ and $v_\mathfrak{p}(b)$ are both odd as their supports are disjoint, and $v_\mathfrak{p}(q) = 0$. This proves the claim.

For each prime $\mathfrak{p}|\mathfrak{m}$, let $E_\mathfrak{p} \subseteq K$ be a generating set for $K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2}$ chosen so that for each $e \in E_\mathfrak{p}$, we have $v_{\mathfrak{p}_0}(e-1) \geq 0$. Fix $e_0 \in K$ such that $\left(\frac{e_0}{\mathfrak{q}}\right) = -1$ and $\left(\frac{e_0}{\mathfrak{p}_0}\right) = 1$.

Now one can construct $p \in K^\times$ so that $(p,q) \in \psi_{L/K}$ with $\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}_0\}$ as it is constructed in [12], Lemma 3.25(c). The remainder of the proof exactly follows Park's after Equation 3.6 (loc. cit.). The only difference is that instances of the *ideal* (q) of the number field K are replaced with the prime $\mathfrak{q}$ of K in this proof. □

3.4. Proof of main theorem

Our general strategy in proving Theorem 1.2 follows that of [8].

Definition 3.18. Given some finite set of primes $\Delta \subseteq S$ of K, consider the semi-local subring $R = \bigcap_{\mathfrak{p} \in \Delta} \mathcal{O}_\mathfrak{p}$ of K. Set

$$\widetilde{R} = \{x \in K : \nexists y \in J(R) \text{ with } xy = 1\}.$$

Lemma 3.19.

1) *If $J(R)$ is diophantine over K, then $\widetilde{R}$ is defined by a universal formula in K.*
2) *$\widetilde{R} = \bigcup_{\mathfrak{p}\in\Delta} \mathcal{O}_\mathfrak{p}$, provided that $\Delta \neq \emptyset$. In particular, $\widetilde{\mathcal{O}_\mathfrak{p}} = \mathcal{O}_\mathfrak{p}$.*

Proof. To see (1), observe that

$$\widetilde{R} = \{x \in K : x = 0 \text{ or } x^{-1} \in K \setminus J(R)\}.$$

Since $J(R)$ is diophantine, its complement is defined by a universal formula, and thus so is $\widetilde{R}$.

Now we prove (2). To see that $\widetilde{R} \subseteq \bigcup_{\mathfrak{p}\in\Delta} \mathcal{O}_\mathfrak{p}$, assume $x \notin \bigcup_{\mathfrak{p}\in\Delta} \mathcal{O}_\mathfrak{p}$. This means that for all $\mathfrak{p} \in \Delta$, $v_\mathfrak{p}(x) < 0$ and hence $v_\mathfrak{p}(x^{-1}) > 0$, giving $x^{-1} \in \bigcap_{\mathfrak{p}\in\Delta} \mathcal{O}_\mathfrak{p} = J(R)$. Hence $x \notin \widetilde{R}$. For the reverse inclusion, suppose $x \in \mathcal{O}_\mathfrak{p}$ for some $\mathfrak{p} \in \Delta$. Then if $y \in J(R)$, we have that $v_\mathfrak{p}(x \cdot y) \geq 1$ and hence $x \cdot y \neq 1$. Thus $x \in \widetilde{R}$. □

Given a modulus $\mathfrak{m}$, let $S(\mathfrak{m}) := \{\mathfrak{p} : \mathfrak{p}|\mathfrak{m}\}$.

Theorem 3.20. *For any global function field K and finite set of primes $S \subset S_K$, with $\mathfrak{m}$ chosen as before,*

$$\mathcal{O}_S = \bigcap_{\mathfrak{p}\in S(\mathfrak{m})\setminus S} \widetilde{\mathcal{O}_\mathfrak{p}} \cap \left(\bigcap_{\sigma\neq(1,1)} \bigcap_{p\in\Phi_\sigma} \widetilde{R_p^\sigma} \right) \cap \bigcap_{(p,q)\in\Psi_K} \widetilde{R_{p,q}^{(1,1)}},$$

where Φ_σ and Ψ_K are the diophantine sets in the previous section.

Proof. For $p \in \Phi_\sigma$ and $(p,q) \in \Psi_K$, all of the sets $\mathbb{P}^\sigma(p)$ and $\Delta_{ap,q} \cap \Delta_{bp,q}$ are nonempty. Thus the right hand side is equal to

$$R_S := \bigcap_{\mathfrak{p}\in S(\mathfrak{m})\setminus S} \mathcal{O}_\mathfrak{p} \cap \left(\bigcap_{\sigma\neq(1,1)} \bigcap_{\mathfrak{p}\in\Phi_\sigma} \bigcup_{\mathfrak{p}\in\mathbb{P}^\sigma(p)} \mathcal{O}_\mathfrak{p} \right) \cap \bigcap_{(p,q)\in\Psi_K} \bigcup_{\mathfrak{p}\in\Delta_{ap,q}\cap\Delta_{bp,q}} R_{p,q}^{(1,1)}.$$

To show R_S is contained in $\mathcal{O}_S$, consider a prime $\mathfrak{p}_0 \notin S$. We need to show that any $x \in R_S$ is integral at $\mathfrak{p}_0$. If $\mathfrak{p}_0|\mathfrak{m}$, this is clear. If not, consider the image of $\mathfrak{p}_0$ under $\psi_{L/K}$. First we assume $\psi_{L/K}(\mathfrak{p}_0) \neq (1,1)$. Then we

claim that we can choose $p, p' \in \Phi_\sigma$ such that

$$\mathcal{O}_{\mathfrak{p}_0} = \bigcup_{\mathfrak{p} \in \mathbb{P}^\sigma(p)} \mathcal{O}_\mathfrak{p} \cap \bigcup_{\mathfrak{p} \in \mathbb{P}^\sigma(p')} \mathcal{O}_\mathfrak{p}.$$

If this claim is true, then $x \in R_S$ implies that $v_{\mathfrak{p}_0}(x) \geq 0$. Suppose $\sigma = (-1,-1)$. Using Lemma 3.14, we find $p \in \Phi_\sigma$ such that $\{\mathfrak{p}_0\} = \mathbb{P}^\sigma(p)$. Now let $\mathfrak{p}_1$ be some other prime of K not dividing $\mathfrak{m}$ with $\psi_{L/K}(\mathfrak{p}_1) = (1,1)$, set $S' = \{\mathfrak{p}_1\}$ and $A := \mathcal{O}_{S'}$. Then using Lemma 3.8, we find a prime $\mathfrak{q}$ of K such that $\mathfrak{q} \cap A$ is in the ideal class of $(\mathfrak{p}_0 \cap A)^{-1}$ in $\mathrm{Cl}(A)$ and $\psi_{L/K}(\mathfrak{q}) = (1,1)$. There exists an element $p' \in A$ such that $(\mathfrak{p}_0 \cap A)(\mathfrak{q} \cap A) = p'A$. Then $p' \in \Phi_{(-1,-1)}$, as $\mathfrak{p}_0, \mathfrak{p}_1$, and $\mathfrak{q}$ do not divide $\mathfrak{m}$, $\mathbb{P}(p') = \{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{q}\}$, and

$$\psi_{L/K}(p') = \psi_{L/K}(\mathfrak{p}_0)\psi_{L/K}(\mathfrak{p}_1)\psi_{L/K}(\mathfrak{q}) = (-1,-1).$$

Thus $\mathbb{P}^{(-1,-1)}(p) \cap \mathbb{P}^{(-1,-1)}(p) = \{\mathfrak{p}_0\}$ and the claim follows; the case of $\sigma = (-1,1)$ and $\sigma = (1,-1)$ is entirely similar.

If $\mathfrak{p}_0$ satisfies $\psi_{L/K}(\mathfrak{p}_0) = (1,1)$ then we have seen in Lemma 3.17 that there exist $(p,q) \in \Psi_K$ such that $\{\mathfrak{p}_0\} = \Delta_{ap,q} \cap \Delta_{bp,q}$ (and consequently $(p,q) \in \Psi_K$), implying

$$\bigcup_{\mathfrak{p} \in \Delta_{ap,q} \cap \Delta_{bp,q}} \mathcal{O}_\mathfrak{p} = \mathcal{O}_{\mathfrak{p}_0}.$$

Thus x is integral at primes outside of S.

To show the reverse inclusion, we claim that membership in R_S imposes no integrality condition at a prime in S. If $\mathfrak{p}_0 \in S$, for any $\sigma \in \mathrm{Gal}(L/K)$ and any $p \in \Phi_\sigma$, we have $\mathfrak{p}_0 \notin \mathbb{P}^\sigma(p)$. Additionally, $\mathfrak{p}_0 \notin \Delta_{ap,q} \cap \Delta_{bp,q}$ for $(p,q) \in \Psi_K$ as $\Delta_{ap,q} \cap \Delta_{bp,q} \subseteq I_\mathfrak{m}$ by Lemma 3.17 part (2). □

Now we are ready to prove our first main theorem.

Theorem 1.2. *For any global function field K with $\mathrm{char}(K) \neq 2$, and any nonempty, finite set of primes S of K, $\mathcal{O}_S$ is defined by a first-order universal formula.*

Proof. Theorem 3.20 shows that for $t \in K$,

$$\begin{aligned} t \in \mathcal{O}_S \iff & t \in \bigcap_{\mathfrak{p}|\mathfrak{m}} \widetilde{\mathcal{O}_\mathfrak{p}} \\ & \wedge \forall p \bigwedge_{\sigma \neq (1,1)} (p \notin \Phi_\sigma \vee t \in \widetilde{R_p^\sigma}) \\ & \wedge \forall p, q \quad (p,q) \notin \Psi_K \vee t \in \widetilde{R_{p,q}^{(1,1)}}. \end{aligned}$$

Given $\sigma \in \mathrm{Gal}(L/K)$, $p \in \Phi_\sigma$, and $(p,q) \in \Psi_K$, we have that $J(R_p^\sigma)$ and $J(R_{p,q}^{(1,1)})$ are diophantine by Lemmas 3.14 and 3.17. The sets Φ_σ and Ψ_K are diophantine by the same lemmas, so their complements are defined by a universal formula. Additionally, membership in $\widetilde{R_p^\sigma}$ is given by a universal formula, along with membership in $\widetilde{R_{p,q}^{(1,1)}}$. Hence membership in $\mathcal{O}_S$ can be given by a universal formula. □

4. Non-squares and non-norms of global fields are diophantine

Now we let K be a global field with $\mathrm{char}(K) \neq 2$. Throughout this section, fix a, b, c, d as in Lemmas 3.8 and 3.10 if K is a global function field, and if K is a number field, choose $a, b \in K^\times$ as in Proposition 3.19 of [12]. Additionally, we fix $c, d \in K^\times$ satisfying the same assumptions as in Lemma 3.10 but now in the case that K is a number field. Corollary 3.20 in [12] is incorrect as stated, and has to be modified as in Corollary 3.11 of our paper. With this modification, the other results from [12] are correct as stated. Set $L := K(\sqrt{a}, \sqrt{b})$ and fix an admissible modulus $\mathfrak{m}$ for L/K where $\mathfrak{m}$ contains all the primes dividing $(2abcd)$, and all real places if K is a number field. In this section we prove Theorems 1.4 and 1.3.

4.1. Non-squares

We begin by proving Theorem 1.4, i.e. that $K \setminus K^{\times 2}$ is diophantine over K. We use the fact that $x \notin K^{\times 2}$ is equivalent to x being a non-square in a completion of K at some prime $\mathfrak{p}$, where $\mathfrak{p}$ may be finite or infinite.

Suppose ∞ is a real archimedean prime of K corresponding to an embedding $\omega : K \hookrightarrow \mathbb{R}$. For $x \in K^\times$, we have that x is not a square in K_∞ if and only if $\omega(x) < 0$. Therefore we require the following lemma:

Lemma 4.1. *Suppose K is a number field and that ∞ is a real archimedean prime of K corresponding to an embedding $\omega : K \hookrightarrow K_{\mathfrak{p}} = \mathbb{R}$. Then the set*

$$K_\omega^\times := \{x \in K^\times : \omega(x) > 0\}$$

is diophantine over K. Moreover, the set

$$\{x \in K^\times : x \text{ is not totally positive }\}$$

is diophantine over K.

Proof. Let $\mathfrak{p}$ be a finite prime of K and let B be the quaternion algebra over K ramified exactly at $\mathfrak{p}$ and ∞. Let $\mathrm{Nrd} : B \to K$ denote the reduced norm map on B. Then by Facts I and II of [20], $\mathrm{Nrd}(B^\times) = K_\omega^\times$. Let b_1, b_2, b_3, b_4 be a K-basis of B. Then

$$q(x_1, x_2, x_3, x_4) := \mathrm{Nrd}\left(\sum_{i=1}^{4} x_i b_i\right)$$

is a quadratic form in the variables $x_1, \ldots, x_4$ with coefficients in K, and

$$K_\omega^\times = \{x \in K^\times : \exists a_1, \ldots, a_4 \in K \text{ s.t. } q(a_1, a_2, a_3, a_4) = x\}.$$

We conclude that $K_\omega^\times$ is diophantine over K. For an alternative proof, see [5], Lemma 10.

Now we will prove the second statement. Let $\omega_1, \ldots, \omega_r$ denote a complete set of representatives of the inequivalent embeddings of K into $\mathbb{R}$. The set of elements which are not totally positive is diophantine over K, since it is the finite union $\bigcup_i -K_{\omega_i}^\times$. □

The main lemma used in proving Theorem 1.4 is the following:

Lemma 4.2. *Let K be a global field with* $\mathrm{char}(K) \neq 2$. *Then*

$$x \notin K^{\times 2} \iff \begin{cases} x \text{ is not totally positive, or} \\ v_{\mathfrak{p}}(x) \text{ is odd for some } \mathfrak{p} | \mathfrak{m}_0, \text{ or} \\ \exists p \in \Phi_{(-1,1)} \text{ such that } x \in a \cdot K^{\times 2} \cdot (1 + J(R_p^{(-1,1)})). \end{cases}$$

Here, $\mathfrak{m}_0$ denotes the finite primes dividing $\mathfrak{m}$, and $\Phi_{(-1,1)}$, $R_p^{(-1,1)}$, a, and $\mathfrak{m}$ are as in Section 3.3. Before proving Lemma 4.2, we will show how to use it to prove Theorem 1.4.

Proof of Theorem 1.4 from Lemma 4.2. We begin by showing the right side of the equivalence in Lemma 4.2 defines a diophantine subset of K. We claim that, for a prime $\mathfrak{p}$ of K, the set

$$\{x \in K^\times : v_\mathfrak{p}(x) \text{ is odd}\}$$

is diophantine over K. To see this, fix $p \in K^\times$ with $v_\mathfrak{p}(p) = 1$. Then $v_\mathfrak{p}(x)$ is odd if and only if $x \in p \cdot K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times$. This is diophantine over K since

$$\mathcal{O}_\mathfrak{p}^\times = \mathcal{O}_\mathfrak{p} \cap \{x \in K^\times : x^{-1} \in \mathcal{O}_\mathfrak{p}\}.$$

Since only finitely many primes divide $\mathfrak{m}_0$, the condition that $v_\mathfrak{p}(x)$ is odd for some $\mathfrak{p}|\mathfrak{m}_0$ is diophantine as well. As noted in Lemma 4.1, the condition that x is not totally positive defines a diophantine set. If K is a global function field, Lemma 3.14 parts (1) and (2) complete the argument that the right side of Lemma 4.2 defines a diophantine subset of K. The number field case follows from parts (a) and (b) of Lemma 3.22 of [12]. Hence Lemma 4.2 shows that $K^\times \setminus K^{\times 2}$ is diophantine. □

We are now left with proving Lemma 4.2, for which we need the following lemma.

Lemma 4.3. *Let $\Phi_{(-1,1)}$, $R_p^{(-1,1)}$, a, b, and $\mathfrak{m}$ be defined as in Section 3.3. Let $p \in \Phi_{(-1,1)}$. Then $x \in a \cdot K^{\times 2} \cdot (1 + J(R_p^{(-1,1)}))$ if and only if there exists an element $t \in K^\times$ such that $\forall \mathfrak{q} \in \mathbb{P}^{(-1,1)}(p)$, $v_\mathfrak{q}(xt^2) = 0$ and the image of xt^2 in the residue field of $\mathfrak{q}$ is not a square.*

Proof. Since $p \in \Phi_{(-1,1)}$, we have that $\mathbb{P}^{(-1,1)}(p) \neq \emptyset$. In the function field setting, this follows from Lemma 3.14, and in the number field setting, it follows from Lemma 3.22 of [12]. We also have that

$$R_p^{(-1,1)} = \bigcap_{\mathfrak{q} \in \mathbb{P}^{(-1,1)}(p)} \mathcal{O}_\mathfrak{q},$$
$$J(R_p^{(-1,1)}) = \bigcap_{\mathfrak{q} \in \mathbb{P}^{(-1,1)}(p)} \mathfrak{q}O_\mathfrak{q}.$$

Suppose there exists $t \in K^\times$ as in the lemma. Let $\mathfrak{q} \in \mathbb{P}^{(-1,1)}(p)$. Then $xt^2 \equiv a$ in $(\mathcal{O}_\mathfrak{q}/\mathfrak{q})^\times/(\mathcal{O}_\mathfrak{q}/\mathfrak{q})^{\times 2}$, since by our choice of a and b,

$$\left(\left(\frac{a}{\mathfrak{q}}\right)_2, \left(\frac{b}{\mathfrak{q}}\right)_2\right) = (\mathfrak{q}, K(\sqrt{a}, \sqrt{b})/K) = (-1, 1).$$

Here $\left(\frac{\cdot}{\mathfrak{q}}\right)_2$ is the degree 2 power residue symbol for K. Thus there is some $s_\mathfrak{q} \in (\mathcal{O}_\mathfrak{q})^\times$ such that $xt^2 = as_\mathfrak{q}^2 \mod \mathfrak{q}$; using the Chinese remainder theorem we find an s so that $xt^2 = as^2 \mod \mathfrak{q}$ for each $\mathfrak{q}$. Since $q := xt^2 - as^2 \in \mathfrak{q}$ for each $\mathfrak{q} \in \mathbb{P}^{(-1,1)}(p)$, it is in their intersection. Thus

$$x = a \cdot (s/t)^2(1 + q/(as^2)).$$

We claim x is in $a \cdot K^{\times 2} \cdot (1 + \bigcap_{\mathfrak{q}\in\mathbb{P}^{(-1,1)}(p)} \mathfrak{q}\mathcal{O}_\mathfrak{q})$. Let $\mathfrak{q} \in \mathbb{P}^{(-1,1)}(p)$. Then $v_\mathfrak{q}(a) = 0$ because (a) is only divisible by primes dividing $\mathfrak{m}$ and $\mathfrak{q} \in I_\mathfrak{m}$. Additionally, $v_\mathfrak{q}(s) = 0$ and $v_\mathfrak{q}(q) \geq 1$, because $s \in \mathcal{O}_\mathfrak{q}^\times$ and $q \in \mathfrak{q}$. The claim follows as

$$v_\mathfrak{q}(q/as^2) \geq 1 - v_\mathfrak{q}(a) - 2v_\mathfrak{q}(s) \geq 1.$$

For the other implication, write $x = at^2(1 + j)$ with $t \neq 0$ and $j \in \bigcap_{\mathfrak{q}\in\mathbb{P}^{(-1,1)}(p)} \mathfrak{q}\mathcal{O}_\mathfrak{q}$. Then

$$v_\mathfrak{q}(x/t^2) = v_\mathfrak{q}(a(1 + j)) = v_\mathfrak{q}(a) = 0$$

for each $\mathfrak{q} \in \mathbb{P}^\sigma(p)$, and $x/t^2 \equiv a$ modulo $\mathfrak{q}$ for $\mathfrak{q} \in \mathbb{P}^{(-1,1)}(p)$. Finally, by construction, a is a non-square in the completion at any prime $\mathfrak{q} \in \mathbb{P}^{(-1,1)}(p)$. □

We now prove Lemma 4.2:

Proof of Lemma 4.2. For the forward implication, suppose x is not a square. If x is not totally positive, or $v_\mathfrak{p}(x)$ is odd for some $\mathfrak{p}|\mathfrak{m}$, we are done, so assume that $v_\mathfrak{p}(x)$ is even for each $\mathfrak{p}|\mathfrak{m}$ and that x is totally positive. Using weak approximation, we may assume that in fact $v_\mathfrak{p}(x) = 0$ for each $\mathfrak{p}|\mathfrak{m}$. This does not change the truth value of either side of the implication in Lemma 4.2, as both statements are invariant under multiplying x by a square.

What we will now show is that there is a $p \in \Phi_{(-1,1)}$ such that $\mathbb{P}^{(-1,1)}(p) = \{\mathfrak{q}\}$, $v_\mathfrak{q}(x) = 0$, and such that x modulo $\mathfrak{q}$ is not a square. Together with Lemma 4.3, this will imply that $x \in a \cdot K^{\times 2} \cdot (1 + J(R_p^{(-1,1)}))$.

As $K(\sqrt{x})$ is a degree 2 extension of K unramified at all $\mathfrak{p}|\mathfrak{m}$, it is linearly disjoint from $L = K(\sqrt{a}, \sqrt{b})$ over K. Let τ be the nontrivial automorphism of $K(\sqrt{x})/K$ and consider $(\tau, (-1, 1)) \in \mathrm{Gal}(K(\sqrt{x})/K) \times \mathrm{Gal}(L/K)$. By

the Chebotarev Density Theorem, there is a prime $\mathfrak{q}$ of K so that its associated Frobenius automorphism is $(\tau, (-1, 1))$. The restriction of this automorphism to $K(\sqrt{x})$ is

$$\tau = (\mathfrak{q}, K(\sqrt{x})/K),$$

implying $\mathfrak{q}$ does not split completely in $K(\sqrt{x})$. Hence x is not a square in the completion of K at $\mathfrak{q}$. The restriction to L is

$$(-1, 1) = (\mathfrak{q}, K(\sqrt{a}, \sqrt{b})/K),$$

so we have that $\mathfrak{q} \in \mathbb{P}^{(-1,1)}$. If K is a global function field, Lemma 3.14 implies there exists an element $p \in K^\times$ so that $\{\mathfrak{q}\} = \mathbb{P}^{(-1,1)}(p)$. In the number field setting, this follows from Lemma 3.22 in [12]. This is the desired element p and prime $\mathfrak{q}$, and finishes the first half of the proof.

For the reverse implication, suppose that there is an element $p \in \Phi_{(-1,1)}$ such that $x \in a \cdot K^{\times 2} \cdot (1 + J(R_p^{(-1,1)}))$. By Lemma 4.3 there exists $t \neq 0$ such that xt^2 is a non-square in the completion of K at each prime $\mathfrak{q} \in \mathbb{P}^{(-1,1)}(p)$. This implies xt^2 itself is not a square in K, i.e. $x \notin K^{\times 2}$. □

4.2. Non-norms

Let K be a global field with $\mathrm{char}(K) \neq 2$. To prove Theorem 1.3, which states that the set

$$\{(x, y) \in K^\times \times K^\times : x \text{ is not a norm of } K(\sqrt{y})\}$$

is diophantine over K, we use the Hasse norm theorem: for a cyclic extension L/K, an element of K is a (relative) norm of an element of L if and only if it is a local norm in every completion of K. We will use the fact that

$$\begin{aligned}(x, y)_\mathfrak{p} = -1 &\Leftrightarrow x \text{ is not a local norm of } K(\sqrt{y}) \\ &\Leftrightarrow y \text{ is not a local norm of } K(\sqrt{x}).\end{aligned}$$

We begin by establishing that, given a finite or infinite prime $\mathfrak{p}$ of K, the collection of pairs $(x, y) \in K^\times \times K^\times$ such that x is not a local norm in the completion of $K(\sqrt{y})$ at $\mathfrak{p}$ is diophantine over K.

First we need the following lemma, which will be used both in the proof of Theorem 4.5 and later in proving Theorem 1.3.

Lemma 4.4. *Let $\mathfrak{p}$ be a finite prime of K with $|\mathbb{F}_\mathfrak{p}|$ odd. Fix $p, s \in K^\times$ so that $v_\mathfrak{p}(p) = 1$ and $v_\mathfrak{p}(s) = 0$ so that $\mathrm{red}_\mathfrak{p}(s)$ is not a square in the residue field of $\mathfrak{p}$. Then for $x, y \in K^\times$, $(x, y)_\mathfrak{p} = -1$ if and only if*

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

Proof. Assume that $(x, y)_\mathfrak{p} = -1$. From the formula for the Hilbert symbol in Section 3.1, at least one of x or y must have odd valuation at $\mathfrak{p}$, so without loss of generality, assume $v_\mathfrak{p}(x)$ is odd. As $(x, y)_\mathfrak{p} = -1$, the formula for the Hilbert symbol implies $((-1)^{v_\mathfrak{p}(x)v_\mathfrak{p}(y)})^{(|\mathbb{F}_\mathfrak{p}|-1)/2} = -1$ and $\mathrm{red}_\mathfrak{p}\left(\frac{x^{v_\mathfrak{p}(y)}}{y^{v_\mathfrak{p}(x)}}\right)^{\frac{|\mathbb{F}_\mathfrak{p}|-1}{2}} = 1$ or vice versa. Then $v_\mathfrak{p}(x/p)$ is even and $x/p \in K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times$.

Case 1. If $v_\mathfrak{p}(y)$ is even, then using weak approximation, choose $t \in K^\times$ so that yt^2 is a $\mathfrak{p}$-adic unit. In this case, $\mathrm{red}_\mathfrak{p}\left(\frac{x^{v_\mathfrak{p}(y)}}{y^{v_\mathfrak{p}(x)}}\right)^{\frac{|\mathbb{F}_\mathfrak{p}|-1}{2}} = -1$ since $(-1)^{v_\mathfrak{p}(x)v_\mathfrak{p}(y)} = 1$. We claim that yt^2 is a non-square modulo $\mathfrak{p}$. This follows from

$$\left(\frac{x^{v_\mathfrak{p}(y)}y^{-v_\mathfrak{p}(x)}yt^2}{\mathfrak{p}}\right)_2 = \left(\frac{(x^{(v_\mathfrak{p}(y))/2}y^{(1-v_\mathfrak{p}(x))/2}t)^2}{\mathfrak{p}}\right)_2 = 1.$$

Since yt^2 is not a square mod $\mathfrak{p}$, an argument similar to the one in the proof of Lemma 4.3 shows that $y \in s \cdot K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p})$.

Case 2. Suppose $v_\mathfrak{p}(y)$ is odd. We claim that, possibly after multiplying by a square of K, $-xy$ is not a square modulo $\mathfrak{p}$. This would imply that

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

which is what we want to show. To prove the claim, use weak approximation to find $t \in K^\times$ such that $v_\mathfrak{p}(xyt^2) = 0$. The following calculation shows $x^{v_\mathfrak{p}(y)}/y^{v_\mathfrak{p}(x)}$ and xyt^2 have the same 2-power residue for the prime $\mathfrak{p}$:

$$\left(\frac{x^{v_\mathfrak{p}(y)}y^{-v_\mathfrak{p}(x)}xyt^2}{\mathfrak{p}}\right)_2 = \left(\frac{(x^{(v_\mathfrak{p}(y)+1)/2}y^{(1-v_\mathfrak{p}(x))/2}t)^2}{\mathfrak{p}}\right)_2 = 1.$$

If $|\mathbb{F}_\mathfrak{p}|$ is 1 modulo 4, then -1 is a square in $\mathbb{F}_\mathfrak{p}$. From the formula for the Hilbert symbol, we must have that $x^{v_\mathfrak{p}(y)}/y^{v_\mathfrak{p}(x)}$ is not a square in the residue field of $\mathfrak{p}$, and hence neither is $-xyt^2$. If $|\mathbb{F}_\mathfrak{p}|$ is 3 mod 4, then considering the formula for $(x, y)_\mathfrak{p}$ again, we have $(-1)^{(|\mathbb{F}_\mathfrak{p}|-1)/2} = -1$ and thus $(x, y)_\mathfrak{p} = -1$

implies xyt^2 is a square modulo $\mathfrak{p}$. But since -1 is not a square modulo $\mathfrak{p}$, this implies xyt^2 is not a square modulo $\mathfrak{p}$, and hence $-xy \in a \cdot K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p})$.

Conversely, if $x \in p \cdot K^{\times 2} \cdot \mathcal{O}_\mathfrak{p}^\times$, then $v_\mathfrak{p}(x)$ is odd. If $y \in s \cdot K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p})$, then for some $t \in K^\times$, yt^2 is a $\mathfrak{p}$-adic unit and is a non-square modulo $\mathfrak{p}$. If $-xy \in s \cdot K^{\times 2} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p})$, then, possibly after multiplying by a square of $K^\times$, $-xy$ is a $\mathfrak{p}$-adic unit and is a non-square modulo $\mathfrak{p}$. Hence $(x, -xy)_\mathfrak{p} = -1$. Since $(x, -x)_\mathfrak{p} = 1$,

$$(x, y)_\mathfrak{p} = (x, -xy)_\mathfrak{p} = -1. \qquad \square$$

Theorem 4.5. *Let $\mathfrak{p}$ be a finite or real infinite prime of K. The set $\{(x, y) \in K^\times \times K^\times : (x, y)_\mathfrak{p} = -1\}$ is diophantine over K.*

Proof. First assume $\mathfrak{p}$ corresponds to a real archimedean absolute value on K. Let $\omega : K \hookrightarrow \mathbb{R}$ be the corresponding embedding of K into $K_\mathfrak{p} = \mathbb{R}$. Then $(x, y)_\mathfrak{p} = -1$ if and only if the equation $xs^2 + yt^2 = 1$ has no solutions in $\mathbb{R} \times \mathbb{R}$, which holds if and only if $\omega(x) < 0$ and $\omega(y) < 0$. These conditions are diophantine by Lemma 4.1.

Now suppose $\mathfrak{p}$ is a finite prime of K. If $|\mathbb{F}_\mathfrak{p}|$ is odd, the lemma follows from Lemma 4.4 since all the sets appearing are diophantine over K. Since our statements are only for global fields K with $\mathrm{char}(K) \neq 2$, the only remaining case is that K is a number field and $\mathfrak{p}|2$.

First we show that there are only finitely many elements in $K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2}$. Let π be a uniformizer for $\hat{\mathfrak{p}}$ and let e be the absolute ramification index, meaning $(\pi)^e = (2)$. Then if $\alpha \in R_\mathfrak{p}^\times$ is in $1 + \hat{\mathfrak{p}}^{2e+1}$, it is a square in $R_\mathfrak{p}^\times$ by Hensel's Lemma. We conclude that $R_\mathfrak{p}^{\times 2}$ is open in the profinite group $R_\mathfrak{p}^\times$ since it contains $1 + \hat{\mathfrak{p}}^{2e+1}$, a neighborhood of 1. As open subgroups of compact groups have finite index, we conclude that $R_\mathfrak{p}^{\times 2}$ has finite index in $R_\mathfrak{p}^\times$. To see that $[K_\mathfrak{p}^\times : K_\mathfrak{p}^{\times 2}]$ is finite, we now just need to observe that squares of $K_\mathfrak{p}^\times$ are of the form $s \cdot \pi^{2k}$ where $s \in R_\mathfrak{p}^{\times 2}$.

Let $s_1, \ldots, s_n \in K$ be a set of representatives for $K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2}$ and define $S_j := s_j \cdot K^{\times 2} \cdot (1 + \mathfrak{p}^{2e+1}\mathcal{O}_\mathfrak{p})$. For $x \in S_i$, $y \in S_j$ we have $(x, y)_\mathfrak{p} = (s_i, s_j)_\mathfrak{p}$.

Now we define

$$S_\mathfrak{p} := \bigcup_{i,j:(s_i,s_j)_\mathfrak{p}=-1} S_i \times S_j.$$

Then $(x, y)_\mathfrak{p} = -1$ if and only if $(x, y) \in S_\mathfrak{p}$. Each set S_i is diophantine over K, and the finite Cartesian product of diophantine sets is again diophantine. Thus $S_\mathfrak{p}$ is diophantine over K. $\square$

Now we prove Theorem 1.3 for a global field K with $\mathrm{char}(K) \neq 2$.

Proof of Theorem 1.3. By the Hasse norm principle, x is not a norm in $K(\sqrt{y})$ if and only if $(x,y)_{\mathfrak{p}} = -1$ for some finite or real infinite prime $\mathfrak{p}$ of K. For $\sigma \neq (1,1) \in \mathrm{Gal}(K(\sqrt{a},\sqrt{b})/K)$, let $s_\sigma = a$ if $\sigma = (-1,\pm 1)$ and $s_\sigma = b$ if $\sigma = (1,-1)$. We claim that $(x,y)_{\mathfrak{p}} = -1$ if and only if one of the following conditions holds:

- $\exists\, \mathfrak{p}|\mathfrak{m}$ such that $(x,y)_{\mathfrak{p}} = -1$,
- $\bigvee_{\sigma\neq(1,1)} \exists p \in \Phi_\sigma$ such that

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

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

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

This will imply the theorem, because we have already shown that the above conditions define diophantine sets. We will first prove the forward implication. If x is not a norm in $K(\sqrt{y})$, there is a prime $\mathfrak{p}$ of K such that $(x,y)_{\mathfrak{p}} = -1$. If $\mathfrak{p}|\mathfrak{m}$ we are done; recall that $\mathfrak{m}$ contains all real infinite primes if K is a number field.

Now assume $\mathfrak{p} \in I_{\mathfrak{m}}$ and that $\psi_{L/K}(\mathfrak{p}) = \sigma \neq (1,1)$. We claim that the second condition holds. We can find $p \in \Phi_\sigma$ such that $\mathbb{P}^\sigma(p) = \{\mathfrak{p}\}$ as before. Corollary 3.11 and the definition of R_p^σ imply $R_p^\sigma = \mathcal{O}_{\mathfrak{p}}$ and $J(R_p^\sigma) = \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. By setting $p := p$ and $s := s_\sigma$, Lemma 4.4 implies that the second condition holds because $v_{\mathfrak{p}}(p)$ is odd and s_σ, by construction, is a $\mathfrak{p}$-adic unit which is not a square modulo $\mathfrak{p}$. For example, if $\sigma = (1,-1)$, then $s_\sigma = b$. The fractional ideal (b) is coprime to $\mathfrak{m}$, and $\psi_{L/K}(\mathfrak{p}) = (1,-1)$ implies that b is not a square mod $\mathfrak{p}$.

Now assume $\mathfrak{p} \in I_{\mathfrak{m}}$ with $\psi_{L/K}(\mathfrak{p}) = (1,1)$. We claim that the third condition holds in this case. We will first show that we can find $(p,q) \in \Psi_K$ with the stated properties if K is a global function field. By Lemma 3.17, there is a $(p,q) \in \Psi_K$ with $\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}\}$. In fact, q can be chosen so that $v_{\mathfrak{p}}(q) = 0$, q is not a square modulo $\mathfrak{p}$, and such that $\mathbb{P}(q) = \{\mathfrak{q}, \mathfrak{p}_0\}$. Here, $\mathfrak{q}$ and $\mathfrak{p}_0$ are primes with $\psi_{L/K}(\mathfrak{q}) = (-1,-1)$ and $\psi_{L/K}(\mathfrak{p}_0) = (1,1)$. Then $q \in \mathcal{O}_{\mathfrak{p}}^\times = (R_{p,q}^{(1,1)})^\times$ by Definition 3.12. By the formula for the Hilbert symbol, $v_{\mathfrak{p}}(ap)$ is odd, and since $\mathfrak{p}$ cannot divide (a), we conclude $v_{\mathfrak{p}}(p)$ is

odd. As $R_{p,q}^{(1,1)} = \mathcal{O}_\mathfrak{p}$ and $J(R_{p,q}^{(1,1)}) = \mathfrak{p}\mathcal{O}_\mathfrak{p}$, we can apply Lemma 4.4 with $s := q$.

If K is a number field, then by Lemma 3.25 in [12], we can find $(p, q) \in \Psi_K$ such that (q) is a prime ideal with $\psi_{L/K}((q)) = (-1, -1)$, q is not a square in $K_\mathfrak{p}$, and such that $\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}\}$. A similar argument as above shows that the second condition holds.

Now we will prove that if one of the three conditions above holds, then for some prime $\mathfrak{p}$, $(x, y)_\mathfrak{p} = -1$. Suppose the second condition holds for some $\sigma \neq (1, 1)$. If K is a global function field, $\mathbb{P}^\sigma(p) \neq \emptyset$ by Lemma 3.14 (2), so $\mathbb{P}^\sigma(p)$ contains some prime $\mathfrak{p}$. Assume, without loss of generality, that

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

Since $v_\mathfrak{p}(p)$ is odd, $v_\mathfrak{p}(x)$ is odd, too. Also, either y or $-xy$ is, possibly after multiplying by a square of $K^\times$, a non-square in $K_\mathfrak{p}$ since $\psi_{L/K}(\mathfrak{p}) = \sigma$ implies s_σ is a non-square in $K_\mathfrak{p}$. By Lemma 4.4, this implies that $(x, y)_\mathfrak{p} = -1$. If K is a number field, an application of Lemma 3.22 (b) in [12] and a similar argument show that $(x, y)_\mathfrak{p} = -1$ for a finite prime $\mathfrak{p}$ of K.

We now prove that the third condition implies that $(x, y)_\mathfrak{p} = -1$ for some $\mathfrak{p}$ with $\psi_{L/K}(\mathfrak{p}) = (1, 1)$. The argument is similar to the one in the second condition. If K is a global function field, $(p, q) \in \Psi_K$ implies that $\Delta_{ap,q} \cap \Delta_{bp,q} \neq \emptyset$ and contains some prime $\mathfrak{p}$ by Lemma 3.17 part (2). Then because $q \in (R_{p,q})^\times$ and $(ap, q)_\mathfrak{p} = (bp, q)_\mathfrak{p} = -1$, q is not a square mod $\mathfrak{p}$ and $v_\mathfrak{p}(p)$ must be odd. Again by Lemma 4.4, this implies that $(x, y)_\mathfrak{p} = -1$. If K is a number field, the same argument, along with Lemma 3.25 (b) from [12], proves the claim. □

Acknowledgments

The first author was partially supported by National Science Foundation grant DMS-1056703. The second author was partially supported by National Science Foundation grants DMS-1056703 and CNS-1617802.

References

[1] E. Artin and J. Tate, Class Field Theory, W. A. Benjamin, Inc., New York-Amsterdam (1968).

[2] J.-L. Colliot-Thélène and J. Van Geel, *Le complémentaire des puissances n-ièmes dans un corps de nombres est un ensemble diophantien*, Compos. Math. **151** (2015), no. 10, 1965–1980.

[3] M. Davis, H. Putnam, and J. Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436.

[4] J. Denef, *The Diophantine problem for polynomial rings of positive characteristic*, in: Logic Colloquium '78 (Mons, 1978), Vol. 97 of Stud. Logic Foundations Math., 131–145, North-Holland, Amsterdam-New York (1979).

[5] J. Denef, *Diophantine sets over algebraic integer rings. II*, Trans. Amer. Math. Soc. **257** (1980), no. 1, 227–236.

[6] P. Dittmann, *Irreducibility of polynomials over number fields is diophantine*, `arXiv:1601.07829`, (2016).

[7] K. Eisenträger, *Hilbert's Tenth Problem for algebraic function fields of characteristic* 2, Pacific J. Math. **210** (2003), no. 2, 261–281.

[8] J. Koenigsmann, *Defining* $\mathbb{Z}$ *in* $\mathbb{Q}$, Ann. of Math. (2) **183** (2016), no. 1, 73–93.

[9] Y. V. Matiyasevich, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282.

[10] B. Mazur, *The topology of rational points*, Experiment. Math. **1** (1992), no. 1, 35–45.

[11] J. Milne, Arithmetic Duality Theorems, BookSurge, LLC, second edition (2006). `ISBN 1-4196-4274-X`.

[12] J. Park, *A universal first-order formula defining the ring of integers in a number field*, Math. Res. Lett. **20** (2013), no. 5, 961–980.

[13] T. Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*, Invent. Math. **103** (1991), no. 1, 1–8.

[14] B. Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), no. 3, 675–682.

[15] B. Poonen, *The set of nonsquares in a number field is Diophantine*, Math. Res. Lett. **16** (2009), no. 1, 165–170.

[16] J. Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114.

[17] M. Rosen, *The Hilbert class field in function fields*, Exposition. Math. **5** (1987), no. 4, 365–378.

[18] M. Rosen, Number Theory in Function Fields, Vol. 210 of Graduate Texts in Mathematics, Springer-Verlag, New York (2002). ISBN 0-387-95335-3.

[19] R. S. Rumely, *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. **262** (1980), no. 1, 195–217.

[20] O. Schilling and H. Hasse, *Die Normen aus einer normalen Divisionsalgebra über einem algebraischen Zahlkörper*, J. Reine Angew. Math. **174** (1936), 248–252.

[21] J. P. Serre, Local Fields, Springer-Verlag New York, Inc, New York (1979).

[22] A. Shlapentokh, *Diophantine classes of holomorphy rings of global fields*, J. Algebra **169** (1994), no. 1, 139–175.

[23] A. Shlapentokh, *Diophantine undecidability over algebraic function fields over finite fields of constants*, J. Number Theory **58** (1996), no. 2, 317–342.

[24] A. Shlapentokh, *On definitions of polynomials over function fields of positive characteristic*, arXiv:1502.02714, (2015).

[25] J. T. Tate, *Global class field theory*, in: Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 162–203, Thompson, Washington, D.C. (1967).

[26] C. R. Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proc. Amer. Math. Soc. **120** (1994), no. 1, 249–253.

Dept. of Mathematics, The Pennsylvania State University
University, Park, PA 16802, USA
E-mail address: eisentra@math.psu.edu
E-mail address: txm950@psu.edu

Received September 30, 2016