Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Number Theory 114 (2005) 170–181
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Integrality at a prime for global fields and the perfect closure of global fields of characteristic $p > 2$

Kirsten Eisenträger[1]

School of Mathematics, Institute for Advanced Study, Einstein Drive, Princeton, NJ 08540, USA

Received 11 October 2003; revised 22 January 2005
Available online 18 July 2005
Communicated by D. Goss

Abstract

Let k be a global field and $\mathfrak{p}$ any nonarchimedean prime of k. We give a new and uniform proof of the well known fact that the set of all elements of k which are integral at $\mathfrak{p}$ is diophantine over k. Let k^{perf} be the perfect closure of a global field of characteristic $p > 2$. We also prove that the set of all elements of k^{perf} which are integral at some prime $\mathfrak{q}$ of k^{perf} is diophantine over k^{perf}, and this is the first such result for a field which is not finitely generated over its constant field. This is related to Hilbert's Tenth Problem because for global fields k of positive characteristic, giving a diophantine definition of the set of elements that are integral at a prime is one of two steps needed to prove that Hilbert's Tenth Problem for k is undecidable.

Keywords: Hilbert's Tenth Problem; Undecidability; Diophantine definition; Brauer group

1. Introduction

Hilbert's Tenth Problem in its original form was to find an algorithm to decide, given a polynomial equation $f(x_1, \ldots, x_n) = 0$ with coefficients in the ring $\mathbb{Z}$ of integers, whether it has a solution with $x_1, \ldots, x_n \in \mathbb{Z}$. Matijasevič [10], building on earlier

E-mail address: eisentra@ias.edu.
[1] The research for this paper was done while the author was at the University of California, Berkeley.

0022-314X/$ - see front matter
doi:10.1016/j.jnt.2005.02.008

work by Davis et al. [2], proved that no such algorithm exists, i.e. Hilbert's Tenth Problem is undecidable.

Since then, analogues of this problem have been studied by asking the same question for polynomial equations with coefficients and solutions in other commutative rings R. We refer to this as Hilbert's Tenth Problem over R. Perhaps the most important unsolved question in this area is Hilbert's Tenth Problem over the field of rational numbers. Diophantine undecidability has been proved for several function fields of characteristic 0: In [3], Denef proves the undecidability of Hilbert's Tenth Problem for rational function fields over formally real fields. In 1992, Kim and Roush [8] showed that the problem is undecidable for the purely transcendental function field $\mathbb{C}(t_1, t_2)$, and in [5] this is generalized to finite extensions of $\mathbb{C}(t_1, \ldots, t_n)$ for $n \geqslant 2$.

Hilbert's Tenth Problem for the function field k of a curve over a finite field is also undecidable. This was proved by Pheidas for $k = \mathbb{F}_q(t)$ with q odd, and by Videla [21] for $\mathbb{F}_q(t)$ with q even. In [19,20], Shlapentokh generalized Pheidas' result to finite extensions of $\mathbb{F}_q(t)$ with q odd and to certain function fields over possibly infinite constant fields of odd characteristic, and the remaining cases in characteristic 2 are treated in [4]. Before we can state the results of this paper we need the following definition.

Definition 1.1. 1. If R is a commutative ring, a *diophantine equation over* R is an equation $P(x_1, \ldots, x_n) = 0$ where P is a polynomial in the variables $x_1, \ldots, x_n$ with coefficients in R.

2. A subset S of R^k is *diophantine* if there is a polynomial $P(x_1, \ldots, x_k, y_1, \ldots, y_m) \in R[x_1, \ldots, x_k, y_1, \ldots, y_m]$ such that

$$S = \{(x_1, \ldots, x_k) \in R^k : \exists\, y_1, \ldots, y_m \in R,\ (P(x_1, \ldots, x_k, y_1, \ldots, y_m) = 0)\}.$$

When R is not a finitely generated algebra over $\mathbb{Z}$, we restrict our attention to diophantine equations whose coefficients are in a finitely generated algebra over $\mathbb{Z}$.

For global fields of positive characteristic, Proposition 1.2 below [19, p. 319] is used to prove undecidability of Hilbert's Tenth Problem. For the purposes of this paper, global fields are algebraic number fields or finite extensions of the rational function fields $\mathbb{F}_q(t)$. A prime of a global field k is an equivalence class of nontrivial absolute values of k. A nonarchimedean prime is an equivalence class of nontrivial nonarchimedean absolute values of k. For a nonarchimedean prime $\mathfrak{p}$ of a global field k we denote by $\operatorname{ord}_{\mathfrak{p}}$ the associated normalized additive discrete valuation $\operatorname{ord}_{\mathfrak{p}} : k^* \twoheadrightarrow \mathbb{Z}$.

Proposition 1.2. *Let k be a global field of positive characteristic, let p be a rational prime, and let $\mathfrak{p}$ be a prime of k. Assume that the sets $p(k) := \{(x, w) \in k^2 : \exists s \in \mathbb{N}, w = x^{p^s}\}$ and $\operatorname{INT}(\mathfrak{p}) := \{x \in k : \operatorname{ord}_{\mathfrak{p}} x \geqslant 0\}$ are diophantine. Then Hilbert's Tenth Problem for k is undecidable.*

So for global fields of positive characteristic, a diophantine definition of the set of elements which are integral at some prime $\mathfrak{p}$ is one of two main steps used to prove undecidability of Hilbert's Tenth Problem.

In this paper we will prove two results. We give a different and more uniform proof of the known fact that for any global field k and any nonarchimedean prime $\mathfrak{p}$ of k the set of elements of k which are integral at $\mathfrak{p}$ is diophantine. For number fields the result was already implicit in the work of Robinson [14,15], and explicitly written down in [7, Proposition 3.1]. Their proof relies on the Hasse principle for quadratic forms. For global function fields the result was proved in [18]. There is also another approach by Rumely [16] that uses the Hasse norm principle. Our approach uses the Brauer group of k. We also prove the following new result:

Theorem 1.3. *Let k be a global field of characteristic $p > 2$, and let k^{perf} be the perfect closure of k. Let $\mathfrak{p}$ be a prime of k^{perf}. The set $\{x \in k^{\mathrm{perf}} : \mathrm{ord}_{\mathfrak{p}}\, x \geqslant 0\}$ is diophantine over k^{perf}.*

The perfect closure of a field k of characteristic p is obtained by adjoining p^nth roots of all elements of k for all $n \geqslant 1$. A prime $\mathfrak{p}$ of k^{perf} is an equivalence class of nontrivial absolute values of k^{perf}. The associated additive valuation $\mathrm{ord}_{\mathfrak{p}}$ is no longer discrete since every element of k^{perf} is a pth power.

The perfect closure of $\mathbb{F}_q(t)$ is $K := \mathbb{F}_q(t, t^{1/p}, t^{1/p^2}, t^{1/p^3}, \ldots)$. We will first prove Theorem 1.3 for K. Let k be any global field of characteristic $p > 0$. Then k is a finite extension of $\mathbb{F}_q(t)$ for some $q = p^n$. We will show in Section 4 that the perfect closure k^{perf} of k is also obtained by adjoining p^nth roots of t, and that the proof for K generalizes to k^{perf}. These perfect closures are not finitely generated over their constant fields. This distinguishes them from all the function fields mentioned above.

2. Background

In this section, we will state some of the definitions and theorem about division algebras and Brauer groups that are needed in the next two sections.

Definition 2.1 (*Quaternion algebras*). Let F be a field of characteristic $\neq 2$. For $a, b \in F^*$, let $H(a, b)$ be the F-algebra with basis $1, i, j, k$ (as an F-vector space) and with multiplication rules

$$i^2 = a,\ j^2 = b, ij = k = -ji.$$

Then $H(a, b)$ is an F-algebra which is called a *quaternion algebra* over F.

One can show that $H(a, b)$ is either a division algebra or isomorphic to $M_2(F)$. (Here $M_2(F)$ is the algebra of 2×2 matrices.)

Definition 2.2. 1. An algebra A is said to be *central simple* over a field F if A is a simple algebra having F as its center.

2. The matrix algebra $M_n(F)$ is called a *split* central simple algebra over F. If A is a finite-dimensional central simple algebra over F, then an extension field E of F is called a splitting field for A if $A \otimes_F E \cong M_n(E)$ for some n.

Proposition 2.3. *Let F be a field of characteristic $\neq 2$. Every 4-dimensional central simple algebra over F is isomorphic to $H(a, b)$ for some $a, b \in F^*$.*

Proof. This is Proposition 1 in [1, p. 128]. □

In characteristic 2 something similar holds:

Proposition 2.4. *Let F be a field of characteristic 2. Let D be a central division algebra over F such that for each $x \in D$, we have $[F(x) : F] \leqslant 2$. Then D admits a basis $(1, u, v, w)$ over F such that*

$$u^2 = a, v^2 = v + b, uv = w, vu = w + u, w^2 = ab, vw = bu,$$

$$wv = bu + w, wu = a + av, uw = av,$$

where $a, b \in F$. We will denote this algebra again by $H(a, b)$.

Proof. This is Exercise 4 in [1, p. 130]. □

Definition 2.5. Let k be a global field. Let $\mathfrak{p}$ be a prime of k, and let $k_{\mathfrak{p}}$ be the completion of k at $\mathfrak{p}$. A quaternion algebra A over k is said to *split* at $\mathfrak{p}$ if

$$A \otimes_k k_{\mathfrak{p}} \cong M_2(k_{\mathfrak{p}}) \quad \text{as} \quad k_{\mathfrak{p}}\text{-algebras.}$$

Otherwise A is ramified at $\mathfrak{p}$.

Notation: For any field F, let F^{sep} denote a separable closure of F.
We have the following proposition.

Proposition 2.6. *Let A be a finite-dimensional central simple algebra over a field F. There exists an F^{sep}-algebra isomorphism $\iota : A \otimes_F F^{\mathrm{sep}} \to M_r(F^{\mathrm{sep}})$. The characteristic polynomial $P_a(x) \in F^{\mathrm{sep}}[x]$ of $\iota(a \otimes 1)$ is independent of the choice of ι. Moreover, $P_a(x) \in F[x]$.*

Proof. This is proved in [13, pp. 113–114]. □

Definition 2.7. Let A be as above. The *reduced trace* $\mathrm{tr}(\alpha)$ of $\alpha \in A$ is defined to be the trace of $\iota(\alpha \otimes 1)$, for any choice of ι as above. Similarly, the *reduced norm* $\mathrm{nr}(\alpha)$ is defined to be the determinant.

We can compute the following:

Lemma 2.8. *Let $H(a, b)$ be a quaternion algebra over a field F of characteristic $\neq 2$. The reduced trace* $\operatorname{tr}(x_1 + x_2 i + x_3 j + x_4 k)$ *equals* $2x_1$, *and the reduced norm* $\operatorname{nr}(x_1 + x_2 i + x_3 j + x_4 k)$ *equals* $x_1^2 - ax_2^2 - bx_3^2 + abx_4^2$ *for any* $x_1, \ldots, x_4 \in F$.

Lemma 2.9. *Let D be a* 4*-dimensional division algebra over a field F of characteristic* 2, *so that $D = H(a, b)$ as in Proposition* 2.4 *for some $a, b \in F^*$. Let $(1, u, v, uv)$ be a basis of D over F as in Proposition* 2.4. *For an element $x_1 + x_2 u + x_3 v + x_4 uv$ we have* $\operatorname{tr}(x_1 + x_2 u + x_3 v + x_4 uv) = x_3$ *and* $\operatorname{nr}(x_1 + x_2 u + x_3 v + x_4 uv) = x_1^2 + x_1 x_3 + bx_3^2 + a(x_2^2 + x_2 x_4 + bx_4^2)$.

Proof. This follows from Proposition 10 in [1, p. 144] and from Exercise 6 in [1, p. 147]. □

Definition 2.10 (*Brauer group*). Let A and B be finite-dimensional central simple algebras over a field F. We say that A and B are similar, $A \sim B$, if $A \otimes_F M_n(F) \cong B \otimes_F M_m(F)$ for some m and n. Define the *Brauer group* of F, $\operatorname{Br}(F)$, to be the set of similarity classes of central simple algebras over F, and write $[A]$ for the similarity class of A. For classes $[A]$ and $[B]$, define

$$[A][B] := [A \otimes_F B].$$

This is well defined and makes $\operatorname{Br}(F)$ into an abelian group.

Each similarity class of $\operatorname{Br}(F)$ is represented by a central division algebra, and two central division algebras representing the same similarity class are isomorphic [11, p. 100].

Theorem 2.11. *Let K be a nonarchimedean local field.*

(1) *The Brauer group of K is isomorphic to $\mathbb{Q}/\mathbb{Z}$.*
(2) *Let D/K be a division algebra of degree n^2. The order of $[D]$ in* $\operatorname{Br}(K)$ *is n.*

Proof.

(1) This is Theorem 9.22 in [6].
(2) This is Theorem 9.23 in [6]. □

Theorem 2.12. *Let k be a global field. There is an exact sequence*

$$0 \to \operatorname{Br}(k) \to \bigoplus_{v \in M_k} \operatorname{Br}(k_v) \to \mathbb{Q}/\mathbb{Z} \to 0,$$

where M_k denotes the set of nonequivalent nontrivial absolute values of k.

Proof. This is Remark (ii) in [13, p. 277]. □

Proposition 2.13. *Let K be a nonarchimedean local field, and let D be a finite-dimensional central division algebra over K. The valuation on K has a unique extension to D.*

Proof. This is proved in [17, p. 182]. □

3. Integrality at a prime for global fields

In this section we will prove the following

Theorem 3.1. *Let k be a global field. Let $\mathfrak{p}$ be a nonarchimedean prime of k. The set $\{x \in k : \operatorname{ord}_{\mathfrak{p}} x \geqslant 0\}$ is diophantine over k.*

Proof. We will first prove this when the characteristic of k is not 2 and then say how the proof has to be modified in characteristic 2.

For any nonarchimedean prime $\mathfrak{p}$ of k let $R_{\mathfrak{p}} := \{x \in k : \operatorname{ord}_{\mathfrak{p}} x \geqslant 0\}$.

Claim. *Given two distinct nonarchimedean primes $\mathfrak{p}$ and $\mathfrak{q}$ of k there exists a subset $S \subseteq R_{\mathfrak{p}} \cap R_{\mathfrak{q}}$ containing a subgroup G of finite index in $R_{\mathfrak{p}} \cap R_{\mathfrak{q}}$, such that S is diophantine over k.*

Proof of Claim. By the approximation theorem we may choose $p, q \in k$ such that $\operatorname{ord}_{\mathfrak{p}} p = 1$, $\operatorname{ord}_{\mathfrak{q}} p = 0$, $\operatorname{ord}_{\mathfrak{p}} q = 0$, and $\operatorname{ord}_{\mathfrak{q}} q = 1$. By Theorem 2.11 and Theorem 2.12 we can find a central division algebra H that is ramified exactly at $\mathfrak{p}$ and $\mathfrak{q}$ and which has degree 4 over k. By Proposition 2.3, $H \cong H(a, b)$ for some $a, b \in k^*$. Let $\mathcal{O}_{\mathfrak{p}}$ be the valuation ring of $k_{\mathfrak{p}}$, where $k_{\mathfrak{p}}$ is the completion of k at the prime $\mathfrak{p}$. Let $A_{\mathfrak{p}}$ be the valuation ring of $H_{\mathfrak{p}} := H \otimes k_{\mathfrak{p}}$. Then $A_{\mathfrak{p}}$ is a free $\mathcal{O}_{\mathfrak{p}}$-module of rank 4. Since $H(a, b) \cong H(ax^2, by^2)$ for $x, y \in k^*$, we can choose $i, j \in H$ that are integral at $\mathfrak{p}$ and $\mathfrak{q}$, and then

$$p^r A_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}} i + \mathcal{O}_{\mathfrak{p}} j + \mathcal{O}_{\mathfrak{p}} ij, \quad \text{and}$$

$$q^r A_{\mathfrak{q}} \subseteq \mathcal{O}_{\mathfrak{q}} + \mathcal{O}_{\mathfrak{q}} i + \mathcal{O}_{\mathfrak{q}} j + \mathcal{O}_{\mathfrak{q}} ij \quad \text{for some} \quad r \geqslant 0.$$

Now let

$$T := \{x_1 \in k : (\exists x_2, x_3, x_4 \in k) : (x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = pq)\}.$$

Then $S = (pq)^r T$ has the desired property. Suppose $x_1 \in T$. Then there exists $\alpha = x_1 + x_2 i + x_3 j + x_4 ij \in H$ whose reduced norm equals pq. Since $pq \in \mathcal{O}_{\mathfrak{p}}$ it follows that $\alpha \in A_{\mathfrak{p}}$. Then $p^r x_1 \in \mathcal{O}_{\mathfrak{p}}$. Similarly, we can show that $q^r x_1 \in \mathcal{O}_{\mathfrak{q}}$, so $(pq)^r x_1 \in \mathcal{O}_{\mathfrak{p}} \cap \mathcal{O}_{\mathfrak{q}}$. Hence $S \subseteq \mathcal{O}_{\mathfrak{p}} \cap \mathcal{O}_{\mathfrak{q}} \cap k = R_{\mathfrak{p}} \cap R_{\mathfrak{q}}$.

Conversely assume that $x_1 \in k$ and that $x_1 \in pR_{\mathfrak{p}} \cap qR_{\mathfrak{q}}$. Then the equation

$$X^2 - 2x_1X + pq = 0$$

is Eisenstein at $\mathfrak{p}$ and $\mathfrak{q}$, so a root β generates a quadratic field extension, and β also generates a quadratic extension $k_{\mathfrak{p}}(\beta)$ of $k_{\mathfrak{p}}$ and a quadratic extension $k_{\mathfrak{q}}(\beta)$ of $k_{\mathfrak{q}}$. By Milne [11, Remark 4.4, p. 110] any quadratic extension field of the local field $k_{\mathfrak{p}}$ is a splitting field for H over $k_{\mathfrak{p}}$. Hence $k_{\mathfrak{p}}(\beta)$ splits H locally, and by Theorem 2.12 it follows that $k(\beta)$ splits H. Since $k(\beta)$ splits H, $k(\beta)$ can be embedded into H [11, Corollary 3.7, p. 103], and we can apply Proposition 10 in [1, p. 144] to conclude that the image of β in D is $c = c_1 + c_2i + c_3ij + c_4ij$ with reduced trace $\mathrm{tr}(c) = 2x_1$ and reduced norm $\mathrm{nr}(c) = pq$. Hence $2c_1 = 2x_1$, so $c_1 = x_1$ and $x_1 \in T$. Then $(pq)^r x_1 \in S$. Thus $S \subseteq R_{\mathfrak{p}} \cap R_{\mathfrak{q}}$ and S contains the subgroup $G := p^{r+1}R_{\mathfrak{p}} \cap q^{r+1}R_{\mathfrak{q}}$ which has index $(pq)^{r+1}$ in $R_{\mathfrak{p}} \cap R_{\mathfrak{q}}$. This proves the claim.

Let $s_1, \dots, s_l$ be coset representatives for G in $R_{\mathfrak{p}} \cap R_{\mathfrak{q}}$. Then for $x \in k$,

$$x \in R_{\mathfrak{p}} \cap R_{\mathfrak{q}} \Leftrightarrow (\exists s \in S)(x = s + s_1) \vee \cdots \vee (x = s + s_l).$$

This proves that $R_{\mathfrak{p}} \cap R_{\mathfrak{q}}$ is diophantine over k.

We can repeat the same argument with $\mathfrak{p}$ and some other finite prime $\ell \neq \mathfrak{q}$ and conclude that $R_{\mathfrak{p}} \cap R_{\ell}$ is diophantine over k. By weak approximation we have

$$R_{\mathfrak{p}} = (R_{\mathfrak{p}} \cap R_{\mathfrak{q}}) + (R_{\mathfrak{p}} \cap R_{\ell}).$$

This proves the theorem when the characteristic of k is not 2.

Characteristic 2 case: When k has Characteristic 2, we can still find a 4-dimensional central division algebra ramified exactly at $\mathfrak{p}$ and $\mathfrak{q}$. We only have to change the definition of T to

$$T := \{x_3 \in k : (\exists x_1, x_2, x_4 \in k) : \mathrm{nr}(x_1 + x_2u + x_3v + x_4uv) = pq)\}.$$

Then we can still show $T \subseteq A_{\mathfrak{p}}$. For the other direction, given $x_3 \in k$ with $x_3 \in pR_{\mathfrak{p}} \cap qR_{\mathfrak{q}}$, we look at the equation

$$X^2 - x_3X + pq = 0.$$

Then the proof proceeds exactly as before. $\square$

4. Integrality at a prime for the perfect closure of global fields of characteristic $p > 2$

Notation: In the following $\mathbb{F}_q$ will be the finite field with $q = p^m$ elements of characteristic $p > 2$, $\mathbb{F}_q(t)$ will denote the field of rational functions over $\mathbb{F}_q$ and K will denote the perfect closure of $\mathbb{F}_q(t)$, i.e. $K = \mathbb{F}_q(t, t^{1/p}, t^{1/p^2}, t^{1/p^3}, \ldots)$. For simplicity of notation we will first prove Theorem 1.3 for the rational function field $\mathbb{F}_q(t)$, and then say how the proof has to be modified for finite extensions k of $\mathbb{F}_q(t)$.

Theorem 4.1. *Let K be as above. Let $\mathfrak{p}$ be a prime of K. The set $\{x \in K : \operatorname{ord}_{\mathfrak{p}} x \geqslant 0\}$ is diophantine over K.*

Proof. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be two primes of K and let $\operatorname{ord}_{\mathfrak{p}_1}$ and $\operatorname{ord}_{\mathfrak{p}_2}$ be the associated additive valuations.

We will show that the set $\{x \in K : \operatorname{ord}_{\mathfrak{p}_1} x \geqslant 0\}$ is diophantine over K.

The restrictions of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ to $\mathbb{F}_q(t)$ are primes of $\mathbb{F}_q(t)$. For simplicity of notation we will denote these restrictions again by $\mathfrak{p}_1$ and $\mathfrak{p}_2$. From Theorems 2.12 and 2.11 it follows that we can find a central division algebra $D/\mathbb{F}_q(t)$ with $[D : \mathbb{F}_q(t)] = 4$ which is ramified exactly at the primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$.

$$\text{Let } \mathcal{O}_D := \{z \in D : \operatorname{ord}_{\mathfrak{p}_1}(z) \geqslant 0 \text{ and } \operatorname{ord}_{\mathfrak{p}_2}(z) \geqslant 0\},$$

$$\text{and } \mathcal{O} := \{z \in \mathbb{F}_q(t) : \operatorname{ord}_{\mathfrak{p}_1}(z) \geqslant 0 \text{ and } \operatorname{ord}_{\mathfrak{p}_2}(z) \geqslant 0\}.$$

The ring $\mathcal{O}$ is an intersection of discrete valuation rings, so $\mathcal{O}$ is a Dedekind domain with finitely many primes. By Jacobson [6, Exercise 15, p. 625] $\mathcal{O}$ is a PID. The ring $\mathcal{O}_D$ is a finitely generated torsion-free $\mathcal{O}$-module. Since $\mathcal{O}$ is a PID, it follows that $\mathcal{O}_D$ is a free $\mathcal{O}$-module of rank 4.

Let $\operatorname{tr} : \mathcal{O}_D \to \mathcal{O}$ be the reduced trace. Then $\operatorname{tr}(1) = 2$, because $[D : \mathbb{F}_q(t)] = 4$. Since 2 is a unit in $\mathcal{O}$, the reduced trace is surjective. Since $\mathcal{O}_D/\mathcal{O}$ is free, the kernel of the reduced trace is free of rank 3, so let a_2, a_3, a_4 be a basis for the kernel. The image of the trace is generated by $\operatorname{tr}(1)$, so $a_1 = 1, a_2, a_3, a_4$ are a basis of $\mathcal{O}_D/\mathcal{O}$. Then $a_1, \ldots, a_4$ are also a basis for $\mathcal{O}_D \otimes_{\mathcal{O}} \mathbb{F}_q(t) = D$ over $\mathbb{F}_q(t)$. Let

$$S := \{x_1 \in \mathbb{F}_q(t) : (\exists\, x_2, x_3, x_4 \in \mathbb{F}_q(t)) : (\operatorname{nr}(x_1a_1 + x_2a_2 + x_3a_3 + x_4a_4) = 1)\}.$$

Then $S \subseteq \mathcal{O}$.

Let $D^{\text{perf}} := D \otimes_{\mathbb{F}_q(t)} K$. Then D^{perf} is still ramified at $\mathfrak{p}_1$ and $\mathfrak{p}_2$, because only elements of order p^{ℓ} in $\operatorname{Br}(\mathbb{F}_q(t))$ get killed in the perfection, D has order 2 in $\operatorname{Br}(\mathbb{F}_q(t))$, and $p \geqslant 3$.

$$\text{Let } \mathcal{O}^{\text{perf}} := \{z \in K : \operatorname{ord}_{\mathfrak{p}_1}(z) \geqslant 0 \text{ and } \operatorname{ord}_{\mathfrak{p}_2}(z) \geqslant 0\},$$

$$\text{and } \mathcal{O}_{D^{\text{perf}}} := \{z \in D^{\text{perf}} : \operatorname{ord}_{\mathfrak{p}_1}(z) \geqslant 0 \text{ and } \operatorname{ord}_{\mathfrak{p}_2}(z) \geqslant 0\}.$$

We will prove that $\mathcal{O}^{\text{perf}}$ is diophantine over K. To do this let

$$T := \{x_1 \in K : (\exists\, x_2, x_3, x_4 \in K) : (\operatorname{nr}(x_1a_1 + x_2a_2 + x_3a_3 + x_4a_4) = 1)\}.$$

We will prove that $\mathcal{O}^{\text{perf}}$ is diophantine by showing that there exist finitely many elements $\alpha_1, \dots, \alpha_r \in K$ such that

$$\mathcal{O}^{\text{perf}} = (T + \alpha_1) \cup (T + \alpha_2) \cup \cdots \cup (T + \alpha_r).$$

First we need the following claim:

Claim. *$\mathcal{O}_{D^{\text{perf}}}$ is a free $\mathcal{O}^{\text{perf}}$-module of rank 4 with basis $a_1 \otimes 1, \dots, a_4 \otimes 1$. Also $a_1 \otimes 1, \dots, a_4 \otimes 1$ are a basis for D^{perf} over K.*

Proof of Claim. For each $i \in \mathbb{N}$ let

$$D_i := D \otimes_{\mathbb{F}_q(t)} \mathbb{F}_q(t^{1/p^i}),$$

$$\mathcal{O}_i := \{z \in \mathbb{F}_q(t^{1/p^i}) : \operatorname{ord}_{\mathfrak{p}_1}(z) \geqslant 0 \text{ and } \operatorname{ord}_{\mathfrak{p}_2}(z) \geqslant 0\}, \quad \text{and}$$

$$\mathcal{O}_{D_i} := \{z \in \mathbb{F}_q(t^{1/p^i}) : \operatorname{ord}_{\mathfrak{p}_1}(z) \geqslant 0 \text{ and } \operatorname{ord}_{\mathfrak{p}_2}(z) \geqslant 0\} = \mathcal{O}_D \otimes_{\mathcal{O}} \mathcal{O}_i.$$

Then $\mathcal{O}_{D_i}$ is a free $\mathcal{O}_i$-module of rank 4 with basis $a_1 \otimes 1, \dots, a_4 \otimes 1$ by Lang [9, Proposition 4.1, p. 623].

We have that $\mathcal{O}_{D^{\text{perf}}} = \mathcal{O}_D \otimes_{\mathcal{O}} \mathcal{O}^{\text{perf}}$, and hence the same proposition implies that $\mathcal{O}_{D^{\text{perf}}}$ is free over $\mathcal{O}^{\text{perf}}$ with basis $a_1 \otimes 1, \dots, a_4 \otimes 1$. These elements are still linearly independent over the quotient field of $\mathcal{O}^{\text{perf}}$, K, so they also form a basis for D^{perf} over K. This proves the claim.

By definition of T, we have that $T \subseteq \mathcal{O}^{\text{perf}}$. Let k_1 and k_2 be the residue fields of $\mathfrak{p}_1$ and $\mathfrak{p}_2$, respectively. The fields k_1 and k_2 are finite extensions of $\mathbb{F}_q$. For $x_1 \in \mathcal{O}^{\text{perf}}$ we have

$$x_1^2 - 1 \bmod \mathfrak{p}_i \notin (k_i)^2 \text{ for } i = 1, 2$$

$$\Rightarrow\ x_1^2 - 1 \notin (K_v^*)^2 \text{ locally at } v = \mathfrak{p}_1, \mathfrak{p}_2 \tag{1}$$

$$\Leftrightarrow\ \begin{cases} X^2 - 2x_1X + 1 \text{ is irreducible over } K_v \text{ for } v = \mathfrak{p}_1, \mathfrak{p}_2 \\ \text{or } x_1 = \pm 1 \end{cases} \tag{2}$$

$$\Leftrightarrow\ x_1 = \pm 1 \text{ or } (\exists\, \alpha \in D^{\text{perf}} \text{ s.t. } K(\alpha) \text{ splits } D^{\text{perf}},$$

$$\text{and } \alpha^2 - 2\alpha x_1 + 1 = 0) \tag{3}$$

$$\begin{aligned}
&\Leftrightarrow\ x_1 = \pm 1 \text{ or } (\exists\, \alpha \in D^{\mathrm{perf}} \text{ s.t. } \mathrm{tr}(\alpha) = 2x_1, \mathrm{nr}(\alpha) = 1, \qquad (4)\\
&\qquad \text{and } [K(\alpha) : K] = 2)\\
&\Leftrightarrow\ \exists\, \alpha \in D^{\mathrm{perf}} \text{ s.t. } \mathrm{tr}(\alpha) = 2x_1, \text{ and } \mathrm{nr}(\alpha) = 1\\
&\Leftrightarrow\ x_1 \in T.
\end{aligned}$$

The equivalence of (1) and (2) comes from solving the equation $X^2 - 2x_1X + 1$ using the quadratic formula. The equivalence of (3) and (4) follows from the fact that every degree 2 field extension $K(\alpha) \subseteq D^{\mathrm{perf}}$ splits the 4-dimensional division algebra D^{perf}.

There exists an $a_1 \in k_1$ such that $(a_1^2 - 1) \notin (k_1)^2$: If $a_1^2 - 1$ were a square for every $a_1 \in k_1$, then we would have $a_1^2 - 1 = b^2$, so $a_1^2 - 2 = b^2 - 1 = c^2$ is a square, so repeating this p times for every square we could show that the number of squares in k_1 is divisible by p. But $k_1 = \mathbb{F}_{p^n}$ for some $n > 0$ and the number of squares in $\mathbb{F}_{p^n}$ is $(p^n + 1)/2$ which is not divisible by p.

The same argument shows that there exists an element $a_2 \in k_2$ such that $(a_2^2 - 1) \notin (k_2)^2$.

Let $a_1 \in k_1$ and $a_2 \in k_2$ be such elements. By the approximation theorem there exists an element $a \in \mathcal{O}^{\mathrm{perf}}$ such that $a \equiv a_1 \bmod \mathfrak{p}_1$ and $a \equiv a_2 \bmod \mathfrak{p}_2$. From the above equivalences it follows that $a \in T$. The approximation theorem implies that for each $i \in k_1$, $j \in k_2$ we can find an element $\alpha_{i,j} \in \mathcal{O}^{\mathrm{perf}}$ with the property that $\alpha_{i,j} \equiv i \bmod \mathfrak{p}_1$ and $\alpha_{i,j} \equiv j \bmod \mathfrak{p}_2$.

Claim.

$$\mathcal{O}^{\mathrm{perf}} = \bigcup_{i \in k_1,\, j \in k_2} (T + \alpha_{i,j}).$$

Proof of Claim. The set T contains all elements

$$\{x \in K : x \equiv a_1 \bmod \mathfrak{p}_1 \text{ and } x \equiv a_2 \bmod \mathfrak{p}_2\}.$$

If $y \in \mathcal{O}^{\mathrm{perf}}$, then for some $i \in k_1$, $j \in k_2$, $y \equiv i \bmod \mathfrak{p}_1$ and $y \equiv j \bmod \mathfrak{p}_2$, so then $y - \alpha_{(i-a_1),(j-a_2)} \in T$. This proves the claim.

The claim implies that $\mathcal{O}^{\mathrm{perf}}$ is diophantine over K. The same argument with $\mathfrak{p}_2$ replaced by some other prime $\mathfrak{p}_3$ shows that the set $\tilde{\mathcal{O}}^{\mathrm{perf}} = \{z \in K : \mathrm{ord}_{\mathfrak{p}_1}(z) \geqslant 0$ and $\mathrm{ord}_{\mathfrak{p}_3} \geqslant 0\}$ is diophantine over K. Then by weak approximation $\{x \in K : \mathrm{ord}_{\mathfrak{p}_1}(x) \geqslant 0\} = \mathcal{O}^{\mathrm{perf}} + \tilde{\mathcal{O}}^{\mathrm{perf}}$. $\square$

Lemma 4.2. *Let k be any global field of characteristic $p > 0$ such that k is a finite extension of $\mathbb{F}_q(t)$ for some $q = p^n$. The perfect closure of k is $k^{\mathrm{perf}} := k(t^{1/p}, t^{1/p^2}, t^{1/p^3}, \ldots)$.*

Proof. Clearly k^{perf} is contained in the perfect closure of k. The field k^{perf} is a finite extension of $K = \mathbb{F}_q(t, t^{1/p}, t^{1/p^2}, t^{1/p^3}, \ldots)$. Since K is perfect, and finite extensions of perfect fields are perfect, k^{perf} is perfect as well, so it must be equal to the perfect closure of k. $\square$

Now we can state the general theorem:

Theorem 4.3. *Let k be a global field of characteristic $p > 2$, and k^{perf} its perfect closure. Let $\mathfrak{p}$ be a prime of k^{perf}. The set $\{x \in k^{\mathrm{perf}} : \mathrm{ord}_{\mathfrak{p}}\, x \geqslant 0\}$ is diophantine over k^{perf}.*

Proof. We can repeat the proof of Theorem 4.1 with $\mathbb{F}_q(t)$ replaced by k. Everything works exactly as before, because the exact sequence of Theorem 2.12 works for all global fields k. $\square$

Acknowledgments

I thank Bjorn Poonen for suggesting the method of proof of Theorem 3.1 and for his comments regarding Section 4.

References

[1] N. Bourbaki, Éléments de Mathématique, XIII: Première Partie: Les Structures Fondamentales de L'analyse, Livre II: Algèbre, Modules et anneaux semi-simples, Actualités Sci. Ind., No. 1261, Hermann, Paris, 1958 (Chapitre VIII).
[2] M. Davis, H. Putnam, J. Robinson, The decision problem for exponential diophantine equations, Ann. Math. (2) 74 (1961) 425–436.
[3] J. Denef, The Diophantine problem for polynomial rings and fields of rational functions, Trans. Amer. Math. Soc. 242 (1978) 391–399.
[4] K. Eisenträger, Hilbert's Tenth Problem for algebraic function fields of characteristic 2, Pacific J. Math. (210) (2003) 261–281.
[5] K. Eisenträger, Hilbert's Tenth Problem for function fields of varieties over $\mathbb{C}$, Internat. Math. Res. Notices (59) (2004) 3191–3205.
[6] N. Jacobson, Basic Algebra: II, second ed., W. H. Freeman and Company, New York, 1989.
[7] K.H. Kim, F.W. Roush, An approach to rational Diophantine undecidability, in: Proceedings of Asian Mathematical Conference, 1990 (Hong Kong, 1990), River Edge, NJ, World Scientific Publishing, Singapore, 1992, pp. 242–248.
[8] K.H. Kim, F.W. Roush, Diophantine undecidability of $\mathbf{C}(t_1, t_2)$, J. Algebra 150 (1) (1992) 35–44.
[9] S. Lang, Algebra, third ed., Springer, New York, 1993.
[10] Yu.V. Matijasevič, The Diophantineness of enumerable sets, Dokl. Akad. Nauk SSSR 191 (1970) 279–282.
[11] J.S. Milne, Class Field Theory, 1997. Available on-line at http://www.jmilne.org/math/.
[12] T. Pheidas, Hilbert's tenth problem for fields of rational functions over finite fields, Invent. Math. 103 (1) (1991) 1–8.
[13] I. Reiner, Maximal Orders, London Mathematical Society Monographs, New Series, vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003.
[14] J. Robinson, Definability and decision problems in arithmetic, J. Symbolic Logic 14 (1949) 98–114.

[15] J. Robinson, The undecidability of algebraic rings and fields, Proc. Amer. Math. Soc. 10 (1959) 950–957.
[16] R.S. Rumely, Undecidability and definability for the theory of global fields, Trans. Amer. Math. Soc. 262 (1) (1980) 195–217.
[17] J.P. Serre, Local Fields, Graduate Texts in Mathematics, vol. 67, Springer, New York, 1979.
[18] A. Shlapentokh, Diophantine classes of holomorphy rings of global fields, J. Algebra 169 (1) (1994) 139–175.
[19] A. Shlapentokh, Diophantine undecidability over algebraic function fields over finite fields of constants, J. Number Theory 58 (2) (1996) 317–342.
[20] A. Shlapentokh, Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic, Pacific J. Math. 193 (2) (2000) 463–500.
[21] C.R. Videla, Hilbert's tenth problem for rational function fields in characteristic 2, Proc. Amer. Math. Soc. 120 (1) (1994) 249–253.