SUMS OF THREE SQUARES IN FUNCTION FIELDS OF CONICS AND CASSELS–CATALAN CURVES

DAVID GRIMM

ABSTRACT. We show that a function field in one variable of genus zero has pythagoras number two if and only if either the base field is hereditarily pythagorean and, in case the function field is nonreal, uniquely ordered, or -1 is a square in the base field. We generalize one implication to function fields of Cassels-Catalan curves.

Keywords: Pythagoras number, function fields, rational points

Classification (MSC 2010): 12D15, 14H05, 14H45, 14G05

1. INTRODUCTION

Let K be a field. We say that K is *real* if -1 is not a sum of squares in K, and *nonreal* otherwise. The pythagoras number of K, denoted $p(K)$, is defined as the smallest positive integer n such that every sum of squares in K is equal to a sum of n squares; if no such integer exists we set $p(K) = \infty$. If $p(K) = 1$ we say that K is *pythagorean*. If K is real and every finite extension of K is pythagorean, we say that K is *hereditarily pythagorean*. Note that any field of characteristic 2 is pythagorean. In the sequel we assume that the characteristic of K is different from 2.

It is very difficult in general to determine the pythagoras number of a given field; we refer to [P, Chap. 7] for an overview on known results.

We consider a function field in one variable F/K (i.e. a finitely generated field extension of transcendence degree one) where K is relatively algebraically closed in F. We refer to [S, Chap. I] for the basic theory of function fields in one variable, including the definition of the genus.

The problem to relate $p(F)$ and $p(K)$ is widely open in general. In particular, it is not known whether $p(F)$ can be bounded in terms of $p(K)$. It follows from [Lam, Chap. VIII, 5.7] that $p(F) \geq 2$. In this article, we study the situation where $p(F) = 2$. Note that if -1 is a square in K then $p(F) = 2$. Hence, the following result, which we will obtain in [3.2], yields a full characterization of function fields of genus zero with pythagoras number two.

Theorem A. *Assume that -1 is not a square in K and that F/K has genus zero. Then $p(F) = 2$ if and only if K is hereditarily pythagorean and, in case F is nonreal, uniquely ordered.*

In the case where F is the rational function field over a real field K this is a known result due to Becker [B, Chap. III, Thm. 4]. When F is an arbitrary function field of genus zero, Tikhonov and Yanchevskiĭ [TY, Thm. 2 & Thm. 3] showed one implication, namely that $p(F) = 2$ is implied by the stated conditions on K. We show the reverse implication.

Without restriction on the genus of F/K, the question was raised in [BV, 4.4] whether $p(F) = 2$ implies that K is hereditarily pythagorean. A partial positive answer to this question was obtained in [BV, 4.3] in the case where F/K has a divisor of odd degree.

A plane curve over K given by an equation $1 = aX^n + bY^m$ where $n, m \in \mathbb{N}$ are prime to the characteristic of K and $a, b \in K^\times$ is called a *Cassels-Catalan curve*. Such affine curves are smooth and geometrically irreducible. The Cassels-Catalan curves in the case $n = m = 2$ correspond exactly to the affine parts of regular conics, whence their function fields are exactly the function fields of genus zero, by [Liu, 7.4.1] and [S, Chap. V, 3.3]. The following second main result yields new cases where [BV, 4.4] has a positive answer.

Theorem B. *Assume that K is not hereditarily pythagorean and that -1 is not a square in K. Assume that F is the function field of a Cassels–Catalan curve over K. Then $p(F) \geq 3$.*

The proof is given in Section 4. The strategy is to find a point on the curve having a nonreal residue field in which -1 is not a square. As we will see in [3.1], this allows to relate a minimal representation of -1 as a sums of squares in the residue field to a sum of squares in F that is not a sum of two squares. In general, finding such a point on a Cassels-Catalan curve is technical. In the special case $n = m = 2$, that is for regular conics, the following statement gives a more conceptual argument for the existence of such a point.

Theorem C. *Assume that K is infinite. Let L/K be a finite separable extension and V a geometrically integral variety over K such that V_L is unirational. Then there exists a regular point $P \in V$ such that $K(P) \cong_K L$.*

We prove this result in Section 2. We do not know whether a similar statement also holds when K is finite.

2. Points on geometrically rational varieties

The main goal of this section is to obtain a proof of Theorem C. A key idea was contributed by Adrian Wadsworth.

An integral variety over a field is called *unirational*, if there exists a dominant morphism from an open subscheme of an affine space to the variety, and moreover *rational* if this morphism has an inverse that is defined on an open subscheme of the variety.

Let V be a K-vector space of dimension $n < \infty$. We call a map $V \to K$ a K-*polynomial function* if it is given by the evaluation of a polynomial in n variables over K, after identifying V with K^n by the choice of an arbitrary basis for V. We call the zero locus $H(g)$ of a nonzero K-polynomial function $g : V \to K$ a K-*hyperplane*, and we call the coarsest topology in V in which every K-hyperplane is closed, the K-*Zariski topology*. The K-Zariski topology on K itself is the cofinite topology.

Given a K-hyperplane $H(g) \subset V$ and another finite dimensional vector space W, a map $\varphi : V \setminus H(g) \to W$ is said to be K-*regular* if there exists $r \in \mathbb{N}$ and a K-polynomial function $f : W \to K$, such that the map $V \setminus H(g) \to K$ given by $v \mapsto (f \circ \varphi)(v) \cdot g(v)^r$ extends to a K-polynomial function on V.

Given two K-regular maps $\varphi : V_1 \setminus H_1 \to V_2$ and $\psi : V_2 \setminus H_2 \to V_3$ with $\varphi^{-1}(H_2) \cup H_1 \neq V_1$, the composition $\psi \circ \varphi$ is defined as a K-regular map on the complement of the hyperplane $\varphi^{-1}(H_2) \cup H_1$ in V_1.

2.1. **Lemma.** *Let L/K be a finite field extension. Then* $\mathrm{mult}_L : L \times L \to L$, $(x, y) \mapsto xy$ *and* $\mathrm{inv}_L : L \setminus \{0\} \to L$, $x \mapsto \frac{1}{x}$ *are K-regular maps.*

Proof. We identify L with a K-subalgebra of $\mathrm{End}_K(L)$, via the algebra homomorphism that assigns to $a \in L$ the left-multiplication $x \mapsto ax$. The multiplication on $\mathrm{End}_K(L)$ is a K-regular map $\mathrm{End}_K(L) \times \mathrm{End}_K(L) \to \mathrm{End}_K(L)$, as can be seen by identifying $\mathrm{End}_K(L)$ with a matrix algebra over K. Hence, its restriction $\mathrm{mult}_L : L \times L \to L$ to L is also a K-regular map. The subset of noninvertible elements of $\mathrm{End}_K(L)$ is a K-hyperplane given by a determinant polynomial. This hyperplane restricts to the single point set $\{0\}$ in L. The inversion map on the invertible elements is a K-regular map on $\mathrm{End}_K(L)$ by Cramer's Rule. Restricting the map to $L \setminus \{0\}$, we obtain that $\mathrm{inv}_L : L \setminus \{0\} \to L$ is also a K-regular map. $\square$

For $f \in K(t)$, choose $g, h \in K[t]$ relatively prime such that $f = \frac{g}{h}$. We write $f : K \dashrightarrow K$ for the regular map $K \setminus H(h) \to K$ defined by $x \mapsto \frac{g(x)}{h(x)}$.

2.2. **Corollary.** *Let L/K be a finite extension and $f \in L(t)$. The L-regular map $f : L \dashrightarrow L$ is a K-regular map.*

Proof. First, we show this in the case where $f \in L[t]$. Let $s = [L : K]$ and fix an arbitrary K-basis $(\ell_1, \ldots, \ell_s)$ of L. Write $f = f_0 + f_1 t + \cdots + f_d t^d$ with $d \in \mathbb{N}$ and $f_0, \ldots, f_d \in L$. For $z \in L$ write $z = r_1\ell_1 + \cdots + r_s\ell_s$ with $r_1, \ldots r_s \in K$. We can consider $f(z) = f(r_1\ell_1 + \cdots + r_s\ell_s)$ as a polynomial function over L in s variables evaluated at $(r_1, \ldots, r_s)$. We can choose $\tilde{f}_1, \ldots, \tilde{f}_s \in K[X_1, \ldots, X_s]$ such that $f(r_1\ell_1 + \cdots + r_s\ell_s) = \tilde{f}_1(r_1, \ldots, r_s)\ell_1 + \cdots + \tilde{f}_s(r_1, \ldots, r_s)\ell_s$. Hence the map $L \to L$, $z \mapsto f(z)$ is given by the polynomials $\tilde{f}_1, \ldots, \tilde{f}_s$ over K. Now assume that $f \in L(t)$. Let $g, h \in L[t]$ be relatively prime such that $f = \frac{g}{h}$. Then the map $L \setminus H(h) \to L$ given by $z \mapsto f(z)$ is given by the following composition of K-regular maps.

$$f : L \setminus H(h) \xrightarrow{(g,h)} L \times (L \setminus H(h)) \xrightarrow{\mathrm{id}\times\mathrm{inv_L}} L \times L \xrightarrow{\mathrm{mult_L}} L,$$

where $(g,h)(x) = (g(x), h(x))$ and $\mathrm{id} \times \mathrm{inv}(x,y) \mapsto (x, y^{-1})$. This composition of K-regular maps is defined. $\square$

2.3. **Lemma.** *Let L/K be a finite field extension. For every $f \in L(t)$ there exist $g \in L[t]$ and $h \in K[t]$ such that $f = \frac{g}{h}$.*

Proof. Choosing $\alpha_1, \ldots, \alpha_n \in L$ such that $L = K[\alpha_1, \ldots, \alpha_n]$, we have that $L(t) = K[\alpha_1, \ldots, \alpha_n](t) = K(t)[\alpha_1, \ldots, \alpha_n]$. $\square$

2.4. **Proposition.** *Assume that K is infinite. Let L/K be a proper finite extension that is not purely inseparable. Let $f \in L(t)$ such that $f(z) \in K$ for every $z \in L$ where $f(z)$ is defined. Then $f \in K$.*

Proof. We first show that $f \in K(t)$. By [2.3], there exists $g \in L[t]$ and $h \in K[t]$ such that $f = \frac{g}{h}$. Write $g = g_0 + g_1 t + \cdots + g_d t^d$ with $d \in \mathbb{N}$ and $g_0, \ldots, g_d \in L$. Evaluating this polynomial in $d+1$ distinct elements $\alpha_0, \ldots, \alpha_d \in K \setminus H(h)$ yields that

$$\begin{pmatrix} 1 & \alpha_0 & \cdots & \alpha_0^d \\ 1 & \alpha_1 & \cdots & \alpha_1^d \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_d & \cdots & \alpha_d^d \end{pmatrix} \cdot \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_d \end{pmatrix} = \begin{pmatrix} f(\alpha_0)h(\alpha_0) \\ f(\alpha_1)h(\alpha_1) \\ \vdots \\ f(\alpha_d)h(\alpha_d) \end{pmatrix} \in K^{d+1}.$$

Since the matrix on the left is invertible, we have that $g_0, \ldots, g_d \in K$. Hence $g \in K[t]$ and thus $f \in K(t)$.

In order to show that $f \in K$, we fix an element $\beta \in L \setminus K$ that is separable over K. Let σ be a K-automorphism of the algebraic closure of L such that $\sigma(\beta) \neq \beta$. Since $f(z) \in K$ for all $z \in L \setminus h^{-1}(\{0\})$, it follows that $g(r_0 + r_1\beta)h(r_0 + r_1\sigma(\beta)) = g(r_0 + r_1\sigma(\beta))h(r_0 + r_1\beta)$ for any $r_0, r_1 \in K$. Since K is infinite, we obtain the polynomial identity $g(X + Y\beta)h(X + Y\sigma(\beta)) = g(X + Y\sigma(\beta))h(X + Y\beta)$ in the variables X and Y. Since the matrix

$$\begin{pmatrix} 1 & \beta \\ 1 & \sigma(\beta) \end{pmatrix}$$

is invertible, we conclude by a linear change of variables the polynomial identity $g(X)h(Y) = g(Y)h(X)$. Hence $f = \frac{g}{h} \in K$. $\square$

2.5. **Proposition.** *Assume that K is an infinite field. Let L/K be a finite separable extension. Let $f \in L(t) \setminus L$. Then there exists $\alpha \in L$ such that $f(\alpha)$ is defined and $K(f(\alpha)) \cong_K L$.*

Proof. By [2.2], the L-regular map $f : L \dashrightarrow L$ is K-regular. Note that the K-open subset in L on which this regular map is defined is K-irreducible. As f is continuous, the image of the map $f : L \dashrightarrow L$ is irreducible. Assume that the image of $f : L \dashrightarrow L$ does not contain a primitive element of L/K, then it is contained in the finite union of the maximal proper subfields of L that contain K. The latter is a finite union of K-vector subspaces of L. None of those maximal proper subfields is contained in the union of the others, hence they are the K-irreducible components of this finite union. Thus the image of $f : L \dashrightarrow L$ is contained in one maximal proper subfield E of L containing K. By [2.4], we obtain that $f \in E$, which contradicts the assumption that $f \notin L$. $\square$

2.6. **Remark.** If K is a finite field of characteristic p and L/K a proper finite extension, then the image of the nonconstant map $L \to L, x \mapsto x^p$ is a proper subfield of L.

The following is the main result of this section. For the used concepts from algebraic geometry we refer to [H, Chap. II].

2.7. **Theorem.** *Assume that K is infinite. Let L/K be a finite separable extension and V be a geometrically integral variety over K such that V_L is unirational. Then the set of regular points $P \in V$ such $K(P) \cong_K L$ is K-Zariski dense in V.*

Proof. Let $n \in \mathbb{N}$ and $U \in \mathbb{A}^n_L$ an open L-subvariety and $U \to V_L$ a dominant morphism. By [H, Chap. II, 8.16], the subset of regular points on V is open dense. Hence, by the dominance of the morphism $U \to V_L$, we can assume V to be regular affine. Let $V \hookrightarrow \mathbb{A}^m_K$ be a closed immersion for some $m \in \mathbb{N}$.

We choose a projection $\mathbb{A}^m_K \to \mathbb{A}^1_K$ such that the composition $V \hookrightarrow \mathbb{A}^m_K \to \mathbb{A}^1_K$ is not constant. Furthermore, we choose a closed immersion $\mathbb{A}^1_L \hookrightarrow \mathbb{A}^n_L$ such that preimage W of U with respect to this immersion is nonempty and such that W is not mapped to a single point in $\mathbb{A}^1_L$. Considering the commutative diagram

$$\begin{tikzcd} W \arrow[r, hook] & U \arrow[r] & V_L \arrow[r, hook] \arrow[d] & \mathbb{A}^m_L \arrow[r] \arrow[d] & \mathbb{A}^1_L \arrow[d, "\varphi_L"] \\ & & V \arrow[r, hook] & \mathbb{A}^m_K \arrow[r] & \mathbb{A}^1_K \end{tikzcd}$$

whose vertical arrows are the base-change morphisms, we see that it is sufficient to find a rational point $P \in W$ that is mapped to a closed point in $\mathbb{A}^1_K$ with residue field L. Equivalently, it is sufficient to find a rational point $P \in W$ whose image in $\operatorname{Spec}(L[Y]) = \mathbb{A}^1_L$ corresponds to a maximal ideal generated by a linear polynomial $Y - \beta$, where $\beta \in L$ is such that $L = K(\beta)$, since the preimage of this maximal ideal under the dual homomorphism to the base change φ_L will be the maximal ideal in $\operatorname{Spec}(K[Y]) = \mathbb{A}^1_K$ generated by the minimal polynomial for β over K.

By shrinking W if necessary, we can assume that $W = \operatorname{Spec}(L[X]_h)$, that is, W is a principal open subscheme of $\mathbb{A}^1_L = \operatorname{Spec}(L[X])$ given by the localization of $L[X]$ after the multiplicative set $\{h^i \mid i \in \mathbb{N}_0\}$ for some $h \in L[X]$. The nonconstant map $W \to \mathbb{A}^1_L$ corresponds to a L-algebra homomorphism

$$\psi : L[Y] \to L[X]_h$$

with $\psi(Y) \notin L$. Say $\psi(Y) = \frac{g}{h^r}$ for some $r \in \mathbb{N}$ and $g \in L[X]$. For arbitrary $\alpha \in L$ such that $h(\alpha) \neq 0$, consider a maximal ideal in $L[X]_h$ containing $\frac{g}{h^r} - \frac{g(\alpha)}{h(\alpha)}$.

Its inverse image in $L[Y]$ is obviously the maximal ideal generated by $Y - \frac{g(\alpha)}{h(\alpha)}$. By [2.5], there exists $\alpha \in L$ with $h(\alpha) \neq 0$ and $L = K(\frac{g(\alpha)}{h(\alpha)})$. This shows the existence of a regular point $P \in V$ with $K(P) \cong_K L$. Let V' denote the complement in V of the closure of the set of regular points $P \in V$ with $K(P) \cong_K L$. If V' is nonempty then V'_L is unirational and we obtain a contradiction to the first part applied to V'. Hence, the set of regular points $P \in V$ with $K(P) \cong_K L$ is dense in V. □

A weak version of Nishimura's Lemma [N] states that the existence of a rational point is invariant under birational equivalence between smooth projective irreducible varieties (also over finite fields). If it could be shown that the same is true for the existence of a closed point with prescribed residue field, then we could extend [2.7] to cover finite fields as well, at least with the additional assumption that the variety is smooth and projective.

3. Sums of squares in function fields of conics

In this section, we will prove Theorem A. The following observation will also play a role in the proof of Theorem B.

3.1. **Proposition.** *Assume that K carries a valuation with value group $\mathbb{Z}$ and with nonreal residue field κ of characteristic different from 2. Let s be the smallest positive integer such that -1 is a sum of s squares in κ. Then $p(K) > s$.*

Proof. Let v denote the valuation. By the choice of s, there exist $x_0, \ldots, x_s \in K$ with $v(x_0) = \ldots = v(x_s) = 0$ and $v(x_0^2 + \ldots + x_s^2) > 0$. If $v(x_0^2 + \ldots + x_s^2) > 1$ we replace x_0 by $x_0 + t$ for any $t \in K$ with $v(t) = 1$. Hence, we may assume that $v(x_0^2 + \ldots + x_s^2) = 1$. We claim that $x_0^2 + \ldots + x_s^2$ is not a sum of s squares in K. Suppose on the contrary that there exist $y_1, \ldots, y_s \in K$ with $y_1^2 + \ldots + y_s^2 = x_0^2 + \ldots + x_s^2$. We can assume that $v(y_1) \leq v(y_2) \leq \ldots \leq v(y_s)$. Then $v(1 + (y_1^{-1}y_2)^2 + \ldots + (y_1^{-1}y_s)^2) > 0$, and we obtain a representation of -1 as a sum of $s-1$ squares in κ, contradicting the choice of s. □

We recall from [GS, 1.3.2 & 1.3.5] that every regular conic over a field of characteristic different from 2 is a generic splitting variety for a quaternion algebra, that is, the base field extensions that split the quaternion algebra are exactly those over which the conic becomes rational.

3.2. **Theorem.** *Assume that K is not hereditarily pythagorean and that -1 is not a square in K. Let F be the function field of a regular conic over K. Then $p(F) \geq 3$.*

Proof. We shall first observe that there exists a finite separable nonreal extension K'' of K such that -1 is a sum of two squares in K''. In the case where K is real, let K' denote a finite real extension of K that is not pythagorean. In the case where K is nonreal, set $K' = K$. In both cases, there exists a sum of two squares σ in K' that is not a square, and we set $K'' = K'(\sqrt{-\sigma})$, which is a finite separable extension of K.

Now consider any maximal algebraic field extension M/K'' in which -1 is not a square. By [Lam, Chap. III, 2.8], every quaternion algebra over M is split, whereby every conic over M is rational. The conic of the statement already splits over some finite nonreal extension L/K contained in M. Note that -1 is not a square in L. In the case where K is real, it is clear that L/K is separable, hence there exists a point on the conic with residue field L by [2.7]. In the case where K is nonreal, there exists a point on the conic whose residue field L' is a subfield of L and contains K. Hence, L is nonreal and -1 is not a square in L. In both cases [3.1] yields $p(F) > 2$. □

We say that K is *euclidean* if it is pythagorean and uniquely ordered. We say that K is *hereditarily euclidean* if K is real and every finite real extension of K is euclidean.

3.3. **Corollary.** *Assume that -1 is not a square in K. Let F/K be a function field in one variable of genus zero.*

(a) *Assume that F is real. Then $p(F) = 2$ if and only if K is hereditarily pythagorean.*
(b) *Assume that F is nonreal. Then $p(F) = 2$ if and only if K is hereditarily euclidean.*

Proof. A real function field of genus zero over a hereditarily pythagorean field has pythagoras number 2, e.g. by [BV, 4.10]. The converse implication follows with [3.2]. This shows (a). Now assume that K is hereditarily euclidean. Then every function field in one variable has pythagoras number 2, by [BV, 4.6]. Assume conversely that $p(F) = 2$ for a nonreal function field of genus zero. It follows by [3.2] that K is hereditarily pythagorean. Hence, F is isomorphic to the function field of the conic $X^2 + Y^2 + Z^2 = 0$. By [BV, 4.7], it follows that K is hereditarily euclidean. This shows (b). □

By [B, Chap. III, Lemma 5], a uniquely ordered hereditarily pythagorean field is already hereditarily euclidean. Hence, [3.3] yields Theorem A.

4. Sums of squares in function fields of Cassels–Catalan curves

In this section we prove Theorem B. We denote by $K^{\times 2}$ the set of nonzero squares in a field K, and by $\pm K^{\times 2}$ we denote the set $K^{\times 2} \cup -K^{\times 2}$. The algebraic closure of K is denoted K_{alg}.

4.1. **Proposition.** *Assume that K is infinite. Let L be a finite separable non-pythagorean extension of K. Then there exists $\xi \in L$ such that $L = K(\xi^2)$ and $\xi^2 + 1 \notin L^{\times 2}$. Moreover, there exists $\sigma \in \sum L^2 \setminus L^{\times 2}$ such that $L = K(\sigma)$ and $\sigma + 1 \notin L^{\times 2}$.*

Proof. Fix $z \in L$ with $z^2+1 \notin L^{\times 2}$. For arbitrary $\nu \in L^\times$, consider the terms $\alpha = \frac{\nu^2}{z^2}$, $\beta = \nu^2 + z^2$, $\gamma = \frac{(z^2+1)^2}{\nu^2} + z^2$, $\delta = \frac{(z^2+1)^2}{z^2\nu^2}$ and $\epsilon = \frac{z^2+1}{\nu^2}$. These terms are rational functions in ν over L. Let $\mathcal{G} = \{x \in L \mid K(x) = L\}$. This is a K-Zariski open subset of L as it is the complement of the finitely many subspaces of L that correspond to the finitely many intermediate extensions of L/K. By [2.5] the preimage of $\mathcal{G}$ under any rational function from $L(t) \setminus L$ is nonempty. Moreover, $\mathcal{G}$ is K-open in L. As the intersection of finitely many nonempty K-open subsets of L is nonempty, there exists $\nu \in L^\times$, such that $\alpha, \beta, \gamma, \delta, \epsilon \in \mathcal{G}$. Note that $\epsilon, \frac{1}{\epsilon} \in \sum L^2 \setminus L^{\times 2}$. If $\epsilon + 1 \notin L^{\times 2}$ we set $\sigma = \epsilon$. Otherwise we have $\frac{1+\epsilon}{\epsilon} = \frac{1}{\epsilon} + 1 \notin L^{\times 2}$ and set $\sigma = \frac{1}{\epsilon}$.

Note also that $\alpha \in L^{\times 2}$ and if $\alpha + 1 \notin L^{\times 2}$, choose $\xi = \frac{\nu}{z}$. Assume now that $\alpha + 1 \in L^{\times 2}$. Then $\beta \in L^{\times 2}$. If $\beta + 1 \notin L^{\times 2}$ choose $\xi \in L$ such that $\xi^2 = \beta$. Assume now that $\beta + 1 \in L^{\times 2}$. Then $\nu^2 + z^2 + 1 \in L^{\times 2}$ and $\nu^2 + z^2 \in L^{\times 2}$. It follows that $\frac{(z^2+1)^2}{\nu^2} + z^2 + 1 \notin L^{\times 2}$ since $z^2+1 \notin L^{\times 2}$. Remember that $\delta = \frac{(z^2+1)^2}{z^2\nu^2}$. If $\delta + 1 \notin L^{\times 2}$, choose $\xi = \frac{z^2+1}{z\nu}$. Otherwise, if $\delta + 1 \in L^{\times 2}$, then $\gamma \in L^{\times 2}$ and $\gamma + 1 \notin L^{\times 2}$ and we choose $\xi \in L$ such that $\xi^2 = \gamma$ in this last case. □

4.2. **Lemma.** *Let $u \in K^\times \setminus \pm K^{\times 2}$ and $r \geq 1$. Let $\gamma \in K_{\text{alg}}$ be such that $\gamma^{2^r} = u$. Then $K^\times \cap K(\gamma)^{\times 2} = K^{\times 2} \cup uK^{\times 2}$.*

Proof. As $-u \notin K^{\times 2}$, and thus $-u \notin 4K^{\times 4}$, the polynomial $T^{2^r} - u$ is irreducible by [La, Chap. VI, 9.1]. Write $d = \gamma^2$, $L = K(d)$ and $M = K(\gamma)$. Note that M/L is a quadratic extension. As $T^{2^{r-1}} - u$ is the minimal polynomial of d over K, the norm of d with respect to L/K is $\pm u$. As $u \notin \pm K^{\times 2}$, it follows that $K^\times \cap dL^{\times 2} = \emptyset$. As $L^\times \cap M^{\times 2} = L^{\times 2} \cup dL^{\times 2}$, we have that

$$K^\times \cap M^{\times 2} = K^\times \cap (L^{\times 2} \cup dL^{\times 2}) = K^\times \cap L^{\times 2}.$$

The statement thus follows by induction on r. □

4.3. **Corollary.** *Suppose $-1 \notin K^{\times 2}$. Let $u \in K^\times \setminus \pm K^{\times 2}$ and $n \in \mathbb{N}$. There exists $x \in K_{\text{alg}}$ with $x^n = u$ and $K^\times \cap K(x)^{\times 2} \subseteq K^{\times 2} \cup uK^{\times 2}$.*

Proof. If n is odd, we can choose $x \in K_{\text{alg}}$ with $x^n = u$ such that $[K(x) : K]$ is odd, whereby $K^\times \cap K(x)^{\times 2} \subseteq K^{\times 2}$. Assume now that n is even. If $u \notin K^{\times 2}$, then we write $n = 2^r m$ with m odd and $r \geq 1$, and apply [4.2] together with the previous case. □

4.4. **Corollary.** *Suppose $-1 \notin K^{\times 2}$. Let $v \in K^\times \setminus -K^{\times 2}$ and $m \in \mathbb{N}$. There exists $y \in K_{\text{alg}}$ such that $y^m = v$ and $-1 \notin K(y)^{\times 2}$.*

Proof. Let $r \in \mathbb{N}$ be maximal such that $2^r | m$ and $v \in K^{\times 2^r}$. Let $u \in K$ be such that $u^{2^r} = v$. We write $m = n2^r$. If n is odd, then we can choose $y \in K_{\text{alg}}$ such that $y^m = v$ and $[K(y) : K]$ is odd, and it follows trivially that $-1 \notin K(y)^{\times 2}$.

Assume that n is even. Then $u \notin K^{\times 2}$ by the maximality of r. Furthermore, we claim that $u \notin -K^{\times 2}$. If $r = 0$ we have that $u = v \notin \pm K^{\times 2}$. If $r > 0$ then

$u \notin -K^{\times 2}$ by the maximality of r and the fact that $(-u)^{2^r} = v$. Using [4.3], we choose $y \in K_{\text{alg}}$ such that $y^n = u$ and $K^\times \cap K(y)^{\times 2} \subseteq K^{\times 2} \cup uK^{\times 2}$. Then $y^m = v$ and $-1 \notin K(y)^{\times 2}$, since $u \notin -K^{\times 2}$. □

4.5. **Proposition.** *Suppose $-1 \notin K^{\times 2}$. Let $u \in K^\times \setminus \pm K^{\times 2}$ and $v \in K^\times \setminus (-K^{\times 2} \cup -uK^{\times 2})$. Let $n, m \geq 1$. Then there exists a finite extension M/K such that $-1 \notin M^{\times 2}$, with $x, y \in M$ such that $x^n = u$ and $y^m = v$, and such that $M = K(x, y)$.*

Proof. We choose $x \in K_{\text{alg}}$ such that $x^n = u$ and $K^\times \cap K(x)^{\times 2} \subseteq K^{\times 2} \cup uK^{\times 2}$. Then $-1, -v \notin K(x)^{\times 2}$. By [4.4] there exists $y \in K_{\text{alg}}$ such that $y^m = v$ and $-1 \notin K(x, y)^{\times 2}$. Set $M = K(x, y)$. □

4.6. **Corollary.** *Let L/K be a finite field extension such that L is real and not pythagorean. Let $a, b \in K$ such that $a, b \in L^{\times 2} \cup -L^{\times 2}$. For integers $n, m \geq 1$, there exists a finite extension M/L, such that $-1 \notin M^{\times 2}$, and with $x, y \in M$ such that $1 = ax^n + by^m$ and $M = K(x, y)$. Moreover, if n or m is even, we can choose M to be nonreal.*

Proof. By [4.1] there exists $\xi \in L$ with $\xi^2 + 1 \in \sum L^{\times 2} \setminus L^{\times 2}$ and $L = K(\xi^2)$, and further $\sigma \in \sum L^{\times 2} \setminus L^{\times 2}$ with $L = K(\sigma)$ and $\sigma + 1 \in \sum L^{\times 2} \setminus L^{\times 2}$.
In the case where $a, b \in L^{\times 2}$, set $u = -\frac{1}{a\sigma}$ and $v = \frac{1}{b}(1 + \frac{1}{\sigma})$. Then $u \notin \pm L^{\times 2}$ and $-v \notin L^{\times 2} \cup uL^{\times 2}$, as $-uv = \frac{1}{ab}\frac{\sigma+1}{\sigma^2}$. Moreover, $1 = au + bv$.
In the case where $-a, -b \in L^{\times 2}$, set $u = \frac{\xi^2+1}{a}$ and $v = \frac{-\xi^2}{b}$. Then $u \notin \pm L^{\times 2}$ and $-v \notin L^{\times 2} \cup uL^{\times 2}$. Moreover, $1 = au + bv$.
In the case where $-a, b \in L^{\times 2}$ set $u = \frac{\sigma+1}{a}$ and $v = \frac{-\sigma}{b}$. Then $u \notin \pm L^{\times 2}$ and $-v \notin L^{\times 2} \cup uL^{\times 2}$. Moreover, $1 = au + bv$.
In the case where $a, -b \in L^{\times 2}$ set $u = \frac{-\sigma}{a}$ and $v = \frac{\sigma+1}{b}$. Then $u \notin \pm L^{\times 2}$ and $-v \notin L^{\times 2} \cup uL^{\times 2}$. Moreover, $1 = au + bv$.

In each case, by [4.5], there exist $x, y \in L_{\text{alg}}$ such that $x^n = u$ and $y^m = v$ and $\sqrt{-1} \notin L(x, y)$. Moreover, since $u \in L(x, y)$ and $K(u) = L$, it follows that $L(x, y) = K(x, y)$. Obviously $1 = ax^n + by^m$ as $1 = au + bv$. Set $M = L(x, y)$. Now suppose that n or m is even. By symmetry, we can assume that n is even. Then $x^n = u$ is both a square in M and, by the choices of u in each case, a negative sum of squares in M. Thus M is not real. □

4.7. **Theorem.** *Assume that K is not hereditarily pythagorean and that -1 is not a square in K. Let F be the function field of a Cassels–Catalan curve over K. Then $p(F) \geq 3$.*

Proof. Assume that F is the function field of the curve $1 = aX^n + bY^m$ for some $a, b \in K^\times$ and $n, m \geq 1$ prime to the characteristic of K. Assume first that K is nonreal. If $-a$ is not a square in K, choose $x \in K_{\text{alg}}$ such that $x^n = \frac{1}{a}$ and $\sqrt{-1} \notin K(x)$ as in [4.4]. Then $P = (x, 0)$ is a point on the curve and -1 is not a square in $K(P)$. If $-b$ is not a square in K we can proceed analogous. So we assume that both $-a$ and $-b$ are not squares in K. Choose $z \in K$ such that z^2+1 is not a square in K. Choose again $x \in K_{\text{alg}}$ such that $x^n = \frac{z^2}{-a}$ and -1 is not a square in $K(x)$. Then $\frac{1}{b}$ is not a square in $K(x)$ and we also find some $y \in K_{\text{alg}}$ such that $y^m = \frac{-1}{b}$ and that -1 is not a square in $K(x,y)$, as in [4.5]. Again P is a point on the curve for which -1 is not a square in $K(P)$. In either case, we obtain that $p(F) \geq 3$ by [3.1] in the case where K is not real.

Now we assume that K is real. Let us first consider the case where n is odd. Then F is clearly an odd degree extension of the rational function field $K(X)$. Then $3 \leq p(K(X)) \leq p(F)$ by Springer's Theorem [Lam, Chap. VII, 2.7] and [3.3]. Hence we assume that n is even. Suppose there exists a finite real extension L/K that is not pythagorean. We can assume that a or $-a$, as well as one of b or $-b$ is a square in L, since we can replace L by one of the four extensions $L(\sqrt{\pm a})(\sqrt{\pm b})$ if necessary; note that none of those extensions is pythagorean, by [Lam, Chap. VIII, 5.7], and at least one of them is real. By [4.6] there exists a point P on the curve such that $K(P)$ is nonreal and -1 is not a square in $K(P)$. Again, [3.1] yields that $p(F) \geq 3$. □

Acknowledgements. This work is part of my PhD thesis at *Universität Konstanz* under the supervision of Karim Johannes Becher. I am grateful for his support. Part of the research was made during a research stay with Kevin Hutchinson at *University College Dublin*. I am further grateful to David Leep, Jan Van Geel and Adrian Wadsworth for taking interest in my work and for helpful discussions. Financial support was received from the *Deutsche Forschungsgemeinschaft* (project *Quadratic Forms and Invariants*, BE2614/3), from the *Science Foundation of Ireland Research Frontiers Programme* (Grant 05/RFP/MAT0022) and from the *Swiss National Science Foundation* (Grant 200020-124785/1).

References

[BV] K.J. Becher, J. Van Geel. *Sums of squares in function fields of hyperelliptic curves*, Math. Z. 261:829–844 (2009).

[B] E. Becker. *Hereditarily-pythagorean fields and orderings of higher level*, Monografias de Mathematica 29, Rio de Janeiro, 1978.

[N] H. Nishimura, *Some remarks on rational points*, Mem. Coll. Sci. Uni. Kyoto. Ser. A. Math. 29: 189–192 (1955).

[H] R. Hartshorne. *Algebraic Geometry*, Graduate Texts in Mathematics, 52. New York-Heidelberg-Berlin: Springer- Verlag. XVI, 1983.

[GS] P. Gille, T. Szamuely. *Central simple algebras and Galois cohomology.* Cambridge Studies in Advanced Mathematics 101. Cambridge: Cambridge University Press. xi, 343 p. (2006)

[Lam] T.Y. Lam. *Introduction to Quadratic Forms over Fields*, AMS Graduate Studies in Mathematics Vol. 67, Rhode Island, 2004.

[La] S. Lang. *Algebra - revised third edition*, Graduate Texts in Mathematics 211, Springer, New York, 2002.

[Liu] Q. Liu. *Algebraic Geometry and Arithmetic Curves*, Oxford Graduate Texts in Mathematics 6, Oxford University Press, 2002.

[P] A. Pfister. *Quadratic Forms with Applications to Algebraic Geometry and Topology*, London Math. Soc. Lecture Note Series 217.

[S] H. Stichtenoth, *Algebraic function fields and codes. 2nd ed.*, Graduate Texts in Mathematics 254, Springer, Berlin 2009.

[TY] S.V. Tikhonov, V.I. Yanchevskiĭ. *pythagoras numbers of function fields of regular conics over hereditarily pythagorean fields*, Dokl. Nats. Akad. Nauk Belarusi 47(2): 5–8 (2003).

Ecole Polytéchnique Fédérale de Lausanne, MA C3, 1015 Lausanne, Suisse
E-mail address: david.grimm@epfl.ch