FUNCTION FIELDS IN ONE VARIABLE WITH PYTHAGORAS NUMBER TWO

DAVID GRIMM

Abstract. We consider function fields in one variable that do not contain $\sqrt{-1}$ and investigate necessary conditions for them to have Pythagoras number two. For function fields of genus zero, we show that the field of constants needs to be hereditarily pythagorean. We apply refined observations on the splitting behavior of quadrics to obtain this result. Using a more technical approach, we can extend our result to a slightly larger class of function fields.

1. Introduction

Let K be a field. We denote by $K^\times$ the multiplicative group, by $K^{\times 2}$ the subgroup of nonzero squares in $K^\times$, and by $\sum K^2$ the subgroup of nonzero sums of squares in K. For $x \in K$ we set

$$\ell_K(x) = \inf\left\{n \in \mathbb{N} \mid x = x_1^2 + \cdots + x_n^2 \text{ for some } x_1, \ldots, x_n \in K\right\} \in \mathbb{N} \cup \{\infty\}$$

and call this the *length of x in K*. Two interesting field invariants related to sums of squares in K are the *level* $s(K) = \ell_K(-1)$ and the *Pythagoras number* $p(K) = \sup\left\{\ell_K(x) \mid x \in \sum K^2\right\}$. For general information on these two invariants we refer to [9, Chap. 3] and [7, Chap. XI].

Recall that K admits a field ordering if and only if $s(K) = \infty$ [7, Chap. VIII, (1.10)]; in this case we say that K is *real*, otherwise *nonreal*. The field K is said to be *pythagorean* if $\sum K^2 = K^{\times 2}$, i.e. if $p(K) = 1$.

Let K be a real base field and F/K a function field. Pfister [9, (6.3.4)] showed that, if K is real closed, then $p(F) \leq 2^n$ where n is the transcendence degree of F/K. The challenge to find weaker conditions on the base field K such that for arbitrary extensions F/K one has a bound on $p(F)$ in terms of $p(K)$ and the transcendence degree arises naturally. Note that it is not known whether $p(K) < \infty$ implies that $p(K(X)) < \infty$.

We say that a field is *hereditarily pythagorean* if it is real and if all its finite real field extensions are pythagorean. The following result [2, Chap. III, Thm. 4] is in a certain sense an improvement of Pfister's result for the special case of rational function fields in one variable.

1.1. **Theorem** (Becker)**.** *Let K be a real field. Then K is hereditarily pythagorean if and only if $p(K(X)) = 2$.*

Note that the hypothesis of K being real can be weakened to $\sqrt{-1} \notin K$, since if K were nonreal and $s(K) \geq 2$, the element $-1 + X^2$ would be a sum of three but not of two squares in $K(X)$, by [7, IX.2.1].

In [12], one implication of (1.1) was generalized to function fields F of smooth conics over K, i.e. it was shown that if K is hereditarily pythagorean then $p(F) = 2$ if F is real or if K is uniquely ordered, and $p(F) = 3$ otherwise.

The other implication of (1.1) will be generalized in (4.2). We show for function fields F of smooth conics over K that $p(F) = 2$ implies that $\sqrt{-1} \in K$ or that K is hereditarily pythagorean, using our observation (2.6) on splitting behavior of varieties like conics.
In fact, using more involved methods, we later generalize this in (5.6) further to function fields F/K of integral affine plane curves $1 = aX^n + bY^m$ where $a, b \in K^\times$ and $n, m \in \mathbb{N}$ are not divisible by $\mathrm{char}(K)$. We say that such function fields are *of generalized Fermat type*. Their genus is $\frac{1}{2}((n-1)(m-1) + 1 - \gcd(n, m))$. In the literature, the function fields in the case $n = m$ are called *of Fermat type*, see [10, VI.3.4]. The function fields of smooth conics correspond to the case $n = m = 2$ in the case of $\mathrm{char}(K) \neq 2$.
The fact that function fields of generalized Fermat type can have arbitrary genus is evidence that the following question raised in [1, 4.4] has a positive answer.

1.2. **Question.** *Let F/K be a function field in one variable not containing $\sqrt{-1}$. Then $p(F) = 2$ only if the field of constants of F is hereditarily pythagorean.*

The methods we apply in this work, however, seem not sufficient to decide this question in its full generality. The central idea to prove (4.2 & 5.6), is to show that if K is not hereditarily pythagorean, then it allows a finite nonreal extension M in which -1 is not a square, and which is the residue field of a smooth point on the curve. Then it follows with (3.2) that $p(F) \geq 3$.

My initial proof of existence of such extension fields M/K was rather technical. Jan Van Geel and Adrian Wadsworth gave me ideas how to make this much more conceptual (at least in the case of conics). The following section developed out of discussions with them. Its main result is the observation that a geomertrically unirational K-variety that is split by a finite separable extension M/K, contains a regular point whose residue field is M. Adrian Wadsworth also simplified many proofs in the following section, in particular getting rid of Galois theoretic arguments where they were not needed.

2. Splitting fields of geometrically unirational varieties

We prove in (2.6) that every finite separable field extension of an infinite field K that splits a geometrically unirational K-prevariety, is the residue field of a point on the variety. In the case of a smooth conic over an infinite field K, this result yields that, if a finite separable extension L/K is the residue field of a point on the conic, then so is every separable finite field extension of L.

Let K be a field and V a K-vector space of dimension $n < \infty$. We call a mapping V to K a *K-polynomial function* if it is given by evaluating a K-polynomial in n variables, after identifying V with K^n via choosing any basis for V. Endowing K with the cofinite topology, that is, the topology where the closed subsets are the finite sets and the set K, we define the *K-topology on V* to be the initial topology of the K-polynomial functions.
A *K-rational function on V* is a partially defined map $V \dashrightarrow K$ that is defined on a nonempty K-open subset of V and that is given by a fraction of K-polynomial functions.
If V, W are two finite dimensional K-vector spaces, we call a map $\varphi : V \to W$ a *K-polynomial map* if, for each basis element w_i of a fixed K-basis $w_1, \ldots, w_m$ of

W, the function $\pi_i \circ \varphi : V \to K$ is a polynomial function, where $\pi_i : W \longrightarrow K$ is the projection

$$(\alpha_1 w_1 + \cdots + \alpha_i w_i + \cdots + \alpha_m w_m) \mapsto \alpha_i.$$

More generally, a partially defined map $\varphi : V \dashrightarrow W$ map defined on a nonempty K-open subset of V, is called a *K-rational map* if the corresponding $\varphi \circ \pi_{w_i}$ are K-rational functions.
Note that if V' is a K-linear subspace of V and φ is a K-rational map on V that is defined on some $P \in V'$, then $\varphi|_{V'}$ is a K-rational map.

2.1. **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 $L(t) = K[\alpha_1, \ldots, \alpha_n](t) = K(t)[\alpha_1, \ldots, \alpha_n]$. □

2.2. **Proposition.** *Let L/K be a finite field extension. Then*

$$\text{mult} : L \times L \to L,\ (x, y) \mapsto xy$$

is a K-morphism and

$$\text{inv} : L \dashrightarrow L,\ x \mapsto \frac{1}{x}$$

is a K-rational map.

Proof. We identify L with a K-subalgebra of $\text{End}_K(L)$, via the algebra homomorphism that asigns to $a \in L$ the left-multiplication map $x \mapsto ax$. The multiplication on $\text{End}_K(L)$ is a K-polynomial map

$$\text{End}_K(L) \times \text{End}_K(L) \to \text{End}_K(L),$$

as can be seen by identifying $\text{End}_K(L)$ with a matrix algebra over K. Hence, its restriction $\text{mult} : L \times L \to L$ to L is also a K-polynomial map. The nonempty subset of invertible elements of $\text{End}_K(L)$ is a K-open subset, as it can be defined by the nonvanishing of the determinant function, which is a K-polynomial function. Finally, the inversion map is a K-rational map on $\text{End}_K(L)$ by Cramer's rule, defined on the invertible elements. Hence, its restriction $\text{inv} : L \dashrightarrow L$ to L is also a K-polynomial map. □

2.3. **Lemma.** *Let L/K be a finite extension and $f \in L(t)$. Then the L-rational map $f : L \dashrightarrow L$ is a K-rational map, i.e. after fixing a K-basis of L the map is given by $[L : K]$ fractions of polynomials in $[L : K]$ variables over K.*

Proof. First, we show this in the case $f \in L[t]$. Write $s = [L : K]$. Let us 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 $f_0, \ldots, f_d \in L$ and $d \in \mathbb{N}$. For $z \in L$ write $z = r_1\ell_1 + \cdots + r_s\ell_s$ with $r_1, \ldots r_s \in K$. One has

$$\begin{aligned} f(z) =& f(r_1\ell_1 + \cdots + r_s\ell_s) \\ =& \sum_{i=0}^{d} f_i \cdot (r_1\ell_1 + \cdots + r_s\ell_s)^i \\ =& \sum_{i=0}^{d} \sum_{\mu_1 + \cdots + \mu_s = i} \left(\frac{i!}{\mu_1! \cdots \mu_s!} \right) \ell_1^{\mu_1} \cdots \ell_s^{\mu_s} f_i \quad r_1^{\mu_1} \cdots r_s^{\mu_s}. \end{aligned}$$

We can consider this as a polynomial function over L in s variables evaluated at $(r_1, \dots, r_s)$. We can choose $\tilde{f}_1, \dots, \tilde{f}_s \in K[X_1, \dots, X_s]$ such that

$$f(r_1\ell_1 + \cdots + r_s\ell_s) = \tilde{f}_1(r_1, \dots, r_s)\ell_1 + \cdots + \tilde{f}_s(r_1, \dots, r_s)\ell_s.$$

Hence the map $f : L \to L$ is given by the polynomials $\tilde{f}_1, \dots, \tilde{f}_s$ 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 $f : L \dashrightarrow L$ is defined on $L \setminus h^{-1}(\{0\})$ and factors into

$$f : L \xrightarrow{(f,g)} L \times L \overset{\mathrm{id}\times\mathrm{inv}}{\dashrightarrow} L \times L \overset{\mathrm{mult}}{\dashrightarrow} L,$$

where $(g, h) : L \to L \times L, x \mapsto (g(x), h(x))$ and $\mathrm{id} \times \mathrm{inv} : L \times L \dashrightarrow L \times L, (x, y) \mapsto (x, y^{-1})$. Since it is a composition of K-rational maps, we conclude that f is a K-rational map. □

2.4. **Proposition.** *Let K be an infinite field and L/K a proper finite field extension that is not purely inseparable. Let $f \in L(t)$ be a rational function. If $f(z) \in K$ for every $z \in L$ where f is defined, then $f \in K$.*

Proof. First, we show that $f \in K(t)$. By (2.1) there exists $g \in L[t]$ and $h \in K[t]$ such that $f = \frac{g}{h}$.
Write $g = (g_0, g_1, \dots, g_d) \cdot (1, t, \dots, t^d)^{\mathrm{t}}$ with $g_0, \dots, g_d \in L$ for some $d \in \mathbb{N}$. Evaluation of this polynomial in distinct elements $\alpha_0, \dots, \alpha_d \in K \setminus h^{-1}(\{0\})$ yields a system of linear equations over k for the indeterminants $g_0, \dots, g_d$.

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

The Vandermonde matrix $(\alpha_i^j)_{0 \le i,j \le d}$ is invertible and defined over K. Therefore $g_0, \dots, g_d \in K$.
Now we are going to show that $\frac{g}{h} \in K$. Let $\beta \in L$ be a separable element over K and let σ be an automorphism of K_{sep}/K such that $\sigma(\beta) \neq \beta$. For any $(r_0, r_1) \in K \times K$ we have $g(r_0 + r_1\beta)\sigma(h(r_0 + r_1\beta)) = \sigma(g(r_0 + r_1\beta))h(r_0 + r_1\beta)$ by the assumption that $f(z) \in K$ for all $z \in L \setminus h^{-1}(\{0\})$. Thus $g(r_0 + r_1\beta)h(r_0 + r_1\sigma(\beta)) = g(r_0 + r_1\sigma(\beta))h(r_0 + r_1\beta)$. Since $K \times K$ is Zariski dense in $K_{\mathrm{alg}} \times K_{\mathrm{alg}}$, the polynomial identity $g(X + Y\beta)h(X + Y\sigma(\beta)) = g(X + Y\sigma(\beta))h(X + Y\beta)$ follows. We obtain that $g(X)h(Y) = g(Y)h(X)$ and consequently that $f = \frac{g}{h} \in K$, by showing that $X + Y\sigma(\beta)$ and $X + Y\beta$ are algebraically independent over K. Assume there exists a polynomial $P \in K[T_1, T_2]$ over K such that $P(X + Y\beta, X + Y\sigma(\beta)) = 0$. For any $a, b \in K_{\mathrm{alg}}$ there are $x, y \in K_{\mathrm{alg}}$ such that

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & \beta \\ 1 & \sigma(\beta) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

as the determinant of the 2×2 matrix does not vanish. Hence $P(a, b) = 0$ for all $(a, b) \in K_{\mathrm{alg}} \times K_{\mathrm{alg}}$ and thus $P(T_1, T_2) = 0$. □

2.5. **Proposition.** *Let L/K be a finite separable extension of infinite fields. Let $f \in L(t)$ be a nonconstant rational function. Let $W \subset L$ be any nonempty K-open subset on which f is defined. Then there exists $\alpha \in W$ such that $f(\alpha)$ is a primitive element of L/K.*

Proof. By (2.3), $f : L \dashrightarrow L$ defines a K-rational map. Note that the K-open subset W is dense in L, and thus irreducible with respect to its subspace topology. As f is continuous with respect to the subspace topology, the topological subspace $f(W) \subset L$ is irreducible. Assume that $f(\alpha)$ is not a primitive element of L/K for any $\alpha \in W$. Then the image of f lies in the finite union of the maximal proper subfields of L containing K, i.e. in the union of finitely many vector subspaces of L. None of those maximal proper subfields is contained in the union of the others. Thus the image of f is contained in one maximal proper subfield F of L containing K, as otherwise, we could write the irreducible image of f as the nontrivial finite union of the relatively closed subsets consisting of the intersections of the image of f with each of the maximal proper subfields.
By (2.4), we obtain the contradiction that $f \in F$, i.e. that f is a constant function. □

2.6. **Theorem.** *Let L/K be a separable finite extension of infinite field and V a K-variety such that V_L is unirational. Then there exists a nonsingular point $P \in V$ such that $K(P) = L$.*

Proof. We can assume that V is affine. Let V^{reg} denote the K-open quasiaffine subprevariety of V that consists of the nonsingular points of V ([4, I.5.3.]). Then V_L^{reg} is unirational. Let

$$\begin{aligned} \varphi : \mathbb{A}^n_L \dashrightarrow & V_L^{\mathrm{reg}} \\ (t_1, \dots, t_n) \mapsto & (\varphi_1(t_1, \dots, t_n), \dots, \varphi_m(t_1, \dots, t_n)) \end{aligned}$$

be a dominant L-rational map. Let $U \subseteq \mathbb{A}^n_L$ an L-open subset on which φ is defined. We can assume that φ_1 is nonconstant. As $L^n \cap U$ is dense in $\mathbb{A}^n$, we can find two L-rational points $P_1, P_2 \in U$, such that $\varphi_1(P_1) \neq \varphi_1(P_2)$. Let $\rho : \mathbb{A}^1_L \to \mathbb{A}^n_L$ denote an morphism whose image contains P_1, P_2. Then $\varphi_1 \circ \rho : \mathbb{A}^1_L \dashrightarrow \mathbb{A}^1_L$ is an L-rational function, i.e. given by a fraction of two polynomials in one variable over L. Thus it restricts to a K-rational function $L \dashrightarrow L$. Let $W \subset L$ denote a nonempty K-open subset of L such that $W \subset \rho^{-1}(U)$. By (2.5) then there exists $\alpha \in W$ such that $\varphi_1(\rho(\alpha))$ is a primitive element for L/K. Thus $L = K(\varphi_1(\rho(\alpha)), \dots, \varphi_1(\rho(\alpha)))$. □

2.7. **Corollary.** *Let L/K be a finite separable extension of infinite fields, and V a quadric over K. Then the following are equivalent:*

i) V_L is rational.
ii) V_L contains a rational point.
iii) There exists a K-valuation v on $K(V)$ with residue field $\kappa_v \hookrightarrow L$.
iv) There exists a K-valuation v on $K(V)$ with residue field $\kappa_v \cong L$.

Proof. The equivalences $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$ are long known, even without the assumption that K is infinite and without placing any restriction on the extension L/K, see e.g. [6, 3.3]. $(iv) \Rightarrow (iii)$ is obvious, and $(i) \Rightarrow (iv)$ follows from (2.6) as, for any regular point $P \in V$, its residue field $K(P)$ is the residue field of a K-valuation on $K(V)$. □

2.8. *Remark.* Note that refinement (2.7) also holds for other kind of varieties, such as for Severi-Braur varieties.

3. valuations, smooth points and sums of squares

Before we can apply the geometric observation of the previous section to conics, we prove a valuation theoretic result that will allow us to say something about the Pythagoras number of the function field of a curve from knowing the level of a nonreal residue field of one of its points.
Given a valuation v on a field K, we denote its valuation ring by $\mathcal{O}_v$, its maximal ideal by $\mathfrak{m}_v$, its residue field by κ_v. We say that v is *discrete* if the ordered value group $v(K^\times)$ is discrete.

3.1. **Proposition.** *Let v be a discrete valuation on K with nonreal residue field κ_v of characteristic different from 2. Then $p(K) > s(\kappa_v)$.*

Proof. Let $s = s(\kappa_v)$. Then there exist $x_0, \ldots, x_s \in \mathcal{O}_v{}^\times$ with $\bar{x}_0^2 + \ldots + \bar{x}_s^2 = 0$. We may assume that $v(x_0^2 + \ldots + x_s^2) \notin 2v(K^\times)$; in fact, if $v(x_0^2 + \ldots + x_s^2) \in 2v(K^\times)$, we simply replace x_s by $(x_s + t)$, where $t \in K$ is such that $v(t)$ is the minimal positive element in $v(K^\times)$. Hence, $v(x_0^2 + \ldots + (x_s + t)^2) = v((x_0^2 + \cdots + x_s^2) + (2x_s t + t^2)) = v(t) \notin 2v(K^\times)$. We claim that $x_0^2 + \ldots + x_s^2$ is not a sum of s squares in K. Suppose otherwise. Then there are $y_1, \ldots, y_s \in K$ with $y_1^2 + \ldots + y_s^2 = x_0^2 + \ldots + x_s^2$. We can assume that $v(y_1) \leq v(y_i)$ for $1 \leq i \leq s$. Denote $z_i = \frac{y_i}{y_1}$, then $z_i \in \mathcal{O}_v$ for $2 \leq i \leq s$. Since $v(y_1^2 + \ldots + y_s^2) \notin 2v(K^\times)$, it follows that $v(1 + z_2^2 + \ldots + z_s^2) > 0$. We obtain that $-1 = \overline{z}_2^2 + \ldots + \overline{z}_s^2$ in κ_v, contradicting $s = s(\kappa_v)$. □

Let K denote a field and $\mathcal{C}$ a curve over K. If $P \in \mathcal{C}$ is a smooth point, then $\mathcal{O}_P$ is a discrete valuation ring of rank one.

3.2. **Corollary.** *Let $\mathcal{C}$ be an irreducible algebraic curve over a real field K that is not hereditarily pythagorean. Then $p(K(C)) \geq 3$ if there exists a smooth point $P \in \mathcal{C}$ such that $K(P)$ is nonreal and $\sqrt{-1} \notin K(P)$.*

4. Function fields of conics

4.1. *Remark.* If $\mathcal{C}$ is a smooth projective conic over a field K with $\mathrm{char}(K) \neq 2$, then the conic can be assumed to be given by a homogeneous equation $Z^2 = aX^2 + bY^2$ for some $a, b \in K^\times$. Furthermore, given an ordering on K, one can assume that a, b are either both positive or both negative with respect to the ordering.
A conic, like any quadric, has the property that it is rational if and only if it has a rational point. ([7, X.4.1.])

4.2. **Theorem.** *Let K be a field. If there exists a function field F of a smooth conic over K with $p(F) = 2$ then K is hereditarily pythagorean or $\sqrt{-1} \in K$.*

Proof. Suppose $\sqrt{-1} \notin K$, in particularly $\mathrm{char}(K) \neq 2$. The conic $\mathcal{C}$ is given by $Z^2 = aX^2 + bY^2$ where $a, b \in K^\times$. First assume that K is finite. Then every quadratic form of dimension at least 3 over K is isotropic, hence the conic has a rational point and thus F/K is the rational function field $K(X)$. It follows that $-1 + X^2$ is a sum of 3 but not 2 squares by the second representation theorem ([7, IX.2.1.]). Suppose K is infinite and nonreal. Then at least one of the four biquadratic extensions $L = K(\sqrt{\pm a}, \sqrt{\pm b})$ does not contain $\sqrt{-1}$ and thus $p(L) \geq s(L) \geq 2$. Let $y \in L$ be such that $\ell_L(1 + y^2) = 2$. Then $M = L(\sqrt{-(1 + y^2)})$ has level 2. M/K is a separable field extension. If $\sqrt{a} \in M$, then $(1 : 0 : \sqrt{a}) \in \mathcal{C}$ is an M-rational point. If $\sqrt{b} \in M$, then $(0 : 1 : \sqrt{b}) \in \mathcal{C}$ is an M-rational point. If $\sqrt{-a}, \sqrt{-b} \in M$, then $(\sqrt{-b} : y\sqrt{-a}\sqrt{-(1 + y^2)ab}) \in \mathcal{C}$ is an M-rational point.

In any case, $\mathcal{C}$ has an M-rational point and we recall that since $\mathcal{C}$ is a conic, this implies that $\mathcal{C}$ is M-rational. Thus $\mathcal{C}$ has a point P with $K(P) = M$ by (2.6). Since $\sqrt{-1} \notin M$ it follows that $p(F) \geq 3$ by (3.2).
Finally, assume that K is a real field but not hereditarily pythagorean. Let L be a finite real extension of K that is not pythagorean. F is the function field of a smooth projective conic $\mathcal{C}$ over K. The conic $\mathcal{C}$ is given by $Z^2 = aX^2 + bY^2$ where $a, b \in K^\times$ such that ab is positive at a given ordering on L. This ordering extends either to $L(\sqrt{a}, \sqrt{b})$ or to $L(\sqrt{-a}, \sqrt{-b})$. At least one of these field extensions is real and by the Diller-Dress Theorem ([7, VIII.5.7]) not pythagorean. We can therefore assume without loss of generality that either $a, b \in L^{\times 2}$ or $-a, -b \in L^{\times 2}$.
Choose $y \in L$ such that $1 + y^2 \notin L^{\times 2}$ and consider $M = L(\sqrt{-(1+y^2)})$. If $a, b \in L^{\times 2}$ then $(\sqrt{a} : 0 : a)$ is an M-rational point of $\mathcal{C}$. If $a, b \in -L^{\times 2}$ then $(\sqrt{-b} : y\sqrt{-a} : \sqrt{ab}\sqrt{-(1+y^2)})$ is an M-rational point of $\mathcal{C}$. In any case, $\mathcal{C}$ has an M-rational point and thus is M-rational. By (2.6) $\mathcal{C}$ has a point P with $K(P) = M$. Since $\sqrt{-1} \notin M$ it follows that $p(F) \geq 3$ by (3.2). □

The following result on the Pythagoras number of function fields of conics over hereditarily pythagorean base fields was obtained in [12, Thm.1, Thm. 2 & Thm. 3].

4.3. **Theorem** (Tikhonov, Yanchevskiĭ)**.** *Let K be a hereditarily pythagorean field and let F be the function field of a smooth conic over K. Then $p(F) = 2$ if F is real. If F is nonreal, then $2 \leq p(F) \leq 3$ and $p(F) = 2$ if and only if K is euclidean*[1].

A field K is called *euclidean* if it is pythagorean and admits a unique ordering (i.e. if the set of squares are an ordering). It is called *hereditarily euclidean* if every finite real field extension of K is euclidean. One can show that a field that is hereditarily pythagorean and euclidean is already hereditarily euclidean. Together with our result (4.2) this yields the following two straight forward generalizations of (1.1).

4.4. **Corollary.** *Let K be a field with $\sqrt{-1} \notin k$. Then the following are equivalent.*
(i) There exists a smooth conic $\mathcal{C}/K$ with $p(K(\mathcal{C})) = 2$.
(ii) K is hereditarily pythagorean.
(iii) K is real and for every conic $\mathcal{C}/K$, we have $p(K(\mathcal{C})) = 2$ if $K(\mathcal{C})$ is real.

Proof. $(i) \Rightarrow (ii)$ follows from (4.2), $(ii) \Rightarrow (iii)$ is (4.3) and for $(iii) \Rightarrow (i)$ we simply choose a split irreducible conic $\mathcal{C}/K$. Then $K(\mathcal{C})$ is the rational function field over K and thus $K(\mathcal{C})$ is real. □

The condition in (4.3) when the nonreal function fields of conics have Pythagoras numer 2 was described in [12] by $|\mathrm{Br}(K(\sqrt{-1})/K)| = 2$. Note that if K is pythagorean, then this condition is equivalent to K being euclidean, as the quaternion algebras $(-1, a)_K$ for $a \in K^\times$ are exactly the ones that split over $K(\sqrt{-1})$ and there is a unique nonsplit such quaternion algebra if and only if K is euclidean. And since K was assumed to be hereditarily pythagorean, this is thus equivalent to the fact that K is hereditarily euclidean.
This part of the result has been strengthened in [1, (4.5)] where it was shown that if the Pythagoras number of the function field of $Y^2 = -(X^2 + 1)$ over some field K is 2, then either $\sqrt{-1} \in K$ or K is hereditarily euclidean, and in [1, (4.6)] it was observed as a consequence of a result of Elman and Wadsworth, that if K is

[1] in [12], the euclidean property is stated in a not immediately obvious way.

hereditarily euclidean then in fact every function field in one variable over K has Pythagoras number two. This yields the following characterization of hereditarily euclidean fields.

4.5. **Corollary.** *Let K be a field with $\sqrt{-1} \notin K$. Then the following are equivalent.*

(i) There is a nonreal function field F of a smooth conic over K with $p(F) = 2$.
(ii) K is hereditarily euclidean.
(iii) $p(F) = 2$ for every function field F/K in one variable.

Proof. $(i) \Rightarrow (ii)$ follows again from (4.2) together with (4.3) which says that $p(F) = 3$ for all nonreal function fields of smooth conics over a hereditarily pythagorean field that is not euclidean.
$(ii) \Rightarrow (iii)$ was observed in [1, (4.6)], and for $(iii) \Rightarrow (i)$ it is enough to see that $Y^2 = -(X^2 + 1)$ defines a smooth conic $\mathcal{C}$ such that $K(\mathcal{C})$ is nonreal. □

5. Function fields of generalized Fermat Type

In the following, we extend (4.2) and show for function fields F/K of generalized Fermat type, that $p(F) = 2$ implies that K is hereditarily pythagorean or that $\sqrt{-1} \in K$. As in the proof for the special case of conics, the idea is to assume that either K is nonreal and $\sqrt{-1} \notin K$, or that there exists a finite real extension of K that is not pythagorean, and to use these assumptions to construct a finite nonreal field extension M/K not containing $\sqrt{-1}$, that is the residue field of a point on an underlying regular curve. Unlike in the situation of a conic, it is not enough to make sure in the construction of M that the underlying curve contains an M-rational point, since this does not automatically imply that M is the residue residue field of some (possibly different) point on the curve.

5.1. **Proposition.** *Let K be an infinite field and L/K be a finite separable extension such that L is not pythagorean. 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 nonconstant K-rational function on L is nonempty. Moreover it 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 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. □

For a field K, we write $\pm K^{\times 2}$ for $K^{\times 2} \cup -K^{\times 2}$.

5.2. **Lemma.** *Let $u \in K^\times \setminus \pm K^{\times 2}$ and $n \in \mathbb{N}$. Let $\gamma \in K^{\mathrm{alg}}$ be such that $\gamma^n = u$ and $M = K(\gamma)$. Then $K^\times \cap M^{\times 2} = K^{\times 2} \cup uK^{\times 2}$.*

Proof. The statement needs to be shown only for $n = 2^r$ with $r \geq 1$. As $-u \notin K^{\times 2}$ and thus $-u \notin 4K^{\times 4}$, the polynomial $T^{2^r} - u$ is irreducible by [8, Chap. VI, (9.1)]. Write $d = \gamma^2$ and $L = K(d)$. 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 $-u$. As $-u \notin K^{\times 2}$, 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. □

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

Proof. Let $r \in \mathbb{N}$ be maximal such that 2^r divides m and $v \in K^{\times 2^r}$. Let $u \in K$ such that $u^{2^r} = v$. Set $n = \frac{m}{2^r}$
If 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 $u \notin -K^{\times 2}$ since $-u \notin K^{\times 2}$ by the maximality of r and the fact that $(-u)^{2^r} = v$.
Let $y \in K^{\mathrm{alg}}$ such that $y^n = u$ and thus $y^m = v$. In the case where n is even it follows by (5.2) that $-1 \notin K(y)^{\times 2}$, since $u \in \pm K^{\times 2}$. If n is odd, then $K(y)$ is an odd degree extension of K and it follows trivially that $-1 \notin K(y)^{\times 2}$. □

5.4. **Proposition.** *Let K be a field with $-1 \notin K^{\times 2}$. 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 with $-1 \notin M^{\times 2}$ and $x, y \in M$ such that $M = K(x, y)$, $x^n = u$ and $y^m = v$.*

Proof. Fix $x \in K^{\mathrm{alg}}$ such that $x^n = u$. Then $-1, -v \notin K(x)^{\times 2}$ by (5.2), as $-1, -v \notin K^{\times 2} \cup uK^{\times 2}$. Then by (5.3) there exists $y \in K^{\mathrm{alg}}$ such that $y^m = v$ and $-1 \notin M^{\times 2}$, where $M = K(x, y)$. □

5.5. **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 any two integers $n, m \geq 1$ there exists a finite extension M/L with $-1 \notin M^{\times 2}$ and $x, y \in M$ such that $1 = ax^n + by^m$ and $M = K(x, y)$. If moreover n or m is even, we can choose M nonreal.*

Proof. By (5.1) there exists $\xi \in L$ with $\xi^2 + 1 \in \sum L^2 \setminus L^{\times 2}$ and $L = K(\xi^2)$, and further $\sigma \in \sum L^2 \setminus L^{\times 2}$ with $L = K(\sigma)$ and $\sigma + 1 \in \sum L^2 \setminus L^{\times 2}$.
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 $-u, u \notin L^{\times 2}$, $-v \notin L^{\times 2}$ and $-uv = \frac{1}{ab}\frac{\sigma+1}{\sigma^2} \notin L^{\times 2}$. 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 $u, -u \notin L^{\times 2}$, $-v \notin L^{\times 2}$ and $-uv \notin L^{\times 2}$ and $1 = au + bv$.
In the case where $-a, b \in L^{\times 2}$ set $u = \frac{\sigma+1}{a}$ and $v = \frac{-\sigma}{b}$. Then $u, -u \notin L^{\times 2}$, $-v \notin L^{\times 2}$ and $-uv \notin L^{\times 2}$ and $1 = au + bv$.
In the case where $a, -b \in L^{\times 2}$ set $u = \frac{-\sigma}{a}$ and $v = \frac{\sigma+1}{b}$. Then $u, -u \notin L^{\times 2}$, $-v \notin L^{\times 2}$ and $-uv \notin L^{\times 2}$ and $1 = au + bv$.
In each case, by (5.4) there exist $x, y \in L^{\mathrm{alg}}$ 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 $1 = ax^{2^r} + by^{2^s}$ as $1 = au + bv$. Set $M = L(x, y)$.

Now suppose n or m is even. By symmetry we can assume that n is even. Then $x^n = u$ is a square in M but also - by the choices of u in each case - a negative sum of squares in M. Thus M is nonreal in this case. □

5.6. **Theorem.** *Let K be field with $\sqrt{-1} \notin K$ and F/K a function field of generalized Fermat type. Then $p(F) = 2$ only if K is hereditarily pythagorean.*

Proof. The function field F/K if is the function field of a smooth affine curve $1 = aX^n + bY^m$ for some $a, b \in K^\times$ and $n, m \in \mathbb{N}$ not divisible by $\mathrm{char}(K)$. Let us first consider the case where n and m are odd. Then F is clearly an odd degree extension of the rational function field $K(X)$. Then $p(K(X)) \leq p(F) \leq 2$ by Springer's theorem [7, VII.2.7] applied to all quadratic forms $\langle -1, -1, \sigma \rangle$ with $\sigma \in \sum K(X)^{\times 2}$. Thus $p(K(X)) = 2$, and the claim follows from (1.1). Thus assume that n or m are even.
We first show that K is real. Assume that K is nonreal. If $-a \notin K^{\times 2}$, choose $x \in K^{\mathrm{alg}}$ such that $x^n = \frac{1}{a}$ and $\sqrt{-1} \notin K(x)$ as in (5.3). Then $(x, 0)$ is a point of the curve. If $-b \notin K^{\times 2}$ we can proceed analogous, so we consider the case where $-a, -b \in K^{\times 2}$. Choose $z \in K$ such that $z^2 + 1 \notin K^{\times 2}$. Choose again $x \in K^{\mathrm{alg}}$ such that $x^n = \frac{z^2}{-a}$ and $\sqrt{-1} \notin K(x)$. Then $\frac{1}{b} \notin K(x)^{\times 2}$ and we also find some $y \in K^{\mathrm{alg}}$ such that $y^m = \frac{-1}{b}$ and $\sqrt{-1} \notin K(x, y)$ as in (5.4). Note that $P = (x, y)$ is a point on $\mathcal{C}$. Then $p(F) > s(K(P)) \geq 2$ by (3.2).Contradiction.
Hence K is real. Suppose there exists a finite real extension L/K that is not pythagorean. We can assume that $a, b \in L^{\times 2} \cup -L^{\times 2}$ since at least one of the four biquadratic extensions $L(\sqrt{\pm a})(\sqrt{\pm b})$ is real and nonpythagorean by the Diller-Dress Theorem [7, VIII.5.7]. By (5.5) there exists a point $P \in \mathcal{C}$ such $\sqrt{-1} \notin K(P)$ and $K(P)$ is nonreal. Thus $p(\tilde{F}) > s(K(P)) \geq 2$ by (3.2). Contradiction. □

References

[1] K.J. Becher, J. Van Geel. *Sums of squares in function fields of hyperelliptic curves*, Math. Z. 261:829–844 (2009).
[2] E. Becker. *Hereditarily-Pythagorean fields and orderings of higher level*, Monografias de Mathematica 29, Rio de Janeiro, 1978.
[3] S. Bosch, W. Lütkebohmert, M. Raynaud. *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, 21. Berlin etc.: Springer-Verlag. x, 325 p. (1990).
[4] R. Hartshorne. *Algebraic Geometry*, Graduate Texts in Mathematics, 52. New York-Heidelberg-Berlin: Springer- Verlag. XVI, 1983.
[5] D.W. Hoffmann. *Pythagoras numbers of fields*, J. Amer. Math. Soc. 12 (3): 839–848 (1999).
[6] M. Knebusch, *Generic splitting on quadratic forms. I*, Proc. London Math. Soc. 33: 65–93 (1976).
[7] T.Y. Lam. *Introduction to Quadratic Forms over Fields*, AMS Graduate Studies in Mathematics Vol. 67, Rhode Island, 2004.
[8] S. Lang. *Algebra - revised third edition*, Graduate Texts in Mathematics 211, Springer, New York 2002.
[9] A. Pfister. *Quadratic Forms with Applications to Algebraic Geometry and Topology*, London Math. Soc. Lecture Note Series 217.
[10] H. Stichtenoth, *Algebraic function fields and codes. 2nd ed.*, Graduate Texts in Mathematics 254 , Springer, Berlin 2009.
[11] S.V. Tikhonov, J. Van Geel, V.I. Yanchevskiĭ. *Pythagoras numbers of function fields of hyperelliptic curves with good reduction*, Manuscripta Math. 119: 305–322 (2006).
[12] S.V. Tikhonov, V.I. Yanchevskiĭ. *Pythagoras numbers of function fields of conics over hereditarily pythagorean fields*, Dokl. Nats. Akad. Nauk Belarusi 47(2): 5–8 (2003).

Universität Konstanz, Fachbereich für Mathematik und Statistik Universitätsstr. 10, 78457 Konstanz, Germany
E-mail address: david.grimm@uni-konstanz.de