PYTHAGORAS NUMBERS OF FUNCTION FIELDS OF HYPERELLIPTIC CURVES WITH GOOD REDUCTION

SERGEY V. TIKHONOV, JAN VAN GEEL AND VYACHESLAV I. YANCHEVSKIĬ

Abstract. It is shown that the Pythagoras number of a real function field of a hyperelliptic curve C with good reduction defined over the real formal power series field is equal to 2. A main tool in the proof is the explicit description of the Brauer group of C. If the function field of such a curve is non-real then it is shown that its Pythagoras number is 3.

1. Introduction

Let k be a field and let $\sum k^2$ denote the set of non-zero elements in k which can be written as a sum of squares in k. The smallest natural number $p(k)$ such that every element in $\sum k^2$ can be written as a sum of p squares in k is called the Pythagoras number of k. (We refer to [14, Chap.7, definition 1.1] for a more formal definition.) The study of the Pythagoras number of a field finds its origin in E. Artin's solution of the 17th problem of Hilbert and in the research that emerged from this work. Hilbert's problem reads as follows; *Let $K = \mathbb{R}(x_1, \dots, x_n)$. Let $f \in K$ be a positive semi-definite function in K (i.e. $f(a) \geq 0$ for all $a \in K^n$). Is it true that f is a sum of squares in K?* Artin showed that the answer is positive and later Pfister obtained a quantitative result namely that a positive semi-definite function in K is a sum of 2^n squares. Pfister's result implies that $p(K) = 2^n$, cf. [13, Chap. 6].

The theory of real fields (also called formally real fields, these are fields admitting an ordering or equivalently fields in which -1 is not equal to a sum of squares) created by E. Artin and O. Schreier, is fundamental for the solution of Hilbert's 17th problem and provides the proper algebraic setting for the above mentioned results. (We refer to [11] for an introduction to this theory and its further developments.) Real fields with no real algebraic extension are called real closed fields. These can be characterized in different ways (cf. [11]). For instance R is a real closed field if and only if one of the following equivalent statements holds;

(a) R admits a unique ordering and the set of positive elements for this ordering is exactly the group of squares, R^{*2} in R.

(b) An algebraic closure R^a of R is a finite extension of R.

Date: October 5, 2004.

This research was supported by INTAS-Project INTAS-99-00817.

The first and the third author were partially supported by RTN Network HPRN-CT-2002-00287 and by the Fundamental Research Foundation of Belarus.

Acknowledgement. Tikhonov and Yanchevskiĭ are grateful to Ghent University (a substantial part of this work was done during their visit to Ghent in 2002).

Property (b) can be replaced by the at first sight stronger statement that the Galois group $\mathrm{Gal}(R^a/R(\sqrt{-1}))$ is trivial.
The above mentioned results of Artin and Pfister, if one formulates them appropriately, hold for any function field of finite transcendence degree over a real closed field. For instance (see [14, Chap.7, 1.4 (4)]), let R be a real closed field and K a field of transcendence degree n over R then $p(K) \leq 2^n$.
The Pythagoras number has been studied for various other classes of fields, a survey of known results can be found in chapter 7 of Pfister's book [14]. In many cases it turns out that the determination of the Pythagoras number is closely related to the arithmetic or the geometry of the field. (For instance the bounds for the Pythagoras number of fields of transcendence degree n over a number fields obtained by Colliot-Thélène and Jannsen (see [14, page 100, 101]) are based on very deep results, namely on a generalized version of Kato's local-global principle and on the Milnor conjectures proved by Orlov, Vishik and Voevodsky.) In this paper we present an other example of this phenomenon. An example of a simpler nature. We consider function fields of curves over the field $\mathbb{R}((t))$ of formal power series over the real numbers. It turns out that the Pythagoras number depends on a cohomological invariant namely the Brauer group of the curve.
There are two motivation to study the Pythagoras number of such fields. First if one considers the Galois theoretic characterization of real closed fields, the "next" class of fields to consider are the fields K for which $\mathrm{Gal}(K^a/K)$ has a simple structure. (This point of view can be found in the work of different authors, see for instance [10], [6], [7]. In [6, Chap. III, theorem 1] the following result is obtained

Theorem 1.1. [6] *Let K be a real field, K^a a fixed algebraic closure of K. Then the Galois group* $\mathrm{Gal}(K^a/K(\sqrt{-1}))$ *is abelian if and only if any real extension (in K^a) of K is pythagorean.*

Here pythagorean means that for all $a, b \in K$, $a^2 + b^2 = c^2$ for some $c \in K$. So in pythagorean fields every sum of squares is a square. Fields satisfying the equivalent properties of the theorem are called hereditarily pythagorean fields. In [6, Chap. III, theorem 4] the following characterization of these fields is given; A field K is hereditarily pythagorean if and only if the Pythagoras number of $K(x)$, the rational function field in one variable over K, is equal to 2. The problem of determining the Pythagoras of function fields of curves over hereditarily pythagorean fields becomes now very natural. In [21] the first and the third author obtained the following result for the function field of a conic over a hereditarily pythagorean field.

Theorem 1.2. [21, Theorem 3] *Let C be a conic defined over a hereditarily pythagorean field K such that the function field $K(C)$ is a real field. Then $p(K(C)) = 2$.*

Theorem 1.3. [21, Theorems 1 and 2] *Let C be a conic defined over a hereditarily pythagorean field K such that the function field $K(C)$ is a non-real field. Then $p(K(C)) = 2$ if and only if the order of the relative Brauer group,* $\mathrm{Br}(K(\sqrt{-1})/K)$*, is equal to 2. If* $|\mathrm{Br}(K(\sqrt{-1})/K)| > 2$ *then $p(K(C))$=3.*

The proof of theorem 1.3 relies on the fact that for function fields of curves over hereditarily pythagorean fields it turns out that the totally positive elements which are not sums of two squares correspond to non-trivial elements in $\mathrm{Br}(C)$, the Brauer group of the curve (cf. lemma 2.7). In the case C is a conic such elements are induced by non-trivial elements in $\mathrm{Br}(K(\sqrt{-1})/K)$. For general curves over hereditarily pythagorean fields we do not have enough information on the Brauer group of C to calculate the Pythagoras number of the function field. However a basic example of a hereditarily pythagorean field is the field $\mathbb{R}((t))$ (cf. [6, page 108])). The results of [21] (theorems 1.2 and 1.3) imply that for a conic C, $p(\mathbb{R}((t))(C) = 2$ if and only if $\mathbb{R}((t))(C)$ is a real field, this since $|\mathrm{Br}(\mathbb{C}((t))/\mathbb{R}((t)))| = |\mathrm{Br}(\mathbb{R}((t))| = 4$. Now it is possible, using a general theorem proved in [15], to determine the Brauer group of hyperelliptic curves with good reduction (cf. definition 2.3) over $\mathbb{R}((t))$. Using this we obtained the main result of this paper,

Theorem 1.4. *(cf. Theorem 3.8 and theorem 4.1). Let C be a hyperelliptic curve over $\mathbb{R}((t))$ with good reduction. If $\mathbb{R}((t))(C)$ is a real field then $p(\mathbb{R}((t))(C)) = 2$. If $\mathbb{R}((t))(C)$ is a non-real field then $p(\mathbb{R}((t))(C)) = 3$.*

The second motivation for studying the Pythagoras number of function fields of curves over $\mathbb{R}((t))$, comes from the study of the structure of central simple algebras of exponent 2 over such fields. In [4] the structure of central simple algebras of exponent 2 over the rational function field $\mathbb{R}((t))(x)$ is studied . Especially so called Ω-algebras were considered. These are algebras that are trivial over all real closures of the function field. The results obtained there rely strongly on the fact that $p(\mathbb{R}((t))(x)) = 2$. Ω-algebra's of exponent 2 turn up naturally in questions concerning quadratic forms. In [5] Becher proved that if K is a field with Pythagoras number ≤ 2 such that the u-invariant of $K(\sqrt{-1})$ is 4 then the u-invariant of K also equals 4. (The u-invariant of a real field is the maximal dimension of anisotropic torsion quadratic forms. We refer to [14, Chap.8] for more details on this invariant.) Becher's result together with our theorem 1.4 implies that if C is a hyperelliptic curve with good reduction over $\mathbb{R}((t))$ such that $\mathbb{R}((t))(C)$ is formally real then the u-invariant of $\mathbb{R}((t))(C)$ is 4.

In section 2 we fix some conventions and notations and we recall some facts on Brauer groups, and on hyperelliptic curves and there function fields. We end the section with the lemma relating the Pythagoras number of $\mathbb{R}((t))(C)$ to the Brauer group of the curve. In section 3 we give a calculation of the Brauer group of a hyperelliptic curves with good reduction over $\mathbb{R}((t))$ in the case the function field $\mathbb{R}((t))(C)$ is real. And we prove theorem 1.4 in this case. In section 4 we prove theorem 1.4 in the case $\mathbb{R}((t))(C)$ is a non-real field.

We restricted ourself to function fields of curves over the real formal power series field $\mathbb{R}((t))$, the example we constantly worked with. However the proofs of the main results work in greater generality. The real number field $\mathbb{R}$ can be replaced by any real closed field. Actually the results also hold for function fields of curves over henselian discrete valued fields with real closed residue field. All arguments work in that generality, one only has to replace the field $\mathbb{R}$ by the residue field and the parameter t by the uniformizing element for the discrete valuation.

The authors are grateful to Karim Becher for various helpful discussions, he also indicated to us the general result of Elman and Lam on the Pythagoras number under quadratic totally positive extension which settles one case in the proof of our main theorem.

2. Notations and preliminary results

We first fix some conventions and notations.

Let A be an abelian group, $n \in \mathbb{N}$, $n > 1$, the n-torsion subgroup of A, i.e. the kernel of the morphism defined by multiplication with n, is denoted with ${}_nA$. (In this paper we are mainly dealing with 2-torsion subgroups.)

Let G be a profinite group and B a discrete G-module, then $H^i(G, B)$ denotes the i-th cohomology group of G with coefficients in B. For a subgroup $H \subset G$ of finite index, $\mathrm{res}^G_H : H^i(G, B) \to H^i(H, B)$ denotes the restriction map and $\mathrm{cor}^H_G : H^i(H, B) \to H^i(G, B)$ the corestriction map (cf. [18, chap. VII]). We will work with Galois cohomology. Let k be a field of characteristic zero, then $\overline{k}$ denotes the algebraic closure of k and $G_k = \mathrm{Gal}(\overline{k}/k)$ denotes the absolute Galois group of k. If l/k be a finite field extension then l is the fixed field of a subgroup of finite index H in G_k and we will write $\mathrm{res}_{l/k}$ for the restriction map $\mathrm{res}^{G_k}_H$ and $\mathrm{cor}_{l/k}$ for the corestriction map $cor^H_{G_k}$.

The Brauer group of k, $\mathrm{Br}(k)$, is a Galois cohomological invariant which plays a key role in the proof of our main result. $\mathrm{Br}(k)$ is the abelian group of Brauer equivalence classes of finite dimensional central simple algebras over k, where central simple algebras A and B over k are called equivalent if and only if there is an isomorphism of matrix algebras $M_n(A) \cong M_m(B)$ for some natural numbers n, m. It is well known that $\mathrm{Br}(k) \cong H^2(G_k, \mathbb{G}_m)$, where $\mathbb{G}_m$ is the multiplicative group defined by $\mathbb{G}_m(K) = K^*$ for all finite field extensions K/k. We will use the following terminology. By an algebra A over k we will mean a central simple k-algebra unless stated otherwise. If we say that A is trivial we mean that the Brauer class $[A]$ is trivial in $\mathrm{Br}(k)$. Let R be a commutative ring then R^* denotes the group of units in R and R^{*2} the subgroup of elements which are squares in R. The Brauer group of R consists of equivalence classes of Azumaya algebras over R with respect to Morita equivalence (cf. [3]).

Let k be a field of characteristic zero and let X be an irreducible smooth projective variety over k, then $k(X)$ denotes the function field of X. For a field extension K/k, we write $X(K)$ for the set of K- rational points on X. Let v be a discrete valuation on $k(X)$, $\mathcal{O}_v$ the associated valuation ring and $k(v)$ its residue field. There exists a ramification homomorphism (cf. [16, chap 5])

$$\partial_v : \mathrm{Br}(k(X)) \to \mathrm{Hom}_{cont}(G_{k(v)}, \mathbb{Q}/\mathbb{Z}) = H^1(G_{k(v)}, \mathbb{Q}/\mathbb{Z}).$$

A central simple algebra over $k(X)$ is said to be ramified in v if and only if $\partial_v([A]) \neq 0$. The kernel of ∂_v can be identified with $\mathrm{Br}(\mathcal{O}_v)$, i.e. the kernel is the image of the natural monomorphism $0 \to \mathrm{Br}(\mathcal{O}_v) \to \mathrm{Br}(k(X))$ induced by the inclusion map $\mathcal{O}_v \subset k(X)$, cf. [2, page 289].

We need to calculate the ramification of central simple algebras A over $k(X)$ of exponent 2. So we consider the restriction of ∂_v to the 2-component ${}_2\mathrm{Br}(k(X))$. This map takes values in $H^1(G_{k(v)}, \mathbb{Z}/2\mathbb{Z}) \cong k(v)^*/k(v)^{*2}$ (the isomorphism is canonical since $k(X)$ contains all the 2th-roots of unity). By a famous theorem of Merkurjev algebras of exponent 2 are equivalent to tensor products of quaternion algebras. For a quaternion algebra $(a,b)_{k(X)}$ the ramification is given by the formula (cf. [16]),

$$\partial_v((a,b)_{k(X)}) = (-1)^{v(a)v(b)}\overline{\left(\frac{a^{v(b)}}{b^{v(a)}}\right)} \in k(v)^*/k(v)^{*2}.$$

The ramification map factors over $\mathrm{Br}(k(X)_v)$, where $k(X)_v$ is the completion of $k(X)$ with respect to the valuation v. Since the characteristic of k is zero, such a completion is of the form $k(v)((z))$, where z is a uniformizing element in $\mathcal{O}_v$.
We consider the special case where $X = C$ is an irreducible smooth projective curve over k. There is a one to one correspondence between the discrete valuation rings in $k(C)$ and the closed points of C, viewed as a scheme over k. A central simple algebra over $k(C)$ is said to be ramified in a closed point of C if it is ramified with respect to the corresponding discrete valuation. It is known that the unramified part of the Brauer group (cf. [8]), $\mathrm{Br}_{nr}(k(C)) := \cap_v \mathrm{Br}(\mathcal{O}_v)$ can be identified with the Brauer group of the curve in the sense of Grothendieck (i.e. $\mathrm{Br}(C) = H^2_{et}(C, \mathbb{G}_m)$). So $\mathrm{Br}(C)$ (using this identification) consists exactly of the classes of central simple algebras over $k(C)$ that are unramified in all the points of C. Our results concerning the Pythagoras number of function fields of hyperelliptic curves depend on the calculation of $\mathrm{Br}(C)$ for such curves.
We also review some facts concerning hyperelliptic curves over a field k.
We denote by $\mathbb{P}^n_{\overline{k}}$ the n-dimensional projective space over an algebraic closure $\overline{k}$ of k. A point of $\mathbb{P}^n_{\overline{k}}$ with homogeneous coordinates $x_0, \ldots, x_n$ will be denoted by $(x_0 : x_1 : \cdots : x_n)$. Also, let $\mathbb{A}^n_{\overline{k},i}$, $i = 0, \ldots, n$, be the affine subsets of $\mathbb{P}^n_{\overline{k}}$ consisting of the points whose i-th homogeneous coordinate is nonzero. For any polynomial $f(x) \in k[x]$ of degree m and without multiple roots, let C_0 be the affine curve over k defined by the equation $y^2 = f(x)$, then the genus of C_0 is:

$$g = \begin{cases} (m-1)/2 & \text{if } m \text{ is odd,} \\ (m-2)/2 & \text{if } m \text{ is even.} \end{cases}$$

The projective closure C of the image of C_0 under the mapping

$$\phi : C_0 \longrightarrow \mathbb{P}^{g+2}_{\overline{k}},\ (x,y) \mapsto (1 : x : x^2 : x^3 : \cdots : x^{g+1} : y)$$

is called the hyperelliptic curve corresponding to the equation $y^2 = f(x)$. It is known that C is a smooth, irreducible projective curve and that

$$C = \begin{cases} (C \cap \mathbb{A}^{g+2}_0) \cup P_\infty & \text{if } m \text{ is odd,} \\ (C \cap \mathbb{A}^{g+2}_0) \cup P_{\infty_1} \cup P_{\infty_2} & \text{if } m \text{ is even.} \end{cases}$$

Here $P_\infty = (0 : 0 : \cdots : 1 : 0)$, $P_{\infty_1}, P_{\infty_2} = \{(0 : 0 : \cdots : 1 : \pm\sqrt{a_m})\} \in \mathbb{A}^{g+2}_{g+1}$, where $a_m \in k$ is the leading coefficient of $f(x)$. The map ϕ gives an isomorphism between the affine curves C_0 and $C \cap \mathbb{A}_0^{g+2}$. We denote by ψ_C the hyperelliptic projection given by

$$\begin{array}{rcl} \psi_C : C & \longrightarrow & \mathbb{P}^1 \\ P & \mapsto & \left\{ \begin{array}{ll} (x:1) & \text{if } P = (1 : x : x^2 : x^3 : \cdots : x^{g+1} : y), \\ (1:0) & \text{if } P \notin \mathbb{A}^{g+2}_{\overline{k},0}. \end{array} \right. \end{array}$$

The ramification points of the double cover $\psi_C : C \to \mathbb{P}^1_k$ are called the Weierstrass points of the hyperelliptic curve C. The hyperelliptic projection ψ_C, which is defined over k, induces embeddings of the rational function field $k(x)$ in the function field $k(C)$ of C.

$$\psi_C^* : k(x) \hookrightarrow k(C),$$

i.e.

$$\psi_C^* : k(x) \hookrightarrow k(x)(\sqrt{f(x)}).$$

Let l/k be an algebraic extension then we also obtain an embedding

$$\psi_{C,l} : l(x) \hookrightarrow l(C),$$

by taking the tensor product with l. We will further identify $k(x)$ with the subfield $\psi_C^*(k(x))$ of $k(C)$. Let v be a discrete valuation on $k(C)$, we need an explicit description of the completion $k(C)_v$. We recall how this can be obtained. We start with the rational function field $k(x)(= k(\mathbb{P}^1_k))$. A discrete valuation v on $k(x)$ is either induced by monic irreducible polynomials $h(x) \in k[x]$ (these are the valuations corresponding to the closed points in $\mathbb{A}^1_k(= \mathbb{A}^1_{k,1})$) or $v = v_\infty$ (the valuation corresponding to the point at infinity of $\mathbb{P}^1_k$). In the first case $h(x)$ is a uniformizing element for v and the completion of $k(x)$ with respect to v is of the form $k(\theta)((f(x)))$ where θ is a root of $h(x)$. The element x^{-1} is a uniformizing element for v_∞ and the completion with respect to this valuation is of the form $k((x^{-1}))$. Now $k(C) = k(x)(\sqrt{f(x)})$ is a quadratic extension of $k(x)$, its discriminant is equal to $4f(x)$. The discrete valuations on $k(C)$ are all obtained from extending discrete valuations on $k(x)$. Let v be a valuation on $k(x)$ corresponding to the irreducible polynomial $h(x)$. If $h(x)$ does not divide $f(x)$, then v extends (up to equivalence) to one or two valuations w on $k(C)$, unramified over $k(x)$. Let w be such an extension of v, then $h(x)$ is a uniformizing element of w. The residue field of w is equal to $k(\theta)(\sqrt{f(\theta)})$ and the completion $k(C)_w$ is of the form $k(\theta)(\sqrt{f(\theta)})((h))$. (Note that the residue field of w is a quadratic extension of the residue field of v if and only $f(\theta) \notin k(\theta)^{*2}$, this is exactly the case when w is the unique extension of v to $k(C)$.) If $f(x) = h(x)g(x)$, then (since $f(x)$ has no multiple roots in $\overline{k}$) $\gcd(g(x), h(x)) = 1$, so $g(x)$ is a unit in $\mathcal{O}_v$. In this case the valuation v ramifies in $k(C)$, so there is (up to equivalence) a unique valuation w on $k(C)$ extending v. The residue field of w is equal to the residue field of v, so it is $k(\theta)$. The completion $k(C)_w$ is a quadratic extension of $k(x)_v$, $k(C)_w = k(\theta)((h))(\sqrt{g(\theta)h(x)})$.

The extension of the valuation v_∞ of $k(x)$ to $k(C)$ depends on the degree m of f. If m is odd there is (up to equivalence) a unique valuation w_∞ extending v_∞ (the valuation corresponding to the unique k-rational point at infinity, $P_\infty \in C(k)$. This extension is ramified over $k(x)$ so the residue field is equal to $k = k(v_\infty)$, and the completion is of the form $k((\sqrt{x^{-1}}))$. If m is even and a_m (the leading coefficient of f) is a square in k then

v_∞ extends to two different valuations w_{∞_1} and w_{∞_2} on $k(C)$, corresponding respectively to the k-rational points P_{∞_1} and P_{∞_2}, the residue field of w_i are equal to k. If a_m is not a square in k then there is only one extension w_∞ (up to equivalence) of v_∞, its residue field is $k(\sqrt{a_m})$. In any case, if m is even, x^{-1} is a uniformizing element for the valuation extending v, and the completion of $k(C)$ with respect to such a valuation is of the form $k(\sqrt{a_m})((x^{-1}))$.
For $\overline{k}(C)$ there is a one to one correspondence between the rational points of the curve, i.e. the elements $P \in C(\overline{k})$ and the discrete valuations v_P on $\overline{k}(C)$. The discrete valuations of $k(C)$ can therefore also be viewed as the restriction of valuations v_P. We reformulate in the following lemma the above facts concerning the completions of $k(C)$.

Lemma 2.1. *Let C be a hyperelliptc curve over k as defined above. Let $P \in C(\overline{k})$ such that $\psi_C(P) = (a:1)$, and let $h(x)$ be a minimal polynomial of a over k. Then*

$$k(C)_P \cong \begin{cases} k(a)(\sqrt{f(a)})((h)) & \text{if } h(x) \text{ does not divide } f(x), \\ k(a)((h))(\sqrt{g(a)h(x)}) & \text{if } f(x) = g(x)h(x); \end{cases}$$

we embed $k(C)$ in $k(C)_P$ by interpreting x as a power series in $k(a)((h))$ such that $x \equiv a \bmod h(x)$.
For $P = P_\infty$ in case m is odd we have

$$k(C)_{P_\infty} \cong k((\sqrt{x^{-1}})),$$

For $P = P_{\infty_1}$ or P_{∞_2} we have

$$k(C)_{\mathbb{P}_{\infty_i}} \cong k((x^{-1}))(\sqrt{a_m}), \quad i = 1, 2.$$

$k(C)$ is viewed as a subfield of $k(C)_{P_\infty}$ (respectively $k(C)_{P_{\infty_i}}$) by interpreting x as the inverse of the series x^{-1}.
The Weierstrass points of C are the points $(\theta, 0)$ with θ a root of $f(x)$ in the case m is even and the same points plus the point at infinity, P_∞, in case m is odd.

We now turn to the function fields $\mathbb{R}((t))(C)$ of hyperelliptic curves C defined over the field of formal power series over the real numbers. As we have seen we can define such a curve C by an equation of the form $y^2 = f(x)$, where $f(x)$ is a polynomial over $\mathbb{R}((t))$ without multiple roots. Since the ground field is $\mathbb{R}((t))$ we can normalise the equation of C even further.

Lemma 2.2. *Let C_0 be an affine plane curve defined by the equation $y^2 = f(x)$, where $f(x)$ is a polynomial without multiple roots over $\mathbb{R}((t))$. Then C_0 is $\mathbb{R}((t))$-isomorphic to an affine plane curve given by the equation $y^2 = \alpha f_0(x)$, where $f_0(x)$ is a monic polynomial with coefficients in $\mathbb{R}[[t]]$ without multiple roots, and $\alpha \in \mathbb{R}[[t]]$. Without loss of generality we may assume that $\alpha \in \{1, -1, t, -t\}$; moreover, if $deg f(x)$ is odd we may assume that $\alpha = 1$.*

Proof: This follows directly from the fact that every element $\sum_{i=0}^{\infty} a_i t^i$ of $\mathbb{R}[[t]]$ with $a_0 > 0$ is a square in $\mathbb{R}[[t]]$. □

We fix the following notation. Let $g(x) = \sum_{i=0}^{n} s_i x^i \in \mathbb{R}[[t]][x]$ be any polynomial over $\mathbb{R}[[t]]$. We denote the reduction of g modulo t by $\overline{g}(x) = \sum_{i=0}^{n} \overline{s_i} x^i \in \mathbb{R}[x]$, where $\overline{s}$ is the image of $s \in \mathbb{R}[[t]]$ under the canonical map $\mathbb{R}[[t]] \to \mathbb{R}$.

Definition 2.3. *A hyperelliptic curve C defined over $\mathbb{R}((t))$ has good reduction if it corresponds to a curve defined by an equation of the form $y^2 = \alpha f_0(x)$ in accordance with lemma 2.2, where $\alpha \in \{1, -1\}$ and $\overline{f}(x) \in \mathbb{R}[x]$ is a polynomial without multiple roots.*

Remark 2.4. The fact that every unit $z(t) \equiv a_0 \bmod t$ in $\mathbb{R}[[t]]$ is an n-the power in $\mathbb{R}[[t]$ for every odd number n and the fact that every unit $u(t) \equiv b_0 \bmod t$, with $b_0 > 0$ is a m-th power for every $m \geq 1$ implies that all finite extensions of $\mathbb{R}((t))$ are of the form $\mathbb{R}((t))(\sqrt[m]{\pm t})$ or of the form $\mathbb{C}((t))(\sqrt[m]{t})$ with $m \in \mathbb{N}$, $m \geq 1$. If $f \in \mathbb{R}[[t]][x]$ such that $\overline{f}$ has no multiple roots in $\mathbb{C}$ then the discriminant of f is not divisible by t and so we see that the splitting field of f is either $\mathbb{R}((t))$ or $\mathbb{C}((t))$. This yields that such f decomposes in a product of irreducible factors of degree at most 2. The irreducible factors of f of degree 2 are equal to a sum of two squares in $\mathbb{R}[[t]][x]$ (this since f is a norm of $\mathbb{C}[[t]][x]$).

In order to proof theorem 1.4 we consider three different cases, described in the following lemma.

Lemma 2.5. *Let C be a hyperelliptic curve over $\mathbb{R}((t))$ with good reduction. Then C is $\mathbb{R}((t))$-birational equivalent to a hyperelliptic curve defined by one of the following type of equations:*
(1) *$y^2 = f(x)$, where $f(x)$ is monic,* $\deg f(x)$ *is odd and $\overline{f}(x)$ is a polynomial without multiple roots;*
(2) *$y^2 = f(x)$, where $f(x)$ is monic,* $\deg f(x)$ *is even, $f(x)$ has no linear divisor and $\overline{f}(x)$ is a polynomial without multiple roots.;*
(3) *$y^2 = -f(x)$, where $f(x)$ is monic,* $\deg f(x)$ *is even, $f(x)$ has no linear divisor and $\overline{f}(x)$ is a polynomial without multiple roots.*
The function field $\mathbb{R}((t))(C)$ is a real field if C is birational equivalent to a curve defined by an equation of type (1) *or* (2). *The function field $\mathbb{R}((t))(C)$ is a non-real field if C is birational equivalent to a curve defined by an equation of type* (3).

Proof: The definition of good reduction (definition 2.3) yields that C is isomorphic to a curve defined by an affine equation of the form $y^2 = \pm f_0(x)$, with $f_0(x)$ a monic polynomial in $\mathbb{R}[[t]]$ without multiple roots. Moreover in case $\deg f_0$ is odd the sign may chosen to be positive. If $\deg f_0$ is even and f_0 has no linear factor over $\mathbb{R}((t))$, it follows from the remark 2.4 that $f_0(x)$ is equal to a sum of two squares in $\mathbb{R}[[t]]$. So we have to show that a curve over $\mathbb{R}[[t]]$ with good reduction and defined by an affine equation of the form $y^2 = \pm f_0(x) = \pm(x-a)g(x)$, with $\deg f_0(x) = 2n$, is birational equivalent to one given by an equation of type (1). Set

$$x - a = u^{-1}, y(x-a)^{-n} = v$$

then

$$v^2 = f_1(u).$$

We have that $f_1(u)$ is a polynomial in $\mathbb{R}[[t]][u]$ without multiple roots and $\deg f_1(u) = \deg f_0(x) - 1$. Up to changing the isomorphism type of the curve C_1 defined by this equation, lemma 2.2 yields that we may assume $f_1(u)$ to be a monic polynomial. We see that C is birationally isomorphic to the hyperelliptic curve C_1 and C_1 is defined by an equation of type (1).

It is clear that in the case of type (2) the function field $\mathbb{R}((t))(C) = \mathbb{R}((t))(x)(\sqrt{f})$ is a real field. This because f is a sum of two squares so all orderings of $\mathbb{R}((t))(x)$ extend to $\mathbb{R}((t))(x)(\sqrt{f})$. In the same way it is easy to see that in the case of type (3) the function field $\mathbb{R}((t))(C) = \mathbb{R}((t)(x)(\sqrt{-f(x)})$ is non-real since -1 is clearly a sum of squares in this field. To see that in the case type (1) the function field $\mathbb{R}((t))(C)$ is a real field it is enough to notice that C has an $\mathbb{R}((t))$-rational point (one sees from lemma 2.1 that the completion of $\mathbb{R}((t))(C)$ in a $\mathbb{R}((t))$-rational point is a real field, cf. also [4]). The latter follows directly from the fact that f is of odd degree and so has a linear factor over $\mathbb{R}((t))$ (by remark 2.4). □

Remark 2.6. The distinction between cases (1) and (2) can be interpreted as follows; in case (1) the field $\mathbb{R}((t))(C)$ is a real but not totally real quadratic extension of $\mathbb{R}((t))(x)$, in case (2) $\mathbb{R}((t))(C)$ is a totally real quadratic extension of $\mathbb{R}((t))(x)$.

To finish this section we give the following general result for function fields of curves over $\mathbb{R}((t))$, which we links the Pythagoras number for real function fields of hyperelliptic curves over $\mathbb{R}((t))$ to the Brauer group of the curve.

Lemma 2.7. *Let C be any irreducible smooth projective curve over $\mathbb{R}((t))$. Let $f_i \in \mathbb{R}((t))(C)$, $i = 1, \ldots, r$. Then the quaternion algebra $A = (-1, \sum_{i=1}^r f_i^2)_{\mathbb{R}((t))(C)}$ over $\mathbb{R}((t))(C)$ is unramified.*

Proof: Let v be a discrete valuation on $\mathbb{R}((t))(C)$. The ramification formula, page 5, yields

$$\partial_v((-1, \sum f_i^2)_{\mathbb{R}((t))(C)}) \equiv (-1)^{v(\sum f_i^2)} \bmod \mathbb{R}((t))(v)^{*2}.$$

If the residue field of v, $\mathbb{R}((t))(v)$, is non-real then remark 2.4 implies that -1 is a square in $\mathbb{R}((t))(v)$, so the ramification is trivial in this case.

If the residue field of v is a real field then the completion $\mathbb{R}((t))(C)_v$ is a formal power series field of the form $\mathbb{R}((t))(v)((\pi))$, with π a uniformizing element for v. We can calculate the valuation of $\sum f_i^2$ as an element of this completion. If necessary renumber the elements f_i, $i = 1, \ldots, r$ such that $v(f_1) \leq v(f_2) \leq v(f_3) \leq \cdots \leq v(f_r)$. Let $v(f_1) = \cdots = v(f_l) < v(f_{l+1})$, then $f_1^2 + \cdots + f_l^2 = \pi^{2k}(a_1^2 + \cdots + a_l^2 + \pi g)$ for some $k \in \mathbb{N}$, $a_1, \ldots, a_l \in \mathbb{R}((t))(v)^*$ and some $g \in \mathbb{R}((t))(v)[\pi]$. Since the $a_i^2, i = 1, \ldots, l$ are non-zero totally positive element in the residue field $\mathbb{R}((t))(v)$, $a_1^2 + \cdots + a_l^2$ is a non-zero element in $\mathbb{R}((t))(v)$. We have $v(\sum_{i=1}^l f_i^2) = 2k < v(f_j^2)$ for all $j = l+1, \ldots, r$, so $v(\sum_{i=1}^r f_i^2) = 2k$. It follows that $\partial_v(-1, \sum f_i^2)_{\mathbb{R}((t))} \equiv 1 \bmod \mathbb{R}((t))(v)^{*2}$. This proves that the algebra A is unramified for all discrete valuations on $\mathbb{R}((t))(C)$. □

Remark 2.8. It is not difficult to see that the proof of lemma 2.7 also holds for function fields of curves over a hereditarily pythagorean field k since the residue fields of the k-discrete valuations are real pythagorean fields or fields in which -1 is a square.

3. The formally real case

Throughout this section C will be a smooth hyperelliptic curve over $\mathbb{R}((t))$ with good reduction such that its function field is a formally real field. The aim of this section is to prove theorem 1.4 for such function fields. Since the function field of C is an invariant of the birational equivalence class of C, lemma 2.5 implies that we may assume that the affine part of C is given by an equation of the form

$$y^2 = f(x), \tag{3.1}$$

with (in view of remark 2.4)

$$f(x) = (x - a_1)...(x - a_{2n+1})g_1(x)...g_m(x), \tag{3.2}$$

where $\overline{a}_i \neq \overline{a}_j$ if $i \neq j$, and g_l, $l = 1, \dots, m$ are different quadratic irreducible polynomials with splitting field $\mathbb{C}((t))$. Without loss of generality we also assume that the coefficients a_i, $i = 1, \dots, 2n + 1$ are enumerated in such a way that $\overline{a}_i < \overline{a}_j$ if $i < j$.
In order to apply lemma 2.7 we need to know the Brauer classes of central simple algebras of exponent 2 over $\mathbb{R}((t))(C)$ that are unramified, so we need to know the Brauer group of the curve C. Consider the following list of elements in ${}_2\mathrm{Br}(\mathbb{R}((t))(C))$

$$\mathcal{A}_i = (-1, (x - a_1)(x - a_i))_{\mathbb{R}((t))(C)},\ i = 2, \dots 2n + 1, \tag{3.3}$$

$$\mathcal{B}_i = (t, (x - a_1)(x - a_i))_{\mathbb{R}((t))(C))},\ i = 2, \dots 2n + 1, \tag{3.4}$$

$$\mathcal{C}_j = (t, g_j(x))_{\mathbb{R}((t))(C)},\ j = 1, \dots m. \tag{3.5}$$

In [20] the first author obtained the following result

Proposition 3.1. *Let C be a hyperelliptic curve defined by equation (3.1).*
(a) *For $j = 1, \dots, n$ the algebras $\mathcal{A}_{2j}$ and $\mathcal{A}_{2j+1}$ are Brauer equivalent.*
(b) *The following classes in ${}_2\mathrm{Br}(\mathbb{R}((t))(C)$*

$$[(-1, -1)], [(-1, t)], [\mathcal{A}_i], [\mathcal{B}_j], [\mathcal{C}_k], i \in \{2, 4, 6, \dots, 2n\}, j \in \{2, 3, \dots, 2n+1\}, k \in \{1, \dots, m\},$$

form a basis of the vector space ${}_2\mathrm{Br}(C)$ over $\mathbb{F}_2$.

For the sake of completeness we will give the proof of this proposition here. It is based on the description of the 2-torsion part of the Brauer group of a hyperelliptic curve in terms of generators and relations which can be found in [15].

Theorem 3.2. *Let k be a field of characteristic not 2. Let H be a hyperelliptic curve with affine part defined by the equation*

$$y^2 = g(x),$$

where $g(x) = (x-b)h_1(x)...h_r(x)$, deg $g(x)$ is odd and $h_1(x), ..., h_r(x)$ are irreducible monic polynomials. Let for $i = 1, \dots r$, b_i be a root of $h_i(x)$ in $\overline{k}$. Then any element of ${}_2\mathrm{Br}\ H$ can be represented as a tensor product of a constant algebra (i.e. algebra defined over k) and an algebra of the form

$$\mathrm{cor}_{k(b_1)(H)/k(H)}\big((c_1, (x - b)(x - b_1))_{k(b_1)(H)}\big) \otimes \dots$$
$$\dots \otimes \mathrm{cor}_{k(b_r)(H)/k(H)}\big((c_r, (x - b)(x - b_r))_{k(b_r)(H)}\big),$$

with $c_i \in k(b_i)$.
Conversely any algebra of the above form is an element of ${}_2\mathrm{Br}(H)$. *It's Brauer class is trivial if and only if the algebra is similar to a tensor product* $D = D_1 \otimes \cdots \otimes D_r$, *with* $D_i \in \mathrm{cor}_{k(b_i)(H)/k(H)}((s_i, (x-b)(x-b_i))_{k(b_i)(H)})$, $s_i = \prod_j (x_j - b_i)^{n_j}$ *such that* $\sum_j n_j(x_j, y_j)$ *is a k-divisor of degree* 0 *on* H *whose support does not contain any Weierstrass points of* H.

Corollary 3.3. *Let* C *be any hyperelliptic curve defined by the affine equation (3.1).*
(a) Every element of ${}_2\mathrm{Br}\, C$ *is represented as a tensor product of a constant algebra and an algebra of the form*

$$\begin{aligned}
&\mathrm{cor}_{\mathbb{C}((t))(C)/\mathbb{R}((t))(C)}((c_1, (x-a_1)(x-\theta_1))_{\mathbb{C}((t))(C)}) \otimes \dots \\
&\quad \otimes \mathrm{cor}_{\mathbb{C}((t))(C)/\mathbb{R}((t))(C)}((c_m, (x-a_1)(x-\theta_m))_{\mathbb{C}((t))(C)}) \\
&\quad \otimes (d_2, (x-a_1)(x-a_2))_{\mathbb{R}((t))(C)} \otimes \cdots \otimes (d_{2n+1}, (x-a_1)(x-a_{2n+1}))_{\mathbb{R}((t))(C)},
\end{aligned}$$

with θ_i *a root of* g_i *and* $c_i \in \{1, t\}$, $d_i \in \{1, t, -1, -t\}$.
(b) Every element of ${}_2\mathrm{Br}(C)$ *is equivalent to a tensor product of algebras taken from the set* $\{(-1,-1)_{\mathbb{R}((t))(C)}, (-1,t)_{\mathbb{R}((t))(C)}, \mathcal{A}_i, i = 2, \dots, 2n+1, \mathcal{B}_j, j = 2, \dots, 2n+1, \mathcal{C}_l, l = 1, \dots, m\}$.

Proof: The first point (a) follows directly from theorem 3.2 and the fact that $\{1, t\}$ represent the square classes of $\mathbb{C}((t))^*$ and that $\{1, t, -1, -t\}$ represent the square classes of $\mathbb{R}((t))^*$. To see the second point note that ${}_2\mathrm{Br}(\mathbb{R}((t)))$ is generated by $(-1,-1)_{\mathbb{R}((t))}$ and $(-1,t)_{\mathbb{R}((t))}$. The statement then follows from the fact that

$$\mathrm{cor}_{\mathbb{C}((t))(C)/\mathbb{R}((t))(C)}((t, (x-a_1)(x-\theta_i))_{\mathbb{C}((t))(C)}) = (t, g_i(x))_{\mathbb{R}((t))(C)}.$$

□

Remark 3.4. Note that corollary 3.3 implies that the Brauer classes of the algebras $\mathcal{A}_i, \mathcal{B}_i$ and $\mathcal{C}_j$ are elements of ${}_2\mathrm{Br}(C)$.

Lemma 3.5. *The algebras*

$$(\otimes_{i\in I}\mathcal{B}_i) \otimes (\otimes_{j \in J}\mathcal{C}_j) \otimes \mathbb{C}((t))(C),$$

with $I \subset \{2, \dots, 2n+1\}$ *and* $J \subset \{1, \dots, m\}$, *are non-trivial in* ${}_2\mathrm{Br}(\mathbb{C}((t))(C))$.

Proof: Let v be the valuation on $\mathbb{C}((t))$. Defining, for $g(x) = \sum a_l x^l \in \mathbb{C}((t))[x]$, $w(g(x)) := \min_l\{v(a_l)\}$ we obtain a discrete valuation w on $\mathbb{C}((t))(x)$ extending the valuation v. We have $w(t) = 1$. The residue field of w is $\mathbb{C}(x)$. Since the polynomial $\overline{f}(x)$ has no multiple roots, $\overline{f}(x)$ is not a square in the residue field $\mathbb{C}(x)$. Hence, the field $\mathbb{C}((t))(C) = \mathbb{C}((t))(x)(\sqrt{f(x)})$ is an unramified extension of $\mathbb{C}((t))(x)$. So the valuation w on $\mathbb{C}((t))(x)$ can be extended to a discrete valuation w' on $\mathbb{C}((t))(C)$ in such a way that $w'(t) = 1$. The residue field of w' is $\mathbb{C}(x)(\sqrt{\overline{f}(x)})$, it is a quadratic extension of $\mathbb{C}(x)$.
For the sake of contradiction we assume that an algebra of the form

$$\mathcal{B}_{i_1} \otimes \cdots \otimes \mathcal{B}_{i_r} \otimes \mathcal{C}_{j_1} \otimes \cdots \otimes \mathcal{C}_{j_s} \otimes_{\mathbb{R}((t))(C)} \mathbb{C}((t))(C) \sim (t, h(x))_{\mathbb{C}((t))(C)}, \tag{3.6}$$

with $h(x) = (x-a_1)^r(x-a_{i_1})\dots(x-a_{i_r})g_{j_1}(x)\dots g_{j_s}(x)$, is trivial in ${}_2\mathrm{Br}(\mathbb{C}((t))(C))$. Then there exist x_1,$x_2 \in \mathbb{C}((t))(C)$ such that $h(x) = x_1^2 - tx_2^2$. Since $h(x)$ is monic and since $w'(x_1^2)$ is even and $w'(x_2^2)$ is odd, it follows that $0 = w'(h(x)) = w'(x_1^2 - tx_2^2) = \min(w'(x_1^2), w'(tx_2^2)) = w'(x_1^2)$. So $\overline{h}(x) = \overline{x_1^2}$ in the residue field $\mathbb{C}(x)(\sqrt{\overline{f}(x)})$. Equivalently we find that $\overline{h}(x) \in \mathbb{C}(x)^{*2}$ or $\overline{f}(x)\overline{h}(x) \in \mathbb{C}(x)^{*2}$. But since C has good reduction it is easy to verify that both $\overline{h}(x)$ and $\overline{f}(x)\overline{h}(x)$ are not in $\mathbb{C}(x)^{*2}$. We obtained a contradiction implying that an algebra of the form (3.6) is non-trivial in ${}_2\mathrm{Br}(\mathbb{C}((t))(C))$. □

The following lemma proves part (a) of proposition 3.1.

Lemma 3.6. *The algebras $\mathcal{A}_{2j}$ and $\mathcal{A}_{2j+1}$ are for every $j = 1,\dots,n$ Brauer equivalent.*

Proof: Let for $i = 1,\dots,m$, $\theta_i = u_i + v_i\sqrt{-1}$, with $u_i, v_i \in \mathbb{R}((t))$, be a root of the quadratic polynomials g_i occurring in the factorisation of f, cf. equation 3.2. Let j be any element in $\{1,\dots,n\}$. Choose $d_1, d_2 \in \mathbb{R}((t))$ such that $\overline{d}_1 \neq \overline{u}_i$, $\overline{d}_2 \neq \overline{u}_i$, for all $i = 1,\dots,m$, $\overline{a}_{2j-1} < \overline{d}_1 < \overline{a}_{2j}$, and $\overline{a}_{2j+1} < \overline{d}_2 < \overline{a}_{2j+2}$ if $1 \leq j < n$, $\overline{a}_{2j+1} < \overline{d}_2$ if $j = n$. It follows from this choice of d_1 and d_2 that $f(d_1)$ and $f(d_2)$ are squares in $\mathbb{R}((t)$. Hence $(d_1, \sqrt{f(d_1)})$ and $(d_2, \sqrt{f(d_2)})$ are $\mathbb{R}((t))$-rational points of the affine part of C. The divisor $(d_1, \sqrt{f(d_1)}) - (d_2, \sqrt{f(d_2)})$ is an $\mathbb{R}((t))$-rational divisor of degree 0 and its support does not contain any Weierstrass points. Applying theorem 3.2 we see that the following algebra

$$\begin{aligned}\mathcal{D} &= \otimes_{i=1}^m \mathrm{cor}_{\mathbb{C}((t))(C)/\mathbb{R}((t)(C)}((d_1-\theta_i)(d_2-\theta_i), (x-a_1)(x-\theta_i))_{\mathbb{C}((t))(C)} \otimes \\ &\quad \otimes_{l=2}^{2n+1} ((d_1-a_l)(d_2-a_l), (x-a_1)(x-a_l))_{\mathbb{R}((t))(C)}\end{aligned}$$

is trivial in ${}_2\mathrm{Br}(C)$.

The choice of d_1 and d_2 also yields the following. For $s \neq 2j, 2j+1$ we have that $(\overline{d}_1 - \overline{a}_s)(\overline{d}_2 - \overline{a}_s) > 0$, implying that $(d_1-a_s)(d_2-a_s) \equiv 1 \bmod \mathbb{R}((t))^{*2}$. For $s = 2j, 2j+1$ we have $(\overline{d}_1 - \overline{a}_s)(\overline{d}_2 - \overline{a}_s) < 0$ implying that $(d_1-a_s)(d_2-a_s) \equiv -1 \bmod \mathbb{R}((t))^{*2}$. For $i = 1,\dots,m$, the elements $(d_1-\theta_i)(d_2-\theta_i)$ are power series in $\mathbb{C}[[t]]^2$ with non-zero constant term, so they are in $\mathbb{C}((t))^{*2}$. It follows that

$$\begin{aligned}\mathcal{D} &\sim ((d_1-a_{2j})(d_2-a_{2j}), (x-a_1)(x-a_{2j}))_{\mathbb{R}((t))(C)} \otimes \\ &\qquad ((d_1-a_{2j+1})(d_2-a_{2j+1}), (x-a_1)(x-a_{2j+1}))_{\mathbb{R}((t))(C)} \\ &\sim \mathcal{A}_{2j} \otimes \mathcal{A}_{2j+1}\end{aligned}$$

So the latter algebra is trivial, proving that $\mathcal{A}_{2j} \sim \mathcal{A}_{2j+1}$ in ${}_2\mathrm{Br}(C)$. □

Lemma 3.7. *Let*

$$\mathcal{A} = \otimes_{i \in I} \mathcal{A}_i,$$

with $I \subset \{2,4,\dots,2n\}$. Then the algebras $\mathcal{A}$, $\mathcal{A} \otimes (-1,-1)$, $\mathcal{A} \otimes (-1,t)$, $\mathcal{A} \otimes (-1,-t)$ are non-trivial in ${}_2\mathrm{Br}(\mathbb{R}((t))(C))$.

Proof: Write $\mathcal{A} = \mathcal{A}_{i_1} \otimes \cdots \otimes \mathcal{A}_{i_r}$ in such a way that $i_j < i_k$ if $j < k$. Choose $c \in \mathbb{R}((t))$ such that $\overline{a}_{i_r-1} < \overline{c} < \overline{a}_{i_r}$. Then $\overline{f}(\overline{c}) > 0$ and therefore $f(c) \in \mathbb{R}((t))^{*2}$. Hence $P = (c, \sqrt{f(c)})$ is $\mathbb{R}((t))$-rational point of C. The completion of $\mathbb{R}((t))(C)_P = \mathbb{R}((t))((x-c))$ (cf. lemma 2.1) is a real field. We obtain (since for a unit $a \in \mathbb{R}[[t]][[x-c]]$, $(x-a) \equiv (c-a) \bmod \mathbb{R}((t))((x-c))^{*2}$),

$$\mathcal{A}_P := \mathcal{A} \otimes_{\mathbb{R}((t))(C)} \mathbb{R}((t))(C)_P \sim (-1,(c-a_1)(c-a_{i_r}))_{\mathbb{R}((t))(C)_P} \sim (-1,-1)_{\mathbb{R}((t))(C)_P} \not\sim 1,$$
$$(A_P \otimes ((-1,t)_{\mathbb{R}((t))(C)_P}) \sim ((-1,-t)_{\mathbb{R}((t))(C)_P}) \not\sim 1$$

and

$$(A_P \otimes (-1,-t)_{\mathbb{R}((t))(C)_P}) \sim ((-1,t)_{\mathbb{R}((t))(C)_P})) \not\sim 1.$$

It follows that $\mathcal{A}, \mathcal{A} \otimes (-1,t)_{\mathbb{R}((t))(C)}$ and $\mathcal{A} \otimes (-1,-t)_{\mathbb{R}((t))(C)}$ are non-trivial. The non-triviality of $\mathcal{A} \otimes ((-1,-1)_{\mathbb{R}((t))(C)}$ can be seen in the same way by taking the completion of $\mathbb{R}((t))(C)$ in the $\mathbb{R}((t))(C)$-rational point $Q = (d, \sqrt{f(d)})$, where d is chosen such that $\overline{d} > \overline{a}_{2n+1}$. □

We can now complete the proof of proposition 3.1.
Proof of proposition 3.1:
We proved point (a) already in lemma 3.6.
To prove point (b) we have to show that the following classes in ${}_2\mathrm{Br}(\mathbb{R}((t))(C)$,

$$[(-1,-1)],[(-1,t)],[\mathcal{A}_i], i \in \{2,4,\ldots,2n\},[\mathcal{B}_j], j \in \{2,3,\ldots,2n+1\},[\mathcal{C}_k], k \in \{1,\ldots,m\}$$

form a basis for the $\mathbb{F}_2$-vector space ${}_2\mathrm{Br}(C)$. Corollary 3.3 and lemma 3.6 yield that the given classes form a set of generators for the $\mathbb{F}_2$-vector space ${}_2\mathrm{Br}(C)$. To show that these classes are linear independent over $\mathbb{F}_2$ we assume that the algebra

$$(-1,-1)^{s_1} \otimes (-1,t)^{p_1} \otimes \mathcal{A}_2^{s_2} \otimes \cdots \otimes \mathcal{A}_{2n}^{s_{2n}} \otimes \mathcal{B}_2^{p_2} \otimes \cdots \otimes \mathcal{B}_{2n+1}^{p_{2n+1}} \otimes \mathcal{C}_1^{q_1} \otimes \cdots \otimes \mathcal{C}_m^{q_m},$$

with $s_i, p_j, q_k \in \{0,1\}$ (and where $\mathcal{D}^0$ is by definition the trivial algebra $\mathbb{R}((t))(C)$), is trivial in ${}_2\mathrm{Br}(C)$. Since $\mathcal{A}_i \otimes \mathbb{C}((t))(C) \sim 1$, it follows from lemma 3.5 that $p_2 = \cdots = p_{2n+1} = q_1 = \cdots = q_m = 0$. Then applying lemma 3.7 we conclude that $s_2 = \cdots = s_{2n} = 0$. Finally one can directly verify that $(-1,-1)_{\mathbb{R}((t))(C)}, (-1,t)_{\mathbb{R}((t))(C)}$ and their tensor product $(-1,-t)_{\mathbb{R}((t))(C)}$ are non-trivial. □

We can now determine the Pythagoras number of a real function field of a hyperelliptic curve with good reduction.

Theorem 3.8. *Let C be a smooth hyperelliptic curve over $\mathbb{R}((t))$ with good reduction such that the function field $\mathbb{R}((t))(C)$ of C is a real field. Then the Pythagoras number of $\mathbb{R}((t))(C))$ is equal to 2.*

Proof: It follows from lemma 2.5 that we may assume that C is defined by an affine equation of the form $y^2 = f(x)$, where $f(x) \in \mathbb{R}[[t]][x]$ is either a monic polynomial of odd degree or a monic polynomial which is equal to a sum of two squares in $\mathbb{R}[[t]][x]$, and where in both cases $\overline{f}(x)$ is a polynomial without multiple roots.
We first deal with the case f is a polynomial of odd degree. Then f is as given in equation 3.2. To prove that the Pythagoras number $p(\mathbb{R}((t))(C)) = 2$, it is enough to prove that for any sum of squares $\sum f_i^2 \in \mathbb{R}((t))(C)$, the quaternion algebra $A = (-1, \sum f_i^2)_{\mathbb{R}((t))(C)}$ is trivial in ${}_2\mathrm{Br}(\mathbb{R}((t))(C))$. From lemma 2.7 it follows that $A \in {}_2\mathrm{Br}(C)$. Proposition 3.1, lemma 3.5 and the proof of lemma 3.7 imply that for any non-trivial algebra $\mathcal{D}$ whose

Brauer class is in ${}_2\mathrm{Br}(C)$ the following holds; either $\mathcal{D} \otimes \mathbb{C}((t))(C) \not\sim 1$ (in case in the expression of $\mathcal{D}$ in the given basis an algebra $\mathcal{B}_i$ or $\mathcal{C}_i$ occurs) or there exists an $\mathbb{R}((t))$-rational point P such that $\mathcal{D}_P \not\sim 1$ (in case $\mathcal{D}$ is in the subspace generated by the algebras $\mathcal{A}_i$, $(-1,-1)_{\mathbb{R}((t))(C)}$ and $(-1,t)_{\mathbb{R}((t))(C)}$, cf. the proof of lemma 3.7).
Clearly the algebra A becomes trivial over $\mathbb{C}((t)(C)$, since -1 is a square in $\mathbb{C}((t))(C)$. Now let P be any $\mathbb{R}((t))(C)$-rational point of C. Lemma 2.1 yields that the completion $\mathbb{R}((t))(C)_P$ is a real hereditarily pythagorean field. It follows that any sum of squares in $\mathbb{R}((t))(C)_P$ is a square, so $A \otimes \mathbb{R}((t))(C)_P$ is trivial. It follows from the above that A is not equivalent to any non-trivial algebra in ${}_2\mathrm{Br}(\mathbb{R}((t))(C)$. Therefore $A \sim 1$, implying that $p(\mathbb{R}((t))(C) = 2$.
In the case that $f = g^2 + h^2$, with $g, h \in \mathbb{R}[[t]][x]$, we have that $\mathbb{R}((t))(C)$ is the totally positive quadratic extension $\mathbb{R}((t))(x)(\sqrt{g^2+h^2})$ of $\mathbb{R}((t))(x)$. The result now follows from the more general fact that if k is a field with $p(k) = 2$ and $k(\sqrt{\alpha})$ is a totally positive quadratic extension of k then $p(k(\sqrt{\alpha})) = 2$, see [9, proposition 3.2] (note that the reduced height as defined in [9, page 22] is exactly the Pythagoras number). This finishes the proof of our theorem. □

Remark 3.9. The proof given in [9] of the fact that for a real field with Pythagoras number 2 the Pythagoras number of a totally positive quadratic extension is also 2, is based on a norm principle for quadratic extension which is proved in the same paper. To state this norm principle let E be a quadratic field extension of F. If φ is a multiplicative quadratic form over F, and $x \in E^*$. Then $N_{E/F}(x)$ is represented by φ over F if and only if $x \in F^* \cdot D_E(\varphi)$ (where $D_E(\varphi)$ is the set of elements in E^* represented by φ over E). The proof of this norm principle relies on the exact triangle for the Witt rings of E and F. Karim Becher explained to us the following direct argument for the fact that if $p(k) = 2$ and $k(\sqrt{\alpha})/k$ is a totally positive extension then $p(k)(\sqrt{\alpha}) = 2$.
It is enough to prove that $p(k(\sqrt{\alpha}) \leq 2$. Consider any sum of squares $\sum f_i^2 \in k(\sqrt{\alpha})$. Let the quaternion algebra $A = (-1, \sum f_i^2)_{k(\sqrt{\alpha})}$. We have to prove that A is trivial in ${}_2\mathrm{Br}(k(\sqrt{\alpha}))$. The corestriction of A is equal to $(-1, N(\sum f_i^2))$, where N is the norm of $k(\sqrt{\alpha})/k$. Note that for a quadratic extension the norm of a sum of squares is again a sum of squares. (This is a special case of the norm principle but can easily be seen directly.) Since the Pythagoras number of k is 2 it follows that $\mathrm{cor}_{k(\sqrt{\alpha})/k}[A] = 0 \in {}_2\mathrm{Br}(k)$. This implies that $A = (-1, \sum f_i^2)_{k(\sqrt{\alpha})} = (-1, g)_k \otimes k(\sqrt{\alpha})$ for some $g \in k$, see [12, proposition 5.0] and [19, (2.6)]. (This fact also follows from the exactness of the sequence ${}_2\mathrm{Br}(k) \stackrel{\mathrm{res}}{\to} {}_2\mathrm{Br}(k(\sqrt{\alpha})) \stackrel{\mathrm{cor}}{\to} {}_2\mathrm{Br}(k)$, see [1]. A sequence which is closely related to the exact triangle for the Witt rings of these fields used in [9]). Let S be any ordering on $k(\sqrt{\alpha})$. And let $k(\sqrt{\alpha})_S$ be the real closure of $k(\sqrt{\alpha})$ with respect to S. Since A is trivial over $k(\sqrt{\alpha})_S$ it follows that g must be positive with respect to S. So g is positive with respect to every ordering on $k(\sqrt{\alpha})$. But then it is also positive with respect to any ordering of k because $k(\sqrt{\alpha})$ is a totally positive extension of k. This implies g is a sum of squares in k. It follows that $(-1, g)_k$ is trivial, so also A is trivial. □

Example 3.10. The condition that C has good reduction cannot be removed in the theorem. Consider the following example. Let C be the elliptic curve defined by the equation $y^2 = (tx-1)(x^2+1)$. It is easy to check that this curve has bad reduction (note that the genus of the reduced curve is zero). The function field $\mathbb{R}((t))(C) = \mathbb{R}((t))(\sqrt{(tx-1)(x^2+1)})$ is a real field since $(tx-1)(x^2+1)$ is positive for every ordering on $\mathbb{R}((t)(x)$ with $x > \frac{1}{t}$. Note that $tx = \frac{y^2+x^2+1}{x^2+1}$ in $\mathbb{R}((t))(C)$. However tx is not a sum of two squares in $\mathbb{R}((t))(x)$ since the quaternion algebra $(-1,tx)_{\mathbb{R}((t))(C)}$ is non-trivial. The latter can be seen by a quadratic form argument. We have to show that the 2-fold Pfister form $\varphi = \langle 1,1,-tx,-tx\rangle$ is anisotropic over $\mathbb{R}((t))(C)$. Assume the contrary, then φ is hyperbolic over $\mathbb{R}((t))(x)(\sqrt{(tx-1)(x^2+1)})$. This is equivalent with the fact that over $\mathbb{R}((t))(x)$ the form $\langle 1,-(tx-1)(1+x^2)\rangle$ is a subform of φ. We obtain that $-(tx-1)(1+x^2)$ is represented by the form $\langle 1,-tx,-tx\rangle$ over $\mathbb{R}((t))(x)$. Or equivalently that $\langle (tx-1)(1+x^2),1,-tx,-tx\rangle$ is isotropic over $\mathbb{R}((t))(x)$. However viewing the latter form over the larger field $\mathbb{R}(x)((t))$ and applying Springer's theorem, (cf. [17, Chap.6, corollary 2.6]), taking residue forms, we obtain $\langle 1,-(1+x^2)\rangle$ for the first residue form and $\langle -x,-x\rangle$ for the second residue form. Both forms are anisotropic over $\mathbb{R}(x)$, therefore $\langle (tx-1)(1+x^2),1,-tx,-tx\rangle$ is anisotropic over $\mathbb{R}(x)((t))$, so also over the smaller field $\mathbb{R}((t))(x)$. This contradicts our assumption. □

It follows that $p(\mathbb{R}((t))(C)) \neq 2$. However we do not know the exact value, it is either 3 or 4.

4. The case of nonreal field

In this final section we determine the Pythagoras number of a non-real function field, $\mathbb{R}((t))(C)$, of a hyperelliptic curve with good reduction over $\mathbb{R}((t))$.

Theorem 4.1. *Let C be a smooth hyperelliptic curve over $\mathbb{R}((t))$ with good reduction and such that $\mathbb{R}((t))(C)$ is non-real. Then $p(\mathbb{R}((t))(C)) = 3$.*

Proof: Lemma 2.5 implies that we may assume that C is defined by an affine equation of the form $y^2 = -f(x)$, with f a sum of two squares in $\mathbb{R}[[t]][x]$. It follows that -1 is a sum of two squares in $\mathbb{R}((t))(C)$. Thus $s(\mathbb{R}((t))(C)) = 2$ and every element of $\mathbb{R}((t))(C)$ is a sum of squares. It is well known (cf. [14, chap. 7, lemma 1.3]) that since the level is finite we have $s(\mathbb{R}((t))(C)) \leq p(\mathbb{R}((t))(C)) \leq s(\mathbb{R}((t))(C)) + 1$. So to proof the theorem it is enough to find an element in $\mathbb{R}((t))(C)$ which is not a sum of two squares.

Consider the algebra $A = (-1,t)_{\mathbb{R}((t))(C)}$. We claim that A is non-trivial in ${}_2\mathrm{Br}(\mathbb{R}((t))(C))$. This then implies that t is not equal to a sum of two squares in $\mathbb{R}((t))(C)$ and we are done. To prove the claim, assume for the sake of contradiction that A is trivial in ${}_2\mathrm{Br}(\mathbb{R}((t))(C))$. Then there exist x_1,$x_2 \in \mathbb{C}((t))(C)$ such that $-1 = x_1^2 - tx_2^2$. Let w be the extension of the valuation v on $\mathbb{R}((t))(C)$, defined in the same way as in the proof of lemma 3.5. Then t is a uniformizing element for w and the residue field of w is equal to $\mathbb{R}(x)(\sqrt{-\overline{f}(x)})$, a quadratic extension of $\mathbb{R}(x)$. We have $0 = w(-1) = w(x_1^2 - tx_2^2) = \min(w(x_1^2), w(tx_2^2)) = w(x_1^2)$ since $w(x_1^2)$ is even and $w(tx_2^2)$ is odd. Hence $-1 = \overline{x}_1^2$ in the residue field $\mathbb{R}(x)(\sqrt{\overline{f}(x)})$, or equivalently $-1 \in \mathbb{R}(x)^{*2}$ or $-\overline{f}(x) \in \mathbb{R}(x)^{*2}$. But this is impossible since -1 and $-\overline{f}(x)$

are both negative for every ordering of $\mathbb{R}(x)$ (the latter because C has good reduction). So we obtained the contradiction we needed. $\square$

References

[1] J. Arason, *Cohomologische Invarianten quadratischer Formen,* J. Algebra **36**, (1975), 448-491.

[2] M. Auslander and A. Brumer, *Brauer groups of discrete valuation rings,* Indag. Math. **71** (1968), 286-296.

[3] M. Auslander and O. Goldman, *The Brauer group of a commutative ring,* Trans. Amer. Matrh. Soc., **97** (1960), 367-409.

[4] D.F., Bazyleu, J., Van Geel and V.I., Yanchevskii, *Ω-Algebras over Henselian Discrete Valued Fields with Real Closed residue Field,* preprint 2004.

[5] K. Becher, *On fields of u-invariant 4*, preprint 2004.

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

[7] L. Bröcker, *Über eine Klasse pythagoreischer Körper,* Arch. Math. **23**, (1970), 405-407.

[8] J.-L. Colliot-Theléné̀, *Birational Invariants, Purity and the Gersten Conjecture*, in: K-theory and Algbraic geometry: Connections with Quadratic Forms and Division Algebras, Proceedings of the 1992 Santa Barbara Summer research Institute (eds. B. Jacob and A. Rosenberg), Proc. Symp. Pure Math. **58.1**, (1995), 1-63.

[9] R. Elman and T.Y. Lam, *Quadratic Forms Under Algebraic Extensions*, Math. Ann. 219, (1976), 21-42.

[10] W.-D. Geyer, *Unedliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist*, J. Number Theory **1** (1969), 346-374.

[11] M. Knebusch and C. Scheiderer, *Einfhrung in die reelle Algebra.*, Vieweg, Braunschweig, 1989.

[12] T.Y. Lam, D.B. Leep and J.-P. Tignol, *Biquaternion Algebras and Quartic Extensions*, IHES nr. 77, (1993), 63-102.

[13] A. Pfister, *Zur Darstellung definiter Funktionen als Summe von Quadraten*, Invent. math. **4** (1967), 229-237.

[14] A. Pfister, *Quadratic Forms with Applications to Algebraic Geometry and Topology,*, LMS Lecture Note Series 217, Cambridge University Press, 1995.

[15] U. Rehmann, S.V. Tikhonov, and V.I. Yanchevskii, *Two-torsion of the Brauer groups of hyperelliptic curves and unramified algebras over their function fields*, Communications in Algebra **29** (2001), $n°$ 9, 3971-3987.

[16] D. J. Saltman, *Lectures on division algebras*, Published by American Mathematicas Society, Providence, RI, 1999.

[17] W. Scharlau, *Quadratic and Hermitian Forms,* Grundleheren der mathematisschen Wissenschaften **270**, Springer Berlin, Heidelberg, New York, Tokyo, 1985.

[18] J.-P. Serre, *Corps locaux,* Hermann, Paris, 1968.

[19] J.-P. Tignol, *Corps à involution neutralisés par une extension abélienne élémentaire,* in *Groupe de Brauer; séminaire, Les Plans-sur-Bex, Suisse, 1980* (M. Kervaire and M. Ojanguren, eds.), Lecture Notes in Math., Vol. **844**, Berlin-Heidelberg-New York, (1981), 1-34.

[20] S.V. Tikhonov, *Brauer groups of hyperelliptic curves with good reduction over real formal power series field*, Vesti Nats. Akad. Nauk Belarusi. (2004), $n°$ 1, 33–36.

[21] S. V. Tikhonov and V. I. Yanchevskiĭ, *Pythagoras numbers of function fields of conics over hereditarily pythagorean fields*, Dokl. Nats. Akad. Nauk Belarusi **47** (2003), $n°$2, 5–8.

Van Geel: Department of Pure Mathematics and Computer Algebra, Ghent University, Galglaan 2, B-9000 Gent, BELGIUM
E-mail address: jvg@cage.rug.ac.be

Tikhonov, Yanchevskiĭ: Institute of Mathematics of the National Academy of Sciences of Belarus, ul. Surganova 11, 220072, Minsk, BELARUS
E-mail address: tsv@im.bas-net.by , yanch@im.bas-net.by