PYTHAGORAS NUMBERS OF FUNCTION FIELDS OF GENUS ZERO CURVES DEFINED OVER HEREDITARILY PYTHAGOREAN FIELDS

Sergey V. Tikhonov\textsuperscript{1} and Vyacheslav I. Yanchevskii\textsuperscript{2}

\textsuperscript{1}Institute of Mathematics of the National Academy of Sciences of Belarus
ul. Surganova 11, 220072 Minsk, Belarus
e-mail: tsv@im.bas-net.by

\textsuperscript{2}Institute of Mathematics of the National Academy of Sciences of Belarus
ul. Surganova 11, 220072 Minsk, Belarus
e-mail: yanch@im.bas-net.by

1. INTRODUCTION

Let $F$ be a field of characteristic 0 and $\Sigma F^2$ the set of all sums of squares of elements of $F$. For $a \in \Sigma F^2$ the minimal $n \in \mathbb{N}$ such that

$$a = a_1^2 + \ldots + a_n^2, \ a_i \in F,$$

is called the length of $a$. It is denoted by $l(a)$. If $-1 \in \Sigma F^2$, then the number $s(F) = l(-1)$ is called the level of $F$.

The number $p(F) = \sup \{ l(a) \mid a \in \Sigma F^2 \}$ is called the Pythagoras number of $F$. If $F$ is nonreal, then $s(F) \leq p(F) \leq s(F) + 1$. A formally real field (= real field) $F$ is called pythagorean if $p(F) = 1$, hereditarily pythagorean (= h. p.) if any real algebraic extension of $F$ is pythagorean. Note that any nonreal extension of a h. p. field contains $\sqrt{-1}$. It is also know that a field $F$ is a h. p. field iff $p(F(x)) = 2$ where $F(x)$ is the rational function field over $F$ in one variable. We refer the reader to [1] for properties of h. p. fields.

Let $C$ be a conic defined over a h. p. field $F$. In this paper we compute the Pythagoras number of the function field $F(C)$ of $C$. This article is an extended version of the short communication [4]. We will consider separately the cases of real and nonreal $F(C)$.

2. PRELIMINARIES

Below we fix the following notations and conventions. For an abelian group $A$, the kernel of the multiplication by 2 is denoted by $2A$. For a field $k$, we denote its algebraic closure by $\overline{k}$. If $R$ is a commutative ring, $R^*$ denotes the group of units in $R$, and $R^{*2}$ denotes the subgroup of squares in $R^*$. If $s \in R^*$, then for the brevity the class $sR^{*2}$ will be denoted by the same symbol $s$.

$\text{Br } L$ denotes the Brauer group of a field $L$. For any finite dimensional $L$-central simple algebra $\mathcal{A}$, we use $[\mathcal{A}]$ to denote its class in $\text{Br } L$. For finite dimensional $L$-central simple algebras $\mathcal{A}$ and $\mathcal{B}$, we write $\mathcal{A} \sim \mathcal{B}$ if $[\mathcal{A}] = [\mathcal{B}]$ in $\text{Br } L$. We write
A \sim 1 if [\mathcal{A}] = 0. For a, b \in L^*, we denote by (a, b) the corresponding quaternion algebra over L. Note that (a, b) \sim 1 iff b \in N_{L(\sqrt{a})/L}(L(\sqrt{a})^*). Br F/L denotes the relative Brauer group of the extension F/L.

Let k be an arbitrary field of characteristic zero, X a smooth projective variety over k, X(k) its function field. The set of k-points of X is denoted by X(k). If L/k is a field extension, we set \( X_L = X \times_{\text{Spec } k} \text{Spec } L \).

For a discrete valuation \( v \) of \( k(X) \) trivial on k with the residue field \( k(v) \), there exists the homomorphism of ramification at \( v \)

\[
\text{ram}_v : \text{Br } k(X) \to \text{Hom}_{\text{cont}}(G_v, \mathbb{Q}/\mathbb{Z}) = H^1(G_v, \mathbb{Q}/\mathbb{Z}),
\]

where \( G_v = \text{Gal}(\overline{k}/k(v)) \). The ramification map is described in [3, Ch. 10]. A central simple algebra \( \mathcal{A} \) over \( K \) is said to be ramified at \( v \) if \( \text{ram}_v([\mathcal{A}]) \neq 0 \); then \( v \) is called a ramification point. The subgroup \( \cap_v \ker \text{ram}_v \), where \( v \) runs over the set of valuations with the aforementioned properties, is called the unramified Brauer group of the field \( k(X) \) and is denoted by \( \text{Br}_{nr} k(X) \).

Let \( \mathcal{A} \) be a \( k(X) \)-algebra of exponent 2. Then \( \text{ram}_v([\mathcal{A}]) \in 2H^1(G_v, \mathbb{Q}/\mathbb{Z}) \cong H^1(G_v, \mathbb{Z}/2) \cong (v(v)/k(v))^{*2} \). Note that for a quaternion algebra \( \mathcal{A} = (a, b) \), \( \text{ram}_v([\mathcal{A}]) = (-1)^{v(a)v(b)}a^{v(a)}b^{v(b)} \in k(v)/k(v)^{*2} \) by “tame symbol” formula.

Let \( C \) be a conic over \( k \). For any point \( P \in C \), there is the corresponding valuation \( v_P \) of \( k(C) \). The residue field of \( v_P \) is \( k(P) \). There is a natural inclusion of \( \text{Br } C \) in \( \text{Br } k(C) \) where \( \text{Br } C \) denotes the Brauer group of a conic \( C \). This inclusion identifies \( \text{Br } C \) with the unramified Brauer group \( \text{Br}_{nr} k(C) \). Below we will write \( \text{Br } C \) instead of \( \text{Br}_{nr} k(C) \) keeping in mind this identification. We need the following

**PROPOSITION 1** Let \( C \) be a curve over a h. p. field \( k \) and \( f_i \in k(C)^* \), \( i = 1, \ldots, n \). Then the \( k(C) \)-algebra \( \mathcal{A} = (-1, \sum_{i=1}^{n} f_i^2) \) is unramified.

**Proof.** Let \( g = \sum_{i=1}^{n} f_i^2 \). The algebra \( \mathcal{A} \) can be ramified at zeros or nodes of \( g \). Let \( P \) be a pole or a zero of \( g \). Choosing numeration one can assume that for the valuation \( v_P \) of \( k(C) \) at the point \( P \) there are the following inequalities \( v_P(f_i) \leq v_P(f_i) \), \( i = 1, \ldots, n \). Then

\[
\mathcal{A} \sim (-1, f_1^2(1 + f_2^2/f_1^2 + \ldots + f_r^2/f_1^2)) \sim (-1, 1 + f_2^2/f_1^2 + \ldots + f_r^2/f_1^2).
\]

If \( 1 + (f_2^2/f_1^2)(P) + \ldots + (f_r^2/f_1^2)(P) \neq 0 \), then \( \mathcal{A} \) is unramified at \( P \) by ”tame symbol” formula.

If \( 1 + (f_2^2/f_1^2)(P) + \ldots + (f_r^2/f_1^2)(P) = 0 \), then \( k(P) \) is nonreal. Hence \(-1\) is a square in \( k(P) \). Therefore \( \text{ram}_P([\mathcal{A}]) = (-1)^{v_P(g)}g^{v_P(-1)} = 1 \).

Thus \( \mathcal{A} \) is unramified and hence \([\mathcal{A}] \in \text{Br } C \). The proposition is proved.
3. THE CASE OF A REAL FIELD

We begin with the following

LEMA 2 Let $C$ be a conic over a h. p. field $k$, $D = (-1, u)$, where $u \in k^*$. Let also $k(C)$ be real. Assume that $C(k) = \emptyset$ and $D \otimes k(C) \not\sim 1$. Then $A \not\sim D \otimes k(C)$ where $A$ is as in Proposition 1.

Proof. Without loss of generality we will assume that $C$ is defined by an affine equation $y^2 = ax^2 + b$, $a, b \in k$. Since $C(k) = \emptyset$, then $a, b \not\in k^*2$ and $-ab \not\in k^*2$. Moreover, $-a \not\in k^*2$ or $-b \not\in k^*2$ since otherwise $k(C)$ is not real.

We will give the proof by breaking it into several cases.

Case 1. Assume $ub \not\in k^*2$.

(i) Let $b \not\in -k^*2$. There exists an ordering of $k$ such that $u < 0$, $b > 0$. Indeed, $k(\sqrt{b})$ is real and $u \not\in k(\sqrt{b})$. Then $L = k(\sqrt{b})(\sqrt{-u})$ is real and there is an ordering of $L$ such that $b > 0$, $u < 0$. We can extend this ordering to $k(x)$ viewing $x$ as an infinitely small element. Then $ax^2 + b > 0$ and $k(C)$ has an ordering such that $u < 0$. Consider a real closure $k(C)^R$ of $k(C)$ corresponding to the constructed ordering. Then

$$ A \otimes k(C)^R \sim 1 \text{ and } D \otimes k(C)^R \sim (-1, u) \otimes k(C)^R \sim (-1, -1) \otimes k(C)^R \not\sim 1. $$

Thus $A \not\sim D \otimes k(C)$.

(ii) Let $b \in -k^*2$. If $ua \in k^*2$, then

$$ D \otimes k(C) \sim (-1, u) \otimes k(C) \sim (-1, a) \otimes k(C) \sim (a, b) \otimes k(C) \sim 1. $$

Since $D \otimes k(C) \not\sim 1$, then $ua \not\in k^*2$.

Then there exists an ordering of $k$ such that $u < 0$, $a > 0$. We can extend this ordering to $k(x)$ viewing $x$ as an infinitely big element. Then $ax^2 + b > 0$ and $A \not\sim D \otimes k(C)$, by an argument analogous to that above.

Case 2. Assume $ub \in k^*2$. If $a \in -k^*2$, then

$$ D \otimes k(C) \sim (-1, u) \otimes k(C) \sim (-1, b) \otimes k(C) \sim (a, b) \otimes k(C) \sim 1. $$

For $au \in k^*2$, one has

$$ D \otimes k(C) \sim (-1, u) \otimes k(C) \sim (u, u) \otimes k(C) \sim (a, b) \otimes k(C) \sim 1. $$

Since $D \otimes k(C) \not\sim 1$, then $a \not\in -k^*2$ and $au \not\in k^*2$.  


There exists an ordering of \( k \) such that \( u < 0, a > 0 \). Hence by arguments analogous to that above we conclude again that \( \mathcal{A} \not\sim \mathcal{D} \otimes k(C) \). The lemma is proved.

Now we are in a position to formulate the main result of this section.

**THEOREM 3** Let \( C \) be a conic defined over a h.p. field \( k \) such that \( k(C) \) is real. Then \( p(k(C)) = 2 \).

**Proof.** Without loss of generality we will assume that \( C \) is defined by an affine equation \( y^2 = ax^2 + b, \ a, b \in k \). Moreover, we will assume that \( C(k) = \emptyset \) since otherwise \( k(C) \) is a rational function field in one variable over \( k \) and then \( p(k(C)) = 2 \). As in the proof of Lemma 2 we obtain that \( a, b \notin k^{*2} \) and \( -ab \notin k^{*2} \). Besides, \(-a \notin k^{*2} \) or \(-b \notin k^{*2} \) since otherwise \( k(C) \) is not real. Let \( g \in \Sigma k(C)^2 \) and \( \mathcal{A} = (-1, g) \).

Proposition 1 implies that \([\mathcal{A}] \in \text{Br} \ C\). Since \( C(k) = \emptyset \), then there is an exact sequence ([2])

\[
0 \longrightarrow < [(a, b)] > \longrightarrow \text{Br} \ k \xrightarrow{\text{res}} \text{Br} \ C \longrightarrow 0,
\]

where \( < [(a, b)] > \) is a subgroup generated by \([(a, b)] \in \text{Br} \ k \).

We will prove that \([\mathcal{A}] = 0 \). Let \( \mathcal{B} \) be a central simple \( k \)-algebra such that \([\mathcal{A}] = \text{res}(B) \). Assume that \( \mathcal{B} \otimes k(C) \not\sim 1 \). If \( \mathcal{B} \otimes k(\sqrt{-1}) \sim 1 \), then \( \mathcal{B} \sim (-1, u) \), where \( u \in k^{*} \), and by Lemma 2 \([\mathcal{A}] \neq \text{res}(B) \).

Now we consider the case where \( \mathcal{B} \otimes k(\sqrt{-1}) \not\sim 1 \). For the conic \( C \) we have two possibilities:

(i) \( C(k(\sqrt{-1})) \neq \emptyset \);

(ii) \( C(k(\sqrt{-1})) = \emptyset \).

In the case (i) \( k(\sqrt{-1})(C) \) is a rational function field in one variable over \( k(\sqrt{-1}) \). Hence \( \mathcal{B} \otimes k(\sqrt{-1})(C) \not\sim 1 \). Since \( \mathcal{A} \otimes k(\sqrt{-1})(C) \sim 1 \), then \( \mathcal{A} \not\sim \mathcal{B} \otimes k(C) \).

In the case (ii) we use an exact sequence

\[
0 \longrightarrow < [(a, b) \otimes k(\sqrt{-1})] > \longrightarrow \text{Br} \ k(\sqrt{-1}) \xrightarrow{\text{res}_{k(\sqrt{-1})}} \text{Br} \ C_{k(\sqrt{-1})} \longrightarrow 0.
\]

If \( \mathcal{A} \sim \mathcal{B} \otimes k(C) \), then \( \mathcal{B} \otimes k(\sqrt{-1})(C) \sim 1 \). Since \( \mathcal{B} \otimes k(\sqrt{-1}) \not\sim 1 \), we obtain that \([\mathcal{B}] \in \ker(\text{res}_{k(\sqrt{-1})}) \). Therefore \( \mathcal{B} \otimes (a, b) \otimes k(\sqrt{-1}) \sim 1 \) and \( \mathcal{B} \sim (a, b) \otimes (-1, u) \) for some \( u \in k^{*} \). Note that \((-1, u) \otimes k(C) \not\sim 1 \) since otherwise \( \text{res}(B) = 0 \). Then \([\mathcal{A}] = \text{res}(B) = \text{res}([(−1, u)]) \), i.e. \( \mathcal{A} \sim (-1, u) \otimes k(C) \). But this contradicts to Lemma 2. Thus \( \mathcal{A} \sim 1 \) and hence \( g \) is a sum of two squares. The theorem is proved.
3. THE CASE OF A NONREAL FIELD

In the case of a nonreal \( k(C) \) we have the following

**THEOREM 4** Let \( C \) be a conic defined over a h.p. field \( k \). Assume that \( k(C) \) is nonreal. Then

\[
p(k(C)) = \begin{cases} 
2 & \text{if } |Br k(\sqrt{-1})/k| = 2, \\
3 & \text{if } |Br k(\sqrt{-1})/k| > 2.
\end{cases}
\]

**Proof.** Without loss of generality we will assume that \( C \) is defined by an affine equation \( y^2 = ax^2 + b, \; a, b \in k \). Since \( k(C) \) is nonreal, then \( C(L) = \emptyset \) for any real algebraic extension \( L/k \). Indeed, assume that there exists a point \( P \in C(L) \) for some real extension \( L/k \). The completion of \( L(C) \) with respect to the valuation corresponding to \( P \) is \( L((z)) \) for some uniformizer \( z \). Since \( L(P) = L \) is real, then \( L((z)) \) is also real. Then \( k(C) \) is real in view of the inclusions \( k(C) \subset L(C) \subset L((z)) \).

This remark implies that we can assume without loss of generality that an affine equation of the conic \( C \) is \( y^2 + x^2 = -1 \). To see this one can observe that \( a \) is negative at any ordering of \( k \) since otherwise \( C \) has a point \((\sqrt{a} : 1 : 0)\) in a real extension. This implies that \(-a\) is a sum in squares in \( k \) and therefore is a square since \( k \) is pythagorean. In a similar way we can obtain that \(-b \in k^{*2} \). Then \( C \) is \( k \)-birationally equivalent to the conic with an affine equation \( y^2 + x^2 = -1 \).

Let \( g \in \Sigma k(C)^2 \) and \( A = (-1, g) \). Proposition 1 implies that \([A] \in Br C \). Note that \((-1, -1) \otimes k(C) \sim 1 \). Since \( C(k) = \emptyset \), then there is an exact sequence

\[
0 \longrightarrow [(−1, −1)] \longrightarrow \text{Br } k \overset{\text{res}}{\longrightarrow} \text{Br } C \longrightarrow 0.
\]

Note that \([A] \in \text{res}(\text{Br } k(\sqrt{-1})/k) \). Indeed, assume that \([A] \notin \text{res}(\text{Br } k(\sqrt{-1})/k) \). Then \([A] = \text{res}(B)\) for some central simple \( k \)-algebra \( B \) such that \( B \otimes k(\sqrt{-1}) \not\cong 1 \). Since \( C(k(\sqrt{-1})) \not= \emptyset \), then \( B \otimes k(\sqrt{-1})(C) \not\cong 1 \). We obtain a contradiction in view of \( A \otimes k(\sqrt{-1})(C) \sim 1 \). Thus \([A] \in \text{res}(\text{Br } k(\sqrt{-1})/k) \).

If \(|\text{Br } k(\sqrt{-1})/k| = 2 \), then the group \( \text{Br } k(\sqrt{-1})/k \) consists of \([(1, -1)], [(−1, −1)] \). Since these elements are in the kernel of \( \text{res} \), then \([A] = 0 \). Thus \( A \sim 1 \) and hence \( g \) is a sum of two squares. Hence \( p(k(C)) = 2 \).

If the cardinality of the group \( \text{Br } k(\sqrt{-1})/k \) is bigger then 2, we can take an element \( u \in k^* \) such that \( \text{res}([(−1, u)]) \neq 0 \). Hence \( u \) is not a sum of two squares. Since \( s(k(C)) = 2 \), then \( 2 \leq p(k(C)) \leq 3 \). Thus \( p(k(C)) = 3 \).

**REFERENCES**

