Geometrical aspects of the level of curves

Johannes Huisman, Louis Mahé
IRMAR, Campus de Beaulieu, F-35042 RENNES-Cedex, France

0 Introduction

The relationship between the sign of a given function on a subset of real points of an algebraic variety, and an expression of this function as a sum of squares, is certainly one of the most basic notions in real algebraic geometry. For example, the classical "Positivstellensatz" states that for an affine variety V defined over the real numbers $\mathbb{R}$, a function f in the ring of real polynomial functions $\mathbb{R}[V]$, is positive on the set of real points $V(\mathbb{R})$ if and only if $fs = 1+t$ for some sums of squares $s, t \in \mathbb{R}[V]$ (see for instance [CT1, Proposition 2]).

There is also a quantitative aspect of the question (which may be described as "arithmetic"): how many squares are really needed in such an expression? This is, in general, much more delicate than the simple positivity, and as this number of squares is irrelevant to the real geometry, one should not normally expect a geometric interpretation.

The clearest case is when $V(\mathbb{R})$ is empty, which translates into -1 is a sum of squares in $\mathbb{R}[V]$: the real geometry is as trivial as possible, but the arithmetic question ("how many squares?") is still there. Let us recall that the level of a ring A is defined as the least number $s = s(A)$ needed to express -1 as a sum of s squares (or ∞, if there is no such expression). The level of an affine $\mathbb{R}$-variety V (denoted by $s(V)$) is defined to be the level of the ring $\mathbb{R}[V]$. A theorem of Pfister [Pf] states that the level of a non formally real field of transcendence degree d over a real closed field is a power of 2 less than or equal to 2^d. Using this theorem, the second named author proved [Ma1, Ma2] that there is a function $B\colon \mathbb{N} \longrightarrow \mathbb{N}$ such that $s(A) \leq B(d)$ for all R-algebras A of transcendence degree $\leq d$ with empty real spectrum, R being any real closed field.

For curves ($d = 1$) the number $B(1)$ is 3 and Dai and Lam [DL] have actually shown that, for $P(X) = (1 + X^2)^2$, the level of the ring $A =$

$\mathbb{R}[X,Y]/(Y^2+P(X))$ is equal to 3, meaning that 3 is a sharp bound for the level of "empty" curves. (We will say that an $\mathbb{R}$-variety is *empty* if it has no real point). But this particular curve is singular because P is a square, and this latter fact was actually used in their proof. So, keeping in mind that the level of the function field of an empty nonsingular geometrically integral curve is 2, one might reasonably wonder whether the level of such a curve would also be 2. Then, the only task left, for a general affine curve C, is deciding between level 2 and 3.

In this work, we will characterize the level 2 smooth affine curves (section 1), by the existence of an element of a particular type in the Picard group of the compactified curve (Theorem 1.2, Theorem 1.8). In the case of hyperelliptic curves (section 2), this characterization is made more precise: a particular element P of the Picard group has to be of finite order (Theorem 2.2). Specializing in section 3 to the case of "hyperelliptic quartics" (see the beginning of section 3 for an explanation of this expression), we are able to give a very explicit criterion (Theorem 3.1). We further specialize (section 4) to hyperelliptic quartics C defined by an equation $Y^2+A(X)B(X)=0$, with $A,B\in\mathbb{Q}[X]$ polynomials of degree 2. In this situation, Mazur's theorem on torsion points of rational elliptic curves [Maz] implies that there are only 3 possible orders for the element P (Theorem 4.1) when C has level 2. We may even write in this case, a kind of parametrization of the coefficients of the polynomials A and B (Theorem 4.3). We then study (section 5) the question of affine curves obtained by removing an arbitrary number r of pairs of complex conjugate points in an empty projective curve defined over $\mathbb{R}$, and produce explicit examples of curves of level 2 and 3 for any r (Remark 5.2, Proposition 5.3).

We also show that for hyperelliptic curves, level 2 curves are rare among "empty" ones (Theorem 2.6), but that in genus 1, they are also dense among empty quartics (Theorem 3.4).

We finish the paper (section 6) by linking this subject with the famous question of deciding when a given polynomial in $\mathbb{R}[X,Y]$ is a sum of 3 squares of fractions. Proposition 6.3 and Theorem 6.5 give a criterion for $P(X,Y)$ being a sum of three squares which is of the same nature as Theorem 1.2 and Theorem 1.8.

The authors are grateful to J.-L. Colliot-Thélène who gave very useful hints that helped to solve the question. They also warmly thank the referee whose contribution considerably improved the paper.

1 The level of a smooth affine real curve

Throughout this section, C denotes a geometrically integral, smooth, affine curve over $\mathbb{R}$ without real points. We will study the level $s(C)$ of C, i.e. the level $s(\mathbb{R}[C])$ of the coordinate ring $\mathbb{R}[C]$ of C.

Let D be a smooth, projective curve over $\mathbb{R}$ containing C as an open dense subset. Since D is smooth and C has no real points, D has no real points either. A theorem of Witt states that -1 is a sum of 2 squares in the function field $\mathbb{R}(D)$ of D [Wi, Satz 2], and thus $s(\mathbb{R}(D)) \leq 2$. As D is geometrically integral, $s(\mathbb{R}(D))$ is exactly 2. Since $\mathbb{R}[C]$ is a subring of $\mathbb{R}(D)$, the level $s(C)$ is at least 2, and as mentioned in the introduction, it is known to be at most 3 [Ma1, Ma2]. Hence

$$s(C) = 2 \quad \text{or} \quad 3.$$

We derive a criterion that allows us to decide whether $s(C)$ is equal to 2 or 3. But first we need to fix some notation and to collect some results from the literature.

Most of the results concerning the projective curve D in this section, have been known for a long time. They may be found (in some form) in the papers of Weichold [We], Comessati [Co], Geyer [Ge]. They are collected in [GH, Proposition 2.2] and in [CP, Proposition 4.1.2].

Let $D' = D \times_{\mathbb{R}} \mathbb{C}$ (resp. $C' = C \times_{\mathbb{R}} \mathbb{C}$) be the complexification of D (resp. C). The Galois group $\Sigma = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \langle \sigma \rangle$ acts naturally on the scheme D'. This action induces an action of Σ on the Picard group $\mathrm{Pic}(D')$ of D'.

Let $p\colon D' \to D$ be the complexification morphism. It induces a morphism $p^\star$ from the Picard group $\mathrm{Pic}(D)$ of D into $\mathrm{Pic}(D')$. In fact, the image of $p^\star$ is contained in the subgroup $\mathrm{Pic}(D')^\Sigma$ of Σ-invariant elements of $\mathrm{Pic}(D')$.

Proposition 1.1. ([GH, Proposition 2.2.(2)]) *The morphism $p^\star$ maps* $\mathrm{Pic}(D)$ *isomorphically into a subgroup of index* 2 *of* $\mathrm{Pic}(D')^\Sigma$.

Proof. Since we need a part of the proof for the next proposition, we reproduce it here. Let M be an Abelian group on which Σ acts. Recall that the cohomology groups $H^i(\Sigma, M)$, for $i > 0$, are given by

$$H^i(\Sigma, M) = \begin{cases} \ker(1+\sigma)/\mathrm{im}(1-\sigma) & \text{if } i \text{ is odd, and} \\ \ker(1-\sigma)/\mathrm{im}(1+\sigma) & \text{if } i \text{ is even,} \end{cases}$$

where $1+\sigma$ (resp. $1-\sigma$) denotes the endomorphism of M that sends m onto $m+\sigma m$ (resp. $m-\sigma m$).

Let div be the morphism from the multiplicative group $\mathbb{C}(D')^\star$ of nonzero rational functions on D' into the group $\mathrm{Div}(D')$ of divisors on D', that associates to a nonzero rational function its divisor. It induces a morphism, again denoted by div, from the quotient $\mathbb{C}(D')^\star/\mathbb{C}^\star$ into $\mathrm{Div}(D')$. Denote by cl the morphism from $\mathrm{Div}(D')$ into $\mathrm{Pic}(D')$ that associates to a divisor its linear equivalence class. Then, one has a Σ-equivariant exact sequence

$$0 \longrightarrow \mathbb{C}(D')^\star/\mathbb{C}^\star \xrightarrow{\mathrm{div}} \mathrm{Div}(D') \xrightarrow{\mathrm{cl}} Pic(D') \longrightarrow 0.$$

Let $\delta\colon \mathrm{Pic}(D')^\Sigma \to H^1(\Sigma, \mathbb{C}(D')^\star/\mathbb{C}^\star)$ be the connecting homomorphism in the associated exact cohomology sequence.

Observe that $\mathrm{Div}(D')^\Sigma = \mathrm{Div}(D)$ and $\mathrm{Div}(D')$ is an induced $\mathbb{Z}[\Sigma]$-module. Hence, using Hilbert's Theorem 90 for $\mathbb{C}^*$, we obtain that the sequence

$$0 \longrightarrow \mathrm{Pic}(D) \xrightarrow{p^\star} \mathrm{Pic}(D')^\Sigma \xrightarrow{\delta} H^1(\Sigma, \mathbb{C}(D')^\star/\mathbb{C}^\star) \longrightarrow 0 \qquad (1)$$

is exact. Hence we have to show that the order of the group $H^1(\Sigma, \mathbb{C}(D')^\star/\mathbb{C}^\star)$ is 2.

An element in $H^1(\Sigma, \mathbb{C}(D')^\star/\mathbb{C}^\star)$ is represented by a function $f \in \mathbb{C}(D')$ such that the norm $N(f)$ of f with respect to the field extension $\mathbb{C}(D')$ over $\mathbb{R}(D)$ is constant, and thus is in $\mathbb{R}^\star$. If $N(f) > 0$, we may assume $N(f) = 1$, and Hilbert's Theorem 90 implies $f = g/\sigma g$, and f represents $0 \in H^1(\Sigma, \mathbb{C}(D')^\star/\mathbb{C}^\star)$. This shows that the order of this group is at most 2. As the level of $\mathbb{R}(D)$ is 2 [Wi, Satz 2], there is a fonction of norm -1 in $\mathbb{C}(D')$, and this provides the nonzero element in $H^1(\Sigma, \mathbb{C}(D')^\star/\mathbb{C}^\star)$. Then $H^1(\Sigma, \mathbb{C}(D')^\star/\mathbb{C}^\star)$ is isomorphic to $\mathbb{Z}/2$ and the proposition is proven. □

Theorem 1.2. *The level of C is 2 if and only if there exists $A \in \mathrm{Div}(D')$ such that*

i) the class $\mathrm{cl}(A)$ of A in the Picard group $\mathrm{Pic}(D')$ belongs to $\mathrm{Pic}(D')^\Sigma \setminus p^\star(\mathrm{Pic}(D))$, and

ii) the support $\mathrm{Supp}(A)$ of A is contained in $D' \setminus C'$.

Proof. (It is already known [GH, Proposition 2.2] that condition *i)* is equivalent to $D(\mathbb{R}) = \emptyset$, and thus to $s(\mathbb{R}(D)) = 2$.) Suppose that the level of C is 2. Then, there are $u, v \in \mathbb{R}[C]$ such that $u^2 + v^2 = -1$. Let $f = u + v\sqrt{-1} \in$

$\mathbb{C}[C']$. Then, f represents a nonzero element in $H^1(\Sigma, \mathbb{C}(D')^\star/\mathbb{C}^\star)$. By exactness of the sequence (1), there is a divisor $A \in \mathrm{Div}(D')$ with $\mathrm{cl}(A) \in \mathrm{Pic}(D')^\Sigma \setminus p^\star \mathrm{Pic}(D)$ such that $A - \sigma^\star A = \mathrm{div}(f)$. One may assume that $\mathrm{Supp}(A) \cap \mathrm{Supp}(\sigma^\star A) = \emptyset$. Since $f \in \mathbb{C}[C']^\star$, it follows that $\mathrm{Supp}(A) \subseteq \mathrm{Supp}(\mathrm{div}(f)) \subseteq D' \setminus C'$. Hence, A satisfies conditions *i)* and *ii)*.

Conversely, suppose that there is a divisor $A \in \mathrm{Div}(D')$ satisfying conditions *i)* and *ii)*. By exactness of the sequence (1), the δ-image of $\mathrm{cl}(A)$ in $H^1(\Sigma, \mathbb{C}(D')^\star/\mathbb{C}^\star)$ is nonzero. Let $f \in \mathbb{C}(D')^\star$ represent this image. Then, $\mathrm{div}(f) = A - \sigma^\star A$. By condition *ii)* one has $\mathrm{Supp}(\mathrm{div}(f)) \subseteq D' \setminus C'$ and thus $f \in \mathbb{C}[C']^\star$. Moreover, $N(f) < 0$ because f represents a nonzero element in $H^1(\Sigma, \mathbb{C}(D')^\star/\mathbb{C}^\star)$. One may then assume that $N(f) = -1$. Writing $f = u + v\sqrt{-1}$, with $u, v \in \mathbb{R}[C]$, one has $u^2 + v^2 = -1$, i.e. the curve C has level 2. □

One also has the following:

Proposition 1.3. ([Ge, (12), p. 91], see also [GH, Proposition 2.2.(2)].) *Let g be the genus of D. If A is a divisor on D' such that $\mathrm{cl}(A) \in \mathrm{Pic}(D')^\Sigma \setminus p^\star(\mathrm{Pic}(D))$, then $\deg(A) \equiv g + 1 \mod 2$.*

Since every element $A \in \mathrm{Div}(D)$ has an even degree when $D(\mathbb{R}) = \emptyset$, we may state:

Corollary 1.4. *Let $B \in \mathrm{Pic}(D')^\Sigma$. If g is odd then $\deg(B)$ is even. If g is even then $\deg(B)$ is even if and only if B is in $p^*(\mathrm{Pic}(D))$.*

Let us define $\mathrm{Pic}^0(D'), \mathrm{Pic}^0(D), \mathrm{Div}^0(D'), \mathrm{Div}^0(D)$ as the kernels of the corresponding degree maps. The action of Σ on $\mathrm{Pic}(D')$ induces an action of Σ on $\mathrm{Pic}^0(D')$.

Proposition 1.5. *Let g be the genus of D.*
a) If g is even, $p^\star(\mathrm{Pic}^0(D)) = \mathrm{Pic}^0(D')^\Sigma$.
b) If g is odd, $p^\star(\mathrm{Pic}^0(D))$ has index 2 in $\mathrm{Pic}^0(D')^\Sigma$.

Proof. Clearly $p^\star(\mathrm{Pic}^0(D)) \subseteq \mathrm{Pic}^0(D')^\Sigma$. Moreover, Proposition 1.1 implies that $[\mathrm{Pic}^0(D')^\Sigma : p^\star(\mathrm{Pic}^0(D))] \leq 2$. Suppose that g is even. Let $B \in \mathrm{Div}(D')$ be such that $\mathrm{cl}(B)$ is in $\mathrm{Pic}^0(D')^\Sigma$. Then $\deg(B) = 0$ and, by Corollary 1.4, $\mathrm{cl}(B) \in \mathrm{Pic}^0(D)$. This proves *a)*. Suppose g is odd. By Proposition 1.1 there exists $\mathrm{cl}(B) \in \mathrm{Pic}(D')^\Sigma \setminus p^\star \mathrm{Pic}(D)$, and $\deg(B)$ is even by Corollary 1.4. As $\mathrm{Div}(D)$ contains a degree 2 divisor, it also contains a divisor B_0 of degree $\deg(B)$. The class $\mathrm{cl}(B - B_0)$ belongs to $\mathrm{Pic}^0(D')^\Sigma \setminus p^\star(\mathrm{Pic}^0(D))$, and this proves *b)*. □

The set of fixed points $\mathrm{Pic}^0(D')^\Sigma$ is a commutative compact real Lie group (not necessarily connected) of dimension g and we have:

Proposition 1.6. ([Co, (12), p. 89]) *The subgroup $p^\star(\mathrm{Pic}^0(D))$ is the neutral component of $\mathrm{Pic}^0(D')^\Sigma$.*

Proof. Since the neutral component of $\mathrm{Pic}^0(D')^\Sigma$ is divisible and since $p^\star(\mathrm{Pic}^0(D))$ has finite index in $\mathrm{Pic}^0(D')^\Sigma$ (Proposition 1.1), the subgroup $p^\star(\mathrm{Pic}^0(D))$ contains the neutral component of $\mathrm{Pic}^0(D')^\Sigma$. Therefore, it suffices to show that $p^\star(\mathrm{Pic}^0(D))$ is a connected subset of $\mathrm{Pic}^0(D')^\Sigma$. Let d be an even integer satisfying $d \geq g$. Choose a divisor A on D of degree d. Denote by $D^{(d)}$ the d-fold symmetric power of D. As usual, identify the set of real points $D^{(d)}(\mathbb{R})$ of $D^{(d)}$ with the set of effective divisors of degree d on D. Consider the map $\gamma\colon D^{(d)}(\mathbb{R}) \longrightarrow p^\star(\mathrm{Pic}^0(D))$ defined by $\gamma(B) = p^\star(\mathrm{cl}(B - A))$. It is clear that γ is continuous (when $D^{(d)}(\mathbb{R})$ is equipped with the strong topology), and by Riemann-Roch, it is surjective.

Since $D(\mathbb{R}) = \emptyset$, the continuous map $\delta\colon D^{(d/2)}(\mathbb{C}) \longrightarrow D^{(d)}(\mathbb{R})$ defined by $\delta(B) = B + \sigma B$ is surjective. As $D^{(d/2)}(\mathbb{C})$ is connected, so is $p^\star(\mathrm{Pic}^0(D))$. □

Applying Proposition 1.6 and Proposition 1.5, one immediately obtains:

Corollary 1.7. *Let g be the genus of D. Then $\mathrm{Pic}^0(D')^\Sigma$ is connected when g is even, and has 2 connected components when g is odd.*

Finally we have:

Theorem 1.8. *Let g be the genus of D. Then*

a) if g is odd, the level of C is 2 if and only if there exists $B \in \mathrm{Div}(D')$ such that $\mathrm{cl}(B) \in \mathrm{Pic}^0(D')^\Sigma$, $\mathrm{Supp}(B) \cap C' = \emptyset$ and $\mathrm{cl}(B)$ is not in the neutral component of $\mathrm{Pic}^0(D')^\Sigma$,

b) if g is even, the level of C is 2 if and only if there exists $B \in \mathrm{Div}(D')$ such that $\mathrm{cl}(B) \in \mathrm{Pic}(D')^\Sigma$, $\mathrm{Supp}(B) \cap C' = \emptyset$ and $\deg B$ is odd.

Proof. By Theorem 1.2, the level of C is 2 if and only if there exists $B \in \mathrm{Div}(D')$ such that $\mathrm{cl}(B) \in \mathrm{Pic}(D')^\Sigma \setminus p^\star(\mathrm{Pic}(D))$ and $\mathrm{Supp}(B) \cap C' = \emptyset$. If g is odd, such a divisor B has even degree by Corollary 1.4. As $\mathrm{Div}(D)$ contains a degree 2 divisor with support in $D' \setminus C'$, it also contains such a divisor B_0 of degree $\deg(B)$. Replacing B by $B - B_0$ as in the proof above, we may assume $B \in \mathrm{Pic}^0(D')^\Sigma \setminus p^\star(\mathrm{Pic}^0(D))$. As $p^\star(\mathrm{Pic}^0(D))$ is the neutral component of $\mathrm{Pic}^0(D')^\Sigma$, part *a)* is proven.

If g is even, $\deg(B)$ is odd by Corollary 1.4, and this proves *b)*. □

Remark 1.9. Replacing the reals $\mathbb{R}$ by any real closed field R, and using the semi-algebraic topology instead of the usual one, one immediately sees that Theorem 1.8 holds in this extended context.

2 Hyperelliptic curves

Definition 2.1. A geometrically integral smooth affine curve C defined over $\mathbb{R}$ may be viewed as the complement of r closed points in a smooth projective completion D. When $C(\mathbb{R}) = \emptyset$, the complexification C' of C is the complement of r pairs of complex conjugate points in D'. We will say that C is an *r-pointed curve.*

Let $\mathrm{Jac}(D)$ denote the Jacobian variety of D. One knows that $\mathrm{Jac}(D)(\mathbb{C}) = \mathrm{Pic}^0(D')$ and that $\mathrm{Jac}(D)(\mathbb{R}) = \mathrm{Pic}^0(D')^\Sigma$.

This section is concerned with the level of 1-pointed curves. As will be seen in section 5, typical examples of such curves are curves given by an irreducible equation $P(X) + Q(Y) = 0$ with P, Q nonnegative on $\mathbb{R}$, one of them being square-free, and such that the greatest common divisor of their degrees is 2. In particular, the affine curves given by an equation $Y^2 + P(X) = 0$ with $P > 0$ on $\mathbb{R}$ and square-free, are 1-pointed curves. By a slight abuse of language, we will call such curves hyperelliptic (affine), even if the genus is less than 2. Instead of interpreting Proposition 1.8 for these hyperelliptic curves only, one may as well do it in this larger context of 1-pointed curves as follows:

Theorem 2.2. *Let C be a 1-pointed curve of genus g, with $C' = D' \setminus \{P, \sigma P\}$. Then*
a) If g is odd, $s(C) = 2$ if and only if there exists $m \in \mathbb{N}$ such that $m\,\mathrm{cl}(P - \sigma P)$ is a 2-torsion point in $\mathrm{Jac}(D)(\mathbb{R})$ contained in the nonneutral component of $\mathrm{Jac}(D)(\mathbb{R})$.
b) If g is even, $s(C) = 2$ if and only if there exists $m \in \mathbb{N}$ odd such that $m\,\mathrm{cl}(P - \sigma P) = 0 \in \mathrm{Jac}(D)(\mathbb{C})$.

Proof. Let g be odd. By statement *a)* of Proposition 1.8, $s(C) = 2$ if and only if there exists $B \in \mathrm{Div}^0(D')$ with support in $D' \setminus C'$ such that $\mathrm{cl}(B)$ is in the nonneutral component of $\mathrm{Pic}^0(D')^\Sigma$. Such a B must be of the form $m(P - \sigma P)$ for some nonzero integer m. Its class $m\,\mathrm{cl}(P - \sigma P) \in \mathrm{Jac}(D)(\mathbb{C})$ is σ-invariant if and only if $m\,\mathrm{cl}(P - \sigma P) = m\,\mathrm{cl}(\sigma P - P)$ in $\mathrm{Jac}(D)(\mathbb{C})$.

This condition is equivalent to $2m\,\mathrm{cl}(P-\sigma P)=0$ in $\mathrm{Jac}(D)(\mathbb{R})$. Since $B=m\,\mathrm{cl}(P-\sigma P)\neq 0$, this proves *a)*. If g is even, by statement *b)* of Proposition 1.8, the level of C is 2 if and only if there exists $B\in\mathrm{Div}(D')$ of odd degree, with support in $D'\setminus C'$ such that $\mathrm{cl}(B)$ is in $\mathrm{Pic}(D')^{\Sigma}$. Such a B must be of the form $aP+b\sigma P$ for some integers a,b, with $a+b$ odd. The condition $B\in\mathrm{Pic}(D')^{\Sigma}$ translates into $(a-b)(P-\sigma P)=0\in\mathrm{Jac}(D)(\mathbb{C})$. As $(a-b)$ is odd, statement *b)* is proven. □

>From now on in this section, C will be a hyperelliptic affine curve (with the generalized meaning indicated above) given by an equation $Y^2+Q(X)=0$, with $Q\in\mathbb{R}[X]$ square-free and strictly positive on $\mathbb{R}$. If D is a smooth projective model for C, there is a degree 2 map π from D to the projective line $\mathbb{P}^1_{\mathbb{R}}$, defined on C by $(X,Y)\mapsto X$. Then $C'=D'\setminus\{P,\sigma P\}$, where $\{P,\sigma P\}=\pi^{-1}(\infty)$, and C is 1-pointed. But even more is true:

Lemma 2.3. *For any hyperelliptic curve defined over* $\mathbb{C}$*, the involution* (-1) *of* $\mathrm{Jac}(D)(\mathbb{C})$ *is induced by the hyperelliptic involution* h *of* D*, defined on* C *as* $h(x,y)=(x,-y)$.

Proof. For any pair of points M,N of $C(\mathbb{C})$, one has $\mathrm{cl}(M+h(M))=\mathrm{cl}(N+h(N))$. Hence $-\mathrm{cl}(M-N)=\mathrm{cl}(h(M)-h(N))=h^{\star}(\mathrm{cl}(M-N))$. Since $\mathrm{Jac}(D)(\mathbb{C})$ is generated by $\{\mathrm{cl}(M-N)\}_{M,N\in C(\mathbb{C})}$, the result follows. □

Remark 2.4. Denote by τ the involution σh of D'. By the preceding lemma, the induced involution $\tau^{\star}$ of the Abelian group $\mathrm{Jac}(D)(\mathbb{C})$ is $h^{\star}\circ\sigma^{\star}=(-1)\circ\sigma^{\star}$. Then, the σ-anti-invariant point $\mathrm{cl}(P-\sigma P)\in\mathrm{Jac}(D)(\mathbb{C})$ becomes a τ-invariant point, and one may compute $m\,\mathrm{cl}(P-\sigma P)$ inside the real part $\mathrm{Jac}(D)(\mathbb{C})^{\tau}$ of the Jacobian variety for this twisted real structure corresponding to τ. Note that the expression "nonneutral component" used in Theorem 2.2 refers to the standard (i.e. associated to σ) real structure.

The following lemma gives us a precise description of the set $\mathrm{Jac}(D)(\mathbb{C})^{\tau}$.

Lemma 2.5. *Let* $\tilde{C}$ *be the affine plane curve defined over* $\mathbb{R}$ *by the equation* $Y^2-Q(X)=0$ *and let* $\tilde{D}$ *be the corresponding smooth projective model. Let* $f\colon C'\longrightarrow\tilde{C}'$ *be the isomorphism defined over* $\mathbb{C}$ *by* $f(x,y)=(x,iy)$*. Then the induced group isomorphism* $f^{\star}$ *between* $\mathrm{Jac}(\tilde{D})(\mathbb{C})$ *and* $\mathrm{Jac}(D)(\mathbb{C})$*, induces an isomorphism between* $\mathrm{Jac}(\tilde{D})(\mathbb{C})^{\sigma}=\mathrm{Jac}(\tilde{D})(\mathbb{R})$ *and* $\mathrm{Jac}(D)(\mathbb{C})^{\tau}$.

Proof. The maps $D' \xrightarrow{\tau} D' \xrightarrow{f} \tilde{D}'$ and $D' \xrightarrow{f} \tilde{D}' \xrightarrow{\sigma} \tilde{D}'$ coincide because

$$f\tau(x,y) = f(\sigma x, -\sigma y) = (\sigma x, -i\sigma y) = (\sigma x, \sigma i y) = \sigma \cdot f(x,y)$$

on the affine part C'. Then $\tau^\star f^\star = f^\star \sigma^\star$ and the lemma follows. □

Let $g \in \mathbb{N}$ and put $k = 2g+2$. Let $H_g \subset \mathbb{R}^k$ be the subset of points $(a_1, \ldots, a_k)$ such that the equation $Y^2 + X^k + \sum_{i=0}^{k-1} a_i X^i = 0$ defines a nonsingular geometrically integral real curve having no real points. Let $H_{g,2}$ denote the subset of H_g corresponding to level 2 curves.

Theorem 2.6. *If $g \neq 0$ the set $H_{g,2}$ has measure zero in the set H_g.*

In other words, this may be interpreted as "the level of an empty affine hyperelliptic curve of positive genus is generally equal to 3".

Proof. Consider the polynomial $Q(X)$ of degree $k = 2g+2$ defined by $Q(X) = X^k + \sum_{i=0}^{k-1} a_i X^i$ over the ring $\mathbb{R}[a_0, \ldots, a_{k-1}]$, with indeterminates a_i. Let $\Delta(a_0, \ldots, a_{k-1})$ denote the discriminant of $Q(X)$ and put $A = \mathbb{R}[a_0, \ldots, a_{k-1}]_\Delta$. Let $\mathcal{C}$ be the relative affine A-curve defined by the equation $Y^2 + Q(X) = 0$. Let us glue the curve $\mathcal{C}$ with the affine curve of equation $Z^2 + R(T) = 0$, where $T = 1/X, R(T) = T^{2g+2}Q(1/T)$ and $Z = T^{g+1}Y$. This gluing can be made over A and provides a smooth projective relative completion of $\mathcal{C}$ called $\mathcal{D}$. Let again $\pi : \mathcal{D} \longrightarrow \mathbb{P}^1_A$ be the 2-fold covering defined on $\mathcal{C}$ by $(x,y) \mapsto x$ and let h denote the hyperelliptic involution of $\mathcal{D}$. Let $A' = A[\sqrt{-1}]$. Computing the subscheme $\pi^{-1}(\infty)$ in $\mathcal{D}$, one sees that the only algebraic extension needed to split it, is the adjunction of a square root of the negative of the leading coefficient of $Q(X)$. One then has over A', $\pi^{-1}(\infty) = \{P, h(P)\}$, where P is an A'-rational point of $\mathcal{D}$, and $\mathrm{cl}(P - h(P))$ is a section over $\mathrm{Spec}(A')$ of the relative Picard scheme $\mathrm{Jac}(\mathcal{D}) \longrightarrow \mathrm{Spec}(A')$. Denoting by $\tilde{\mathcal{C}}$ the A-curve of equation $Y^2 - Q(X) = 0$ and $\tilde{\mathcal{D}}$ its relative completion, according to Remark 2.4 and through the isomorphism constructed in Lemma 2.5, $\mathrm{cl}(P - h(P))$ may actually be viewed as a section φ over $\mathrm{Spec}(A)$ of $\mathrm{Jac}(\tilde{\mathcal{D}}) \longrightarrow \mathrm{Spec}(A)$.

Let us state the following lemma:

Lemma 2.7. *Let D be a hyperelliptic $\mathbb{R}$-curve of positive genus with $D(\mathbb{R}) \neq \emptyset$, let $\pi : D \longrightarrow \mathbb{P}^1_{\mathbb{R}}$ be a 2-fold covering, and let h be the associated involution. Then there exists $M \in D(\mathbb{R})$ such that $\mathrm{cl}(M - h(M))$ is not a torsion element.*

Proof. Choose $P \in D(\mathbb{R})$. If $\mathrm{cl}(P - h(P))$ is not torsion, then we are done. If not, consider the map from $D(\mathbb{R})$ to $\mathrm{Jac}(D)(\mathbb{R})$ defined by $M \mapsto \mathrm{cl}(M - P)$. Since D is not rational, this map is injective and cannot map the uncountable set $D(\mathbb{R})$ into the countable torsion subgroup of $\mathrm{Jac}(D)(\mathbb{R})$. Therefore, there exists $M \in D(\mathbb{R})$ such that $\mathrm{cl}(M - P)$ is not torsion. Since by Lemma 2.3 $\mathrm{cl}(M - h(M) + h(P) - P) = \mathrm{cl}(M - P) - \mathrm{cl}(h(M) - h(P)) = 2\,\mathrm{cl}(M - P)$, $\mathrm{cl}(M - h(M))$ is not torsion. □

Corollary 2.8. *Let $\mathcal{T}_n$ be the kernel of the multiplication by a positive integer n in $\mathrm{Jac}(\tilde{\mathcal{D}})$. Then $\varphi^{-1}(\mathcal{T}_n)$ has positive codimension in $\mathrm{Spec}(A)$.*

Proof. It is enough to see that the image under φ of $\mathrm{Spec}(A)(\mathbb{R}) = \mathbb{R}^k \setminus \{\Delta = 0\}$ is not contained in $\mathcal{T}_n(\mathbb{R})$. Let D be a hyperelliptic $\mathbb{R}$-curve of genus g with $D(\mathbb{R}) \neq \emptyset$. By Lemma 2.7 there is a point $M \in D(\mathbb{R})$ such that $n\,\mathrm{cl}(M - h(M)) \neq 0$. Setting $x = \pi(M)$, the curve $D \setminus \pi^{-1}(x)$, equipped with the restriction of π onto the affine line $\mathbb{P}^1_{\mathbb{R}} \setminus \{x\}$, is a hyperelliptic affine curve that has an equation $Y^2 - X^k + \sum_{i=0}^{k-1} a_i X^i = 0$ for some values $a_i \in \mathbb{R}$ such that $(a_0, \ldots, a_{k-1}) \in \mathbb{R}^k \setminus \{\Delta = 0\}$.

Set $z = (a_0, \ldots, a_{k-1})$ and write $\tilde{\mathcal{D}}_z, P_z, h(P)_z$ respectively, for the specialization at z of $\tilde{\mathcal{D}}, P, h(P)$. By construction of z, one has $\{M, h(M)\} = \{P_z, h(P_z)\} \subset \tilde{D}_z$ and $n\varphi(z) = n\,\mathrm{cl}(P_z - h(P_z)) = \pm n\,\mathrm{cl}(M - h(M)) \neq 0$. Thus $\varphi(z) \notin \mathcal{T}_n(\mathbb{R})$ and the corollary is proven. □

Now Theorem 2.2 implies that $H_{g,2}$ is contained in $\bigcup_{i\in\mathbb{N}} \varphi^{-1}(\mathcal{T}_n)(\mathbb{R}) \cap H_g$ and $\varphi^{-1}(\mathcal{T}_n)$ has positive codimension in $\mathrm{Spec}(A)$ for every $n > 0$ by Corollary 2.8. As H_g is a semialgebraic set of dimension k in $\mathbb{R}^k \setminus \{\Delta = 0\}$, $\varphi^{-1}(\mathcal{T}_n)(\mathbb{R}) \cap H_g$ is a thin set in H_g for every positive n. Thus, $\bigcup_{i\in\mathbb{N}} \varphi^{-1}(\mathcal{T}_n)(\mathbb{R}) \cap H_g$ is also a thin set in H_g, forcing $H_{g,2}$ to be thin in H_g. This proves Theorem 2.6. □

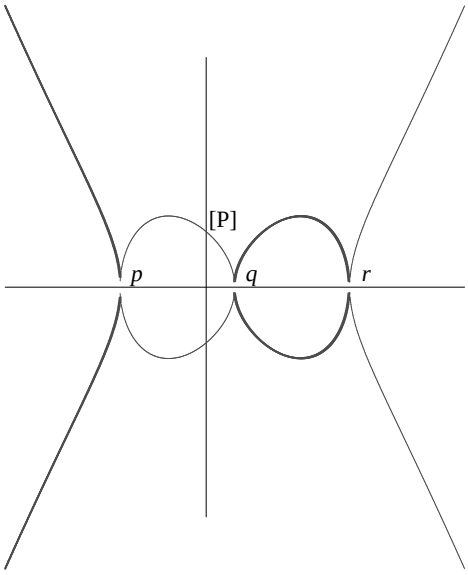
3 Empty hyperelliptic quartics

In this section, we study the case of smooth affine hyperelliptic quartics C with $C(\mathbb{R}) = \emptyset$. That means that C has an equation $Y^2 + Q(X) = 0$, with Q monic, square-free of degree 4. The genus g of such a curve is 1, and the results of the preceding sections apply here: if D is a smooth projective model of C and if $P, h(P)$ are the two points of D' above the point at infinity in $\mathbb{P}^1_{\mathbb{C}}$, one knows that $s(C) = 2$ if and only if there exists $m \in \mathbb{N}$ such that

$m\,\mathrm{cl}(P - h(P))$ is a 2-torsion point lying on the nonneutral component of $\mathrm{Jac}(D)(\mathbb{R})$.

Up to some affine change in X, one may assume that $Q(X) = ((X+b)^2+1)((X-b)^2+c^2)$ with $c > 0$. As $\tilde{C}$ (defined by $Y^2 - Q(X) = 0$) has $\mathbb{R}$-rational points, by a classical transformation (see for instance [ST, p. 23]), one obtains a Weierstrass equation $\beta^2 = W(\alpha) = (\alpha+4b^2)(\alpha-(c-1)^2)(\alpha-(c+1)^2)$ for $\tilde{D}$, for which the point at infinity is the image of $h(P)$ through the isomorphism f of Lemma 2.5. Then a Weierstrass equation for $\mathrm{Jac}(D)$ is $\beta^2 = -W(\alpha)$.

The real curve $\mathrm{Jac}(D)(\mathbb{R})$ is the subset $\mathrm{Jac}(D)(\mathbb{C})^\sigma$ of $\mathrm{Jac}(D)(\mathbb{C})$, and through the isomorphism of Lemma 2.5, $\mathrm{Jac}(\tilde{D})(\mathbb{R})$ may also be identified with $\mathrm{Jac}(D)(\mathbb{C})^\tau \subset \mathrm{Jac}(D)(\mathbb{C})$. A point of $\mathrm{Jac}(D)(\mathbb{R})$ or $\mathrm{Jac}(\tilde{D})(\mathbb{R})$ will then be considered as a point of $\mathrm{Jac}(D)(\mathbb{C})$. For example, the points in the intersection of the two real curves are the points of $\mathrm{Jac}(D)(\mathbb{C})$ which are at the same time σ-invariant and anti-invariant: they are exactly the points of $\mathrm{Jac}(D)(\mathbb{C})$ killed by 2. The point $[\mathrm{P}] := \mathrm{cl}(P - h(P)) \in \mathrm{Jac}(D)(\mathbb{C})$ is anti-invariant and thus is in $\mathrm{Jac}(D)(\mathbb{C})^\tau$.



In the figure, we represent the real parts of the 2 curves as subsets of the complex curve $\mathrm{Jac}(D)(\mathbb{C})$, given by the equation $\beta^2 + W(\alpha) = 0$ with the following conventions. The bold curve $\beta^2 = -W(\alpha)$ corresponds to

$\mathrm{Jac}(D)(\mathbb{R}) = \mathrm{Jac}(D)(\mathbb{C})^\sigma \subset \mathrm{Jac}(D)(\mathbb{C})$, and the thin curve $\beta^2 = W(\alpha)$ corresponds to $\mathrm{Jac}(\tilde{D})(\mathbb{R})$. The horizontal axis is the α-axis for both curves, and the vertical axis is the β-axis for the bold one. Viewing the thin curve as $\mathrm{Jac}(D)(\mathbb{C})^\tau \subset \mathrm{Jac}(D)(\mathbb{C})$, one must think of the vertical axis as being the $i\beta$-axis for this curve.

The point $[\mathrm{P}] = \mathrm{cl}(P - h(P))$ of $\mathrm{Jac}(D)(\mathbb{C})$ has then coordinates $(0, ib(c^2 - 1))$.

The points $p = (-4b^2, 0), q = ((1-c)^2, 0), r = ((1+c)^2, 0)$ are the three order 2 points of $\mathrm{Jac}(D)(\mathbb{C})$, named from left to right in the above figure.

Then Theorem 2.2 reads as follows:

Theorem 3.1. *Let C be a smooth affine empty hyperelliptic quartic given by the equation $Y^2 + Q(X) = 0$, and let $[\mathrm{P}]$ denote the point $\mathrm{cl}(P - h(P)) \in \mathrm{Jac}(D)(\mathbb{C})$. Then the level of C is 2 if and only if there exists $m \in \mathbb{N}$ such that $2m[\mathrm{P}] = r$ or $(2m+1)[\mathrm{P}] = q$.*

Proof. Actually q and r are the two order 2 points on the nonneutral component of $\mathrm{Jac}(D)(\mathbb{R})$, and according to Theorem 2.2 case *a)*, $s(C) = 2$ if and only if some multiple of $[\mathrm{P}]$ is q or r. Since $[\mathrm{P}]$ is on the nonneutral component of $\mathrm{Jac}(D)(\mathbb{C})^\tau$, an odd multiple is also on this component and it must be q, the intersection of the nonneutral components of $\mathrm{Jac}(D)(\mathbb{C})^\tau$ and $\mathrm{Jac}(D)(\mathbb{C})^\sigma$, while an even multiple must be on the neutral component of $\mathrm{Jac}(D)(\mathbb{C})^\tau$ and must be r. □

The two examples below are to some extent, the extremal cases, and correspond to the two following possibilities for a positive polynomial Q of the shape $Q(X) = R(X^2)$.

Corollary 3.2. *Let $Q = R(X^2)$ where $R \in \mathbb{R}[X]$ is a monic polynomial of degree 2 with positive coefficients and nonnegative discriminant Δ. Then the curve $Y^2 + Q(X) = 0$ has level 3.*

Proof. Up to an affine change of coordinates, one has $Q = (X^2+1)(X^2+c^2)$. If $\Delta = 0$, then $c^2 = 1$ and one recovers the Dai-Lam example quoted in the introduction. If not, as the number b defined above is 0, one has $[\mathrm{P}] = (0,0) = p$ and thus any multiple of this point is the origin $\mathcal{O}$ or p itself and cannot be q or r. □

Corollary 3.3. *Let $Q = R(X^2)$ where $R \in \mathbb{R}[X]$ is a monic polynomial of degree 2 with negative discriminant. Then the curve $Y^2 + Q(X) = 0$ has level 2.*

Proof. In this case, up to an affine change of coordinates, one may write $Q(X) = ((X+b)^2+1)((X-b)^2+1)$ with $b \neq 0$, and the number c defined above is 1. So $[\mathrm{P}] = (0,0) = q$ and the level is 2. □

Note that in this latter case the expression of -1 as a sum of two squares is easily obtained by writing $R = (X+s)^2 + t^2$ with $t \neq 0, s \in \mathbb{R}$.

There is a counterpart to Theorem 2.6. Let $H_1, H_{1,2}$ be the sets defined in Theorem 2.6, then:

Theorem 3.4. *The set $H_{1,2}$ is dense for the real topology in the set H_1.*

Proof. Take some $z \in H_1$, and let $C = C_z$ be the affine curve given by the equation $Y^2 + Q_z(X) = 0$. Then C is isomorphic (through an affine transformation), to a curve of equation $Y^2 + Q(X) = 0$ with $Q(X) = Q_{b,c}(X) := ((X+b)^2+1)((X-b)^2+c^2)$ with $c > 0$. So, defining H_1' as the semialgebraic subset of points $(b,c) \in \mathbb{R}^2$ such that the equation $Y^2 + Q_{b,c}(X) = 0$ defines a smooth affine hyperelliptic quartic without real points (i.e. $Q_{b,c}$ is square-free and positive), and defining $H_{1,2}'$ as the subset of H_1' corresponding to level 2 curves, one is reduced to show that $H_{1,2}'$ is dense in H_1'.

Let us consider the rational mapping $f\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ given by $f(b,c) = (\lambda,\mu)$ with $\lambda = (4b^2+(c+1)^2)/(4b^2+(c-1)^2) > 1, \mu = 4b^2/(4b^2+(c-1)^2)$. One may check that, starting from the equation $\beta^2 = W(\alpha)$ for $\mathrm{Jac}(\tilde{D_{b,c}})$, and making the change $v = (4b^2+\alpha)/(4b^2+(c-1)^2)$, one obtains the normalized Weierstrass equation $\gamma^2 = v(v-1)(v-\lambda)$ for $\mathrm{Jac}(\tilde{D_{b,c}})$, while μ is the v-coordinate of the point [P] in this model.

Let us call π_1, π_2 the two projections from $\mathbb{R}^2$ to $\mathbb{R}$, such that $\pi_1 \circ f(b,c) = \lambda, \pi_2 \circ f(b,c) = \mu$. Then, when the couples (b',c') vary in $(\pi_1 \circ f)^{-1}(\lambda)$, the associated Jacobian curves $\mathrm{Jac}(\tilde{D_{b',c'}})$ are all equal to $\mathrm{Jac}(\tilde{D_{b,c}})$ (that we may denote by $\mathrm{Jac}(\tilde{D}_\lambda)$), and one knows that the points $\mathcal{M} \in (\mathrm{Jac}\,\tilde{D}_\lambda)(\mathbb{R})$ for which there exists n with $n\mathcal{M} = q$ or r, are dense in the nonneutral component of $(\mathrm{Jac}\,\tilde{D}_\lambda)(\mathbb{R})$. Such a point $\mathcal{M}$ with v-coordinate μ' may then be chosen as close to μ as desired. Since f is an homeomorphism from H_1' onto its image, $(b',c') = f^{-1}(\lambda,\mu')$ is as close as desired to (b,c). Since $[\mathrm{P}]_{b',c'} = \mathcal{M}$, (b',c') is in $H_{1,2}'$ and this gives us the result. □

4 The case of rational coefficients

Assume now that $Q(X)$ is a given fourth degree polynomial, positive on $\mathbb{R}$, with rational coefficients, and consider the level of the affine $\mathbb{R}$-curve C

defined by $Y^2+Q(X)=0$. In particular, the leading coefficient of Q (say u) is positive and, with the change of coordinates $Y=Z\sqrt{u}$, C is $\mathbb{R}$-isomorphic to the curve given by the equation $Z^2+Q(X)/u=0$. As long as the level of $\mathbb{R}[C]$ is concerned, one may thus always assume that Q is monic. Then, the two points of the projective curve $\tilde{D}$ projecting on the point at infinity of $\mathbb{P}^1_{\mathbb{R}}$ are $\mathbb{Q}$-rational points, and the Weierstrass equation $\beta^2=W(\alpha)$, already computed for $\mathrm{Jac}(\tilde{D})$, has rational coefficients.

The polynomial $Q(X)$ can be factored over the real algebraic numbers and an appropriate change of variable in $\mathbb{R}[X]$ gives us $Q(X)=((X+b)^2+a^2)((X-b)^2+c^2)$, with real algebraic numbers a,b,c.

Call $\{P,h(P)\}$ the complement of C' in D'. If the ring $\mathbb{R}[C]$ has level 2, the $\mathbb{Q}$-rational point $[\mathrm{P}]=\mathrm{cl}(P-h(P))\in\mathrm{Jac}(\tilde{D})(\mathbb{R})$ is a torsion point of order $2n$ (for some n) of the real, and thus of the rational Mordell-Weil group $\mathrm{Jac}(\tilde{D})(\mathbb{Q})$. Mazur's theorem [Maz] (see also [ST], p. 58) states that the order of [P] is ≤ 12, and as [P] has even order, there are only 6 possibilities. These 6 cases correspond respectively to $[\mathrm{P}]=q, 2[\mathrm{P}]=r, 3[\mathrm{P}]=q, 4[\mathrm{P}]=r, 5[\mathrm{P}]=q, 6[\mathrm{P}]=r$ and each case is precisely described by a polynomial relation $T_n(a,b,c)=0$ for $n=1$ to 6.

Deciding whether the real curve C determined by (a,b,c) has level 2, reduces to knowing whether $T_n(a,b,c)=0$ for some $n\leq 6$. This is still difficult to explore completely, especially for the largest n. It is easier when Q factors over the rationals, and this case will now be worked out in detail.

Theorem 4.1. *Let $a^2,b,c^2\in\mathbb{Q}$ with a,c positive real numbers, and $Q(X)=((X+b)^2+a^2)((X-b)^2+c^2)$. Then the ring $\mathbb{R}[X,Y]/(Y^2+Q(X))$ has level 2 if and only if $T_n(a,b,c)=0$ for some $n\leq 3$, where the T_n's are polynomials defined as follows:*

$T_1(a,b,c)=c-a$

$T_2(a,b,c)=(4b)^2ac-(c^2-a^2)^2$

$T_3(a,b,c)=(16b^2(c+a))^2ac-((c^2-a^2)^2-16b^2ac)^2$.

Proof. If $c=a$ and $b=0$, the curve C is singular, but still has level 2. In the other cases, computation shows that these polynomial identities express respectively that $[\mathrm{P}]=q, 2[\mathrm{P}]=r$ and $3[\mathrm{P}]=q$. Thus, if (a,b,c) is a real zero of one of these three polynomials, with a,c positive, the point [P] satisfies the conditions of Theorem 3.1, and the curve C has level 2.

Conversely, assume that the level of the ring is 2, we are going to show that the order of [P] is at most 6, and this will show that only the three cases above can appear.

The Weierstrass equation already computed for Jac $\tilde{D}$ is $\beta^2 = W(\alpha)$ with $W(\alpha) = (\alpha + 4b^2)(\alpha - \alpha_q)(\alpha - \alpha_r)$. Putting $u_1 = \alpha + 4b^2, \beta_1 = \beta$, one gets a new equation $\beta_1^2 = W_1(u_1) = u_1(u_1^2 + A_1 u_1 + B_1)$, and the u_1-coordinate of the point [P] is $4b^2$. Let Γ_1 be the Mordell-Weil group of this curve. Let Γ_2 be the Mordell-Weil group of the curve defined by $\beta_2^2 = W_2(u_2) = u_2(u_2^2 + A_2 u_2 + B_2)$ with $A_2 = -2A_1, B_2 = A_1^2 - 4B_1$. There are group homomorphism (associated to a degree 2 isogeny) $\varphi : \Gamma_1 \longrightarrow \Gamma_2, \psi : \Gamma_2 \longrightarrow \Gamma_1$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are both multiplication by 2. The morphisms φ, ψ are defined by

$\varphi(u_1, \beta_1) = \left(\left(\frac{\beta_1}{u_1} \right)^2, \frac{\beta_1(u_1^2 - B_1)}{u_1^2} \right)$ if $u_1 \neq 0$ and $\varphi(p_1) = \varphi(\mathcal{O}_1) = \mathcal{O}_2$, with $p_1 = (0,0) \in \Gamma_1$ and $\mathcal{O}_1, \mathcal{O}_2$ the origins of Γ_1, Γ_2 and

$\psi(u_2, \beta_2) = \left(\left(\frac{\beta_2}{2u_2} \right)^2, \frac{\beta_2(u_2^2 - B_2)}{8u_2^2} \right)$ if $u_2 \neq 0$ and $\psi(p_2) = \psi(\mathcal{O}_2) = \mathcal{O}_1$, with $p_2 = (0,0) \in \Gamma_2$.

Since the u_1-coordinate $4b^2$ of [P] $\in \Gamma_1$ is a square in $\mathbb{Q}$, there is a point [Q] $\in \Gamma_2$ such that [P] $= \psi([Q])$. Since the level of C is 2, [P] is a torsion point of even order, and the same holds for [Q]. If $2k$ is the order of [Q], then k[Q] is one of the points of order 2 in Γ_2. If k[Q] $\neq p_2$, then $\psi(k[Q]) = k[P] = p_1$, which is excluded when C has level 2. It follows that k[Q] $= p_2$ and $\psi(k[Q]) = k[P] = \psi(p_2) = \mathcal{O}_1$. This shows that the order of [P] divides k, and thus k must be an even integer $2n$. This implies that the order $2k$ of [Q] in Γ_2, is $4n$. Actually one may easily check that the order of [P] is exactly $k = 2n$.

Since Γ_2 is also defined over $\mathbb{Q}$, Mazur's theorem can be applied to Γ_2, and the order $2k = 4n$ of [Q] satisfies $4n \leq 12$, and thus $n \in \{1, 2, 3\}$. □

Remark 4.2. Note that in Theorem 4.1, the numbers a, c are *positive algebraic numbers*. We really need a sign condition (actually $ac > 0$ would be sufficient) to distinguish between the points q and r : q has the smaller α-coordinate ($(c-a)^2$ with the chosen condition) and r has the bigger α-coordinate, $(c+a)^2$. In particular, the conditions of the proposition do not describe algebraic curves over $\mathbb{Q}$ or even over $\mathbb{R}$ (except for $T_1 = 0$). Of course, it would be possible to replace these conditions by purely polynomial conditions on a^2, b, c^2 avoiding the sign condition. But these polynomials would not be homogeneous and would be of higher degree than T_n.

Nevertheless, even though the conditions of Theorem 4.1 do not define algebraic sets over $\mathbb{Q}$, the next statement produces a sort of "rational

parametrization" of level 2 curves having an equation $Y^2 + P(X) = 0$ with P as in Theorem 4.1, in the following sense. For $i = 1, 2, 3$, there exists a polynomial map $f_i \colon \mathbb{Q}^3 \longrightarrow \mathbb{Q}^3$ such that the curve determined by (a^2, b, c^2) has level 2 if and only if $(a^2, b, c^2) \in \bigcup_{i=1}^{3} f_i(\mathbb{Q}_+^2 \times \mathbb{Q}^\star)$, where $\mathbb{Q}_+$ denotes the positive rationals.

Theorem 4.3. *Let $a^2, b, c^2 \in \mathbb{Q}$ with a, c real numbers, and $P(X) = ((X + b)^2 + a^2)((X - b)^2 + c^2)$. The real affine curve C of equation $Y^2 + P(X) = 0$ has level 2 if and only if one of the three following conditions is satisfied:*

i) $c^2 = a^2$

ii) there exist positive rationals u, v and a nonzero rational l such that $(a^2, b, c^2) = (l^2 u^3 v, \frac{1}{4} l(u^2 - v^2), l^2 u v^3)$

iii) there exist positive rationals u, v and a nonzero rational l such that $(a^2, b, c^2) = (l^2 u^5 v(u^2 + uv + v^2), \frac{1}{4} l(u^4 - v^4), l^2 u v^5 (u^2 + uv + v^2))$

Proof. It is easy to check that if condition *i)* (resp. *ii)*, *iii)*) holds and if a, c are positive, then (a, b, c) is a zero of the polynomials T_1 (resp. T_2, T_3) defined above, and $s(C) = 2$. As neither these conditions nor $s(C)$ depend on the sign of a, c, condition *i)* or *ii)* or *iii)* implies $s(C) = 2$.

For the converse, we may always assume that a, c are positive. Then by Theorem 4.1, $s(C) = 2$ if and only if $T_1 T_2 T_3(a, b, c) = 0$. Clearly $T_1(a, b, c) = 0$ implies condition *i)*. Suppose that $T_2(a, b, c) = 0$. One may assume $b \neq 0$ or otherwise $c = a$ and we are done. Then ac and $c/a = ac/a^2$ are rational and $c^2/a^2 = (v/u)^2$ for coprime positive integers u, v. This implies $c^2 = v^2 r, a^2 = u^2 r$ for some positive rational r. As $a^2 c^2 = (uvr)^2 = [(c^2 - a^2)/4b]^4$ is a fourth power of a rational, one deduces that $r = uvl^2$ for some rational l. Thus $a^2 = u^3 v l^2, c^2 = uv^3 l^2$ and $b = \pm \left(\frac{c^2 - a^2}{4\sqrt{ac}} \right) = \pm \frac{1}{4} l(v^2 - u^2)$. Replacing l by $-l$ if necessary, we obtain $b = \frac{1}{4} l(v^2 - u^2)$.

Suppose $T_3(a, b, c) = 0$. Again, one may assume $b \neq 0$. Expanding this equation, one sees that ac must be rational. Since $a \neq 0$, one may write $b' = b/a, c' = c/a$ and the equation $T_3(a, b, c) = 0$ turns into

$$c' = \left(\frac{(c'^2 - 1)^2 - 16 b'^2 c'}{(c' + 1) 16 b'^2} \right)^2$$

Since $b'^2 = b^2/a^2$ and $c' = ac/a^2$ are rational, c' must be the square of a rational and one may write $c' = c/a = v^2/u^2$ for coprime $u, v \in \mathbb{N}$. Then

$c^2/a^2 = v^4/u^4$ implies that $c^2 = v^4k, a^2 = u^4k$ for some $k \in \mathbb{Q}_+$. Then, replacing b'^2 by $b^2/(u^4k)$ in the above equation, one gets

$$v^2u^2\left((v^2+u^2)16b^2\right)^2 = \left(k(v^4-u^4)^2 - v^2u^216b^2\right)^2$$

which is equivalent to

$$vu(v^2+u^2)16b^2 = \epsilon\left(k(v^4-u^4)^2 - v^2u^216b^2\right)$$

for $\epsilon = \pm 1$. This may also be written

$$vu(v^2+\epsilon uv+u^2)16b^2 = \epsilon k(v^4-u^4)^2$$

and since k and the left hand side are positive, one must have $\epsilon = 1$ and $k = vu(u^2+uv+v^2)l^2$, for a rational l.

Finally, a^2, b, c^2 must be of the following type, for some coprime integers u, v and some rational l:

$$\begin{aligned} a^2 &= u^5v(u^2+uv+v^2)l^2 \\ c^2 &= uv^5(u^2+uv+v^2)l^2 \\ b &= \tfrac{1}{4}l(v^4-u^4) \end{aligned}$$

This finishes the proof. □

Remark 4.4. One may also consider the curves defined in $\mathbb{P}^2_{\mathbb{R}}$ by the homogeneous polynomial equations $T_n = 0$. It is clear that $T_1 = 0$ is isomorphic to $\mathbb{P}^1_{\mathbb{R}}$.

For $T_2 = 0$, we find the singular points $(b, a, c) = (0, \pm 1, 1)$ and $(1, 0, 0)$. They are ordinary points of multiplicity 2, and since the degree of T_2 is 4, the genus g of the curve $T_2 = 0$ is $g = 3 \cdot 2/2 - 3(2 \cdot 1/2) = 0$. Actually, replacing u and v by their squares in the formula *ii)* and extracting square roots of a^2, c^2, we obtain the following parametrization of the curve over the real numbers:

$$(a, b, c) = (u^3v, \left(\frac{u^4-v^4}{4}\right), uv^3).$$

For the curve $T_3 = 0$, the complex singular points consist also of three ordinary multiple points (the same coordinates as above), each one of multiplicity 4. Since $\deg(T_3) = 8$, the genus g is $7 \cdot 6/2 - 3(4 \cdot 3/2) = 3$. One may check that the operation done in the above paragraph on the formula *ii)*, cannot be done on the formula *iii)* to provide a parametrization of the curve $T_3 = 0$ over the real (or complex) numbers.

One has the following easy consequence of Theorem 4.1:

Corollary 4.5. *Let $P(X) = ((X+b)^2+a)((X-b)^2+c))$ with $a, b, c \in \mathbb{Q}$, a polynomial positive on $\mathbb{R}$. If $ac \notin \mathbb{Q}^{\star 2}$, then the level of the real curve given by the equation $Y^2 + P(X) = 0$ is 3.*

5 Construction of r-pointed curves

Let D be a smooth projective empty curve defined over $\mathbb{R}$, and let C be a geometrically integral affine curve such that $C' = D' \setminus E$ where $E = \{P_1, \bar{P}_1, \ldots, P_r, \bar{P}_r\}$ is a set of $r > 1$ pairs of complex conjugate points of D'. Recall that such an affine curve is called an r-pointed curve (cf section 2). In this section, we will apply the techniques developed in sections 2 and 3 to produce examples of r-pointed curves of level 2 and 3, for any $r > 1$. Define an $\mathbb{R}$-curve to be $C(n, r)$ if it is an r-pointed curve of level n.

In genus 1, we may produce $C(2, r)$ and $C(3, r)$ curves for any r (Proposition 5.3). However, for a fixed genus $g > 1$, this seems more difficult. The end of the section (Proposition 5.8 and Example 5.9) produces examples of $C(3, r)$ curves of odd genus $g > 1$ for odd integers r. This genus may be rendered as big as wanted, but anyway depends on r. Note that we do not have a single example of $C(3, r)$ curve of even genus.

Define $[Q]$ to be $\mathrm{cl}(Q - P_1) \in \mathrm{Jac}(D')$ for any $Q \in D'$.

Lemma 5.1. *Let C be an r-pointed curve of odd genus and assume that for every $i, 1 \leq i \leq r$, $[\bar{P}_i]$ is in $\mathrm{Jac}(D)(\mathbb{R})$. Then*

i) if some $[\bar{P}_i]$ is on the nonneutral component, C has level 2.

ii) if every $[\bar{P}_i], i = 1 \ldots r$ is on the neutral component of $\mathrm{Jac}(D)(\mathbb{R})$, C has level 3.

Proof. According to Proposition 1.8, since the genus is odd, C has level 2 if and only if one can find integers n_i, m_i, $i = 1 \ldots r$ such that the class of the divisor $A = \sum_{i=1}^{r}(n_i P_i + m_i \bar{P}_i)$ lies in $\mathrm{Pic}^0(D')^{\Sigma} \setminus \mathrm{Pic}^0(D)$. Since $-m_1 \,\mathrm{cl}(P_1 + \bar{P}_1) + m_1 \,\mathrm{cl}(P_2 + \bar{P}_2) \in \mathrm{Pic}^0(D)$, we may add it to $\mathrm{cl}(A)$ without changing its class modulo $\mathrm{Pic}^0(D)$. This reduces to assuming $m_1 = 0$ and $n_1 = -\sum_{i \neq 1}(m_i + n_i)$. The condition for having level 2 reduces to the existence of integers $a_i, b_i, i = 2 \ldots r$ such that $\sum_{i=2}^{r} \mathrm{cl}(a_i(P_i - P_1) + b_i(\bar{P}_i - P_1)) = \sum_{i=2}^{r}(a_i[P_i] + b_i[\bar{P}_i])$ lies in the nonneutral component of $\mathrm{Jac}(D)(\mathbb{R})$. If some $[\bar{P}_{i_0}]$ is on the nonneutral component, then let $b_{i_0} = 1$ and let each

of the other $a_i's$ and b_i's be equal to 0. Then the condition above is fulfilled and the level of C is 2. This proves *i)*.

For $[Q] \in \mathrm{Jac}(D)(\mathbb{R})$ one has $[Q] = \sigma([Q]) = \mathrm{cl}(\bar{Q} - \bar{P}_1) = \mathrm{cl}(\bar{Q} - P_1) - \mathrm{cl}(\bar{P}_1 - P_1) = [\bar{Q}] - [\bar{P}_1]$. In particular, if every $[\bar{P}_i]$ is on the neutral component, then it is so for every $[P_i] = [\bar{P}_i] - [\bar{P}_1]$ and for any linear combination of them. Applying Theorem 1.8 we see that the level of C is 3. This proves *ii)*. □

Remark 5.2. If C_1 is a $C(2,1)$-curve and if we remove $r-1$ closed points, we obtain an r-pointed curve C_2 of same genus, with a morphism $\mathbb{R}[C_1] \longrightarrow \mathbb{R}[C_2]$, and thus the level of C_2 must also be 2. As we have constructed $C(2,1)$-curves of genus 1 in section 3, it is easy to obtain $C(2,r)$-curves of genus 1 for any $r \geq 1$, and we will focus on $C(3,r)$-curves in the next proposition.

Proposition 5.3. *For any integer $r \geq 1$, there exist $C(3,r)$ genus 1 curves.*

Proof. The proof depends on the parity of r.

A) r is odd

The existence of $C(3,1)$ curves was shown in section 3, and so the case $r = 1$ is covered. Start with the affine plane curve C defined over $\mathbb{R}$ by

$$v^2 + (u^2 + b)^2 - c^2 = 0 \tag{1}$$

with $b, c > 0$ and $b - c > 0$. It is a 1-pointed affine hyperelliptic quartic, and corollary 3.2 asserts that it has level 3, because in the real part of the Jacobian curve defined by the equation

$$-\beta^2 = \alpha(\alpha^2 - 4b\alpha + 4c^2), \tag{2}$$

the point $[\bar{P}_1]$ (P_1 being the infinity point taken as origin) is the 2-torsion point lying on the neutral component, and has coordinates $(0,0)$.

Taking any point $[P_2]$ on the neutral component, the four points $\pm[P_2]$, $\pm[\bar{P}_2]$ are also in the neutral component, and together with $[\bar{P}_1]$, they form the intersection with the elliptic curve (2), of the union of two lines given by the equations $\beta \pm m_2\alpha = 0$, for some real slope m_2. The inverse image of this union of lines, in the initial hyperelliptic quartic C, has equation $u^2 + m_2^2/4 = 0$, and has exactly four points in C'. Removing this subvariety of C', one obtains a 3-pointed curve inside a genus 1 curve. One can do this

for any number s of points $[P_2], \ldots, [P_{s+1}]$ on the neutral component of the Jacobian curve (2), corresponding to different values of $m_j^2, j = 2 \ldots s+1$, remove the subvariety $\prod_{j=2}^{s+1}(u^2 + m_j^2/4) = 0$, and then obtain a $C(3, 2s+1)$ curve. For this, one must choose the slopes m_j such that the lines $\beta = \pm m_j \alpha$ intersect the curve (2) only on the neutral component. This is realized when $|m_j| > \sqrt{4b + 2c}$ which is the largest slope of the lines through the origin that are tangent to the curve.

For example the affine space curve given by the equations

$$v^2 + (u^2 + 2)^2 - 1 = 0, \qquad z \prod_{j=1}^{s} (u^2 + (1+j)^2) = 1$$

is a $2s+1$-pointed curve of genus 1 and has level 3, because $m_j^2 = 4(1+j)^2 \geq 16 > 4b + 2c = 10$.

B) r is even

Consider the affine space curve C defined over $\mathbb{R}$ by

$$X^2 + Y^2 = 1, \qquad (X - a)^2 + Z^2 = c^2. \tag{3}$$

The set C' is the complement in D' of the two pairs of conjugate points at infinity defined with the homogeneous coordinates $(X : Y : Z : T)$ by $(i : \pm 1 : \pm 1 : 0)$. The projective curve D is smooth and has genus 1 when $ac \neq 0, a \pm 1 \neq \pm c$, and is empty if $a > c+1, c > 0$. Under these assumptions, C is a 2-pointed curve.

Let us compute the level of C. The projection of C on the YOZ-plane is the isomorphic affine geometrically integral plane curve

$$(Z^2 - Y^2 + 1 + a^2 - c^2)^2 + 4a^2(Y^2 - 1) = 0. \tag{4}$$

The four points at infinity in (3) map to two double points at infinity in (4) with homogeneous $(Y : Z : T)$-coordinates $A = (1 : 1 : 0), B = (-1 : 1 : 0)$.

Putting $U = Z - Y$ and $\delta = 1 + a^2 - c^2$ in (4), one has, with homogeneous coordinates,

$$4Y^2(U^2 + a^2T^2) + 4UY(U^2 + \delta T^2) + U^4 + 2\delta U^2T^2 + (\delta^2 - 4a^2)T^4 = 0. \tag{5}$$

The change of variable $aVT^2 = 2(U^2 + a^2T^2)Y + U(U^2 + \delta T^2)$ gives

$$T^2V^2 + U^4 + 2(\delta - 2)U^2T^2 + (\delta^2 - 4a^2)T^4 = 0. \tag{6}$$

Note that when $T = 1$, this equation has the form $V^2 + R(U^2) = 0$, with R a second degree polynomial having discriminant $16c^2 > 0$. By Corollary 3.2, the level of this affine curve is 3.

Now, the double point B in (4) maps to the double point B' at infinity of (6), and the double point A maps to two simple points in the affine part of (6), given in (U,V)-coordinates by $A_1 = (ia, i(c^2-1)), A_2 = -(ia, i(c^2-1))$.

The same computation as in section 3 produces a homogeneous Weierstrass equation for $\mathrm{Jac}(D)(\mathbb{R})$ from equation (6), which is

$$-\gamma^2 T = \alpha(\alpha^2 - 4\alpha(\delta - 2)T + 16c^2T^2). \tag{7}$$

The double point B' of (6) splits in (7) into two simple points $[P_1]$, the origin of $\mathrm{Jac}(D)(\mathbb{R})$, and $[\bar{P}_1] = (\alpha, \gamma) = (0, 0)$. The two other points A_1, A_2 map to $[P_2] = (\alpha, \gamma) = (-4, -8a)$ and $[\bar{P}_2] = (-4c^2, -8ac^2)$. But as the neutral component of $\mathrm{Jac}(D)(\mathbb{R})$ is defined in (7) by $\alpha \leq 0$, $[\bar{P}_1]$ and $[\bar{P}_2]$ are on this neutral component. As C' is the complement of $\{P_1, \bar{P}_1, P_2, \bar{P}_2\}$ in D', the level of C is 3 by part *ii)* of Lemma 5.1. This provides the desired $C(3, 2)$ curve.

We are now in the same situation as in case A), but with an initial curve C that misses two pairs of points. If we remove the subvariety of C defined by $\prod_{j=1}^{s}(U^2 + m_j^2/4) = 0$ in (6) and (5), corresponding to $\prod_{j=1}^{s}((bZ - Y)^2 + m_j^2/4) = 0$ in (4) and (3), the resulting affine curve is a $2s+2$-pointed curve, for $s \geq 1$. The critical slopes are now $\pm 2\sqrt{\delta - 2 \pm 2c}$, and if, for every $j = 1$ to s, $m_j^2 > 4(\delta - 2 + 2c)$, the curve has level 3, and so is a $C(3, 2s + 2)$ curve. □

Example 5.4. As an explicit example, consider, for $s \geq 1$, the following affine $2s + 2$-pointed curve described with (Y, Z, T)-coordinates in $\mathbb{R}^3$ by

$$(Z^2 - Y^2 + 9)^2 + 36(Y^2 - 1) = 0, \qquad T\prod_{j=1}^{s}((Z - Y)^2 + (3 + j)^2) = 1.$$

It has level 3, because, with the notation above, $a = 3, b = 1, c = 1$, and the squares of the critical slopes are 36 and 20. Thus, the critical values for U^2 are 9 and 5, and $(3 + j)^2 > 9$ when $j \geq 1$. On the other hand, because 4 is smaller than the smallest critical value for U^2 (which is 5), the curve defined by the equations

$$(Z^2-Y^2+9)^2+36(Y^2-1) = 0, \qquad t((Z-Y)^2+4)\prod_{j=1}^{s-1}((Z-Y)^2+(3+j)^2) = 1$$

is a $C(2, 2s+2)$ curve.

We are only left to find a $C(2,2)$ curve. For this, one slightly modifies the equation 3 by taking

$$X^2 + Y^2 = -1, \qquad (X-a)^2 + Z^2 = c^2. \tag{8}$$

When $ac \neq 0 \in \mathbb{R}$, this defines a smooth affine geometrically integral 2-pointed curve, which may be described as the following affine plane quartic

$$(Z^2 - Y^2 - 1 + a^2 - c^2)^2 + 4a^2(Y^2+1) = 0. \tag{9}$$

It clearly has level 2, because $-1 = X^2 + Y^2$ is one of the equations in (8). This is the $C(2,2)$ example.

It is much easier to produce (somewhat simpler) examples of $C(2,r), C(3, 2s+1)$ for $s \geq 0, r \geq 1$, if we relax the requirement "genus 1" in the above proposition, and if we use the results below (Proposition 5.7, Proposition 5.9). However, these techniques do not seem to easily produce examples of $C(3, 2s)$ curves.

Recall some well-known features of the polynomials of the form $P(X) + Q(Y)$.

Proposition 5.5. *Let $P(T), Q(T) \in \mathbb{C}[T]$ be two polynomials of respective degrees m, n, and let C be the affine plane curve given by the equation $P(X) - Q(Y) = 0$. If $d = \gcd(m,n)$, then C' has exactly d points at infinity in a smooth projective model.*

Proof. Let $m = m_1 d$, $n = n_1 d$. Write $P = X^m(a + \epsilon(1/X)), Q = Y^n(b + \eta(1/Y)$ with $a, b \in \mathbb{C}^\star$, $\epsilon, \eta \in \mathbb{C}[T]$ such that $\epsilon(0) = \eta(0) = 0$, and put $u = 1/X, v = 1/Y$. In the convergent power series ring $\mathbb{C}\{u,v\}$, one has $a + \epsilon(u) = s^n, b + \eta(v) = t^m$, for certain units s, t. Then, if ξ is a primitive root of unity,

$$\frac{P(X) - Q(Y)}{X^m Y^n} = (sv)^n - (tu)^m = \prod_{i=1}^{d} ((sv)^{n_1} - \xi^i (tu)^{m_1}).$$

As m_1, n_1 are coprime, the terms $((sv)^{n_1} - \xi^i (tu)^{m_1})$ are irreducible in $\mathbb{C}\{u,v\}$ for every i and the factorization above is complete. After a sequence of blowings up, these d germs of analytic branches provide the d points at infinity. $\square$

Corollary 5.6. *Let $P(T), Q(T) \in \mathbb{R}[T]$ be nonnegative on $\mathbb{R}$, and assume that $P(X)+Q(Y)$ is irreducible in $\mathbb{C}[X,Y]$. Let $d = 2r = \gcd(\deg(P), \deg(Q))$. If the affine plane curve C defined by the equation $P(X) + Q(Y) = 0$ is smooth, it is an r-pointed curve.*

Proof. The curve C clearly has no real points, and is geometrically integral by assumption. Proposition 5.5 implies that C' misses $2r$ points at infinity, and these points must be pairwise conjugate. As C is smooth, it is an r-pointed curve. □

Example 5.7. For any integer $r > 0$, consider the Fermat curve given by the equation $X^{2r} + Y^{2r} + 1 = 0$. It is easy to see that the curve is smooth, geometrically integral, and that the level is 2. It follows immediately from corollary 5.6 that it is a $C(2, r)$ curve.

The following proposition is a useful tool in producing examples of level 3 curves of high degree.

Proposition 5.8. *Let C be a level 3, affine plane curve, defined over $\mathbb{R}$ by the equation $F(X,Y) = 0$. If $P(T), Q(T) \in \mathbb{R}[T]$ are any odd degree polynomials, then the curve $\tilde{C}$ defined by the equation $F(P(X), Q(Y)) = 0$ has level 3.*

Proof. We easily reduce to the case $Q(Y) = Y$. If $d = \deg(P)$, then the ring $\mathbb{R}[X]$ is an integral extension of degree d of $\mathbb{R}[P(X)]$. If $\alpha = P(X)$, then, for any polynomial $H \in \mathbb{R}[\alpha, Y]$, one has a degree d integral extension $\mathbb{R}[\alpha, Y]/H \longrightarrow \mathbb{R}[X,Y]/H$.

Let $H(X) = F(\alpha, Y) = F(P(X), Y)$. If $s(\tilde{C}) \leq 2$, then $-1 = u^2 + v^2 \in \mathbb{R}[X,Y]/H$, and if $N\colon \mathbb{R}[X,Y]/H \longrightarrow \mathbb{R}[\alpha,Y]/H$ is induced by the norm $\mathbb{R}[X] \longrightarrow \mathbb{R}[\alpha]$, one has $N(-1) = -1$ (because d is odd), and $N(u^2 + v^2) = s^2 + t^2$ (because $u^2 + v^2$ is itself a norm $N'\colon \mathbb{C}[X,Y]/H \longrightarrow \mathbb{R}[X,Y]/H$ "commuting" with N). This implies that the level of $\mathbb{R}[\alpha,Y]/F(\alpha,Y)$ is ≤ 2. But because $P(X)$ is transcendental over $\mathbb{R}$, $\alpha \mapsto X$ induces an isomorphism between $\mathbb{R}[\alpha]$ and $\mathbb{R}[X]$ and between $\mathbb{R}[\alpha,Y]/F(\alpha,Y)$ and $\mathbb{R}[X,Y]/F(X,Y)$ which has level 3. This contradiction shows that $s(\tilde{C}) = 3$. □

Example 5.9. Consider any odd positive integers r, s. It has been shown in the proof of Proposition 5.3 that $Y^2 + (X^2+2)^2 - 1 = 0$ is the equation of a $C(3,1)$ plane curve. Replacing X by X^{rs} and Y by Y^r, we consider the affine curve C given by the equation $Y^{2r} + (X^{2rs} + 2)^2 - 1 = 0$. Proposition 5.8

implies that C has level 3. Since it is smooth and geometrically integral, corollary 5.6 implies that it is an r-pointed curve and thus a $C(3,r)$ curve. The associated homogeneous curve is equipped with a morphism of degree $2r$ on $\mathbf{P}^1$, which is ramified at $4rs$ points of the affine part. Hence we may apply Hurwitz formula to see that the genus g of this curve is $g = 1+2r[s(2r-1)-1]$.

6 Sums of three squares

The following problem is still completely open: characterize the nonnegative polynomials in $\mathbb{R}[X,Y]$ which are sums of 3 squares of rational functions. It is well-known that nonnegative polynomials of $\mathbb{R}[X,Y]$ are sums of at most four squares of rational functions, and it has been proved that some of them are not a sum of only three squares. Cassels, Ellison and Pfister [CEP] first proved this for the Motzkin polynomial $X^2Y^4 + X^2(X^2-3)Y^2 + 1$. Later, Christie [Chr] used a variation of their proof, to show (up to filling a gap [Mac]) that a family of polynomials $P(X,Y) = Y^4 + a(X)Y^2 + b(X)$, with $a, b \in \mathbb{R}[X]$ also has this property. Both proofs are based on the fact that a square-free polynomial $P(Y) = Y^4 + aY^2 + b \in k[Y]$, k a formally real field, is a sum of three squares in $k(Y)$ if and only if a particular k-defined elliptic curve associated to the polynomial $P(Y)$, has a point of a particular type. More recently, Colliot-Thélène [CT2] proved that if the polynomial $P(X,Y) \in \mathbb{R}[X,Y]$, of degree at least 6, has sufficiently general coefficients (actually algebraically independent), then P is not a sum of three squares of rational functions. In [Mac] new families of such polynomials are given, using essentially the methods of Cassels, Ellison, Pfister.

In this section we will show that a variant of the ideas used in Theorem 1.2 and Theorem 1.8 may also be used to characterize the polynomials which are sums of three squares (Proposition 6.3, Theorem 6.5). We will finish the section by a new proof of Theorem 6.1 below.

In positive characteristic different from 2, every ring has level at most 2 and every sum of squares is a sum of at most 3 squares, and so the questions studied here would have no interest. Thus, every field used in this section is assumed to have characteristic 0.

Let us recall the starting point of [CEP]:

Theorem 6.1. [CEP][theorem 2.1] *Let k be a formally real field and $P(Y) = Y^4 + aY^2 + b \in k[Y]$ be a square-free polynomial. Then P is a sum of three*

squares in $k(Y)$ if and only if the elliptic curve $-\beta^2 = \alpha(\alpha^2 - 2a\alpha + a^2 - 4b)$ has a k-rational point (α, β) such that α and $-(\alpha^2 - 2a\alpha + a^2 - 4b)$ are sums of two squares in k (such a point is called special*).*

In [CEP], this elliptic curve and the condition on α appear in the course of some very explicit computation. We will prove this theorem at the end of the section using the general theory developed in the previous sections.

The equation $-\beta^2 = \alpha(\alpha^2 - 2a\alpha + a^2 - 4b)$ is actually a Weierstrass equation of the Jacobian curve of the smooth affine hyperelliptic quartic $Z^2 + P(Y) = 0$ defined over k, as computed in section 3. This is already an explanation of the presence of the elliptic curve in Theorem 6.1, and it is natural to feel that there should be a strong relationship with the material already discussed.

On the other hand, there is another known, simple characterization of sums of three squares:

Proposition 6.2. *Let k be a field, let $P(Y)$ be in $k[Y]$, monic and not the negative of a square in $k[Y]$, and let C be the affine plane curve given by the equation $Z^2 + P(Y) = 0$ defined over k. Then P is a sum of three squares in $k(Y)$ if and only if the level of the function field $k(C)$ is at most 2.*

Proof. see [CT2][lemma 1.2] □

Thus, knowing whether P is a sum of three squares in $k(Y)$ amounts to computing the level of $k(C)$, and this may be formulated in terms of Picard groups as in section 1, but with some significant differences.

If k is a field of level greater than 1, and D is a projective curve defined over k, one may use the formalism introduced at the beginning of section 1. Replacing $\mathbb{R}$ by k, $\mathbb{C}$ by $k' = k(\sqrt{-1})$ and $\Sigma = \mathrm{Gal}(k'/k) = \langle\sigma\rangle$. The short exact sequence (1) of section 1 becomes

$$0 \longrightarrow \mathrm{Pic}(D) \xrightarrow{p^*} \mathrm{Pic}(D')^{\Sigma} \xrightarrow{\delta} H^1(\Sigma, k'(D')^*/k'^*) \longrightarrow 0. \qquad (10)$$

Let $k[2]$ denote the multiplicative group of nonzero sums of two squares in k. The map $1 + \sigma\colon k'(D')^* \longrightarrow k(D)^*$ induces a group monomorphism $H^1(\Sigma, k'(D')^*/k'^*) \xrightarrow{\eta} k^*/k[2]$. Let $\pi = \eta\delta$.

Proposition 6.3. *Let k be a field of level greater than 1, $P \in k[Y]$ be monic, nonconstant and square-free, C be the plane affine k-curve defined by $Z^2 + P(Y) = 0$, and D be a smooth projective model of C. Then, with the above notation, P is a sum of three squares in $k(Y)$ if and only if $-1 \in \mathrm{Im}(\pi)$.*

Proof. As $-1 \notin k^2$ and P is nonconstant and square-free, k' and $k'(C') = k'(D')$ are fields and one may use the formalism above. Then $-1 \in \mathrm{Im}(\pi) = H^1(\Sigma, k'(D')^\star/k'^\star)$ if and only if there exists some $f \in k'(D')^\star$ such that $f \cdot \sigma f = -1$. This means that the level of $k(C)$ is at most 2 (actually exactly 2), or equivalently that P is a sum of three squares in $k(Y)$, by Proposition 6.2. □

Proposition 1.3 admits the following generalization.

Lemma 6.4. *Let k be a formally real field and $k' = k(\sqrt{-1})$. Let C (resp. D) be an affine (resp. projective) hyperelliptic curve of genus g defined by the square-free, monic, even degree polynomial P above, and let C' (resp. D') be its extension to k'. Let $A \in \mathrm{Div}(D')$ be such that $\mathrm{cl}(A) \in \mathrm{Pic}\, D'$ belongs to $\pi^{-1}(-1)$ in $\mathrm{Pic}(D')^\Sigma$. Then $\deg A = g - 1 \bmod 2$.*

Proof. The proof is essentially the same as for Proposition 1.3 (see [GH, proposition 2.2]). Let $A \in \mathrm{Div}(D')$ be such that $\mathrm{cl}(A) \in \pi^{-1}(-1) \subset \mathrm{Pic}(D')^\Sigma$, and let $L(A)$ denote the k'-vector space $L(A) = \{g \in k'(D') \mid \mathrm{div}(g) \geq -A\}$. Let $f \in k'(D')$ be such that $\mathrm{div}(f) = A - \sigma^\star A$. Because $A \in \pi^{-1}(-1)$, one has $N(f) = f\sigma f = -1$. For $g \in L(A)$, define $\tau(g) = \sigma(fg)$. As $\mathrm{div}(g) \geq -A$, one has $\mathrm{div}(\sigma(fg)) \geq \mathrm{div}(\sigma f) - \sigma^\star A = \sigma^\star A - A - \sigma^\star A = -A$. As $\tau^2(g) = -g$, τ defines an anti-linear automorphism of $L(A)$ such that $\tau^2 = -\mathrm{id}$. This implies that $l(A) = \dim(L(A))$ is even.

Since P is monic with even degree, there is a degree 2 divisor $U \in \mathrm{Div}(D)$ at infinity. Adding to A a large multiple of U if need be, one may assume that A has a large positive degree. Now the Riemann-Roch Theorem applies, and one has $l(A) = \deg(A) + 1 - g$. This shows that $\deg(A) = g - 1 \bmod 2$. □

Using this lemma, one may mimic Theorem 1.8 to get the following:

Theorem 6.5. *Let k, k', D, D', g be as above, with g odd, and π^0 be the restriction of π to $\mathrm{Pic}^0(D')^\Sigma$. Then P is a sum of three squares in $k(Y)$ if and only if $-1 \in \mathrm{Im}(\pi^0)$.*

Proof. Apply Proposition 6.3 to reduce to the existence of A such that $\pi(\mathrm{cl}\, A) = -1$ with $\mathrm{cl}\, A \in \mathrm{Pic}(D')^\Sigma$ and Lemma 6.4 to see that $\deg A$ is even. Then one may subtract from $\mathrm{cl}\, A$ the needed multiple of $\mathrm{cl}\, U$ in order to land in the preimage of π^0 in $\mathrm{Pic}^0(D')^\Sigma$. □

Theorem 6.5 admits two interesting consequences. The first one is a specialization to the case of a base field k in which every sum of squares is a sum of two squares (such as $\mathbb{R}(X)$), and gives a "topological" characterization of sums of three squares. Such a field k is said to have a "Pythagoras number" at most 2. Let us first give a definition.

Definition 6.6. Let k be a formally real field, and let A be an Abelian variety over k. Denote by k_γ the real closure of k for an ordering γ of k. A point $P \in A(k)$ is called *topologically special* if for each ordering γ of k, the point P_γ of $A(k_\gamma)$ is in the nonneutral (semi-algebraic) component of $A(k_\gamma)$.

Proposition 6.7. *Let k be a formally real field of Pythagoras number at most 2, let $P(Y)$ be a monic, square-free polynomial in $k[Y]$, of positive degree $d = 0 \bmod 4$, and let D be a smooth projective model of the affine plane k-curve $Z^2 + P(Y) = 0$. Then P is a sum of three squares in $k(Y)$ if and only if there is a point $[\mathrm{P}] \in \mathrm{Jac}(D)(k)$ which is topologically special.*

Proof. If $d = 0 \bmod 4$, the genus $g = (d-2)/2$ of D is odd and Theorem 6.5 implies that P is a sum of three squares if and only if there exists a point $[\mathrm{P}] \in \mathrm{Pic}^0(D')^\Sigma$ such that $\pi^0([\mathrm{P}]) = -1$. Then, for any ordering γ of k, $\pi^0([\mathrm{P}]_\gamma) = -1$ means that the point $[\mathrm{P}]_\gamma$ is on the nonneutral semi-algebraic component of $(\mathrm{Pic}^0 D'_\gamma)^\Sigma = \mathrm{Jac}(D_\gamma)(k_\gamma)$. Conversely, if there is a point $[\mathrm{P}] \in \mathrm{Pic}^0(D')^\Sigma$ such that for any ordering γ of k, the point $[\mathrm{P}]_\gamma$ is on the nonneutral component, then $\pi^0([\mathrm{P}]_\gamma) = -1$. Thus, if $[\mathrm{P}] = \mathrm{cl}(A)$, for $A \in \mathrm{Div}^0(D')$, and $f \in k(D')$ is a rational function such that $A - \bar{A} = \mathrm{div}(f)$, then $N(f)_\gamma$ is negative in k_γ, for every γ. Then, $N(f)$ is the negative of a sum of squares in k^*, and hence of a sum of two squares, by the assumption on the Pythagoras number of k. Therefore, $\pi([\mathrm{P}]) = -1 \in k^*/k[2]$ and $P(Y)$ is a sum of three squares in $k(Y)$. □

As the Pythagoras number of $\mathbb{R}(X)$ is 2, in the context of Theorem 6.1, the topologically special points are exactly the special points and so this particular case of Theorem 6.1 appears as a consequence of Proposition 6.7. But even more is true because for an arbitrary base field k, Theorem 6.1 may be viewed as a special case of Theorem 6.5:

Proof of Theorem 6.1

Let k be any field, $P(Y) = Y^4 + aY^2 + b \in k[Y]$ be square-free, and let D be the smooth projective curve associated to $Z^2 + P(Y) = 0$. Then the

Jacobian curve $\mathrm{Jac}(D)$ has an affine equation $-\beta^2 = \alpha(\alpha^2 - 2a\alpha + a^2 - 4b)$, and, associated to the order 2 point $S = (0,0) \in \mathrm{Jac}(D)$, there is a degree 2 isogeny $\mathrm{Jac}(D) \longrightarrow \mathcal{E} := \mathrm{Jac}(D)/\langle S \rangle$, together with an exact sequence

$$\mathcal{E}(k) \xrightarrow{\phi} \mathrm{Jac}(D)(k) \xrightarrow{\gamma} k^*/k^{*2},$$

with $\gamma(\alpha, \beta) = -\alpha k^{*2}$ when $\alpha \neq 0$. Now, $\mathrm{Jac}(D)$ acts on D by translation, and in particular the point S determines an involution u on D (given by $u(Y,Z) = (-Y,-Z)$). The quotient of D under this involution u, gives a curve $E = D/u$, and $\mathcal{E}$ is precisely the Jacobian of E.

There are two points at infinity in D' for $k' = k(\sqrt{-1}), D' = D \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, k'$. One of them (say O) has been chosen as the origin for $\mathrm{Jac}(D)$, and the other, which is the conjugate $\bar{O}$, is such that $\mathrm{cl}(\bar{O} - O)$ corresponds to the point $S = (0,0) \in \mathrm{Jac}(D)$. (This is a general feature of monic quartic polynomials of the form $P(Y) = Q(Y^2)$, as it can be already seen in the particular case $k = \mathbb{R}$ at corollaries 3.2 and 3.3.) The curve E has a k-rational point, corresponding to the class $\{O, \bar{O}\}$, and one has $\mathrm{Pic}^0(E) = \mathrm{Pic}^0(E')^{\Sigma} \simeq \mathrm{Jac}(E)(k)$. Let $\psi\colon D \longrightarrow E$ denote the 2-fold covering. Then, there is a morphism $\psi^*\colon \mathrm{Pic}^0(E) \longrightarrow \mathrm{Pic}^0(D)$, fitting in the following commutative diagram of exact sequences, with g being an isomorphism:

$$\begin{array}{ccccccc} & & \mathrm{Pic}^0(E) \simeq \mathrm{Jac}(E)(k) & \xrightarrow{\phi} & \mathrm{Jac}(D)(k) & \xrightarrow{\gamma} & k^*/k^{*2} \\ & & \downarrow \psi^* & & \downarrow g & & \\ 0 & \longrightarrow & \mathrm{Pic}^0(D) & \longrightarrow & \mathrm{Pic}^0(D')^{\Sigma} & \xrightarrow{\pi^0} & k^*/k[2] \end{array}$$

This shows that $\pi^0 g = \mathrm{Jac}(D)(k) \xrightarrow{\gamma} \mathrm{Im}\,\gamma \longrightarrow k^*/k[2]$.

Theorem 6.5 implies that the polynomial P is a sum of three squares in $k(Y)$ if and only if $-1 \in \mathrm{Im}\,\pi^0$. As this is equivalent to $-1 \in \mathrm{Im}\,\gamma$, this implies Theorem 6.1. □

For completeness sake, we briefly relate this material to the method used by Colliot-Thélène in [CT2]. In that paper, he proves that certain polynomials $P(X,Y) \in \mathbb{R}[X,Y]$ are not a sum of three squares of rational functions. For this, rather than considering the curve D over $\mathbb{R}(X)$ with affine equation $Z^2 + P(X,Y) = 0$, he treats it as a surface S over $\mathbb{R}$. The function field is the same and Proposition 6.2 still applies. Also, rather than considering the condition that the level of $\mathbb{R}(S)$ is ≤ 2, he uses the equivalent condition that the quaternion algebra $(-1,-1)$ splits over $\mathbb{R}(S)$.

Then, the exact sequence

$$0 \longrightarrow \mathrm{Pic}(S) \longrightarrow \mathrm{Pic}(S')^{\Sigma} \longrightarrow \mathrm{Br}(\mathbb{R}) \longrightarrow \mathrm{Br}(\mathbb{R}(S)),$$

is considered and the Noether-Lefschetz theorem is applied to the particular choice of S, giving the surjectivity of $\mathrm{Pic}(S) \longrightarrow \mathrm{Pic}(S')^{\Sigma}$, and so the injectivity of $\mathrm{Br}(\mathbb{R}) \longrightarrow \mathrm{Br}(\mathbb{R}(S))$. This provides the nonsplitting of $(-1,-1)$ over $\mathbb{R}(S)$, which is the desired conclusion.

References

[CEP] J.W.S. Cassels, W.J. Ellison and A. Pfister, On sums of squares and on elliptic curves over function fields, *J. of Number Theory* **3** (1971), 125-149.

[Chr] M. R. Christie, Positive Definite Rational Functions of Two Variables Which Are Not the Sum of Three Squares, *J. of Number Theory* **8** (1976), 224-232.

[Co] A. Comessatti, Sulle varietà Abeliane reali I, *Ann. Mat. Pura Appl.* **2** (1924), 67-106.

[CP] C. Ciliberto, C. Pedrini, Real Abelian varieties and real algebraic curves, Lectures in real geometry (Madrid, 1994), pp. 167–256, in "de Gruyter Exp. Math." **23**, 1996.

[CT1] J.-L. Colliot-Thélène, Variantes du Nullstellensatz réel et anneaux formellement réels, in "Géométrie Algébrique Réelle et Formes Quadratiques", pp. 98-108, *Lecture Notes in Math.* **959**, Springer, Berlin, 1982.

[CT2] J.-L. Colliot-Thélène, The Noether-Lefschetz theorem and sums of 4 squares in the rational function field $R(X,Y)$, *Compositio* **86** (1993), 235-243 .

[DL] Z.D. Dai, T.Y. Lam, Levels in Algebra and Topology, *Comment. Math. Math. Helvet.* **59** (1984), 376-424.

[Ge] W.-D. Geyer, Ein algebraischer Beweis des Satzes von Weichold über reelle algebraische Funktionenkörper, Algebraische Zahlentheorie (Ber. Tagung Math. Forschungsinst. Oberwolfach, 1964) pp. 83–98 Bibliographisches Institut, Mannheim, 1967.

[GH] B. Gross, J. Harris, Real algebraic curves, *Ann. scient. Ec. Norm. Sup.*, 4^e s»rie, **14** (1981), 157-182.

[Ma1] L. Mahé, Sommes de carrés et anneaux de Witt réduits, *C.R. Acad. Sc.* **300** (1985), 5-7.

[Ma2] L. Mahé, Level and Pythagoras number of some geometric rings, *Math. Z.* **204** (1990), 615-629 and Erratum, *Math. Z.* **209 (1992)**, 481-483.

[Mac] O. Macé, Sommes de trois carrés en deux variables et représentation de bas degré pour le niveau des courbes réelles, Thèse université de Rennes 1, 2000.

[Maz] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129-162.

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

[ST] J.H. Silverman, J. Tate, "Rational points on elliptic curves", in Undergraduate texts in mathematics, Springer-Verlag, 1992.

[We] G. Weichold, Über symmetrische Riemannsche Flächen und die Periodizitätsmoduln der zugehörigen Abelschen Normalintegrale erster Gattung (Leipziger Dissertation), Zeitschrift f. Math. u. Phys. 28, 321-351, 1883.

[Wi] E. Witt, Zerlegung reeller algebraischer Funktionen in Quadrate, *J. reine angew. Math.* **171** (1934), 4-11.