London Mathematical Society ISSN 1461–1570

HILBERT'S SEVENTEENTH PROBLEM AND HYPERELLIPTIC CURVES

VALÉRY MAHÉ

Abstract

This article deals with a constructive aspect of Hilbert's seventeenth problem: producing a collection of real polynomials in two variables, of degree 8 in one variable, which are positive but are not sums of three squares of rational fractions.

To do this we use a reformulation of this problem in terms of hyperelliptic curves due to Huisman and Mahé and we follow a method of Cassels, Ellison and Pfister which involves the computation of a Mordell–Weil rank over $\mathbb{R}(x)$.

Introduction

Let $P \in \mathbb{R}[X_1, \ldots, X_n]$ be a polynomial. If P is a sum of squares in $\mathbb{R}(X_1, \ldots, X_n)$ then P is a positive polynomial (that is, $P(x_1, \ldots, x_n)$ is nonnegative for every element $(x_1, \ldots, x_n) \in \mathbb{R}^n$). Conversely, when P is a positive polynomial one can ask whether P is a sum of squares in $\mathbb{R}(X_1, \ldots, X_n)$. This question is called Hilbert's seventeenth problem and was answered positively by Artin in 1927 (see [**1**]).

A related question is how to compute the minimal number r such that every positive polynomial can be written as a sum of r squares in $\mathbb{R}(X_1, \ldots, X_n)$. The answer is not completely known. Hilbert proved that every positive polynomial $P \in \mathbb{R}[X, Y]$ is a sum of four squares in $\mathbb{R}(X, Y)$ (see [**13**]). He proved a little more: every positive polynomial $P \in \mathbb{R}[X, Y]$ of total degree at most 4 is a sum of three squares of polynomials. The first of these two results was generalized by Pfister in the following way: every positive polynomial $P \in \mathbb{R}[X_1, \ldots, X_n]$ is a sum of 2^n squares in $\mathbb{R}(X_1, \ldots, X_n)$ (see [**25**]).

There is no known effective characterization of sums of three squares in $\mathbb{R}(X, Y)$. However, in 1971, Cassels, Ellison and Pfister showed that Motzkin's polynomial

$$M(X, Y) = 1 + X^2Y^4 + X^4Y^2 - 3X^2Y^2$$

is positive (thus a sum of four squares in $\mathbb{R}(X, Y)$), but is not a sum of three squares in $\mathbb{R}(X, Y)$ (see [**7**]). To prove this theorem, they consider, for each positive polynomial

$$F(X, Y) = 1 \ + \ A(X)Y^2 \ + \ B(X)Y^4$$

with $A, B \in \mathbb{R}(X)$ such that $B(A^2 - 4B) \neq 0$, the elliptic curve $\mathcal{E}_F$ defined over

This work is part of my PhD Thesis at the Université de Rennes 1 and was financed by the French government. The publication of this article was supported by EPSRC grant EP/E012590/1.
Received 12 October 2007, revised 14 January 2008; *published* 28 October 2008.
2000 Mathematics Subject Classification 14H40, 14G05, 14H05, 14P99, 14Q05
© 2008, Valéry Mahé

https://doi.org/10.1112/S1461157000000618 Published online by Cambridge University Press

$\mathbb{R}(x)$ by the equation

$$-\beta^2 = \alpha(\alpha^2 - 2A(x)\alpha + A(x)^2 - 4B(x))$$

and they show that F is a sum of three squares in $\mathbb{R}(X, Y)$ if and only if the elliptic curve $\mathcal{E}_F$ has an $\mathbb{R}(x)$-point (α, β) such that both

$$\alpha \quad \text{and} \quad -\left(\alpha^2 - 2A\left(x\right)\alpha + A\left(x\right)^2 - 4B(x)\right)$$

are sums of two squares in $\mathbb{R}(x)$ (i.e., take only nonnegative values on $\mathbb{R}$). A similar method allowed Christie (in 1976, see [**9**]), then Macé (in 2000, see [**18**]), and then Macé and Mahé (in 2005, see [**19**]) to construct other families of positive polynomials in two variables that are not sums of three squares of rational fractions.

Using a totally different strategy (based on the Noether–Lefschetz theorem [**11**]), Colliot-Thélène proved in 1993 the existence of positive polynomials in two variables, of degree in one of the variables even and greater than or equal to 6, that are not sums of three squares of rational fractions.

Using the method of Cassels, Ellison and Pfister one can only study polynomials of the form $F(X, Y) = 1 + A(X)Y^2 + B(X)Y^4$; we need the elliptic curve $\mathcal{E}_F$ above. In 2001, Huisman and Mahé generalized the construction of $\mathcal{E}_F$ by introducing the concept of antineutral point (see Definition 3.1.3). In [**15**], they showed that a nonconstant monic squarefree polynomial $P(X, Y)$ of degree in Y divisible by 4 is a sum of three squares in the field $\mathbb{R}(X, Y)$ if and only if an $\mathbb{R}(x)$-point of the Jacobian variety associated to the hyperelliptic curve $\mathcal{C}$ defined over $\mathbb{R}(x)$ by the equation $z^2 + P(x, y) = 0$ is antineutral.

In this article we generalize the method of Cassels, Ellison and Pfister using the results of Huisman and Mahé in order to construct families of positive polynomials in two variables, of degree 8 in one variable, that are not sums of three squares in $\mathbb{R}(x, y)$. As a corollary we get a positive polynomial with coefficients in $\mathbb{Q}$, of degree 8 in one variable, that is not a sum of three squares in $\mathbb{R}(x, y)$ (such an example was not known before). Using the notion of antineutral point, we also give examples of products of four sums of three squares in $\mathbb{R}(x, y)$ that are sums of three squares in $\mathbb{R}(x, y)$.

1. *Notation*

All the hyperelliptic curves we consider are smooth and projective. To simplify our statements we consider an elliptic curve as a genus 1 hyperelliptic curve (i.e., we do not assume a hyperelliptic curve to have genus at least 2).

The Jacobian variety associated to a curve $\mathcal{C}$ is denoted by $\mathrm{Jac}(\mathcal{C})$. For background on Mumford representation, semi-reduced divisors, reduced divisors and Cantor's algorithm we refer to [**23**] and [**5**] (see also [**10**] and [**12**]). A semi-reduced divisor with Mumford representation (u, v) is denoted by $\mathrm{div}(u, v)$. A linear equivalence class with Mumford representation (u, v) is denoted by $<u, v>$.

When D is a divisor on a curve $\mathcal{C}$ defined over a field k and K is an extension of k we denote by $\mathrm{Supp}_K(D)$ the support of D considered as a divisor on $\mathcal{C} \times_k K$.

For every abelian group A and for every $n \in \mathbb{N}^*$ we denote by $[n]_A$ (or $[n]$) the multiplication-by-n endomorphism of A, by $A[n]$ the kernel of $[n]_A$ and by A_{tors} the torsion subgroup of A.

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

For background on places of function fields we refer to [28] (we use notation from there; in particular by a function field over a field k we mean a transcendence degree 1 extension of k). When F_1 is a function field and F_2/F_1 is a finite extension and $\mathcal{P}$ is a place of F_2 above a place $\mathfrak{p}$ of F_1, we denote by $e(\mathcal{P}|\mathfrak{p})$ the ramification index of $\mathcal{P}$ above $\mathfrak{p}$ and by $f(\mathcal{P}|\mathfrak{p})$ the relative degree.

2. *Statement of the results*

NOTATION 2.1. Let η, ω and ρ be real numbers. We assume that $|\omega|$ and $|\eta|$ are distinct. Denote by b_1 the element

$$b_1 := \frac{\rho^2-\eta^2}{\omega^2-\eta^2} + \frac{\eta^2-\omega^2}{4}.$$

In this article we consider the polynomial

$$P(x^2,y^2) := \left(y^2+1\right)\left(y^2+C\left(x^2\right)\right)\left(y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)\right)$$

with

$$B(x) := (x+b_1)^2-\eta^2 \quad \text{and} \quad C(x) := 2(x+b_1)+\omega^2-\eta^2-1.$$

This polynomial is defined over the field $k := \mathbb{Q}(\eta,\omega,\rho)$. We denote by $\mathcal{C}$ the hyperelliptic curve defined over $k(x)$ by the affine equation $z^2+P(x^2,y^2)=0$.

ASSUMPTION 2.2. We assume the following three inequalities:

$$\omega > 1+|\eta|, \qquad \omega^2-\eta^2 > 2\omega \quad \text{and} \quad b_1 > 1+\frac{\omega^2-\eta^2}{2}.$$

ASSUMPTION 2.3. We assume that all the following elements are different from 0:

$$\eta,\ \rho,\ \left(\omega^2-\eta^2-2\right)^2-4\eta^2,\ \left(\omega^2-\eta^2-2\right)^2-4\eta^2-4,\ \left(\omega^2-\eta^2-1\right)^2-4\eta^2,$$
$$\left(\omega^2-\eta^2-1\right)^2-4\eta^2-1 \quad \text{and} \quad \left(\omega^2-\eta^2\right)^2-4\eta^2.$$

ASSUMPTIONS 2.4. We assume that none of the following elements is a square in k:

(1) $\left(\omega^2-\eta^2\right)^2-4\omega^2 = \left(\omega^2-\eta^2-2\omega\right)\left(\omega^2-\eta^2+2\omega\right)$,
(2) $(2b_1-2+\omega^2-\eta^2)(\omega^2-\eta^2-2\omega)$,
(3) $(2b_1-2+\omega^2-\eta^2)(\omega^2-\eta^2+2\omega)$,
(4) $2(\omega^2-\eta^2-2\omega)(b_1-1-\omega)$,
(5) $2(\omega^2-\eta^2+2\omega)(b_1-1+\omega)$,
(6) $2\left(2b_1-2+\omega^2-\eta^2\right)(b_1-1+\omega)$,
(7) $2\left(2b_1-2+\omega^2-\eta^2\right)(b_1-1-\omega)$,
(8) $\left((b_1-1)^2-\omega^2\right)\left(\left(\omega^2-\eta^2\right)^2-4\omega^2\right)$,
(9) $2\left(\omega^2-\eta^2\right)\left(\omega^2-\eta^2-2\omega\right)\left(\left(\omega+1\right)^2-\eta^2\right)^n$ (for each $n\in\{0,1\}$),
(10) $2\left(\omega^2-\eta^2\right)\left(\omega^2-\eta^2+2\omega\right)\left(\left(\omega-1\right)^2-\eta^2\right)^n$ (for each $n\in\{0,1\}$),
(11) $\left((b_1-1)^2-\omega^2\right)^{n_1}\left(\left(\omega-1\right)^2-\eta^2\right)^{n_2}\left(\left(\omega+1\right)^2-\eta^2\right)^{n_3}$,
(for each $(n_1,n_2,n_3)\in\{0,1\}^3-\{(0,0,0)\}$),
(12) $2\left(\omega^2-\eta^2\right)\left(2b_1-2+\omega^2-\eta^2\right)$,

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

(13) $2^{n_1}\left(\omega^2-\eta^2+2\omega\right)(b_1-1+\omega)\left(\omega^2-\eta^2\right)^{n_1}\left(2b_1-2+\omega^2-\eta^2\right)^{1-n_1}$
$\times(\omega-1-\eta)^{1-n_2}(\omega-1+\eta)^{n_2}$
(for each n_1, $n_2\in\mathbb{N}$),

(14) $2^{1-n_1}\left(\omega^2-\eta^2+2\omega\right)\left(\omega^2-\eta^2\right)^{n_1}\left(2b_1-2+\omega^2-\eta^2\right)^{n_1}$
$\times(\omega-1-\eta)^{1-n_2}(\omega-1+\eta)^{n_2}$
(for each n_1, $n_2\in\mathbb{N}$),

(15) $b_1^2-\eta^2$ and

(16) $2b_1+\omega^2-\eta^2-1$.

Remark. When we refer to a hypothesis by giving the associated number between two parentheses, we mean the corresponding hypothesis in Assumptions 2.4.

Theorem 2.5. *We use Notation 2.1. Then, under Assumptions 2.2, 2.3 and 2.4, the polynomial $P(x^2,y^2)$ is positive but is not a sum of three squares in $\mathbb{R}(x,y)$.*

Proof. Denote by $\mathcal{C}$ the hyperelliptic curve defined over $\mathbb{R}(x)$ by the affine equation

$$z^2+P(x^2,y^2)=0.$$

Proposition 3.1.4 asserts that $P(x^2,y^2)$ is a sum of three squares in $\mathbb{R}(x,y)$ if and only if $\mathrm{Jac}(\mathcal{C})$ has an antineutral point. From Corollary 4.3.6 we know that $\mathrm{Jac}(\mathcal{C})$ has no antineutral torsion point. Theorem 2.5 follows from the finiteness of the group $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ (this finiteness is a consequence of Theorem 5.4.3; to check its hypotheses we use Propositions 6.6, 6.7, 6.8 and 6.9). □

Corollary 2.6. *Consider the two polynomials*

$$B(x):=x^2+\frac{14063}{22}x+\frac{196743825}{1936}\quad\textit{and}\quad C(x):=2x+\frac{27835}{22}.$$

Then the positive polynomial with coefficients in $\mathbb{Q}$

$$P(x^2,y^2):=\left(y^2+1\right)\left(y^2+C\left(x^2\right)\right)\left(y^4+\left(1+C\left(x^2\right)\right)y^2+B\left(x^2\right)\right)$$

is not a sum of three squares in $\mathbb{R}(x,y)$.

Proof. Apply Theorem 2.5 with $\eta:=23$, $\omega:=34$ and $\rho:=547$. □

Corollary 2.7. *We use Notation 2.1. Under Assumptions 2.2, if η, ω, and ρ are algebraically independent over $\mathbb{Q}$, then the polynomial $P(x^2,y^2)$ is positive but is not a sum of three squares in $\mathbb{R}(x,y)$.*

In [**25**], Pfister showed the product of two sums of 2^n squares is a sum of 2^n squares. In general a product of two sums of three squares is not a sum of three squares. Looking for antineutral torsion points we give examples of products of four sums of three squares in $\mathbb{R}(x,y)$ that are sums of three squares in $\mathbb{R}(x,y)$.

Proposition 2.8. *Let α, β, $\gamma\in\mathbb{R}(x)^\times$ be three nonzero rational fractions. Consider the three rational fractions*

$$a:=1+\alpha^2(1+\beta^2)(1+\gamma^2),$$

$$b:=1+\alpha^2(1+\beta^2)^2(1+\gamma^2)\quad\textit{and}$$

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

$$c := 1 + \alpha^2(1+\beta^2)(1+\gamma^2)^2.$$

Then the polynomial $P(x,y) := (y^2+1)(y^2+a)(y^2+b)(y^2+c)$ *is a sum of three squares in* $\mathbb{R}(x,y)$:

$$\begin{aligned} P(x,y) \quad = \quad & \left(\tfrac{(a-1)y(y^2+a)}{\alpha} + \alpha\beta\gamma((1-\beta\gamma)y+\beta+\gamma)(y^2+1)\right)^2 \\ & + \left(\tfrac{(a-1)(y^2+a)}{\alpha} + \alpha\beta\gamma(1-\beta\gamma-(\beta+\gamma)y)(y^2+1)\right)^2 \\ & + \left((y^2+1)(y^2+a-\beta\gamma(a-1))\right)^2. \end{aligned}$$

Heuristic. Denote by $\mathcal{C}$ the hyperelliptic curve defined over $\mathbb{R}(x)$ by the affine equation $z^2 + P(x,y) = 0$. Proposition 2.8 is obtained by choosing the coefficients a, b, c such that $\mathrm{Jac}(\mathcal{C})$ has an antineutral point T of order 4:

- Proposition 4.2.1 and Proposition 4.2.2 give conditions on a, b, c for the existence of the point T;
- Proposition 3.2.1 gives conditions on a, b, c for the antineutrality of T.

3. *Sums of three squares and antineutral points*

3.1. *The results of Huisman and Mahé*

Let Σ be the Galois group $\mathrm{Gal}(\mathbb{C}(x)/\mathbb{R}(x)) = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and σ be its nontrivial element. Let $\boxed{2}_{\mathbb{R}(x)}$ be the group of nonzero elements of $\mathbb{R}(x)$ which are a sum of two squares in $\mathbb{R}(x)$.

Let $\mathcal{D}$ be a geometrically integral smooth projective curve over $\mathbb{R}(x)$ with odd genus. Let $\mathcal{D}' := \mathcal{D} \times_{\mathbb{R}(x)} \mathbb{C}(x)$ be its complexification and $p : \mathcal{D}' \longrightarrow \mathcal{D}$ be the projection. The Galois group Σ acts naturally on $\mathcal{D}'$. This action induces an action of Σ on the Picard group $\mathrm{Pic}(\mathcal{D}')$.

The projection p induces a morphism p^* from $\mathrm{Pic}(\mathcal{D})$ to $\mathrm{Pic}(\mathcal{D}')$. The image of p^* is contained in the subgroup $\mathrm{Pic}(\mathcal{D}')^\Sigma$ of Σ-invariant elements of $\mathrm{Pic}(\mathcal{D}')$. To characterize the image of p^*, we define a group homomorphism

$$\delta : \mathrm{Pic}(\mathcal{D}')^\Sigma \longrightarrow H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^\times/\mathbb{C}(x)^\times).$$

Let $cl(A) \in \mathrm{Pic}(\mathcal{D}')^\Sigma$ be the class of a divisor A. Because of the Σ-invariance of $cl(A)$, the divisor $A - \sigma^* A$ is the principal divisor associated to a function $f \in \mathbb{C}(x)(\mathcal{D}')^\times$. The principal divisor of $\mathbb{R}(x)(\mathcal{D})$ associated to $f\sigma(f)$ is 0. Thus $f\sigma(f)$ is an element of $\mathbb{R}(x)^\times$. The element $\delta(cl(A))$ is chosen as the class of f in $H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^\times/\mathbb{C}(x)^\times)$.

Lemma 3.1.1. *The following is an exact sequence:*

$$0 \longrightarrow Pic(\mathcal{D}) \xrightarrow{p^*} Pic(\mathcal{D}')^\Sigma \xrightarrow{\delta} H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^\times/\mathbb{C}(x)^\times) \longrightarrow 0.$$

Remark. The map δ is a coboundary map; it can be defined by looking at the long exact sequence associated to the short exact sequence:

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

Notation 3.1.2. We use the notation above. The map

$$1+\sigma \ : \ \mathbb{C}(x)(\mathcal{D}')^\times \ \longrightarrow \ \mathbb{R}(x)(\mathcal{D})^\times$$

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

induces a monomorphism

$$\eta : H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^\times/\mathbb{C}(x)^\times) \longrightarrow \mathbb{R}(x)^\times/\boxed{2}_{\mathbb{R}(x)}.$$

We denote by $\varpi : \mathrm{Pic}^0(\mathcal{D}')^\Sigma \longrightarrow \mathbb{R}(x)^\times/\boxed{2}_{\mathbb{R}(x)}$ the restriction of the map $\eta \circ \delta$ to $\mathrm{Pic}^0(\mathcal{D}')^\Sigma$.

Definition 3.1.3. *An element $\beta \in Pic^0(\mathcal{D}')^\Sigma$ is said to be antineutral when $\varpi(\beta) = -1$.*

Proposition 3.1.4. *Let $P(y) \in \mathbb{R}(x)[y]$ be a squarefree nonconstant monic totally positive polynomial of degree divisible by 4. Let $\mathcal{D}$ be the hyperelliptic curve defined over $\mathbb{R}(x)$ by the affine equation $z^2 + P(y) = 0$. We use Notation 3.1.2 (relative to $\mathcal{D}$). Then $P(y)$ is a sum of three squares in $\mathbb{R}(x, y)$ if and only if $Pic^0(\mathcal{D}')^\Sigma$ has an antineutral element.*

Proof. See [**15**, Theorem 6.5]. □

3.2. *An effective version*

Let k be a subfield of $\mathbb{R}$. Denote by k' the field $k(i)$. Let Σ be the Galois group $\mathrm{Gal}(k'(x)/k(x)) = \mathrm{Gal}(k'/k)$ and σ be its nontrivial element. Let $Q \in k(x)[y]$ be a monic polynomial such that $(y^2 + 1)Q(y^2)$ is squarefree. Let $\mathcal{C}$ be the hyperelliptic curve defined over $k(x)$ by the affine equation

$$\mathcal{C} : z^2 + (y^2 + 1)Q(y^2) = 0$$

and let $\mathcal{C}' := \mathcal{C} \times_{k(x)} k'(x)$ be its complexification.

Let g be the degree of the polynomial Q. Assume that g is odd and $d := -Q(-1) \in k(x)$ is nonzero. Let $\widetilde{\mathcal{C}}$ be the $k(x)$-hyperelliptic curve given in coordinates (s, t) by the affine equation

$$\widetilde{\mathcal{C}} : t^2 = -\frac{s}{d}(s - d)^{2g} Q\big(-\left(\tfrac{s+d}{s-d}\right)^2\big)$$

and let $\widetilde{\mathcal{C}}' := \widetilde{\mathcal{C}} \times_{k(x)} k'(x)$ be its complexification. The two curves $\mathcal{C}'$ and $\widetilde{\mathcal{C}}'$ have a $k'(x)$-rational point. The map

$$\begin{array}{rccc} \gamma : & k'(x)(\mathcal{C}') & \longrightarrow & k'(x)(\widetilde{\mathcal{C}}') \\ & A(y, z) & \longmapsto & A\left(i\frac{s+d}{s-d}, \frac{2idt}{(s-d)^{g+1}}\right) \end{array}$$

is an isomorphism. Denote by ω the $k'(x)$-automorphism $\sigma^{-1} \circ \gamma \circ \sigma \circ \gamma^{-1}$ of $k'(x)(\widetilde{\mathcal{C}}')$. This automorphism sends s to $\frac{d^2}{s}$ and t to $(-1)^g \frac{d^{g+1}t}{s^{g+1}}$. The $k'(x)$-automorphism ω induces a $k'(x)$-automorphism $\widetilde{\omega}$ of $\widetilde{\mathcal{C}}'$ and a $k'(x)$-automorphism Ω of $\mathrm{Jac}(\widetilde{\mathcal{C}}')$.

Remark. The curve $\mathcal{C}'$ has two $k'(x)$-rational Weierstrass points: $(s, t) = (i, 0)$ and $(s, t) = (-i, 0)$. The map γ is obtained by considering a map from $\mathcal{C}'$ to $\widetilde{\mathcal{C}}'$ that sends $(i, 0)$ to infinity and $(-i, 0)$ to $(0, 0)$.

Remark. The degree of the polynomial $\frac{s}{d}(s-d)^{2g}Q\big(-\left(\frac{s+d}{s-d}\right)^2\big)$ is odd. In particular the Mumford representation can be used to compute in the group $\mathrm{Jac}(\widetilde{\mathcal{C}}')(k'(x))$ (which can be identified with the group $\mathrm{Pic}^0(\widetilde{\mathcal{C}}')$).

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

REMARK. We consider the case $k = \mathbb{R}$. The group Σ acts on $\mathrm{Jac}(\widetilde{\mathcal{C}'})$ in two different ways:

- the natural action under base change of Σ on $\widetilde{\mathcal{C}} \times_{\mathbb{R}(x)} \mathbb{C}(x)$ induces an action $\sigma_{\star\widetilde{\mathcal{C}}}$ of σ on $\mathrm{Jac}(\widetilde{\mathcal{C}'})$; we also denote by $\sigma_{\star\widetilde{\mathcal{C}}}$ the corresponding action of σ on $\mathrm{Div}^0(\widetilde{\mathcal{C}'})$;
- looking at $\widetilde{\mathcal{C}}$ as a $\mathbb{C}(x)/\mathbb{R}(x)$-form of $\mathcal{C}$, the natural action under base change of Σ on $\mathcal{C} \times_{\mathbb{R}(x)} \mathbb{C}(x)$ can be transported into an action $\sigma_{\star\mathcal{C}}$ of σ on $\mathrm{Jac}(\widetilde{\mathcal{C}'})$; this action is the action of Σ on $\mathrm{Jac}(\widetilde{\mathcal{C}'})$ associated to the 1-cocycle $\Sigma \longrightarrow \mathrm{Aut}_{\mathbb{C}(x)}(\mathrm{Jac}(\widetilde{\mathcal{C}'}))$ whose value at σ is Ω (see [**3**]); we also denote by $\sigma_{\star\mathcal{C}}$ the corresponding action of σ on $\mathrm{Div}^0(\widetilde{\mathcal{C}'})$.

The action of Σ on $\mathrm{Jac}(\widetilde{\mathcal{C}'})$ involved in the definition of antineutral points is the action $\sigma_{\star\mathcal{C}}$.

PROPOSITION 3.2.1. *We use the notation above and Notation 3.1.2. We put $\tau := \sigma \circ \omega$. Let $\beta = <u, v>$ be a $\mathbb{C}(x)$-point of $\mathrm{Jac}(\widetilde{\mathcal{C}})$ such that $u(0) \neq 0$. Denote by $\check{v}$ the unique polynomial of degree less than or equal to $\deg(u)$ such that $\check{v}(0) = 0$ and $\check{v} \equiv v \bmod u$.*

1. *The point β is invariant under $\sigma_{\star\mathcal{C}}$ if and only if one of the two following conditions holds:*
   (a) either $\deg_s(u)$ is even and
   $$s^{\deg_s(u)}\tau(u) = \sigma(u(0))u(s) \quad \text{and} \quad -\left(\frac{s}{d}\right)^{g+1}\tau(v) \equiv v \bmod u,$$
   (b) or the degree of u is g and
   $$\left(\frac{s}{d}\right)^{g+1}\tau(\check{v}) = \check{v} \quad \text{and} \quad \sigma(u(0))(f - \check{v}^2) = su(s)s^g\tau(u(s)).$$
2. *If β is invariant under $\sigma_{\star\mathcal{C}}$ and the degree of u is strictly less than g, then $\varpi(\beta)$ is the identity element.*
3. *If β is invariant under $\sigma_{\star\mathcal{C}}$ and the degree of u is g, then β is antineutral if and only if $u(0)$ is a sum of squares in $\mathbb{R}(x)$. Moreover if β is antineutral, then we have $-d^{g-1} = u(0)h\tau(h)$ where h denotes the function $\frac{t+\check{v}}{su(s)}$.*

Proof. Let D be the semi-reduced divisor $\mathrm{div}(u, v)$. The point β is invariant under $\sigma_{\star\mathcal{C}}$ if and only if the divisors D and $\sigma_{\star\mathcal{C}}(D) = \sigma_{\star\widetilde{\mathcal{C}}}(\widetilde{\omega}(D))$ are linearly equivalent. To study the invariance of β under $\sigma_{\star\mathcal{C}}$, we use Cantor's algorithm (see [**5**]).

Let e and ϵ be respectively the quotient and the remainder of the Euclidean division of $\deg_s(u) + 1$ by 2. Using the definition of the Mumford representation for the two divisors D and $\widetilde{\omega}(D) + \mathrm{div}(s^e)$, and using the equalities

$$\omega(u) = u\left(\frac{d^2}{s}\right) \quad \text{and} \quad \omega(t - v) = (-1)^g\frac{d^{g+1}}{s^{g+1}}t - v\left(\frac{d^2}{s}\right),$$

we can check that the divisor $\widetilde{\omega}(D) + \mathrm{div}(s^e)$ is semi-reduced with Mumford representation

$$\left(\frac{1}{u(0)}s^{2e}u\left(\frac{d^2}{s}\right), \hat{v}\right)$$

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

where $\hat{v}$ denotes the remainder of the Euclidean division of

$$-\left(\frac{s}{d}\right)^{g+1} v\left(\frac{d^2}{s}\right) \qquad \text{by} \qquad s^{2e} u\left(\frac{d^2}{s}\right).$$

Case 1: *if the degree of u is strictly less than g.* Then the divisor $\sigma_{\star\widetilde{\mathcal{C}}}(\widetilde{\omega}(D))+\operatorname{div}(s^e)$ is reduced. In particular it can be linearly equivalent to D only if it is equal to D. In that case the degree of u is even (notice that the degree of $s^{2e}\sigma(u)(\frac{d^2}{s})$ is even). If β is invariant under $\sigma_{\star\mathcal{C}}$ then $D-\sigma_{\star\widetilde{\mathcal{C}}}(\widetilde{\omega}(D)) = \operatorname{div}(s^e)$ and thus $\varpi(\beta)$ is the identity element.

Case 2: *if the degree of u is equal to g.* We consider

1. w the remainder of the Euclidean division of $-\check{v}$ by $\frac{f-\check{v}^2}{su(s)}$;
2. $\widetilde{v}$ the remainder of the Euclidean division of $-\left(\frac{s}{d}\right)^{g+1}\sigma(v)(\frac{d^2}{s})$ by $s^{\deg(u)}\sigma(u)$.

The divisor $\sigma_{\star\widetilde{\mathcal{C}}}(\widetilde{\omega}(D)) - D$ is equal to

$$\operatorname{div}\left(\tfrac{1}{\sigma(u(0))}s^{\deg(u)}\sigma(u)\left(\tfrac{d^2}{s}\right),\widetilde{v}\right) - \operatorname{div}(s^{e-1}) - \operatorname{div}(su(s),\check{v}) =$$
$$\operatorname{div}\left(\tfrac{1}{\sigma(u(0))}s^{\deg(u)}\sigma(u)\left(\tfrac{d^2}{s}\right),\widetilde{v}\right) - \operatorname{div}\left(\tfrac{f-\check{v}^2}{su(s)},w\right) + \operatorname{div}\left(\tfrac{t+\check{v}}{s^e u(s)}\right).$$

Thus $\sigma_{\star\widetilde{\mathcal{C}}}(\widetilde{\omega}(D))-D$ is principal if and only if the two reduced divisors $\operatorname{div}\left(\frac{f-\check{v}^2}{su(s)},w\right)$ and $\operatorname{div}\left(\frac{1}{\sigma(u(0))}s^{\deg(u)}\sigma(u)\left(\frac{d^2}{s}\right),\widetilde{v}\right)$ are equal. If $\sigma(u(0))(f-\check{v}^2) = su(s)s^g\tau(u(s))$, then applying τ we show that $\widetilde{v}=w$ holds if and only if $\left(\frac{s}{d}\right)^{g+1}\tau(\check{v}) = \check{v}$ holds.

If β is invariant under $\sigma_{\star\mathcal{C}}$ then $\sigma(u(0))^{-1} = \frac{f-\check{v}^2}{s^{g+1}u(s)\tau(u)(s)}$ is σ-invariant (it is a τ-invariant element of $\mathbb{C}(x)$) and $\sigma_{\star\mathcal{C}}(D)-D = \operatorname{div}\left(\frac{t+\check{v}}{s^e u(s)}\right)$. In that case, since $\sigma(u(0))\left(\frac{t+\check{v}}{s^e u(s)}\right)\tau\left(\frac{t+\check{v}}{s^e u(s)}\right) = -1$, the image $\varpi(\beta)$ is the class of $-u(0)$. □

4. *Finding antineutral torsion points*

4.1. *The 2-primary torsion subgroup*

The following Proposition helps us to restrict our study of the existence of an antineutral torsion point to the search for an antineutral 2-primary torsion point.

PROPOSITION 4.1.1. *We use the notation of Proposition 3.1.4. Then $Pic^0(\mathcal{D}')^\Sigma$ has an antineutral torsion element if and only if $Pic^0(\mathcal{D}')^\Sigma$ has an antineutral 2-primary torsion element.*

Proof. Assume the existence of an antineutral torsion element D of $\operatorname{Pic}^0(\mathcal{D}')^\Sigma$. The order of D is $2^n m$ with $m\in\mathbb{N}$ odd and $n\in\mathbb{N}$. The morphism $\eta\circ\delta$ takes values in the group $\mathbb{R}(x)^\times/\boxed{2}_{\mathbb{R}(x)}$ which has exponent 2. Thus the image of a double under $\eta\circ\delta$ is the identity element. The integer m being odd, D and mD have the same image under $\eta\circ\delta$. As a consequence, the 2^n-torsion point mD is an antineutral point. □

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

4.2. *The image of the multiplication-by-2 map*

Let K be a characteristic 0 field and $\overline{K}$ be an algebraic closure of K. Let $\mathcal{H}$ be a hyperelliptic curve defined over K by an affine equation $\mathcal{H} : y^2 = f(x)$ where $f(x)$ is a monic separable polynomial of odd degree.

Let g be the genus of $\mathcal{H}$. The polynomial $f(x)$ has degree $2g+1$. Let $\alpha_1, \ldots, \alpha_{2g+1}$ be the roots of f in $\overline{K}$. Denote by ∞ the point at infinity of the curve $\mathcal{H}$ and by P_i the point $(\alpha_i, 0)$. Let $W := \{P_1, \ldots, P_{2g+1}, \infty\}$ be the set of Weierstrass points of $\mathcal{H}$. Denote by $\mathrm{Div}^0_W(\mathcal{H})$ the set

$$\{D \in \mathrm{Div}(\mathcal{H}) \mid \deg(D) = 0 \text{ and } \mathrm{Supp}_{\overline{K}}(D) \cap W = \emptyset\}.$$

Denote by L the algebra $K[T]/(f(T))$ and by $\overline{L}$ the algebra $\overline{K}[T]/(f(T))$. The class of a polynomial $u \in K[T]$ (respectively $u \in \overline{K}[T]$) in $L^\times/L^{\times 2}$ (respectively in $\overline{L}^\times/\overline{L}^{\times 2}$) is denoted by $[u]$.

We consider an element D of $\mathrm{Div}^0_W(\mathcal{H} \times_K \overline{K})$ (which is defined in the same way as $\mathrm{Div}^0_W(\mathcal{H})$ except that we replace K by $\overline{K}$). We write $D = \sum_{i \in I} n_i Q_i$ with $Q_i \notin W$ a point of $\mathcal{H} \times_K \overline{K}$. We define a map $\overline{\phi_{\mathcal{H}}} : \mathrm{Div}^0_W(\mathcal{H} \times_K \overline{K}) \longrightarrow \overline{L}^\times/\overline{L}^{\times 2}$ by sending D to the class

$$\overline{\phi_{\mathcal{H}}}(D) := \left[\prod_{i \in I} (x(Q_i) - T)^{n_i}\right] \in \overline{L}^\times/\overline{L}^{\times 2}.$$

Letting $\mathrm{Gal}(\overline{K}/K)$ act trivially on the class $[T] \in \overline{L}^\times/\overline{L}^{\times 2}$ we define a structure of $\mathrm{Gal}(\overline{K}/K)$-module on $\overline{L}$. We can think of L as the set of $\mathrm{Gal}(\overline{K}/K)$-invariant elements of $\overline{L}$. Doing this we deduce from $\overline{\phi_{\mathcal{H}}}$ a map $\phi_{\mathcal{H}} : \mathrm{Div}^0_W(\mathcal{H}) \longrightarrow L^\times/L^{\times 2}$.

PROPOSITION 4.2.1. *We use the notation above. Then the map $\phi_{\mathcal{H}}$ induces a morphism $\pi_{\mathcal{H}} : \mathrm{Jac}(\mathcal{H})(K) \longrightarrow L^\times/L^{\times 2}$ with kernel $2\mathrm{Jac}(\mathcal{H})(K)$ and with image contained in the kernel of the norm map $N_{L/K} : L^\times/L^{\times 2} \longrightarrow K^\times/K^{\times 2}$.*

Proof. See [**26**, Theorems 1.1 and 1.2]. □

REMARK. The morphism $\pi_{\mathcal{H}}$ can be described in terms of the Mumford representation. Assume $D \in \mathrm{Div}^0(\mathcal{H})$ is a semi-reduced divisor i.e. D can be written $D = \sum_{i \in I} n_i(Q_i - \infty)$ with $n_i \in \mathbb{N}$ and Q_i a point of $\mathcal{H}$ defined over $\overline{K}$ such that:

- $x(Q_i) \neq x(Q_j)$ for all $i \neq j$;
- $n_i \in \{0, 1\}$ when $y(Q_i) = 0$.

The Mumford representation for D is the unique couple (u, v) of elements of $k[T]$ such that:

- $u(T) = \prod_{i \in I} (T - x(Q_i))^{n_i}$ and $v(x(Q_i)) = y(Q_i)$;
- the degree of v is strictly less than $\deg_T(u)$;
- the polynomial $u(T)$ divides $v(T)^2 - f(T)$.

If the Mumford representation for D is (u, v) then $\pi_{\mathcal{H}}$ sends the linear equivalence class of D to the class $\left[(-1)^{\deg(u)} u(T)\right] \in L^\times/L^{\times 2}$.

To apply Proposition 4.2.1 we use the following characterization of the squares in a quadratic extension.

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

PROPOSITION 4.2.2. *Let k_0 be a field of characteristic different from 2. Let δ be an element of k_0 which is not a square in k_0. Denote by k the quadratic extension $k := k_0[U]/(U^2 - \delta)$.*

1. *Let α and β be two elements of k_0. We assume that α is nonzero. Then $\alpha U + \beta$ is a square in k if and only if there exist γ, $\eta \in k_0$ such that*
$$N_{k/k_0}(\alpha U + \beta) = \gamma^2 \quad \text{and} \quad \frac{\beta + \gamma}{2} = \eta^2.$$
2. *Let β be an element of k_0. Then β is a square in k if and only if β or $\delta\beta$ is a square in k_0.*

4.3. *A family of Jacobian varieties without antineutral torsion point*

NOTATION 4.3.1. Let B and C be two elements of $\mathbb{R}(x)$. We consider the polynomial $P(x, y^2) := (y^2 + 1)(y^2 + C)(y^4 + (1 + C)y^2 + B)$ which is assumed to be square-free. Let $\mathcal{C}$ be the hyperelliptic curve defined over $\mathbb{R}(x)$ by the affine equation $\mathcal{C} : z^2 + P(x, y^2) = 0$.

We use the notation of Proposition 3.2.1 relative to the curve $\mathcal{C}$. In particular we introduce $d := (1 - C)(B - C)$ and the three polynomials
$$g_1(s) := \frac{-(s + d)^2 + (s - d)^2}{-4d} = s,$$
$$g_2(s) := \frac{-(s + d)^2 + C(s - d)^2}{C - 1} \quad \text{and}$$
$$g_3(s) := \frac{(s + d)^4 - (1 + C)(s + d)^2(s - d)^2 + B(s - d)^4}{B - C}.$$

We denote by σ be the complex conjugation. The curve $\mathcal{C}' := \mathcal{C} \times_{\mathbb{R}(x)} \mathbb{C}(x)$ is birationally equivalent to the curve $\widetilde{\mathcal{C}}' := \widetilde{\mathcal{C}} \times_{\mathbb{R}(x)} \mathbb{C}(x)$ with $\widetilde{\mathcal{C}}$ the hyperelliptic curve defined over $\mathbb{R}(x)$ by the affine equation $\widetilde{\mathcal{C}} : t^2 = g_1(s)g_2(s)g_3(s)$. For every index $i = 1, 2, 3$, we denote by k_i the algebra $\mathbb{C}(x)[T]/(g_i(T))$. Let
$$\pi_{\widetilde{\mathcal{C}}} \ : \ \mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x)) \longrightarrow k_1^\times/k_1^{\times 2} \times k_2/k_2^{\times 2} \times k_3/k_3^{\times 2}$$
be the morphism obtained by applying Proposition 4.2.1 to the curve $\widetilde{\mathcal{C}}$. We denote by $\pi_{\widetilde{\mathcal{C}},i} \ : \ \mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x)) \longrightarrow k_i/k_i^{\times 2}$ the ith coordinate of $\pi_{\widetilde{\mathcal{C}}}$.

PROPOSITION 4.3.2. *We use Notation 4.3.1. We assume B, C and $(1 + C)^2 - 4B$ are not squares in $\mathbb{C}(x)$. Then the 2-torsion subgroup of $\mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x))$ is generated by the two points $<g_1, 0>$ and $<g_2, 0>$.*

Proof. The hypotheses imply that the three polynomials g_1, g_2 and g_3 are irreducible. This is sufficient since the 2-torsion points are the points $<u, 0>$ with u a divisor of $g_1g_2g_3$ of degree less than or equal to the genus g of the curve $\widetilde{\mathcal{C}}$ (see [**23**]). □

PROPOSITION 4.3.3. *We use Notation 4.3.1. We assume B, C and $(1 + C)^2 - 4B$ are not squares in $\mathbb{C}(x)$. If $<g_1, 0>$ is a double in $\mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x))$, then either*
$$(B - C) \ \in \ \mathbb{C}(x)^{\times 2} \quad \text{or} \quad C(B - C) \in \mathbb{C}(x)^{\times 2}.$$

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

Proof. The image of an element of $2\mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x))$ under $\pi_{\widetilde{\mathcal{C}},2}$ is trivial. In particular, if $<g_1, 0>$ is a double in $\mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x))$, then the class of $-T$ in k_2 is a square. The result is a reformulation of this condition obtained by using Proposition 4.2.2 together with the isomorphism

$$\begin{array}{rccc} \varphi_2 \ : & \mathbb{C}(x)[U]/(U^2 - 4C(B-C)^2) & \longrightarrow & k_2 \\ & U & \longmapsto & T + (1+C)(B-C)\,. \end{array}$$

□

PROPOSITION 4.3.4. *We use Notation 4.3.1 and the notation of Proposition 3.2.1. Then*

- *the point* $<s-d, 8d^3>$ *is an 8-torsion element of* $\mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x))$*;*
- *the double* $[2]<s-d, 8d^3>$ *is not* $\sigma_{\star\mathcal{C}}$*-invariant but* $[4]<s-d, 8d^3>$ *is equal to* $<g_1g_2, 0>$*.*

Proof. Use Cantor's algorithm (for the addition in $\mathrm{Jac}(\widetilde{\mathcal{C}'})(\mathbb{C}(x))$) and Proposition 3.2.1. □

PROPOSITION 4.3.5. *Let B and C be two elements of $\mathbb{R}(x)$. Let $\mathcal{C}$ be the hyperelliptic curve defined over $\mathbb{R}(x)$ by the affine equation*

$$z^2 + (y^2+1)(y^2+C)(y^4+(1+C)y^2+B) = 0.$$

We assume that B, C, $C(B-C)$, $B-C$, $(B-C)(1-C)$ and $(1+C)^2-4B$ are not squares in $\mathbb{C}(x)$. Then the 2-primary torsion subgroup of $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ is finite.

Proof. Since C, $1-C$, $B-C$, B and $(1+C)^2-4B$ are different from 0, the polynomial $P(x,y^2) := (y^2+1)(y^2+C)(y^4+(1+C)y^2+B)$ is squarefree.

We use Notation 4.3.1. Following Propositions 4.3.2 and 4.3.4, the 2-torsion subgroup $\mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x))[2]$ is generated by $<g_1, 0>$ and $<g_1g_2, 0> = [4]<s-d, 8d^3>$. In particular, since $<g_1, 0>$ is not a double, $\mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x))[8]$ is generated by $<g_1, 0>$ and $<s-d, 8d^3>$.

The image of $n_1<g_1, 0> + n_2<s-d, 8d^3>$ under $\pi_{\widetilde{\mathcal{C}},1}$ is $d^{6n_1}d^{n_2}$. Since d is not a square in k_1, a given 8-torsion point is a double if and only if it is a 4-torsion point. As a consequence every 2-primary torsion element of $\mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x))$ has order 8. In particular the 2-primary torsion subgroup of $\mathrm{Jac}(\widetilde{\mathcal{C}})(\mathbb{C}(x))$ is finite. □

COROLLARY 4.3.6. *We use the notation and hypotheses of Proposition 4.3.5. Then the group $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ has no antineutral torsion point.*

Proof. Using Proposition 3.2.1, we check that no 8-torsion point is antineutral (for a computation of the 8-torsion subgroup, see the proof of Proposition 4.3.5). □

5. *Simplifying some Mordell–Weil rank computations*

5.1. *An application of the Lang–Néron theorem*

THEOREM 5.1.1 (Lang, Néron). *Let k be a field. Let F be the function field of a variety defined over k. Let A be an abelian variety defined over F. We assume that no abelian subvariety B of A can be obtained by extension of scalar from an abelian variety defined over k and of dimension at least 1. Then the group of rational points $A(F)$ is finitely generated.*

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

Proof. See [**17**, Theorem 4.2]. □

COROLLARY 5.1.2. *Let B and C be two elements of $\mathbb{R}(x)$. Let $\mathcal{C}$ be the hyperelliptic curve defined over $\mathbb{R}(x)$ by the affine equation*

$$z^2 + (y^2+1)(y^2 + C(x^2))(y^4 + (1 + C(x^2))y^2 + B(x^2)) = 0.$$

We assume the polynomials $B(x^2)$, $C(x^2)$, $C(x^2)(B(x^2) - C(x^2))$, $B(x^2) - C(x^2)$, $(B(x^2) - C(x^2))(1 - C(x^2))$ and $(1 + C(x^2))^2 - 4B(x^2)$ are not squares in $\mathbb{C}(x)$. Then the abelian group $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ is finitely generated.

Proof. No abelian subvariety A of $\mathrm{Jac}(\mathcal{C})$ of dimension at least 1 can be defined by extension of scalar from an abelian variety defined over $\mathbb{C}$. In fact, if such a variety did exist, then the 2-primary torsion subgroup of $A(\mathbb{C})$ would be a set of infinite order (since $\mathbb{C}$ is algebraically closed) and we would have a contradiction with Corollary 4.3.5. Thus the hypotheses of Theorem 5.1.1 are satisfied. □

5.2. *Involutions and Mordell–Weil rank*

The group of rational points of a given Jacobian variety defined over a field k can be computed using divisor class groups of function fields. For the convenience of the reader we recall the definition of the divisor class group $\mathrm{Pic}(F/k)$ of a given function field F/k.

NOTATION 5.2.1. We use notation and definitions from [**28**]. Let k be a characteristic 0 field. Let F be a function field of full constant field k (i.e., a finite extension of $k(\alpha)$ for some transcendental element $\alpha \in F$ such that k is algebraically closed in F). Denote by $M_{F/k}$ the set of places of F/k.

We denote by $\mathrm{Div}(F/k)$ the group of divisors of F/k, i.e. the free abelian group generated by $M_{F/k}$, and by $\mathrm{Div}^0(F/k)$ (or $\mathrm{Div}^0(F)$) the subgroup of divisors of degree 0 of F/k, i.e. the subgroup of divisors

$$\sum_{\mathcal{P}\in M_{F/k}} n_{\mathcal{P}}\mathcal{P} \in \mathrm{Div}(F/k) \quad \text{such that} \sum_{\mathcal{P}\in M_{F/k}} n_{\mathcal{P}} = 0.$$

When F/k is a function field and f is an element of F, we denote by $\mathrm{div}_{F/k}(f)$ the principal divisor

$$\sum_{\mathcal{P}\in M_{F/k}} n_{\mathcal{P}} v_{\mathcal{P}}(f)$$

associated to f. We denote by $\mathrm{Pr}(F/k)$ the group of principal divisors of F/k, by $\mathrm{Pic}(F/k)$ the quotient group $\mathrm{Div}(F/k)/\mathrm{Pr}(F/k)$, and by $\mathrm{Pic}^0(F/k)$ (or $\mathrm{Pic}^0(F)$) the quotient group $\mathrm{Div}^0(F/k)/\mathrm{Pr}(F/k)$.

LEMMA 5.2.2. *We use the notation above. Then the order of the 4-torsion subgroup of $Pic^0(F/k)$ is finite.*

Proof. The field F is the function field of some geometrically integral smooth projective curve $\mathcal{D}$ defined over k. Since $\mathrm{Pic}^0(F/k)$ can be injected in $\mathrm{Jac}(\mathcal{D})(k)$, Lemma 5.2.2 follows from the finiteness of the order of $\mathrm{Jac}(\mathcal{D})(k)$[4]. □

NOTATION 5.2.3. Let F be a function field with full constant field k and let F_2 be a finite extension of F with full constant field k_2. When $\mathfrak{p}$ is a place of F/k, we

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

denote by $Cn_{F_2/F}(\mathfrak{p})$ the divisor $\sum_{\mathcal{P}|\mathfrak{p}} e(\mathcal{P}|\mathfrak{p})\mathcal{P} \in \mathrm{Div}(F_2/k_2)$. By linearity we get a homomorphism

$$Cn_{F_2/F} \ : \ \mathrm{Div}^0(F/k) \ \longrightarrow \ \mathrm{Div}^0(F_2/k_2).$$

The homomorphism $Cn_{F_2/F}$ induces a group homomorphism $CN_{F_2/F}$ from the quotient $\mathrm{Pic}^0(F/k)$ to the group $\mathrm{Pic}^0(F_2/k_2)$.

When ρ is an automorphism of a field F, we denote by F^ρ the subfield of ρ-invariant elements of F.

Proposition 5.2.4. *Let k be a characteristic 0 field. Let $P(T) \in k[T]$ be a nonconstant polynomial and let $\mathcal{H}$ be the hyperelliptic curve defined over k by the affine equation $z^2 + P(y) = 0$. Denote by $\iota : k(\mathcal{H}) \longrightarrow k(\mathcal{H})$ the hyperelliptic involution. Let $\rho : k(\mathcal{H}) \longrightarrow k(\mathcal{H})$ be an involution distinct from the identity map and from ι. We assume that the two involutions ι and ρ commute.*

Then the homomorphism $\varphi := +\circ\left(CN_{k(\mathcal{H})/k(\mathcal{H})^{\iota\circ\rho}} \times CN_{k(\mathcal{H})/k(\mathcal{H})^\rho}\right)$ has a finite kernel and its image contains $2Pic^0(k(\mathcal{H})/k)$.

Proof. We divide the proof into four steps.

Step 1. Let $\mathfrak{p}$ be a place of $k(\mathcal{H})^\rho$. Since $k(\mathcal{H})/k(\mathcal{H})^\rho$ is a degree 2 Galois extension with Galois group $\{\mathrm{Id}, \rho\}$,

1. for every place $\mathcal{P}$ above $\mathfrak{p}$ the ramification indexes $e(\mathcal{P}|\mathfrak{p})$ and $e(\rho(\mathcal{P})|\mathfrak{p})$ are equal (see [**28**, Corollary III.7.2]);
2. ρ induces a bijection from the set of places above $\mathfrak{p}$ into itself.

In particular every element of the image of $Cn_{k(\mathcal{H})/k(\mathcal{H})^\rho}$ is ρ-invariant.

Step 2. Let D be a divisor of $k(\mathcal{H})^\rho$ such that $Cn_{k(\mathcal{H})/k(\mathcal{H})^\rho}(D) = \mathrm{div}_{k(\mathcal{H})/k}(f)$ for some function $f \in k(\mathcal{H})$. Following Step 1, the divisor $Cn_{k(\mathcal{H})/k(\mathcal{H})^\rho}(2D)$ is equal to

$$\begin{aligned} Cn_{k(\mathcal{H})/k(\mathcal{H})^\rho}(D) + \rho(Cn_{k(\mathcal{H})/k(\mathcal{H})^\rho}(D)) &= \mathrm{div}_{k(\mathcal{H})/k}(f\rho(f)) \\ &= Cn_{k(\mathcal{H})/k(\mathcal{H})^\rho}(\mathrm{div}_{k(\mathcal{H})^\rho/k^\rho}(f\rho(f))) \end{aligned}$$

The injectivity of $Cn_{k(\mathcal{H})/k(\mathcal{H})^\rho}$ gives $2D = \mathrm{div}_{k(\mathcal{H})^\rho/k^\rho}(f\rho(f))$. This shows that the kernel of $CN_{k(\mathcal{H})/k(\mathcal{H})^\rho}$ is included in the 2-torsion subgroup of $\mathrm{Pic}^0(k(\mathcal{H})^\rho/k^\rho)$.

Step 3. Notice that Step 1 and Step 2 are still true when ρ is replaced by $\iota\circ\rho$. Let $(\alpha_\rho, \alpha_{\iota\circ\rho})$ be an element of $\mathrm{Ker}(\varphi)$. Then $CN_{k(\mathcal{H})/k(\mathcal{H})^{\iota\circ\rho}}(\alpha_{\iota\circ\rho}) = -CN_{k(\mathcal{H})/k(\mathcal{H})^\rho}(\alpha_\rho)$ is ι-invariant (since it is both ρ-invariant and $\iota\circ\rho$-invariant; see Step 1). Thus its order is at most 2. Applying Step 2 for $2\alpha_\rho$ and $2\alpha_{\iota\circ\rho}$ together with Lemma 5.2.2, we show there are only finitely many choices for α_ρ and $\alpha_{\iota\circ\rho}$.

Step 4. Let D be a degree 0 divisor of $k(\mathcal{H})/k$. Then $D + \rho\ (D)$ is in the image of $Cn_{k(\mathcal{H})/k(\mathcal{H})^\rho}$ and $D + \iota\circ\rho\ (D)$ is in the image of $Cn_{k(\mathcal{H})/k(\mathcal{H})^{\iota\circ\rho}}$. In particular the linear equivalence class of $D + \rho\ (D) + D + \iota\circ\rho\ (D)$ is in the image of φ. Since $\rho\ (D) + \iota\circ\rho\ (D)$ is principal, the image of φ contains the linear equivalence class of $2D$. □

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

LEMMA 5.2.5. *Let $\mathcal{D}$ be a smooth projective geometrically integral curve defined over $\mathbb{R}(x)$. Assume that $\mathcal{D}$ has a $\mathbb{C}(x)$-point. Then the following inclusions hold:*

$$2\mathrm{Jac}(\mathcal{D})(\mathbb{R}(x)) \subset Pic^0(\mathbb{R}(x)(\mathcal{D})) \subset \mathrm{Jac}(\mathcal{D})(\mathbb{R}(x)).$$

Proof. Let $\mathcal{D}' := \mathcal{D} \times_{\mathbb{R}(x)} \mathbb{C}(x)$ be the complexified of $\mathcal{D}$. Denote by Σ the Galois group $\mathrm{Gal}(\mathbb{C}(x)/\mathbb{R}(x)) = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Following Lemma 3.1.1 we have an exact sequence

$$0 \longrightarrow \mathrm{Pic}(\mathbb{R}(x)(\mathcal{D})) \xrightarrow{p^*} \mathrm{Pic}(\mathbb{C}(x)(\mathcal{D}'))^{\Sigma} \xrightarrow{\delta} H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times}).$$

Using p^* we identify $\mathrm{Pic}(\mathbb{R}(x)(\mathcal{D}))$ with a subgroup of $\mathrm{Pic}(\mathbb{C}(x)(\mathcal{D}'))^{\Sigma}$. The exponent of $H^1(\Sigma, \mathbb{C}(x)(\mathcal{D}')^{\times}/\mathbb{C}(x)^{\times})$ is 2. Thus $\ker(\delta) = \mathrm{Pic}(\mathbb{R}(x)(\mathcal{D}))$ contains $2\mathrm{Pic}(\mathbb{C}(x)(\mathcal{D}'))^{\Sigma}$. To conclude we notice that $\mathrm{Jac}(\mathcal{D})(\mathbb{R}(x)) = \mathrm{Pic}^0(\mathbb{C}(x)(\mathcal{D}'))^{\Sigma}$. □

PROPOSITION 5.2.6. *Let $P(T) \in \mathbb{R}(x)[T]$ be a nonconstant polynomial and $\mathcal{C}$ be the hyperelliptic curve defined over $\mathbb{R}(x)$ by the affine equation $z^2 + P(y^2) = 0$. Assume that $\mathcal{C}$ has a $\mathbb{C}(x)$-rational point and that $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ is finitely generated. Consider the two following $\mathbb{R}(x)$-hyperelliptic curves*

$$\mathcal{C}^+ : t^2 + sP(s) = 0 \quad \textit{and} \quad \mathcal{C}^- : \beta^2 + P(\alpha) = 0.$$

Then the Mordell–Weil rank of $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ is the sum of the Mordell–Weil ranks of the groups $\mathrm{Jac}(\mathcal{C}^+)(\mathbb{R}(x))$ and $\mathrm{Jac}(\mathcal{C}^-)(\mathbb{R}(x))$.

Proof. Apply Lemma 5.2.5 for $\mathcal{C}, \mathcal{C}^+$ and $\mathcal{C}^-$, and Proposition 5.2.4 to the involution $\rho : \mathbb{R}(x)(\mathcal{C}) \longrightarrow \mathbb{R}(x)(\mathcal{C}), A(y,z) \longmapsto A(-y,z)$. □

PROPOSITION 5.2.7. *Let k be a characteristic 0 field and $f(x,y) \in k(x)[y]$ be a polynomial of odd degree in y. Denote by $\mathcal{C}$ the hyperelliptic curve defined over $k(x)$ by the affine equation $z^2 = f(x^2, y)$. For each $\delta \in k(x)^{\times}$ denote by $\mathcal{C}_\delta$ the $k(x)$-hyperelliptic curve given by the affine equation $t^2 = \delta^{\deg_y(f)} f\left(x, \frac{s}{\delta}\right)$. Then the Mordell–Weil rank of $\mathrm{Jac}(\mathcal{C})(k(x))$ is the sum of the Mordell–Weil ranks of $\mathrm{Jac}(\mathcal{C}_1)(k(x))$ and $\mathrm{Jac}(\mathcal{C}_x)(k(x))$.*

Proof. Apply Proposition 5.2.4 to the the involution of $k(x)(\mathcal{C})$ preserving k, y and z, and sending x to $-x$. □

5.3. *A 2-descent*

5.3.1. *The application of a result of Christie*

PROPOSITION 5.3.1.1. *Let k_0 be a subfield of $\mathbb{C}$. Let $f \in k_0(x)[y]$ be a squarefree polynomial of odd degree and $\mathcal{C}$ be the hyperelliptic curve defined over $k_0(x)$ by the affine equation $z^2 = f(y)$. We assume that the 2-primary torsion subgroup of $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ is finite. Then $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ is equal to $\mathrm{Jac}(\mathcal{C})(K(x))$ for some finite extension K of k_0.*

Proof. For every $\mathbb{C}(x)$-point P of $\mathrm{Jac}(\mathcal{C})$ denote by K_P the smallest subfield of $\mathbb{C}$ containing k_0 and such that P is defined over $K_P(x)$. If K_P is not a finite extension of k_0, then K_P is a finite extension of $k_0(t_1, \ldots, t_n)$ with $t_1, \ldots, t_n$ algebraically independent over k_0. In that case, by specializing $t_1, \ldots, t_n$ over $\mathbb{C}$, the point P gives uncountably many $\mathbb{C}$-points of $\mathrm{Jac}(\mathcal{C})$. This is a contradiction because $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

is finitely generated (as in the proof of Corollary 5.1.2, apply Theorem 5.1.1). Thus K_P is a finite extension of k_0.

The group $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ is generated by a finite family $(P_i)_{i=1}^r$ (see Corollary 5.1.2). The smallest subfield K of $\mathbb{C}$ containing all the fields K_{P_i} is a finite extension of k_0 and the group $\mathrm{Jac}(\mathcal{C})(K(x))$ contains all the points P_i. In particular $\mathrm{Jac}(\mathcal{C})(\mathbb{C}(x))$ and $\mathrm{Jac}(\mathcal{C})(K(x))$ are equal. □

For a better understanding of the field K defined by Proposition 5.3.1.1, we use the following result of Christie.

PROPOSITION 5.3.1.2 (Christie [**9**]). *Let Γ be a finite group and $\mathcal{A}$ be a finitely generated free abelian group on which Γ acts. Assume the triviality of the action of Γ on $\mathcal{A}/2\mathcal{A}$. Then $\mathcal{A}$ has a basis $(a_i)_{i=1}^t$ such that $\tau(a_i) \in \{-a_i, a_i\}$ for every $\tau \in \Gamma$.*

PROPOSITION 5.3.1.3. *Let k be a subfield of $\mathbb{R}$. Let $f \in k(x)[y]$ be a polynomial of odd degree $2g+1$. Let $\mathcal{C}$ be the hyperelliptic curve defined over $k(x)$ by the affine equation $z^2 = f(y)$. Denote by J the Jacobian variety associated to $\mathcal{C}$. Assume that*

1. *the 2-primary torsion of $J(\mathbb{C}(x))$ is finite, and*
2. *the action of $\mathrm{Gal}(\mathbb{C}/k)$ on $J(\mathbb{C}(x))/2J(\mathbb{C}(x))$ is trivial.*

For each $d \in k^\times$ denote by $\mathcal{C}_d$ the hyperelliptic curve defined over $k(x)$ by the affine equation $z^2 = d^{2g+1} f(\frac{y}{d})$. Then the Mordell–Weil rank of $J(\mathbb{R}(x))$ is 0 if and only if for every positive element $d \in k^\times$ the $k(x)$-Mordell–Weil rank of $\mathrm{Jac}(\mathcal{C}_d)$ is 0.

Proof. Since the 2-primary torsion subgroup of $J(\mathbb{C}(x)$ is finite, Corollary 5.3.1.1 asserts the existence of a finite extension K of k such that $J(\mathbb{C}(x)) = J(K(x))$. The Galois group $\Gamma := \mathrm{Gal}(K/k)$ is finite. Following Theorem 5.1.1, the free abelian group $\mathcal{A} := J(K(x))/J(K(x))_{\mathrm{tors}}$ is finitely generated.

Let σ be the complex conjugation. Since the group $\Gamma := \mathrm{Gal}(\mathbb{C}/k)$ contains σ, the actions of Γ and σ commute (use Proposition 5.3.1.2). Thus Γ acts on the subgroup $\mathcal{A}^\sigma$ of σ-invariant elements of $\mathcal{A}$. The action of Γ on $\mathcal{A}/2\mathcal{A}$ is trivial. The quotient $\mathcal{A}$ being a free abelian group, the intersection $\mathcal{A}^\sigma \cap 2\mathcal{A}$ is equal to $2\mathcal{A}^\sigma$. This implies the triviality of the action of Γ on $\mathcal{A}^\sigma/2\mathcal{A}^\sigma$.

Assume that the Mordell–Weil rank of $J(\mathbb{R}(x))$ is different from 0. Applying Proposition 5.3.1.2 to $\mathcal{A}^\sigma$ and Γ we obtain a basis $(a_i)_{i=1}^t$ of $\mathcal{A}^\sigma$ such that $\tau(a_i) \in \{-a_i, a_i\}$ for every $\tau \in \Gamma$. Let $P_i \in J(K(x))$ be an element in the class a_i. Let m be the exponent of $J(K(x))_{\mathrm{tors}}$. The point mP_i is fixed by a subgroup Γ_i of Γ of index at most 2. The field K^{Γ_i} of elements in K invariant under the action of Γ_i is an extension of k of degree at most 2, i.e. is equal to $k(\sqrt{d_i})$ for some $d_i \in k^\times$. Since σ belongs to Γ_i, the field $k(\sqrt{d_i})$ is contained in $\mathbb{R}$. In particular d_i is positive.

If $\Gamma_i = \Gamma$, then mP_i is an element of $J(k(x)) = \mathrm{Jac}(\mathcal{C}_1)(k(x))$ of infinite order. Assume the existence of $\tau_i \in \Gamma$ such that $\tau_i(a_i) = -a_i$. Then d_i is not a square in k. The degree of f being odd, the curves $\mathcal{C}$ and $\mathcal{C}_{d_i}$ have a $k(x)$-rational point above the point at infinity of $\mathbb{P}^1$. Applying Proposition 5.2.4 for the involution τ_i we get the existence of an element of infinite order in $\mathrm{Jac}(\mathcal{C}_1)(k(x)) \times \mathrm{Jac}(\mathcal{C}_{d_i})(k(x))$.

Conversely, when for some positive element $d \in k^\times$ the group $\mathrm{Jac}(\mathcal{C}_d)(k(x))$ has an infinite order element P_1, a change of variable over $k(\sqrt{d})$ sends P_1 to an infinite order element of $\mathrm{Jac}(\mathcal{C})(k(\sqrt{d})(x)) \subset \mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$. □

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

5.3.2. *A first study of the image of $\pi_{\mathcal{C}}$*

Let k be a characteristic 0 field. For each monic polynomial $P(y) \in k(x)[y]$ denote by K_P the algebra $k(x)[y]/(P(y))$ and by y_P the class of y in K_P.

Let $f \in k[x][y]$ be a squarefree monic polynomial of odd degree and let $\mathcal{C}$ be the hyperelliptic curve defined over $k(x)$ by the affine equation $z^2 = f(y)$. Let $f(y) = \prod_{l \in \widetilde{I}} \mu_l(y)$ be the decomposition of $f(y)$ into monic prime elements of $k(x)[y]$. For each $l \in \widetilde{I}$ we assume that μ_l belongs to $k[x][y]$. Let $f'(y)$ be the usual derivative of $f(y)$. For each index $l \in \widetilde{I}$ denote by T_l the class $f'(y_{\mu_l})$ of $f'(y)$ in $K_{\mu_l} = k(x)[y]/(\mu_l(y))$.

PROPOSITION 5.3.2.1. *We use the notation above. Let l be an element of $\widetilde{I}$. We consider a semi-reduced divisor* $\operatorname{div}(u, v) \in \operatorname{Div}^0(k(x)(\mathcal{C}))$ *such that u is coprime to f.*

Then the finite places of K_{μ_l} at which $u(y_{\mu_l})$ has odd valuation are in the support $\operatorname{Supp}_{K_{\mu_l}}(T_l)$ *of* $\operatorname{div}(T_l)$.

NOTATION 5.3.2.2. We use the notation of Proposition 5.3.2.1. Let $u = \prod_{i \in I} p_i^{n_i}$ be the decomposition of u into monic prime elements of $K_{\mu_l}[y]$ (it exists since u is monic). Consider an index $i \in I$. Denote by K_{p_i,μ_l} the field $K_{\mu_l}[y]/(p_i(y))$ and by y_{p_i} the class of y in K_{p_i,μ_l}.

LEMMA 5.3.2.3. *We use Notation 5.3.2.2. We consider a finite place $\mathfrak{p}$ of K_{μ_l} such that $v_{\mathfrak{p}}(p_i(y_{\mu_l})) \neq 0$. If $\mathcal{P}$ is a place of K_{p_i,μ_l} above $\mathfrak{p}$ such that $v_{\mathcal{P}}(T_l) = 0$, then the valuation $v_{\mathcal{P}}(y_{p_i} - y_{\mu_l})$ is even.*

Proof. Assume that $v_{\mathcal{P}}(y_{p_i} - y_{\mu_l})$ is nonzero (if $v_{\mathcal{P}}(y_{p_i} - y_{\mu_l}) = 0$ the result is straightforward). From our hypotheses we know the coprimality of p_i and f. Following the definition of the Mumford representation we have $f(y) \equiv v(y)^2 \bmod p_i(y)$. In particular $v_{\mathcal{P}}(f(y_{p_i}))$ is even. Since $\mu_l(y)$ divides $f(y)$, the element $f(y_{\mu_l})$ is equal to 0. Taylor's formula gives

$$f(y_{p_i}) = (y_{p_i} - y_{\mu_l}) \Big(T_l + (y_{p_i} - y_{\mu_l})^{2g} + \Big(\sum_{j=1}^{2g-1} f_j (y_i - y_{\mu_l})^j \Big) \Big) \tag{1}$$

where $f_j \in K_{\mu_l}$ satisfies $v_{\mathfrak{p}}(f_j) \geqslant 0$ (because $f \in k[x][y]$). Lemma 5.3.2.3 is obtained by applying the parity of $v_{\mathcal{P}}(f(y_{p_i}))$ and the parity of

$$v_{\mathcal{P}} \Big(T_l + (y_{p_i} - y_{\mu_l})^{2g} + \Big(\sum_{j=1}^{2g-1} f_j (y_{p_i} - y_{\mu_l})^j \Big) \Big)$$

(which is equal to either $v_{\mathcal{P}}(T_l)$ or $v_{\mathcal{P}}((y_{p_i} - y_{\mu_l})^{2g})$; use the triangle inequality) to equation (1). □

Proof of Proposition 5.3.2.1. We use Notation 5.3.2.2. Let $\mathfrak{p}$ be a finite place of K_{μ_l} at which $p_i(y_{\mu_l})$ has odd valuation. Assume that $v_{\mathfrak{p}}(T_l)$ is equal to 0. For each place $\mathcal{P}$ of K_{p_i,μ_l} above $\mathfrak{p}$, the valuation $v_{\mathcal{P}}(T_l) = e(\mathcal{P}|\mathfrak{p}) v_{\mathfrak{p}}(T_l)$ is equal to 0. Following Lemma 5.3.2.3, for each place $\mathcal{P}$ above $\mathfrak{p}$, the valuation $v_{\mathcal{P}}(y_{p_i} - y_{\mu_l})$ is even. A classical computation shows that $v_{\mathfrak{p}}(N_{K_{p_i,\mu_l}/K_{\mu_l}}(y_{p_i} - y_{\mu_l}))$ is equal to

$$\sum_{\mathcal{P} \text{ place of } K_{p_i,\mu_l} \text{ above } \mathfrak{p}} f(\mathcal{P}|\mathfrak{p}) v_{\mathcal{P}}(y_{p_i} - y_{\mu_l})$$

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

(see [**30**] for the Dedekind rings case). Thus $v_{\mathfrak{p}}(p_i(y_{\mu_l}))$ is even. This contradicts our choice for the place $\mathfrak{p}$. □

5.3.3. *The action of the Galois group modulo the doubles*
Let $k \subset \mathbb{R}$ be a field and $\mathcal{C}$ be a hyperelliptic curve over $k(x)$ such that the 2-primary torsion of $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ is finite. To compute the Mordell–Weil rank of $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$, we want to do a 2-descent by applying Proposition 5.3.1.3. The hypotheses of Proposition 5.3.1.3 are not satisfied in general. Proposition 5.3.3.1 gives conditions on $\mathcal{C}$ under which Proposition 5.3.1.3 can be applied.

PROPOSITION 5.3.3.1. *Let k be a subfield of $\mathbb{R}$. Let $f(y) \in k[x][y]$ be a squarefree monic polynomial of odd degree $2g+1$. Denote by $\mathcal{C}$ the hyperelliptic curve defined over $k(x)$ by the affine equation $z^2 = f(y)$. We assume the existence of $2g$ elements $e_1, \ldots, e_{2g-1}, H$ of $k[x]$ and the existence of a polynomial $\mu(y) \in k[x][y]$ of degree 2 such that*

$$f(y) \;=\; \mu(y) \prod_{i=1}^{2g-1} (y - He_i).$$

We also assume:

- *the discriminant $\Delta(f)$ of $f(y)$ splits into linear factors over k,*
- *the discriminant $\Delta(\mu)$ of μ is equal to H^2Q^2D with $D \in k[x]$ a polynomial of degree 1 and $Q \in k[x]$,*
- *$\Delta(f) = Q^2Q_1$ with $Q_1 \in k[x]$ coprime to Q, and*
- *$D(\alpha)$ is a square in k for every root $\alpha \in k$ of H.*

Denote by L the algebra $\mathbb{C}(x)[t]/(f(t))$. Let $\pi_{\mathcal{C}} : \mathrm{Jac}(\mathcal{C})(\mathbb{C}(x)) \longrightarrow L^{\times}/L^{\times 2}$ be the morphism defined by Proposition 4.2.1. Then the action of $\mathrm{Gal}(\mathbb{C}/k)$ on the image of $\pi_{\mathcal{C}}$ is trivial.

LEMMA 5.3.3.2. *We keep the notation and hypotheses of Proposition 5.3.3.1. We assume that μ is irreducible. We denote by $K_{\mu,\mathbb{C}}$ the algebra $\mathbb{C}(x)[y]/(\mu(y))$ and by y_μ the class of y in $K_{\mu,\mathbb{C}}$. We denote by s the element $\frac{\mu'(y_\mu)}{2HQ}$. Then the minimal polynomial of s over $\mathbb{C}(x)$ is $y^2 - D(x)$. Thus $\mathbb{C}[x,s]$ is a unique factorization domain and its fractions field is $K_{\mu,\mathbb{C}}$.*

LEMMA 5.3.3.3. *We keep the notation and hypotheses of Lemma 5.3.3.2. Let $\alpha \in k$ be a root of the resultant $\mathrm{Res}_T(f'(T), \mu(T))$ such that $Q(\alpha) \neq 0$. Let β be a prime element of $\mathbb{C}[x,s]$ such that $N_{K_{\mu,\mathbb{C}}/\mathbb{C}(x)}(\beta) = \lambda(x-\alpha)$ for some constant $\lambda \in \mathbb{C}$. Then the valuation v_β is invariant under the action of $\mathrm{Gal}(\mathbb{C}/k)$.*

Proof. Since it belongs to $\mathbb{C}[x,s]$, the element β can be written as $\beta = \beta_1 s + \beta_0$ with $\beta_0, \beta_1 \in \mathbb{C}[x]$. The degree of D is 1 and $\lambda(x-\alpha)$ is equal to $\mathbb{N}_{\mathbb{C}(x)(s)/\mathbb{C}(x)}(\beta) = \beta_0^2 - \beta_1^2 D$. Thus β_0 and β_1 are in $\mathbb{C}$ and $\beta_0^2 = \beta_1^2 D(\alpha)$. Lemma 5.3.3.3 is proven by noticing that if $D(\alpha)$ is a square in k then $\widetilde{\lambda}\beta$ belongs to $k[x,s]$ for some $\widetilde{\lambda} \in \mathbb{C}^{\times}$.

The resultant $\mathrm{Res}_T(f'(T), \mu(T))$ is equal to $\Delta(\mu)\prod_{i=1}^{2g-1}\mu(He_i)$ with $\Delta(\mu) = H^2Q^2D$. Hence α is either a root of H or a root of D or a root of $\prod_{i=1}^{2g-1}\mu(He_i)$. If α is a root of H or a root of D, then $D(\alpha)$ is a square in k. Assume $H(\alpha) \neq 0$ and $\mu(He_i)(\alpha) = 0$ for some index i. Applying Taylor's formula to $\mu(T)$ at He_i we get

$$\mu(T) = (T - He_i)^2 + (T - He_i)\mu'(He_i) + \mu(He_i).$$

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

From this equality we deduce $\Delta(\mu)$: it is equal to $(\mu'(He_i))^2 - 4\mu(He_i)$. In particular,

$$D(\alpha) = \frac{\Delta(\mu)(\alpha)}{(H(\alpha)Q(\alpha))^2} = \left(\frac{\mu'(He_i)(\alpha)}{H(\alpha)Q(\alpha)}\right)^2$$

is a square in k. □

LEMMA 5.3.3.4. *We keep the notation and hypotheses of Lemma 5.3.3.2. Let $\alpha \in k$ be a root of Q and β be a prime element of $\mathbb{C}[x,s]$ such that $N_{K_{\mu,\mathbb{C}}/\mathbb{C}(x)}(\beta) = \lambda(x-\alpha)$ for some constant $\lambda \in \mathbb{C}^\times$.*

Let $\operatorname{div}(u,v) \in \operatorname{Div}^0(\mathbb{C}(x)(\mathcal{C}))$ be a semi-reduced divisor with u coprime to f and let σ be an element of $\operatorname{Gal}(\mathbb{C}/k)$. Then the valuation $v_\beta(u(y_\mu)\sigma(u(y_\mu)))$ is even.

Proof. The polynomial μ admits y_μ as a root in $K_{\mu,\mathbb{C}}$ and is totally split over $K_{\mu,\mathbb{C}}$. Denote by ι the unique $\mathbb{C}(x)$-automorphism of $K_{\mu,\mathbb{C}} = \mathbb{C}(x)(y_\mu)$ sending y_μ to the other root of μ. Since $\beta\iota(\beta) = N_{\mathbb{C}(x,s)/\mathbb{C}(x)}(\beta) = \lambda(x-\alpha)$, the set of prime factors of $\lambda(x-\alpha)$ is $\{\beta, \iota(\beta)\}$. Thus, $x-\alpha$ being σ-invariant, the sets $\{\sigma^{-1}(\beta), \sigma^{-1}\circ\iota(\beta)\}$ and $\{\beta, \iota(\beta)\}$ are equal. When $v_\beta = v_{\sigma^{-1}(\beta)}$ the result is straightforward.

Assume that $v_{\sigma^{-1}(\beta)} = v_{\iota(\beta)} = v_{\iota^{-1}(\beta)}$. Since it divides Q_1 the polynomial $f'(He_i)$ is coprime to $x-\alpha$. Following Proposition 5.3.2.1 this implies the parity of the valuations $v_{x-\alpha}(u(He_i))$ and $v_\beta(u(He_i)) = e(\beta|x-\alpha)v_{x-\alpha}(u(He_i))$.

Denote by $K_{u,\mu,\mathbb{C}}$ the algebra $K_{\mu,\mathbb{C}}[y]/(u(y))$. By definition of the Mumford representation,

$$f(y) = (y-y_\mu)(y-\iota(y_\mu))\prod_{i=1}^{2g-1}(y-He_i)$$

is a square modulo u. In particular the valuation at β of

$$N_{K_{u,\mu,\mathbb{C}}/K_{\mu,\mathbb{C}}}(f(y)) = u(y_\mu)u(\iota(y_\mu))\prod_{i=1}^{2g-1}u(He_i)$$

is even. Since $v_\beta(u(He_i))$ is also even, we get the parity of $v_\beta(u(y_\mu)u(\iota(y_\mu))$. This is enough to conclude because $v_{\sigma^{-1}(\beta)} = v_{\iota^{-1}(\beta)}$. □

Proof of Proposition 5.3.3.1. For every prime factor $p \in \mathbb{C}[x][y]$ of f denote by $K_{p,\mathbb{C}}$ the field $\mathbb{C}(x)[y]/(p(y))$ and by y_p the class of y in $K_{p,\mathbb{C}}$. Under the hypotheses of Proposition 5.3.3.1 the field $K_{p,\mathbb{C}}$ is the fraction field of a unique factorization domain $\mathcal{O}_{p,\mathbb{C}}$ (see Lemma 5.3.3.2).

Let $\operatorname{div}(u,v) \in \operatorname{Div}^0(\mathbb{C}(x)(\mathcal{C}))$ be a semi-reduced divisor with u coprime to f, let p be a prime factor of f and let σ be an element of $\operatorname{Gal}(\mathbb{C}/k)$. We prove that the class of $u(y_p)\sigma(u(y_p))$ in $K_{p,\mathbb{C}}$ is a square. Since every element of $\mathcal{O}_{p,\mathbb{C}}^\times = \mathbb{C}^\times$ is a square and since $\mathcal{O}_{p,\mathbb{C}}$ is a unique factorization domain it is sufficient to show that $v_\beta(u(y_p)\sigma(u(y_p)))$ is even for every prime $\beta \in \mathcal{O}_{p,\mathbb{C}}$.

Assume the existence of a prime element $\beta \in \mathcal{O}_{p,\mathbb{C}}$ such that $v_\beta(u(y_p)\sigma(u(y_p))) = v_\beta(u(y_p)) + v_{\sigma^{-1}(\beta)}(u(y_p))$ is odd. Eventually replacing β by $\sigma^{-1}(\beta)$ we can assume that $v_\beta(u(y_p))$ is odd and that $v_{\sigma^{-1}(\beta)}(u(y_p))$ is even. Following Proposition 5.3.2.1 the norm $N_{K_{p,\mathbb{C}}/\mathbb{C}(x)}(\beta)$ is a divisor of $N_{K_{p,\mathbb{C}}/\mathbb{C}(x)}(f'(y_p)) = \operatorname{res}_T(f'(T), p(T))$. In particular $N_{K_{p,\mathbb{C}}/\mathbb{C}(x)}(\beta)$ divides $\Delta(f)$. Since $\Delta(f)$ splits into linear factors over k the norm $N_{K_{p,\mathbb{C}}/\mathbb{C}(x)}(\beta)$ is equal to $\lambda(x-\alpha)$ for some $\lambda \in \mathbb{C}^\times$ and some $\alpha \in k$.

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

Case 1: *if the degree of p is* 1. Then β is equal to $\lambda(x-\alpha)$. In particular the valuations v_β and $v_{\sigma(\beta)}$ are equal. This is in contradiction with the definition of β.

Case 2: *if $p=\mu$ is an irreducible polynomial of degree* 2. Then we apply Lemma 5.3.3.3 and Lemma 5.3.3.4. □

COROLLARY 5.3.3.5. *We use Notation 2.1. We assume that the elements η, ω, ρ, $\omega^2-\eta^2$, $2b_1-2+\omega^2-\eta^2$, $\left(\omega^2-\eta^2-2\right)^2-4\eta^2$, $\left(\omega^2-\eta^2\right)^2-4\omega^2$, $\left(\omega^2-\eta^2-1\right)^2-4\eta^2$, $2b_1+\omega^2-\eta^2-1$, $b_1^2-\eta^2$ and $(b_1-1)^2-\omega^2$ are nonzero. For each $\delta\in k(x)^\times$ denote respectively by $\mathcal{C}_\delta^+$ and $\mathcal{C}_\delta^-$ the two following $k(x)$-hyperelliptic curves:*

$$\mathcal{C}_\delta^+ : z^2 = y(y-\delta)(y-\delta C(x))(y^2-\delta[1+C(x)]y+\delta^2B(x)) \quad \textit{and}$$
$$\mathcal{C}_\delta^- : z^2 = y(y^2-\delta[(1-C(x))^2-2(B(x)-C(x))]y+\delta^2[B(x)-C(x)]^2).$$

Then the $\mathbb{R}(x)$-Mordell–Weil rank of $\mathrm{Jac}(\mathcal{C})$ *is zero if and only if for every positive element $\zeta\in k^\times$ the $k(x)$-Mordell–Weil ranks of* $\mathrm{Jac}(\mathcal{C}_\zeta^+)$, $\mathrm{Jac}(\mathcal{C}_{\zeta x}^+)$, $\mathrm{Jac}(\mathcal{C}_\zeta^-)$ *and* $\mathrm{Jac}(\mathcal{C}_{\zeta x}^-)$ *are zero.*

Proof. Following Proposition 5.2.6, the Mordell–Weil rank of $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ is the sum of the Mordell–Weil ranks of $\mathrm{Jac}(\mathcal{C}^+)(\mathbb{R}(x))$, $\mathrm{Jac}(\mathcal{C}^-)(\mathbb{R}(x))$ with

$$\mathcal{C}^+ : \beta^2 = \alpha(\alpha-1)(\alpha-C(x^2))\left(\alpha^2-[1+C(x^2)]\alpha+B(x^2)\right),$$
$$\mathcal{C}^- : \beta^2 = \alpha\left(\alpha^2-[(1-C(x^2))^2-2(B(x^2)-C(x^2))]\alpha+(B(x^2)-C(x^2))^2\right).$$

Applying Proposition 5.2.7 to $\mathcal{C}^+$ and then to $\mathcal{C}^-$ we show that the $\mathbb{R}(x)$-Mordell–Weil rank of $\mathrm{Jac}(\mathcal{C})$ is zero if and only if the groups $\mathrm{Jac}(\mathcal{C}_1^+)(\mathbb{R}(x))$, $\mathrm{Jac}(\mathcal{C}_x^+)(\mathbb{R}(x))$, $\mathcal{C}_1^-(\mathbb{R}(x))$ and $\mathcal{C}_x^-(\mathbb{R}(x))$ are finite. To prove Corollary 5.3.3.5 we apply Proposition 5.3.1.3 to $\mathcal{C}_1^-$, $\mathcal{C}_x^-$, $\mathcal{C}_1^+$ and $\mathcal{C}_x^+$; we check the hypotheses of Proposition 5.3.1.3 by using Proposition 5.3.3.1 and Proposition 4.3.5 (to apply it, use the results from subsection 5.2). □

5.4. *Richelot's isogenies*

PROPOSITION 5.4.1. *Let K be a characteristic* 0 *field. Let J and $\widehat{J}$ be two abelian varieties defined over K. We assume that $J(K)$ is finitely generated. We assume the existence of two isogenies $\varphi : J\longrightarrow\widehat{J}$ and $\widehat{\varphi}:\widehat{J}\longrightarrow J$ such that $\varphi\circ\widehat{\varphi}=[2]_{\widehat{J}}$ and $\widehat{\varphi}\circ\varphi=[2]_J$. Then the K-Mordell–Weil rank of J is zero if and only if*

$$J(K)/\widehat{\varphi}(\widehat{J}(K)) = J(K)_{\mathrm{tors}}/\widehat{\varphi}(\widehat{J}(K)) \quad \textit{and} \quad \widehat{J}(K)/\varphi(J(K)) = \widehat{J}(K)_{\mathrm{tors}}/\varphi(J(K)).$$

NOTATION 5.4.2. We consider the following data:

- a characteristic 0 field k;
- a monic squarefree polynomial $f\in k[x][y]$ with odd degree;
- a decomposition $f=\prod_{i=1}^{r}P_i(y)$ of f into prime elements of $k(x)[y]$.

Let $\mathcal{H}$ be the hyperelliptic curve defined over $k(x)$ by the affine equation $z^2=f(y)$. We denote

- by K_i the field $k(x)[y]/(P_i(y))$ and by y_i the class of y in K_i;

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

- by $\pi_{\mathcal{H}} : \mathrm{Jac}(\mathcal{H})(k(x)) \longrightarrow \prod_{i=1}^{r} K_i^{\times}/K_i^{\times 2}$ the morphism obtained by applying Proposition 4.2.1 to $\mathcal{H}$;
- by $\pi_{\mathcal{H},i} : \mathrm{Jac}(\mathcal{H})(k(x)) \longrightarrow K_i^{\times}/K_i^{\times 2}$ the ith coordinate of $\pi_{\mathcal{H}}$.

The norm map $N_{K_i/k(x)}$ associated to the field extension $K_i/k(x)$ induces a homomorphism $N_{K_i/k(x)} : K_i^{\times}/K_i^{\times 2} \longrightarrow k(x)^{\times}/k(x)^{\times 2}$. We denote by $\Xi_{\mathcal{H},i}$ the composite map $N_{K_i/k(x)} \circ \pi_{\mathcal{H},i}$. We denote by

$$\Xi_{\mathcal{H}} : \mathrm{Jac}(\mathcal{H})(k(x)) \longrightarrow \prod_{i=1}^{r} k(x)^{\times}/k(x)^{\times 2}$$

the homomorphism with ith coordinate $\Xi_{\mathcal{H},i}$ (for $i \in \{1, \ldots, r\}$).

THEOREM 5.4.3. *We use Notation 2.1. We assume the hypotheses of Corollary 5.3.3.5 are satisfied. For each $\delta \in k(x)^{\times}$ we consider the hyperelliptic curves $\mathcal{C}_{\delta}^{+}$, $\widehat{\mathcal{C}}_{\delta}^{+}$, $\mathcal{C}_{\delta}^{-}$, $\widehat{\mathcal{C}}_{\delta}^{-}$ defined over $k(x)$ by the affine equations*

$$\begin{aligned}
\mathcal{C}_{\delta}^{+} &: z^2 = \left(y + \tfrac{\delta(1+C(x))}{2}\right)\left(y^2 - \left(\tfrac{\delta(1-C(x))}{2}\right)^2\right)\left(y^2 - \tfrac{\delta^2[(1+C(x))^2 - 4B(x)]}{4}\right)\\
\widehat{\mathcal{C}}_{\delta}^{+} &: z^2 = (y + \delta(1+C(x)))(y^2 - 4\delta^2 B(x))(y^2 - 4\delta^2 C(x))\\
\mathcal{C}_{\delta}^{-} &: z^2 = y(y^2 - \delta[(1-C(x))^2 - 2(B(x) - C(x))]y + \delta^2(B(x) - C(x))^2)\\
\widehat{\mathcal{C}}_{\delta}^{-} &: z^2 = y\left(y + \delta(1-C(x))^2\right)\left(y + \delta[(1-C(x))^2 - 4(B(x) - C(x))]\right).
\end{aligned}$$

We use Notation 5.4.2 for $\mathcal{H} \in \{\mathcal{C}_{\delta}^{-}, \widehat{\mathcal{C}}_{\delta}^{-}, \mathcal{C}_{\delta}^{+}, \widehat{\mathcal{C}}_{\delta}^{+}\}$ with:

- *$P_1 = y$ when $\mathcal{H} = \mathcal{C}_{\delta}^{-}$ or $\mathcal{H} = \widehat{\mathcal{C}}_{\delta}^{-}$;*
- *$P_1 = y + \frac{\delta(1+C(x))}{2}$, $P_2 = y - \frac{\delta(1-C(x))}{2}$, $P_3 = y + \frac{\delta(1-C(x))}{2}$ and $P_4 = y^2 - \frac{\delta^2[(1+C(x))^2 - 4B(x)]}{4}$ when $\mathcal{H} = \mathcal{C}_{\delta}^{+}$;*
- *$P_1 = y + \delta(1+C(x))$, $P_2 = y^2 - 4\delta^2 B(x)$, $P_3 = y^2 - 4\delta^2 C(x)$ when $\mathcal{H} = \widehat{\mathcal{C}}_{\delta}^{+}$.*

If for every positive element $\zeta \in k^{\times}$ the images of the eight homomorphisms

$$\Xi_{\mathcal{C}_{\zeta}^{-},1}, \Xi_{\mathcal{C}_{\zeta x}^{-},1}, \Xi_{\widehat{\mathcal{C}}_{\zeta}^{-},1}, \Xi_{\widehat{\mathcal{C}}_{\zeta x}^{-},1}, \Xi_{\widehat{\mathcal{C}}_{\zeta}^{+}}, \Xi_{\widehat{\mathcal{C}}_{\zeta x}^{+}},$$

$$\Pi_{\mathcal{C}_{\zeta}^{+}} := \left(\Xi_{\mathcal{C}_{\zeta}^{+},1}, \Xi_{\mathcal{C}_{\zeta}^{+},2}.\Xi_{\mathcal{C}_{\zeta}^{+},3}, \Xi_{\mathcal{C}_{\zeta}^{+},4}\right) : \mathrm{Jac}(\mathcal{C}_{\zeta}^{+}) \longrightarrow \prod_{i=1}^{3} k(x)^{\times}/k(x)^{\times 2} \quad \textit{and}$$

$$\Pi_{\mathcal{C}_{\zeta x}^{+}} := \left(\Xi_{\mathcal{C}_{\zeta x}^{+},1}, \Xi_{\mathcal{C}_{\zeta x}^{+},2}.\Xi_{\mathcal{C}_{\zeta x}^{+},3}, \Xi_{\mathcal{C}_{\zeta x}^{+},4}\right) : \mathrm{Jac}(\mathcal{C}_{\zeta x}^{+}) \longrightarrow \prod_{i=1}^{3} k(x)^{\times}/k(x)^{\times 2}$$

are respectively the images of the $k(x)$-rational torsion subgroups of

$$\mathcal{C}_{\zeta}^{-}, \mathcal{C}_{\zeta x}^{-}, \widehat{\mathcal{C}}_{\zeta}^{-}, \widehat{\mathcal{C}}_{\zeta x}^{-}, \mathrm{Jac}(\widehat{\mathcal{C}}_{\zeta}^{+}), \mathrm{Jac}(\widehat{\mathcal{C}}_{\zeta x}^{+}), \mathrm{Jac}(\mathcal{C}_{\zeta}^{+}) \textit{ and } \mathrm{Jac}(\mathcal{C}_{\zeta x}^{+}),$$

then the $\mathbb{R}(x)$-Mordell–Weil rank of $\mathrm{Jac}(\mathcal{C})$ is zero.

Proof. Following Corollary 5.3.3.5, $\mathrm{Jac}(\mathcal{C})(\mathbb{R}(x))$ is finite if and only if for every positive element $\zeta \in k^{\times}$ the groups $\mathcal{C}_{\zeta}^{-}(k(x))$, $\mathcal{C}_{\zeta x}^{-}(k(x))$, $\mathrm{Jac}(\mathcal{C}_{\zeta}^{+})(k(x))$, and $\mathrm{Jac}(\mathcal{C}_{\zeta x}^{+})(k(x))$ are finite (notice that even if the curve $\mathcal{C}_{\delta}^{+}$ is not given by the same equation as in Corollary 5.3.3.5, both curves are isomorphic over $k(x)$).

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

There is an isogeny $\varphi_\delta^+ : \mathrm{Jac}(\mathcal{C}_\delta^+) \longrightarrow \mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)$ of degree 2 (a Richelot isogeny) such that $\ker(\Pi_{\mathcal{C}_\delta^+}) = \widehat{\varphi}_\delta^+(\mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)(k(x)))$ (with $\widehat{\varphi}_\delta^+$ the dual isogeny of φ_δ^+) and $\ker(\Xi_{\widehat{\mathcal{C}}_\delta^+}) = \varphi_\delta^+(\mathrm{Jac}(\mathcal{C}_\delta^+)(k(x)))$ (see [**8**, chapters 9 and 10]). Applying Lemma 5.4.1 to φ_δ^+ we get that $\mathrm{Jac}(\mathcal{C}_\delta^+)(k(x))$ is finite if and only if the images of $\Pi_{\mathcal{C}_\delta^+}$ and $\Xi_{\widehat{\mathcal{C}}_\delta^+}$ are respectively the images of the torsion subgroups of $\mathrm{Jac}(\mathcal{C}_\delta^+)(k(x))$ and $\mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)(k(x))$.

In the same way, applying Lemma 5.4.1 to a well-chosen 2-isogeny $\varphi_\delta^- : \mathcal{C}_\delta^- \longrightarrow \widehat{\mathcal{C}}_\delta^-$ (see [**27**, sections III.4 and III.5]), we show that $\mathcal{C}_\delta^-(k(x))$ is finite if and only if the images of $\Xi_{\mathcal{C}_\delta^-}$ and $\Xi_{\widehat{\mathcal{C}}_\delta^-}$ are respectively the images of the torsion subgroups of $\mathcal{C}_\delta^-(k(x))$ and $\widehat{\mathcal{C}}_\delta^-(k(x))$. □

6. *Checking the triviality of the Mordell–Weil rank*

In this section the class in $k(x)^\times/k(x)^{\times 2}$ of a given rational fraction $\alpha \in k(x)^\times$ is denoted by $[\alpha]$.

PROPOSITION 6.1. *We use Notation 5.4.2. For each couple $i, j \in \{1, \ldots, r\}$ of integers such that $j \neq i$, we denote by $d_{i,j}$ the rational fraction*

$$d_{i,j} := \mathrm{Gcd}\Big(N_{K_i/k(x)}\Big(P_i'(y)\prod_{k\neq i} P_k(y)\Big), N_{K_j/k(x)}\Big(P_j'(y)\prod_{k\neq j} P_k(y)\Big)\Big).$$

Then each element of the image of $\Xi_{\mathcal{H}}$ is a class

$$\Big(\Big[\prod_{j\neq 1}\mu_{1,j}\Big], \ldots, \Big[\prod_{j\neq r}\mu_{r,j}\Big]\Big)$$

for some family $(\mu_{i,j})_{1\leqslant i\leqslant r,\, j\neq i}$ of squarefree elements of $k[x]$ such that $\mu_{i,j} = \mu_{j,i}$ and such that the prime factors of $\mu_{i,j}$ are prime factors of $d_{i,j}$.

Proof. Let β be an element of $\mathrm{Jac}(\mathcal{H})(k(x))$ and let $\mathrm{div}(u, v)$ be a semi-reduced divisor on the curve $\mathcal{H}$ with linear equivalence class β. Following Proposition 5.3.2.1, the norm $N_{K_i/k(x)}((-1)^{\deg(u)}u(y_i))$ is equal to $\beta_i^2\prod_{k\in I_i} p_{i,k}$ where $\beta_i \in k(x)^\times$ and $p_{i,k} \in k[x]$ are irreducible polynomials appearing in the decomposition of the norm

$$N_{K_i/k(x)}(f'(y_i)) = N_{K_i/k(x)}\Big(P_i'(y_i)\prod_{j\neq i} P_j(y_i)\Big)$$

into prime factors. Denote the product $\prod_{k\in I_i} p_{i,k}$ by α_i.

For $\mu_{i,j}$ we take $\mathrm{Gcd}(\alpha_i, \alpha_j)$; the leading coefficient of $\mu_{i,j}$ can be chosen such that α_i and $\prod_{j\neq i}\mu_{i,j}$ have the same leading coefficient. Following Proposition 4.2.1 the product $\prod_{i=1}^r \Xi_{\mathcal{H},i}(\beta)$ is the identity element of $k(x)^\times/k(x)^{\times 2}$. In particular for every prime p we have

$$v_p\Big(\prod_{j\neq i}^r \alpha_j\Big) \equiv v_p(\alpha_i) \bmod 2 \quad \text{and thus} \quad v_p\Big(\prod_{j\neq i}\mu_{i,j}\Big) \equiv v_p(\alpha_i) \bmod 2$$

(notice that α_i and α_j are squarefree). This implies that $\prod_{j\neq i}\mu_{i,j} = \gamma^2\alpha_i$ for some $\gamma \in k(x)^\times$ (because α_i and $\prod_{j\neq i}\mu_{i,j}$ have the same leading coefficient). In other words $\Xi_{\mathcal{H},i}(\beta)$ is the class of $\prod_{j\neq i}\mu_{i,j}$. □

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

NOTATION 6.2. Let $\mathcal{P}$ be a place of $k(x)$ and $\mathcal{O}_{\mathcal{P}}$ be the associated valuation ring. Let α, β be elements of $\mathcal{O}_{\mathcal{P}}^{\times}$. The element α is equivalent to β modulo $\mathcal{P}$ and modulo squares (and we write $\alpha \sim \beta \mod \mathcal{P}$) if there is $\gamma \in \mathcal{O}_{\mathcal{P}}^{\times}$ such that α and $\beta\gamma^2$ are congruent modulo $\mathcal{P}$.

NOTATION 6.3. Let k be a characteristic 0 field. Let A be an element of $k(x)$. Denote the algebra $k(x)[T]/(T^2 - A)$ by K and the class of T in K by t. Let $\mathcal{P}$ be a place of $k(x)$, $\mathcal{O}_{\mathcal{P}}$ be the associated valuation ring, $v_{\mathcal{P}}$ be the valuation at $\mathcal{P}$, and p be a local parameter at $\mathcal{P}$.

PROPOSITION 6.4. *We use Notation 6.2 and Notation 6.3. We denote by $\widetilde{A}$ the element $p^{-v_{\mathcal{P}}(A)}A \in \mathcal{O}_{\mathcal{P}}^{\times}$. Let $u := u_0(y^2) + yu_1(y^2) \in k(x)[y]$ be a polynomial. Denote by α the element $p^{-v_{\mathcal{P}}(N_{K/k(x)}(u(t)))}N_{K/k(x)}(u(t)) \in \mathcal{O}_{\mathcal{P}}^{\times}$. Assume that $v_{\mathcal{P}}(A)$ is odd.*

1. *If $v_{\mathcal{P}}(N_{K/k(x)}(u(t)))$ is even, then $\alpha \sim 1 \bmod \mathcal{P}$;*
2. *if $v_{\mathcal{P}}(N_{K/k(x)}(u(t)))$ is odd, then $\alpha \sim -\widetilde{A} \bmod \mathcal{P}$ and*

$$\frac{v_{\mathcal{P}}(A)+1}{2} + v_{\mathcal{P}}(u_1(A)) \leqslant v_{\mathcal{P}}(u_0(A)). \tag{2}$$

PROPOSITION 6.5. *We use Notation 6.2 and Notation 6.3. We assume*

- *that the valuation $v_{\mathcal{P}}(A)$ is even;*
- *that $p^{-v_{\mathcal{P}}(A)}A$ is not a square in the residual field $\mathcal{O}_{\mathcal{P}}/\mathcal{P}$.*

Then, for every polynomial $u \in k(x)[y]$, the valuation $v_{\mathcal{P}}(N_{K/k(x)}(u(t)))$ is even.

PROPOSITION 6.6. *We use the notation and assumptions of Theorem 2.5 and the notation of Theorem 5.4.3. Let $\zeta > 0$ be an element of k and δ be either ζ or ζx. Then the image of $\Xi_{\mathcal{C}_\delta^-,1} = \Xi_{\mathcal{C}_\delta^-,2}$ is trivial.*

Proof. For a more detailed proof, see [**22**, Propositions 6.2.5 and 6.2.6].

Let (α, β) be a $k(x)$-point of the curve $\mathcal{C}_\delta^-$. Following Proposition 6.1, the image $\Xi_{\mathcal{C}_\delta^-,1}(\alpha,\beta)$ is the class in $k(x)^{\times}/k(x)^{\times 2}$ of a squarefree divisor μ of $\delta(B-C)$.

We apply Proposition 6.4 with $\mathcal{P}$ the infinite place of $k(x)$,

$$A := \frac{\delta^2(1-C)^2((1-C)^2 - 4(B-C))}{4}$$

$$\text{and } u(y) = y - \alpha + \frac{\delta((1-C)^2 - 2(B-C))}{2}.$$

Since ζ and the leading coefficient of $(1-C)^2 - 4(B-C)$ are positive, and since

$$\frac{-\deg(A)+1}{2} > -\deg\left(\frac{\delta((1-C)^2 - 2(B-C))}{2}\right),$$

Proposition 6.4 implies that μ is monic with even degree (use inequality (2) to study α and notice that $\alpha N_{K/k(x)}(-u(t))$ is a square in $k(x)$; here K and t are defined as in Notation 6.3).

Let $\theta, \psi \in k[x]$ be two coprime polynomials such that $\alpha = \mu\frac{\theta^2}{\psi^2}$. The equation of $\mathcal{C}_\delta^-$ gives the existence of $\nu \in k[x]$ such that

$$\mu\nu^2 = \mu^2\theta^4 - \delta[(1-C(x))^2 - 2(B(x)-C(x))]\mu\theta^2\psi^2 + \delta^2(B(x)-C(x))^2\psi^4.$$

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

Reducing modulo $1-C$ we get that either

$$\mu \sim 1 \bmod (1-C) \quad \text{or} \quad \mu \sim -\delta(B-C) \bmod (1-C). \tag{3}$$

When $(\delta, \mu) = (\zeta, B-C)$ the first relation contradicts hypothesis (1) and the second relation contradicts the positivity of ζ. Thus, when $\delta = \zeta$, the polynomial μ is equal to 1.

From now we assume that $\delta = \zeta x$. A reduction at x similar to the reduction at $1-C$ gives the relation $x^{-v_x(\mu)}\mu \sim \zeta^{v_x(\mu)} \bmod x$. When $\mu = B-C$ this relation contradicts hypothesis (11) (with $n_1 = 1$ and $n_2 = n_3 = 0$; see Assumption 2.4). When $\mu \notin \{1, B-C\}$,

- the relation $\mu \sim 1 \bmod (1-C)$ contradicts either hypothesis (2) or hypothesis (3);
- the equivalences $\mu \sim -\delta(B-C) \bmod (1-C)$ and $x^{-v_x(\mu)}\mu \sim \zeta^{v_x(\mu)} \bmod x$ can be written as two equations with solutions in k (see Notation 6.2); taking the product of those two equations we get a contradiction with either hypothesis (4) or hypothesis (5).

In particular, equivalences (3) show that the case $\mu \notin \{1, B-C\}$ does not happen. □

Proposition 6.7. *We use the notation and assumptions of Theorem 2.5 and the notation of Theorem 5.4.3. Let $\zeta > 0$ be an element of k and δ be either ζ or ζx. Then the image of $\Xi_{\widehat{\mathcal{C}}_\delta^-,1}$ is the subgroup of $k(x)^\times/k(x)^{\times 2}$ generated by $\Xi_{\widehat{\mathcal{C}}_\delta^-,1}(-\delta(1-C)^2, 0)$ and $\Xi_{\widehat{\mathcal{C}}_\delta^-,1}(0,0)$.*

Proof. For a more detailed proof, see [**22**, Propositions 6.3.5 and 6.3.6].

Let (α, β) be a $k(x)$-point of the curve $\widehat{\mathcal{C}}_\delta^-$. Following Proposition 6.1, the image $\Xi_{\widehat{\mathcal{C}}_\delta^-,1}(\alpha, \beta)$ is the class in $k(x)^\times/k(x)^{\times 2}$ of a squarefree divisor μ of

$$\delta(1-C)[(1-C)^2 - 4(B-C)].$$

Since $[-\delta] = \Xi_{\widehat{\mathcal{C}}_\delta^-,1}(-\delta(1-C)^2, 0)$ and $[(1-C)^2 - 4(B-C)] = \Xi_{\widehat{\mathcal{C}}_\delta^-,1}(0,0)$, we can assume without loss of generality that μ divides $1-C$.

Write $B - C = p_1 p_2$ with $p_i \in k[x]$ of degree 1. Using a specialization at p_i (analogous to the specialization at $1-C$ in the proof of Proposition 6.6) we show the existence of $m_i \in \{0, 1\}$ such that

$$\mu \sim (-\delta)^{m_i} \bmod p_i \tag{4}$$

When μ is a constant. Equivalences (4) prove Proposition 6.7:

- when $\delta = \zeta$, we have either $\mu \in k^{\times 2}$ or $-\delta\mu \in k^{\times 2}$, that is,
$$\mu \in \Xi_{\widehat{\mathcal{C}}_\delta^-,1}(-\delta(1-C)^2, 0)\ ;$$
- when $\delta = \zeta x$, hypothesis (11) implies that μ is a square in k (consider the product of the two equations in k given by equivalences (4)).

When μ is divisible by $1-C$. Specializing at $1-C$ (as in the proof of Proposition 6.6), we show that $-\delta(B-C) \sim 1 \bmod (1-C)$. When $\delta = \zeta$, this equivalence contradicts the positivity of ζ and $(\omega^2 - \eta^2)^2 - 4\omega^2$.

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

We assume that $\delta = \zeta x$. Taking the product of the two equations with solutions in k given by equivalences (4) (see Notation 6.2) and using the value of ζ given by the equivalence $-\delta(B-C) \sim 1 \bmod (1-C)$, we get a contradiction with one of the hypotheses (1), (6), (7) or (8) □

PROPOSITION 6.8. *We use the notation and assumptions of Theorem 2.5 and the notation of Theorem 5.4.3. Let $\zeta > 0$ be an element of k and δ be either ζ or ζx. Then the image of $\Pi_{\mathcal{C}_\delta^+}$ is generated by the images of the 2-torsion elements of $\mathrm{Jac}(\mathcal{C}_\delta^+)(k(x))$ under $\Pi_{\mathcal{C}_\delta^+}$.*

Proof. For a more detailed proof, see [**22**, Propositions 6.4.7. and 6.4.8].

Let β be a $k(x)$-point of $\mathrm{Jac}(\mathcal{C}_\zeta^+)$. We consider the polynomials $\mu_{i,j}$ defined by the application of Proposition 6.1 to $\mathcal{C}_\delta^+$. Without loss of generality we can choose the polynomials $\mu_{i,j}$ such that $\mu_{1,4}$ is coprime to δ and $\mu_{1,2} = \mu_{2,4} = 1$, i.e. such that

$$\Xi_{\mathcal{C}_\delta^+}(\beta) = ([\mu_{1,3}\mu_{1,4}], [\mu_{2,3}], [\mu_{1,3}\mu_{2,3}\mu_{3,4}], [\mu_{1,4}\mu_{3,4}]).$$

Adding to β a 2-torsion point (if needed), we can assume without loss of generality that

- $\mu_{1,3} \in k^\times$ is a constant,
- $\mu_{1,4} = \epsilon_{1,4}\,(x + b_1 + \eta)^{n_1}$ with $\epsilon_{1,4} \in k^\times$ and $n_1 \in \{0,1\}$,
- $\mu_{2,3} \in k[x]$ is a squarefree divisor of $\delta(1-C)(B-C)$, and
- $\mu_{3,4} = \epsilon_{3,4} x^{n_6 v_x(\delta)}\,(x + b_1 - 1 + \omega)^{n_2}\,(x + b_1 - 1 - \omega)^{n_4 v_x(\delta)}$ with $\epsilon_{3,4} \in k^\times$ and $n_2, n_4, n_6 \in \{0,1\}$.

To prove Proposition 6.8, we specialize the maps $\Xi_{\mathcal{C}_\delta^+,i}$ at different places of $k(x)$. The idea is to choose places $\mathcal{P}$ of $k(x)$ such that the reduction of the polynomial

$$\Big(y + \frac{\delta(1+C(x))}{2}\Big)\Big(y^2 - \Big(\frac{\delta(1-C(x))}{2}\Big)^2\Big)\Big(y^2 - \frac{\delta^2[(1+C(x))^2 - 4B(x)]}{4}\Big)$$

at $\mathcal{P}$ is divisible by the square of a nonconstant polynomial.

As an example we can use the fact that $y^2 - \big(\frac{\delta(1-C(x))}{2}\big)^2$ is a square modulo $1-C$. Since $\Xi_{\mathcal{C}_\delta^+,2}(\beta).\Xi_{\mathcal{C}_\delta^+,3}(\beta)$ is the class in $k(x)^\times/k(x)^{\times 2}$ of the resultant

$$R := \mathrm{Res}_y\Big((-1)^{\deg(u)}u(y), y^2 - \Big(\frac{\delta(1-C(x))}{2}\Big)^2\Big)$$

for some polynomial $u \in k[x][y]$ of degree at most 2, we have either

$$\mu_{1,3}\mu_{3,4} \sim 1 \bmod (1-C) \quad \text{or} \quad \mu_{1,3}\mu_{3,4} \sim \delta(B-C) \bmod (1-C) \tag{5}$$

(the second equivalence may happen in the case when R is divisible by $1-C$ and is obtained by noticing that $\Xi_{\mathcal{C}_\delta^+,1}(\beta).\Xi_{\mathcal{C}_\delta^+,4}(\beta)$ is also the class of $\mu_{1,3}\mu_{3,4}$).

In the same way, specializing the map

$$\Xi_{\mathcal{C}_\delta^+,2}.\Xi_{\mathcal{C}_\delta^+,3}.\Xi_{\mathcal{C}_\delta^+,4} : \mathrm{Jac}(\mathcal{C}_\delta^+)(k(x)) \longrightarrow k(x)^\times/k(x)^{\times 2}$$

at each prime factor of $B-C$, we prove the existence of two integers $n_3, n_5 \in \{0,1\}$ such that

$$\begin{aligned} &\mu_{1,3}\mu_{1,4} \sim \delta^{n_2} C^{n_3} \bmod (x + b_1 - 1 + \omega) \quad \text{and} \\ &\mu_{1,3}\mu_{1,4} \sim \delta^{n_4 v_x(\delta)} C^{n_5} \bmod (x + b_1 - 1 - \omega) \end{aligned} \tag{6}$$

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

(notice that the polynomial

$$\Big(y^2 - \Big(\frac{\delta(1-C(x))}{2}\Big)^2\Big)\Big(y^2 - \frac{\delta^2[(1+C(x))^2 - 4B(x)]}{4}\Big)$$

is a square modulo $B - C$).

Taking the product of the two equations with solutions in k given by equivalences (6), and using a sign argument, we show that $n_1 \equiv (n_2 + n_4)v_x(\delta) \mod 2$.

Applying Proposition 6.4 we study the specialization of $\Xi_{\mathcal{C}_\delta^+,4}(\beta)$ at the infinite place of $k(x)$. We get

$$(\eta^2 - \omega^2)^{n_1 + n_6 v_x(\delta) + n_2 + n_4 v_x(\delta)} \epsilon_{1,4}\epsilon_{3,4} \in k^2. \tag{7}$$

Case (1): *$\mu_{1,4}$ and $\mu_{3,4}$ are constants.* Then n_1, n_2 and $n_4 v_x(\delta)$ are equal to 0. Taking the product of the equations with solutions in k given by equivalences (6), we deduce from hypothesis (11) that $n_3 = n_5 = 0$. In particular equivalences (6) imply that $\mu_{1,3}\mu_{1,4} \in k^{\times 2}$. Relation (7) gives $\mu_{1,4}\mu_{3,4} \in k^{\times 2}$. Thus $\Pi_{\mathcal{C}_\delta^+}(\beta) = ([\mu_{1,3}\mu_{1,4}], [\mu_{1,3}\mu_{3,4}], [\mu_{1,4}\mu_{3,4}])$ is the identity element.

Case (2): *$\delta = \zeta$ and $\mu_{3,4}$ is not a constant.* Since $n_1 \equiv (n_2 + n_4)v_x(\delta) \bmod 2$, the polynomial $\mu_{1,4}$ is constant. We have $\mu_{3,4} = \epsilon_{3,4}\,(x + b_1 - 1 + \omega)$. Taking products of the equations with solutions in k given by equivalences (5), relation (7) and equivalences (6) leads to a contradiction with either hypothesis (9) or hypothesis (10).

Case (3): *$\delta = \zeta x$ and $\mu_{1,4} \in k^\times$ but $\mu_{3,4}$ is not a constant.* Considering the product of the equations with solutions in k given by equivalences (6), we deduce from hypothesis (11) that $n_1 = n_2 = n_3 = n_4 = n_5 = 0$. Taking products of the equations with solutions in k given by equivalences (5), relation (7) and equivalences (6) we get a contradiction either to the positivity of ζ and $(\omega^2 - \eta^2)((\omega^2 - \eta^2)^2 - 4\omega^2)$ or to hypothesis (12).

Case (4): *$\mu_{1,4}$ is not a constant.* Since $n_1 \equiv (n_2 + n_4)v_x(\delta) \bmod 2$, we have $\delta = \zeta x$, and n_2 and n_4 have a different parity. Taking the product of the equations with solutions in k given by equivalences (5), relation (7) and equivalences (6), and using a sign argument, we contradict hypothesis (13) (when n_2 is odd) and hypothesis (14) (when n_2 is even). □

PROPOSITION 6.9. *We use the notation and assumptions of Theorem 2.5 and the notation of Theorem 5.4.3. Let $\zeta > 0$ be an element of k and δ be either ζ or ζx. Then the image of $\Xi_{\widehat{\mathcal{C}}_\delta^+}$ is generated by the images of the 2-torsion elements of $\mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)(k(x))$ under $\Xi_{\widehat{\mathcal{C}}_\delta^+}$.*

Proof. For a more detailed proof, see [**22**, Proposition 6.5.5].

Let β be a $k(x)$-point of $\mathrm{Jac}(\widehat{\mathcal{C}}_\delta^+)$. Proposition 6.1 applies and asserts the existence of

- $\mu_{1,2} \in k[x]$ a squarefree divisor of $\delta((1+C)^2 - 4B)$,
- $\mu_{1,3} \in k[x]$ a squarefree divisor of $\delta(1 - C)$, and
- $\mu_{2,3} \in k[x]$ a squarefree divisor of $\delta(B - C)$

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

such that $\Xi_{\widehat{\mathcal{C}}^+_\delta}(\beta) = ([\mu_{1,2}\mu_{1,3}], [\mu_{1,2}\mu_{2,3}], [\mu_{1,3}\mu_{2,3}])$. Adding $<y + \delta(1 + C), 0>$ to β (if needed), we can assume without loss of generality that $\mu_{1,2}$ is a divisor of δ.

For each prime factor p of $B - C$, we deduce the coprimality of $\mu_{1,3}\mu_{2,3}$ and p from hypothesis (11) (apply Proposition 6.5, with $\mathcal{P}$ the place with local parameter p, to the study of $\Xi_{\widehat{\mathcal{C}}^+_\delta,3}$). In particular $\mu_{2,3}$ is a divisor of δ.

Assume for now that δ is equal to ζx. Applying Proposition 6.5 with $A := \delta^2 B$ and $\mathcal{P}$ the place with local parameter x (use hypothesis (15)), we show that $v_x(\mu_{1,2}\mu_{2,3})$ is even. In the same way, applying Proposition 6.5 with $A := \delta^2 C$ and $\mathcal{P}$ the place with local parameter x (use hypothesis (16)), we prove that $v_x(\mu_{1,3}\mu_{2,3})$ is even. In particular the valuations $v_x(\mu_{1,2})$, $v_x(\mu_{1,3})$ and $v_x(\mu_{2,3})$ have the same parity.

Now suppose we are in the general case (so δ may be different from ζx). Replacing $\mu_{i,j}$ by $x^{-1}\mu_{i,j}$ (if needed) we can assume without loss of generality that $\mu_{1,2}$ and $\mu_{2,3}$ are constants and that $\mu_{1,3} = \epsilon$ or $\mu_{1,3} = \epsilon(1 - C)$ for some $\epsilon \in k^\times$.

Applying Proposition 6.4 with $\mathcal{P}$ the infinite place of $k(x)$ to the study of $\Xi_{\widehat{\mathcal{C}}^+_\delta,3}$ we show that $\epsilon\mu_{2,3} \in k^{\times 2}$. Moreover an application of Proposition 6.4 with $A := 4\delta^2 B$ and $\mathcal{P}$ a place with local parameter one of the prime factors of B gives $\mu_{1,2}\mu_{2,3} \in k^{\times 2}$. Thus $\mu_{1,2}\mu_{1,3}$ has the same class in $k(x)^\times/k(x)^{\times 2}$ as either 1 or $1 - C$.

Assume that $\mu_{1,2}\mu_{1,3}(1 - C) \in k(x)^{\times 2}$. Let p be a prime factor of $B - C$. As in the proof of Proposition 6.8, expressing the image $\Xi_{\widehat{\mathcal{C}}^+_\delta,2}(\beta)\Xi_{\widehat{\mathcal{C}}^+_\delta,3}(\beta)$ as a resultant

$$\mathrm{Res}_y\left((-1)^{\deg(u)}u(y), \left(y^2 - 4\delta^2 B\right)\left(y^2 - 4\delta^2 C\right)\right)$$

(where $u(y) \in k[x][y]$ is a polynomial) and noticing that $(y^2 - 4\delta^2 B)(y^2 - 4\delta^2 C)$ is a square modulo p and that C is not a square modulo p, we show that the equivalence $\mu_{1,2}\mu_{1,3} \sim 1 \bmod p$ holds. In particular $\eta^2 - \omega^2 - 2\omega$ and $\eta^2 - \omega^2 + 2\omega$ are squares in k (use the property $\mu_{1,2}\mu_{1,3}(1 - C) \in k(x)^{\times 2}$). This contradicts hypothesis (1). As a consequence $\Xi_{\widehat{\mathcal{C}}^+_\delta}(\beta) = ([\mu_{1,2}\mu_{1,3}], [\mu_{1,2}\mu_{2,3}], [\mu_{1,3}\mu_{2,3}])$ is the identity. □

Acknowledgements. I want to thank warmly my thesis advisors D. Lubicz and L. Mahé. I also thank the referee and G. Everest, P. Satgé and S. Stevens for their helpful suggestions and comments.

References

1. E. Artin, 'Über die Zerlegung definiter Funktionen in Quadrate', *Hamb. Abh* 5 (1927) 100–115. 298
2. J. Bochnak, M. Coste and M.-F. Roy, *Real algebraic geometry*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)] 36 (Springer, Berlin, 1998). Translated from the 1987 French original, revised by the authors.
3. S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)] 21 (Springer, Berlin, 1990). 304
4. J.-B. Bost and J.-F. Mestre, 'Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2', *Gaz. Math.* 38 (1988) 36–64.

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

5. D. G. Cantor, 'Computing in the Jacobian of a hyperelliptic curve', *Math. Comp.* 48 (1987) 95–101. 299, 304

6. J. W. S. Cassels, 'The Mordell-Weil group of curves of genus 2', *Arithmetic and geometry, Vol. I*, Progr. Math. 35 (Birkhäuser, Boston, MA, 1983) 27–60.

7. J. W. S. Cassels, W. J. Ellison and A. Pfister, 'On sums of squares and on elliptic curves over function fields', *J. Number Theory* 3 (1971) 125–149. 298

8. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series 230 (Cambridge University Press, Cambridge, 1996). 318

9. M. R. Christie, 'Positive definite rational functions of two variables which are not the sum of three squares', *J. Number Theory* 8 (1976) 224–232. 299, 312

10. H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren (eds), *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton) (Chapman & Hall/CRC, Boca Raton, FL, 2006). 299

11. J.-L. Colliot-Thélène, 'The Noether-Lefschetz theorem and sums of 4-squares in the rational function field $\mathbb{R}(x, y)$', *Compositio Math.* 86 (1993) 235–243. 299

12. P. Gaudry, 'Algorithmique des courbes hyperelliptiques et applications à la cryptologie', PhD thesis, École Polytechnique, 2000. 299

13. D. Hilbert, 'Über die Darstellung definiter Formen als Summen von Formen-Quadraten', *Math. Ann* 32 (1888) 342–350. 298

14. M. Hindry and J. H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics 201 (Springer, New York, 2000).

15. J. Huisman and L. Mahé, 'Geometrical aspects of the level of curves', *J. Algebra* 239 (2001) 647–674. 299, 303

16. T. Y. Lam, *The algebraic theory of quadratic forms*, Mathematics Lecture Note Series (W. A. Benjamin, Reading, MA, 1973).

17. S. Lang, *Survey of Diophantine Geometry* (Springer, 1997). 309

18. O. Macé, 'Sommes de trois carrés en deux variables et représentation de bas degré pour le niveau des courbes réelles', PhD thesis, Université de Rennes 1, 2000, http://tel.ccsd.cnrs.fr/documents/archives0/00/00/62/39/index_fr.html. 299

19. O. Macé and L. Mahé, 'Sommes de trois carrés de fractions en deux variables', *Manuscripta Math.* 116 (2005) 421–447. 299

20. L. Mahé, 'Level and Pythagoras number of some geometric rings', *Math. Z.* 204 (1990) 615–629; erratum *Math. Z.* 209 (1992) 481–483.

21. V.A. Mahé, 'Calculs dans les jacobiennes de courbes algébriques, applications en géométrie algébrique réelle', PhD thesis, Université de Rennes 1, 2006, http://tel.archives-ouvertes.fr/tel-00124040/

22. V.A. Mahé, 'Using hyperelliptic curves to find positive polynomials that are not a sum of three squares in $\mathbb{R}(x, y)$', Preprint, 2007, http://arxiv.org/abs/math/0703722v2. 319, 320, 321, 322

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press

23. D. Mumford, *Tata lectures on theta II*, Progress in Mathematics 43 (Birkhäuser, Boston, MA, 1984). Jacobian theta functions and differential equations. With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. 299, 307

24. F. Oort and K. Ueno, 'Principally polarized abelian varieties of dimension two or three are Jacobian varieties', *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 20 (1973) 377–381.

25. A. Pfister, 'Zur Darstellung definiter Funktionen als Summe von Quadraten', *Invent. Math.* 4 (1967) 229–237. 298, 301

26. E.F. Schaefer, '2-descent on the Jacobians of hyperelliptic curves', *J. Number Theory* 51 (1995) 219–232. 306

27. J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics (Springer, New York, 1992). 318

28. H. Stichtenoth, *Algebraic function fields and codes*, Universitext (Springer, Berlin, 1993). 300, 309, 310

29. M. Stoll, 'Implementing 2-descent for s of hyperelliptic curves', *Acta Arith.* 98 (2001) 245–277.

30. O. Zariski and P. Samuel, *Commutative algebra, Vol. I*, The University Series in Higher Mathematics (Van Nostrand, Princeton, NJ, 1958). With the cooperation of I. S. Cohen. 314

Valéry Mahé v.mahe@uea.ac.uk

School of Mathematics,
University of East Anglia,
Norwich NR4 7TJ, United Kingdom

https://doi.org/10.1112/S1461157000000619 Published online by Cambridge University Press