Bull. Soc. math. France
132 (4), 2004, p. 617–634

NON-SUPERSINGULAR HYPERELLIPTIC JACOBIANS

by Yuri G. Zarhin

Abstract. — Let K be a field of odd characteristic p, let $f(x)$ be an irreducible separable polynomial of degree $n \geq 5$ with big Galois group (the symmetric group or the alternating group). Let C be the hyperelliptic curve $y^2 = f(x)$ and $J(C)$ its jacobian. We prove that $J(C)$ does not have nontrivial endomorphisms over an algebraic closure of K if either $n \geq 7$ or $p \neq 3$.

Résumé (*Jacobiennes hyperelliptiques non supersingulières*). — Soient K un corps de caractéristique impaire p et $f(x)$ un polynôme irréductible séparable dans $K[x]$ de degré $n \geq 5$, avec grand groupe de Galois (le groupe symétrique ou le groupe alterné). Soit C la courbe hyperelliptique $y^2 = f(x)$ et $J(C)$ sa jacobienne. Nous montrons que $J(C)$ n'a pas d'endomorphisme non trivial sur une clôture algébrique de K si $n \geq 7$ ou $p \neq 3$.

1. Introduction

Let K be a field and K_a its algebraic closure. Assuming that $\mathrm{char}(K) = 0$, the author [25] proved that the jacobian $J(C) = J(C_f)$ of a hyperelliptic curve

$$C = C_f : \ y^2 = f(x)$$

Texte reçu le 12 novembre 2003, accepté le 24 novembre 2003

Yuri G. Zarhin, Department of Mathematics, Pennsylvania State University, University Park, PA 16802 (USA) • *E-mail :* zarhin@math.psu.edu

2000 Mathematics Subject Classification. — 14H40, 14K05.

Key words and phrases. — Hyperelliptic jacobians, Endomorphisms of abelian varieties, Supersingular abelian varieties.

© Société Mathématique de France

has only trivial endomorphisms over K_a if the Galois group $\mathrm{Gal}(f)$ of the irreducible polynomial $f \in K[x]$ is "very big". Namely, if $n = \deg(f) \geq 5$ and $\mathrm{Gal}(f)$ is either the symmetric group $\mathbb{S}_n$ or the alternating group $\mathbb{A}_n$ then the ring $\mathrm{End}(J(C_f))$ of K_a-endomorphisms of $J(C_f)$ coincides with $\mathbb{Z}$. Later the author [25], [29] extended this result to the case of positive $\mathrm{char}(K) > 2$ but under the additional assumption that $n \geq 9$, *i.e.*, the genus of C_f is greater or equal than 4. We refer the reader to [15], [16], [9], [10], [14], [11], [25], [27], [29], [28], [30] for a discussion of known results about, and examples of, hyperelliptic jacobians without complex multiplication.

The aim of the present paper is to extend this result to the case when either $n \geq 7$ or when $n \geq 5$ but $\mathrm{char}(K) > 3$. Notice that it is known [25] that in those cases either $\mathrm{End}(J(C)) = \mathbb{Z}$ or $J(C)$ is a supersingular abelian variety and the real problem is how to prove that $J(C)$ is *not* supersingular.

We also discuss the case of two-dimensional $J(C)$ in characteristic 3.

2. Main result

Throughout this paper we assume that K is a field of characteristic p different from 2. We fix its algebraic closure K_a and write $\mathrm{Gal}(K)$ for the absolute Galois group $\mathrm{Aut}(K_a/K)$.

Theorem 2.1. — *Let K be a field with $p = \mathrm{char}(K) > 2$, K_a its algebraic closure, $f(x) \in K[x]$ an irreducible separable polynomial of degree n. Let us assume that $\mathrm{Gal}(f) = \mathbb{S}_n$ or $\mathbb{A}_n$. Suppose that n enjoys one of the following properties:*

(i) $n = 7$ *or* 8*;*

(ii) $n = 5$ *or* 6. *In addition,* $p = \mathrm{char}(K) > 3$.

Let C_f be the hyperelliptic curve $y^2 = f(x)$. Let $J(C_f)$ be its jacobian, $\mathrm{End}(J(C_f))$ the ring of K_a-endomorphisms of $J(C_f)$. Then $\mathrm{End}(J(C_f)) = \mathbb{Z}$.

Remark 2.2. — Replacing K by a suitable finite separable extension, we may assume in the course of the proof of Theorem 2.1 that $\mathrm{Gal}(f) = \mathbb{A}_n$. Taking into account that $\mathbb{A}_n$ is simple non-abelian and replacing K by its abelian extension obtained by adjoining to K all 2-power roots of unity, we may also assume that K contains all 2-power roots of unity.

Remark 2.3. — Let $f(x) \in K[x]$ be an irreducible separable polynomial of *even* degree $n = 2m \geq 6$ such that $\mathrm{Gal}(f) = \mathbb{S}_n$. Let $\alpha \in K_a$ be a root of f and $K_1 = K(\alpha)$ be the corresponding subfield of K_a. We have

$$f(x) = (x - \alpha) f_1(x)$$

with $f_1(x) \in K_1[x]$. Clearly, $f_1(x)$ is an irreducible separable polynomial over K_1 of degree $n - 1 = 2m - 1$, whose Galois group is $\mathbb{S}_{n-1}$. It is also clear that the polynomials

$$h(x) = f_1(x+\alpha), \quad h_1(x) = x^{n-1}h(1/x) \in K_1[x]$$

are irreducible separable of degree $n-1$ with the same Galois group $\mathbb{S}_{n-1}$.

The standard substitution

$$x_1 = \frac{1}{x-\alpha}, \quad y_1 = \frac{y}{(x-\alpha)^m}$$

establishes a birational isomorphism between C_f and a hyperelliptic curve

$$C_{h_1} : \, y_1^2 = h_1(x_1).$$

In light of results of [26], [30] and Remarks 2.2 and 2.3, our Theorem 2.1 is an immediate corollary of the following auxiliary statement.

THEOREM 2.4. — *Let K be a field with $p = \mathrm{char}(K) > 2$, K_a its algebraic closure, $f(x) \in K[x]$ an irreducible separable polynomial of degree n. Let us assume that n and the Galois group $\mathrm{Gal}(f)$ of f enjoy one of the following properties:*

(i) *$n = 5$ and $\mathrm{Gal}(f) = \mathbb{A}_5$;*

(ii) *$n = 7$ and $\mathrm{Gal}(f) = \mathbb{A}_7$. In addition, $p = \mathrm{char}(K) > 3$.*

Let C be the hyperelliptic curve $y^2 = f(x)$ and let $J(C)$ be the jacobian of C. Then $J(C)$ is not a supersingular abelian variety.

We will prove Theorem 2.4 in Section 3.

Throughout the paper we write $\mathrm{End}^0(X)$ for the endomorphism algebra $\mathrm{End}(X) \otimes \mathbb{Q}$ of an abelian variety X over an algebraically closed field F_a. Recall [25] that the semisimple $\mathbb{Q}$-algebra $\mathrm{End}^0(X)$ has dimension $(2\dim(X))^2$ if and only if $p := \mathrm{char}(F_a) \neq 0$ and X is a supersingular abelian variety. We write $\mathbb{H}_p$ is the quaternion $\mathbb{Q}$-algebra unramified exactly at p and ∞. It is well known that if X is a supersingular abelian variety in characteristic p then $\mathrm{End}^0(X)$ is isomorphic to the matrix algebra $\mathrm{M}_g(\mathbb{H}_p)$ of size $g := \dim(X)$ over $\mathbb{H}_p$. We will use freely these facts throughout the paper.

3. Proof of Theorem 2.4

We deduce Theorem 2.4 from the following statement.

THEOREM 3.1. — *Let K be a field with $p = \mathrm{char}(K) > 2$, K_a its algebraic closure, Let $n = q$ be an odd prime, $f(x) \in K[x]$ an irreducible separable polynomial of degree q. Let us assume that the Galois group $\mathrm{Gal}(f)$ of f is $\mathrm{L}_2(q) := \mathrm{PSL}_2(\mathbb{F}_q)$, and that it acts doubly transitively on the roots of f. Suppose that either $q = 5$ or $q = 7$. Let C be the hyperelliptic curve $y^2 = f(x)$ and let $J(C)$ be the jacobian of C. If $J(C)$ is a supersingular abelian variety then $n = 5$ and $p = 3$.*

Proof of Theorem 2.4 (modulo Theorem 3.1). — If $n=5$ then $\mathbb{A}_5 \cong \mathrm{L}_2(5)$ and we are done. Suppose that $n=7$. It is well-known that the simple non-abelian group

$$\mathrm{L}_2(7) \cong \mathrm{L}_3(2) := \mathrm{PSL}_3(\mathbb{F}_2)$$

acts doubly transitively on the 7-element projective plane $\mathbb{P}^2(\mathbb{F}_2)$ and therefore is isomorphic to a doubly transitive subgroup of $\mathbb{A}_7$. Hence there exists a finite algebraic extension K_1 of K such that the Galois group of f over K_1 is $\mathrm{L}_2(7)$ acting doubly transitively on the roots of $f(x)$. Applying Theorem 3.1 to K_1 and f, we conclude that if $3 \neq \mathrm{char}(K_1) = \mathrm{char}(K) = p$ then $J(C)$ is not supersingular. □

The following results will be used in order to prove Theorem 3.1.

Lemma 3.2. — *Let K be a field with $\mathrm{char}(K) \neq 2$ K_a its algebraic closure, $\mathrm{Gal}(K) = \mathrm{Aut}(K_a)$ the Galois group of K. Let $f(x) \in K[x]$ be an irreducible separable polynomial of odd degree n. Let us assume that $n \geq 5$ and the Galois group $\mathrm{Gal}(f)$ of f acts doubly transitively on the roots of $f(x)$. Let C be the hyperelliptic curve $y^2 = f(x)$ and let $J(C)$ be the jacobian of C. Let $J(C)_2$ be the group of points of order 2 in $J(C)(K_a)$ viewed as $\mathbb{F}_2$-vector space provided with a natural structure of $\mathrm{Gal}(K)$-module.*

Then the image of $\mathrm{Gal}(K)$ in $\mathrm{Aut}_{\mathbb{F}_2}(J(C)_2)$ is isomorphic to $\mathrm{Gal}(f)$ and

$$\mathrm{End}_{\mathrm{Gal}(K)}\big(J(C)_2\big) = \mathrm{End}_{\mathrm{Gal}(f)}\big(J(C)_2\big) = \mathbb{F}_2.$$

Theorem 3.3. — *Let F be a field with characteristic $p>2$ and assume that F contains all 2-power roots of unity. Let F_a be an algebraic closure of F. Let $G \neq \{1\}$ be a finite perfect group. Suppose that g is a positive integer, X is a supersingular g-dimensional abelian variety defined over F. Let $\mathrm{End}(X)$ be the ring of all F_a-endomorphisms of X and $\mathrm{End}^0(X) = \mathrm{End}(X) \otimes \mathbb{Q}$. Let us assume that the image of $\mathrm{Gal}(F)$ in $\mathrm{Aut}(X_2)$ is isomorphic to G and the corresponding faithful representation*

$$\bar\rho : G \hookrightarrow \mathrm{Aut}(X_2) \cong \mathrm{GL}(2g, \mathbb{F}_2)$$

satisfies $\mathrm{End}_G X_2 = \mathbb{F}_2$.

Then there exists a surjective group homomorphism

$$\pi_1 : G_1 \twoheadrightarrow G$$

enjoying the following properties:

(a) *The group G_1 is a perfect finite group. The kernel of π_1 is an elementary abelian 2-group.*
(b) *One may lift $\bar\rho\pi_1 : G_1 \to \mathrm{Aut}(X_2)$ to a faithful absolutely irreducible symplectic representation*

$$\rho : G_1 \hookrightarrow \mathrm{Aut}_{\mathbb{Q}_2}(V_2(X))$$

of G_1 over $\mathbb{Q}_2$ in such a way that the following conditions hold:

- ▹ *the character χ of ρ takes values in $\mathbb{Q}$;*
- ▹ $\rho(G_1) \subset (\mathrm{End}^0(X))^*$*;*
- ▹ *the homomorphism from the group algebra $\mathbb{Q}[G_1]$ to $\mathrm{End}^0(X)$ induced by ρ is surjective and identifies $\mathrm{End}^0(X) \cong \mathrm{M}_g(\mathbb{H}_p)$ with the direct summand of $\mathbb{Q}[G_1]$ attached to χ.*

(c) *p divides the order of G and $p \leq 2g+1$.*

(d) *Suppose that either every homomorphism from G to $\mathrm{GL}(g-1, \mathbb{F}_2)$ is trivial or the G-module X_2 is very simple in the sense of* [26], [29], [31]*. Then $\ker \pi_1$ is a central cyclic subgroup of order 1 or 2.*

LEMMA 3.4. — *Let p be an odd prime. Let q be an odd prime and $\Gamma = \mathrm{SL}_2(\mathbb{F}_q)$ or $\mathrm{PSL}_2(\mathbb{F}_q)$. Suppose that $q = 5$ or 7 and let us put $g = \frac{1}{2}(q-1)$. Suppose that $\mathbb{Q}[\Gamma]$ contains a direct summand isomorphic to the matrix algebra $\mathrm{M}_g(\mathbb{H}_p)$. Then $p = 3$ and $q = 5$.*

Theorem 3.3 and Lemmas will be proven in Sections 5 and 4.

Proof of Theorem 3.1 (modulo Theorem 3.3 and Lemmas 3.2 and 3.4)
Let us put

$$X = J(C), \quad G = \mathrm{PSL}_2(\mathbb{F}_q), \quad g = \frac{1}{2}(q-1).$$

Clearly, either $q = 5$, $g = 2$ or $q = 7$, $g = 3$. In both cases $g = \dim(X)$, the group G is simple and $\mathrm{GL}(g-1, \mathbb{F}_2)$ is solvable. It follows that every homomorphism from G to $\mathrm{GL}(g-1, \mathbb{F}_2)$ is trivial. It follows from Lemma 3.2 that the image of $\mathrm{Gal}(K)$ in $\mathrm{Aut}(X_2)$ is isomorphic to G and the corresponding faithful representation

$$\bar{\rho} : G \hookrightarrow \mathrm{Aut}(X_2) \cong \mathrm{GL}(2g, \mathbb{F}_2)$$

satisfies $\mathrm{End}_G X_2 = \mathbb{F}_2$.

Let us assume that X is supersingular. We need to get a contradiction.

Applying Theorem 3.3, we conclude that there exist a finite perfect group G_1 and a surjective homomorphism

$$\pi_1 : G_1 \twoheadrightarrow G = \mathrm{PSL}_2(\mathbb{F}_q)$$

enjoying the following properties:

(i) either $G_1 \cong G$ or $Z_1 = \ker(\pi_1)$ is a central subgroup of order 2 in G_1;

(ii) there exists a direct summand of $\mathbb{Q}[G_1]$ isomorphic to $\mathrm{M}_g(\mathbb{H}_p)$).

The well-known description of central extensions of $\mathrm{PSL}_2(\mathbb{F}_q)$ when q is an odd prime [4, §4.15, Prop. 4.233] implies that either $G_1 = \mathrm{PSL}_2(\mathbb{F}_q)$ or $G_1 = \mathrm{SL}_2(\mathbb{F}_q)$. Applying Lemma 3.4, we arrive to the desired contradiction. □