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 $K_\alpha$ its algebraic closure. Assuming that $\text{char}(K) = 0$, the author [25] proved that the jacobian $J(C) = J(C_f)$ of a hyperelliptic curve $C = C_f : y^2 = f(x)$ does not have nontrivial endomorphisms over $K_\alpha$ if either $n \geq 7$ or $p \neq 3$. The proof relies on the theory of endomorphisms of abelian varieties.

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.
has only trivial endomorphisms over $K_a$ if the Galois group $\text{Gal}(f)$ of the irreducible polynomial $f \in K[x]$ is “very big”. Namely, if $n = \deg(f) \geq 5$ and $\text{Gal}(f)$ is either the symmetric group $S_n$ or the alternating group $A_n$, then the ring $\text{End}(J(C_f))$ 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 $\text{char}(K) > 2$ 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 $n = 7$ or when $n = 5$ but $\text{char}(K) > 3$. Notice that it is known [25] that in those cases either $\text{End}(J(C)) = \mathbb{Z}$ 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 $\text{Gal}(K)$ for the absolute Galois group $\text{Aut}(K_a/K)$.

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

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

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

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

**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 $\text{Gal}(f) = A_n$. Taking into account that $A_n$ 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 $\text{Gal}(f) = S_n$. 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 $S_{n-1}$. 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 \( p = \text{char}(K) > 2 \), \( K_a \) its algebraic closure, \( f(x) \in K[x] \) an irreducible separable polynomial of degree \( n \). Let us assume that \( n \) and the Galois group \( \text{Gal}(f) \) of \( f \) enjoy one of the following properties:

(i) \( n = 5 \) and \( \text{Gal}(f) = \mathbb{A}_5 \);
(ii) \( n = 7 \) and \( \text{Gal}(f) = \mathbb{A}_7 \). In addition, \( p = \text{char}(K) > 3 \).

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 \( \text{End}^0(X) \) for the endomorphism algebra \( \text{End}(X) \otimes \mathbb{Q} \) of an abelian variety \( X \) over an algebraically closed field \( F_q \).

Recall [25] that the semisimple \( \mathbb{Q} \)-algebra \( \text{End}^0(X) \) has dimension \( (2 \dim(X))^2 \) if and only if \( p := \text{char}(F_q) \neq 0 \) and \( X \) is a supersingular abelian variety. We write \( \mathbb{H}_p \) is the quaternion \( \mathbb{Q} \)-algebra unramified exactly at \( p \) and \( \infty \). It is well known that if \( X \) is a supersingular abelian variety in characteristic \( p \) then \( \text{End}^0(X) \) is isomorphic to the matrix algebra \( M_g(\mathbb{H}_p) \) 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 \( p = \text{char}(K) > 2 \), \( K_a \) 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 \( \text{Gal}(f) \) of \( f \) is \( \text{L}_2(q) := \text{PSL}_2(\mathbb{F}_q) \), 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 \( \mathbb{A}_5 \cong S_5 \) and we are done. Suppose that \( n = 7 \). It is well-known that the simple non-abelian group
\[
L_2(7) \cong PSL_3(2) := PGL_3(2)
\]
acts doubly transitively on the 7-element projective plane \( \mathbb{P}^2(F_2) \) and therefore is isomorphic to a doubly transitive subgroup of \( S_7 \). Hence there exists a finite algebraic extension \( K_1 \) of \( K \) such that the Galois group of \( f \) over \( K_1 \) is \( L_2(7) \) acting doubly transitively on the roots of \( f(x) \). Applying Theorem 3.1 to \( K_1 \) and \( f \), we conclude that if \( 3 \neq \text{char}(K_1) = \text{char}(K) = p \) then \( J(C) \) is not supersingular.

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

**Lemma 3.3.** — Let \( K \) be a field with \( \text{char}(K) \neq 2 \) \( K_a \) its algebraic closure, \( \text{Gal}(K) = \text{Aut}(K_a) \) 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 \( \text{Gal}(f) \) 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 \( F_2 \)-vector space provided with a natural structure of \( \text{Gal}(K) \)-module.

Then the image of \( \text{Gal}(K) \) in \( \text{Aut}(J(C)^2) \) is isomorphic to \( \text{Gal}(f) \) and
\[
\text{End}_{\text{Gal}(f)}(J(C)^2) = \text{End}_{\text{Gal}(K)}(J(C)^2) = F_2.
\]

**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 \( G \cong \mathbb{A}_g \) be a finite perfect group. Suppose that \( g \) is a positive integer, \( X \) is a supersingular \( g \)-dimensional abelian variety defined over \( F \). Let \( \text{End}(X) \) be the ring of all \( F_a \)-endomorphisms of \( X \) and \( \text{End}^0(X) = \text{End}(X) \otimes \mathbb{Q} \). Let us assume that the image of \( \text{Gal}(F) \) in \( \text{Aut}(X_2) \) is isomorphic to \( G \) and the corresponding faithful representation
\[
\rho : G \to \text{Aut}(X_2) \cong \text{GL}(2g, F_2)
\]
satisfies
\[
\text{End}_G X_2 = F_2.
\]

Then there exists a surjective group homomorphism
\[
\pi_1 : G_1 \to G
\]
enjoying the following properties:

(a) The group \( G_1 \) is a perfect finite group. The kernel of \( \pi_1 \) is an elementary abelian 2-group.

(b) One may lift \( \rho \pi_1 : G_1 \to \text{Aut}(X_2) \) to a faithful absolutely irreducible symplectic representation
\[
\rho : G_1 \to \text{Aut}_{\mathbb{Q}_2}(V_2(X))
\]
of \( G_1 \) over \( \mathbb{Q}_2 \) in such a way that the following conditions hold:
The character $\chi$ of $\rho$ takes values in $\mathbb{Q}$;

$\rho(G_1) \subset (\text{End}^0(X))^*$;

the homomorphism from the group algebra $\mathbb{Q}[G_1]$ to $\text{End}^0(X)$ induced by $\rho$ is surjective and identifies $\text{End}^0(X) \cong M_g(\mathbb{H}_p)$ with the direct summand of $\mathbb{Q}[G_1]$ attached to $\chi$.

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

d) Suppose that either every homomorphism from $G$ to $GL(g-1, \mathbb{F}_2)$ 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 $\Gamma = SL_2(\mathbb{F}_q)$ or $PSL_2(\mathbb{F}_q)$. 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 $M_g(\mathbb{H}_p)$. 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

$$X = J(C), \quad G = PSL_2(\mathbb{F}_q), \quad g = \frac{1}{2}(q - 1).$$

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

$$\bar{\rho} : G \hookrightarrow \text{GL}(2g, \mathbb{F}_2)$$

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

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

$$\pi_1 : G_1 \twoheadrightarrow G = PSL_2(\mathbb{F}_q)$$

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 $M_g(\mathbb{H}_p)$.

The well-known description of central extensions of $PSL_2(\mathbb{F}_q)$ when $q$ is an odd prime [4, §4.15, Prop. 4.233] implies that either $G_1 = PSL_2(\mathbb{F}_q)$ or $G_1 = SL_2(\mathbb{F}_q)$. Applying Lemma 3.4, we arrive to the desired contradiction. 

BULLETIN DE LA SOCIETE MATHEMATIQUE DE FRANCE
4. Proof of Lemmas 3.2 and 3.4

We start with some auxiliary constructions related to the permutation groups \([12], [17], [7]\). Let \(B\) be a finite set consisting of \(n \geq 5\) elements. We write \(\text{Perm}(B)\) for the group of permutations of \(B\). A choice of ordering on \(B\) gives rise to an isomorphism \(\text{Perm}(B) \cong S_n\). Let us assume that \(n\) is odd and consider the permutation module \(F_B^2\): the \(\mathbb{F}_2\)-vector space of all functions \(\varphi : B \to \mathbb{F}_2\). The space \(F_B^2\) carries a natural structure of \(\text{Perm}(B)\)-module and contains the stable hyperplane \(Q_B := (F_B^2)^0\) of functions \(\varphi\) with \(\sum_{\alpha \in B} \varphi(\alpha) = 0\). Clearly, \(Q_B\) carries a natural structure of faithful \(\text{Perm}(B)\)-module. For each permutation group \(H \subset \text{Perm}(B)\) the corresponding \(H\)-module is called the heart of the permutation representation of \(H\) on \(B\) over \(\mathbb{F}_2\) (see \([12], [17], [7]\)).

**Lemma 4.1.** \(|\text{End}_H(Q_B)| = \mathbb{F}_2\) if \(n\) is odd and \(H\) acts \(2\)-transitively on \(B\).

*Proof.* — See Satz 4 in \([12]\).

**Proof of Lemma 3.2.** — Suppose \(f(x) \in K[x]\) is a polynomial of odd degree \(n \geq 5\) without multiple roots and \(X := J(f) = C_f : y^2 = f(x)\). It is well-known that \(g := \dim(X) = \frac{1}{2}(n - 1)\). It is also well-known (see for instance Section 5 of \([26]\)) that the image of \(\text{Gal}(K) \to \text{Aut}(X_2)\) is isomorphic to \(\text{Gal}(f)\). More precisely, let \(\mathfrak{R} \subset K_a\) be the \(n\)-element set of roots of \(f\), let \(K(\mathfrak{R})\) be the splitting field of \(f\) and \(\text{Gal}(f) = \text{Gal}(K(\mathfrak{R})/K)\) the Galois group of \(f\), viewed as a subgroup of of the group \(\text{Perm}(\mathfrak{R})\) of all permutations of \(\mathfrak{R}\). We have \(\text{Gal}(f) \subset \text{Perm}(\mathfrak{R})\). It is well-known (see for instance, Thm 5.1 on p. 478 of \([26]\)) that \(\text{Gal}(K) \to \text{Aut}(X_2)\) factors through the canonical surjection \(\text{Gal}(K) \to \text{Gal}(K(\mathfrak{R})/K) = \text{Gal}(f)\) and the \(\text{Gal}(f)\)-modules \(X_2\) and \(Q_{\mathfrak{R}}\) are isomorphic. In particular,

\[
\text{End}_{\text{Gal}(K)}(X_2) = \text{End}_{\text{Gal}(f)}(X_2) = \text{End}_{\text{Gal}(f)}(Q_{\mathfrak{R}}).
\]

Assuming that \(\text{Gal}(f)\) acts doubly transitively on \(\mathfrak{R}\) and applying Lemma 4.1, we conclude that

\[
\text{End}_{\text{Gal}(f)}(X_2) = \text{End}_{\text{Gal}(f)}(Q_{\mathfrak{R}}) = \mathbb{F}_2.
\]

**Remark 4.2.** — The assertion of Lemma 3.2 is implicitly contained in the proof of Prop. 3 in \([16]\).

**Proof of Lemma 3.4.** — It is known \([8, \text{Cor. on p. 4}]\) that \(Q[\text{PSL}_2(\mathbb{F}_q)]\) is a direct product of matrix algebras (for all power primes \(q\)). Since \(\ker(\text{SL}_2(\mathbb{F}_q) \to \text{PSL}_2(\mathbb{F}_q))\) is the only proper normal subgroup in \(\text{SL}_2(\mathbb{F}_q)\), it suffices to deal only with the group \(\text{SL}_2(\mathbb{F}_q)\) with \(q = 5, g = 2\) or \(q = 7, g = 3\) and consider only direct summands of \(Q[\text{SL}_2(\mathbb{F}_q)]\) that correspond (in the sense of Lemma 24.7 on p. 124 of \([2]\)) to faithful irreducible characters of degree \(q - 1\) with values in \(\mathbb{Q}\).
Let $\chi$ be an irreducible faithful irreducible character of degree $q - 1$ with values in $\mathbb{Q}$. Then (in the notations of [2, §38]) $\chi = \theta_j$ where $j$ is an integer with $1 \leq j \leq \frac{1}{2}(q - 1)$. If $z$ is the only nontrivial central element of $\text{SL}_2(\mathbb{F}_q)$ then $\theta_j(z) = (-1)^j(q - 1)$. The faithfulness of $\chi$ implies (thanks to Lemma 2.19 of [6]) that $\theta_j(z) \neq q - 1$, i.e. $j$ is odd. Let $b \in \text{SL}_2(\mathbb{F}_q)$ be an element of order $q$ and $\sigma$ a primitive $q + 1$th root of unity. Then [2, p. 228]

$$\chi(b) = \theta_1(b) = -(\sigma^j + \sigma^{-j}).$$

Assume that $q = 7$. Then either $j = 1$ or $j = 3$. Also $q + 1 = 8$ and we may choose $\sigma = (1 + \sqrt{-1})/\sqrt{2}$. Then if $j = 1$ then $\chi(b) = -\sqrt{2}$ and if $j = 3$ then $\chi(b) = \sqrt{2}$. In both cases $\chi(b)$ does not lie in $\mathbb{Q}$. It follows that $\mathbb{Q}[\text{SL}_2(\mathbb{F}_7)]$ does not have direct summands isomorphic to the matrix algebras of size 3 over quaternion $\mathbb{Q}$-algebras (including $\mathbb{H}_p$).

Assume that $q = 5$. Then $j = 1$ and $\chi = \theta_1$. Then $q + 1 = 6$ and the multiplicative order $n$ of $\sigma^j$ equals $6 = 2 \cdot 3$. Also $\sigma^3 = \sigma^2$ is a primitive cubic root of unity. Let $D$ be the direct summand of $\mathbb{Q}[\text{SL}_2(\mathbb{F}_5)]$ attached to $\chi$. It follows from the case (c) of theorem on p. 4 of [8] (see also [3, Thm 6.1 (ii)] (with $\epsilon = \delta = 1$)) that $D$ is isomorphic to the matrix algebra $M_2(\mathbb{H})$ where $H$ is a quaternion $\mathbb{Q}$-algebra ramified (exactly) at $\infty$ and 3. (This means that $H \cong \mathbb{H}_3$ and $D \cong M_2(\mathbb{H}_3)$.) It follows that if $D$ is isomorphic to $M_2(\mathbb{H}_p)$ then $p = 3$.

5. Not supersingularity

We keep all the notations and assumptions of Theorem 3.3. We write $T_2(X)$ for the 2-adic Tate module of $X$ and $\rho_{2,X} : \text{Gal}(F) \rightarrow \text{Aut}_{\mathbb{Z}_2}(T_2(X))$ for the corresponding 2-adic representation. It is well-known that $T_2(X)$ is a free $\mathbb{Z}_2$-module of rank $2\dim(X) = 2g$ and

$$X_2 = T_2(X)/2T_2(X)$$

(the equality of Galois modules). Let us put

$$H = \rho_{2,X}(\text{Gal}(F)) \subset \text{Aut}_{\mathbb{Z}_2}(T_2(X)).$$

Clearly, the natural homomorphism

$$\bar{\rho}_{2,X} : \text{Gal}(F) \rightarrow \text{Aut}(X_2)$$

defining the Galois action on the points of order 2 is the composition of $\rho_{2,X}$ and (surjective) reduction map modulo 2

$$\text{Aut}_{\mathbb{Z}_2}(T_2(X)) \rightarrow \text{Aut}(X_2).$$

This gives us a natural (continuous) surjection

$$\pi : H \rightarrow \bar{\rho}_{2,X}(\text{Gal}(F)) \cong G,$$

BULLETIN DE LA SOCIETE MATHEMATIQUE DE FRANCE
whose kernel consists of elements of $1 + 2\text{End}_{\mathbb{Z}/2}(T_2(X))$. The choice of polarization on $X$ gives rise to a non-degenerate alternating bilinear form (Riemann form) [18]

$$e : V_2(X) \times V_2(X) \to \mathbb{Q}_2(1) \cong \mathbb{Q}_2.$$ 

Since $F$ contains all 2-power roots of unity, $e$ is Gal($F$)-invariant and therefore is $H$-invariant. In particular,

$$H \subset \text{Sp}(V_2(X), e) \subset \text{SL}(V_2(X)).$$

Here $\text{Sp}(V_2(X), e)$ is the symplectic group attached to $e$. In particular, the $H$-module $V_2(X)$ is symplectic.

There exists a finite Galois extension $L$ of $F$ such that all endomorphisms of $X$ are defined over $L$. Clearly, Gal($L$) = Gal($F_a/L$) is an open normal subgroup of finite index in Gal($F$) and

$$H' = \rho_{2,X}(\text{Gal}(L)) \subset \text{Aut}_{\mathbb{Z}/2}(T_2(X)) \subset \text{Aut}_{\mathbb{Q}_2}(V_2(X))$$

is an open normal subgroup of finite index in $H$. We write $\text{End}^0(X)$ for the $\mathbb{Q}$-algebra $\text{End}(X) \otimes \mathbb{Q}$ of endomorphisms of $X$.

There exists a finite Galois extension $L$ of $F$ such that all endomorphisms of $X$ are defined over $L$. We write $\text{End}^0(X)$ for the $\mathbb{Q}$-algebra $\text{End}(X) \otimes \mathbb{Q}$ of endomorphisms of $X$. Since $X$ is supersingular,

$$\dim_{\mathbb{Q}} \text{End}^0(X) = (2\dim(X))^2 = (2g)^2.$$ 

Recall (see [18]) that the natural map

$$\text{End}^0(X) \otimes \mathbb{Q} \cong \text{End}_{\mathbb{Q}_2}V_2(X)$$

is an embedding. Dimension arguments imply that

$$\text{End}^0(X) \otimes \mathbb{Q} \cong \text{End}_{\mathbb{Q}_2}V_2(X).$$

Since all endomorphisms of $X$ are defined over $L$, the image

$$\rho_{2,X}(\text{Gal}(L)) \subset \rho_{2,X}(\text{Gal}(F)) \subset \text{Aut}_{\mathbb{Z}/2}(T_2(X)) \subset \text{Aut}_{\mathbb{Q}_2}(V_2(X))$$

commutes with $\text{End}^0(X)$. This implies that $\rho_{2,X}(\text{Gal}(L))$ commutes with $\text{End}_{\mathbb{Q}_2}V_2(X)$ and therefore consists of scalars. Since

$$\rho_{2,X}(\text{Gal}(L)) \subset \rho_{2,X}(\text{Gal}(F)) \subset \text{SL}(V_2(X)),$$

$\rho_{2,X}(\text{Gal}(L))$ is a finite group. Since Gal($L$) is a subgroup of finite index in Gal($F$), the group $H = \rho_{2,X}(\text{Gal}(F))$ is also finite. In particular, the kernel of the reduction map modulo 2

$$\text{Aut}_{\mathbb{Z}/2}(T_2(X)) \supset H \to G \subset \text{Aut}(X_2)$$

consists of periodic elements and, thanks to Minkowski-Serre Lemma [23], $Z := \ker(\pi : H \to G)$ has exponent 1 or 2. In particular, $Z$ is commutative. Since

$$Z \subset H \subset \text{Sp}(V_2(X)) \cong \text{Sp}(2g, \mathbb{Q}_2),$$
$Z$ is a $\mathbb{F}_2$-vector space of dimension $\leq g$.

Let $G_1$ be a minimal subgroup of $H$ such that $\pi(G_1) = G$. (Since $H$ is finite, such $G_1$ always exists.) Since $G$ is perfect, $G_1$ is also perfect. (Otherwise, we may replace $G_1$ by smaller $[G_1, G_1]$.) Clearly,

$$Z_1 := \ker(\pi : G_1 \to G) \subset Z$$

is also a $\mathbb{F}_2$-vector space of dimension $\leq g$. We have

$$Z_1 \subset G_1 \subset H \subset \text{Sp}(V_2(X)) \cong \text{Sp}(2g, \mathbb{Q}_2).$$

In particular, the symplectic $G_1$-module is a lifting of the $G_1(\to G)$-module $X_2$.

I claim that the natural representation of $G_1$ in the $2g$-dimensional $\mathbb{Q}_2$-vector space $V_2(X)$ is absolutely irreducible. Indeed, let us put

$$E := \text{End}_{G_1}(V_2(X)) \subset \text{End}_{\mathbb{Q}_2}(V_2(X)).$$

Clearly,

$$O_E = E \cap \text{End}_{\mathbb{Z}_2}(T_2(X)) \subset \text{End}_{\mathbb{Z}_2}(T_2(X))$$

is a $\mathbb{Z}_2$-algebra that is a free $\mathbb{Z}_2$-module, whose $\mathbb{Z}_2$-rank coincides with $\dim_{\mathbb{Q}_2}(E)$. Notice that $O_E$ is a pure $\mathbb{Z}_2$-submodule in $\text{End}_{\mathbb{Z}_2}(T_2(X))$, i.e. the quotient $\text{End}_{\mathbb{Z}_2}(T_2(X))/O_E$ is a torsion-free (finitely generated) $\mathbb{Z}_2$-module and therefore a free $\mathbb{Z}_2$-module of finite rank. It follows that the natural map

$$O_E/2O_E \longrightarrow \text{End}_{\mathbb{Z}_2}(T_2(X))/2\text{End}_{\mathbb{Z}_2}(T_2(X)) = \text{End}_{\mathbb{F}_2}(X_2)$$

is an embedding. Clearly, the image of $O_E/2O_E$ in $\text{End}_{\mathbb{F}_2}(X_2)$ lies in $\text{End}_G(X_2)$. Since $\text{End}_G(X_2) = \mathbb{F}_2$, we conclude that the rank of the free $\mathbb{Z}_2$-module $O_E$ is 1, i.e. $\dim_{\mathbb{Q}_2}(E) = 1$. This means that $E = \mathbb{Q}_2$, i.e. the $G_1$-module $V_2(X)$ is absolutely simple.

Let $\chi : G_1 \to \mathbb{Q}_2$ be the character of the absolutely irreducible faithful representation of $G_1$ in $V_2(X)$. Clearly, $\chi$ is a faithful (absolutely) irreducible character of degree $2g$. We need to prove that $\chi(G_1) \subset \mathbb{Q}$.

Let $F_1 \subset F$ be the subfield of invariants of the subgroup

$$\{ \sigma \in \text{Gal}(F) \mid \rho_{2, X}(\sigma) \in G_1 \} \subset \text{Gal}(F).$$

Clearly, $F_1$ is a finite separable algebraic extension of $F$ and

$$G_1 = \rho_{2, X}(\text{Gal}(F_1)).$$

Clearly, the image $\rho_{2, X}(\text{Gal}(F_1)) \subset \text{Aut}(X_2)$ coincides with

$$\pi \rho_{2, X}(\text{Gal}(F_1)) = \pi(G_1) = \pi_1(G_1) = G \subset \text{Aut}(X_2).$$

Let $L_1$ be the finite Galois extension of $F_1$ attached to

$$\rho_{2, X} : \text{Gal}(F_1) \longrightarrow \text{Aut}(T_2(X)).$$

Clearly, $\text{Gal}(L_1/F_1) = G_1$. In addition, all 2-power torsion points of $X$ are defined over $L_1$. It follows that all the endomorphisms of $X$ are defined over $L_1$ (see [22]). On the other hand, I claim that the ring $\text{End}_{F_1}(X)$ of
\(F_1\)-endomorphisms of \(X\) coincides with \(\mathbb{Z}\). Indeed, there is a natural embedding

\[
\text{End}_{F_1}(X) \otimes \mathbb{Z}/2\mathbb{Z} \to \text{End}_{\text{Gal}(F_1)}(X_2) = F_2
\]

that implies that the rank of the free \(\mathbb{Z}\)-module \(\text{End}_{F_1}(X)\) does not exceed 1 and therefore equals 1, i.e. \(\text{End}_{F_1}(X) = \mathbb{Z}\).

Since all the endomorphisms of \(X\) are defined over \(L_1\), there is a natural homomorphism

\[
\kappa : G_1 = \text{Gal}(L_1/F_1) \to \text{Aut}(\text{End}(X))
\]

such that

\[
\text{End}_{F_1}(X) = \{ u \in \text{End}(X) \mid \kappa(\sigma)u = u, \ \forall \sigma \in \text{Gal}(L_1/F_1) = G_1 \},
\]

\[
\sigma(ux) = (\kappa(\sigma)u)(\sigma(x)), \ \forall x \in X(L_1), \ u \in \text{End}(X), \ \sigma \in \text{Gal}(L_1/F_1) = G_1.
\]

Further we write \(\kappa(\sigma)u\) for \(\kappa(\sigma)(u)\). Since \(\text{End}_{F_1}(X) = \mathbb{Z}\), we conclude that

\[
\mathbb{Z} = \{ u \in \text{End}(X) \mid \kappa(\sigma)u = u, \ \forall \sigma \in \text{Gal}(L_1/F_1) = G_1 \}.
\]

Since all 2-power torsion points of \(X\) defined over \(L_1\),

\[
\sigma(ux) = \kappa(\sigma)u(\sigma(x)), \ \forall x \in T_2(X), \ u \in \text{End}(X), \ \sigma \in G_1.
\]

Since \(\text{Aut}(\text{End}(X)) \subset \text{Aut}(\text{End}^0(X))\), one may view \(\kappa\) as

\[
\kappa : G_1 = \text{Gal}(L_1/F_1) \to \text{Aut}(\text{End}^0(X)), \ u \mapsto \kappa(\sigma)u, \ u \in \text{End}^0(X), \ \sigma \in G_1
\]

and we have

\[
\mathbb{Q} = \{ u \in \text{End}^0(X) \mid \kappa(\sigma)u = u, \ \forall \sigma \in \text{Gal}(L_1/F_1) = G_1 \},
\]

\[
\sigma(ux) = \kappa(\sigma)u(\sigma(x)), \ \forall x \in V_2(X), \ u \in \text{End}^0(X), \ \sigma \in G_1.
\]

Recall that

\[
\text{End}^0(X) \subset \text{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_2 = \text{End}_{\mathbb{Q}_2}(V_2(X)),
\]

\[
G_1 \subset \text{GL}(V_2(X)) = (\text{End}_{\mathbb{Q}_2}(V_2(X)))^*.
\]

It follows that

\[
\sigma u \sigma^{-1} = \kappa(\sigma)u, \ \forall u \in \text{End}^0(X), \ \sigma \in G_1.
\]

By Skolem-Noether Theorem, every automorphism of the central simple \(\mathbb{Q}_2\)-algebra \(\text{End}^0(X) \cong M_q(\mathbb{H}_p)\) is an inner one. This implies that for each \(\sigma \in G_1\) there exists \(w_\sigma \in \text{End}^0(X)^*\) such that

\[
\sigma u \sigma^{-1} = \kappa(\sigma)u = w_\sigma u w_\sigma^{-1}, \ \forall u \in \text{End}^0(X).
\]

Since the center of \(\text{End}^0(X)\) is \(\mathbb{Q}\), the choice of \(w_\sigma\) is unique up to multiplication by a non-zero rational number. This implies that \(w_\sigma w_\tau\) equals \(w_{\sigma \tau}\) times a non-zero rational number.

Let us put

\[
c'_\sigma = \sigma w_\sigma^{-1} \in (\text{End}_{\mathbb{Q}_2}(V_2(X)))^*.
\]
Clearly, each $c'_\sigma$ commutes with $\text{End}^0(X)$ and therefore with $\text{End}^0(X) \otimes \mathbb{Q}_2 = \text{End}_{\mathbb{Q}_2}(V_2(X))$. It follows that all $c'_\sigma$ are scalars, i.e. lie in $\mathbb{Q}_2^* \text{Id}$. (Here Id is the identity map on $V_2(X)$.) Clearly, the image

$$c_\sigma \in \mathbb{Q}_2^* \text{Id}/\mathbb{Q}^* \text{Id} \cong \mathbb{Q}_2^*/\mathbb{Q}^*$$

of $c'_\sigma$ in $\mathbb{Q}_2^*/\mathbb{Q}^*$ does not depend on the choice of $w_\sigma$. It is also clear that the map

$$G_1 \longrightarrow \mathbb{Q}_2^*/\mathbb{Q}^*, \quad \sigma \longmapsto c'_\sigma$$

is a group homomorphism. Since $G_1$ is perfect and $\mathbb{Q}_2^*/\mathbb{Q}^*$ is commutative, this homomorphism is trivial, i.e. $c_\sigma = 1$ for all $\sigma \in G_1$. This means that

$$c_\sigma \in \mathbb{Q}^* \text{Id}, \quad \forall \sigma \in G_1$$

and therefore

$$\sigma = (c'_\sigma)^{-1} w_\sigma \in \text{End}^0(X)^*, \quad \forall \sigma \in G_1.$$  

Recall [18] that if one view an element $u \in \text{End}^0(X)$ as linear operator in $V_2(X)$ then the characteristic polynomial $P_u(t)$ of $u$ has rational coefficients; in particular, the trace of $u$ is a rational number. It follows that $\chi(G_1) \subset \mathbb{Q}$.

Let $M$ be the image of $\mathbb{Q}[G_1] \rightarrow \text{End}^0(X)$. Clearly, $M \otimes \mathbb{Q}_2$ coincides with the image of

$$\mathbb{Q}_2[G_1] \longrightarrow \text{End}^0(X) \otimes \mathbb{Q}_2 = \text{End}_{\mathbb{Q}_2}(V_2(X)).$$

Since the $G_1$-module $V_2(X)$ is absolutely simple,

$$\mathbb{Q}_2[G_1] \longrightarrow \text{End}_{\mathbb{Q}_2}(V_2(X))$$

is surjective. This implies that

$$\dim_\mathbb{Q}(M) = \dim_\mathbb{Q}(\text{End}^0(X))$$

and therefore, $M = \text{End}^0(X)$, i.e. $\mathbb{Q}[G_1] \rightarrow \text{End}^0(X)$ is surjective. The semi-simplicity of $\mathbb{Q}[G_1]$ allows us to identify $\text{End}^0(X)$ with a direct summand of $\mathbb{Q}[G_1]$.

If $\ell$ is a prime number that does not divide order of $G_1$ then it is well-known that the group algebra $\mathbb{Q}_\ell[G_1]$ is a direct product of matrix algebras over (commutative) fields. It follows that $p$ divides order of $G_1$. Since $\#(G_1)$ equals $\#(G)$ times a power of 2 and $p$ is odd, we conclude that $p$ divides $\#(G)$. In particular, $G_1$ contains an element $u$ of exact order $p$. Since

$$u \in G_1 \subset \text{End}^0(X) \subset \text{End}_{\mathbb{Q}_2}(V_2(X)),$$

$P_u(t)$ is a polynomial of degree $2g$ with rational coefficients and one of its roots is a primitive $p$th root of unity. It follows that $P_u(t)$ is divisible in $\mathbb{Q}[t]$ by the $p$-th cyclotomic polynomial $\Phi_p(t) = (t^p - 1)/(t - 1)$. Since the degree of $\Phi_p$ is $p - 1$, we conclude that the degree $2g$ of $P_u(t)$ is greater or equal than $p - 1$, i.e. $2g \geq p - 1$. 

BULLETIN DE LA SOCIÉTÉ MATHEMATIQUE DE FRANCE
Assume for a while that the $G$-module $X_2$ is very simple. Since $G_1 \to G$ is surjective, the $G_1$-module $X_2$ and its lifting $V_2(X)$ are also very simple $G_1$-modules [29, Remark 5.2 (i,v(a))]. Since $Z_1$ is normal in $G_1$, we conclude, thanks to [29, Remark 5.2 (vii)] that either the $Z_1$-module $V_2(X)$ is absolutely simple or $Z_1$ consists of scalars. Since $Z_1$ is a finite commutative group, it does not admit absolutely irreducible representations of dimension $>1$. Since $\dim_{\mathbb{Q}_2}(V_2(X)) = 2g > 1$, we conclude that $Z_1$ consists scalars; in particular, $Z_1$ is a central subgroup in $G_1$. Since $Z_1 \subseteq G_1 \subset \text{Sp}_2(V_2(X)) \cong \text{Sp}(2g, \mathbb{Q}_2)$, either $Z = \{1\}$ or $Z = \{\pm 1\}$. This implies that $Z_1$ is a cyclic group of order 1 or 2.

Further we no longer assume that the $G$-module $X_2$ is very simple. Assume instead that every homomorphism from $Z$ to $\text{GL}(g-1, \mathbb{F}_2)$ is trivial. I claim that in this case $Z$ is again a central subgroup of $G_1$. Indeed, the short exact sequence

$$1 \to Z \to G_1 \to G \to 1$$

defines, in light of commutativeness of $Z$, a natural homomorphism

$$\eta : G \to \text{Aut}(Z)$$

which is trivial if and only if $Z$ is central in $G_1$. Clearly, $\eta(G)$ is a finite perfect group. Recall that $Z$ is an elementary 2-group, i.e. $Z \cong \mathbb{F}_2^r$ for some nonnegative integer $r$. Clearly, we may assume that $r \geq 1$ and therefore $\text{Aut}(Z) \cong \text{GL}(r, \mathbb{F}_2)$. If $r \leq g-1$ then we are done. Suppose that $r = g$. Then $Z$ must contain

$$\{\pm 1\} \subset \text{Sp}_2(V_2(X)).$$

Since $\{\pm 1\}$ is a central subgroup of $G_1$, the elements of $\eta(G) \subset \text{Aut}(Z)$ act trivially on $\{\pm 1\}$. Since the quotient $Z/\{\pm 1\}$ has $\mathbb{F}_2$-dimension $g-1$, elements of $\eta(G)$ act trivially on $Z/\{\pm 1\}$. This implies that $\eta(G)$ is isomorphic to a subgroup of the commutative group $\text{Hom}(Z/\{\pm 1\}, \{\pm 1\})$. Since $\eta(G)$ is perfect, we conclude that $\eta(G) = \{1\}$, i.e. $Z$ is a central subgroup and therefore is either $\{1\}$ or $\{\pm 1\}$.

6. Hyperelliptic two-dimensional jacobians in characteristic 3

Throughout this section $K$ is a field of characteristic $p = 3$ and $K_a$ its algebraic closure, $n = 5$ or 6,

$$f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$$

a separable polynomial of degree $n$, i.e. all $a_i \in K, a_n \neq 0$ and $f$ has no multiple roots. We write $\text{Gal}(f) \subset S_n$ for the Galois group of $f$ over $K$. 

TOME 132 – 2004 – 8° 4
Let $C_f$ be the hyperelliptic curve $y^2 = f(x)$ over $K_a$.

**Lemma 6.1.** — Suppose that $n = \deg(f) = 5$ and $a_4 = 0$.

(i) The jacobian $J(C_f)$ of $C_f$ is a supersingular abelian variety over $K_a$ if and only if $a_1 = a_2 = 0$, i.e.,

$$f(x) = a_5x^5 + a_3x^3 + a_0.$$ 

If this is the case then $J(C_f)$ is isogenous but not isomorphic to a self-product of a supersingular elliptic curve.

(ii) Suppose that $a_0 \neq 0$ (e.g., $f(x)$ is irreducible over $K$) and $J(C_f)$ is a supersingular abelian variety. Then $\text{Gal}(f) \subset \mathbb{A}_5$ if and only if $-1$ is a square in $K$, i.e. $K$ contains $\mathbb{F}_9$.

**Proof.** — Since $p = 3$, $f(x)^{(p-1)/2} = f(x)$. Let us consider the matrices

$$M := \begin{pmatrix} a_{p-1} & a_{p-2} \\ a_{2p-1} & a_{2p-2} \end{pmatrix} = \begin{pmatrix} a_2 & a_1 \\ a_5 & 0 \end{pmatrix}, \quad M^{(3)} := \begin{pmatrix} a_3^3 & a_1^3 \\ a_5^3 & 0 \end{pmatrix}.$$ 

Extracting cubic roots from all entries of $M$ one gets the Hasse-Witt/Cartier-Manin matrix $M^{(3)}$ of $C$ (with respect to the standard basis in the space of differentials of the first kind) [13], [24], [5, p. 129]. Recall (see [13, p. 78], [19], [24, Thm 3.1], [5, Lemma 1.1]) that the jacobian $J(C)$ is a supersingular abelian surface not isomorphic to a product of two supersingular elliptic curves if and only if $M \neq 0$ but

$$M^{(3)}M = 0.$$ 

Clearly, $M \neq 0$, because $a_5 \neq 0$. It is also clear that

$$\det(M^{(3)}) = \det(M^{(3)}) \det(M) = (-a_1a_2^3)(-a_1a_5) = a_1^4a_5^4.$$ 

Hence, if $M^{(3)}M = 0$ then $a_1 = 0$. Suppose that $a_1 = 0$. Then

$$M = \begin{pmatrix} a_2 & 0 \\ a_5 & 0 \end{pmatrix}, \quad M^{(3)} = \begin{pmatrix} a_3^3 & 0 \\ a_5^3 & 0 \end{pmatrix}, \quad M^{(3)}M = \begin{pmatrix} a_2^2 & a_5^2 \\ a_3^2a_5 & 0 \end{pmatrix}.$$ 

We conclude that $M^{(3)}M = 0$ if and only if $a_1 = a_2 = 0$. It follows that $J(C)$ is a supersingular abelian surface if and only if $a_1 = a_2 = 0$. Since $M \neq 0$, the jacobian $J(C)$ is not isomorphic to a product of two supersingular elliptic curves. This proves (i).

In order to prove (ii), let us assume that $J(C_f)$ is supersingular, i.e.,

$$f(x) = a_5x^5 + a_3x^3 + a_0.$$ 

We know that $a_0 \neq 0, a_5 \neq 0$. Let us put

$$h(x) := a_5^{-1}f(x) = x^5 + b_3x^3 + b_0$$

where $b_3 = a_3/a_5, b_0 = a_0/a_5$. Clearly, $b_0 \neq 0$ and the Galois groups of $f(x)$ and $h(x)$ coincide. So, it suffices to check that $\text{Gal}(h) \subset \mathbb{A}_5$ if and only if $-1$ is a square in $K$. 

**Bulletin de la Société Mathématique de France**
The derivative $h'(x)$ of $h(x)$ is $5x^4 = -x^4$. Let $\alpha_1, \ldots, \alpha_5$ be the roots of $h$. Clearly,

$$\prod_{i=1}^{5} \alpha_i = -b_0.$$  

It is well-known that the Galois group of $h$ lies in the alternating group if and only if its discriminant

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

is a square in $K$. On the other hand, it is also well-known that

$$\prod_{i=1}^{5} h'(\alpha_i) = R(h, h') = (-1)^{\frac{1}{2} \deg(h)(\deg(h)-1)} D.$$  

(Here $R(h, h')$ is the resultant of $h$ and $h'$.) It follows that

$$R(h, h') = \prod_{i=1}^{5} (-\alpha_i^4) = -\left( \prod_{i=1}^{5} \alpha_i \right)^4 = -(-b_0)^4 = -b_0^4$$

and therefore $D = -b_0^4$. Clearly, $D$ is a square in $K$ if and only if $-1$ is a square in $K$.

**Example 6.2 (Counterexamples for $A_5$ and $S_5$).** — Let $k$ be an algebraically closed field of characteristic $p = 3$. Let $K = k(z)$ be the field of rational functions in variable $z$ with constant field $k$. We write $k(z)$ for an algebraic closure of $k(z)$. According to Abhyankar [1], the Galois group of the polynomial

$$h(x) = x^5 - zx^2 + 1 \in k(z)[x] = K[x]$$

is $A_5$ (see also [20, §3.3]). It follows that the Galois group of the polynomial

$$f(x) = x^5 h\left(\frac{1}{x}\right) = x^5 - zx^3 + 1 = \sum_{i=1}^{5} a_i x^i$$

is also $A_5$. (Here $a_5 = 1, a_4 = a_2 = a_1 = 0, a_3 = -z, a_0 = 1$.)

Let us consider the hyperelliptic curve

$$C : y^2 = x^5 - zx^3 + 1$$

of genus 2 over $\overline{k(z)}$. It follows from Lemma 6.1 that the jacobian $J(C)$ of $C$ is a supersingular abelian surface that is not isomorphic to a product of two supersingular elliptic curves. Hence $\text{End}(J(C))$ is isomorphic to a certain order in the matrix algebra of size 2 over the quaternion $\mathbb{Q}$-algebra ramified exactly at 3 and $\infty$. See [5, Prop. 2.19]) for an explicit description of this order.

Assume now that $k$ is an algebraic closure of $F_3$. Let us put

$$K_0 = F_3(z) \subset K = k(z) \subset \overline{k(z)}.$$
Clearly, $-1$ is not a square in $K_0$ and $\overline{k(z)}$ is an algebraic closure of $K_0$. Also, $f(x) \in K_0[x]$. An elementary calculation (as in the proof of Lemma 6.1 (ii)) shows that the discriminant of $f(x)$ is $-1$. This implies that the Galois group of $f(x)$ over $K_0$ does not lie in $A_5$. It follows that the Galois group of $f(x) = x^5 - zx^3 + 1$ over $K_0$ is $S_5$. However, as we have already seen, the jacobian of $y^2 = x^5 - zx^3 + 1$ is supersingular.

**Theorem 6.3.** — Let $K$ be a field with char$(K) = 3$, $K_a$ its algebraic closure, $f(x) \in K[x]$ an irreducible separable polynomial of degree $n = 5$ or $6$. Let us assume that the Galois group Gal$(f)$ of $f$ is the full symmetric group $S_n$. Assume, in addition, that $-1$ is a square in $K$, i.e. $K$ contains $\mathbb{F}_9$.

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

**Proof of Theorem 6.3.** — Thanks to Remark 2.3, we may and will assume that $n = 5$. We have

$$f(x) = \sum_{i=0}^{5} a_i x^i \in K[x]$$

where all the coefficients $a_i \in K$ and $a_0 \neq 0$. Let us put

$$\gamma := \frac{a_4}{5a_0}, \quad h(x) := f(x - \gamma).$$

Clearly, $h(x) \in K[x]$ is an irreducible polynomial of degree 5 and Gal$(h) = \text{Gal}(f) = S_5$. It is also clear that if

$$h(x) = \sum_{i=0}^{5} b_i x^i \in K[x]$$

then $b_4 = 0$, $b_5 = a_5 \neq 0$. The substitution $x_1 = x + \gamma$, $y_1 = y$ establishes a $K$-bireational isomorphism between hyperelliptic curves $C = C_f : y^2 = f(x)$ and $C_1 = C_h : y_1^2 = h(x_1)$ and induces an isomorphism of the jacobians $J(C_f)$ and $J(C_h)$.

Suppose that $\text{End}(J(C_f)) \neq \mathbb{Z}$. Then it follows from Theorem 2.1 of [25] that $J(C_f)$ is a supersingular abelian variety. It follows that $J(C_h) \cong J(C_f)$ is also a supersingular abelian variety. Applying Lemma 6.1 (ii) to $h$, we conclude that Gal$(h) \subset A_5$, because $-1$ is a square in $K$. However, Gal$(h) = S_5$. We obtained the desired contradiction. \qed

**Example 6.4.** — Let $k$ be an algebraically closed field of characteristic 3. Let $K = k(z)$ be the field of rational functions in variable $z$ with constant field $k$. We write $k(z)$ for an algebraic closure of $k(z)$. Let $h(x) \in k[x]$ be a Morse polynomial of degree 5. This means that the derivative $h'(x)$ of $h(x)$ has $\deg(h) - 1 = 4$ distinct roots $\beta_1, \ldots, \beta_4$ and $h(\beta_i) \neq h(\beta_j)$ while $i \neq j$. (For example, $x^5 - x$ is a Morse polynomial.) Then a theorem of Hilbert (see
[21, Thm 4.4.5, p. 41]) asserts that the Galois group of \( h(x) - z \) over \( k(z) \) is \( S_n \).

Let us consider the hyperelliptic curve

\[
C : \quad y^2 = h(x)
\]

of genus 2 over \( \overline{k(z)} \) and its jacobian \( J(C) \). It follows from Theorem 6.3 that \( \text{End}(J(C_f)) = \mathbb{Z} \). (The case of \( h(x) = x^5 - x \) was earlier treated by Mori [15].)

7. A corollary

Combining Theorems 2.1 and 6.3 together with Theorem 2.3 of [29] and Theorem 2.1 of [25], we obtain the following statement.

**Theorem 7.1.** — Let \( K \) be a field with \( \text{char}(K) \neq 2 \), \( K_a \) its algebraic closure, \( f(x) \in K[x] \) an irreducible separable polynomial of degree \( n \geq 5 \) such that the Galois group of \( f \) is either \( S_n \) or \( A_n \). If \( \text{char}(K) = 3 \) and \( n \leq 6 \) then we additionally assume that \( \text{Gal}(f) = S_n \) and \( K \) contains \( F_9 \).

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

**BIBLIOGRAPHY**


