HYPERELLIPTIC JACOBIANS WITHOUT COMPLEX MULTIPLICATION IN POSITIVE CHARACTERISTIC

YURI G. ZARHIN

1. Introduction

The aim of this note is to prove that in positive characteristic \( p \neq 2 \) the jacobian \( J(C) = J(C_f) \) of a hyperelliptic curve

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

has only trivial endomorphisms over an algebraic closure of the ground field \( K \) if the Galois group \( \text{Gal}(f) \) of the polynomial \( f \in K[x] \) of even degree is “very big”.

More precisely, if \( f \) is a polynomial of even degree \( n \geq 10 \) and \( \text{Gal}(f) \) is either the symmetric group \( S_n \) or the alternating group \( A_n \) then \( \text{End}(J(C)) = \mathbb{Z} \). Notice that it is known \(^1\) that in this case (and even for all integers \( n \geq 5 \)) 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.

There are some results of this type in the literature. Previously Mori \(^1\), \(^3\) has constructed explicit examples of hyperelliptic jacobians without nontrivial endomorphisms. Namely, he proved that if \( K = k(z) \) is a field of rational functions in variable \( z \) with constant field \( k \) of characteristic \( p \neq 2 \) then for each integer \( g \geq 2 \) the jacobian of a hyperelliptic \( K \)-curve

\[ y^2 = x^{2g+1} - x + z \]

has no nontrivial endomorphisms if \( p \) does not divide \( g(2g+1) \).

Our result stated above implies, in particular, that for each integer \( g \geq 4 \) the jacobian of a hyperelliptic \( K \)-curve

\[ y^2 = x^{2g+2} - x + z \]

has no nontrivial endomorphisms if \( p \) does not divide \( (g+1)(2g+1) \), since in this case the Galois group of \( x^{2g+2} - x + z \) over \( K \) is \( S_{2g+2} \).

2. Main result

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

---

\(^1\) Partially supported by the NSF.
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 even degree $n \geq 10$ such that the Galois group of $f$ is either $S_n$ or $A_n$. 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 $\text{End}(J(C_f)) = \mathbb{Z}$.

Examples 2.2. Let $k$ be a field of odd characteristic $p$. Let $k(z)$ be the field of rational functions in variable $z$ with constant field $k$.

1. Suppose $K_n = k(z_1, \ldots, z_n)$ is the field of rational functions in $n$ independent variables $z_1, \ldots, z_n$ over $k$. Then the Galois group of a polynomial $x^n - z_1 x^{n-1} + \cdots + (-1)^n z_n$ over $K_n$ is $S_n$. Therefore if $n \geq 10$ is even then the jacobian of the curve $y^2 = x^n - z_1 x^{n-1} + \cdots + (-1)^n z_n$ has no nontrivial endomorphisms over an algebraic closure of $K_n$.

2. Suppose $h(x) \in k[x]$ is a Morse polynomial of degree $n$ and $p$ does not divide $n$. This means that the derivative $h'(x)$ of $h(x)$ has $n-1$ distinct roots $\beta_1, \ldots, \beta_{n-1}$ (in an algebraic closure of $k$) and $h(\beta_i) \neq h(\beta_j)$ while $i \neq j$. For example, $h(x) = x^n - x$ enjoys these properties if and only if $p$ does not divide $n(n-1)$.

Then the Galois group of $h(x) - z$ over $k(z)$ is the symmetric group $S_n$ (\cite{1}, Th. 4.4.5, p. 41). Hence if $n \geq 10$ is even and $p$ does not divide $n(n-1)$ then the jacobian of the curve $y^2 = h(x) - z$ has no nontrivial endomorphisms over an algebraic closure of $k(z)$.

3. Suppose $k$ is algebraically closed. Suppose $n = q + t$ where $q$ is a power of $p$ and $t > q$ is a positive integer not divisible by $p$. Then the Galois group of $x^n - xz^t + 1$ over $k(z)$ is the alternating group $A_n$ (\cite{1}, Th. 1, p. 67). Clearly, if $t$ is odd then $n = q + t$ is even and $n > 2q \geq 6$, i.e., $n \geq 8$. In addition, $n \geq 10$ unless $q = 3, t = 5$. This implies that if $t$ is odd and $(q,t) \neq (3,5)$ then the jacobian of the curve $y^2 = x^n - xz^t + 1$ has no nontrivial endomorphisms over an algebraic closure of $k(z)$.

As was already pointed out, in light of Th. 2.1 of \cite{10}, Theorem 2.1 is an immediate corollary of the following auxiliary statement.

Theorem 2.3. Suppose $n = 2g + 2$ is an even integer which is greater than or equal to 10. Suppose $f(x) \in K[x]$ is a separable polynomial of degree $n$, whose Galois group is either $A_n$ or $S_n$. Suppose $C$ is the hyperelliptic curve $y^2 = f(x)$ of genus $g$ over $K$ and $J(C)$ is the jacobian of $C$.

Then $J(C)$ is not a supersingular abelian variety.

Remark 2.4. Replacing $K$ by its proper quadratic extension, we may assume in the course of the proof of Theorem 2.1 that $\text{Gal}(f) = A_n$. Also, replacing $K$ by its abelian extension obtained by adjoining to $K$ all 2-power roots of unity, we may assume that $K$ contains all 2-power roots of unity.

We prove Theorem 2.3 in the next Section.
3. Proof of Theorem 2.3

So, we assume that $K$ contains all 2-power roots of unity, $f(x) \in K[x]$ is an irreducible separable polynomial of even degree $n = 2g + 2 \geq 10$ and $\text{Gal}(f) = A_n$. Therefore $J(C)$ is a $g$-dimensional abelian variety defined over $K$. The group $J(C)_2$ of its points of order 2 is a $2g$-dimensional $F_2$-vector space provided with the natural action of $\text{Gal}(K)$. It is well-known (see for instance [11]) that the image of $\text{Gal}(K)$ in $\text{Aut}(J(C)_2)$ is canonically isomorphic to $\text{Gal}(f)$.

Now Theorem 2.3 becomes an immediate corollary of the following two assertion.

Lemma 3.1. Let $F$ be a field, whose characteristic is not 2 and assume that $F$ contains all 2-power roots of unity. Let $g$ be a positive integer and $G$ a finite simple non-abelian group enjoying the following properties:

(a) Each nontrivial representation of $G$ in characteristic 0 has dimension $> 2g$;

(b) If $G' \to G$ is a surjective group homomorphism, whose kernel is a central subgroup of order 2 then each faithful irreducible representation of $G'$ in characteristic zero has dimension $\neq 2g$.

(c) Each nontrivial representation of $G$ in characteristic 2 has dimension $\geq 2g$.

If $X$ is a $g$-dimensional abelian variety over $F$ such that the image of $\text{Gal}(F)$ in $\text{Aut}(X_2)$ is isomorphic to $G$ then $X$ is not supersingular.

Lemma 3.2. Suppose $n = 2g + 2 \geq 10$ is an even integer. Let us put $G = A_n$. Then

(a) Each nontrivial representation of $G$ in characteristic 0 has dimension $\geq n - 1 > 2g$;

(b) Each nontrivial proper projective representation of $G$ in characteristic 0 has dimension $\neq 2g$;

(c) Each nontrivial representation of $G$ in characteristic 2 has dimension $\geq 2g$.

Lemma 3.1 will be proven in the next Section. We prove Lemma 3.2 in Section 5.

4. Not supersingularity

We keep all the notations of Lemma 3.1. Assume that $X$ is supersingular. Our goal is to get a contradiction. We write $T_2(X)$ for the 2-adic Tate module of $X$ and $\rho_{2,X} : \text{Gal}(F) \to \text{Aut}_{Z_2}(T_2(X))$ for the corresponding 2-adic representation. It is well-known that $T_2(X)$ is a free $Z_2$-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
\[ \bar{\rho}_{2,X} : \text{Gal}(F) \to \text{Aut}(X_2) \]
defining the Galois action on the points of order 2 is the composition of \( \rho_{2,X} \) and (surjective) reduction map modulo 2
\[ \text{Aut}_{\mathbb{Z}_2}(T_2(X)) \to \text{Aut}(X_2). \]
This gives us a natural (continuous) surjection
\[ \pi : H \to \bar{\rho}_{2,X}(\text{Gal}(F)) \cong G, \]
whose kernel consists of elements of \( 1 + 2 \text{End}_{\mathbb{Z}_2}(T_2(X)) \). It follows from the property 3.1(c) and equality \( \dim_{\mathbb{F}_2}(X_2) = 2g \) that the \( G \)-module \( X_2 \) is absolutely simple and therefore the \( H \)-module \( X_2 \) is also absolutely simple.

Here the structure of \( H \)-module is defined on \( X_2 \) via
\[ H \subset \text{Aut}_{\mathbb{Z}_2}(T_2(X)) \to \text{Aut}(X_2). \]
Let \( V_2(X) = T_2(X) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2 \) be the \( \mathbb{Q}_2 \)-Tate module of \( X \). It is well-known that \( V_2(X) \) is the \( 2g \)-dimensional \( \mathbb{Q}_2 \)-vector space and \( T_2(X) \) is a \( \mathbb{Z}_2 \)-lattice in \( V_2(X) \). This implies easily that the \( \mathbb{Q}_2[H] \)-module \( V_2(X) \) is also absolutely simple.

The choice of polarization on \( X \) gives rise to a non-degenerate alternating bilinear form (Riemann form) \[ e : V_2(X) \times V_2(X) \to \mathbb{Q}_2(1) \cong \mathbb{Q}_2. \]
Since \( F \) contains all 2-power roots of unity, \( e \) is \( \text{Gal}(F) \)-invariant and therefore is \( H \)-invariant. In particular,
\[ H \subset \text{SL}(V_2(X)). \]

There exists a finite Galois extension \( L \) of \( K \) 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 (3) that the natural map
\[ \text{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_2 \to \text{End}_{\mathbb{Q}_2}V_2(X) \]
is an embedding. Dimension arguments imply that
\[ \text{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_2 = \text{End}_{\mathbb{Q}_2}V_2(X). \]
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 \( \text{Gal}(L) \) is a subgroup of finite index in \( \text{Gal}(F) \), the group \( H = \rho_{2, X}(\text{Gal}(F)) \) is also finite. In particular, the kernel of the reduction map modulo 2

\[
\text{Aut}_{\mathbb{Z}_2} T_2(X) \supset H \rightarrow G \subset \text{Aut}(X_2)
\]

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

\[
Z \subset H \subset \text{SL}(V_2(X)),
\]

\( Z \) is a \( \mathbf{F}_2 \)-vector space of dimension \( d < 2g \). This implies that the adjoint action

\[
G \rightarrow \text{Aut}(Z) \cong \text{GL}_d(\mathbf{F}_2)
\]

is trivial, in light of property (3.1)(c). This means that \( Z \) lies in the center of \( H \). Since the \( \mathbb{Q}_2[H] \)-module \( V_2(X) \) is faithful absolutely simple, \( Z \) consists of scalars. This implies that either \( Z = \{1\} \) or \( Z = \{\pm 1\} \). If \( Z = \{1\} \) then \( H \cong G \) and \( V_2(X) \) is a faithful \( \mathbb{Q}_2[G] \)-module of dimension \( 2g \) which contradicts the property (3.1)(a). Therefore \( Z = \{\pm 1\} \) and \( H \rightarrow G \) is a surjective group homomorphism, whose kernel is a central subgroup of order 2. But \( V_2(X) \) is a faithful absolutely simple \( \mathbb{Q}_2[H] \)-module of dimension \( 2g \) which contradicts the property (3.1)(b). This ends the proof of Lemma 3.1.

5. Representation theory

Proof of Lemma 3.1. The property (a) follows easily from Th. 2.5.15 on p. 71 of [3]. The property (c) follows readily from Th. 1.1 on p. 127 of [8].

In order to prove the property (b), recall (Th. 1.3(ii) on pp. 583-584 of [4]) that each proper projective representation of \( \mathbf{A}_n \) in characteristic \( \neq 2 \) has dimension divisible by \( 2^{[(n-s-1)/2]} \) where \( s \) is the exact number of terms in the dyadic expansion of \( n \). We have \( n = 2^{w_1} + \cdots + 2^{w_s} \) where \( w_i \)'s are distinct nonnegative integers. In particular, if \( s = 1 \) then \( n = 2^w \geq 16 \) and \( 2^{[(n-s-1)/2]} = 2^{(n-2)/2} > n - 2 \). This proves the property (b) if \( s = 1 \).

If \( s = 2 \) then

\[
2^{[(n-s-1)/2]} = 2^{(n-4)/2} = \frac{1}{2} 2^{(n-2)/2} > (n-2)
\]

if \( n - 2 > 8 \). This proves the property (b) in the case of \( n = 2^{w_1} + 2^{w_2} > 10 \).

The remaining case \( n = 10 \) follows from Tables in [4].

Further we assume that \( s \geq 3 \). In particular, \( n \geq 14 \) and \( n - 2 \) is not a power of 2. Since \( n \) is even, all \( w_i \geq 1 \) and \( n \geq 2(2^s - 1) \). If \( n = 2(2^s - 1) \) then \( n - 2 = 2(2^s - 2) \) is not divisible by \( 2^3 \). Therefore if \( [(n-s-1)/2] \geq 3 \) then the property (b) holds. On the other hand, if \( [(n-s-1)/2] \leq 3 \) then \( n - s - 1 \leq 2 \cdot 3 + 1 \), i.e., \( 2(2^s - 1) - s - 1 \leq 7 \) which implies that \( s < 3 \). We get a contradiction which, in turn, implies that \( n > 2(2^s - 1) \) and therefore \( n > 2^{s+1} \). This implies easily that \( n \geq 2^{s+1} + 6 \geq 20 \). In particular, \( s < \log_2(n) - 1 \) and \( 2^{[(n-s-1)/2]} \geq 2^{(n-\log_2(n))/2} > (2^n/n)^{1/2} \).

Since \( n - 2 \) is not a power of 2, there are no proper projective representations of \( \mathbf{A}_n \) of dimension \( 2g = n - 2 \) in characteristic 0 if \( 2^{[(n-s-1)/2]} >
(n − 2)/2. Clearly, this inequality holds if \((2^n/n)^{1/2}/2 > (n - 2)/2\). But this inequality is equivalent to

\[2^n > n(n - 2)^2\]

which holds for all \(n \geq 20\).

References

[1] S. S. Abhyankar, Alternating group coverings of the affine line for characteristic greater than two. Math. Ann. 296 (1993), 63–68.
[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups. Clarendon Press, Oxford, 1985.
[3] G. James, A. Kerber, The representation theory of the symmetric group. Addison Wesley Publishing Company, Reading, MA 1981.
[4] Sh. Mori, The endomorphism rings of some abelian varieties. Japanese J. Math, 2(1976), 109–130.
[5] Sh. Mori, The endomorphism rings of some abelian varieties. II, Japanese J. Math, 3(1977), 105–109.
[6] D. Mumford, Abelian varieties, Second edition, Oxford University Press, London, 1974.
[7] J.-P. Serre, Topics in Galois Theory. Jones and Bartlett Publishers, Boston-London, 1992.
[8] A. Wagner, The faithful linear representations of \(S_n\) and \(A_n\) over a field of characteristic 2. Math. Z. 151 (1976), 127–137.
[9] A. Wagner, An observation on the degrees of the symmetric and alternating group over an arbitrary field. Arch. Math. 39 (1977), 583–589.
[10] Yu. G. Zarhin, Hyperelliptic jacobians without complex multiplication. Math. Res. Letters 7(2000), 123–132.
[11] Yu. G. Zarhin Hyperelliptic jacobians and modular representations. In: Moduli of abelian varieties (C. Faber, G. van der Geer, F. Oort, eds.), Birkhäuser, to appear.

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

E-mail address: zarhin@math.psu.edu