Mathematical Research Letters **8**, 429–435 (2001)

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 K_a of the ground field K if the Galois group $\mathrm{Gal}(f)$ 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 $\mathrm{Gal}(f)$ is either the symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$ then $\mathrm{End}(J(C)) = \mathbf{Z}$. Notice that it is known [14] that in this case (and even for all integers $n \geq 5$) either $\mathrm{End}(J(C)) = \mathbf{Z}$ 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 [7], [8] 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 g-dimensional jacobian of a hyperelliptic K-curve

$$y^2 = x^{2g+1} - x + z$$

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

I am deeply grateful to the referee for helpful suggestions.

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 $\mathrm{Gal}(K)$ 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 even degree $n \geq 10$ such that the Galois group of f is either $\mathbf{S}_n$ or $\mathbf{A}_n$. Let C_f be the hyperelliptic curve*

Received February 2, 2001.
Partially supported by the NSF.

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

Examples 2.2. Let k be a field of odd prime characteristic p. Let $k(z)$ be the field of rational functions in variable z with constant field k. We write $\overline{k(z)}$ for an algebraic closure of $k(z)$.

(i) Suppose $K_n = k(z_1, \cdots, z_n)$ is the field of rational functions in n independent variables $z_1, \cdots, z_n$ 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 $\mathbf{S}_n$. Therefore if $n \ge 10$ 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.

(ii) Suppose p does not divide n and $h(x) \in k[x]$ is a *Morse polynomial* of degree n. This means that the derivative $h'(x)$ of $h(x)$ has $n-1$ distinct roots $\beta_1, \cdots \beta_{n-1}$ (in an algebraic closure of k) and $h(\beta_i) \ne h(\beta_j)$ while $i \ne j$. 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 $\mathbf{S}_n$ ([10], Th. 4.4.5, p. 41). Hence if $n \ge 10$ is even then the jacobian of the curve $y^2 = h(x) - z$ has no nontrivial endomorphisms over $\overline{k(z)}$. In particular, for each integer $g \ge 4$ the g-dimensional jacobian of a hyperelliptic K-curve $y^2 = x^{2g+2} - x - z$ has no nontrivial endomorphisms over $\overline{k(z)}$ if p does not divide $(g+1)(2g+1)$.

(iii) Suppose k is algebraically closed. Suppose an integer $q > 1$ is a power of p and t is a positive integer not divisible by p. Let us choose a positive integer s and a non-zero element a of k.

(a) Assume that $t > q$ and let us put $n = q + t$. The Galois group of $x^n - zx^t + 1$ over $k(z)$ is $\mathbf{A}_n$ ([1], Th. 1, p. 67). Clearly, if t is odd then $n = q + t$ is even and $n > 2q \ge 6$, i.e., $n \ge 8$. In addition, $n \ge 10$ unless $q = 3, t = 5$. This implies that if t is odd and $(q, t) \ne (3, 5)$ then the jacobian of the curve $y^2 = x^n - zx^t + 1$ has no nontrivial endomorphisms over $\overline{k(z)}$.

(b) Assume that $n = 2pd \ge 10$ for some positive integer d and $1 < t < pd$. Assume, in addition that t and n are relatively prime and s is divisible by t (e.g., $t = s = pd - 1$ if d is even). The Galois group of $x^n - ax^t + z^s$ over $k(z)$ is $\mathbf{A}_n$ ([2], p. 107). Therefore the jacobian of the hyperelliptic curve $y^2 = x^n - ax^t + z^s$ has no nontrivial endomorphisms over $\overline{k(z)}$.

As was already pointed out, in light of Th. 2.1 of [14], our 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* $\mathbf{A}_n$ *or* $\mathbf{S}_n$. *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 (in the case of $\mathrm{Gal}(f) = \mathbf{S}_n$) K by its proper quadratic extension, we may assume in the course of the proof of Theorem 2.3 that $\mathrm{Gal}(f) = \mathbf{A}_n$. 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 $\mathrm{Gal}(f) = \mathbf{A}_n$. 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 $\mathbf{F}_2$-vector space provided with the natural action of $\mathrm{Gal}(K)$. It is well-known (see for instance [15], Sect. 5) that the image of $\mathrm{Gal}(K)$ in $\mathrm{Aut}(J(C)_2)$ is canonically isomorphic to $\mathrm{Gal}(f)$.

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

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 be 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 absolutely 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 $\mathrm{Gal}(F)$ in $\mathrm{Aut}(X_2)$ is isomorphic to G then X is not supersingular.

In order to state the second assertion we need to recall the following definition ([13], p. 584). If V is a finite-dimensional vector space over an algebraically closed field then a projective representation $\rho : G \to \mathrm{PGL}(V)$ is called *proper* if there is no a linear representation $\rho' : G \to \mathrm{GL}(V)$ such that $\rho = \pi\rho'$ where $\pi : \mathrm{GL}(V) \twoheadrightarrow \mathrm{PGL}(V)$ is the natural surjection.

Lemma 3.2. *Suppose $n = 2g + 2 \geq 10$ is an even integer. Let us put $G = \mathbf{A}_n$. Then:*

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

$$\rho_{2,X} : \mathrm{Gal}(F) \to \mathrm{Aut}_{\mathbf{Z}_2}(T_2(X))$$

for the corresponding 2-adic representation. It is well-known that $T_2(X)$ is a free $\mathbf{Z}_2$-module of rank $2\dim(X) = 2g$ and

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

(the equality of Galois modules). Let us put

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

Clearly, the natural homomorphism

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

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

$$\mathrm{Aut}_{\mathbf{Z}_2}(T_2(X)) \to \mathrm{Aut}(X_2).$$

This gives us a natural (continuous) *surjection*

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

whose kernel consists of elements of $1 + 2\mathrm{End}_{\mathbf{Z}_2}(T_2(X))$. It follows from the property 3.1(c) and equality $\dim_{\mathbf{F}_2}(X_2) = 2g$ 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

$$H \subset \mathrm{Aut}_{\mathbf{Z}_2}(T_2(X)) \to \mathrm{Aut}(X_2).$$

The absolute simplicity of the H-module X_2 means that the natural homomorphism

$$\mathbf{F}_2[H] \to \mathrm{End}_{\mathbf{F}_2}(X_2)$$

is surjective ([4], Th. 9.2 on p. 145). By Nakayama's Lemma, this implies that another natural homomorphism

$$\mathbf{Z}_2[H] \to \mathrm{End}_{\mathbf{Z}_2}(T_2(X))$$

is also surjective (see [6], p. 252).

Let $V_2(X) = T_2(X) \otimes_{\mathbf{Z}_2} \mathbf{Q}_2$ be the $\mathbf{Q}_2$-Tate module of X. It is well-known that $V_2(X)$ is the $2g$-dimensional $\mathbf{Q}_2$-vector space and $T_2(X)$ is a $\mathbf{Z}_2$-lattice in $V_2(X)$. Clearly, the $\mathbf{Q}_2[H]$-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) [9]

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

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

$$H \subset \mathrm{SL}(V_2(X)).$$

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

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

Recall ([9]) that the natural map

$$\mathrm{End}^0(X) \otimes_{\mathbf{Q}} \mathbf{Q}_2 \to \mathrm{End}_{\mathbf{Q}_2} V_2(X)$$

is an embedding. Dimension arguments imply that

$$\mathrm{End}^0(X) \otimes_{\mathbf{Q}} \mathbf{Q}_2 = \mathrm{End}_{\mathbf{Q}_2} V_2(X).$$

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

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

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

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

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

$$\mathrm{Aut}_{\mathbf{Z}_2} T_2(X) \supset H \to G \subset \mathrm{Aut}(X_2)$$

consists of periodic elements and, thanks to Minkowski-Serre Lemma [11], $Z := \ker(H \to G)$ has exponent 1 or 2. In particular, Z is commutative. Since

$$Z \subset H \subset \mathrm{SL}(V_2(X)),$$

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

$$H \to H/Z = G \to \mathrm{Aut}(Z) \cong \mathrm{GL}_d(\mathbf{F}_2)$$

is trivial, in light of property 3.1(c). This means that Z lies in the center of H. Since the $\mathbf{Q}_2[H]$-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 $\mathbf{Q}_2[G]$-module of dimension $2g$ which contradicts the property 3.1(a). Therefore $Z = \{\pm 1\}$ and $H \to G$ is a surjective group homomorphism, whose kernel is a central subgroup of order 2. But $V_2(X)$ is a faithful absolutely simple $\mathbf{Q}_2[H]$-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 3.2. The property (a) follows easily from Th. 2.5.15 on p. 71 of [5]. The property (c) follows readily from Th. 1.1 on p. 127 of [12]. The rest of this Section is devoted to the proof of the property (b). First, notice that the case $n = 10$ follows from Tables in [3]. So, further we assume that $n \geq 12$.

We start with an elementary discussion of the dyadic expansion $n = 2^{w_1} + \cdots + 2^{w_s}$ of n. Here w_i's are distinct nonnegative integers with $w_1 < \cdots < w_s$ and s is the exact number of terms (non-zero digits) in the dyadic expansion of n. Since n is even, $w_1 \geq 1$ and therefore each $w_i \geq i$. This implies that $n \geq 2(2^s - 1) = 2^{s+1} - 2$.

By a theorem of Wagner (Th. 1.3(ii) on pp. 583–584 of [13]), each proper projective representation of $\mathbf{A}_n$ in characteristic $\neq 2$ has dimension divisible by $N := 2^{\lfloor \frac{n-s-1}{2} \rfloor}$. So, in order to prove (b), it suffices to check that $n - 2$ is *not* divisible by N for all even $n \geq 12$.

If $n = 12$, it is verified immediately. If $n \geq 14$ then $2^{n-2} > (n+1)(n-2)^2$. Then $2^{n-\log_2(n+1)-2} > (n-2)^2$. It is easy to see that $s \leq \log_2(n+1)$, so $2^{n-s-2} > (n-2)^2$. Taking square roots at both sides, we get $2^{\frac{n-s-2}{2}} > n - 2$. Then we see easily that $2^{\lfloor \frac{n-s-1}{2} \rfloor} > n - 2$. This finishes the proof of (b). □

6. Corrigendum to [15]

Page 475, Remarks 2.2, last line: read "absolutely simple" instead of "also very simple".

Page 478, line -5: read "Gal(K)" instead of "$G(K)$".

References

[1] S. S. Abhyankar, *Alternating group coverings of the affine line for characteristic greater than two*, Math. Ann. **296** (1993), 63–68.

[2] ———, *Galois theory on the line in nonzero characteristic*, Bull. Amer. Math. Soc. **27** (1992), 68–133.

[3] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Oxford, 1985.

[4] I. M. Isaacs, *Character theory of finite groups*, Pure and Applied Mathematics, No. 69, Academic Press, New York–San Francisco–London, 1976.

[5] G. James and A. Kerber, *The representation theory of the symmetric group*, Addison Wesley Publishing Company, Reading, MA, 1981.

[6] B. Mazur, *Deformation theory of Galois representations*, Modular forms and Fermat's last theorem (G. Cornell, J. H. Silverman, G. Stevens, eds.), Springer-Verlag, New York, 1997, pp. 243–311.

[7] Sh. Mori, *The endomorphism rings of some abelian varieties*, Japan. J. Math. **2** (1976), 109–130.

[8] ———, *The endomorphism rings of some abelian varieties* II, Japan. J. Math. **3** (1977), 105–109.

[9] D. Mumford, *Abelian varieties*, second edition, Oxford University Press, London, 1974.

[10] J.-P. Serre, *Topics in Galois Theory,* Res. Notes Math. **1**, Jones and Bartlett Publishers, Boston-London, 1992.

[11] A. Silverberg and Y. G. Zarhin, *Variations on a theme of Minkowski and Serre*, J. Pure Appl. Algebra **111** (1996), 285–302.
[12] A. Wagner, *The faithful linear representations of* $\mathbf{S}_n$ *and* $\mathbf{A}_n$ *over a field of characteristic* 2, Math. Z. **151** (1976), 127–137.
[13] ———, *An observation on the degrees of the symmetric and alternating group over an arbitrary field*, Arch. Math. **29** (1977), 583–589.
[14] Y. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*, Math. Res. Lett. **7** (2000), 123–132.
[15] ———, *Hyperelliptic jacobians and modular representations*, Moduli of abelian varieties (eds. G. van der Geer, C. Faber, F. Oort), Progr. Math. **195**, Birkhäuser, Basel–Boston–Berlin, 2001, pp. 473–490.

Dept. of Mathematics, Pennsylvania State University, University Park, PA 16802.
Institute for Mathematical Problems in Biology, Russian Academy of Sciences, Pushchino, Moscow Region, 142292, RUSSIA.
E-mail address: zarhin@math.psu.edu