HYPERELLIPTIC JACOBIANS AND PROJECTIVE LINEAR
GALOIS GROUPS

YURI G. ZARHIN

1. Introduction

In [14] the author proved that in characteristic 0 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 $K_\alpha$ of the ground field $K$ 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 $\alpha$-endomorphisms of $J(C_f)$ coincides with $\mathbb{Z}$. Later the author [15] proved that $\text{End}(J(C_f)) = \mathbb{Z}$ for an infinite series of $\text{Gal}(f) = L_{22r+1}(2^r) := \text{PSL}(2^{2r+1})$ and $n = 2(2^{2r+1}) + 1$ (with $\dim(J(C_f)) = 2^{4r+1}$). He also proved the same assertion when $n = 11$ or 12 and $\text{Gal}(f)$ is the Mathieu group $M_{11}$ or $M_{12}$. (In those cases $J(C_f)$ has dimension 5.)

We refer the reader to [12], [13], [7], [8], [9], [14], [15] for a discussion of known results about, and examples of, hyperelliptic jacobians without complex multiplication.

In the present paper we prove that $\text{End}(J(C_f)) = \mathbb{Z}$ when the set $\mathcal{R}_f$ of roots of $f$ can be identified with the $(m-1)$-dimensional projective space $\mathbb{P}^{m-1}(\mathbb{F}_q)$ over a finite field $\mathbb{F}_q$ of odd characteristic in such a way that $\text{Gal}(f)$, viewed as a permutation group of $\mathcal{R}_f$, becomes either the projective linear group $\text{PGL}(m, \mathbb{F}_q)$ or the projective special linear group $\text{PSL}(m, \mathbb{F}_q)$. Here we assume that $m > 2$. In this case

$$n = \deg(f) = \#(\mathbb{P}^{m-1}(\mathbb{F}_q)) = \frac{q^m - 1}{q - 1}$$

and $\dim(J(C_f))$ is $\lfloor \frac{q^m - 1}{q - 1} - 1 \rfloor / 2$, i.e. the integral part of $\frac{q^m - 1}{q - 1} - 1 / 2$.

Our proof is based on a result of Guralnick [3], who proved that in the “generic” case the dimension of each nontrivial irreducible representation of $\text{L}_m(q) := \text{PSL}(m, \mathbb{F}_q)$ in characteristic 2 is greater than or equal to

$$2\lfloor \frac{(q^m - 1)(q - 1)}{2} \rfloor.$$ 

We also discuss the similar problem when $K$ has prime characteristic $> 2$. It turns out that $\text{End}(J(C_f)) = \mathbb{Z}$ under an additional assumption that $m$ is even (i.e., when $n$ is even). The case of $n = 12$ and $\text{Gal}(f) = M_{12}$ is also treated.

Partially supported by NSF grant DMS-0070664.
2. Main results

Throughout this paper we assume that $K$ is a field with $\text{char}(K) \neq 2$. We fix its algebraic closure $K_a$ and write $\text{Gal}(K)$ for the absolute Galois group $\text{Aut}(K_a/K)$. If $X$ is an abelian variety defined over $K$ then we write $\text{End}(X)$ for the ring of $K_a$-endomorphisms of $X$.

Suppose $f(x) \in K[x]$ is a separable polynomial of degree $n \geq 5$. Let $\mathcal{R} = \mathcal{R}_f \subset K_a$ be the set of roots of $f$, let $K(\mathcal{R}_f) = K(\mathcal{R})$ be the splitting field of $f$ and $\text{Gal}(f) := \text{Gal}(K(\mathcal{R})/K)$ the Galois group of $f$, viewed as a subgroup of $\text{Perm}(\mathcal{R})$. 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 $J(C_f)$.

**Theorem 2.1.** Assume that there exist a positive integer $m > 2$ and an odd power prime $q$ such that $n = \frac{q^m - 1}{q - 1}$ and $\text{Gal}(f)$ contains a subgroup isomorphic to $L_m(q)$. (E.g., $\text{Gal}(f)$ is isomorphic either to $\text{PGL}_m(F_q)$ or to $L_m(q) = \text{PSL}_m(F_q)$.)

Then either $\text{End}(J(C_f)) = \mathbb{Z}$ or $m$ is odd, $\text{char}(K) > 0$ and $J(C_f)$ is a supersingular abelian variety.

**Remark 2.2.** Clearly $m$ is even if and only if $n$ is even.

**Remark 2.3.** Replacing $K$ by $K(\mathcal{R})^{L_m(q)}$, we may assume that $\text{Gal}(f) = L_m(q)$.

Also, taking into account that $L_m(q)$ is simple non-abelian and replacing $K$ by its abelian extension obtained by adjoining all 2-power roots of unity, we may assume that $K$ contains all 2-power roots of unity.

**Theorem 2.4.** Suppose $n = 12$ and $\text{Gal}(f)$ is isomorphic to the Mathieu group $M_{12}$. Then $\text{End}(J(C_f)) = \mathbb{Z}$.

**Remark 2.5.** When $\text{char}(K) = 0$ the assertion of Theorem 2.4 is proven in [13]. Taking into account that $M_{12}$ is simple non-abelian and replacing $K$ by its abelian extension obtained by adjoining all 2-power roots of unity, we may assume that $K$ contains all 2-power roots of unity.

We will prove Theorems 2.1 and 2.4 in §4.

3. Permutation groups and permutation modules

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 $G$ be a subgroup of $\text{Perm}(B)$. For each $b \in B$ we write $G_b$ for the stabilizer of $b$ in $G$; it is a subgroup of $G$.

**Remark 3.1.** Assume that the action of $G$ on $B$ is transitive. It is well-known that each $G_b$ is of index $n$ in $G$ and all the $G_b$’s are conjugate in $G$. Each conjugate of $G_b$ in $G$ is the stabilizer of a point of $B$. In addition, one may identify the $G$-set $B$ with the set of cosets $G/G_b$ with the standard action by $G$. 
Let $F$ be a field. We write $F^B$ for the $n$-dimensional $F$-vector space of maps $h : B \to F$. The space $F^B$ is provided with a natural action of $\text{Perm}(B)$ defined as follows. Each $s \in \text{Perm}(B)$ sends a map $h : B \to F$ into $sh : b \mapsto h(s^{-1}(b))$. The permutation module $F^B$ contains the $\text{Perm}(B)$-stable hyperplane

$$(F^B)^0 = \{ h : B \to F \mid \sum_{b \in B} h(b) = 0 \}$$

and the $\text{Perm}(B)$-invariant line $F \cdot 1_B$ where $1_B$ is the constant function 1. The quotient $F^B/(F^B)^0$ is a trivial 1-dimensional $\text{Perm}(B)$-module.

Clearly, $(F^B)^0$ contains $F \cdot 1_B$ if and only if $\text{char}(F)$ divides $n$. If this is not the case then there is a $\text{Perm}(B)$-invariant splitting

$$F^B = (F^B)^0 \oplus F \cdot 1_B.$$

Clearly, $F^B$ and $(F^B)^0$ carry natural structures of $G$-modules. Their characters depend only on the characteristic of $F$.

Let us consider the case of $F = Q$. Then the character of $Q^B$ is called the permutation character of $B$. Let us denote by $\chi = \chi_B : G \to Q$ the character of $(Q^B)^0$. Clearly, $1 + \chi$ is the permutation character of $B$.

Now, let us consider the case of $F = F_2$. If $n$ is even then let us define the $\text{Perm}(B)$-module

$$Q_B := (F^B_2)^0 / (F^B_2 \cdot 1_B).$$

If $n$ is odd then let us put

$$Q_B := (F^B_2)^0.$$

**Remark 3.2.** Clearly, $Q_B$ is a faithful $G$-module. If $n$ is odd then $\dim_{F_2}(Q_B) = n - 1$. If $n$ is even then $\dim_{F_2}(Q_B) = n - 2$.

Let $G^{(2)}$ be the set of 2-regular elements of $G$. Clearly, the Brauer character of the $G$-module $F^B$ coincides with the restriction of $1 + \chi_B$ to $G^{(2)}$. This implies easily that the Brauer character of the $G$-module $(F^B_2)^0$ coincides with the restriction of $\chi_B$ to $G^{(2)}$.

**Remark 3.3.** Let us denote by $\phi_B = \phi$ the Brauer character of the $G$-module $Q_B$. One may easily check that $\phi_B$ coincides with the restriction of $\chi_B$ to $G^{(2)}$ if $n$ is odd and with the restriction of $\chi_B - 1$ to $G^{(2)}$ if $n$ is even.

We refer to [15] for a discussion of the following definition.

**Definition 3.4.** Let $V$ be a vector space over a field $F$, let $G$ be a group and $\rho : G \to \text{Aut}_F(V)$ a linear representation of $G$ in $V$. We say that the $G$-module $V$ is very simple if it enjoys the following property:

If $R \subset \text{End}_F(V)$ is an $F$-subalgebra containing the identity operator $\text{Id}$ such that

$$\rho(\sigma)R\rho(\sigma)^{-1} \subset R \quad \forall \sigma \in G$$

then either $R = F \cdot \text{Id}$ or $R = \text{End}_F(V)$.

**Remarks 3.5.**

(i) If $G'$ is a subgroup of $G$ and the $G'$-module $V$ is very simple then obviously the $G$-module $V$ is also very simple.

(ii) A very simple module is absolutely simple (see [15], Remark 2.2(ii)).

(iii) If $\dim_F(V) = 1$ then obviously the $G$-module $V$ is very simple.
(iv) Assume that the $G$-module $V$ is very simple and $\dim_F(V) > 1$. Then $V$ is not induced from a subgroup $G$ (except $G$ itself) and is not isomorphic to a tensor product of two $G$-modules, whose $F$-dimension is strictly less than $\dim_F(V)$ (see [15], Examples 7.1).

(v) If $F = F_2$ and $G$ is perfect then properties (ii)-(iv) characterize the very simple $G$-modules (see [14], Th. 7.7).

The following statement provides a criterion of very simplicity over $F_2$.

**Theorem 3.6.** Suppose a positive integer $N > 1$ and a group $H$ enjoy the following properties:

- $H$ does not contain a subgroup of index dividing $N$ except $H$ itself.
- Let $N = ab$ be a factorization of $N$ into a product of two positive integers $a > 1$ and $b > 1$. Then either there does not exist an absolutely simple $F_2[H]$-module of $F_2$-dimension $a$ or there does not exist an absolutely simple $F_2[H]$-module of $F_2$-dimension $b$.

Then each absolutely simple $F_2[H]$-module of $F_2$-dimension $N$ is very simple.

**Proof.** This is Corollary 4.12 of [15].

**Theorem 3.7.** Suppose that there exist a positive integer $m > 2$ and an odd power prime $q$ such that $n = q^m - 1$. Suppose $G$ is a subgroup of $S_n$. Suppose $G$ contains a subgroup isomorphic to $L_m(q)$. Then the $G$-module $Q_B$ is very simple.

The rest of this section is devoted to the proof of Theorem 3.7. In light of Remark 3.5, we may assume that $G = L_m(q)$.

"Generic" case. Assume that $(m, q) \neq (4, 3)$. Then it follows from Theorem 1.1 (applied to $p = 2$) and the Table III of [3] that each nontrivial (absolutely) irreducible representation of $L_m(q)$ in characteristic 2 has dimension which is greater or equal than $N := \dim_{F_2}(Q_B)$. Taking into account that $L_m(q)$ is (simple) not solvable and $Q_B$ is a faithful $L_m(q)$-module, we conclude that $Q_B$ is absolutely simple.

Now we claim that the group $G = L_m(q)$ does not contain a subgroup of index dividing $N := \dim_{F_2}(Q_B)$ except $G$ itself.

Indeed, if $G'$ is a subgroup of $G$ such that $G' \neq G$ and $[G : G']$ divides $\dim_{F_2}(Q_B)$ then the simple group $G$ acts faithfully on $B' = G/G'$ and therefore $[G : G'] \geq 5$. In particular, we get a faithful $G$-module $Q_{B'}$, whose dimension is strictly less than $\dim_{F_2}(Q_B)$.

Since each strict divisor $a$ of $N$ lies strictly between 1 and $N$, there does not exist an absolutely simple $F_2[G]$-module of $F_2$-dimension $a$.

Now the very simplicity of the $G$-module $Q_B$ follows from Theorem 3.6.

**The special case of** $m = 4, q = 3$. We have $n = \#(B) = 40$ and $\dim_{F_2}(Q_B) = 38$. According to the Atlas ([4], pp. 68-69), $G = L_4(3)$ has two conjugacy classes of maximal subgroups of index 40. All other maximal subgroups have index greater than 40. Therefore all subgroups of $G$ (except $G$ itself) have index greater than $39 > 38$. This implies that each action of $G$ on $B$ is transitive. The permutation character (in notations of [2]) is (in both cases) $1 + \chi_4$, i.e., $\chi = \chi_4$. Since 40 is even, we need to consider the restriction of $\chi - 1$ to the set of 2-regular elements of $G$ and this restriction coincides with the absolutely irreducible Brauer character $\phi_4$ (in notations of [3], p. 165). In particular, the corresponding $G$-module $Q_B$ is
Proof. This is Corollary 5.3 of [15].

4. Proof of Theorems 2.1 and 2.4

Recall that \( \text{Gal}(f) \subset \text{Perm}(\mathfrak{R}) \). In addition, it is known that the natural homomorphism \( \text{Gal}(K) \rightarrow \text{Aut}_{\mathbb{F}_2}(J(C)_2) \) factors through the canonical surjection \( \text{Gal}(K) \rightarrow \text{Gal}(K(\mathfrak{R})/K) = \text{Gal}(f) \) and the \( \text{Gal}(f) \)-modules \( J(C)_2 \) and \( Q_{\mathfrak{R}} \) are isomorphic (see, for instance, Th. 5.1 of [13]). In particular, if the \( \text{Gal}(f) \)-module \( Q_{\mathfrak{R}} \) is very simple then the \( \text{Gal}(f) \)-modules \( J(C)_2 \) is also very simple and therefore is absolutely simple.

**Lemma 4.1.** If the \( \text{Gal}(f) \)-module \( Q_{\mathfrak{R}} \) is very simple then either \( \text{End}(J(C)_f) = \mathbb{Z} \) or \( \text{char}(K) > 0 \) and \( J(C)_f \) is a supersingular abelian variety.

**Proof.** This is Corollary 5.3 of [15].

It follows from Theorem 3.7 that under the assumptions of Theorem 2.1, the \( \text{Gal}(f) \)-module \( Q_{\mathfrak{R}} \) is very simple. Applying Lemma 4.1, we conclude that either \( \text{End}(J(C)_f) = \mathbb{Z} \) or \( \text{char}(K) > 0 \) and \( J(C)_f \) is a supersingular abelian variety.

If \( n = 12 \) and \( \text{Gal}(f) \cong M_{12} \) then the \( \text{Gal}(f) \)-module \( Q_{B} \) is also very simple (13, Th. 7.12(ii)). Again we conclude that under the assumptions of Theorem 2.4 either \( \text{End}(J(C)_f) = \mathbb{Z} \) or \( \text{char}(K) > 0 \) and \( J(C)_f \) is a supersingular abelian variety (13, Th. 7.13(ii)).

In order to finish the proof of Theorem 2.1 we need only to check that \( J(C)_f \) is not supersingular if \( m \) is even. Similarly, in order to prove Theorem 2.4 we need only to check that if \( (n, \text{Gal}(f)) = (12, M_{12}) \) then \( J(C)_f \) is not supersingular. Using Remarks 2.3 and 2.5 we may assume that either \( \text{Gal}(f) = L_m(q) \) or \( (n, \text{Gal}(f)) = (12, M_{12}) \) and in both cases \( K \) contains all 2-power roots of unity. Clearly, the desired assertions are immediate corollaries of the following statement.

**Lemma 4.2.** Suppose an even positive integer \( n \) and a finite simple non-abelian group \( G \) enjoy one of the following two properties.

(i) There exist an odd power prime \( q \) and an even integer \( m \geq 4 \) such that \( n = (q^m - 1)/(q - 1) \) and \( G \cong L_m(q) \);

(ii) \( n = 12 \) and \( G \cong M_{12} \).

Let us put \( g = (n - 2)/2 \). Suppose \( F \) is a field, whose characteristic is not 2. Suppose that \( F \) contains all 2-power roots of unity. Suppose that \( X \) is a 2-dimensional abelian variety over \( F \) such that the image of \( \text{Gal}(F) \) in \( \text{Aut}(X_2) \) is isomorphic to \( G \) and the \( G \)-module \( X_2 \) is absolutely simple. Then \( X \) is not supersingular.

**Proof of Lemma 4.2.** Every nontrivial representation of \( G \) in characteristic 2 has dimension \( > g \). Indeed, first assume that \( G = L_m(q) \). Then in the “generic” case of \( (m, q) \neq (4, 3) \) such a representation must have dimension \( \geq 2g > g \), thanks to the already cited Th. 1.1 and Table III of [3]. If \( (m, q) = (4, 3) \) then \( n = 40, 2q = 38 \) and the smallest dimension is \( 26 > 19 = g \), according to the Tables in [1]. Second, if \( G = M_{12} \) then this assertion follows from Th. 8.1 on p. 80 in [3]; see also the Tables in [3].
Proposition 4.3. Suppose $G' \rightarrow G$ is a central extension of $G$. In addition, assume that either $G' = G$ or $G'$ is a double cover of $G$, i.e., $\ker(G' \rightarrow G)$ is a central cyclic subgroup of order 2 in $G'$. Suppose $V$ is a finite-dimensional $\mathbb{Q}_2$-vector space and

$$\rho : G' \rightarrow \text{Aut}_{\mathbb{Q}_2}(V)$$

is an absolutely irreducible faithful representation of $G'$ over $\mathbb{Q}_2$. Then

$$\dim_{\mathbb{Q}_2}(V) \neq 2g.$$

Proof of Proposition 4.3. Clearly, $\rho$ defines an absolutely irreducible projective representation of $G$ in $V$ over $\mathbb{Q}_2$.

Assume first that $G = \text{L}_{m}(q)$. Then in the “generic” case every absolutely irreducible nontrivial projective representation of $G$ in characteristic 0 must have dimension $\geq 2g + 1 > 2g$ (see [3], Table II). If $(m, q) = (4, 3)$ then the Proposition follows from the Tables in [2].

Second, suppose $G = \text{M}_{12}$. Then $n = 12, 2g = 10$. All faithful absolutely irreducible representations of $\text{M}_{12}$ in characteristic zero have dimension $\geq 11 > 10$ ([2], p. 33). This proves the Proposition in the case when $G' = G = \text{M}_{12}$ and also when $G'$ is a trivial double cover, i.e., is isomorphic to a product of $\text{M}_{12}$ and a cyclic group of order 2. If $G'$ is a nontrivial double cover of $\text{M}_{12}$ then it has precisely two non-isomorphic 10-dimensional absolutely irreducible representations in characteristic 0 (up to an isomorphism) [4]. However, none of them is defined over $\mathbb{Q}_2$. Indeed, each character of $G'$ of degree 10 takes on a value, whose square is $-2$ ([4], Table 1 on p. 410; [2], p. 33).

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

$$\rho_{2, X} : \text{Gal}(F) \rightarrow \text{Aut}_{\mathbb{Z}_2}(T_2(X))$$

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

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

(as 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 the (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

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

whose kernel consists of elements of $1 + 2\text{End}_{\mathbb{Z}_2}(T_2(X))$. We have assumed that the $G$-module $X_2$ is absolutely simple. This implies that the $H$-module $X_2$ is also absolutely simple. Here the structure of $H$-module is defined on $X_2$ via

$$H \subset \text{Aut}_{\mathbb{Z}_2}(T_2(X)) \rightarrow \text{Aut}(X_2).$$
The absolute simplicity of the $H$-module $X_2$ means that the natural homomorphism

$$F_2[H] \to \text{End}_{F_2}(X_2)$$

is surjective. By Nakayama’s Lemma, this implies that the natural homomorphism

$$Z_2[H] \to \text{End}_{Z_2}(T_2(X))$$

is also surjective (see [10], p. 252).

Let $V_2(X) = T_2(X) \otimes_{Z_2} Q_2$ be the $Q_2$-Tate module of $X$. It is well-known that $V_2(X)$ is the $2g$-dimensional $Q_2$-vector space and $T_2(X)$ is a $Z_2$-lattice in $V_2(X)$. Clearly, the $Q_2[H]$-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) [11]

$$e : V_2(X) \times V_2(X) \to Q_2(1) \cong Q_2.$$

Since $F$ contains all 2-power roots of unity, $e$ is $\text{Gal}(F)$-invariant and therefore is $H$-invariant. This means that $H$ is a subgroup of the corresponding symplectic group $\text{Sp}(V_2(X), e)$. We have

$$H \subset \text{Sp}(V_2(X), e) \cong \text{Sp}_{2g}(Q_2) \subset \text{Sp}_{2g}(Q_2).$$

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 $Q$-algebra $\text{End}(X) \otimes Q$ of endomorphisms of $X$. Since $X$ is supersingular,

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

Recall ([11]) that the natural map

$$\text{End}^0(X) \otimes_Q Q_2 \to \text{End}_{Q_2}V_2(X)$$

is an embedding. Dimension arguments imply that

$$\text{End}^0(X) \otimes_Q Q_2 = \text{End}_{Q_2}V_2(X).$$

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

$$\rho_{2,X}(\text{Gal}(L)) \subset \rho_{2,X}(\text{Gal}(F)) \subset \text{Aut}_{Z_2}(T_2(X)) \subset \text{Aut}_{Q_2}(V_2(X))$$

commutes with $\text{End}^0(X)$. This implies that $\rho_{2,X}(\text{Gal}(L))$ commutes with $\text{End}_{Q_2}V_2(X)$ and therefore consists of scalars. Since

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

$\rho_{2,X}(\text{Gal}(L))$ 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

$$\text{Aut}_{Q_2}T_2(X) \supset H \to G \subset \text{Aut}(X_2)$$

consists of elements of finite order and, thanks to the Minkowski-Serre Lemma, $Z := \ker(H \to G)$ has exponent 1 or 2. In particular, $Z$ is commutative. We have

$$Z \subset H \subset \text{Sp}(V_2(X), e) \cong \text{Sp}_{2g}(Q_2) \subset \text{Sp}_{2g}(Q_2).$$

Since $Z$ consists of semisimple elements and rank of $\text{Sp}_{2g}$ is $g$, the group $Z$ is isomorphic (“conjugate”) to a multiplicative subgroup of $(Q_2^2)^g$. Since the exponent of $Z$ is either 1 or 2, the group $Z$ is isomorphic to a multiplicative subgroup of $\{1, -1\}^g$. Hence $Z$ is an $F_2$-vector space of dimension $d \leq g$. This implies that the adjoint action

$$H \to H/Z = G \to \text{Aut}(Z) \cong \text{GL}_d(F_2)$$
is trivial, since every nontrivial representation of $G$ in characteristic 2 must have dimension strictly greater than $g \geq d$. This means that $Z$ lies in the center of $H$. Since the $\mathbb{Q}_2[H]$-module $V_2(X)$ is faithful and absolutely simple, $Z$ consists of scalars. This implies that either $Z = \{1\}$ or $Z = \{\pm 1\}$. In other words, either $H \cong G$ or $H \to G$ is a double cover. In both cases $V_2(X)$ is an absolutely irreducible representation of $H$ of dimension $2g$ over $\mathbb{Q}_2$. But by Proposition 4.3 applied to $G' = H$ and $V = V_2(X)$,

$$\dim_{\mathbb{Q}_2}(V_2(X)) \neq 2g.$$  

This gives us the desired contradiction. This ends the proof of Lemma 4.2 and therefore of Theorems 2.1 and 2.4.

Example 4.4. Suppose $p$ is an odd prime, $q > 1$ is a power of $p$, $m > 2$ is an even integer. Let us put $n = (q^m - 1)/(q - 1)$. Suppose $k$ is an algebraically closed field of characteristic $p$ and $K = k(z)$ is the field of rational functions. The Galois group of $x^m + z x + 1$ over $K$ is $L_m(q)$ and the Galois group of $x^m + x + z$ over $K$ is $\text{PGL}_m(\mathbb{F}_q)$ ([1], p. 1643). Therefore the jacobians of the hyperelliptic curves $y^2 = x^m + z x + 1$ and $y^2 = x^m + x + z$ have no nontrivial endomorphisms over an algebraic closure of $K$.

References

[1] S. S. Abhyankar, Projective polynomials. Proc. AMS 125 (1997), 1643–1650.
[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] R. M. Guralnick, Pham Huu Tiep, Low-dimensional representations of special linear groups in cross characteristic. Proc. London Math. Soc. 78 (1999), 116–138.
[4] J. F. Humphreys, The projective characters of the Mathieu group $M_{12}$ and of its automorphism group. Math. Proc. Camb. Phil. Soc. 87 (1980), 401–412.
[5] G. D. James, The modular characters of the Mathieu groups. J. Algebra 27 (1973), 57–111.
[6] Ch. Jansen, K. Lux, R. Parker, R. Wilson, An Atlas of Brauer characters. Clarendon Press, Oxford, 1995.
[7] N. Katz, Monodromy of families of curves: applications of some results of Davenport-Lewis. In: Séminaire de Théorie des Nombres, Paris 1979-80 (ed. M.-J. Bertin); Progress in Math. 12, pp. 171–195, Birkhäuser, Boston-Basel-Stuttgart, 1981.
[8] N. Katz, Affine cohomological transforms, perversity, and monodromy. J. Amer. Math. Soc. 6 (1993), 149–222.
[9] D. Masser, Specialization of some hyperelliptic jacobians. In: Number Theory in Progress (eds. K. Györy, H. Iwaniec, J. Urbanowicz), vol. 1, pp. 293–307; de Gruyter, Berlin-New York, 1999.
[10] B. Mazur, Deformation theory of Galois representations. In: Modular forms and Fermat’s last theorem (G. Cornell, J. H. Silverman, G. Stevens, eds.), pp. 243–311, Springer-Verlag, New York, 1997.
[11] D. Mumford, Abelian varieties, Second edition, Oxford University Press, London, 1974.
[12] Sh. Mori, The endomorphism rings of some abelian varieties. Japanese J. Math, 2(1976), 109–130.
[13] Sh. Mori, The endomorphism rings of some abelian varieties. II, Japanese J. Math, 3(1977), 105–109.
[14] Yu. G. Zarhin, Hyperelliptic jacobians without complex multiplication. Math. Res. Letters 7(2000), 123–132.
[15] Yu. G. Zarhin, Hyperelliptic jacobians and modular representations, http://xxx.lanl.gov/abs/math.AG/0003002. to appear in Texel volume “Moduli of abelian varieties” (eds. G. van der Geer, C. Faber, F. Oort), Birkhäuser.
DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA 16802, USA

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