Mathematical Research Letters **7**, 123–132 (2000)

HYPERELLIPTIC JACOBIANS WITHOUT COMPLEX MULTIPLICATION

Yuri G. Zarhin

1. Introduction

The aim of this note is to prove 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 of the ground field K if the Galois group $\mathrm{Gal}(f)$ of the polynomial $f \in K[x]$ is "very big".

More precisely, if f is a polynomial of degree $n \geq 5$ and $\mathrm{Gal}(f)$ is either the symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$ then $\mathrm{End}(J(C)) = \mathbb{Z}$. Notice that it easily follows that the ring of K-endomorphisms of $J(C)$ coincides with $\mathbb{Z}$ and the real problem is how to prove that every endomorphism of $J(C)$ is defined over K.

There are some results of this type in the literature. Previously Mori [8], [9] has constructed explicit examples (in all characteristics) of hyperelliptic jacobians without nontrivial endomorphisms. In particular, he provided examples over $\mathbb{Q}$ with semistable C_f and big (doubly transitive) $\mathrm{Gal}(f)$ [9]. The semistability of C_f implies the semistability of $J(C_f)$ and, thanks to a theorem of Ribet [14], all endomorphisms of $J(C_f)$ are defined over $\mathbb{Q}$. (Applying to $C_f/\mathbb{Q}$ the Shafarevich conjecture [17] (proven by Fontaine [3] and independently by Abrashkin [1], [2]) and using Lemma 4.4.3 and arguments on p. 42 of [16], one may prove that the Galois group $\mathrm{Gal}(f)$ of the polynomial f involved is $\mathbf{S}_{2g+1}$ where $\deg(f) = 2g + 1$.)

André ([7], pp. 294-295) observed that results of Katz ([5], [6]) give rise to examples of hyperelliptic jacobians $J(C_f)$ over the field of rational function $\mathbb{C}(z)$ with $\mathrm{End}(J(C_f)) = \mathbb{Z}$. Namely, one may take $f(x) = h(x) - z$ where $h(x) \in \mathbb{C}[x]$ is a *Morse function*. In particular, this explains Mori's example [8]

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

over $\mathbb{C}(z)$.

Notice that if h is a *Morse polynomial* of degree n then the Galois group of $h(x) - z$ over $\mathbb{C}(z)$ is the symmetric group $\mathbf{S}_n$ ([16], Th. 4.4.5, p. 41).

Received September 17, 1999.

Masser [7] constructed a completely different class of hyperelliptic jacobians $J(C_f)$ over $\mathbb{C}(z)$ with $\mathrm{End}(J(C_f)) = \mathbb{Z}$. In his examples f splits into a product of linear factors over $\mathbb{C}(z)$ as follows.

$$f(x) = x(x - z^{\alpha(1)})(x - z^{\beta(1)}) \cdots (x - z^{\alpha(g)})(x - z^{\beta(g)}),$$

where

$$0 \le \alpha(1) < \beta(1) < \cdots < \alpha(g) < \beta(g),$$

and the differences $\alpha(1) - \beta(1), \dots, \alpha(g) - \beta(g)$ are distinct. Masser's proof is purely analytic in character.

This paper was written during my stay in Glasgow. I would like to thank the Department of Mathematics of University of Glasgow for its hospitality.

2. Main result

Throughout this paper we assume that K is a field of characteristic 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 $\mathrm{char}(K) \neq 2$, K_a its algebraic closure, $f(x) \in K[x]$ an irreducible separable polynomial of degree $n \ge 5$ such that the Galois group of f is either $\mathbf{S}_n$ or $\mathbf{A}_n$. Let C_f be the hyperelliptic curve $y^2 = f(x)$. Let $J(C_f)$ be its jacobian, $\mathrm{End}(J(C_f))$ the ring of K_a-endomorphisms of $J(C_f)$. Then either $\mathrm{End}(J(C_f)) = \mathbb{Z}$ or $\mathrm{char}(K) > 0$ and $J(C_f)$ is a supersingular abelian variety.*

Examples 2.2.

1. The polynomial $x^n - x - 1$ has Galois group $\mathbf{S}_n$ over $\mathbb{Q}$ ([16], p. 42). Hence the jacobian of the curve $y^2 = x^n - x - 1$ has no nontrivial endomorphisms over $\bar{\mathbb{Q}}$ and therefore over $\mathbb{C}$ for all $n \ge 5$.
2. The Galois group of the "truncated exponential"

$$\exp_n(x) := 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \cdots + \frac{x^n}{n!} \in \mathbb{Q}[x],$$

is either $\mathbf{S}_n$ or $\mathbf{A}_n$ [15]. Hence the jacobian of the curve $y^2 = \exp_n(x)$ has no nontrivial endomorphisms over $\bar{\mathbb{Q}}$ and therefore over $\mathbb{C}$ for all $n \ge 5$.

Remark 2.3. Let $f(x) \in K[x]$ be an irreducible separable polynomial of even degree $n = 2m \ge 5$ such that the Galois group of f is either $\mathbf{S}_n$ or $\mathbf{A}_n$. Then $n \ge 6$. 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 odd degree $2m - 1 = n - 1 \ge 5$, whose Galois group is either $\mathbf{S}_{n-1}$ or $\mathbf{A}_{n-1}$ respectively. 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 odd degree $2m-1=n-1\ge 5$ with the same Galois group equal $\mathbf{S}_{n-1}$ or $\mathbf{A}_{n-1}$ respectively.

The standard substitution

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

establishes a birational isomorphism between C_f and a hyperelliptic curve

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

It follows readily that in order to prove Theorem 2.1 it suffices to do the case of *odd* n.

We deduce Theorem 2.1 from the following auxiliary statement.

Theorem 2.4. *Suppose $n=2g+1$ is an odd integer which is greater than or equal to 5. 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 a hyperelliptic curve $y^2=f(x)$ of genus g over K. Suppose $J(C)$ is the jacobian of C and $J(C)_2$ is the group of its points of order 2, viewed as a $2g$-dimensional $\mathbf{F}_2$-vector space provided with the natural action of* $\mathrm{Gal}(K)$.

Let R be a subalgebra of $\mathrm{End}_{\mathbf{F}_2}(J(C)_2)$ *which contains the identity operator* Id. *Assume that for each $u\in R, \sigma\in\mathrm{Gal}(K)$ the subalgebra R contains*

$$^{\sigma}u : x \mapsto \sigma u \sigma^{-1}(x), \quad x\in J(C)_2.$$

Either $R=\mathbf{F}_2\cdot\mathrm{Id}$ or $R=\mathrm{End}_{\mathbf{F}_2}(J(C)_2)$.

We prove Theorem 2.4 in Section 4. In the next section we deduce Theorem 2.1 from Theorem 2.4.

3. Proof of main result

So, we assume that $f(x)\in K[x]$ satisfies the conditions of Theorem 2.1. In light of Remark 2.3, we may assume that $n=2g+1$ is odd. Therefore $J(C)$ is a g-dimensional abelian variety defined over K.

Since $J(C)$ is defined over K, one may associate with every $u\in\mathrm{End}(J(C))$ and $\sigma\in\mathrm{Gal}(K)$ an endomorphism $^{\sigma}u\in\mathrm{End}(J(C))$ such that

$$^{\sigma}u(x) = \sigma u(\sigma^{-1}x) \quad \forall x\in J(C)(K_a).$$

Let us put

$$R := \mathrm{End}(J(C))\otimes\mathbb{Z}/2\mathbb{Z} \subset \mathrm{End}_{\mathbf{F}_2}(J(C)_2).$$

Clearly, R satisfies all the conditions of Theorem 2.4. This implies that either $R=\mathbf{F}_2\cdot\mathrm{Id}$, or $R=\mathrm{End}_{\mathbf{F}_2}(J(C)_2)$. If $\mathrm{End}(J(C))\otimes\mathbb{Z}/2\mathbb{Z}=R=\mathbf{F}_2\cdot\mathrm{Id}$, then the free abelian group $\mathrm{End}(J(C))$ has rank 1 and therefore coincides with $\mathbb{Z}$. If $\mathrm{End}(J(C))\otimes\mathbb{Z}/2\mathbb{Z}=R=\mathrm{End}_{\mathbf{F}_2}(J(C)_2)$, then the free abelian group $\mathrm{End}(J(C))$ has rank $(2\dim(J(C)))^2=(2g)^2$, and therefore the semisimple $\mathbb{Q}$-algebra $\mathrm{End}^0(J(C))=\mathrm{End}(J(C))\otimes\mathbb{Q}$ has dimension $(2g)^2$.

Now Theorem 2.1 becomes an immediate corollary of the following assertion.

Lemma 3.1. *Let X be an abelian variety of dimension g over an algebraically closed field F. Assume that the semisimple $\mathbb{Q}$-algebra $\mathrm{End}^0(X) = \mathrm{End}(X) \otimes \mathbb{Q}$ has dimension $(2g)^2$. Then $\mathrm{char}(F) > 0$ and X is supersingular.*

Proof. Let us fix a prime $\ell \neq \mathrm{char}(F)$ and consider the ℓ-adic Tate module $T_\ell(X)$ of X. Let $V_\ell(X) = T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ be the corresponding $\mathbb{Q}_\ell$-vector space of dimension $2g$. There is a canonical embedding

$$\mathrm{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X)),$$

and dimension arguments imply that this embedding is an isomorphism. In particular, $\mathrm{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is isomorphic to the matrix algebra of size $2g$ over $\mathbb{Q}_\ell$. Since the center of the matrix algebra over $\mathbb{Q}_\ell$ has dimension 1 over $\mathbb{Q}_\ell$, the center of $\mathrm{End}^0(X)$ has dimension 1 over $\mathbb{Q}$ and therefore coincides with $\mathbb{Q}$. This implies that $\mathrm{End}^0(X)$ is a central simple $\mathbb{Q}$-algebra of dimension $(2g)^2$. Hence, there exists a *simple* abelian variety Y over F and a positive integer r such that X is isogenous to Y^r over F. This implies that

$$g = \dim(X) = r\dim(Y),$$

$\mathrm{End}^0(Y)$ is a division algebra over $\mathbb{Q}$ and $\mathrm{End}^0(X)$ is isomorphic to the matrix algebra of size r over $\mathrm{End}^0(Y)$. In particular,

$$\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) = r^2\dim_{\mathbb{Q}}(\mathrm{End}^0(Y)).$$

Since the center of $\mathrm{End}^0(X)$ coincides with $\mathbb{Q}$, the center of $\mathrm{End}^0(Y)$ also coincides with $\mathbb{Q}$. It follows from Albert's classification ([11], Sect. 21) that either $\mathrm{End}^0(Y) = \mathbb{Q}$ or $\mathrm{End}^0(Y)$ is a quaternion algebra over $\mathbb{Q}$.

If $\mathrm{End}^0(Y) = \mathbb{Q}$ then $\mathrm{End}^0(X)$ has dimension $r^2 \le (r\dim(Y))^2 = g^2 < (2g)^2$. This implies that $\mathrm{End}^0(Y)$ is a quaternion $\mathbb{Q}$-algebra and therefore

$$\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) = r^2\dim_{\mathbb{Q}}(\mathrm{End}^0(Y)) = 4r^2 = (2r)^2.$$

On the other hand, $\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) = (2g)^2$. This implies that $2r = 2g$, i.e., $r = g = \dim(X)$ and Y is an elliptic curve. Since $\mathrm{End}^0(Y)$ is the quaternion algebra, Y is a supersingular elliptic curve and $\mathrm{char}(F) > 0$. Since X is isogenous to Y^r, it is a supersingular abelian variety. □

4. Points of order 2 on hyperelliptic jacobians

Let C be a hyperelliptic curve over K defined by an equation $y^2 = f(x)$ where $f(x) \in K[x]$ is a polynomial of odd degree n without multiple roots. The rational function $x \in K(C)$ defines a canonical double cover $\pi : C \to \mathbf{P}^1$. Let $B' \subset C(K_a)$ be the set of ramification points of π (Weierstraß points). Clearly, the restriction of π to B' is an injective map $\pi : B' \hookrightarrow \mathbf{P}^1(K_a)$, whose image is the disjoint union of ∞ and the set R_f of roots of f. By abuse of notation, we also denote by ∞ the ramification point lying above ∞. Clearly, $\infty \in C(K)$. We denote by B the complement of ∞ in B'. Clearly,

$$B = \{(\alpha, 0) \mid f(\alpha) = 0\} \subset C(K_a),$$

and π defines a bijection between B and R_f which commutes with the action of $\mathrm{Gal}(K)$.

We write Q_B for the $\mathbf{F}_2$-vector space of subsets of B of *even* cardinality with symmetric difference as a sum. There is a natural structure of $\mathrm{Gal}(K)$-module on Q_B.

Here is an explicit description of the group $J(C)_2$ of points of order 2 on the jacobian $J(C)$. Namely, let $T \subset B'$ be a subset of even cardinality. Then ([12], Ch. IIIa, Sect. 2, Lemma 2.4; [10], pp. 190–191; see also [9]) the divisor $e_T = \sum_{P \in T}(P) - \#(T)(\infty)$ on C has degree 0 and $2e_T$ is principal. If T_1, T_2 are two subsets of even cardinality in B' then the divisors e_{T_1} and e_{T_2} are linearly equivalent if and only if either $T_1 = T_2$ or $T_2 = B' \setminus T_1$. Also, if $T = T_1 \triangle T_2$ then the divisor e_T is linearly equivalent to $e_{T_1} + e_{T_2}$. Hereafter we use the symbol $\triangle$ for the symmetric difference of two sets. Counting arguments imply easily that each point of $J(C)_2$ is the class of e_T for some T. We know that such a choice is not unique. However, if we demand that T does not contain ∞ then such a choice always exists and unique. This observation leads to a canonical group isomorphism

$$Q_B \cong J(C)_2, \quad T \mapsto \mathrm{cl}(e_T).$$

Here cl stands for the linear equivalence class of a divisor. Clearly, this isomorphism commutes with natural actions of $\mathrm{Gal}(K)$. In other words, the $\mathrm{Gal}(K)$-modules Q_B and $J(C)_2$ are canonically isomorphic.

One may describe explicitly the Galois action on Q_B. In order to do that let us consider the splitting field $L \subset K_a$ of f and let $G = \mathrm{Gal}(L/K)$ be its Galois group. Clearly, G may be viewed as a group of permutations of R_f and therefore (via π) as a subgroup in the group $\mathrm{Perm}(B)$ of permutations of B. This induces obvious embeddings

$$G \subset \mathrm{Perm}(B) \subset \mathrm{Aut}(Q_B),$$

and $\mathrm{Gal}(K)$ acts on Q_B via the composition of the canonical *surjection* $\mathrm{Gal}(K) \to \mathrm{Gal}(L/K) = G$ and the embedding

$$G \subset \mathrm{Perm}(B) \subset \mathrm{Aut}(Q_B).$$

Now one may easily check that Theorem 2.4 follows readily from the following purely group-theoretic statement.

Theorem 4.1. *Let B be a finite set of odd cardinality $n \ge 5$, Q_B the $\mathbf{F}_2$-vector space of its subsets of* even *cardinality with symmetric difference as a sum. Let $S = \mathrm{Perm}(B)$ be the group of permutation of B viewed as a subgroup of $\mathrm{Aut}(Q_B)$. Let G be a subgroup of S which is isomorphic either to $\mathbf{S}_n$ or to $\mathbf{A}_n$.*

Let R be a subalgebra of $\mathrm{End}_{\mathbf{F}_2}(Q_B)$ which contains the identity operator Id. *Assume that*

$$uRu^{-1} \subset R \quad \forall u \in G \subset S \subset \mathrm{Aut}(Q_B).$$

Either $R = \mathbf{F}_2 \cdot \mathrm{Id}$ or $R = \mathrm{End}_{\mathbf{F}_2}(Q_B)$.

We prove Theorem 4.1 in the next Section.

5. Representation theory

We keep all the notations and assumptions of Theorem 4.1. Clearly, $S \cong \mathbf{S}_n$. We write A for the only subgroup in S of index 2. Clearly, A is normal and isomorphic to the alternating group $\mathbf{A}_n$. It is well-known that the group A is simple of order $n!/2$. Cardinality arguments imply easily that either $G = S$ or $G = A$.

We have

$$A \subset S \subset \mathrm{Aut}(Q_B), \quad \dim_{\mathbf{F}_2}(Q_B) = n - 1.$$

This provides Q_B with a natural structure of S-module defined as follows. Each element s of S sends a subset $T \in Q_B$ into $s(T) = \{s(b) \mid b \in T\}$.

Let us consider the n-dimensional $\mathbf{F}_2$-vector space $\mathbf{F}_2^B$ of all maps $\varphi : B \to \mathbf{F}_2$. The space $\mathbf{F}_2^B$ is provided with a natural action of S defined as follows. Each $s \in S$ sends a map $\varphi : B \to \mathbf{F}_2$ into $s\varphi : b \mapsto \varphi(s^{-1}(b))$.

It is well-known that one may view $\mathbf{F}_2^B$ as the $\mathbf{F}_2$-vector space of *all* subsets of B with symmetric difference as a sum. Namely, a subset T corresponds to its characteristic function $\chi_T : B \to \{0, 1\} = \mathbf{F}_2$ and a function $\varphi : B \to \mathbf{F}_2$ corresponds to its support $\mathrm{supp}(\varphi) = \{x \in B \mid \varphi(x) = 1\}$. Under this identification each $s \in S$ sends T into $s(T) = \{s(b) \mid b \in T\}$.

Clearly, Q_B is a hyperplane in $\mathbf{F}_2^B$ and the inclusion map $Q_B \subset \mathbf{F}_2^B$ is a homomorphism of the S-modules. In particular, Q_B is an S-stable hyperplane in $\mathbf{F}_2^B$.

Since $n = \#(B)$ is odd, the set B does not belong to Q_B. Clearly, $B \in \mathbf{F}_2^B$ is S-invariant. Let L be the one-dimensional subspace of $\mathbf{F}_2^B$ generated by B. Clearly, S acts trivially on L and there is an S-invariant splitting

$$\mathbf{F}_2^B = Q_B \oplus L,$$

which is also H-invariant for each subgroup $H \subset S$. It is also clear that $\mathrm{End}_H(L) = \mathrm{End}_{\mathbf{F}_2}(L) = \mathbf{F}_2$. This implies that $\dim_{\mathbf{F}_2}(\mathrm{End}_H(L)) = 1$. Obviously, $\dim_{\mathbf{F}_2}(\mathrm{End}_H(Q_B)) \geq 1$.

Lemma 5.1. *Suppose $H \subset S = \mathrm{Perm}(B)$ is a doubly transitive permutation group. Then $\mathrm{End}_H(Q_B) = \mathbf{F}_2$. In particular, if the H-module Q_B is semisimple then it is absolutely simple.*

Proof. In order to prove that $\mathrm{End}_H(Q_B) = \mathbf{F}_2$, it suffices to check that $\dim_{\mathbf{F}_2}(\mathrm{End}_H(Q_B)) \leq 1$.

The H-invariant splitting $\mathbf{F}_2^B = Q_B \oplus L$ implies that

$$\begin{aligned}\dim_{\mathbf{F}_2}(\mathrm{End}_H(\mathbf{F}_2^B)) &\geq \dim_{\mathbf{F}_2}(\mathrm{End}_H(Q_B)) + \dim_{\mathbf{F}_2}(\mathrm{End}_H(L)) \\ &= \dim_{\mathbf{F}_2}(\mathrm{End}_H(Q_B)) + 1.\end{aligned}$$

Since H acts doubly transitively on B, we have $\dim_{\mathbf{F}_2}(\mathrm{End}_H(\mathbf{F}_2^B)) = 2$ ([13], Lemma 7.1 on p. 52). This implies that $1 \geq \dim_{\mathbf{F}_2}(\mathrm{End}_H(Q_B))$ and therefore $\mathrm{End}_H(Q_B) = \mathbf{F}_2$.

Now assume that the H-module Q_B is semisimple. Since $\mathbf{F}_2 = \mathrm{End}_H(Q_B)$ is a field, Q_B is simple. Applying Th. 9.2 on p. 145 of [4], we conclude that the H-module Q_B is absolutely simple. □

Lemma 5.2. *The A-module Q_B is absolutely simple.*

Proof. Since $n \geq 5$, the group $A = \mathbf{A}_n$ is doubly transitive. Thanks to Lemma 5.1, it suffices to check that Q_B is simple. Let U be a non-zero A-stable subspace in Q_B. Let $T \in U$ be a non-empty subset of B with smallest possible cardinality. Since n is odd, $T \neq B$. If T consists of 2 elements then we are done, because A acts doubly transitively on B and each subset in B of even cardinality could be presented as a symmetric difference (disjoint union) of 2-element sets. So, assume that T consists of at least 4 elements. Pick elements $t \in T$ and $b \in B \setminus T$. Then there is an *even* permutation $s \in A$ such that $s(T) = T \setminus \{t\} \bigcup \{b\}$. Clearly, the symmetric difference $T \triangle s(T) \in U$ consists of two elements which contradicts the choice of T. This proves the simplicity of Q_B. □

Since G always contains A, Theorem 4.1 is an immediate corollary of the following statement.

Theorem 5.3. *Let R be a subalgebra of $\mathrm{End}_{\mathbf{F}_2}(Q_B)$ which contains the identity operator* Id. *Assume that*

$$uRu^{-1} \subset R \quad \forall u \in A \subset \mathrm{Aut}(Q_B).$$

Either $R = \mathbf{F}_2 \cdot \mathrm{Id}$ or $R = \mathrm{End}_{\mathbf{F}_2}(Q_B)$.

Recall (Lemma 5.2) that the A-module Q_B is absolutely simple. Also, A is not isomorphic to a subgroup of $\mathbf{S}_{n-1}$, because $\#(A) = \frac{n!}{2} > (n-1)! = \#(\mathbf{S}_{n-1})$. Now Theorem 5.3 becomes an immediate corollary of the following statement.

Theorem 5.4. *Let $H \subset \mathrm{Aut}(Q_B)$ be a non-abelian simple group. Suppose that the H-module Q_B is absolutely simple and H is not isomorphic to a subgroup of $\mathbf{S}_{n-1}$. Assume, in addition, that either $\#(H) > 2^{n-1}$ or $n = 2p+1$ where p is a prime.*

Let R be a subalgebra of $\mathrm{End}_{\mathbf{F}_2}(Q_B)$ which contains the identity operator Id. *Assume that*

$$uRu^{-1} \subset R \quad \forall u \in H \subset \mathrm{Aut}(Q_B).$$

Either $R = \mathbf{F}_2 \cdot \mathrm{Id}$ or $R = \mathrm{End}_{\mathbf{F}_2}(Q_B)$.

Proof of Theorem 5.4. Clearly, Q_B is a faithful R-module and

$$uRu^{-1} = R \quad \forall u \in H \subset \mathrm{Aut}(Q_B).$$

Step 1. Q_B is a *semisimple* R-module. Indeed, let $U \subset Q_B$ be a simple R-submodule. Then $U' = \sum_{s \in H} sU$ is a non-zero H-stable subspace in Q_B and therefore must coincide with Q_B. On the other hand, each sU is also a R-submodule in Q_B, because $s^{-1}Rs = R$. In addition, if $W \subset sU$ is an R-submodule then $s^{-1}W$ is an R-submodule in U, because

$$Rs^{-1}W = s^{-1}sRs^{-1}W = s^{-1}RW = s^{-1}W.$$

Since U is simple, $s^{-1}W = \{0\}$ or U. This implies that sU is also simple. Hence $Q_B = U'$ is a sum of simple R-modules and therefore is a semisimple R-module.

Step 2. The R-module Q_B is *isotypic*. Indeed, let us split the semisimple R-module Q_B into the direct sum

$$Q_B = V_1 \oplus \cdots \oplus V_r,$$

of its isotypic components. Dimension arguments imply that $r \le \dim(Q_B) = n-1$. It follows easily from the arguments of the previous step that for each isotypic component V_i its image sV_i is an isotypic R-submodule for each $s \in H$ and therefore is contained in some V_j. Similarly, $s^{-1}V_j$ is an isotypic submodule obviously containing V_i. Since V_i is the isotypic component, $s^{-1}V_j = V_i$ and therefore $sV_i = V_j$. This means that s permutes the V_i; since Q_B is H-simple, H permutes them transitively. This gives rise to the homomorphism $H \to \mathbf{S}_r$ which must be either injective or trivial, since H is simple. If the homomorphism is injective then H is isomorphic to a subgroup of $\mathbf{S}_r$ and therefore to a subgroup of $\mathbf{S}_{n-1}$, because $r \le n-1$. This gives us a contradiction and therefore the homomorphism $H \to \mathbf{S}_r$ is trivial.

This means that $sV_i = V_i$ for all $s \in H$ and $Q_B = V_i$ is isotypic.

Step 3. Since Q_B is isotypic, there exist a simple R-module W and a positive integer d such that $Q_B \cong W^d$. We have

$$d \cdot \dim(W) = \dim(Q_B) = n-1.$$

Clearly, $\mathrm{End}_R(Q_B)$ is isomorphic to the matrix algebra $\mathrm{Mat}_d(\mathrm{End}_R(W))$ of size d over $\mathrm{End}_R(W)$.

Let us put

$$k = \mathrm{End}_R(W).$$

Since W is simple, k is a finite division algebra of characteristic 2. Therefore k is a finite field of characteristic 2. We have $\mathrm{End}_R(Q_B) \cong \mathrm{Mat}_d(k)$. Clearly, $\mathrm{End}_R(Q_B) \subset \mathrm{End}_{\mathbf{F}_2}(Q_B)$ is stable under the adjoint action of H. This induces a homomorphism

$$\alpha : H \to \mathrm{Aut}(\mathrm{End}_R(Q_B)) = \mathrm{Aut}(\mathrm{Mat}_d(k)).$$

Since k is the center of $\mathrm{Mat}_d(k)$, it is stable under the action of H, i.e., we get a homomorphism $H \to \mathrm{Aut}(k)$, which must be trivial, since H is a simple group and $\mathrm{Aut}(k) = \mathrm{Gal}(k/\mathbf{F}_2)$ is abelian. This implies that the center k of $\mathrm{End}_R(Q_B)$ commutes with H. Since $\mathrm{End}_H(Q_B) = \mathbf{F}_2$, we have $k = \mathbf{F}_2$. This implies that $\mathrm{End}_R(Q_B) \cong \mathrm{Mat}_d(\mathbf{F}_2)$ and

$$\alpha : H \to \mathrm{Aut}(\mathrm{Mat}_d(\mathbf{F}_2)) = \mathrm{GL}(d, \mathbf{F}_2)/\mathbf{F}_2^* = \mathrm{GL}(d, \mathbf{F}_2),$$

is trivial if and only if $\mathrm{End}_R(Q_B) \subset \mathrm{End}_H(Q_B) = \mathbf{F}_2 \cdot \mathrm{Id}$. Since $\mathrm{End}_R(Q_B) \cong \mathrm{Mat}_d(\mathbf{F}_2)$, α is trivial if and only if $d = 1$, i.e., Q_B is an absolutely simple R-module. It follows from the Jacobson density theorem that $R \cong \mathrm{Mat}_m(\mathbf{F}_2)$ with $dm = n-1$. This implies that α is trivial if and only if $R \cong \mathrm{Mat}_{n-1}(\mathbf{F}_2)$, i.e., $R = \mathrm{End}_{\mathbf{F}_2}(Q_B)$.

The adjoint action of H on R gives rise to a homomorphism

$$\beta : H \to \mathrm{Aut}(\mathrm{Mat}_m(\mathbf{F}_2)) = \mathrm{GL}(m, \mathbf{F}_2).$$

Clearly, β is trivial if and only if R commutes with H, i.e., $R = \mathbf{F}_2 \cdot \mathrm{Id}$.

Step 4. It follows from the previous step that we are done if either α or β is trivial. Clearly, we are done if either $m = 1$ or $d = 1$. So, further we assume that $m > 1$, $d > 1$. Notice also that $\mathrm{GL}(2, \mathbf{F}_2) \cong \mathbf{S}_3$ is solvable and therefore every homomorphism from the simple group H to $\mathrm{GL}(2, \mathbf{F}_2)$ is trivial. This implies that we are done if either $m = 2$ or $d = 2$. But when $n = 2p + 1$ with prime p we have $2p = n - 1 = md$ and one of the factors m and d must be equal to 2. This proves Theorem 5.4 in the case of $n = 2p + 1$.

Since $md = n - 1$, either $m \le \sqrt{n-1}$ or $d \le \sqrt{n-1}$. This implies that either $\#(\mathrm{GL}(m, \mathbf{F}_2)) < 2^{n-1}$ or $\#(\mathrm{GL}(d, \mathbf{F}_2)) < 2^{n-1}$ respectively. Taking into account the simplicity of H, we conclude that if $\#(H) > 2^{n-1}$ then either every homomorphism from H to $\mathrm{GL}(m, \mathbf{F}_2)$ is trivial or every homomorphism from H to $\mathrm{GL}(d, \mathbf{F}_2)$ is trivial. This proves Theorem 5.4 in the case when $\#(H) > 2^{n-1}$. □

References

[1] V.A. Abrashkin, *Group schemes of period p over the ring of Witt vectors*, Dokl. Akad. Nauk SSSR **283** (1985), 1289–1294; Soviet Math. Dokl. **32** (1985), 310–315.

[2] ———, *Honda systems of group schemes of period p*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), 451–484; Math. USSR Izv. **30** (1988), 419–453.

[3] J.-M. Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbb{Z}$, Invent. Math. **81** (1985), 515–538.

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

[5] N. Katz, *Monodromy of families of curves: applications of some results of Davenport-Lewis*, Séminaire de Théorie des Nombres, Paris 1979-80 (ed. M.-J. Bertin), pp. 171–195, Progr. Math., 12, Birkhäuser, Boston-Basel-Stuttgart, 1981.

[6] ———, *Affine cohomological transforms, perversity, and monodromy*, J. Amer. Math. Soc. **6** (1993), 149–222.

[7] D. Masser, *Specialization of some hyperelliptic jacobians*, Number Theory in Progress (eds. K. Győry, H. Iwaniec, J. Urbanowicz), vol. I, pp. 293–307, de Gruyter, Berlin-New York, 1999.

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

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

[10] D. Mumford, *Theta characteristics of an algebraic curve*, Ann. Sci. École Norm. Sup. (4) **4** (1971), 181–192.

[11] ———, *Abelian varieties*, Second edition, Oxford University Press, London, 1974.

[12] ———, *Tata Lectures on Theta. II*, Progress in Mathematics, 43, Birkhäuser, Boston-Basel-Stuttgart, 1984.

[13] D. Passman, *Permutation groups*, W.A. Benjamin, Inc., New York-Amsterdam, 1968.

[14] K. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*. Ann. of Math. (2) **101** (1977), 555–562.

[15] I. Schur, *Gleichungen ohne Affect*, Sitz. Preuss. Akad. Wiss. 1930, Physik-Math. Klasse 443–449 (= Ges. Abh. III, 191–197).

[16] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett Publishers, Boston-London, 1992.

[17] I.R. Shafarevich, *Algebraic number fields*, Proc. Internat. Congr. Math. (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 163–176, Amer. Math. Soc. Transl. (2) **31** (1963), 25–39.

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

Institute for Mathematical Problems in Biology, Russian Academy of Sciences, Pushchino, Moscow Region, 142292, RUSSIA

Department of Mathematics, University of Glasgow, 15 University Gardens, Glasgow G12 8QW, Scotland, UK

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