PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 131, Number 1, Pages 95–102
S 0002-9939(02)06689-3
Article electronically published on May 22, 2002

HYPERELLIPTIC JACOBIANS AND SIMPLE GROUPS $\mathbf{U}_3(2^m)$

YURI G. ZARHIN

(Communicated by David E. Rohrlich)

ABSTRACT. In a previous paper, the author proved that in characteristic zero the jacobian $J(C)$ of a hyperelliptic curve $C : y^2 = f(x)$ has only trivial endomorphisms over an algebraic closure K_a of the ground field K if the Galois group $\mathrm{Gal}(f)$ of the irreducible polynomial $f(x) \in K[x]$ is either the symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$. Here $n > 4$ is the degree of f. In another paper by the author this result was extended to the case of certain "smaller" Galois groups. In particular, the infinite series $n = 2^r + 1, \mathrm{Gal}(f) = \mathbf{L}_2(2^r) := \mathrm{PSL}_2(\mathbf{F}_{2^r})$ and $n = 2^{4r+2} + 1, \mathrm{Gal}(f) = \mathbf{Sz}(2^{2r+1})$ were treated. In this paper the case of $\mathrm{Gal}(f) = \mathbf{U}_3(2^m) := \mathrm{PSU}_3(\mathbf{F}_{2^m})$ and $n = 2^{3m} + 1$ is treated.

1. INTRODUCTION

In [15] 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_a of the ground field K if the Galois group $\mathrm{Gal}(f)$ of the irreducible polynomial $f \in K[x]$ is "very big". Namely, if $n = \deg(f) \geq 5$ and $\mathrm{Gal}(f)$ is either the symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$, then the ring $\mathrm{End}(J(C_f))$ of K_a-endomorphisms of $J(C_f)$ coincides with $\mathbf{Z}$. Later the author [16] proved that $\mathrm{End}(J(C_f)) = \mathbf{Z}$ for an infinite series of $\mathrm{Gal}(f) = \mathrm{PSL}_2(\mathbf{F}_{2^r})$ and $n = 2^r + 1$ (with $\dim(J(C_f)) = 2^{r-1}$) or when $\mathrm{Gal}(f)$ is the Suzuki group $\mathbf{Sz}(2^{2r+1})$ and $n = 2^{2(2r+1)} + 1$ (with $\dim(J(C_f)) = 2^{4r+1}$). We refer the reader to [12], [13], [9], [10], [11], [15], [16], [17] for a discussion of known results about, and examples of, hyperelliptic jacobians without complex multiplication.

We write $\mathfrak{R} = \mathfrak{R}_f$ for the set of roots of f and consider $\mathrm{Gal}(f)$ as the corresponding permutation group of $\mathfrak{R}$. Suppose $q = 2^m > 2$ is an integral power of 2 and $\mathbf{F}_{q^2}$ is a finite field consisting of q^2 elements. Let us consider a non-degenerate Hermitian (wrt $x \mapsto x^q$) sesquilinear form on $\mathbf{F}_{q^2}^3$. In the present paper we prove that

$$\mathrm{End}(J(C_f)) = \mathbf{Z}$$

Received by the editors August 30, 2001.
2000 *Mathematics Subject Classification.* Primary 14H40; Secondary 14K05.
Key words and phrases. Hyperelliptic jacobians, endomorphisms of abelian varieties, Steinberg representations, unitary groups, Hermitian curves.
This work was partially supported by NSF grant DMS-0070664.

when $\mathfrak{R}_f$ can be identified with the corresponding "Hermitian curve" of isotropic lines in the projective plane $\mathbf{P}^2(\mathbf{F}_{q^2})$ in such a way that $\mathrm{Gal}(f)$ becomes either the projective unitary group $\mathrm{PGU}_3(\mathbf{F}_q)$ or the projective special unitary group $\mathbf{U}_3(q) := \mathrm{PSU}_3(\mathbf{F}_q)$. In this case $n = \deg(f) = q^3+1 = 2^{3m}+1$ and $\dim(J(C_f)) = q^3/2 = 2^{3m-1}$.

Our proof is based on an observation that the Steinberg representation is the only absolutely irreducible nontrivial representation (up to an isomorphism) over $\mathbf{F}_2$ of $\mathbf{U}_3(2^m)$, whose dimension is a power of 2.

I am deeply grateful to the referee for useful comments.

2. Main results

Throughout this paper we assume that K is a field with $\mathrm{char}(K) \neq 2$. We fix its algebraic closure K_a and write $\mathrm{Gal}(K)$ for the absolute Galois group $\mathrm{Aut}(K_a/K)$. If X is an abelian variety defined over K, then we write $\mathrm{End}(X)$ 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 $\mathfrak{R} = \mathfrak{R}_f \subset K_a$ be the set of roots of f, let $K(\mathfrak{R}_f) = K(\mathfrak{R})$ be the splitting field of f and let $\mathrm{Gal}(f) := \mathrm{Gal}(K(\mathfrak{R})/K)$ be the Galois group of f, viewed as a subgroup of $\mathrm{Perm}(\mathfrak{R})$. 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 $J(C_f)$.

Theorem 2.1. *Recall that* $\mathrm{char}(K) \neq 2$. *Assume that there exists a positive integer* $m > 1$ *such that* $n = 2^{3m}+1$ *and* $\mathrm{Gal}(f)$ *contains a subgroup isomorphic to* $\mathbf{U}_3(2^m)$. *Then either* $\mathrm{End}(J(C_f)) = \mathbf{Z}$ *or* $\mathrm{char}(K) > 0$ *and* $J(C_f)$ *is a supersingular abelian variety.*

Remark 2.2. It would be interesting to find explicit examples of irreducible polynomials $f(x)$ of degree $2^{3m}+1$ with Galois group $\mathbf{U}_3(2^m)$. It follows from results of Belyi [1] that such a polynomial always exists over a certain abelian number field K (depending on m). The celebrated Shafarevich conjecture implies that such polynomials must exist over the field $\mathbf{Q}$ of rational numbers.

We will prove Theorem 2.1 in §5.

3. Permutation groups, permutation modules and very simplicity

Let B be a finite set consisting of $n \geq 5$ elements. We write $\mathrm{Perm}(B)$ for the group of permutations of B. A choice of ordering on B gives rise to an isomorphism

$$\mathrm{Perm}(B) \cong \mathbf{S}_n.$$

Let G be a subgroup of $\mathrm{Perm}(B)$. For each $b \in B$ we write G_b for the stabilizer of b in G; it is a subgroup of G. Further we always assume that n is *odd*.

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.

We write $\mathbf{F}_2^B$ for the n-dimensional $\mathbf{F}_2$-vector space of maps $h : B \to \mathbf{F}_2$. The space $\mathbf{F}_2^B$ is provided with a natural action of $\mathrm{Perm}(B)$ defined as follows. Each

$s \in \mathrm{Perm}(B)$ sends a map $h : B \to \mathbf{F}_2$ into $sh : b \mapsto h(s^{-1}(b))$. The permutation module $\mathbf{F}_2^B$ contains the $\mathrm{Perm}(B)$-stable hyperplane

$$Q_B := \{h : B \to \mathbf{F}_2 \mid \sum_{b\in B} h(b) = 0\}$$

and the $\mathrm{Perm}(B)$-invariant line $\mathbf{F} \cdot 1_B$ where 1_B is the constant function 1. Since n is odd, there is a $\mathrm{Perm}(B)$-invariant splitting

$$\mathbf{F}_2^B = Q_B \oplus \mathbf{F}_2 \cdot 1_B.$$

Clearly,

$$\dim_{\mathbf{F}_2}(Q_B) = n - 1$$

and $\mathbf{F}_2^B$ and Q_B carry natural structures of G-modules. Clearly, Q_B is a faithful G-module. It is also clear that the G-module Q_B can be viewed as the reduction modulo 2 of the $\mathbf{Q}[G]$-module

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

It is well-known that the $\mathbf{Q}[G]$-module $(\mathbf{Q}^B)^0$ is absolutely simple if and only if the action of G on B is doubly transitive ([14], Sect. 2.3, Ex. 2).

Remark 3.2. Assume that G acts on B doubly transitively and that

$$\#(B) - 1 = \dim_{\mathbf{Q}}((\mathbf{Q}_B)^0)$$

coincides with the largest power of 2 dividing $\#(G)$. Then it follows from a theorem of Brauer-Nesbitt ([14], Sect. 16.4, pp. 136–137; [7], p. 249) that Q_B is an absolutely simple $\mathbf{F}_2[G]$-module. In particular, Q_B is (the reduction of) the Steinberg representation [7], [3].

We refer to [16] for a discussion of the following definition.

Definition 3.3. Let V be a vector space over a field $\mathbf{F}$, let G be a group and $\rho : G \to \mathrm{Aut}_{\mathbf{F}}(V)$ a linear representation of G in V. We say that the G-module V is *very simple* if it enjoys the following property:

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

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

then either $R = \mathbf{F} \cdot \mathrm{Id}$ or $R = \mathrm{End}_{\mathbf{F}}(V)$.

Remarks 3.4. (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 [16], Remark 2.2(ii)).
(iii) If $\dim_{\mathbf{F}}(V) = 1$, then obviously the G-module V is very simple.
(iv) Assume that the G-module V is very simple and $\dim_{\mathbf{F}}(V) > 1$. 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 $\mathbf{F}$-dimension is strictly less than $\dim_{\mathbf{F}}(V)$ (see [16], Example 7.1).
(v) If $\mathbf{F} = \mathbf{F}_2$ and G is *perfect*, then properties (ii)-(iv) characterize the very simple G-modules (see [16], Th. 7.7).

The following statement provides a criterion of very simplicity over $\mathbf{F}_2$.

Theorem 3.5. *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 $\mathbf{F}_2[H]$-module of $\mathbf{F}_2$-dimension a or there does not exist an absolutely simple $\mathbf{F}_2[H]$-module of $\mathbf{F}_2$-dimension b.*

Then each absolutely simple $\mathbf{F}_2[H]$-module of $\mathbf{F}_2$-dimension N is very simple.

Proof. This is Corollary 7.9 of [16]. □

4. Steinberg representation

We refer to [7] and [3] for a definition and basic properties of Steinberg representations.

Let us fix an algebraic closure of $\mathbf{F}_2$ and denote it by $\mathcal{F}$. We write $\phi:\mathcal{F}\to\mathcal{F}$ for the Frobenius automorphism $x\mapsto x^2$. Let $q=2^m$ be a positive integral power of two. Then the subfield of invariants of $\phi^m:\mathcal{F}\to\mathcal{F}$ is a finite field $\mathbf{F}_q$ consisting of q elements. Let q' be an integral positive power of q. If d is a positive integer and i is a non-negative integer, then for each matrix $u\in \mathrm{GL}_d(\mathcal{F})$ we write $u^{(i)}$ for the matrix obtained by raising each entry of u to the 2^ith power.

Remark 4.1. Recall that an element $\alpha\in\mathbf{F}_q$ is called *primitive* if $\alpha\ne 0$ and has multiplicative order $q-1$ in the cyclic multiplicative group $\mathbf{F}_q^*$.

Let $M<q-1$ be a positive integer. Clearly, the set

$$\mu_M(\mathbf{F}_q)=\{\alpha\in\mathbf{F}_q\mid \alpha^M=1\}$$

is a cyclic multiplicative subgroup of $\mathbf{F}_q^*$ and its order M' divides both M and $q-1$. Since $M<q-1$ and $q-1$ is odd, the ratio $(q-1)/M'$ is an *odd* integer >1. This implies that $3\le (q-1)/M'$ and therefore

$$M'=\#(\mu_M(\mathbf{F}_q))\le (q-1)/3.$$

Lemma 4.2. *Let $q>2$, let d be a positive integer and let G be a subgroup of $\mathrm{GL}_d(\mathbf{F}_{q'})$. Assume that one of the following two conditions holds:*

(i) *There exists an element $u\in G\subset \mathrm{GL}_d(\mathbf{F}_{q'})$, whose trace α lies in $\mathbf{F}_q^*$ and has multiplicative order $q-1$.*

(ii) *There exist a positive integer $r>\frac{q-1}{3}$, distinct $\alpha_1,\cdots,\alpha_r\in\mathbf{F}_q^*$ and elements*

$$u_1,\cdots,u_r\in G\subset \mathrm{GL}_d(\mathbf{F}_{q'})$$

such that the trace of u_i is α_i for all $i=1,\cdots,r$.

Let $V_0=\mathcal{F}^d$ and $\rho_0: G\subset \mathrm{GL}_d(\mathbf{F}_{q'})\subset \mathrm{GL}_d(\mathcal{F})=\mathrm{Aut}_{\mathcal{F}}(V_0)$ be the natural d-dimensional representation of G over $\mathcal{F}$. For each positive integer $i<m$ let us put $V_i:=V_0$ and define a d-dimensional $\mathcal{F}$-representation

$$\rho_i: G\to \mathrm{Aut}(V_i)$$

as the composition of

$$G\hookrightarrow \mathrm{GL}_d(\mathbf{F}_{q'}),\quad x\mapsto x^{(i)}$$

and the inclusion map

$$\mathrm{GL}_d(\mathbf{F}_{q'}) \subset \mathrm{GL}_d(\mathcal{F}) \cong \mathrm{Aut}_{\mathcal{F}}(V_i).$$

Let S be a subset of $\{0, 1, \dots, m-1\}$. Let us define a $d^{\#(S)}$-dimensional $\mathcal{F}$-representation ρ_S of G as the tensor product of representations ρ_i for all $i \in S$. If S is a proper subset of $\{0, 1, \dots, m-1\}$, then there exists an element $u \in G$ such that the trace of $\rho_S(u)$ does not belong to $\mathbf{F}_2$. In particular, ρ_S could not be obtained by extension of scalars to $\mathcal{F}$ from a representation of G over $\mathbf{F}_2$.

Proof. Clearly,

$$\mathrm{tr}(\rho_i(u)) = \mathrm{tr}(\rho_0(u))^{2^i} \quad \forall u \in G.$$

This implies easily that

$$\mathrm{tr}(\rho_S(u)) = \prod_{i \in S} \mathrm{tr}(\rho_i(u)) = \mathrm{tr}(\rho_0(u))^M$$

where $M = \sum_{i \in S} 2^i$. Since S is a *proper* subset of $\{0, 1, \cdots, m-1\}$, we have

$$0 < M < \sum_{i=0}^{m-1} 2^i = 2^m - 1 = \#(\mathbf{F}_q^*).$$

Assume that condition (i) holds. Then there exists $u \in G$ such that $\alpha = \mathrm{tr}(\rho_0(u))$ lies in $\mathbf{F}_q^*$ and the exact multiplicative order of α is $q - 1 = 2^m - 1$.

This implies that $0 \ne \alpha^M \ne 1$. Since $\mathbf{F}_2 = \{0, 1\}$, we conclude that $\alpha^M \notin \mathbf{F}_2$. Therefore

$$\mathrm{tr}(\rho_S(u)) = \mathrm{tr}(\rho_0(u))^M = \alpha^M \notin \mathbf{F}_2.$$

Now assume that condition (ii) holds. It follows from Remark 4.1 that there exists $\alpha = \alpha_i \ne 0$ such that $\alpha^M \ne 1$ for some i with $1 \le i \le r$. This implies that if we put $u = u_i$, then

$$\mathrm{tr}(\rho_S(u)) = \mathrm{tr}(\rho_0(u))^M = \alpha^M \notin \mathbf{F}_2.$$

$\square$

Now, let us put $q' = q^2 = p^{2m}$. We write $x \mapsto \bar{x}$ for the involution $a \mapsto a^q$ of $\mathbf{F}_{q^2}$. Let us consider the special unitary group $\mathrm{SU}_3(\mathbf{F}_q)$ consisting of all matrices $A \in \mathrm{SL}_3(\mathbf{F}_{q^2})$ which preserve a nondegenerate Hermitian sesquilinear form on $\mathbf{F}_{q^2}^3$, say,

$$x, y \mapsto x_1\bar{y_3} + x_2\bar{y_2} + x_3\bar{y_1} \quad \forall x = (x_1, x_2, x_3), y = (y_1, y_2, y_3).$$

It is well-known that the conjugacy class of the special unitary group in $\mathrm{GL}_3(\mathbf{F}_{q^2})$ does not depend on the choice of Hermitian form and that $\#(\mathrm{SU}_3(\mathbf{F}_q)) = (q^3 + 1)q^3(q^2 - 1)$. Clearly, for each $\beta \in \mathbf{F}_q^*$ the group $\mathrm{SU}_3(\mathbf{F}_q)$ contains the diagonal matrix $u = \mathrm{diag}(\beta, 1, \beta^{-1})$ with eigenvalues $\beta, 1, \beta^{-1}$; clearly, the trace of u is $\beta + \beta^{-1} + 1$.

Theorem 4.3. *Suppose $G = \mathrm{SU}_3(\mathbf{F}_q)$. Suppose V is an absolutely simple nontrivial $\mathbf{F}_2[G]$-module. Assume that $m > 1$. If $\dim_{\mathbf{F}_2}(V)$ is a power of 2, then it is equal to q^3. In particular, V is the Steinberg representation of $\mathrm{SU}_3(\mathbf{F}_q)$.*

Proof. Recall ([4], p. 77, 2.8.10c) that the adjoint representation of G in $\mathrm{End}_{\mathbf{F}_{q^2}}(\mathbf{F}_{q^2}^3)$ splits into a direct sum of the trivial one-dimensional representation (scalars) and an absolutely simple $\mathbf{F}_{q^2}[G]$-module St_2 of dimension 8 (traceless operators). The kernel of the natural homomorphism

$$G = \mathrm{SU}_3(\mathbf{F}_q) \to \mathrm{Aut}_{\mathbf{F}_{q^2}}(\mathrm{St}_2) \cong \mathrm{GL}_8(\mathbf{F}_{q^2})$$

coincides with the center $Z(G)$ which is either trivial or a cyclic group of order 3 depending on whether $(3, q+1) = 1$ or 3. In both cases we get an embedding

$$G' := G/Z(G) = \mathbf{U}_3(q) = \mathrm{PSU}_3(\mathbf{F}_q) \subset \mathrm{GL}_8(\mathbf{F}_{q^2}).$$

If $m = 2$ (i.e., $q = 4$), then $G = \mathrm{SU}_3(\mathbf{F}_4) = \mathbf{U}_3(4)$ and one may use Brauer character tables [8] in order to study absolutely irreducible representations of G in characteristic 2. Notice ([8], p. 284) that the reduction modulo 2 of the irrational constant b5 does not lie in $\mathbf{F}_2$. Using the table on p. 70 of [8], we conclude that there is only one (up to an isomorphism) absolutely irreducible representation of G defined over $\mathbf{F}_2$ and its dimension is $64 = q^3$. This proves the assertion of the theorem in the case of $m = 2, q = 4$. So further we assume that

$$m \geq 3, \quad q = 2^m \geq 8.$$

Clearly, for each $u \in G \subset \mathrm{GL}_3(\mathbf{F}_{q^2})$ with trace $\delta \in \mathbf{F}_{q^2}$ the image u' of u in G' has trace $\bar{\delta}\delta - 1 \in \mathbf{F}_q$. In particular, if $u = \mathrm{diag}(\beta, 1, \beta^{-1})$ with $\beta \in \mathbf{F}_q^*$, then the trace of u' is

$$t_\beta := \mathrm{tr}(u') = (1 + \beta + \beta^{-1})(1 + \beta + \beta^{-1}) - 1 = (\beta + \beta^{-1})^2.$$

Now let us start to vary β in the $q-2$-element set

$$\mathbf{F}_q \setminus \mathbf{F}_2 = \mathbf{F}_q^* \setminus \{1\}.$$

One may easily check that the set of all t_β's consists of $\frac{q-2}{2}$ elements of $\mathbf{F}_q^*$. Since $q \geq 8$,

$$r := \frac{q-2}{2} > \frac{q-1}{3}.$$

This implies that $G' \subset \mathrm{GL}_8(\mathbf{F}_{q^2})$ satisfies the conditions of Lemma 4.2 with $d = 8$. In particular, none of representations ρ_S of G' could be realized over $\mathbf{F}_2$ if S is a *proper* subset of $\{0, 1, \cdots, m-1\}$. On the other hand, it is known ([4], p. 77, Example 2.8.10c) that each absolutely irreducible representation of G over $\mathcal{F}$ either has dimension divisible by 3 or is isomorphic to the representation obtained from some ρ_S via $G \to G'$. The rest is clear. □

Theorem 4.4. *Suppose $m > 1$ is an integer and let us put $q = 2^m$. Let B be a (q^3+1)-element set. Let H be a group acting faithfully on B. Assume that H contains a subgroup G' isomorphic to $\mathbf{U}_3(q)$. Then the H-module Q_B is very simple.*

Proof. First, $\mathbf{U}_3(q)$ is a simple non-abelian group whose order is $q^3(q^3+1)(q^2-1)/\nu$ where $\nu = (3, q+1)$ is 1 or 3 according to whether m is even or odd ([2], p. XVI, Table 6; [4], pp. 39–40). Second, notice that $\mathbf{U}_3(q) \subset H$ acts transitively on B. Indeed, the list of maximal subgroups of $\mathbf{U}_3(q)$ ([5], p. 158; see also [4], Th. 6.5.3 and its proof, pp. 329–332) is as follows:

(1) Groups of order $q^3(q^2-1)/\nu$. The preimage of any such group in $\mathrm{SU}_3(\mathbf{F}_q)$ leaves invariant a certain one-dimensional subspace in $\mathbf{F}_{q^2}^3$ (the *centre* of an *elation*; see [5], pp. 142, 158).
(2) Groups of order $(q+1)(q^2-1)/\nu$.
(3) Groups of order $6(q+1)^2/\nu$.
(4) Groups of order $3(q^2-q+1)\nu$.
(5) $\mathbf{U}_3(2^r)$ where r is a factor of m and m/r is an odd prime.
(6) Groups containing $\mathbf{U}_3(2^r)$ as a normal subgroup of index 3 when r is odd and $m=3r$.

The classification of maximal subgroups of $\mathbf{U}_3(q)$ easily implies that each subgroup of $\mathbf{U}_3(q)$ has index $\geq q^3+1=\#(B)$ (see also [6], pp. 213–214). This implies that $\mathbf{U}_3(q)$ acts transitively on B. Third, we claim that this action is, in fact, doubly transitive. Indeed, the stabilizer $\mathbf{U}_3(q)_b$ of a point $b\in B$ has index q^3+1 in $\mathbf{U}_3(q)$ and therefore is a maximal subgroup. It follows easily from the same classification that the maximal subgroup $\mathbf{U}_3(q)_b$ is (the image of) the stabilizer (in $\mathrm{SU}_3(\mathbf{F}_q)$) of a one-dimensional subspace L in $\mathbf{F}_{q^2}^3$. The counting arguments easily imply that L is isotropic. Hence $\mathbf{U}_3(q)_b$ is (the image of) the stabilizer of an isotropic line in $\mathbf{F}_{q^2}^3$. Taking into account that the set of isotropic lines in $\mathbf{F}_{q^2}^3$ has cardinality $q^3+1=\#(B)$, we conclude that $B=\mathbf{U}_3(q)/\mathbf{U}_3(q)_b$ is isomorphic (as $\mathbf{U}_3(q)$-set) to the set of isotropic lines on which $\mathbf{U}_3(q)$ acts doubly transitively and we are done.

By Remark 3.2, the double transitivity implies that the $\mathbf{F}_2[\mathbf{U}_3(q)]$-module Q_B is absolutely simple. Since $\mathrm{SU}_3(\mathbf{F}_q)\to\mathbf{U}_3(q)$ is surjective, the corresponding $\mathbf{F}_2[\mathrm{SU}_3(\mathbf{F}_q)]$-module Q_B is also absolutely simple.

Recall that $\dim_{\mathbf{F}_2}(Q_B)=\#(B)-1=q^3=2^{3m}$. By Theorem 4.3, there are no absolutely simple nontrivial $\mathbf{F}_2[\mathrm{SU}_3(\mathbf{F}_q)]$-modules whose dimension *strictly* divides 2^{3m}. This implies that Q_B is *not* isomorphic to a tensor product of absolutely simple $\mathbf{F}_2[\mathrm{SU}_3(\mathbf{F}_q)]$-modules of dimension >1. Therefore Q_B is *not* isomorphic to a tensor product of absolutely simple $\mathbf{F}_2[\mathbf{U}_3(q)]$-modules of dimension >1. Recall that all subgroups in $G'=\mathbf{U}_3(q)$ that are different from $\mathbf{U}_3(q)$ itself have index $\geq q^3+1>q^3=\dim_{\mathbf{F}_2}(Q_B)$. It follows from Theorem 3.5 that the G'-module Q_B is very simple. Now the desired very simplicity of the H-module Q_B is an immediate corollary of Remark 3.4(i). □

5. Proof of Theorem 2.1

Recall that $\mathrm{Gal}(f)\subset\mathrm{Perm}(\mathfrak{R})$. It is also known that the natural homomorphism $\mathrm{Gal}(K)\to\mathrm{Aut}_{\mathbf{F}_2}(J(C)_2)$ factors through the canonical surjection $\mathrm{Gal}(K)\twoheadrightarrow\mathrm{Gal}(K(\mathfrak{R})/K)=\mathrm{Gal}(f)$, and the $\mathrm{Gal}(f)$-modules $J(C)_2$ and $Q_{\mathfrak{R}}$ are isomorphic (see, for instance, Th. 5.1 of [16]). In particular, if the $\mathrm{Gal}(f)$-module $Q_{\mathfrak{R}}$ is very simple, then the $\mathrm{Gal}(f)$-module $J(C)_2$ is also very simple and therefore is absolutely simple.

Lemma 5.1. *If the* $\mathrm{Gal}(f)$*-module* $Q_{\mathfrak{R}}$ *is very simple, then either* $\mathrm{End}(J(C_f))=\mathbf{Z}$ *or* $\mathrm{char}(K)>0$ *and* $J(C_f)$ *is a supersingular abelian variety.*

Proof. This is Corollary 5.3 of [16]. □

It follows from Theorem 4.4 that under the assumptions of Theorem 2.1, the $\mathrm{Gal}(f)$-module $Q_{\mathfrak{R}}$ is very simple. Applying Lemma 5.1, we conclude that either $\mathrm{End}(J(C_f))=\mathbf{Z}$ or $\mathrm{char}(K)>0$ and $J(C_f)$ is a supersingular abelian variety.

References

[1] G. V. Belyi, *On extensions of the maximal cyclotomic field having a given classical Galois group*. J. Reine Angew. Math. **341** (1983), 147–156. MR **84h:**12010

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups. Clarendon Press, Oxford, 1985. MR **88g:**20025

[3] Ch. W. Curtis, *The Steinberg character of a finite group with a* (B, N)*-pair*. J. Algebra **4** (1966), 433–441. MR **34:**1406

[4] D. Gorenstein, R. Lyons, R. Solomon, The classification of the finite simple groups, Number 3. Mathematical Surveys and Monographs 40.3, AMS, Providence, RI, 1998. MR **98j:**20011

[5] R. W. Hartley, *Determination of the ternary collineation groups whose coefficients lie in the* $GF(2^n)$. Ann. of Math. **27** (1926), 140–158.

[6] A. R. Hoffer, *On unitary collineation groups*. J. Algebra **22** (1972), 211–218. MR **46:**780

[7] J. E. Humphreys, *The Steinberg representation*. Bull. AMS (N.S.) **16** (1987), 247–263. MR **88c:**20050

[8] Ch. Jansen, K. Lux, R. Parker, R. Wilson, An Atlas of Brauer characters. Clarendon Press, Oxford, 1995. MR **96k:**20016

[9] 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. MR **83d:**14012

[10] N. Katz, *Affine cohomological transforms, perversity, and monodromy*. J. Amer. Math. Soc. **6** (1993), 149–222. MR **94b:**14013

[11] D. Masser, *Specialization of some hyperelliptic jacobians*. In: Number Theory in Progress (eds. K. Györy, H. Iwaniec, J.Urbanowicz), vol. I, pp. 293–307; de Gruyter, Berlin-New York, 1999. MR **2000j:**11088

[12] Sh. Mori, *The endomorphism rings of some abelian varieties*. Japanese J. Math. **2** (1976), 109–130. MR **56:**12013

[13] Sh. Mori, *The endomorphism rings of some abelian varieties*. II, Japanese J. Math. **3** (1977), 105–109. MR **80e:**14009

[14] J.-P. Serre, Linear representations of finite groups, Springer-Verlag, 1977. MR **56:**8675

[15] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Res. Letters **7** (2000), 123–132. MR **2001a:**11097

[16] Yu. G. Zarhin, *Hyperelliptic jacobians and modular representations*. In: Moduli of abelian varieties (C. Faber, G. van der Geer, F. Oort, eds.), pp. 473–490, Progress in Math., Vol. 195, Birkhäuser, Basel–Boston–Berlin, 2001. MR **2002b:**11082

[17] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication in positive characteristic*. Math. Res. Letters **8** (2001), 429–435.

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

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