HYPERELLIPTIC JACOBIANS WITHOUT COMPLEX MULTIPLICATION, DOUBLY TRANSITIVE PERMUTATION GROUPS AND PROJECTIVE REPRESENTATIONS

YURI G. ZARHIN

1. Introduction

Let $K$ be a field of characteristic zero, $K_a$ its algebraic closure, $n \geq 5$ an integer, $f(x)$ an irreducible polynomial over $K$ of degree $n$, whose Galois group $\text{Gal}(f)$ acts doubly transitively on the set $\mathcal{R}$ of roots of $f$. Let $C : y^2 = f(x)$ be the corresponding hyperelliptic curve and $X = J(C)$ its jacobian defined over $K$. Earlier, the author [20], [21], [25] has proven that the ring $\text{End}(X)$ of all $K_a$-endomorphisms coincides with $\mathbb{Z}$ if $\text{Gal}(f)$ is either the full symmetric group $S_n$ or the corresponding alternating group $A_n$ or a small Mathieu group $M_n$ (with $n = 11$ or $12$) or $\mathcal{R}$ could be identified with the projective space $\mathbb{P}_{m-1}(F_q)$ over a finite field $F_q$ of odd characteristic in such a way that $\text{Gal}(f)$ contains the projective special linear group $\text{PSL}_m(F_q)$ while $m \geq 3$ and $(m, q) \neq (4, 3)$. (Similar results were obtained when $\text{Gal}(f) = L_2(2^r), Sz(2^{2r+1})$ or $U_3(2^r)$ [21], [24].) The proof was based on an observation that in all these cases the natural (faithful) representation of $\text{Gal}(f)$ is very simple; in particular, it is absolutely irreducible. (See [21], [22], [23] for the definition and basic properties of very simple representations.) We refer the reader to [9], [10], [4], [5], [8], [20], [21], [22], [24], [25] for a discussion of known results about, and examples of, hyperelliptic jacobians without complex multiplication.

In the present paper we suggest a new approach to already known examples when $\text{End}(X) = \mathbb{Z}$ from [20], [21] and [25]. Namely, instead of very simplicity, we use a theorem of Feit-Tits [2] complemented by results of Kleidman-Liebeck [6]. Besides obtaining new proofs of already known results, we get new examples when $\text{End}(X) = \mathbb{Z}$ with reducible (but still absolutely indecomposable) $\text{Gal}(f)$-module $X_2$. Namely, we prove that $\text{End}(X) = \mathbb{Z}$ when $\text{Gal}(f)$ is a big Mathieu group (with $n = 22, 23$ or $24$) or $\mathcal{R}$ could be identified with the projective space $\mathbb{P}^{m-1}(F_q)$ over a finite field $F_q$ of characteristic 2 in such a way that $\text{Gal}(f)$ becomes either the projective special linear group $L_m(q) := \text{PSL}_m(F_q)$ or the projective linear group $\text{PGL}_m(F_q)$ with $m > 2$ (except $(m, q) = (4, 2), (3, 4)$). We refer to Theorem 5.4 (and Definitions 3.1 and 3.6) for a justification for the long title of the present article.

The paper is organized as follows. In §3 we state the main results. Section 3 contains auxiliary results from representation theory. In §4 we discuss fields of definitions for endomorphisms of abelian varieties. Section 5 contains proofs of the main results.

Partially supported by the NSF.
2. Main results

Throughout this paper we assume that $K$ is a field of characteristic 0. We fix its algebraic closure $K_a$ and write $\text{Gal}(K)$ for the absolute Galois group $\text{Aut}(K_a/K)$.

**Theorem 2.1.** Let $K$ be a field of characteristic zero, $K_a$ its algebraic closure, $f(x) \in K[x]$ an irreducible polynomial of degree $n$. Suppose $n = 11, 12, 22, 23$ or 24 and the Galois group of $f$ is the corresponding Mathieu group $M_n$. Let $C_f$ be the hyperelliptic curve $y^2 = f(x)$. Let $J(C_f)$ be its jacobian, $\text{End}(J(C_f))$ the ring of $K_a$-endomorphisms of $J(C_f)$. Then $\text{End}(J(C_f)) = \mathbb{Z}$.

**Remark 2.2.** The case of small Mathieu groups was done in Th. 7.13 on p. 489 of [21] (see also [25]). However, in this paper we give a unified proof for all Mathieu groups.

**Theorem 2.3.** Let $K$ be a field of characteristic zero, $K_a$ its algebraic closure, $f(x) \in K[x]$ an irreducible polynomial of degree $n$ and $\mathfrak{R} \subset K_a$ the set of its roots. We write $\text{Gal}(f)$ for the Galois group of $f$. Suppose there exist integers $m > 2$ and $r \geq 1$ such that $n = \frac{2^r - 1}{q - 1}$ where $q = 2^r$ and $(m, q) \neq (2, 2), (4, 2), (3, 4)$. Assume, in addition, that $\mathfrak{R}$ could be identified with the projective space $\mathbb{P}^{m-1}(\mathbb{F}_q)$ over the finite field $\mathbb{F}_q$ in such a way that $\text{Gal}(f)$ contains $\text{L}_m(q) := \text{PSL}_m(\mathbb{F}_q)$ as a subgroup. (E.g., $\text{Gal}(f) = \text{L}_m(q)$ or $\text{PGL}_m(\mathbb{F}_q)$.) Let $C_f$ be the hyperelliptic curve $y^2 = f(x)$. Let $J(C_f)$ be its jacobian, $\text{End}(J(C_f))$ the ring of $K_a$-endomorphisms of $J(C_f)$. Then $\text{End}(J(C_f)) = \mathbb{Z}$.

**Remark 2.4.** In the case of $m = 2$ this assertion is proven in [21].

**Theorem 2.5.** Let $K$ be a field of characteristic zero, $K_a$ its algebraic closure, $f(x) \in K[x]$ an irreducible polynomial of degree $n$ and $\mathfrak{R} \subset K_a$ the set of its roots. We write $\text{Gal}(f)$ for the Galois group of $f$. Assume that there exist an odd power prime $q \geq 3$ and an integer $m \geq 3$ such that $n = \frac{2^r - 1}{q - 1}$ and the set $\mathfrak{R}$ could be identified with the projective space $\mathbb{P}^{m-1}(\mathbb{F}_q)$ over the prime field $\mathbb{F}_q$ in such a way that $\text{Gal}(f)$ contains $\text{L}_m(q) := \text{PSL}_m(\mathbb{F}_q)$ as a subgroup. (E.g., $\text{Gal}(f) = \text{L}_m(q)$ or $\text{PGL}_m(\mathbb{F}_q)$.) Let $C_f$ be the hyperelliptic curve $y^2 = f(x)$. Let $J(C_f)$ be its jacobian, $\text{End}(J(C_f))$ the ring of $K_a$-endomorphisms of $J(C_f)$. Then $\text{End}(J(C_f)) = \mathbb{Z}$.

**Remark 2.6.** When $(m, q) \neq (4, 3)$ this assertion is already proven in [25]. However, in this paper we give a unified proof for all $(m, q)$.

3. Group theory

**Definition 3.1.** Suppose $\mathcal{G} \neq \{1\}$ is a perfect finite group and $g > 1$ is an integer. We say that $\mathcal{G}$ is $g$-unbounded if it enjoys the following properties:

(i) Each homomorphism $\mathcal{G} \to \text{PSL}(g - 1, \mathbb{C})$ is trivial;

(ii) Either $g$ is odd and each homomorphism $\mathcal{G} \to \text{PSL}(g, \mathbb{Q}) = \text{SL}(g, \mathbb{Q})$ is trivial or $g$ is even and each homomorphism $\mathcal{G} \to \text{PSL}(g, \mathbb{R}) = \text{SL}(g, \mathbb{R})/\{\pm 1\}$ is trivial.

**Remark 3.2.** (i) Clearly, if every nontrivial irreducible projective representation of $\mathcal{G}$ in characteristic zero has dimension $> g$ then all nontrivial projective representations of $\mathcal{G}$ in characteristic zero have dimension $> g$ and therefore $\mathcal{G}$ is $g$-unbounded.
(ii) Clearly, if \( H \) is a simple non-abelian group isomorphic to a subgroup of \( G \) then the \( g \)-unboundedness of \( H \) implies the \( g \)-unboundedness of \( G \).

(iii) Clearly, if every nontrivial projective representation of \( G \) in characteristic 2 has dimension \( > g \) then all nontrivial projective representations of \( G \) in characteristic zero have dimension \( > g \) and therefore \( G \) is \( g \)-unbounded.

(iv) Every \( G \) is 2-unbounded. Indeed, it suffices to check that each homomorphism from \( G \) to \( \text{PSL}(2, \mathbb{R}) \) is trivial. But each finite subgroup in \( \text{PSL}(2, \mathbb{R}) \) is the image of a finite subgroup in \( \text{SL}(2, \mathbb{R}) \). Since each finite subgroup of \( \text{SL}(2, \mathbb{R}) \) is commutative, the image \( \pi(G) \) of each homomorphism \( \pi: G \rightarrow \text{PSL}(2, \mathbb{R}) \) is commutative. The perfectness of \( G \) implies that \( \pi(G) \) is also perfect. This implies that \( \pi(G) = \{1\} \), i.e., \( \pi \) is trivial.

**Example 3.3.** Suppose \( g \geq 4 \) is an integer. Then the alternating groups \( A_{2g+1} \) and \( A_{2g+2} \) are \( g \)-bounded. Indeed, \( 2g + 1 > 8 \) and, by a theorem of Wagner [19], every nontrivial linear representation of \( A_{2g+1} \) in characteristic 2 has dimension \( \geq 2g \). Since the Schur multiplier of \( A_{2g+1} \) is 2, one may easily deduce that every nontrivial projective representation of \( A_{2g+1} \) in characteristic 2 also has dimension \( \geq 2g > g \). By Remark 3 (iii), \( A_{2g+1} \) \( g \)-bounded. Since \( A_{2g+1} \) is isomorphic to a subgroup of \( A_{2g+2} \), the group \( A_{2g+2} \) is also \( g \)-bounded.

**Examples 3.4.** (a) The Mathieu groups \( M_{23} \) and \( M_{24} \) are 11-unbounded. Indeed, it follows from the Tables in [1] that all nontrivial irreducible projective representations of \( M_{23} \) in characteristic zero have dimension \( \geq 22 \). This implies that \( M_{23} \) is \( d \)-unbounded for all \( d < 22 \). Since \( M_{23} \) is isomorphic to a subgroup of \( M_{24} \), the group \( M_{24} \) is also \( d \)-unbounded for all \( d < 22 \).

(b) The Mathieu group \( M_{22} \) is 10-unbounded. Indeed, it follows from the Tables in [1] that in characteristic zero all nontrivial irreducible projective representations of \( M_{22} \) have dimension \( \geq 10 \) and there are no nontrivial irreducible linear 10-dimensional representations. This implies that all homomorphisms \( M_{22} \rightarrow \text{PGL}(9, \mathbb{C}) \) are trivial. Now in order to establish the 10-unboundedness of \( M_{22} \) we need only to check that each homomorphism from \( M_{22} \) to \( \text{PSL}(10, \mathbb{R}) \) is trivial. Let us assume that \( \rho: M_{22} \rightarrow \text{PSL}(10, \mathbb{R}) = \text{SL}(10, \mathbb{R})/\{\pm 1\} \) is a nontrivial group homomorphism. Clearly, \( \rho \) lifts to a nontrivial homomorphism

\[
\rho': M_{22}' \rightarrow \text{SL}(10, \mathbb{R})
\]

where \( M_{22}' \) sits in a central extension

\[
\{1\} \rightarrow \{\pm 1\} \rightarrow M_{22}' \rightarrow M_{22} \rightarrow \{1\}.
\]

This extension is non-splittable, since there are no nontrivial homomorphisms from \( M_{22} \) to \( \text{SL}(10, \mathbb{R}) \) [3]. On the other hand, it also follows from the Tables in [1] that there are no 10-dimensional linear irreducible representations of \( M_{22}' \) defined over \( \mathbb{R} \). This implies easily that there are no nontrivial 10-dimensional linear representations of \( M_{22}' \) defined over \( \mathbb{R} \). This gives us the desired contradiction and proves the 10-unboundedness of \( M_{22} \).

(c) Suppose \( r \geq 1 \) and \( m \geq 2 \) are positive integers and assume that \((m, r) \neq (2, 1), (2, 2), (3, 2), (4, 2)\). Let us put \( q = 2^r \). We define a positive integer \( g \) as follows,

\[
g = q/2 \text{ if } m = 2 \text{ and } g = \frac{1}{2} \frac{m-q}{r-1} \text{ if } m > 2.
\]
Then the group $L_m(q) = PSL_m(F_q)$ is $g$-unbounded. Indeed, it is known that under our assumptions on $(m, q)$ all nontrivial irreducible projective representations of $L_m(q)$ in characteristic zero have dimension $\geq \frac{q^m - 1}{q - 1} - 1 > g$ if $m > 2$. It is also known that all nontrivial irreducible projective representations of $L_2(q)$ in characteristic zero have dimension $\geq q - 1 > g$ if $q > 4$.

(d) Suppose $q \geq 3$ is an odd power prime, $m \geq 3$ is an integer. Let us put

$$g := \left[\frac{1}{2} \left(\frac{q^m - 1}{q - 1} - 1\right)\right] = \left[\frac{1}{2} \left(\frac{q^m - q}{q - 1}\right)\right].$$

Then the group $L_m(q) = PSL_m(F_q)$ is $g$-bounded. Indeed, it is known that if $(q, m) \neq (3, 4)$ then all nontrivial irreducible projective representations of $L_m(q)$ in characteristic zero have dimension $\geq \frac{q^m - 1}{q - 1} - 1 > g$.

If $(q, m) = (3, 4)$ then $g = 19$. It follows from the Tables in [1] that all nontrivial irreducible projective representations of $L_4(3)$ in characteristic zero have dimension $\geq 26 > 19$.

Example 3.5. The Mathieu groups $M_{11}$ and $M_{12}$ are $5$-unbounded. Indeed, it follows from the Tables in [1] that all nontrivial irreducible projective representations of $M_{11}$ in characteristic zero have dimension $\geq 10$. This implies that $M_{11}$ is $d$-unbounded for all $d < 10$. Since $M_{11}$ is isomorphic to a subgroup of $M_{12}$, the group $M_{12}$ is also $d$-unbounded for all $d < 10$.

Definition 3.6. Suppose $G$ is a simple non-abelian group, $\ell$ is a prime. Suppose

$$\{1\} \rightarrow N \rightarrow G' \rightarrow G \rightarrow \{1\}$$

is a short exact sequence of finite groups where $N$ is a group of exponent $1$ or $\ell$ and no proper subgroup of $G'$ maps onto $G$. (In particular, $G'$ is perfect.) Then $G'$ is called a minimal cover of $G$.

In addition, if either $N = \{1\}$ (i.e., $G' = G$) or the exponent of $N$ is $\ell$ then we say that $G'$ is a minimal $\ell$-cover of $G$.

Remark 3.7. Clearly, the minimal cover $G'$ is always perfect. It is also clear that each normal subgroup in $G'$ except $G'$ itself lies in $N$. This implies easily that if $\rho : G' \rightarrow M$ is a nontrivial group homomorphism then $\ker(\rho)$ lies in $N$ and therefore the image $\rho(G')$ is also a minimal cover of $G$. In addition, if $G'$ is a minimal $\ell$-cover then $\rho(G')$ is also one.

Remark 3.8. Suppose $G$ is a simple non-abelian group and $\gamma : H \rightarrow G$ is a surjective homomorphism of finite groups. Let $G'$ be a subgroup of smallest order among the subgroups $H'$ of $H$ such that $\gamma(H') = G$. (Clearly, such $G'$ always exists.) Then $\gamma : G' \rightarrow G$ is a minimal cover. In addition, if the kernel of is either trivial or has exponent $\ell$ then $\gamma : G' \rightarrow G$ is a minimal $\ell$-cover.

Examples 3.9. (i) Suppose $G$ is a simple non-abelian group isomorphic either to $A_5 \cong L_2(4)$ or to $A_6$. Suppose $G'$ is a minimal cover of $G$. Then, by Remark 3.2(iv), the perfect group $G'$ is $2$-bounded.
(ii) Suppose \( G \) is a simple non-abelian group isomorphic either to \( L_3(2) \cong L_2(7) \) or to \( A_7 \) or to \( A_6 \cong L_4(2) \). Notice that in all these cases the order of \( G \) is divisible by 7.

Suppose \( G' \) is a minimal cover of \( G \). Then \( G' \) is 3-bounded. Indeed, if \( \pi_2 : G' \to PSL(2, C) \) is a nontrivial homomorphism then, by Remark 3.3, its image \( H' := \pi(G') \subset PSL(2, C) \) is also a minimal cover of \( G \). In particular, \( H_2 \) is a perfect finite group having a quotient isomorphic to \( G \). This implies that nonsolvable \( H_2 \subset PSL(2, C) \) is not isomorphic to \( A_5 \) which could not be true (ibid, Remark 3.11). Kleidman and Liebeck [6] studied the case of simple groups of Lie type in characteristic 2. In particular, they proved the following assertion (ibid, Remark 3.11. Th. 6.17 on p. 404). The obtained contradiction implies that there are no nontrivial homomorphisms from \( G' \) to \( PSL(2, C) \).

Now assume that there exists a nontrivial homomorphism \( \pi_3 : G' \to SL(3, Q) \). As above, the image \( H_3 := \pi(G') \subset SL(3, Q) \) is also a minimal cover of \( G \). In particular, \( H_3 \) is a finite group having a quotient isomorphic to \( G \); in particular, 7 divides the order of \( H_3 \) and therefore \( H_3 \subset SL(3, Q) \) contains an element of order 7. But this is not true, since the degree of the 7th cyclotomic field over \( Q \) is 6 > 3. The obtained contradiction ends the proof of the 3-unboundness of \( G' \).

We will use the following result of Feit-Tits (8, Theorem on pp. 1092–1093 and Prop. 4.1 on p. 1098) concerning complex projective representations of minimum degree. (See also 3.)

**Theorem 3.10** (Feit-Tits Theorem). Suppose \( G \) is a known simple non-abelian group that is not a group of Lie type in characteristic 2. Suppose \( G' \to G \) is a minimal cover of \( G \) and \( d \) is the smallest positive integer such that there exists a nontrivial homomorphism \( G' \to PGL(d, C) \). Then the kernel of each homomorphism \( G' \to PGL(d, C) \) contains \( \ker(\gamma) \). In particular, \( G \) is isomorphic to a subgroup of \( PGL(d, C) \).

**Remark 3.11.** Kleidman and Liebeck [1] studied the case of simple groups of Lie type in characteristic 2. In particular, they proved the following assertion (ibid, Th. 3 on p. 316). Suppose \( q \) is a power of 2 and \( m \geq 2 \) is an integer such that \((m, q) \neq (2, 2)\) (i.e., \( L_m(q) \) is a simple non-abelian group). If \( m \) is a positive integer and \( G' \) is a minimal cover of \( L_m(q) \) such that \( G' \) is isomorphic to a subgroup of \( PGL(g, C) \) then either \( m = 4 \) and \( g \geq q^3 \) or \( L_m(q) \) is isomorphic to a subgroup of \( PGL(g, C) \).

**Lemma 3.12.** Suppose \( q \geq 2 \) is an integral power of 2 and \( m \geq 2 \) is an integer such that \((m, q) \neq (2, 2), (2, 4), (3, 2), (4, 2)\). Suppose \( G' \) is a minimal cover of \( L_m(q) \).

(i) If \( m > 2 \) then \( G' \) is \( \frac{1}{2} \frac{(q^m - q)}{q - 1} \)-unbounded.

(ii) If \( m > 2 \) then \( G' \) is \( \frac{3}{2} \)-unbounded.

**Proof.** Let us start with the case of \( m = 2 \). Let us put \( g = \frac{q}{2} \). Let \( \rho : G' \to PGL(g, C) \) be a nontrivial group homomorphism. By Remark 3.3 the image \( \rho(G') \subset PGL(g, C) \) is also a minimal cover of \( L_2(q) \). Applying Remark 3.11 to \( \rho(G') \), we conclude that \( L_2(q) \) is isomorphic to a subgroup of \( PGL(g, C) \). By Example 3.4(c), this is not true. The obtained contradiction implies that there are no nontrivial homomorphisms from \( G' \) to \( PGL(g, C) \).

Now assume that \( m > 2 \). Let us put \( g = \frac{1}{2} \frac{(q^m - q)}{q - 1}. \) Notice that if \( m = 4 \) then

\[
g = \frac{1}{2}(q^3 + q^2 + q) < q^3.
\]
Let $\rho : G' \to \text{PGL}(g, \mathbb{C})$ be a nontrivial group homomorphism. Again, the image $\rho(G') \subset \text{PGL}(g, \mathbb{C})$ is also a minimal cover of $\text{L}_m(q)$. Applying Remark 3.11 to $\rho(G')$, we conclude that either $m = 4$ and $g \geq q^3$ or $\text{L}_m(q)$ is isomorphic to a subgroup of $\text{PGL}(g, \mathbb{C})$. But we have already seen that if $m = 4$ then $g < q^3$. This implies that $\text{L}_m(q)$ is isomorphic to a subgroup of $\text{PGL}(g, \mathbb{C})$. By Example 3.4(c), this is not true. The obtained contradiction implies that there are no nontrivial homomorphisms from $G'$ to $\text{PGL}(g, \mathbb{C})$.

\begin{lemma}
Suppose a simple non-abelian finite group $G$ and an integer $g > 1$ enjoy one of the following properties:

(a) $g = 11$ and $G = M_{23}$ or $M_{24}$;
(b) $g = 10$ and $G = M_{22}$;
(c) $g = 5$ and $G = M_{11}$ or $M_{12}$;
(d) $g = \left[\frac{q^m}{q-1} - 1\right]$ where $q \geq 3$ is an odd power prime, $m \geq 3$ is an integer and $G = \text{L}_m(q)$;
(e) $G = A_{2g+1}$ or $A_{2g+2}$.

If $G'$ is a minimal cover of $G$ then $G'$ is $g$-bounded.
\end{lemma}

\begin{proof}
Case (a). We have seen that there are no nontrivial homomorphisms to $\text{PSL}(11, \mathbb{C})$ either from $M_{23}$ or $M_{24}$. It follows from the Feit–Tits theorem that the same is true for the minimal cover $G'$.

Case (c). We have seen that there are no nontrivial homomorphisms to $\text{PSL}(5, \mathbb{C})$ either from $M_{11}$ or $M_{12}$. It follows from the Feit–Tits theorem that the same is true for the minimal cover $G'$.

Case (d). It follows from the Feit–Tits theorem combined with Example 3.4(d) that there are no nontrivial homomorphisms from $G'$ to $\text{PGL}(g, \mathbb{C})$.

Case (b). Since every homomorphism from $M_{22}$ to $\text{PSL}(9, \mathbb{C})$ is trivial, we conclude that, thanks to the Feit–Tits theorem, that every homomorphism from $G'$ to $\text{PSL}(9, \mathbb{C})$ is also trivial. In order to finish the proof we have to check that every homomorphism from $G'$ to $\text{PSL}(10, \mathbb{R})$ is also trivial. Let us assume that $\rho' : G' \to \text{PSL}(10, \mathbb{R}) = \text{SL}(10, \mathbb{R})/\{\pm 1\}$ is a nontrivial group homomorphism. Let us consider the composition $\pi : G' \overset{\rho'}{\longrightarrow} \text{PSL}(10, \mathbb{R}) \subset \text{PSL}(10, \mathbb{C})$ of $\rho'$ and the natural embedding $\text{PSL}(10, \mathbb{R}) \subset \text{PSL}(10, \mathbb{C})$. Clearly, the composition $\pi : G' \to \text{PSL}(10, \mathbb{C})$ is a nontrivial group homomorphism. Since $G'$ is a minimal cover of $M_{22}$ and 10 is the smallest dimension of a nontrivial projective representation of $M_{22}$ over $\mathbb{C}$, the Feit–Tits theorem implies that $\ker(\pi)$ contains $\ker(G' \to M_{22})$. Since the image of $\pi$ lies in $\text{PSL}(10, \mathbb{R}) \subset \text{PSL}(10, \mathbb{C})$, we conclude that $\pi$ gives rise to a nontrivial homomorphism $M_{22} \to \text{PSL}(10, \mathbb{R})$. Contradiction.

Case (e) follows easily from the Feit–Tits theorem combined with Examples 3.4 and Lemma 3.12.
\end{proof}

\begin{theorem}
Suppose $g > 1$ is an integer, $D$ a finite-dimensional semisimple $\mathbb{Q}$-algebra enjoying the following properties:

(i) Let us split $D$ into a direct sum $D = \oplus_{i=1}^r D_i$ of simple $\mathbb{Q}$-algebras $D_i$. Then the number $r$ of summands does not exceed $g$;
\end{theorem}
(ii) Let us present a summand $D_i$ as the algebra of square matrices of size $d_i$ over a division $\mathbb{Q}$-algebra $T_i$. Then every $T_i$ admits a positive involution. In addition,

$$\bigoplus_{i=1}^r d_i \leq g.$$ 

(iii) If $r = 1$ (i.e., $D = D_1$ is simple) then $n_1 \cdot \text{dim}_{\mathbb{Q}}(T_1)$ divides $2g$. In addition, the center of $D_1$ is either a totally real number field of degree dividing $g$ or a CM-field of degree dividing $2g$. Also, if $n_1 \cdot \text{dim}_{\mathbb{Q}}(T_1) = 2g$ and $T_1$ is a quaternion $\mathbb{Q}$-algebra then it is indefinite.

Suppose $H$ is a $g$-unbounded group and $\rho : H \to \text{Aut}(D)$ is a group homomorphism such that the subalgebra

$$D^H = \{ u \in D \mid \rho(h)u = u \quad \forall h \in H \}$$

of $H$-invariants coincides with $\mathbb{Q}$. Then $D = \mathbb{Q}$.

**Proof.** Let $C_i$ be the center of $D_i$. Then $C_i$ is either a totally real number field or a CM-field. Clearly,

$$C = \bigoplus_{i=1}^r C_i$$

is the center of $D$. This implies that $C$ is $H$-stable and the action of $H$ permutes $C_i$’s. This gives rise to a homomorphism from $H$ to the group $S_r$ of permutations in $r$ letters which must be trivial. Indeed, the perfectness of $H$ implies that its image in $S_r$ lies in the alternating subgroup $A_r$, which embeds into $\text{PSL}(r-1, \mathbb{C})$ if $r > 2$ and the inequality $r \leq g$ and the triviality of homomorphisms implies in this case that $H \to S_r$ is trivial. If $r \leq 2$ then $A_r$ is itself trivial. So, $H$ leaves stable each $C_i$. This implies easily that $\bigoplus_{i=1}^r Q$ consists of $H$-invariants. Since $D^H = \mathbb{Q}$, we conclude that $r = 1$ and therefore $D = D_1$ and $C = C_1$ is also the center of $M_1$. So, $C$ is either a totally real number field of degree dividing $g$ or a purely imaginary quadratic extension of a totally real number field $C^+$ where $[C^+ : \mathbb{Q}]$ divides $g$. In the case of totally real $C$ let us put $C^+ := C$. Clearly, in both cases $C^+$ is the largest totally real subfield of $C$ and therefore the action of $H$ leaves $C^+$ stable. Let us put $d := [C^+ : \mathbb{Q}]$. I claim that $d = 1$, i.e., $C^+ = \mathbb{Q}$. Indeed, suppose $d > 1$. Clearly, one may identify $\text{Aut}(H)$ with a subgroup of $GL(d-1, \mathbb{Q})$ and therefore the action of $H$ on $C^+$ gives us a homomorphism

$$H \to \text{Aut}(C^+) \subset GL(d-1, \mathbb{Q}),$$

whose triviality we need to check. Assume the contrary. The perfectness of $H$ implies that the nontrivial image of the composition $H \to GL(d-1, \mathbb{Q})$ is, in fact, a perfect subgroup of $SL(d-1, \mathbb{Q})$. This perfectness implies, in turn, that the image of $H$ in $\text{PSL}(d-1, \mathbb{Q})$ is also nontrivial. Taking into account the inequality $d \leq g$ and the inclusion $\text{PSL}(d-1, \mathbb{Q}) \subset \text{PSL}(d-1, \mathbb{C})$, we obtain a nontrivial homomorphism $H \to \text{PSL}(d-1, \mathbb{C})$. This contradicts to the $g$-unboundedness of $H$. Hence $d = 1$ and $C^+ = \mathbb{Q}$.

Now I claim that $C = \mathbb{Q}$. Indeed, if $C \neq \mathbb{Q}$ then $C$ is an imaginary quadratic field and $\text{Aut}(C)$ is a cyclic group of order 2. The perfectness of $H$ implies that $H \to \text{Aut}(C)$ is trivial and therefore $C$ consists of $H$-invariants. Since $D^H = \mathbb{Q}$, we get a contradiction. Hence $C = \mathbb{Q}$.

So, $T_1$ is a central simple $\mathbb{Q}$-algebra with a positive involution. Hence either $T_1 = \mathbb{Q}$ or a quaternion $\mathbb{Q}$-algebra.

Assume that $T_1 = \mathbb{Q}$. Then $D = D_1$ is the matrix algebra of size $d_1$ over $\mathbb{Q}$. Clearly, $d_1 \leq g$. By Skolem-Noether theorem, $\text{Aut}(D)$ is $\text{PGL}(d_1, \mathbb{Q})$. So, perfect $H$
acts on \(D\) via \(\rho : H \to \text{Aut}(D) = \text{PGL}(d_1, \mathbb{Q})\), whose image must lie in \(\text{PSL}(d_1, \mathbb{Q})\). Since \(d_1 \leq g\), \(\text{PSL}(d_1, \mathbb{Q})\) is a subgroup of \(\text{PSL}(g, \mathbb{Q})\), we obtain the triviality of \(\rho : H \to \text{Aut}(D) = \text{PGL}(d_1, \mathbb{Q}) \subset \text{PSL}(g, \mathbb{Q})\). This implies that the whole \(D\) consists of \(H\)-invariants. Since \(D^H = \mathbb{Q}\), we conclude that \(D = \mathbb{Q}\).

Now assume that \(T_1\) is a quaternion \(\mathbb{Q}\)-algebra. Then \(D \neq \mathbb{Q}\) and therefore \(\rho : H \to \text{Aut}(D)\) is nontrivial. We need to arrive to a contradiction.

We have \(\dim_{\mathbb{Q}}(D_1) = 4\) and \(4n_1 \leq 2g\).

Assume that \(4n_1 = 2g\). Then \(g = 2n_1\) is even and \(T_1 \otimes_{\mathbb{Q}} \mathbb{R}\) is isomorphic to the matrix algebra of size 2 over \(\mathbb{R}\). This implies that \(D_{\mathbb{R}} := D \otimes_{\mathbb{Q}} \mathbb{R}\) is the matrix algebra of size \(g\) and

\[
\text{Aut}(D) \subset \text{Aut}_{\mathbb{R}}(D_{\mathbb{R}}) = \text{PGL}(g, \mathbb{R}).
\]

Therefore the nontrivial \(\rho\) gives rise to a nontrivial homomorphism \(H \to \text{PGL}(g, \mathbb{R})\). Again, the perfectness of \(H\) implies that the image lies in \(\text{PSL}(g, \mathbb{R})\) and we get a nontrivial homomorphism \(H \to \text{PSL}(g, \mathbb{R})\). Contradiction.

Assume that \(4n_1 < 2g\). Then \(D_{\mathbb{C}} := D \otimes_{\mathbb{Q}} \mathbb{C}\) is the matrix algebra over \(\mathbb{C}\) of size \(2n_1 < g\) and

\[
\text{Aut}(D) \subset \text{Aut}_{\mathbb{C}}(D_{\mathbb{C}}) = \text{PGL}(2n_1, \mathbb{C}).
\]

Therefore the nontrivial \(\rho\) gives rise to a nontrivial homomorphism \(H \to \text{PGL}(g - 1, \mathbb{C})\). Again, the perfectness of \(H\) implies that the image of \(H\) lies in \(\text{PSL}(g - 1, \mathbb{C})\) and we get a nontrivial homomorphism \(H \to \text{PSL}(g - 1, \mathbb{C})\). Contradiction.

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 us consider the permutation module \(\mathbb{F}_2^B\): the \(\mathbb{F}_2\)-vector space of all functions \(\varphi : B \to \mathbb{F}_2\). The space \(\mathbb{F}_2^B\) carries a natural structure of \(\text{Perm}(B)\)-module and contains the stable line \(\mathbb{F}_2 \cdot 1_B\) of constant functions and the stable hyperplane \((\mathbb{F}_2^B)^0\) of functions \(\varphi\) with \(\sum_{\alpha \in B} \varphi(\alpha) = 0\). Clearly, \((\mathbb{F}_2^B)^0\) contains \(\mathbb{F}_2 \cdot 1_B\) if and only if \(n\) is even. Let us put \(Q_B := (\mathbb{F}_2^B)^0\) if \(n\) is odd and \(Q_B := (\mathbb{F}_2^B)^0/(\mathbb{F}_2 \cdot 1_B)\) if \(n\) is even. Clearly, \(Q_B\) carries a natural structure of faithful \(\text{Perm}(B)\)-module. For each permutation group \(H \subset \text{Perm}(B)\) the corresponding \(H\)-module is called the heart of the permutation representation of \(H\) on \(B\) over \(\mathbb{F}_2\).

**Lemma 3.15.** \(\text{End}_H(Q_B) = \mathbb{F}_2\) if either \(n\) is odd and \(H\) acts 2-transitively on \(B\) or \(n\) is even and \(H\) acts 3-transitively on \(B\).

**Proof.** See Satz 4 in [3].

**Lemma 3.16.** Suppose \(q > 2\) is an integral odd power prime, \(m \geq 3\) is an integer, \(B = \mathbb{P}^{m-1}(\mathbb{F}_q)\) is the corresponding \((m - 1)\)-dimensional projective space over the finite field \(\mathbb{F}_q\) and \(H = \text{L}_m(q) = \text{PSL}_m(\mathbb{F}_q) \subset \text{Perm}(B)\) is the corresponding projective special linear group over \(\mathbb{F}_q\) acting naturally and faithfully on the projective space. Then the \(H\)-module \(Q_B\) is absolutely simple. In particular, \(\text{End}_H(Q_B) = \mathbb{F}_2\).

**Proof.** See [1], Table 1 on page 2.
Remark 3.17. Suppose \( q = 2^r \) is an integral power of 2 and \( m \geq 2 \) is an integer such that either \( m \geq 3 \) or \( q > 4 \). Suppose \( B = \mathbb{P}^{m-1}(\mathbb{F}_q) \) is the corresponding \((m-1)\)-dimensional projective space over the finite field \( \mathbb{F}_q \) and \( H = \mathbb{L}_m(q) = \text{PSL}_m(\mathbb{F}_q) \subset \text{Perm}(B) \) is the corresponding projective special linear group over \( \mathbb{F}_q \) acting naturally and faithfully on the projective space. Then \( \text{End}_H(Q_B) = \mathbb{F}_2 \). Indeed, it is well-known that \( H = \text{PSL}_m(\mathbb{F}_q) \) acts doubly transitively on \( B = \mathbb{P}^{m-1}(\mathbb{F}_q) \). Clearly, \( \#(B) = \frac{2^m-1}{q-1} \) is odd and therefore the assertion follows from Lemma 3.15. Notice that if \( m \geq 3 \) then the \( H \)-module \( Q_B \) is reducible \([11] \); see §5 of [3] for details. If \( m = 2 \) then the \( H \)-module \( Q_B \) is absolutely simple \([11] \) (and even very simple \([21] \)).

4. Endomorphisms of abelian varieties

Let \( K \) be a field of characteristic zero. We fix its algebraic closure \( K_a \) and write \( \text{Gal}(K) \) for the absolute Galois group \( \text{Aut}(K_a/K) \). Let \( X \) be an abelian variety of positive dimension defined over \( K \). Then the group \( X(K_a) \) of its algebraic points has a natural structure of \( \text{Gal}(K) \)-module. If \( m \) is a positive integer then we write \( X_m \) for the kernel of multiplication by \( m \) in \( X(K_a) \). It is well-known \([12] \) that \( X_m \) is a free \( \mathbb{Z}/m\mathbb{Z} \)-module of rank \( 2\dim(X) \) provided with the structure of \( \text{Gal}(K) \)-module inherited from \( X(K_a) \). We denote by \( \tilde{\rho}_{m,X} \) the corresponding homomorphism

\[
\tilde{\rho}_{m,X} : \text{Gal}(K) \to \text{Aut}(X_m) \cong \text{GL}(2\dim(X), \mathbb{Z}/m\mathbb{Z})
\]

which defines the structure of Galois module on \( X_m \). We have

\[
\tilde{\rho}_{m,X}(\sigma)(x) = \sigma(x) \quad \forall \sigma \in \text{Gal}(K), x \in X_m \subset X(K_a).
\]

We write

\[
\tilde{G}_{m,X,K} = \tilde{\rho}_{m,X}(\text{Gal}(K))
\]

for the image of \( \text{Gal}(K) \) in \( \text{Aut}(X_m) \). If \( K(X_m) \) is the field of definition of all points of order \( m \) on \( X \) then it is a finite Galois extension of \( K \), whose Galois group \( \text{Gal}(K(X_m)/K) = \tilde{G}_{m,X,K} \).

Suppose \( m > 1 \). Clearly, \( X_m = mX_{m^2} \) coincides with the kernel of multiplication by \( m \) in \( X_{m^2} \). In particular, every endomorphism of the commutative group \( X_{m^2} \) leaves \( X_m \) stable. Therefore the restriction to \( X_m \) gives rise to a natural (obviously surjective) ring homomorphism (the reduction modulo \( m \))

\[
\text{red}_m : \text{End}(X_{m^2}) \to \text{End}(X_m) ; \quad \text{red}_m(u)(x) = ux \quad \forall u \in \text{End}(X_{m^2}), x \in X_m.
\]

Clearly, \( \ker(\text{red}_m) = m\text{End}(X_{m^2}) \). This implies that each \( v \in \ker(\text{red}_m) \) satisfies \( v^2 = 0 = mv \).

Restricting \( \text{red}_m \) to the automorphism group \( \text{Aut}(X_{m^2}) \) of \( X_{m^2} \), we obtain the (obviously surjective) group homomorphism

\[
\text{red}_m^* : \text{Aut}(X_{m^2}) \to \text{Aut}(X_m) ; \quad \text{red}_m^*(u)(x) = ux \quad \forall u \in \text{Aut}(X_{m^2}), x \in X_m.
\]

Clearly, \( \ker(\text{red}_m^*) = \text{Id} + m\text{End}(X_{m^2}) \). (Here \( \text{Id} \) is the identity automorphism of \( X_{m^2} \).) This implies that each \( u \in \ker(\text{red}_m^*) \) is of the form \( \text{Id} + v \) with \( v^2 = 0 = mv \). This implies that \( u^m = \text{Id} \).

Remark 4.1. Notice that the homomorphisms \( \text{red}_m \) and \( \text{red}_m^* \) do not depend on the choice of the field of definition \( K \) for \( X \). In particular, they both are \( \text{Gal}(K) \)-equivariant.
Clearly,
\[ \tilde{\rho}_{m^2,X} = \text{red}^*_m \rho_{m,X}; \]
in particular,
\[ \tilde{G}_{m,X,K} = \text{red}^*_m (\tilde{G}_{m^2,X,K}). \]

There is an important special case when \( m = \ell \) is a prime. Then \( X_m = X_\ell \) is a \( 2\dim(X) \)-dimensional \( F_\ell \)-vector space provides with the structure of Gal\((K)\)-module inherited from \( X(K_a) \). We have \( u^\ell = \text{Id} \) for each \( u \in \ker(\text{red}_\ell^*) \) and therefore the exponent of the nontrivial finite group \( \ker(\text{red}_\ell^*) \) is \( \ell \). We also have
\[ \tilde{G}_{\ell,X,K} = \text{red}^*_\ell (\tilde{G}_{\ell^2,X,K}) \]
and therefore the kernel of the surjective group homomorphism
\[ \text{red}^*_\ell : \tilde{G}_{\ell^2,X,K} \rightarrow \tilde{G}_{\ell,X,K} \]
is either trivial or a finite group of exponent \( \ell \).

**Remark 4.2.** Assume that \( \tilde{G}_{\ell,X,K} \) contains a simple non-abelian subgroup \( G \). Let \( H \subset \tilde{G}_{\ell^2,X,K} \) be the preimage of \( G \) with respect to \( \text{red}^*_\ell : \tilde{G}_{\ell,X,K} \rightarrow \tilde{G}_{\ell,X,K} \).

Clearly, \( \text{red}^*_\ell : H \rightarrow G \) is a surjective homomorphism, whose kernel is either trivial or has exponent \( \ell \). According to Remark 3.8 there exists a subgroup \( G' \subset H \subset \tilde{G}_{\ell^2,X,K} \) such that \( \text{red}^*_\ell : G' \rightarrow G \) is a minimal \( \ell \)-cover.

We write \( \text{End}(X) \) for the ring of all \( K_a \)-endomorphisms of \( X \) and \( \text{End}_K(X) \) for the ring of all \( K \)-endomorphisms of \( X \). We have
\[ Z = Z \cdot \text{Id}_X \subset \text{End}_K(X) \subset \text{End}(X) \]
where \( \text{Id}_X \) is the identity automorphism of \( X \).

Since \( X \) is defined over \( K \), one may associate with every \( u \in \text{End}(X) \) and \( \sigma \in \text{Gal}(K) \) an endomorphism \( \sigma u \in \text{End}(X) \) such that
\[ \sigma u(x) = \sigma u(\sigma^{-1}x) \quad \forall x \in X(K_a). \]

In fact, there is a group homomorphism
\[ \kappa_X : \text{Gal}(K) \rightarrow \text{Aut}(\text{End}(X)); \quad \kappa_X(\sigma)(u) = \sigma u \quad \forall \sigma \in \text{Gal}(K), u \in \text{End}(X). \]

It is well-known that \( \text{End}_K(X) \) coincides with the subring of \( \text{Gal}(K) \)-invariants in \( \text{End}(X) \), i.e.,
\[ \text{End}_K(X) = \{ u \in \text{End}(X) \mid \sigma u = u \quad \forall \sigma \in \text{Gal}(K) \}. \]

It is also well-known, that \( \text{End}(X) \), viewed as a group (with respect to addition) is a free commutative group of finite rank and \( \text{End}_K(X) \) is its pure subgroup, i.e., the
Remark 4.3. It is proven in [13] that all the endomorphisms of \( \ker(X) \) are defined over \( K \), i.e.,
\[
\text{Gal}(K') \subseteq \ker(\kappa_X) \subset \text{Gal}(K).
\]

Remark 4.4. (i) Let us put \( \text{End}^0(X) := \text{End}(X) \otimes \mathbb{Q} \). It is well-known (¶21) that \( \text{End}^0(X) \) is a semisimple finite-dimensional \( \mathbb{Q} \)-algebra. Clearly, the natural map
\[
\text{Aut}(\text{End}(X)) \to \text{Aut}(\text{End}^0(X))
\]
is an embedding.

(ii) Recall that \( X \) is isogenous over \( K_a \) to a product \( \prod_{i=1}^r Y_i^{d_i} \) where \( Y_i \)'s are mutually non-isogenous absolutely simple abelian varieties (of positive dimension) over \( K_a \). Then
\[
g = \dim(X) = \sum_{i=1}^r d_i \cdot \dim(Y_i) \geq \sum_{i=1}^r d_i.
\]

Let us put \( T_i := \text{End}^0(Y_i) \) and denote by \( D_i \) the algebra of square matrices of size \( d_i \) over \( T_i \). Then each \( T_i \) is a division \( \mathbb{Q} \)-algebra admitting a positive involution (¶21). Let us denote by \( C_i \) the center of \( T_i \). Then either \( C_i \) is a totally real number field and \([C_i : \mathbb{Q}]\) divides \( \dim(Y_i) \) or \( C_i \) is a CM-field and \([C_i : \mathbb{Q}]\) divides \( 2\dim(Y_i) \). It is also clear that \( C_i \) is the center of \( D_i \).

Since \( \text{char}(K_a) = 0 \), the number \( \dim_{\mathbb{Q}}(T_i) \) divides \( 2\dim(Y_i) \) (¶21, p. 202). Clearly, \( D_i = \text{End}^0(Y_i^{d_i}) \) and
\[
\text{End}^0(X) = \oplus_{i=1}^r D_i.
\]

(iii) Assume now that \( r = 1 \), i.e., \( X \) is isogenous to \( Y_1^{d_1} \) and \( \text{End}^0(X) = D_1 \). Then
\[
g = \dim(X) = d_1 \cdot \dim(Y_1).
\]

Hence either \( C_1 \) is totally real number field and \([C_1 : \mathbb{Q}]\) divides \( g \) or \( C_1 \) is a CM-field and \([C_1 : \mathbb{Q}]\) divides \( 2g \). It is also clear that \( d_1 \cdot \dim_{\mathbb{Q}}(T_1) \) divides \( d_1 \cdot 2\dim(Y_1) = 2\dim(X) = 2g \). If \( C_1 = \mathbb{Q} \) then \( T_1 \) is either \( \mathbb{Q} \) or a quaternion \( \mathbb{Q} \)-algebra.

(iv) We continue to assume that \( r = 1 \). If \( T_1 \) a quaternion \( \mathbb{Q} \)-algebra and \( d_1 \cdot \dim_{\mathbb{Q}}(T_1) = 2g \) then, taking into account that \( \dim_{\mathbb{Q}}(T_1) = 4 \), we conclude that \( g \) is even, \( d_1 = g/2 \) and \( Y_1 \) is an absolutely simple abelian surface. Since in characteristic zero the endomorphism algebra of an absolutely simple abelian surface is either a field or an indefinite quaternion \( \mathbb{Q} \)-algebra (see also [14]), we conclude that \( T_1 = \text{End}^0(Y_1) \) is an indefinite quaternion \( \mathbb{Q} \)-algebra.
Theorem 4.5. Suppose $K$ is a field of characteristic 0, suppose $X$ is an abelian variety over a $K$ of dimension $g > 1$. Suppose $\ell$ is a prime, 

$$\tilde{G}_{\ell,X,K} = \tilde{\rho}_{\ell,X}(\text{Gal}(K)) \subset \text{Aut}(X_{\ell})$$

is the image of $\text{Gal}(K)$ in $\text{Aut}(X_{\ell})$. Let us put $g = \dim(X)$ and assume that $g > 1$ (i.e., $X$ is not an elliptic curve). Assume that $\tilde{G}_{\ell,X,K}$ contains a simple non-abelian subgroup $G$ such that

$$\text{End}_G(X_{\ell}) = F_{\ell}$$

and one of the following conditions holds:

(a) $\ell$ is odd and $G$ is $g$-unbounded.

(b) $\ell = 2$ and every 2-minimal cover of $G$ is $g$-unbounded.

Then the ring $\text{End}(X)$ of all $K_a$-endomorphisms of $X$ coincides with $\mathbb{Z}$.

Proof. First, using Remark 4.2 we may replace $K$ by its finite separable algebraic extension $L$ in such a way that $\tilde{G}_{\ell,X,L} = G$ and

$$\text{red}_{L}^{\ast} : \tilde{G}_{\ell,X,L} \hookrightarrow \tilde{G}_{\ell,X,L} = G$$

is a minimal $\ell$-cover. Clearly, $\tilde{G}_{\ell,X,L}$ is $g$-unbounded if $\ell$ is odd. If $\ell = 2$ then it follows from Remark 4.2 that $\tilde{G}_{\ell,X,L}$ is a minimal 2-cover of $\tilde{G}_{2,X,L} = G$ and therefore is $g$-unbounded.

Second, I claim that $\text{End}_L(X) = \mathbb{Z}$. Indeed, it is well-known that there is an embedding

$$\text{End}_L(X) \otimes \mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \text{End}_{\text{Gal}(K)}(X_{\ell}).$$

On the other hand, since $\rho_{\ell,X}(\text{Gal}(L)) = \tilde{G}_{\ell,X,L},$

$$\text{End}_{\text{Gal}(K)}(X_{\ell}) = \text{End}_{\tilde{G}_{\ell,X,L}}(X_{\ell}) = \text{End}_G(X_{\ell}) = F_{\ell},$$

the rank of free commutative group $\text{End}_L(X)$ is either 0 or 1. Clearly, it must be 1 and this implies that $\text{End}_L(X) = \mathbb{Z}$.

Now let us put $D := \text{End}^{0}(X)$. Clearly, $\text{End}(X)$ is a $\mathbb{Z}$-lattice in the $\mathbb{Q}$-vector space $D$. Let $\text{Aut}(D)$ be the group of automorphisms of the $\mathbb{Q}$-algebra $D$. We have $\text{Aut}(\text{End}(X)) \subset \text{Aut}(D)$. We have

$$\kappa_{X}(\text{Gal}(L)) = \Gamma_L \subset \text{Aut}(\text{End}(X)) \subset \text{Aut}(D).$$

Clearly, we have

$$D^{\Gamma_{L}} = \text{End}(X)^{\Gamma_{L}} \otimes \mathbb{Q} = \text{End}_L(X) \otimes \mathbb{Q} = \mathbb{Z} \otimes \mathbb{Q} = \mathbb{Q}.$$  

We are going to finish the proof, using Theorem 3.14. Let us put $H := \tilde{G}_{\ell,X,L}$ if $\ell$ is odd and $H := \tilde{G}_{4,X,L}$ if $\ell = 2$. Clearly, in both cases $H$ is $g$-unbounded. Thanks to Remark 4.3 there exists a surjective homomorphism

$$\rho : H \twoheadrightarrow \Gamma_{L} \subset \text{Aut}(D).$$

Clearly, $D^{H} = D^{\Gamma_{L}} = \mathbb{Q}$.

In light of Remark 4.4 the semisimple $\mathbb{Q}$-algebra $D = \text{End}^{0}(X)$ satisfies all the conditions of Theorem 3.14 with $g = \dim(X)$. Applying Theorem 3.14 we conclude that $D = \mathbb{Q}$, i.e., $\text{End}^{0}(X) = \mathbb{Q}$ and therefore $\text{End}(X) = \mathbb{Z}$. \qed
5. Hyperelliptic Jacobians

Theorem 5.1. Let $K$ be a field of characteristic zero, $K_a$ its algebraic closure, $f(x) \in K[x]$ a polynomial of degree $n \geq 5$ and $\mathfrak{R} \subset K_a$ the set of its roots. Let $K(\mathfrak{R}) \subset K_a$ be the splitting field of $f$ and $\text{Gal}(f) := \text{Gal}(K(\mathfrak{R})/K)$ the Galois group of $f$, viewed as a subgroup of of the group $\text{Perm}(\mathfrak{R})$ of all permutations of $\mathfrak{R}$. Suppose $\text{Gal}(f)$ contains a simple non-abelian group $\mathcal{G}$ enjoying one of the following two properties:

(i) $n$ is odd and $\mathcal{G}$ acts 2-transitively on $\mathfrak{R}$. In addition, every 2-minimal cover of $\mathcal{G}$ is $\frac{n-1}{2}$-bounded.

(ii) $n$ is even and $\mathcal{G}$ acts 3-transitively on $\mathfrak{R}$. In addition, every 2-minimal cover of $\mathcal{G}$ is $\frac{n-2}{2}$-bounded.

(iii) $n$ is even and $\text{End}_\mathcal{G}(Q_\mathfrak{R}) = F_2$. In addition, every 2-minimal cover of $\mathcal{G}$ is $\frac{n-2}{2}$-bounded.

Let $J(C_f)$ be the jacobian of the hyperelliptic curve $C = C_f : y^2 = f(x)$. Then the ring $\text{End}(J(C_f))$ of all $K_a$-endomorphisms of $J(C_f)$ coincides with $\mathbb{Z}$.

Proof. Suppose $f(x) \in K[x]$ is a polynomial of degree $n \geq 5$ without multiple roots and $X := J(C_f)$ is the jacobian of $C = C_f : y^2 = f(x)$. It is well-known that $g := \text{dim}(X) = \frac{n-1}{2}$ if $n$ is odd and $g := \text{dim}(X) = \frac{n-2}{2}$ if $n$ is even. It is also well-known (see for instance Sect. 5 of [21]) that $\tilde{G}_{2,X,K} \cong \text{Gal}(f)$. More precisely, let $K(\mathfrak{R})$ be the splitting field of $f$ and $\text{Gal}(f) := \text{Gal}(K(\mathfrak{R})/K)$ the Galois group of $f$, viewed as a subgroup of of the group $\text{Perm}(\mathfrak{R})$ of all permutations of $\mathfrak{R}$. We have

$$\text{Gal}(f) \subset \text{Perm}(\mathfrak{R})$$

and the action of $\text{Gal}(f)$ on $\mathfrak{R}$ is transitive if and only if $f$ is irreducible.

Now let us consider the heart (end of [1]) of the permutation representation of $\text{Gal}(f)$ on $\mathfrak{R}$: the faithful $\text{Gal}(f)$-module $Q_\mathfrak{R}$. It is well-known (see for instance, Th. 5.1 on p. 478 of [21]) that the homomorphism $\rho_{2,X} : \text{Gal}(K) \rightarrow \text{Aut}(X_2)$ factors through the canonical surjection $\text{Gal}(K) \twoheadrightarrow \text{Gal}(K(\mathfrak{R})/K) = \text{Gal}(f)$ and the $\text{Gal}(f)$-modules $X_2$ and $Q_\mathfrak{R}$ are isomorphic. In particular,

$$\text{Gal}(f) = \rho_{2,X}(\text{Gal}(K)) = \tilde{G}_{2,X,K}.$$

Now assume that $f$ satisfies the conditions of Theorem 5.1 and let us put

$$H := \mathcal{G} \subset \text{Gal}(f) \subset \text{Perm}(\mathfrak{R}) \subset \text{Aut}(Q_\mathfrak{R}) = \text{Aut}(X_2).$$

It follows easily from Lemma 3.15 that we always have

$$\text{End}_\mathcal{G}(X_2) = \text{End}_H((Q_\mathfrak{R})) = F_2.$$

Now the assertion of Theorem 5.1 follows readily from Theorem 4.3. \qed

Proof of Theorem 2.4. It is well-known that all Mathieu groups $M_n \subset S_n$ are, at least, 3-transitive permutation groups. Now Theorem 4.1 becomes an immediate corollary of Theorem 5.1 combined with Lemma 3.13 (a-c). \qed

Proof of Theorem 2.3. Recall that $q$ is a power of 2. It is well-known that $\text{L}_m(q) = \text{PSl}_m(\mathbb{F}_q)$ acts doubly transitively on $\mathbb{P}^{m-1}(\mathbb{F}_q) = \mathfrak{R}$. It is also clear that $n = \#(\mathbb{P}^{m-1}(\mathbb{F}_q)) = \frac{q^m-1}{q-1}$ is odd. Now Theorem 2.3 becomes an immediate corollary of Theorem 5.1 combined with Examples 3.9 and Lemma 3.12. \qed
Proof of Theorem 2.3. It is an immediate corollary of Theorem 5.1 combined with Lemma 3.13(d) and Lemma 3.16. (Notice that in this case one may check that the Gal($f$)-module $J(C_f)_2$ is very simple.)

Remark 5.2. Combining Remark 3.13(e) and Lemma 3.15 with Theorem 5.1, we obtain immediately that $\text{End}(J(C_f)_2) = \mathbb{Z}$ if $n \geq 5$ and Gal($f$) contains $A_n$. This assertion was proven by a different method (based on the very simplicity of $J(C_f)_2$) in [20].

References

[1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups. Clarendon Press, Oxford, 1985.
[2] W. Feit, J. Tits, Projective representations of minimum degree of group extensions. Canad. J. Math. 30 (1978), 1092–1102.
[3] A. A. Ivanov, Ch. E. Praeger, On finite affine 2-Arc transitive graphs. Europ. J. Combinatorics 14 (1993), 421–444.
[4] 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.
[5] N. Katz, Affine cohomological transforms, perversity, and monodromy. J. Amer. Math. Soc. 6 (1993), 149–222.
[6] P. B. Kleidman, M. W. Liebeck, On a theorem of Feit and Tits. Proc. AMS 107 (1989), 315–322.
[7] M. Klemm, Über die Reduktion von Permutationsmoduln. Math. Z. 143 (1975), 113–117.
[8] 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.
[9] Sh. Mori, The endomorphism rings of some abelian varieties. II. Japanese J. Math, 2(1976), 109–130.
[10] Sh. Mori, The endomorphism rings of some abelian varieties. II. Japanese J. Math, 3(1977), 105–109.
[11] B. Mortimer, The modular permutation representations of the known doubly transitive groups. Proc. London Math. Soc. (3) 41 (1980), 1–20.
[12] D. Mumford, Abelian varieties, Second edition, Oxford University Press, London, 1974.
[13] F. Oort, Endomorphism algebras of abelian varieties. Algebraic Geometry and Commutative Algebra in Honor of M. Nagata (1987, Ed. H. Hijikata et al), Kinokuniya Cy, Tokyo 1988; Vol. II, pp. 469 - 502.
[14] F. Oort, Yu. G. Zarhin, Endomorphism algebras of complex tori. Math. Ann. 303 (1995), 11-29.
[15] A. Silverberg, Fields of definition for homomorphisms of abelian varieties. J. Pure Appl. Algebra 77 (1992), 253–262.
[16] A. Silverberg, Yu. G. Zarhin, Variations on a theme of Minkowski and Serre. J. Pure and Applied Algebra 111 (1996), 285–302.
[17] M. Suzuki, Group Theory I. Springer-Verlag, 1982.
[18] Pham Huu Tiep, A. E. Zalesskii, Minimal characters of the finite classical groups. Comm. Algebra 24(1996), 2093–2167.
[19] A. Wagner, The faithful linear representations of $S_n$ and $A_n$ over a field of characteristic 2. Math. Z. 151 (1976), 127–137.
[20] Yu. G. Zarhin, Hyperelliptic jacobians without complex multiplication. Math. Res. Letters 7 (2000), 123–132.
[21] 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.
[22] Yu. G. Zarhin, Hyperelliptic jacobians without complex multiplication in positive characteristic. Math. Res. Letters 8 (2001), 429–435.
[23] Yu. G. Zarhin, *Cyclic covers of the projective line, their jacobians and endomorphisms*, http://xxx.lanl.gov/abs/math.AG/0003002, to appear in J. reine angew. Math.

[24] Yu. G. Zarhin, *Hyperelliptic jacobians and simple groups $U_3(2^m)$*. Proc. AMS, to appear.

[25] Yu. G. Zarhin, *Very simple 2-adic representations and hyperelliptic jacobians*, http://arXiv.org/abs/math.AG/0109014.

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

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

_E-mail address_: zarhin@math.psu.edu