DEL PEZZO SURFACES OF DEGREE 1 AND JACOBIANS

YU. G. ZARHIN

1. Introduction

Let K be a field of characteristic zero, $\bar{K}$ its algebraic closure and $\mathrm{Gal}(K) = \mathrm{Aut}(\bar{K}/K)$ its absolute Galois group.

In [26] the author constructed explicitly g-dimensional abelian varieties (jacobians) without non-trivial endomorphisms for every $g > 1$. This construction may be described as follows. Let $n = 2g + 1$ or $2g + 2$. Let us choose an n-element set $\mathfrak{R} \in \bar{K}$ that constitutes a Galois orbit over K and assume, in addition, that the Galois group of $K(\mathfrak{R})$ over K coincides either with the full symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$. Let $f(x) \in K[x]$ be the irreducible polynomial of degree n, whose set of roots coincides with $\mathfrak{R}$. Let us consider the genus g hyperelliptic curve $C_f : y^2 = f(x)$ over $\bar{K}$ and let $J(C_f)$ be its jacobian, which is the g-dimensional abelian variety. Then the ring $\mathrm{End}(J(C_f))$ of all $\bar{K}$-endomorphisms of $J(C_f)$ coincides with $\mathbb{Z}$.

It is well-known that every genus 2 curve is hyperelliptic. However, there is a plenty of non-hyperelliptic genus 3 curves: namely, a curve of genus 3 is non-hyperelliptic if and only if it is isomorphic to a smooth plane quartic. So, one may ask for a natural construction of such quartics, whose jacobians have no nontrivial endomorphisms. In order to do that, suppose that we are given seven $\bar{K}$-points on the projective plane *in general position*, i.e., no three points lie on a one line and no six on a one conic. Assume also that $\mathrm{Gal}(K)$ permutes those seven points transitively. By blowing them up, we obtain a Del Pezzo surface of degree 2 that is defined over K ([11, §3], [3, Th. 1 on p. 27]). Suppose that the 7-element Galois orbit has *large* Galois group, namely, either $\mathbf{S}_7$ or the alternating group $\mathbf{A}_7$. It is proven in [30] that if we consider the anticanonical map of the Del Pezzo surface onto the projective plane then the jacobian of the corresponding branch curve has no nontrivial endomorphisms over $\bar{K}$. (Recall [4, Ch. VII, Sect. 4] that this curve is a smooth plane quartic.) Also, starting with an irreducible degree 7 polynomial with large Galois group, we provided an explicit construction of a 7-element Galois orbit in general position and with the same Galois group. (If one starts with an irreducible quartic polynomial $f(x)$ over K with Galois group $\mathbf{S}_4$ and consider a smooth plane quartic $C_{f,3} : y^3 = f(x)$ then it turns out that the endomorphism ring of its jacobian is $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ if K contains $\sqrt{-3}$) [31].)

The aim of this paper is to prove a similar result while dealing with eight points, Del Pezzo surfaces of degree 1 and their branch curves with respect to bi-anticanonical maps. (In this case the curve involved is a (non-hyperelliptic) genus 4 curve with vanishing theta characteristic [3, 4]). Notice that Del Pezzo surfaces of degree 1 do depend on 8 "parameters" while the moduli space of genus 4 curves

Supported by SFB 701 "Spektrale Strukturen und topologische Methoden in der Mathematik" (Fakultät für Mathematik der Universität Bielefeld).

has dimension 9. So, it is not *apriori* obvious (at least, to the author) why there exists (even over the field $\mathbb{C}$ of complex numbers) a degree 1 Del Pezzo surface with simple jacobian of its branch curve.

We prove that the endomorphism algebra of the corresponding jacobian (over $\bar{K}$) is either $\mathbb{Q}$ or a quadratic field; in particular, the jacobian is an absolutely simple abelian fourfold. Also, starting with an irreducible degree 8 polynomial with large Galois group (S_8 or A_8), we provide an explicit construction of a 8-element Galois orbit with the same Galois group and in general position. (In the case of *eight* points, we have to check additionally that there is no cubic that contains all the points and one of those points is singular on the cubic [11, Sect. 3], [3, Th. 1 on p. 27]). In particular, we prove the following statement.

Theorem 1.1. *Let $f(t) \in K[t]$ be an irreducible degree 8 polynomial, whose Galois group is either $\mathbf{S}_8$ or $\mathbf{A}_8$. Let $\mathfrak{R} \subset K_a$ be the set of roots of f. Then:*

(i) *the 8-element set*

$$B(h) = \{(\alpha^3 : \alpha : 1) \in \mathbb{P}^2(K_a) \mid \alpha \in \mathfrak{R}\}$$

is in general position.

(ii) *Let $S_{B(f)}$ be the Del Pezzo surfaces of degree 1 obtained by blowing up the points of $B(f)$. Let $C_{B(f)}$ be the branch curve of $S_{B(f)}$ with respect to its bi-anticanonical map. Let $J(C_{B(f)})$ be the jacobian of $C_{B(f)}$. Then the endomorphism algebra $\mathrm{End}^0(J(C_{B(f)}))$ of $J(C_{B(f)})$ (over $\bar{K}$) is either $\mathbb{Q}$ or a quadratic field; in particular, $J(C_{B(f)})$ is an absolutely simple abelian fourfold.*

(3) *Let $h(t) \in K[t]$ be another irreducible degree 8 polynomial, whose Galois group is either $\mathbf{S}_8$ or $\mathbf{A}_8$. Assume that the splitting fields of f and h are linearly disjoint over K. Then $J(C_{B(f)})$ and $J(C_{B(h)})$ are not isomorphic as abelian varieties over $\bar{K}$ and therefore the surfaces $S_{B(f)}$ and $S_{B(h)}$ are not biregularly isomorphic over over $\bar{K}$.*

Example 1.2. If $K = \mathbb{Q}$ and $f_1(x) = x^8 - x - 1$ then the Galois group of f_1 is $\mathbf{S}_8$ [24, p. 45, Rem. 2]. Clearly, $S_{B(f_1)}$, $C_{B(f_1)}$ and $J(C_{B(f_1)})$ are defined over $\mathbb{Q}$ and, thanks to Theorem 1.1, $\mathrm{End}^0(J(C_{B(f_1)}))$ is either $\mathbb{Q}$ or a quadratic field. (Recall that $J(C_{B(f_1)})$ has the same endomorphism algebra over $\bar{\mathbb{Q}}$ and $\mathbb{C}$.) This implies that $J(C_{B(f_1)})$ is simple, viewed as a complex abelian fourfold.

Example 1.3. If $K = \mathbb{Q}$, $\mathbb{Q}(t)$ and $\bar{\mathbb{Q}}(t)$ are the fields of rational functions in one variable t over $\mathbb{Q}$ and $\bar{\mathbb{Q}}$ respectively then the polynomial $f_t(x) = x^8 - x - 1 \in \mathbb{Q}(t) \subset \bar{\mathbb{Q}}(t)$ has Galois group $\mathbf{S}_8$ over $\bar{\mathbb{Q}}(t)$ [23, p. 139]. Now Hilbert's irreducibility theorem [23, Sect. 10.1] implies that there exists an infinite set N of rational numbers such that for each $n \in N$ the polynomial $f_n(t) = x^8 - x - n$ has Galois group $\mathbf{S}_8$ over $\mathbb{Q}$ and the splitting fields of f_n are linearly disjoint for distinct n. Clearly, $S_{B(f_n)}$, $C_{B(f_n)}$ and $J(C_{B(f_n)})$ are defined over $\mathbb{Q}$ and, thanks to Theorem 1.1, $\mathrm{End}^0(J(C_{B(f_n)}))$ is either $\mathbb{Q}$ or a quadratic field. In addition, abelian varieties $J(C_{B(f_n)})$'s are not isomorphic over $\bar{\mathbb{Q}}$ for distinct n. Since all $\mathbb{C}$-isomorphisms among $J(C_{B(f_n)})$'s are defined over $\bar{\mathbb{Q}}$, the *complex* abelian varieties $J(C_{B(f_n)})$'s are *not* isomorphic for distinct n. This implies that the surfaces $S_{B(f_n)}$'s are not biregularly isomorphic over $\mathbb{C}$ for distinct n.

The Del Pezzo surfaces involved look rather special. That is why we prove that the assertion about the endomorphism algebra of the corresponding jacobian remains true when the corresponding Galois image in $W(E_8)$ contains a subgroup that is a conjugate of the $\mathbf{A}_8$. In particular, the jacobian of the branch curve of "generic" Del Pezzo surface of degree 1 is absolutely simple.

On the other hand, assuming that the Galois action on the Picard group of a Del Pezzo surface of degree 1 is *maximal* (i.e., the Galois image coincides with $W(E_8)$), we prove that the jacobian of the corresponding branch curve has no non-trivial endomorphisms. It would be interesting to find explicit examples of degree 1 surfaces with maximal Galois action. (See [6] for explicit examples of cubic surfaces with maximal Galois image. The case of degree 2 is discussed in [8]).

The paper is organized as follows. In Section 2 we discuss interrelations between Picard groups of a Del Pezzo surface of small degree and the corresponding branch curve. Our exposition is based on letters of Igor Dolgachev to the author. Section 3 deals with abelian fourfolds whose Galois module of points of order 2 has a rather special structure. Our main results are stated and proved in Section 4. In Section 5 we describe an algorithm for finding an (explicit) equation for a (singular) plane birational model of $C_{B(f)}$ in terms of f.

I am deeply grateful to Igor Dolgachev for his interest to this paper and generous help.

This work was started during the special semester "Rational and integral points on higher-dimensional varieties" at the MSRI (Spring 2006). The author is grateful to the MSRI and the organizers of this program.

2. Del Pezzo surfaces of degree 1

2.1. Let $d = 1$ or 2. We write $I^{1,9-d}$ for the standard odd unimodular hyperbolic lattice of rank $10-d$ and signature $(1, 9-d)$. This means that $I^{1,9-d}$ is a free $\mathbb{Z}$-module of rank $10-d$ provided with the unimodular symmetric bilinear form $(,) : I^{1,9-d} \times I^{1,9-d} \to \mathbb{Z}$ and the standard orthogonal basis $\{e_0, e_1, \ldots, e_{9-d}\}$ such that

$$(e_0, e_0) = 1,\ (e_i, e_i) = -1\ \forall i \geq 1.$$

We write $\mathrm{O}(I^{1,9-d})$ for the group of isometries of $I^{1,9-d}$.

Let us put $\omega_{9-d} := -3e_0 + e_1 + \ldots + e_{9-d}$. Clearly, $(\omega_{9-d}, \omega_{9-d}) = d \neq 0$. Let us consider the orthogonal complement $\omega_{9-d}^{\perp}$ of ω_{9-d} in $I^{1,9-d}$. Clearly, $\omega_{9-d}^{\perp}$ is a free $\mathbb{Z}$-(sub)module of rank $9-d$ and the restriction

$$(,) : \omega_{9-d}^{\perp} \times \omega_{9-d}^{\perp} \to \mathbb{Z}$$

is a negative-definite non-degenerate symmetric bilinear form. (If $d = 1$ then it is even unimodular.) It is known [16, Th. 23.9] that there exists an isometry

$$\omega_{9-d}^{\perp} \to Q(E_{9-d}),$$

where $Q(E_{9-d})$ is the root lattice of type E_{9-d} equipped with the scalar product with opposite sign. In addition, if we identify (via this isometry) $\omega_{9-d}^{\perp}$ and $Q(E_{9-d})$ then the orthogonal group $\mathrm{O}(\omega_{9-d}^{\perp})$ of $\omega_{9-d}^{\perp}$ coincides with the corresponding Weyl group $W(E_{9-d})$ [16, Th. 23.9]. This implies that the special orthogonal group $\mathrm{SO}(\omega_{9-d}^{\perp})$ of $\omega_{9-d}^{\perp}$ coincides with the (index 2 sub)group $W^+(E_{9-d})$ of elements of determinant 1 in $W(E_{9-d})$.

There is a natural injective homomorphism $\mu : \mathbf{S}_{9-d} \hookrightarrow \mathrm{O}(I^{1,9-d})$ defined as follows.

$$\tau \mapsto \mu(\tau) : I^{1,9-d} \to I^{1,9-d},\ e_0 \mapsto e_0, e_i \mapsto e_{\tau(i)}\ \forall i \ge 1 \qquad (0).$$

This provides $I^{1,9-d}$ with the natural structure of faithful $\mathbf{S}_{9-d}$-module. Clearly, each $\mu(\tau)$ leaves invariant ω_{9-d} and therefore induces an isometry of $\omega_{9-d}^{\perp}$, which we denote by

$$\iota(\tau) \in \mathrm{O}(\omega_{9-d}^{\perp}) = W(E_{9-d}).$$

Obviously, if $v : I^{1,9-d} \to I^{1,9-d}$ is an isometry that leaves ω_{9-d} invariant and coincides with $\iota(\tau)$ on $\omega_{9-d}^{\perp}$ then $v = \mu(\tau)$. This implies that $\omega_{9-d}^{\perp}$ is a faithful $\mathbf{S}_{9-d}$-submodule. We write

$$\iota : \mathbf{S}_{9-d} \hookrightarrow \mathrm{O}(\omega_{9-d}^{\perp}) = W(E_{9-d}),\ \tau \mapsto \iota(\tau)$$

for the corresponding defining homomorphism.

Suppose now that $d = 1$. Then $9 - d = 8$ and $(\omega_8, \omega_8) = 1$. This gives us a $\mathbf{S}_8$-invariant orthogonal splitting

$$I^{1,8} = \mathbb{Z} \cdot \omega_8 \oplus \omega_8^{\perp}$$

and allows us to identify $W(E_8)$ with a certain subgroup of $\mathrm{O}(I^{1,8})$, namely,

$$W(E_8) = \mathrm{O}(\omega_8^{\perp}) = \{v \in \mathrm{O}(I^{1,8}) \mid v(\omega_8) = \omega_8\}.$$

(Notice that under this identification $\iota(\tau) \in \mathrm{O}(\omega_8^{\perp})$ goes into $\mu(\tau) \in \mathrm{O}(I^{1,8})$.)

2.2. Let S be a Del Pezzo surface over $\bar{K}$ of degree $d = 1$ (or 2). It is well-known [16, Ch. IV, Sect. 24] that $\mathrm{Pic}(S)$ is a free $\mathbb{Z}$-module of rank $10 - d$ provided with unimodular bilinear intersection form

$$(,) : \mathrm{Pic}(S) \times \mathrm{Pic}(S) \to \mathbb{Z}$$

of signature $(1, 9 - d)$; The anticanonical class $-\mathrm{K}_S$ is ample, $(\mathrm{K}_S, \mathrm{K}_S) = d$,

$$\dim_{\bar{K}} H^0(S, \mathcal{O}_S(-\mathrm{K}_S)) = d + 1$$

and

$$H^0(S, \mathcal{O}_S(n\mathrm{K}_S)) = \{0\},\ H^1(S, \mathcal{O}_S(\pm n\mathrm{K}_S)) = \{0\} \qquad (1)$$

for all positive integers n [3, Cor. 3 on p. 65]. If E is an exceptional curve of the first kind on S then

$$< E \cdot K_S >= -1$$

[16, Sect. 26]. Let us put

$$L := \mathrm{K}_S^{\perp} \subset \mathrm{Pic}(S),$$

i.e., L is the orthogonal complement of K_S in $\mathrm{Pic}(S)$ with respect to the intersection pairing. Clearly, L is a free $\mathbb{Z}$-module of rank $9 - d$ and (the restriction)

$$(,) : L \times L \to \mathbb{Z}$$

is a non-degenerate symmetric bilinear form. We write $\mathrm{O}(L)$ (resp. $\mathrm{SO}(L)$) for the group of automorphisms of L (resp. automorphisms of L with determinant 1) preserving the intersection pairing.

Recall [4] that a *marking* of S is an isometry $\phi : \mathrm{Pic}(S) \to I^{1,9-d}$ such that $\phi(\mathrm{K}_S) = \omega_{9-d}$. It is known that a marking always exists [16, Prop. 25.1]. In addition, each marking is a *geometric marking*, i.e. can be realized in such a way

that $\phi^{-1}(e_i)$ (for positive i) are the classes of the exceptional curves under some blow-up $f : S \to \mathbb{P}^2$ [5, Ch. 8, Sect. 8.2]. A marking induces an isometry of lattices

$$\phi : L = \mathrm{K}_S^{\perp} \cong \omega_{9-d}^{\perp} = Q(E_{9-d})$$

and gives rise to a group isomorphism

$$\mathrm{O}(L) \to W(E_{9-d}), u \mapsto \phi u \phi^{-1}.$$

Let w_0 be the nontrivial center element of $W(E_{9-d})$ which acts as -1 on the root lattice. There exists a unique automorphism g_0 of S (called the Geiser ($d = 2$), or Bertini ($d = 1$) involution) such that $\phi g_0 \phi^{-1} = w_0$ [15, Th. 4.7], [3, pp. 66-69], [5, Ch. 8, Sect. 8.2]. Let $C = S^{g_0}$ be the fixed locus of g_0. It is a smooth irreducible projective curve of genus 3 (resp. 4).

We write $J(C)$ for the jacobian of C: it is an abelian variety over $\bar{K}$ of dimension 3 (resp. 4). We write $\mathrm{Pic}(C)_2$ for the kernel of multiplication by 2 in $\mathrm{Pic}(C)$. Clearly, $\mathrm{Pic}(C)_2$ coincides with the group $J(C)_2$ of points of order 2 on J; it is a $\mathbb{F}_2$-vector space of dimension 6 (resp. 8) provided with the alternating nondegenerate bilinear form called the *Weil pairing* [18, 19]

$$<,>: J(C)_2 \times J(C)_2 \to \mathbb{F}_2.$$

Recall that if D is a divisor on S then

$$H^0(S, \mathcal{O}_S(D)) = \mathcal{L}(S, D) := \{u \in \bar{K}(S) \mid \mathrm{div}(u) + D \geq 0\} \subset \bar{K}(S).$$

Lemma 2.3. *Let E be an exceptional curve of the first kind on S and n a positive integer. Then:*

(i) $\mathcal{L}(S, E) = \bar{K}$, $\mathcal{L}(S, E + n\mathrm{K}_S) = \{0\}$.
(ii) $H^1(S, \mathcal{O}_S(-E + n\mathrm{K}_S)) = \{0\}$, $H^1(S, \mathcal{O}_S(E - (n-1)\mathrm{K}_S) = \{0\}$.

Proof. (i) Since the self-intersection index of irreducible curve E is negative, the linear system $\mid E \mid$ consists of single divisor E. This implies that $\mathcal{L}(S, E) = \bar{K}$. Clearly,

$$\mathcal{L}(S, E + n\mathrm{K}_S) \subset \mathcal{L}(S, E) = \bar{K}.$$

Since $-n\mathrm{K}_S$ is ample, $\mathcal{L}(S, E + n\mathrm{K}_S) = \{0\}$.

In order to prove (ii), let us consider the exact sequence

$$0 \to \mathcal{O}_S(-E + n\mathrm{K}_S) \to \mathcal{O}_S(n\mathrm{K}_S) \to \mathcal{O}_E(n\mathrm{K}_S) \to 0,$$

which leads to the cohomological exact sequence

$$H^0(E, n\mathrm{K}_S \mid E) = H^0(S, \mathcal{O}_E(n\mathrm{K}_S)) \to H^1(S, \mathcal{O}_S(-E+n\mathrm{K}_S)) \to H^1(S, \mathcal{O}_S(n\mathrm{K}_S)).$$

Since $(n\mathrm{K}_S, E) = -n < 0$, we have $H^0(E, n\mathrm{K}_S \mid E) = \{0\}$. By (1), $H^1(S, \mathcal{O}_S(nK_S)) = \{0\}$. Now the exactness of the cohomological sequence implies that $H^1(S, \mathcal{O}_S(-E + n\mathrm{K}_S) = \{0\}$. By Serre's duality, we obtain that $H^1(S, \mathcal{O}_S(E - (n-1)\mathrm{K}_S)) = \{0\}$. □

Recall [19] that a divisor class η on a smooth curve C is called a *theta characteristic* if $2\eta = \mathrm{K}_C$. It is called *even* (odd) if $h^0(\eta)$ is even (odd). A theta characteristic η defines a quadratic form on $\mathrm{Pic}(C)_2$ by

$$q_\eta(x) = h^0(\eta + x) + h^0(\eta) \bmod 2.$$

The associated bilinear form $e(x, y) = q_\eta(x + y) + q_\eta(x) + q_\eta(y)$ coincides with $<,>$ on $J(C)_2 = \mathrm{Pic}(C)_2$. In particular, if η is an *even* theta characteristic then

$$< x, y >= h^0(\eta + x + y) + h^0(\eta + x) + h^0(\eta + y) \bmod 2 \qquad (2).$$

Lemma 2.4. *Let $r : \mathrm{Pic}(S) \to \mathrm{Pic}(C)$ be the restriction homomorphism. Then*

(i) *$r(a) \in \mathrm{Pic}(C)_2$ for all $a \in L$. In other words,*

$$r(2L) = 0.$$

(ii *If E is an exceptional curve of the first kind on S then $r(E)$ is an odd theta characteristic on C; more precisely,*

$$h^0(C, r(E)) := \dim_{\bar{K}}(H^0(C, r(E))) = 1.$$

In addition, if $d = 1$ then $r(-\mathrm{K}_S)$ is a theta characteristic on C.

Proof. (i) Since g_0 acts on C as identity map, we have $r(g_0(a)) = g_0(r(a)) = r(a)$. Since $g_0|L = -1$, we get $r(-a) = r(a)$ and hence $2r(a) = 0$.

(ii) Recall that if D is a divisor on C then

$$H^0(C, \mathcal{O}_C(D)) = \mathcal{L}(C, D) := \{u \in \bar{K}(C) \mid \mathrm{div}(u) + D \geq 0\} \subset \bar{K}(C).$$

If u is a non-constant rational function on C then the degree of the divisor of poles of u coincides with the degree of field extension $\bar{K}(C)/\bar{K}(u)$ [14, Th. 2.2].

($d = 2$) Recall that $|-\mathrm{K}_S|$ defines a finite map $\mathfrak{f}$ of degree 2 from S to $\mathbb{P}^2$ and the corresponding involution of S is g_0. Thus the image of C is a smooth plane quartic, and hence $C \in |-2\mathrm{K}_S|$ [3, p. 67]. For any irreducible curve R on S we have $R + g_0(R) = \mathfrak{f}^*(k\ell)$, where ℓ is the class of a line on P^2 and k is an integer. Intersecting with $-\mathrm{K}_S = \mathfrak{f}^*(\ell)$ we get $-2\mathrm{K}_S \cdot R = 2k$. In particular, if $R = E$ is an exceptional curve of the first kind, then $E \cdot \mathrm{K}_S = -1$, we get $E + g_0(E) = \mathfrak{f}^*(\ell) = -\mathrm{K}_S$. Since $E|C = g_0(E)|C$, we obtain $2r(E) = -r(\mathrm{K}_S)$. By the adjunction formula, $\mathrm{K}_C = r(\mathrm{K}_S + C) = -r(\mathrm{K}_S)$. This proves that $r(E)$ is a theta characteristic. It is certainly effective, and therefore we may view $r(E)$ as the linear equivalence class of an effective divisor D of degree 2 on C. We need to prove that $\dim_{\bar{K}}(\mathcal{L}(C, D)) = 1$.

If $u \in \mathcal{L}(C, D)$ is not a constant then the degree of its polar divisor is either 1 or 2. In the former case, $\bar{K}(C) = \bar{K}(u)$ and C is rational, which is not the case, because C has genus 3. In the latter case, $\bar{K}(C)/\bar{K}(u)$ is a quadratic extension and therefore C is hyperelliptic, which is not the case, because C is a plane smooth quartic [10, Ch. 5, Exercise 3.2 and Example 5.2.1]. This implies that $\mathcal{L}(C, D)$ consists of scalars and therefore has dimension 1.

($d = 1$) The linear system $|-2\mathrm{K}_S|$ defines a double cover $\mathfrak{f} : S \to Q$, where Q is a quadratic cone in $\mathbb{P}^3$. The branch curve W is a curve of genus 4, the intersection of Q with a cubic surface [5, Ch. 8, Example 8.2.4]. This implies that $\mathfrak{f}^*(W) = 2C \in |-6\mathrm{K}_S|$, hence $C \in |-3\mathrm{K}_S|$ [3, pp. 68–69]. By adjunction formula, $\mathrm{K}_C = r(-3\mathrm{K}_S + \mathrm{K}_S) = -2r(\mathrm{K}_S)$. Now similar to the case $d = 2$, we obtain $E + g_0(E) = -2K_S$ and $2r(E) = -2r(\mathrm{K}_S) = \mathrm{K}_C$. This proves that $r(-\mathrm{K}_S)$ and $r(E)$ are theta characteristics. Clearly, $r(E)$ is effective and therefore $H^0(C, r(E)) \neq \{0\}$. The short exact sequence

$$0 \to \mathcal{O}_S(E + 3\mathrm{K}_S) = \mathcal{O}_S(E - C) \to \mathcal{O}_S(E) \to \mathcal{O}_C(E) \to 0$$

gives rise to the exact cohomological sequence

$$H^0(S, \mathcal{O}_S(E)) \to H^0(S, \mathcal{O}_C(E)) = H^0(C, r(E)) \to H^1(S, \mathcal{O}_S(E + 3\mathrm{K}_S)).$$

Suppose that we know that $H^1(S, \mathcal{O}_S(E + 3\mathrm{K}_S)) = \{0\}$. This implies that $H^0(S, \mathcal{O}_S(E)) \to H^0(C, r(E))$ is a surjection. Since $H^0(S, \mathcal{O}_S(E))$ is one-dimensional,

thanks to Lemma 2.3(i) and $H^0(C, r(E)) \neq \{0\}$, we conclude that $H^0(S, \mathcal{O}_S(E)) \cong H^0(C, r(E))$; in particular, $h^0(C, r(E)) = 1$.

So, in order to finish the proof, we need to check that

$$H^1(S, \mathcal{O}_S(E + 3\mathrm{K}_S)) = \{0\}.$$

By Serre's duality, it suffices to prove that $H^1(S, \mathcal{O}_S(-E-2\mathrm{K}_S)) = \{0\}$. In order to do that, recall that $-2K_S = E+g_0(E)$ in $\mathrm{Pic}(S)$ where $g_0(E)$ is also an exceptional curve of the first kind. This implies that

$$-E - 2\mathrm{K}_S = -E + E + g_0(E) = g_0(E).$$

Applying Lemma 2.3 to $g_0(E)$ and $n = 1$, we conclude that $H^1(S, \mathcal{O}_S(g_0(E))) = \{0\}$ and therefore $H^1(S, \mathcal{O}_S(-E - 2\mathrm{K}_S)) = H^1(S, \mathcal{O}_S(g_0(E))) = \{0\}$. □

Remark 2.5. If $d = 1$ then the only one theta characteristic of C with $h^0 > 1$ is the vanishing one equal to $r(-\mathrm{K}_S)$ (see below).

Remark 2.6. If $d = 1$ then K_C is very ample [5, Ch. 8, Example 8.2.4]. This implies that C is *not* hyperelliptic.

Lemma 2.7. *Assume $d = 1$. Then:*

- *$r(-\mathrm{K}_S)$ is an even theta characteristic on C.*
- *Let $\phi : \mathrm{Pic}(S) \to I^{1,8}$ be a marking and $E_i = \phi^{-1}(e_i), i = 1, \dots, 8$. Then $v_i = E_i + \mathrm{K}_S \in L$ and points $x_i = r(v_i) \in \mathrm{Pic}(C)_2 = J(C)_2$ satisfy $< x_i, x_j >= 1$ if $i \neq j$.*

Proof. Let $\eta_0 = r(-\mathrm{K}_S)$. By Lemma 2.4(ii), η_0 is a theta characteristic. The short exact sequence

$$0 \to \mathcal{O}_S(2\mathrm{K}_S) = \mathcal{O}_S(-\mathrm{K}_S - C) \to \mathcal{O}_S(-\mathrm{K}_S) \to \mathcal{O}_C(-\mathrm{K}_S) \to 0$$

gives rise to the exact cohomological sequence

$$H^0(S, \mathcal{O}_S(2\mathrm{K}_S)) \to H^0(S, \mathcal{O}_S(-\mathrm{K}_S)) \to H^0(C, -\mathrm{K}_S \mid C) = H^0(C, \eta_0) \to H^1(S, \mathcal{O}_S(2\mathrm{K}_S)).$$

Since $H^0(S, \mathcal{O}_S(2\mathrm{K}_S)) = 0$ and $H^1(S, \mathcal{O}_S(2\mathrm{K}_S)) = 0$, the $\bar{K}$-vector spaces $H^0(C, \eta_0)$ and $H^0(S, \mathcal{O}_S(-\mathrm{K}_S))$ are isomorphic; in particular, $h^0(C, \eta_0) = h^0(-\mathrm{K}_S) = 2$. Thus η_0 is an even theta characteristic.

We have

$$\eta_0 + x_i = r(-\mathrm{K}_S) + r(E_i + \mathrm{K}_S) = r(E_i),\ \eta_0 + x_j = r(E_j),$$

$$\eta_0 + x_i + x_j = r(E_i) + r(E_j + \mathrm{K}_S) = r(E_i + E_j + \mathrm{K}_S).$$

Applying (2) to $\eta = \eta_0$, we conclude that

$$< x_i, x_j >= h^0(\eta_0 + x_i + x_j) + h^0(\eta_0 + x_i) + h^0(\eta_0 + x_j) \bmod 2 =$$

$$= h^0(r(E_i + E_j + \mathrm{K}_S)) + h^0(r(E_i)) + h^0(r(E_j)) \bmod 2 =$$

$$= h^0(r(E_i + E_j + \mathrm{K}_S)) + 1 + 1 \bmod 2 = h^0(r(E_i + E_j + \mathrm{K}_S)) \bmod 2.$$

(Here we used Lemma 2.4 that tells us that $h^0(r(E_i)) = h^0(r(E_j)) = 1$.)

Since $r(2L) = 0$ and $E_j + \mathrm{K}_S \in L$, we obtain that $r(E_i + E_j + \mathrm{K}_S) = r(E_i - E_j - \mathrm{K}_S)$ and therefore

$$< x_i, x_j >= h^0(r(E_i - E_j - \mathrm{K}_S)) \bmod 2.$$

Now

$$(E_i - E_j - \mathrm{K}_S, \mathrm{K}_S) = -1,\ (E_i - E_j - \mathrm{K}_S, E_i - E_j - \mathrm{K}_S) = -1.$$

It is known [16, Th. 26.2(i)] that this implies that $E_i - E_j - \mathrm{K}_S$ is linearly equivalent to the class of an exceptional curve of the first kind. By Lemma 2.4, we obtain $h^0(r(E_i - E_j - \mathrm{K}_S)) = 1$. So, $< x_i, x_j >= 1$. □

Now we need the following elementary result from linear algebra.

Lemma 2.8. *Let $\mathbb{F}$ be a field of characteristic 2, V a finite-dimensional $\mathbb{F}$-vector space,*

$$\phi : V \times V \to \mathbb{F}$$

an alternating $\mathbb{F}$-bilinear form, c a non-zero element of $\mathbb{F}$. Let m be a positive even integer and $\{z_1, \dots z_m\}$ an m-tuple of vectors in V such that

$$\phi(z_i, z_j) = c \ \forall \ i \neq j.$$

Then:

(i) *$\{z_1, \dots z_m\}$ is a set of linearly independent vectors; in particular, it is a basis if $m = \dim(V)$.*

(ii) *Let V_m be the subspace of V generated by all z_i's. Then the restriction of ϕ to V_m is nondegenerate. In particular, if $m = \dim(V)$ then $V_m = V$ and ϕ is non-degenerate.*

Both assertions of Lemma 2.8 follow immediately from the next statement.

Proposition 2.9. *Let $\{a_1 \dots, a_m\}$ be an m-tuple of elements of $\mathbb{F}$ such that $z = \sum_{i=1}^m a_i z_i$ satisfies $\phi(z, z_j) = 0 \ \forall \ j$. Then all a_i's vanish.*

Proof of Proposition 2.9. Let us put

$$b = \sum_{i=1}^{m} a_i.$$

Since for all j with $1 \le j \le r$

$$\phi(z_j, z_j) = 0 = \phi(z, z_j) = \phi\left(\sum_{i=1}^{r} a_i z_i, z_j\right) = \sum_{i \neq j} a_i \cdot c,$$

we have $c \cdot \sum_{i \neq j} a_i = 0$. This implies that $b - a_j = \sum_{i \neq j} a_i = 0 \ \forall j$. It follows that

$$0 = \sum_{j=1}^{m} (b - a_j) = mb - \sum_{j=1}^{m} a_j = mb - b = (m-1)b = b,$$

since m is even and $\mathrm{char}(\mathbb{F}) = 2$. So, $b = 0$. Since every $b - a_j = 0$, we conclude that every $a_j = 0$. □

Theorem 2.10. *Assume $d = 1$. The map $L/2L \to \mathrm{Pic}(C)_2$ induced by r is an isometry with respect to the bilinear intersection form $<,>$ on L reduced modulo 2 and the Weil pairing $<,>$ on $\mathrm{Pic}(C)_2$.*

Proof. Let $v_1, \dots, v_8 \in L$ be as in Lemma 2.7. We have

$$(v_i, v_j) = (E_i + \mathrm{K}_S, E_j + \mathrm{K}_S) = -1$$

and therefore $1 = (v_i, v_j) \bmod 2 =< r(v_i), r(v_j) >$. It follows from Lemma 2.8 that $r(v_i)$'s form a basis in $\mathrm{Pic}(C)_2$. This implies that $\{r(v_1), \dots, r(v_8)\}$ is a basis in $L/2L$ and moreover the restriction map r mod 2 of the 8-dimensional vector spaces over $\mathbb{F}_2$ preserves the corresponding non-degenerate bilinear forms. Obviously it implies that the map is an isometry. □

Remark 2.11. A similar assertion is true in the case $d = 2$ and is proven in [4, pp. 160–162]. One can give it a similar proof without using the Smith exact sequence. We put $x_i = r(E_i - E_1)$, where $\{E_1, \dots, E_7\}$ are defined similar to the above $(i = 2, \dots, 7)$. We take the odd theta characteristic $\eta = r(E_1)$ and compute the associated bilinear form of the quadratic form q_η. We do the similar computation, using the fact that the seven odd theta characteristics $\eta_i = r(E_i)$ form an *Aronhold set*, i.e., $\eta_i + \eta_j - \eta_k$ is an even theta characteristic for any distinct i, j, k [4, pp. 166–169]. (See also [5, Ch. 6, Sect. 6.1].)

Remark 2.12. Suppose that S is defined over a field K. Then $\mathrm{Pic}(S)$ carries the natural structure of $\mathrm{Gal}(K)$-module, the intersection pairing and K_S are Galois-invariant [16, Ch. IV]. In addition, g_0 is defined over K [15, Th. 4.7] and therefore C is a K-curve on S. It follows easily from Theorem 2.10 that L is a Galois submodule and $L/2L \to \mathrm{Pic}(C)_2$ is an isomorphism of Galois modules.

3. Abelian varieties

A surjective homomorphism of finite groups $\pi : \mathcal{G}_1 \twoheadrightarrow \mathcal{G}$ is called a *minimal cover* if no proper subgroup of $\mathcal{G}_1$ maps onto $\mathcal{G}$ [9]. Clearly, if G is perfect and $\mathcal{G}_1 \twoheadrightarrow \mathcal{G}$ is a minimal cover then $\mathcal{G}_1$ is also perfect.

Let F be a field, F_a its algebraic closure and $\mathrm{Gal}(F) := \mathrm{Aut}(F_a/F)$ the absolute Galois group of F. If X is an abelian variety of positive dimension over F_a then we write $\mathrm{End}(X)$ for the ring of all its F_a-endomorphisms and $\mathrm{End}^0(X)$ for the corresponding $\mathbb{Q}$-algebra $\mathrm{End}(X) \otimes \mathbb{Q}$. We write $\mathrm{End}_F(X)$ for the ring of all F-endomorphisms of X and $\mathrm{End}^0_F(X)$ for the corresponding $\mathbb{Q}$-algebra $\mathrm{End}_F(X) \otimes \mathbb{Q}$ and $\mathfrak{C}$ for the center of $\mathrm{End}^0(X)$. Both $\mathrm{End}^0(X)$ and $\mathrm{End}^0_F(X)$ are semisimple finite-dimensional $\mathbb{Q}$-algebras.

The group $\mathrm{Gal}(F)$ of F acts on $\mathrm{End}(X)$ (and therefore on $\mathrm{End}^0(X)$) by ring (resp. algebra) automorphisms and

$$\mathrm{End}_F(X) = \mathrm{End}(X)^{\mathrm{Gal}(F)},\ \mathrm{End}^0_F(X) = \mathrm{End}^0(X)^{\mathrm{Gal}(F)},$$

since every endomorphism of X is defined over a finite separable extension of F.

If n is a positive integer that is not divisible by $\mathrm{char}(F)$ then we write X_n for the kernel of multiplication by n in $X(F_a)$; the commutative group X_n is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2\dim(X)$ [18]. In particular, if $n = 2$ then X_2 is an $\mathbb{F}_2$-vector space of dimension $2\dim(X)$.

If X is defined over F then X_n is a Galois submodule in $X(F_a)$ and all points of X_n are defined over a finite separable extension of F. We write $\bar{\rho}_{n,X,F} : \mathrm{Gal}(F) \to \mathrm{Aut}_{\mathbb{Z}/n\mathbb{Z}}(X_n)$ for the corresponding homomorphism defining the structure of the Galois module on X_n,

$$\tilde{G}_{n,X,F} \subset \mathrm{Aut}_{\mathbb{Z}/n\mathbb{Z}}(X_n)$$

for its image $\bar{\rho}_{n,X,F}(\mathrm{Gal}(F))$ and $F(X_n)$ for the field of definition of all points of X_n. Clearly, $F(X_n)$ is a finite Galois extension of F with Galois group $\mathrm{Gal}(F(X_n)/F) = \tilde{G}_{n,X,F}$. If $n = 2$ then we get a natural faithful linear representation

$$\tilde{G}_{2,X,F} \subset \mathrm{Aut}_{\mathbb{F}_2}(X_2)$$

of $\tilde{G}_{2,X,F}$ in the $\mathbb{F}_2$-vector space X_2.

Now and till the end of this Section we assume that $\mathrm{char}(F) \neq 2$. It is known [22] that all endomorphisms of X are defined over $F(X_4)$; this gives rise to the

natural homomorphism

$$\kappa_{X,4} : \tilde{G}_{4,X,F,} \to \mathrm{Aut}(\mathrm{End}^0(X))$$

and $\mathrm{End}^0_F(X)$ coincides with the subalgebra $\mathrm{End}^0(X)^{\tilde{G}_{4,X,F}}$ of $\tilde{G}_{4,X,F}$-invariants [29, Sect. 1].

The field inclusion $F(X_2) \subset F(X_4)$ induces a natural surjection [29, Sect. 1]

$$\tau_{2,X} : \tilde{G}_{4,X,F} \twoheadrightarrow \tilde{G}_{2,X,F}.$$

The following definition has already appeared in [7].

Definition 3.1. We say that F is 2-*balanced* with respect to X if $\tau_{2,X}$ is a minimal cover.

Remark 3.2. Clearly, there always exists a subgroup $H \subset \tilde{G}_{4,X,F}$ such that $H \to \tilde{G}_{2,X,F}$ is surjective and a minimal cover. Let us put $L = F(X_4)^H$. Clearly,

$$F \subset L \subset F(X_4),\ L \bigcap F(X_2) = F$$

and L is a maximal overfield of F that enjoys these properties. It is also clear that There exists an overfield L such that

$$F \subset L \subset F(X_4),\ L \bigcap F(X_2) = F,$$

$$F(X_2) \subset L(X_2),\ L(X_4) = F(X_4), \tilde{G}_{2,X,L} = \tilde{G}_{2,X,F}$$

and L is 2-*balanced* with respect to X (see [7, Remark 2.3]).

Theorem 3.3. *Suppose that* $E := \mathrm{End}^0_F(X)$ *is a field that contains the center* $\mathfrak{C}$ *of* $\mathrm{End}^0(X)$. *Let* $\mathfrak{C}_{X,F}$ *be the centralizer of* $\mathrm{End}^0_F(X)$ *in* $\mathrm{End}^0(X)$.

Then:

(i) $\mathfrak{C}_{X,F}$ *is a central simple* E*-subalgebra in* $\mathrm{End}^0(X)$. *In addition, the centralizer of* $\mathfrak{C}_{X,F}$ *in* $\mathrm{End}^0(X)$ *coincides with* $E = \mathrm{End}^0_F(X)$ *and*

$$\dim_E(\mathfrak{C}_{X,F}) = \frac{\dim_{\mathfrak{C}}(\mathrm{End}^0(X))}{[E : \mathfrak{C}]^2}.$$

(ii) *Assume that* F *is* 2*-balanced with respect to* X *and* $\tilde{G}_{2,X,F}$ *is a non-abelian simple group. If* $\mathrm{End}^0(X) \neq E$ *(i.e., not all endomorphisms of* X *are defined over* F*) then there exist a finite perfect group* $\Pi \subset \mathfrak{C}^*_{X,F}$ *and a surjective homomorphism* $\Pi \to \tilde{G}_{2,X,F}$ *that is a minimal cover. In addition, the induced homomorphism* $\mathbb{Q}[\Pi] \to \mathfrak{C}_{X,F}$ *is surjective, i.e.,* $\mathfrak{C}_{X,F}$ *is isomorphic to a direct summand of the group algebra* $\mathbb{Q}[\Pi]$.

Proof. This is Theorem 2.4 of [7]. □

Lemma 3.4. *Assume that* X_2 *does not contain proper* $\tilde{G}_{2,X,F}$*-invariant even-dimensional subspaces and the centralizer* $\mathrm{End}_{\tilde{G}_{2,X,F}}(X_2)$ *has* $\mathbb{F}_2$*-dimension* 2.

Then X *is* F*-simple and* $\mathrm{End}^0_F(X)$ *is either* $\mathbb{Q}$ *or a quadratic field.*

Proof. If Y is a proper abelian F-subvariety of X then Y_2 is a proper Galois-invariant $2\dim(Y)$-dimensional subspace in X_2. So, Y_2 is even-dimensional and $\tilde{G}_{2,X,F}$-invariant. This implies that such Y does not exist, i.e., X is F-simple. This

implies that $\mathrm{End}_F(X)$ has no zero-divisors. This implies that $\mathrm{End}_F^0(X)$ is a finite-dimensional $\mathbb{Q}$-algebra without zero divisors and therefore is division algebra over $\mathbb{Q}$. On the other hand, the action of $\mathrm{End}_F(X)$ on X_2 gives rise to an embedding

$$\mathrm{End}_F(X) \otimes \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{End}_{\mathrm{Gal}(F)}(X_2) = \mathrm{End}_{\tilde{G}_{2,X,F}}(X_2).$$

This implies that the rank of free $\mathbb{Z}$-module $\mathrm{End}_F(X)$ does not exceed 2, i.e., is either 1 or 2. It follows that $\mathrm{End}_F^0(X)$ has $\mathbb{Q}$-dimension 1 or 2 and therefore is commutative. Since $\mathrm{End}_F^0(X)$ is division algebra, it is a field. If $\dim_{\mathbb{Q}}\mathrm{End}_F^0(X) = 1$ then $\mathrm{End}_F^0(X) = \mathbb{Q}$. If $\dim_{\mathbb{Q}}\mathrm{End}_F^0(X) = 2$ then $\mathrm{End}_F^0(X)$ is a quadratic field. □

Lemma 3.5. *Let us assume that* $g := \dim(X) > 0$ *and the center of* $\mathrm{End}^0(Y)$ *is a field, i.e,* $\mathrm{End}^0(X)$ *is a simple* $\mathbb{Q}$*-algebra.*

Then:

(i) $\dim_{\mathbb{Q}}(\mathrm{End}^0(X))$ *divides* $(2g)^2$.

(ii) *If* $\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) = (2g)^2$ *then* $\mathrm{char}(F) > 0$ *and* Y *is a supersingular abelian variety.*

Proof. (ii) is proven in [26, Lemma 3.1] (even without any assumptions on the center).

In order to prove (ii), notice that there exist an absolutely simple abelian variety Y over F_a and a positive integer r such that X is isogenous (over F_a) to a self-product Y^r. We have

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

It follows readily from Albert's classification ([18, Sect. 21], [20]) that $\dim_{\mathbb{Q}}(\mathrm{End}^0(Y))$ divides $(2\dim(Y))^2$. The rest is clear. □

Let B be an 8-element set. We write $\mathrm{Perm}(B)$ for the group of all permutations of B. The choice of ordering on B establishes an isomorphism between $\mathrm{Perm}(B)$ and the symmetric group S_8. We write $\mathrm{Alt}(B)$ for the only subgroup of index 2 in $\mathrm{Perm}(B)$. Clearly, every isomorphism $\mathrm{Perm}(B) \cong \mathrm{S}_8$ induces an isomorphism between $\mathrm{Alt}(B)$ and the alternating group $\mathbf{A}_8$. Let us consider the 8-dimensional $\mathbb{F}_2$-vector space $\mathbb{F}_2^B$ of all $\mathbb{F}_2$-valued functions on B provided with the natural structure of faithful $\mathrm{Perm}(B)$-module. Notice that the standard symmetric bilinear form

$$\mathbb{F}_2^B \times \mathbb{F}_2^B \to \mathbb{F}_2,\ \phi, \psi \mapsto \sum_{b\in B} \phi(b)\psi(b)$$

is non-degenerate and $\mathrm{Perm}(B)$-invariant.

Since $\mathrm{Alt}(B) \subset \mathrm{Perm}(B)$, one may view $\mathbb{F}_2^B$ as faithful $\mathrm{Alt}(B)$-module.

Lemma 3.6. (i) *The centralizer* $\mathrm{End}_{\mathrm{Alt}(B)}(\mathbb{F}_2^B)$ *has* $\mathbb{F}_2$*-dimension* 2.

(ii) $\mathbb{F}_2^B$ *does not contain a proper* $\mathrm{Alt}(B)$*-invariant even-dimensional subspace.*

Proof. Since $\mathrm{Alt}(B)$ is doubly transitive, (i) follows from [21, Lemma 7.1].

Notice that the subspace of $\mathrm{Alt}(B)$-invariants

$$M_0 := (\mathbb{F}_2^B)^{\mathrm{Alt}(B)} = \mathbb{F}_2 \cdot 1_B,$$

where 1_B is the constant function 1. In order to prove (ii), recall that

$$M_0 \subset M_1 \subset \mathbb{F}_2^B$$

where M_1 is the hyperplane of functions with zero sum of values. It is known [17] that M_1/M_0 is a simple $\mathrm{Alt}(B)$-module; clearly, $\dim(M_1/M_0) = 6$. It follows

that if W is a a proper even-dimensional $\mathrm{Alt}(B)$-invariant subspace of $\mathbb{F}_2^B$ then $\dim(W) = 2$ or 6. Clearly, the orthogonal complement W' of W in $\mathbb{F}_2^B$ with respect to the standard bilinear form is also $\mathrm{Alt}(B)$-invariant and $\dim(W) + \dim(W') = 8$. It follows that either $\dim(W) = 2$ or $\dim(W') = 2$. On the other hand, $\mathrm{Alt}(B) = \mathrm{A}_8$ must act trivially on any two-dimensional $\mathbb{F}_2$-vector space, since $\mathbf{A}_8$ is simple non-abelian and $\mathrm{GL}_2(\mathbb{F}_2)$ is solvable. Since the subspace of $\mathrm{Alt}(B)$-invariants is one-dimensional, we conclude that there are no two-dimensional $\mathrm{Alt}(B)$-invariant subspaces of $\mathbb{F}_2^B$. The obtained contradiction proves the desired result. □

Theorem 3.7. *Let X be a four-dimensional abelian variety over F. Suppose that there exists a group isomorphism $\tilde{G}_{2,X,F} \cong \mathrm{Alt}(B)$ such that the $\mathrm{Alt}(B)$-module X_2 is isomorphic to $\mathbb{F}_2^B$.*

Then one of the following two conditions holds:

(i) $\mathrm{End}^0(X)$ *is either $\mathbb{Q}$ or a quadratic field. In particular, X is absolutely simple.*
(ii) $\mathrm{char}(F) > 0$ *and X is a supersingular abelian variety.*

Remark 3.8. Lemmas 3.4 and 3.6 and Remark 3.2 imply that in the course of the proof of Theorem 3.7, we may assume that $\mathrm{End}_F^0(X)$ is either $\mathbb{Q}$ or a quadratic field and F is 2-*balanced* with respect to X; in particular, we may assume that $\tilde{G}_{4,X,F}$ is perfect, since $\tilde{G}_{2,X,F} = \mathbf{A}_8$ is perfect.

Proof of Theorem 3.7. Following Remark 3.8, we assume that $\tilde{G}_{4,X,F}$ is perfect, $\tau_{2,X} : \tilde{G}_{4,X,F} \twoheadrightarrow \tilde{G}_{2,X,F} = \mathbf{A}_8$ is a minimal cover and $\mathrm{End}_F^0(X)$ is either $\mathbb{Q}$ or a quadratic field. Since $\tilde{G}_{4,X,F}$ is perfect, it does not contain a subgroup of index $2, 3$ or 4. Recall that $\mathfrak{C}$ is the center of $\mathrm{End}^0(X)$.

Lemma 3.9. *Either $\mathfrak{C} = \mathbb{Q} \subset \mathrm{End}_F^0(X)$ or $\mathfrak{C} = \mathrm{End}_F^0(X)$ is a quadratic field.*

Proof of Lemma 3.9. Suppose that $\mathfrak{C}$ is not a field. Then it is a direct sum

$$\mathfrak{C} = \oplus_{i=1}^r \mathfrak{C}_i$$

of number fields $\mathfrak{C}_1, \dots, \mathfrak{C}_r$ with $1 < r \le \dim(X) = 4$. Clearly, the center $\mathfrak{C}$ is a $\tilde{G}_{4,X,F}$-invariant subalgebra of $\mathrm{End}^0(X)$; it is also clear that $\tilde{G}_{4,X,F}$ permutes summands $\mathfrak{C}_i$'s. Since $\tilde{G}_{4,X,F}$ does not contain proper subgroups of index ≤ 4, each $\mathfrak{C}_i$ is $\tilde{G}_{4,X,F}$-invariant. This implies that the r-dimensional $\mathbb{Q}$-subalgebra

$$\oplus_{i=1}^r \mathbb{Q} \subset \oplus_{i=1}^r \mathfrak{C}_i$$

consists of $\tilde{G}_{4,X,F}$-invariants and therefore lies in $\mathrm{End}_F^0(X)$. It follows that $\mathrm{End}_F^0(X)$ has zero-divisors, which is not the case. The obtained contradiction proves that $\mathfrak{C}$ is a field.

It is known [18, Sect. 21] that $\mathfrak{C}$ contains a totally real number (sub)field $\mathfrak{C}_0$ with $[\mathfrak{C}_0 : \mathbb{Q}] \mid \dim(X)$ and such that either $\mathfrak{C} = \mathfrak{C}_0$ or $\mathfrak{C}$ is a purely imaginary quadratic extension of C_0. Since $\dim(X) = 4$, the degree $[\mathfrak{C}_0 : \mathbb{Q}]$ is $1, 2$ or 4; in particular, the order of $\mathrm{Aut}(\mathfrak{C}_0)$ does not exceed 4. Clearly, $\mathfrak{C}_0$ is $\tilde{G}_{4,X,F}$-invariant; this gives us the natural homomorphism $\tilde{G}_{4,X,F} \to \mathrm{Aut}(\mathfrak{C}_0)$, which must be trivial and therefore $\mathfrak{C}_0$ consists of $\tilde{G}_{4,X,F}$-invariants. This implies that $\tilde{G}_{4,X,F}$ acts on $\mathfrak{C}$ through a certain homomorphism $\tilde{G}_{4,X,F} \to \mathrm{Aut}(\mathfrak{C}/\mathfrak{C}_0)$ and this homomorphism is trivial, because the order of $\mathrm{Aut}(\mathfrak{C}/\mathfrak{C}_0)$ is either 1 (if $\mathfrak{C} = \mathfrak{C}_0$) or 2 (if $\mathfrak{C} \ne \mathfrak{C}_0$). So,

the whole $\mathfrak{C}$ consists of $\tilde{G}_{4,X,F}$-invariants, i.e.,

$$\mathfrak{C} \subset \mathrm{End}^0(X)^{\tilde{G}_{4,X,F}} = \mathrm{End}^0_F(X).$$

This implies that if $\mathfrak{C} \ne \mathbb{Q}$ then $\mathrm{End}^0_F(X)$ is also not $\mathbb{Q}$ and therefore is a quadratic field containing $\mathfrak{C}$, which implies that $\mathfrak{C} = \mathrm{End}^0_F(X)$ is also a quadratic field. □

It follows that $\mathrm{End}^0(X)$ is a simple $\mathbb{Q}$-algebra (and a central simple $\mathfrak{C}$-algebra). Let us put $E := \mathrm{End}^0_F(X)$ and denote by $\mathfrak{C}_{X,F}$ the centralizer of E in $\mathrm{End}^0(X)$. We have

$$\mathfrak{C} \subset E \subset \mathfrak{C}_{X,F} \subset \mathrm{End}^0(X).$$

Combining Lemma 3.9 with Theorem 3.3 and Lemma 3.5, we obtain the following assertion.

Proposition 3.10. (i) *$\mathfrak{C}_{X,F}$ is a central simple E-subalgebra in* $\mathrm{End}^0(X)$,

$$\dim_E(\mathfrak{C}_{X,F}) = \frac{\dim_{\mathfrak{C}}(\mathrm{End}^0(X))}{[E:\mathfrak{C}]^2}$$

and $\dim_E(\mathfrak{C}_{X,F})$ *divides* $(2\dim(X))^2 = 8^2$.

(ii) *If* $\mathrm{End}^0(X) \ne E$ *(i.e., not all endomorphisms of X are defined over F) then there exist a finite perfect group* $\Pi \subset \mathfrak{C}^*_{X,F}$ *and a surjective homomorphism* $\pi : \Pi \to \tilde{G}_{2,X,F}$ *that is a minimal cover.*

End of Proof of Theorem 3.7. If $\mathrm{End}^0(X) = E$ then we are done. If $\dim_E(\mathfrak{C}_{X,F}) = 8^2$ then $\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) \ge \dim_{\mathfrak{C}}(\mathrm{End}^0(X)) \ge \dim_E(\mathfrak{C}_{X,F}) = 8^2 = (2\dim(X))^2$ and it follows from Lemma 3.9 that $\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) = (2\dim(X))^2$ and X is a supersingular abelian variety. So, further we may and will assume that

$$\mathrm{End}^0(X) \ne E,\ \dim_E(\mathfrak{C}_{X,F}) \ne 8^2.$$

We need to arrive to a contradiction. Let $\Pi \subset \mathfrak{C}^*_{X,F}$ be as in 3.10(ii). Since Π is perfect, $\dim_E(\mathfrak{C}_{X,F}) > 1$. It follows from Proposition 3.10(i) that $\dim_E(\mathfrak{C}_{X,F}) = d^2$ where $d = 2$ or 4.

Let us fix an embedding $E \hookrightarrow \mathbb{C}$ and an isomorphism $\mathfrak{C}_{X,F} \otimes_E \mathbb{C} \cong \mathrm{M}_d(\mathbb{C})$. This gives us an embedding $\Pi \hookrightarrow \mathrm{GL}(d,\mathbb{C})$. Further we will identify Π with its image in $\mathrm{GL}(d,\mathbb{C})$. Clearly, only central elements of Π are scalars. It follows that there is a central subgroup $\mathcal{Z}$ of Π such that the natural homomorphism $\Pi/\mathcal{Z} \to \mathrm{PGL}(d,\mathbb{C})$ is an embedding. The simplicity of $\tilde{G}_{2,X,F} = \mathbf{A}_8$ implies that Z lies in the kernel of $\Pi \twoheadrightarrow \tilde{G}_{2,X,F} = \mathbf{A}_8$ and the induced map $\Pi/Z \to \tilde{G}_{2,X,F}$ is also a minimal cover. However, the smallest possible degree of nontrivial projective representation of $\mathbf{A}_8 \cong \mathbf{L}_4(2)$ (in characteristic zero) is $7 > d$ [2]. Applying Theorem on p. 1092 of [9] and Theorem 3 on p. 316 of [13], we obtained a desired contradiction. □

Theorem 3.11. *Suppose that X is as in Theorem 3.7. Suppose that Y is an abelian fourfold over F that enjoys the following properties:*

(i) *$\tilde{G}_{2,Y,F}$ is solvable;*

(ii) *The fields $F(X_2)$ and $F(Y_2)$ are linearly disjoint over F.*

If $\mathrm{char}(F) = 0$ *then X and Y are not isomorphic over $\bar{K}$.*

Proof of Theorem 3.11. Replacing F by $F(Y_2)$, we may and will assume that $\tilde{G}_{2,Y,F} = \{1\}$, i.e., the Galois module Y_2 is trivial. Clearly, the Galois modules X_2 and Y_2 are *not* isomorphic. By Theorem 3.7, $\mathrm{End}^0(X)$ is either $\mathbb{Q}$ or a quadratic field say, L. In

the former case all the endomorphisms of X are defined over F. In the latter case, all the endomorphisms of X are defined either over F or over a certain quadratic extension of F, because the automorphism group of L is the cyclic group of order 2. Replacing if necessary F by the corresponding quadratic extension, we may and will assume that all the endomorphisms of X are defined over F. In particular, all the automorphisms of X are defined over F; in both cases the whole group $\mathrm{Aut}(X)$ is a finite cyclic group.

Let $u : X \to Y$ be an $\bar{F}$-isomorphism of abelian varieties. We need to arrive to a contradiction. Since the Galois modules X_2 and Y_2 are *not* isomorphic, u is *not* defined over F. Let us consider the cocycle

$$c : \mathrm{Gal}(K) \to \mathrm{Aut}(X),\ \sigma \mapsto c_\sigma := u^{-1}\sigma u.$$

Since the Galois group acts trivially on $\mathrm{Aut}(X)$, the map $c : \mathrm{Gal}(K) \to \mathrm{Aut}(X)$ is a (continuous) group homomorphism. Since $\mathrm{Aut}(X)$ is a finite cyclic group, there is a finite cyclic extension F'/F such that

$$c_\sigma = 1\ \forall \sigma \in \mathrm{Gal}(\bar{F}/F') = \mathrm{Gal}(F') \subset \mathrm{Gal}(F).$$

It follows that u is defined over F' and therefore the $\mathrm{Gal}(F')$-modules X_2 and Y_2 are isomorphic. Clearly, the $\mathrm{Gal}(F')$-module Y_2 remains trivial. However, since F'/F is cyclic and $\tilde{G}_{2,Y,F} \cong \mathbf{A}_8$ is simple non-abelian.

$$\tilde{G}_{2,Y,F'} = \tilde{G}_{2,Y,F} \cong \mathbf{A}_8$$

and therefore the $\mathrm{Gal}(F')$-module X_2 is *not* trivial. This implies that X_2 is not isomorphic to Y_2 as $\mathrm{Gal}(F')$-module and we get a desired contradiction. □

3.12. Let us consider the 8-element set $\mathcal{B} = \{1, 2, \dots, 7, 8\}$. Then

$$\mathrm{Perm}(\mathcal{B}) = \mathbf{S}_8, \mathrm{Alt}(\mathcal{B}) = \mathbf{A}_8, \mathbb{F}_2^{\mathcal{B}} = \mathbb{F}_2^8.$$

Let us put $d = 1$. Then $9 - d = 8$ and $\omega_8^\perp$ carries the natural structure of $\mathbf{S}_8$-submodule in $I^{1,8}$ (Sect. 2.1). The inclusion $\mathbf{A}_8 \subset \mathbf{S}_8$ provides $\omega_8^\perp$ with the natural structure of $\mathbf{A}_8$-module.

Lemma 3.13. *The $\mathbf{S}_8$-modules $\mathbb{F}_2^8$ and $\omega_8^\perp \otimes \mathbb{Z}/2\mathbb{Z}$ are isomorphic. In particular, the $\mathbf{A}_8$-modules $\mathbb{F}_2^8$ and $\omega_8^\perp \otimes \mathbb{Z}/2\mathbb{Z}$ are also isomorphic.*

Proof. Recall that there is an orthogonal $\mathbf{S}_8$-invariant splitting

$$I^{1,8} = \mathbb{Z} \cdot \omega_8 \oplus \omega_8^\perp.$$

Let us consider the nine-dimensional $\mathbb{F}_2$-vector space $I^{1,8} \otimes \mathbb{Z}/2\mathbb{Z}$. We write $\bar{e}_i$ for the image of e_i in $I^{1,8} \otimes \mathbb{Z}/2\mathbb{Z}$. The image of ω_8 in $I^{1,8} \otimes \mathbb{Z}/2\mathbb{Z}$ coincides with

$$\bar{\omega} = \sum_{i=0}^{8} \bar{e}_i.$$

The unimodular pairing on $I^{1,8}$ induces a non-degenerate pairing

$$(I^{1,8} \otimes \mathbb{Z}/2\mathbb{Z}) \times (I^{1,8} \otimes \mathbb{Z}/2\mathbb{Z}) \to \mathbb{F}_2;$$

with respect to this pairing, all $\bar{e}_i$'s constitute an orthonormal basis of $I^{1,8} \otimes \mathbb{Z}/2\mathbb{Z}$.

Clearly, the splitting

$$I^{1,8} \otimes \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2 \cdot \bar{\omega} \oplus (\omega_8^\perp \otimes \mathbb{Z}/2\mathbb{Z})$$

is $\mathbf{S}_8$-invariant and orthogonal. In particular, $\omega_8^\perp \otimes \mathbb{Z}/2\mathbb{Z}$ coincides with the orthogonal complement of $\bar{\omega}$ in $I^{1,8} \otimes \mathbb{Z}/2\mathbb{Z}$.

It follows that

$$\omega_8^{\perp} \otimes \mathbb{Z}/2\mathbb{Z} = \{\sum_{i=0}^{8} c_i \bar{e}_i \mid \sum_{i=0}^{8} c_i = 0\}.$$

Now the map

$$\sum_{i=0}^{8} c_i \bar{e}_i \mapsto \{c_i\}_{i=1}^{8} \in \mathbb{F}_2^8$$

establishes an isomorphism between the $\mathbf{S}_8$-modules $\omega_8^{\perp} \otimes \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{F}_2^8$. □

3.14. We refer to [1, Ch. VI, Sect. 4, Ex. 1], [2, p. 85] for the definition and basic properties of the finite simple non-abelian group $\mathrm{O}^+(8) = \mathrm{O}^+(q_8)$ of order $2^{12} \cdot 3^5 \cdot 5^2 \cdot 7$. In particular, every maximal subgroup in $\mathrm{O}^+(8)$ has index ≥ 120 [2, p. 85]. This implies that every subgroup of $\mathrm{O}^+(8)$ (except $\mathrm{O}^+(8)$ itself) has index > 8.

It is known [12, p. 232] that every faithful representation of $\mathrm{O}^+(8)$ in characteristic 2 has dimension ≥ 8. It follows that every faithful representation of $\mathrm{O}^+(8)$ in a 8-dimension $\mathbb{F}_2$-vector space is absolutely irreducible and does not split into a tensor product of two non-trivial representations.

We refer to [27, 28] for the definition and basic properties of *very simple* representations.

Theorem 3.15. *Let X be a four-dimensional abelian variety over F. Suppose that there exists a group isomorphism $\tilde{G}_{2,X,F} \cong \mathrm{O}^+(8)$.*

Then one of the following two conditions holds:

(i) $\mathrm{End}(X) = \mathbb{Z}$. *In particular, X is absolutely simple.*
(ii) $\mathrm{char}(F) > 0$ *and X is a supersingular abelian variety.*

Proof. Since the natural representation of $\mathrm{O}^+(8)$ in the 8-dimension $\mathbb{F}_2$-vector space X_2 is faithful, it is absolutely irreducible and does not split into a tensor product of two non-trivial representations, thanks to Sect. 3.14. Since every subgroup in $\mathrm{O}^+(8)$ (except $\mathrm{O}^+(8)$ itself) has index > 8 (3.14), this (8-dimensional) representation is not induced from a subgroup. It follows from [27, Th. 7.7] that the $\mathrm{O}^+(8)$-module X_2 is *very simple*. Now our Theorem follows from [27, Lemma 2.3]. □

4. Jacobians

4.1. Let K be a field of characteristic zero, $\bar{K}$ its algebraic closure and $\mathrm{Gal}(K) := \mathrm{Aut}(\bar{K}/K)$ the absolute Galois group of K.

We use the notation of Section 2. Let S be a Del Pezzo surface of degree $d = 1$ over $\bar{K}$, let L be the orthogonal complement of K_S in $\mathrm{Pic}(S)$ with respect to the intersection pairing. Let us fix a marking $\phi : \mathrm{Pic}(S) \to I^{1,8}$.

Suppose that S is defined over K. Recall (Remark 2.12) that the Bertini involution on S and the corresponding branch curve C are also defined over K. In addition, there is the natural Galois action of $\mathrm{Gal}(K)$ on $\mathrm{Pic}(S)$, which preserves the intersection pairing and K_S. This action is defined by a certain continuous homomorphism

$$\rho_S : \mathrm{Gal}(K) \to \mathrm{Aut}(\mathrm{Pic}(S)),$$

whose (finite) image consists of isometries; in addition,

$$\rho_S(\sigma)(\mathrm{K}_S) = \mathrm{K}_S \ \forall \sigma \in \mathrm{Gal}(K).$$

The continuous homomorphism

$$\rho_\phi : \mathrm{Gal}(K) \to \mathrm{O}(I^{1,8}),\ \sigma \mapsto \phi\rho_S(\sigma)\phi^{-1}$$

provides $I^{1,8}$ with a structure of $\mathrm{Gal}(K)$-module. Clearly, $\phi : \mathrm{Pic}(S) \to I^{1,8}$ is an isomorphism (and isometry) of Galois modules.

Since $\phi(\mathrm{K}_S) = \omega_8$, the Galois group leaves invariant ω_8. This implies that $\phi(L) = \omega_8^\perp$ and

$$\phi : L \to \omega_8^\perp$$

is an isomorphism (isometry) of Galois modules and therefore the Galois modules $L/2L$ and $\omega_8^\perp \otimes \mathbb{Z}/2Z$ are isomorphic. In addition,

$$I^{1,8} = \mathbb{Z} \cdot \omega_8 \oplus \omega_8^\perp$$

is a Galois-invariant orthogonal splitting and therefore

$$\rho_\phi(\mathrm{Gal}(K)) \subset \mathrm{O}(\omega_8^\perp) \subset \mathrm{O}(I^{1,8}).$$

Here we identify $\mathrm{O}(\omega_8^\perp)$ with the subgroup of $\mathrm{O}(I^{1,8})$ that consists of all isometries preserving ω_8. This gives rise to the continuous homomorphism

$$\rho'_\phi : \mathrm{Gal}(K) \to \mathrm{O}(\omega_8^\perp) = W(E_8)$$

such that ρ_ϕ coincides with the composition of ρ'_ϕ and the inclusion map $\mathrm{O}(\omega_8^\perp) \subset \mathrm{O}(I^{1,8})$. Clearly, ρ'_ϕ is nothing else but the defining homomorphism of the Galois module $\omega_8^\perp$.

Lemma 4.2. *The Galois modules $J(C)_2$ and $\omega_8^\perp \otimes \mathbb{Z}/2Z$ are isomorphic.*

Proof. Since both Galois modules $J(C)_2$ and $\omega_8^\perp \otimes \mathbb{Z}/2Z$ are isomorphic to $L/2L$ (Remark 2.12 and Sect. 4.1), $J(C)_2$ and $\omega_8^\perp \otimes \mathbb{Z}/2Z$ are isomorphic. □

Theorem 4.3. *Let S be a Del Pezzo surface of degree 1 that is defined over K. Suppose that $\rho'_\phi(\mathrm{Gal}(K)) = W(E_8)$ or $W^+(E_8)$. Then $\mathrm{End}(J(C)) = \mathbb{Z}$.*

Proof. Recall (Sect. 2.1) that $W^+(E_8) = \mathrm{SO}(\omega_8^\perp) = \mathrm{SO}(Q(E_8))$. Replacing (if necessary) K by its suitable quadratic extension, we may and will assume that $\rho'_\phi(\mathrm{Gal}(K)) = W^+(E_8)$. By Lemma 4.2, $J(C)_2$ and $\omega_8^\perp \otimes \mathbb{Z}/2Z$ are isomorphic. In light of Theorem 3.15, in order to finish the proof, it suffices to check that the image of $W^+(E_8)$ in $\mathrm{Aut}(Q(E_8) \otimes \mathbb{Z}/2\mathbb{Z})$ is isomorphic to $\mathrm{O}^+(8)$. But this assertion follows easily from [1, Ch. VI, Sect. 4, Ex. 1]. □

Theorem 4.4. *Let S be a Del Pezzo surface of degree 1 that is defined over K. Suppose that $\rho'_\phi(\mathrm{Gal}(K))$ contains a subgroup that is a conjugate of $\iota(\mathbf{A}_8)$ in $W(E_8)$.*

Then $\mathrm{End}^0(J(C))$ is either $\mathbb{Q}$ or a quadratic field. In particular, $J(C)$ is absolutely simple.

Proof. Replacing ϕ by its composition with a suitable element of $W(E_8) = \mathrm{O}(\omega_8^\perp)$, we may and will assume that $\rho'_\phi(\mathrm{Gal}(K))$ contains $\iota(\mathbf{A}_8)$. Replacing (if necessary) K by its suitable finite algebraic extension, we may and will assume that

$$\rho'_\phi(\mathrm{Gal}(K)) = \iota(\mathbf{A}_8).$$

Clearly, the map

$$\rho_{\mathbf{A}} : \mathrm{Gal}(K) \to \mathbf{A}_8,\ \sigma \mapsto \iota^{-1}(\rho'_\phi(\sigma))$$

is a continuous *surjective* group homomorphism and

$$\rho'_\phi = \iota\ \rho_{\mathbf{A}}.$$

Let us consider the 8-element set $\mathcal{B} = \{1, 2 \dots, 8\}$ and the 8-dimensional vector space $\mathbb{F}_2^8 = \mathbb{F}_2^{\mathcal{B}}$ provided with the natural structure of $\mathbf{A}_8$-module. The surjective homomorphism $\rho_{\mathbf{A}} : \mathrm{Gal}(K) \twoheadrightarrow \mathbf{A}_8$ provides $\mathbb{F}_2^8$ with the natural structure of $\mathrm{Gal}(K)$-module; in addition, the image of $\mathrm{Gal}(K)$ in $\mathrm{Aut}(\mathbb{F}_2^8)$ coincides with $\mathbf{A}_8$. It follows from Lemma 3.13 that the Galois modules $\omega_8^{\perp} \otimes \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{F}_2^8$ are isomorphic. On the other hand, thanks to Lemma 4.2, $J(C)_2$ and $\omega_8^{\perp} \otimes \mathbb{Z}/2Z$ are isomorphic. This implies that the Galois modules $\mathbb{F}_2^{\mathcal{B}} = \mathbb{F}_2^8$ and $J(C)_2$ are isomorphic. Now the assertion follows from Theorem 3.7. □

4.5. Let $B \subset \mathbb{P}^2(\bar{K})$ be an 8-element set of points on the projective plane that enjoys the following properties:

(i) The set B is *general position*, i.e., no 3 points lie on a line, no 6 points line on a conic, B does not lie on a singular cubic in such a way that the singular point belongs to B.
(ii) The group $\mathrm{Gal}(K)$ permutes transitively points of B and therefore we get a natural homomorphism $\rho_B : \mathrm{Gal}(K) \to \mathrm{Perm}(B) \cong \mathrm{S}_8$ from $\mathrm{Gal}(K)$ to the group $\mathrm{Perm}(B)$ of permutations of B.

We write G_B for the image of $\mathrm{Gal}(K)$ in $\mathrm{Perm}(B)$ and consider the 8-dimensional $\mathbb{F}_2$-vector space $\mathbb{F}_2^B$ of all $\mathbb{F}_2$-valued functions on B provided with the natural structure of Galois module. Let $K(B) \subset \bar{K}$ be the smallest extension of K over which every point of B is defined. Clearly, $K(B)/K$ is a finite Galois extension that corresponds to the kernel of $\mathrm{Gal}(K) \twoheadrightarrow G_B$ and $\mathrm{Gal}(K(B)/K)$ is canonically isomorphic to G_B.

Let S_B be surface that is obtained by blowing up points of B. Then S_B is defined over K. Since B is in general position, S_B is a Del Pezzo surface of degree 1 ([11, Sect. 3], [3, Th. 1 on p. 27]). We write C_B for the corresponding branch curve.

Lemma 4.6. *The Galois modules $J(C_B)_2$ and $\mathbb{F}_2^B$ are isomorphic. In particular, $K(J(C_B)_2) = K(B)$, the groups $\tilde{G}_{2,J(C_B),K}$ and G_B are isomorphic and the field extension $K(J(C_B)_2)/K$ corresponds to the kernel of*

$$\mathrm{Gal}(K) \twoheadrightarrow G_B \subset \mathrm{Perm}(B).$$

Proof. Recall that $J(C_B)_2 = \mathrm{Pic}(C_B)_2$. In light of Remark 2.12, it suffices to check that the Galois modules $\mathbb{F}_2^B$ and $L/2L$ are isomorphic.

We mimick the proof of Lemma 3.13. For each $b \in B$ we write ℓ_b for the class in $\mathrm{Pic}(S_B)$ of the corresponding exceptional curve in S. We write f_0 for the class in $\mathrm{Pic}(S_B)$ of the preimage of line in $\mathbb{P}^2$. Clearly,

$$\sigma(f_0) = f_0,\ \ell_{\sigma(b)} = \sigma(\ell_b)\ \forall b \in B, \sigma \in \mathrm{Gal}(K).$$

It is known [16, Sect. 25.1.2] that f_0 and $\{\ell_b\}_{b \in B}$ constitute a basis of the free commutative group $\mathrm{Pic}(S_B)$,

$$K_{S_B} = -3f_0 + \sum_{b \in B} \ell_B \in \mathrm{Pic}(S_B),$$

$$(f_0, f_0) = 1, (\ell_b, \ell_b) = -1, (\ell_b, f_0) = 0\ \forall b \in B$$

and $(\ell_{b_1}, \ell_{b_2}) = 0$ if $b_1 \neq b_2$.

Recall that $(\mathrm{K}_{S_B}, \mathrm{K}_{S_B}) = 1$. It follows that $\mathrm{Pic}(S_B)$ splits into orthogonal Galois-invariant direct sum

$$\mathrm{Pic}(S_B) = \mathbb{Z} \cdot \mathrm{K}_{S_B} \oplus L.$$

We write $\bar{f}_0$ and $\bar{\ell}_b$ for the images in $\mathrm{Pic}(S_B)/2\mathrm{Pic}(S_B)$ of f_0 and ℓ_b respectively. Clearly, the image of K_{S_B} in $\mathrm{Pic}(S_B)/2\mathrm{Pic}(S_B)$ coincides with

$$\bar{\omega} := \bar{f}_0 + \sum_{b\in B} \bar{\ell}_b;$$

notice that $\bar{f}_0$ and $\{\bar{\ell}_b\}_{b\in B}$ constitute a basis of the $\mathbb{F}_2$-vector space $\mathrm{Pic}(S_B)/2\mathrm{Pic}(S_B)$. The unimodular intersection pairing on $\mathrm{Pic}(S_B)$ induces a non-degenerate pairing

$$\mathrm{Pic}(S_B)/2\mathrm{Pic}(S_B) \times \mathrm{Pic}(S_B)/2\mathrm{Pic}(S_B) \to \mathbb{F}_2.$$

Clearly, the splitting

$$\mathrm{Pic}(S_B)/2\mathrm{Pic}(S_B) = \mathbb{F}_2 \cdot \bar{\omega} \oplus L/2L$$

is Galois-invariant and orthogonal. In particular, $L/2L$ coincides with the orthogonal complement of $\bar{\omega}$ in $\mathrm{Pic}(S_B)/2\mathrm{Pic}(S_B)$. It follows that

$$L/2L = \{c\bar{f}_0 + \sum_{b\in B} c_b\bar{\ell}_b \mid c + \sum_{b\in B} c_b = 0\}.$$

Now the map

$$c\bar{f}_0 + \sum_{b\in B} c_b\bar{\ell}_b \to \{b \mapsto c_b\}$$

establishes an isomorphism of Galois modules $L/2L$ and $\mathbb{F}_2^B$. □

Let us consider the jacobian $J(C_B)$ of C_B; it is a four-dimensional abelian variety defined over K.

Theorem 4.7. *Suppose that $G_B = \mathrm{Perm}(B)$ or $\mathrm{Alt}(B)$. Then:*

(i) *$\mathrm{End}^0(J(C_B))$ is either $\mathbb{Q}$ or a quadratic field. In particular, $J(C_B)$ is absolutely simple.*

(ii) *Let $T \subset \mathbb{P}^2(\bar{K})$ be another Galois-invariant set of 8 points in general position. Assume that either G_T is a solvable group or $K(S)$ and $K(T)$ are linearly disjoint over K. Then the abelian varieties $J(C_B)$ and $J(C_T)$ are not isomorphic over $\bar{K}$.*

Proof. Replacing (if necessary) K by suitable quadratic extension, we may and will assume that $G_B = \mathrm{Alt}(B)$. Now, combining Theorem 3.7 and Lemma 4.6, we obtain the assertion (i). Applying Theorem 3.11 to $X = J(C_B)$ and $Y - J(C_T)$, we obtain the assertion (ii). □

The next statement explains how to construct points in general position.

Proposition 4.8. *Suppose that $E \subset \mathbb{P}^2$ is an absolutely irreducible cubic curve that is defined over K. Suppose that $B \subset E(K_a)$ is a 8-element set that is a $\mathrm{Gal}(K)$-orbit. Let us assume that the image G_B of $\mathrm{Gal}(K)$ in the group $\mathrm{Perm}(B)$ of all permutations of B coincides either with $\mathrm{Perm}(B)$ or with $\mathrm{Alt}(B)$. Then B is in general position.*

Proof. Notice that $\mathrm{Gal}(K)$ acts 3-transitively on B.

Step 1. Suppose that D is a line in $\mathbb{P}^2$ that contains three points of B say,

$$\{P_1, P_2, P_3\} \subset \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8\} = B.$$

Clearly, $D \bigcap E = \{P_1, P_2, P_3\}$. There exists $\sigma \in \mathrm{Gal}(K)$ such that $\sigma(\{P_1, P_2, P_3\}) = \{P_1, P_2, P_4\}$. It follows that the line $\sigma(D)$ contains $\{P_1, P_2, P_4\}$ and therefore

$\sigma(D) \bigcap E = \{P_1, P_2, P_4\}$. In particular, $\sigma(D) \ne D$. However, the distinct lines D and $\sigma(D)$ meet each other at *two* distinct points P_1 and P_2. Contradiction.

Step 2. Suppose that Y is a conic in $\mathbb{P}^2$ such that Y contains six points of B say, $\{P_1, P_2, P_3, P_4, P_5, P_6\} = B \setminus \{P_7, P_8\}$. Clearly, $Y \bigcap E = B \setminus \{P_7, P_8\}$. If Y is reducible, i.e., is a union of two lines D_1 and D_2 then either D_1 or D_2 contains (at least) three points of B, which is not the case, thanks to Step 1. Therefore Y is *irreducible*.

There exists $\sigma \in \mathrm{Gal}(K)$ such that $\sigma(P_1) = P_7, \sigma(P_8) = P_8$. Then $\sigma(P_7) = P_i$ for some positive integer $i \le 6$. This implies that $\sigma(B \setminus \{P_7, P_8\}) = B \setminus \{P_i, P_8\}$ and the irreducible conic $\sigma(Y)$ contains $B \setminus \{P_i, P_8\}$. Clearly, $\sigma(Y) \bigcap E = B \setminus \{P_i, P_8\}$ contains P_7. In particular, $\sigma(Y) \ne Y$. However, both conics contain the 5-element set $B \setminus \{P_i, P_7, P_8\}$. Contradiction.

Step 3. Suppose that Z is a cubic in $\mathbb{P}^2$ such that $B \subset Z$ and say, $P_1 \in B$ is a singular point of Z. If Z is reducible then either there is a line with 3 points of B or a conic with 6 points of B. So, Z is irreducible and therefore P_1 is the only singular point of Z. Clearly, for each $\sigma \in \mathrm{Gal}(K)$ the cubic $\sigma(Z)$ also contains B and $\sigma(P_1)$ is the only singular point of $\sigma(Z)$. Pick σ with $\sigma(P_1) = P_2 \in B$. Then $\sigma(Z) \ne Z$. The cubics Z and $\sigma(Z)$ meet at all 8 points of B. In addition, the local intersection index at singular P_1 and $\sigma(P_1) = P_2$ is, at least, 2. This implies that the intersection index of Z and $\sigma(Z)$ is, at least 10, which is not true, since the index is 9. □

Proof of Theorem 1.1. Let $f(t) \in K[t]$ be an irreducible degree 8 polynomial, whose Galois group $\mathrm{Gal}(f)$ is either $\mathbf{S}_8$ or $\mathbf{A}_8$. Let $\mathfrak{R} \subset K_a$ be the set of roots of f. Then the 8-element set

$$B(h) = \{(\alpha^3 : \alpha : 1) \in \mathbb{P}^2(K_a) \mid \alpha \in \mathfrak{R}\}$$

lies on the absolutely irreducible K-cubic $xz^2 - y^3 = 0$ and $G_{B(h)} \cong \mathbf{S}_8$ or $\mathbf{A}_8$ respectively. It follows from Proposition 4.8 that $B(f)$ is in general position, which proves (i). Clearly, $K(B(f))$ coincides with the *splitting field* $K(\mathfrak{R})$ of f. Therefore

$$G_{B(f)} = \mathrm{Gal}(K(B(f))/K) = \mathrm{Gal}(K(\mathfrak{R})/K) = \mathrm{Gal}(f),$$

which implies that $G_{B(f)}$ is either $\mathrm{Perm}(B)$ or $\mathrm{Alt}(B)$. Now the assertions (ii) and (iii) follow from the first and second assertions of Theorem 4.7 respectively.

□

Example 4.9. Let $L = \mathbb{C}(y_1, \dots, y_8)$ be the field of rational functions in 8 independent variables over $\mathbb{C}$. There is the natural action of $\mathbf{S}_8$ on L by $\mathbb{C}$-linear field automorphisms such that each permutation s sends every y_i to $y_{s(i)}$. Let K be the subfield of $\mathbf{S}_8$-invariants of L. Clearly, $\mathbb{C} \subset L$, the field extension L/K is a finite Galois extension, $\mathrm{Gal}(L/K) = \mathbf{S}_8$ and $\bar{L} = \bar{K}$. Let us choose $c \in K$ (e.g., $c = 0$ or $c = (\sum_{i=1}^8 y_i)/8$) and consider the 8-element set

$$B = \{(y_i - c)^3 : (y_i - c) : 1) \mid 1 \le i \le 8\} \subset \mathbb{P}^2(L) \subset \mathbb{P}^2(\bar{L}) = \mathbb{P}^2(\bar{K}).$$

Clearly, B is $\mathrm{Gal}(K)$-invariant and $G_B = \mathrm{Perm}(B)$. It follows that B is in *in general position*.

Applying Theorem 4.7, we conclude that $\mathrm{End}^0(J(C_B))$ is either $\mathbb{Q}$ or a quadratic field; in particular, $J(C_B)$ is an (absolutely) simple abelian variety.

5. Explicit formulas

Let $h(t) \in K[t]$ be an irreducible degree 8 polynomial, whose Galois group is either $\mathbf{S}_8$ or $\mathbf{A}_8$. In order to simplify slightly our computations, we assume that $h(t)$ is *monic* and the sum of its roots iz zero, i.e.,

$$h(t) = t^8 + \sum_{i=0}^{6} h_i t^i;\ h_i \in K.$$

The irreducibility of $h(t)$ implies that $h_0 \ne 0$. Let $K[t]_7$ be the 8-dimensional subspace in $K[t]$ that consists of all polynomials, whose degree does not exceed 7. We write

$$D_h : K[t] \twoheadrightarrow K[t]_7$$

for the surjective K-linear map that sends any polynomial into its remainder with respect to division by $h(t)$. By definition, $f - D_h(f)$ is divisible by h for all $f \in K[t]$.

Let $K[x]$ and $K[x,y]$ be the ring of polynomials in independent variables x and x, y respectively. We write

$$A : K[t] \to K[x] \oplus y \cdot K[x] \oplus y^2 \cdot K[x] \subset K[x,y]$$

for the K-linear map that sends t^{3i} to x^i, t^{3i+1} to $x^i y$ and t^{3i+2} to $x^i y^2$ respectively (for each nonnegative integer i).

Clearly, if $g(t) \in K[t]$ and $G(x,y) = A(g)$ then $g(t) = G(t^3, t)$ and $G(x,y) - g(y)$ is divisible by $x - y^3$ in $K[x,y]$. In addition, $\deg(G) \ge \deg(g)/3$. On the other hand, if $\deg(g) \le 3d$ for some positive integer d and g does *not* have a term of degree $3d-1$ then $\deg(G) \le d$. For example, if $\deg(g) = 9$ and g does not contain term t^8 then G contains term x^3 and $\deg(G) = 3$. Another examples: a)if $\deg(g) \le 7$ then $\deg(G) \le 3$; b)if $\deg(g) = 16$ then G contains term $x^5 y$ and $\deg(G) = 6$.

Let us put

$$B = B(h).$$

Our first goal is to describe explicitly the (two-dimensional) $\bar{K}$-vector space H of all cubic forms (in homogeneous coordinates $(x : y : z)$ and with coefficients in $\bar{K}$) that do vanish at all points of B and find the "nineth point". Clearly, one of those forms is $u := xz^2 - y^3$. Another cubic form $v(x,y,z)$ is defined by $v(x,y,1) = A(th(t))$. Since $v(x,y,1) - yh(y) = A(th(t)) - yh(y)$ is divisible by $x - y^3$, the form v does vanish at all points of B. Since $th(t)$ has degree 9, the polynomial $A(th(t))$ contains the term x^3 and therefore has x-degree 3. It follows that v also has x-degree 3. Since u and v have different x-degrees, they are not proportional one to another and therefore the two-dimensional

$$H = \bar{K} \cdot u \oplus \bar{K} \cdot v.$$

Clearly, both u and v do vanish at $(0:0:1)$: this is the nineth point [10, Ch. 5, Sect. 4, Cor. 4.5] and the set of common zeros of u and v coincides with $B \cup \{(0:0:1)\}$.

Recall that S_B is obtained from $\mathbb{P}^2$ by blowing up points of B. We write

$$g_B : S_B \to \mathbb{P}^2$$

for the corresponding regular birational map. For each $b \in B$ its preimage $E_b := g_B^{-1}(b)$ is a smoth projective rational curve with self-intersection index -1. By definition, g_B establishes a biregular isomorphism between $S_B \setminus \bigcup_{b \in B} E_b$ and $\mathbb{P}^2 \setminus B$.

Clearly, the line $L : z = 0$ does not meet B. Further, we view L as a divisor on $\mathbb{P}^2$. It is known [16, Sect. 25.1 and 25.1.2 on pp. 126–127] that

$$\mathrm{K}_{S_B} := -3g_B^*(L) + \sum_{b\in B} E_b = -g_B^*(3L) + \sum_{b\in B} E_b$$

is a *canonical* divisor on S_B. Clearly, for each form $q \in H$ the rational function q/z^3 on $\mathbb{P}^2$ satisfies $\mathrm{div}(q/z^3) + 3L \geq 0$, i.e., $q/z^3 \in \Gamma(\mathbb{P}^2, 3L)$. Also q/z^3 is defined and vanishes at every point in B. It follows that q/z^3 (viewed as a rational function on S_B) lies in $\Gamma(S_B, 3g_B^*(L) - \sum_{b\in B} E_b) = \Gamma(S_B, -\mathrm{K}_{S_B})$. Since the latter space is two-dimensional,

$$\Gamma(S_B, -\mathrm{K}_{S_B}) = \bar{K} \cdot \frac{u}{z^3} \oplus \bar{K} \cdot \frac{v}{z^3}.$$

This gives us a rational anticanonical map

$$S_B \xrightarrow{g_B} \mathbb{P}^2 \xrightarrow{(u:v)} \mathbb{P}^1,$$

which is regular outside the (preimage of the) base point $(0 : 0 : 1)$.

Now let us consider the space H_2 of degree 6 forms that vanish with all its partial derivatives of first order at every point of B. For example,

$$u^2, uv, v^2 \in H_2;$$

they are linearly independent over $\bar{K}$, because they have (distinct) x-degrees $2, 4, 6$ respectively. (Notice that all of them do vanish at $(0 : 0 : 1)$.) One may easily check (using, for instance, [25, Ch. IV, Sect. 3.1]) that if $F \in H_2$ then F/z^6 (viewed as a rational function on S_B) lies in $\Gamma(S_B, 6g_B^*(L) - \sum_{b\in B} 2E_b) = \Gamma(S_B, -2\mathrm{K}_{S_B})$. Recall [3, p. 68] that the space $\Gamma(S_B, -2\mathrm{K}_{S_B})$ is four-dimensional. This implies that if a form $w \in H_2$ does not vanish at $(0 : 0 : 1)$ then it is *not* a linear combination of u^2, uv, v^2 and therefore $\{u^2, uv, v^2, w\}$ is a basis of H_2 and

$$\Gamma(S_B, -2\mathrm{K}_{S_B}) = \bar{K} \cdot \frac{u^2}{z^6} \oplus \bar{K} \cdot \frac{uv}{z^6} \oplus \bar{K} \cdot \frac{v^2}{z^6} \oplus \bar{K} \cdot \frac{w}{z^6}.$$

This gives us a regular doubly-anticanonical map

$$\pi_B : S_B \xrightarrow{g_B} \mathbb{P}^2 \xrightarrow{(u^2:uv:v^2:w)} \mathbb{P}^3.$$

Recall that C_B is the branch curve of π_B. This allows us to describe explicitly the plane projective curve $g_B(C_B)$, which is birationally isomorphic to C_B. Indeed, $g_B(C_B) \setminus B$ coincides with the set of points of $\mathbb{P}^2 \setminus B$ where the the tangent map to

$$(x : y : z) \mapsto (u(x, y, z)^2 : u(x, y, z)v(x, y, z) : v(x, y, z)^2 : w(x, y, z))$$

is *not* injective. Since $B \bigcup \{(0 : 0 : 1)\}$ is the set of common zeros of F_1 and F_2, the curve $g_B(C_B) \setminus B \setminus \{(0 : 0 : 1)\}$ coincides with the set of points of $\mathbb{P}^2 \setminus B \setminus \{(0 : 0 : 1)\}$ where the form

$$Q(x, y, z) := \begin{vmatrix} u_x & u_y & u_z \\ v_x & v_y & v_z \\ w_x & w_y & w_z \end{vmatrix}$$

does vanish. Since C_B is an irreducible projective curve, $g_B(C_B)$ is also projective ireducible and coincides with the set of zeros of Q, i.e.,

$$g_B(C_B) = \{(x : y : z) \in \mathbb{P}^2 \mid Q(x, y, z) = 0\} \subset \mathbb{P}^2.$$

Clearly, Q has coefficients in K and degree 9. Since $g_B(C_B)$ is irreducible and C_B has genus 4, the curve C_B is singular and $Q(x, y, z)$ is an irreducible polynomial.

Indeed, if Q is reducible then the irreducibility of $g_B(C_B)$ implies that Q is a power of an irreducible polynomial, i.e., Q is either a 9th power of a linear form or a cube of a cubic form. In the former case, $g_B(C_B)$ has genus 0 while in the latter one its genus is either 0 or 1. However, $g_B(C_B)$ is birationally isomorphic to the genus 4 curve C_B, which rules out both possibilities for the reducibility of Q. Since $\deg(Q) = 9$ and $4 \ne (9-1)(9-2)/2$, the curve $g_B(C_B)$ is singular. Clearly, all its singular points must lie in B. Since Q has coefficients in K and B constitutes a Galois orbit, all points of B are singular and have the same multiplicity. A well-known formula for the genus of (the normalization of) a plane curve [25, Ch. IV, Sect. 4.1] implies that all points of B have multiplicity 3.

The rest of this Section is devoted to an explicit construction of w. Let us consider the polynomial

$$h(t)^2 = t^{16} + \sum_{i=0}^{14} c_i t^i,\ c_i \in K, c_0 = h_0^2 \ne 0.$$

Clearly, all the coefficients c_i can be expressed explicitly in terms of the coefficients of $h(t)$. Let us put $F(x,y) := A(h(t)^2)$. Clearly, $\deg(F) = 6$ and $F(x,y) - h(y)^2$ is divisible by $x - y^3$. In particular, F does vanish at all points (α^3, α) where α is a root of $h(t)$. It also follows that $3y^2F_x + F_y$ does vanish at (α^3, α). (On the other hand, F does *not* vanish at $(0,0)$.) If $G(x,y)$ is any polynomial then clearly, both $H(x,y) = F(x,y) - G(x,y)(x - y^3)$ and $3y^2H_x + H_y$ do vanish at (α^3, α) while H does *not* vanish at $(0,0)$. I want to find such G that $\deg(G) \le 3$ and H_x does vanish at all (α^3, α). Since $3y^2H_x + H_y$ do vanish at (α^3, α), we conclude that both H_x and H_y do vanish at each (α^3, α). After that, we define the degree 6 form w by $w(x,y,1) := H(x,y)$, i.e.

$$w(x,y,z) = z^6 H(x/z, y/z).$$

Clearly, w vanishes at all points of $B = B(h)$ with its partial derivatives of first order with respect to x and to y. By Euler's theorem,

$$xw_x + yw_y + zw_z = 6w.$$

It follows that w_z also does vanish at all points of B. However,

$$w(0,0,1) = H(0,0) \ne 0.$$

So, such w enjoys the desired properties and now our task boils down to finding such H (i.e., finding such G).

Now let us put

$$p(t) := D_h(F_x(t^3,t)) \in K[t]_7 \subset K[t],\ G(x,y) := A(p(t)) = A(D_h(F_x(t^3,t)).$$

I claim that $\deg(G) \le 3$ and $G(\alpha^3, \alpha) = F_x(\alpha^3, \alpha)$. Indeed, $\deg(p(t)) \le 7$ and therefore $G(x,y) = A(p(t))$ has degree, at most 3. Since $F_x(t^3,t) - D_h(F_x(t^3,t)$ is divisible by $h(t)$ and $h(\alpha) = 0$, the values of $F_x(t^3,t)$ and $p(t)$ at $t = \alpha$ do coincide, i.e., $F_x(\alpha^3, \alpha) = p(\alpha)$. On the other hand, $G(x,y) - p(y)$ is divisible by $x - y^3$ and therefore $G(\alpha^3, \alpha) = p(\alpha)$. We have

$$G(\alpha^3, \alpha) = p(\alpha) = F_x(\alpha^3, \alpha).$$

If we put (as above) $H := F - (x - y^3)G$ then

$$H_x(\alpha^3, \alpha) = F_x(\alpha^3, \alpha) - \{G_x(\alpha^3, \alpha)\cdot(\alpha^3 - \alpha^3) + G(\alpha^3, \alpha)\cdot 1\} = F_x(\alpha^3, \alpha) - G(\alpha^3, \alpha) = 0.$$

We are done.

References

[1] N. Bourbaki, Groupes et algèbres de Lie, Chapitres IV, V, VI. Hermann, Paris, 1968.

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

[3] M. Demazure, *Surfaces de Del Pezzo* II, III, IV, V. In: Séminaire sur les singularités des surfaces (M. Demazure, H. Pinkham, B. Teissier, ed.), Springer Lecture Notes in Math. **777** (1980), 23–69.

[4] I. Dolgachev, D. Ortland, Point sets in projective spaces and theta functions, Astérisque **165** (1986).

[5] I. Dolgachev, Topics in classical agebraic geometry, Part 1, Chapters 1–11; available at http://www.math.lsa.umich.edu/ idolga/lecturenotes.html .

[6] T. Ekedahl, *An effective version of Hilbert's irreducibility theorem*. In: Séminaire de Théorie des Nombres, Paris 1988-89. Birkhäuser, Boston 1990, pp. 241–249.

[7] A. Elkin, Yu. G. Zarhin, *Endomorphism algebras of hyperelliptic Jacobians and finite projective lines*. J. Ramanujan Math. Soc. **21** (2006), 169–187; arXiv:math.AG/0508120 .

[8] R. Erné, *Construction of a del Pezzo surface with maximal Galois action on its Picard group*. J. Pure Applied Algebra **97** (1994), 15–27.

[9] W. Feit, J. Tits, *Projective representations of minimum degree of group extensions*. Canad. J. Math. **30** (1978), 1092–1102.

[10] R. Hartshorne, Algebraic Geometry, GTM **52**, Springer-Verlag, 1977.

[11] V. A. Iskovskikh, *Minimal models of rational surfaces over arbitrary fields*. Izv. Akad. Nauk Ser. Mat. **43** (1979), 19–43; Math. USSR-Izv. **14** (1980), 17–39.

[12] Ch. Jansen, Kl. Lux, R. Parker and R. Wilson, The Atlas of Brauer Characters. Oxford University Press, 1995.

[13] P. B. Kleidman, M. W. Liebeck, *On a theorem of Feit and Tits*. Proc. Amer. Math. Soc. **107** (1989), 315–322.

[14] S. Lang, *Introduction to algebraic and abelian functions*, 2nd edition. GTM **89**, Springer Verlag New York, 1982.

[15] Yu. I. Manin, *Rational surfaces over perfect fields*. II. Mat. Sb. (N.S.) **72 (114)** (1967), 161–192; Math USSR Sbornik **1** (1967), 141–168.

[16] Yu. I. Manin, Cubic forms, second edition, North Holland, 1986.

[17] B. Mortimer, *The modular permutation representations of the known doubly transitive groups*. Proc. London Math. Soc. (3) **41** (1980), 1–20.

[18] D. Mumford, Abelian varieties, 2nd edn, Oxford University Press, 1974.

[19] D. Mumford, *Theta characteristics of an algebraic curve*. Annales Sci. ENS (4) **4** (1971), 181–192.

[20] F. Oort, *Endomorphism algebras of abelian varieties*. In: Algebraic Geometry and Commutative Algebra in Honor of M. Nagata (Ed. H. Hijikata et al), Kinokuniya Cy, Tokyo 1988; Vol. **II**, pp. 469 - 502.

[21] D.S. Passman, Permutation groups. W.A. Benjamin, Inc., New York Amsterdam, 1968.

[22] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*. J. Pure Applied Algebra **77** (1992), 253–262.

[23] J.-P. Serre, Lectures on Mordell-Weil Theorem. 2nd ed. Braunschweig and Wisbaden, F. Viehweg und Sohn, 1989.

[24] J.-P. Serre, Topics in Galois Theory. Boston and London, Jones and Bartlett Publ. 1992.

[25] I. R. Shafarevich, Basic Algebraic Geometry, 2nd edition, vol. 1. Springer Verlag, 1994.

[26] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Res. Letters **7** (2000), 123–132.

[27] Yu. G. Zarhin, *Hyperelliptic jacobians and modular representations*. In: Moduli of abelian varieties (eds. C. Faber, G. van der Geer and F. Oort). Progress in Math., vol. **195** (2001), Birkhäuser, pp. 473–490.

[28] Yu. G. Zarhin, *Very simple representations: variations on a theme of Clifford*. In: Progress in Galois Theory (H. Völklein, T. Shaska eds.), Springer Verlag, 2005, pp. 151–168.

[29] Yu. G. Zarhin, *Homomorphisms of abelian varieties*. In: "Arithmetic, Geometry and Coding Theory (AGCT 2003)" (Y. Aubry, G. Lachaud, eds.), Séminaires et Congrés **11** (2005), 189–215.

[30] Yu. G. Zarhin, *Del Pezzo surfaces of degree* 2 *and jacobians without complex multiplication*. Proceedings of St. Petersburg Math. Soc. **11** (2005), 81–91; AMS Translations - Series 2, vol. **218** (2006), 67–75; arXiv:math.AG/0405156 .
[31] Yu. G. Zarhin, *Endomorphisms of superelliptic jacobians*. arXiv:math.AG/0605028 .

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA
E-mail address: zarhin@math.psu.edu