DEL PEZZO SURFACES OF DEGREE 2 AND JACOBIANS WITHOUT COMPLEX MULTIPLICATION

YU. G. ZARHIN

To my friend Sergei Vostokov

1. Notations and Statements

In a series of his articles [10, 12, 13, 15] the author constructed explicitly m-dimensional abelian varieties without non-trivial endomorphisms for every m > 1. This construction may be described as follows. Let $K_a$ be an algebraic closure of a perfect field $K$ with char($K$) $\neq 2$. Let $n = 2m + 1$ or $2m + 2$. Let us choose an $n$-element set $R \in K_a$ that constitutes a Galois orbit over $K$ and assume, in addition, that the Galois group of $K(R)$ over $K$ is “big” say, coincides with full symmetric group $S_n$ or the alternating group $A_n$. Let $f(x) \in K[x]$ be the irreducible polynomial of degree $n$, whose set of roots coincides with $R$. Let us consider the hyperelliptic curve $C_f$: $y^2 = f(x)$ over $K_a$ and let $J(C_f)$ be its jacobian which is the $m$-dimensional abelian variety. Then the ring $\text{End}(J(C_f))$ of all $K_a$-endomorphisms of $J(C_f)$ coincides with $\mathbb{Z}$ if either $n > 6$ or char($K$) $\neq 3$.

The aim of this paper is to construct abelian threefolds without complex multiplication, using jacobians of non-hyperelliptic curves of genus 3. It is well-known that these curves are smooth plane quartics and closely related to Del Pezzo surfaces of degree 2. (We refer to [8, 6, 7, 2, 3, 4, 9] for geometric and arithmetic properties of Del Pezzo surfaces. In particular, relations between the degree 2 case and plane quartics are discussed in detail in [2, 3, 4]). On the other hand, Del Pezzo surfaces of degree 2 could be obtained by blowing up seven points on the projective plane $\mathbb{P}^2$ when these points are in general position, i.e., no three points lie on a one line, no six on a one conic ([6, §3], [2, Th. 1 on p. 27]).

In order to describe our construction, let us start with the projective plane $\mathbb{P}^2$ with homogeneous coordinates $(x : y : z)$. Let us consider a 7-element set $B \subset \mathbb{P}^2(K_a)$ of points in general position and assume that the absolute Galois group $\text{Gal}(K)$ of $K$ permutes elements of $B$ in such a way that $B$ constitutes a Galois orbit. We write $Q_B$ for the 6-dimensional $\mathbb{F}_2$-vector space of maps $\varphi : B \to \mathbb{F}_2$ with $\sum_{b \in B} \varphi(b) = 0$. The action of $\text{Gal}(K)$ on $B$ provides $Q_B$ with the natural structure of $\text{Gal}(K)$-module. Let $G_B$ be the image of $\text{Gal}(K)$ in the group $\text{Perm}(B) \cong S_7$ of all permutations of $B$. Clearly, $Q_B$ carries a natural structure of faithful $\text{Perm}(B)$-module and the structure homomorphism $\text{Gal}(K) \to \text{Aut}(Q_B)$ coincides with the composition of $\text{Gal}(K) \to G_B$ and $G_B \subset \text{Perm}(B) \to \text{Aut}(Q_B)$.

Let $H_B$ be the $K_a$-vector space of homogeneous cubic forms in $x, y, z$ that vanish on $B$. It follows from proposition 4.3 and corollary 4.4(i) in Ch. 5, §4 of [5] that $H_B$ is 3-dimensional and $B$ coincides with the set of common zeros of elements of $H_B$. Since $B$ is $\text{Gal}(K)$-invariant, $H_B$ is defined over $K$, i.e., it has a $K_a$-basis $u, v, w$ such that the forms $u, v, w$ have coefficients in $K$.
We write $V(B)$ for the Del Pezzo surface of degree 2 obtained by blowing up $B$. Then $V(B)$ is a smooth projective surface that is defined over $K$ (see Remark 19.5 on pp. 89–90 of [8]). We write
definition

$$g_B : V(B) \to \mathbb{P}^2$$

for the corresponding birational map defined over $K$. Recall that for each $b \in B$ its preimage $E_b$ is a a smooth projective rational curve with self-intersection number $-1$. By definition, $g_B$ establishes a $K$-biregular isomorphism between $V(B) \setminus \bigcup_{b \in B} E_b$ and $\mathbb{P}^2 \setminus B$. Clearly,

$$\sigma(E_b) = E_{\sigma(b)} \quad \forall \ b \in B, \sigma \in \text{Gal}(K).$$

Let $\Omega_{V(B)}$ be the canonical (invertible) sheaf on $V(B)$. Let us consider the line $L : z = 0$ as a divisor in $\mathbb{P}^2$. Clearly, $B$ does not meet the $K$-line $L$; otherwise, the whole $\text{Gal}(K)$-orbit $B$ lies in $L$ which is not true, since no 3 points of $B$ lie on a one line. It is known [8, Sect. 25.1 and 25.1.2 on pp. 126–127] that

$$K_{V(B)} := -3g_B^*(L) + \sum_{b \in B} E_b = -g_B^*(3L) + \sum_{b \in B} E_b$$

is a canonical divisor on $V(B)$. Clearly, for each form $q \in H_B$ the rational function $\frac{1}{z} \text{ div}(\frac{a}{z}) + 3L \geq 0$, i.e., $\frac{a}{z} \in \Gamma(\mathbb{P}^2, 3L)$. Also $\frac{1}{z}$ is defined and vanishes at every point of $B$. It follows easily that $\frac{a}{z}$ (viewed as rational function on $V(B)$) lies in $\Gamma(V(B), 3g_B^*(L) - \sum_{b \in B} E_b) = \Gamma(V(B), -K_{V(B)})$. Since $\Gamma(V(B), -K_{V(B)})$ is 3-dimensional [8, theorem 24.5 on p. 121],

$$\Gamma(V(B), -K_{V(B)}) = K_a \cdot \frac{u}{z^3} \oplus K_a \cdot \frac{v}{z^3} \oplus K_a \cdot \frac{w}{z^3}.$$

Using proposition 4.3 in [5, Ch. 5, §4], one may easily get a well-known fact that the sections of $\Gamma(V(B), -K_{V(B)})$ have no common zeros on $V(B)$. This gives us a regular anticanonical map

$$\pi : V(B) \xrightarrow{g_B} \mathbb{P}^2 \xrightarrow{(u:v:w)} \mathbb{P}^2$$

which is obviously defined over $K$. It is known that $\pi$ is a regular double cover map, whose ramification curve is a smooth quartic

$$C_B \subset \mathbb{P}^2$$

(see [2, pp. 67–68], [3, Ch. 9]). Clearly, $C_B$ is a genus 3 curve defined over $K$. Let $J(B)$ be the jacobian of $C_B$; clearly, it is a three-dimensional abelian variety defined over $K$. We write $\text{End}(J(B))$ for the ring of $K_a$-endomorphisms of $J(B)$.

The following assertion is based on Lemmas 1-2 on pp. 161–162 of [3].

**Lemma 1.1.** Let $J(B)_2$ be the kernel of multiplication by 2 in $J(B)(K_a)$. Then the Galois modules $J(B)_2$ and $Q_B$ are canonically isomorphic.

Using Lemma [1,1] and results of [10,15], one may obtain the following statement.

**Theorem 1.2.** Let $B \subset \mathbb{P}^2(K_a)$ be a 7-element set of points in general position. Assume that $\text{Gal}(K)$ permutes elements of $B$ and the image of $\text{Gal}(K)$ in $\text{Perm}(B) \cong S_7$ coincides either with the full symmetric group $S_7$ or with the alternating group $A_7$. Then $\text{End}(J(B)) = Z$.

This leads to a question: how to construct such $B$ in general position? The next lemma provides us with desired construction.
Lemma 1.3. Let $f(t) \in K[t]$ be a separable irreducible degree 7 polynomial, whose 
Galois group $\text{Gal}(f)$ is either $S_7$ or $A_7$. Let $\mathfrak{A}_f \subset K_a$ be the 7-element set of roots 
of $f$. Then the 7-element set
\[ B_f = \{ (\alpha^3 : \alpha : 1) \mid \alpha \in \mathfrak{A}_f \} \subset \mathbb{P}^2(K_a) \]
is in general position.

Clearly, $\text{Gal}(K)$ permutes transitively elements of $B_f$ and the image of $\text{Gal}(K)$ 
in $\text{Perm}(B)$ coincides either with $S_7$ or with $A_7$; in particular, $B_f$ constitutes a 
Galois orbit. This implies the following statement.

Corollary 1.4. Let $f(t) \in K[t]$ be a separable irreducible degree 7 polynomial, 
whose Galois group $\text{Gal}(f)$ is either $S_7$ or $A_7$. Then $\text{End}(J(B_f)) = \mathbb{Z}$.

2. Proofs

Proof of Lemma 1.3. Let $\text{Pic}(V(B))$ be the Picard group of $V(B)$ over $K_a$. It is 
known [3 Sect. 25.1 and 25.1.2 on pp. 126–127] that $\text{Pic}(V(B))$ is a free commutative group of rank 8 provided with the natural structure of Galois module. More 
precisely, it has canonical generators $l_0 = \text{the class of } g_B(L)$ and $\{l_b\}_{b \in B}$ where $l_b$ 
is the class of the exceptional curve $E_b$. Clearly, $l_0$ is Galois invariant and
\[ \sigma(l_b) = l_{\sigma(b)} \quad \forall b \in B, \sigma \in \text{Gal}(K). \]
Clearly, the class of $K_{V(B)}$ equals $-3l_0 + \sum_{b \in B} l_b$ and obviously is Galois-invariant.
There is a non-degenerate Galois invariant symmetric intersection form
\[ (, ) : \text{Pic}(V(B)) \times \text{Pic}(V(B)) \to \mathbb{Z}. \]
In addition (ibid),
\[ (l_0, l_0) = 1, (l_b, l_0) = 0, (l_b, l_b) = -1, (l_b, l_{b'}) = 0 \quad \forall b \neq b'. \]
Clearly, the orthogonal complement $\text{Pic}(V(B))_0$ of $K_{V(B)}$ in $\text{Pic}(V(B))$ coincides with
\[ \{ a_0l_0 + \sum_{b \in B} a_bl_b \mid a_0, a_b \in \mathbb{Z}, -3a_0 + \sum_{b \in B} a_b = 0 \}; \]
it is a Galois-invariant pure free commutative subgroup of rank 7.

Notice that one may view $C_B$ as a $K$-curve on $V(B)$ [3 p. 160]. Then the 
inclusion map $C_B \subset V(B)$ induced the homomorphism of Galois modules
\[ r : \text{Pic}(V(B)) \to \text{Pic}(C_B) \]
where $\text{Pic}(C_B)$ is the Picard group of $C_B$ over $K_a$. Recall that $J(B)(K_a)$ is a Galois 
submodule of $\text{Pic}(C_B)$ that consists of divisor classes of degree zero. In particular, 
$J(B)_2$ coincides with the kernel $\text{Pic}(C_B)_2$ of multiplication by 2 in $\text{Pic}(C_B)$. It is 
known (Lemma 1 on p. 161 of [3]) that
\[ r(\text{Pic}(V(B))_0) \subset \text{Pic}(C_B)_2 = J(B)_2. \]
This gives rise to the homomorphism
\[ \tilde{r} : \text{Pic}(C_B)_0/2\text{Pic}(C_B)_0 \to J(B)_2, \quad D + 2\text{Pic}(C_B)_0 \mapsto r(D) \]
of Galois modules. By Lemma 2 on pp. 161-162 of [3], the kernel of \( \tilde{r} \) is as follows. The intersection form on Pic(\( V(B) \)) defines by reduction modulo 2 a symmetric bilinear form

\[
\psi : \text{Pic}(V(B))/2\text{Pic}(V(B)) \times \text{Pic}(V(B))/2\text{Pic}(V(B)) \to \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2,
\]

\[
D + 2\text{Pic}(V(B)), D' + 2\text{Pic}(V(B)) \mapsto (D, D') + 2\mathbb{Z}
\]

and we write

\[
\psi_0 : \text{Pic}(V(B))_0/2\text{Pic}(V(B))_0 \times \text{Pic}(V(B))_0/2\text{Pic}(V(B))_0 \to \mathbb{F}_2
\]

for the restriction of \( \psi \) to Pic(\( V(B) \))_0. Then the kernel (radical) of \( \psi_0 \) coincides with ker(\( \tilde{r} \)). (The same Lemma also asserts that \( \tilde{r} \) is surjective.)

Let us describe explicitly the kernel of \( \psi_0 \). Since Pic(\( V(B) \))_0 is a pure subgroup of Pic(\( V(B) \)), we may view Pic(\( V(B) \))_0/2Pic(\( V(B) \))_0 as a 7-dimensional \( \mathbb{F}_2 \)-vector subspace (even Galois submodule) in Pic(\( V(B) \))/2Pic(\( V(B) \)). Let \( \tilde{l}_0 \) (resp. \( \tilde{l}_b \)) be the image of \( l_0 \) (resp. \( l_b \)) in Pic(\( V(B) \))/2Pic(\( V(B) \)). Then \( \{ \tilde{l}_0, \{ \tilde{l}_b \}_{b \in B} \} \) constitute an orthonormal (with respect to \( \psi \)) basis of the \( \mathbb{F}_2 \)-vector space Pic(\( V(B) \))/2Pic(\( V(B) \)). Clearly, \( \psi_0 \) is non-degenerate. It is also clear that

\[
\text{Pic}(V(B))_0/2\text{Pic}(V(B))_0 = \{ a_0\tilde{l}_0 + \sum_{b \in B} a_b\tilde{l}_b \mid a_0, a_b \in \mathbb{F}_2, a_0 + \sum a_b = 0 \}
\]

is the orthogonal complement of isotropic

\[
\tilde{v}_0 = \tilde{l}_0 + \sum_{b \in B} \tilde{l}_b
\]

in Pic(\( V(B) \))/2Pic(\( V(B) \)) with respect to \( \psi \). Notice that \( \tilde{v}_0 \) is Galois-invariant. The non-degeneracy of \( \psi \) implies that the kernel of \( \psi_0 \) is the Galois-invariant one-dimensional \( \mathbb{F}_2 \)-subspace generated by \( \tilde{v}_0 \).

This gives us the injective homomorphism

\[
(\text{Pic}(V(B))_0/2\text{Pic}(V(B))_0)/\mathbb{F}_2\tilde{v}_0 \hookrightarrow J(B)_2
\]

of Galois modules; dimension arguments imply that it is an isomorphism. So, in order to finish the proof, it suffices to construct a surjective homomorphism Pic(\( V(B) \))_0/2Pic(\( V(B) \))_0 \to Q_B of Galois modules, whose kernel coincides with \( \mathbb{F}_2\tilde{v}_0 \). In order to do that, let us consider the homomorphism

\[
\kappa : \text{Pic}(V(B))_0/2\text{Pic}(V(B))_0 \to Q_B
\]

that sends \( z = a_0\tilde{l}_0 + \sum_{b \in B} a_b\tilde{l}_b \) to the function \( \kappa(z) : b \mapsto a_b + a_0 \). Since

\[
a_0 + \sum_{b \in B} a_b = 0 \quad \text{and} \quad \#(B)a_0 = 7a_0 = a_0 \in \mathbb{F}_2,
\]

indeed we have \( \kappa(z) \in Q_B \). It is also clear that \( \kappa(z) \) is identically zero if and only if \( a_0 = a_b \forall b \), i.e. \( z = 0 \) or \( \tilde{v}_0 \). Clearly, \( \kappa \) is a surjective homomorphism of Galois modules and ker(\( \kappa \)) = \( \mathbb{F}_2\tilde{v}_0 \).

\( \square \)

Proof of Lemma 1.3: We will use a notation \( (x : y : z) \) for homogeneous coordinates on \( \mathbb{P}^2 \). Suppose that here are three points of \( B_f \) that lie on a line \( ax + by + cz = 0 \). This means that there are distinct roots \( \alpha_1, \alpha_2, \alpha_3 \) of \( f \) and elements \( a, b, c \in K_a \) such that all \( a\alpha_i^2 + b\alpha_i + c = 0 \) and, at least, one of \( a, b, c \) does not vanish. It follows
that the polynomial \( at^3 + bt + c \in K_a[t] \) is not identically zero and has three distinct roots \( \alpha_1, \alpha_2, \alpha_3 \). This implies that \( a \neq 0 \) and
\[
 at^3 + bt + c = a(t - \alpha_1)(t - \alpha_2)(t - \alpha_3).
\]
It follows that \( \alpha_1 + \alpha_2 + \alpha_3 = 0 \). Let us denote the remaining roots of \( f \) by \( \alpha_4, \alpha_5, \alpha_6, \alpha_7 \). Clearly, \( \text{Gal}(K) \) acts 3-transitively on \( \mathfrak{R}_f \). This implies that there exists \( \sigma \in \text{Gal}(K) \) such that
\[
\sigma(\alpha_1) = \alpha_4, \sigma(\alpha_2) = \alpha_5, \sigma(\alpha_3) = \alpha_6
\]
and therefore \( \alpha_2 + \alpha_3 + \alpha_4 = \sigma(\alpha_2 + \alpha_3 + \alpha_1) = 0 \) and therefore \( \alpha_1 = \alpha_4 \) which is not the case. The obtained contradiction proves that no three points of \( B_f \) lie on a one line.

Suppose that six points of \( B_f \) lie on a one conic. Let
\[
 a_0 z^2 + a_1 yz + a_2 y^2 + a_3 xz + a_4 xy + a_6 x^2 = 0
\]
be an equation of the conic. Then not all \( a_i \) do vanish and there are six distinct roots \( \alpha_1, \cdots, \alpha_6 \) of \( f \) such that all \( a_6 \alpha_i^6 + \sum_{i=0}^{4} a_i \alpha_i^4 = 0 \). This implies that the polynomial \( a_6 t^6 + \sum_{i=0}^{4} a_i t^i \) is not identically zero and has 6 distinct roots \( \alpha_1, \cdots, \alpha_6 \).

It follows that \( a_6 \neq 0 \) and
\[
 a_6 t^6 + \sum_{i=0}^{4} a_i t^i = a_6 \prod_{i=1}^{6} (t - \alpha_i).
\]
This implies that \( \sum_{i=1}^{6} \alpha_i = 0 \). Since the sum of all roots of \( f \) lies in \( K \), the remaining seventh root of \( f \) lies in \( K \). This contradicts to the irreducibility of \( f \). The obtained contradiction proves that no six points of \( B_f \) lie on a one conic. \( \square \)

**Lemma 2.1.** Let \( B \subset \mathbb{P}^2(K_a) \) be a 7-element set of points in general position. Assume that \( \text{Gal}(K) \) permutes elements of \( B \) and the image of \( \text{Gal}(K) \) in \( \text{Perm}(B) \cong S_7 \) coincides either with the full symmetric group \( S_7 \) or with the alternating group \( A_7 \); in particular, \( B \) constitutes a Galois orbit. Then either \( \text{End}(J(B)) = \mathbb{Z} \) or \( \text{char}(K) > 0 \) and \( J(B) \) is a supersingular abelian variety.

**Proof of Lemma 2.1.** Recall that \( G_B \) is the image of \( \text{Gal}(K) \) in \( \text{Perm}(B) \). By assumption, \( G_B = S_7 \) or \( A_7 \). It is known [11, Ex. 7.2] that the \( G_B \)-module \( Q_B \) is very simple in the sense of [11, 14, 13]. In particular,
\[
\text{End}_{G_B}(Q_B) = \mathbb{F}_2.
\]
The surjectivity of \( \text{Gal}(K) \rightarrow G_B \) implies that the \( \text{Gal}((K)) \)-module \( Q_B \) is also very simple. Applying Lemma 1.1, we conclude that the \( \text{Gal}((K)) \)-module \( J(B)_{\mathbb{Q}} \) is also very simple. Now the assertion follows from lemma 2.3 of [11]. \( \square \)

**Proof of Theorem 1.2.** In light of Lemma 2.1 we may and will assume that \( \text{char}(K) > 0 \) and \( J(B) \) is a supersingular abelian variety. We need to arrive to a contradiction. Replacing if necessary \( K \) by its suitable quadratic extension we may and will assume that \( G_B = A_7 \). Adjoining to \( K \) all 2-power roots of unity, we may and will assume that \( K \) contains all 2-power roots of unity and still \( G_B = A_7 \). It follows from Lemma 1.1 that \( A_7 \) is isomorphic to the image of \( \text{Gal}(K) \rightarrow \text{Aut}_{\mathbb{Q}_2}(J(B)_{\mathbb{Q}}) \) and the \( A_7 \)-module \( J(B)_{\mathbb{Q}} \) is very simple; in particular, \( \text{End}_{A_7}(J(B)_{\mathbb{Q}}) = \mathbb{F}_2 \). Applying Theorem 3.3 of [13], we conclude that there exists a central extension \( G_1 \rightarrow A_7 \) such that \( G_1 \) is perfect, \( \text{ker}(G_1 \rightarrow A_7) \) is a central cyclic subgroup of order 1 or 2.
and there exists a symplectic absolutely irreducible 6-dimensional representation of $G_1$ in characteristic zero. This implies (in notations of [1]) that either $G_1 \cong A_7$ or $G_1 \cong 2A_7$. However, the table of characters on p. 10 of [1] tells us that neither $A_7$ nor $2A_7$ admits a symplectic absolutely irreducible 6-dimensional representation in characteristic zero. The obtained contradiction proves the Theorem. □

3. EXPLICIT FORMULAS

In this section we describe explicitly $H_B$ when $B = B_f$. We have

$$f(t) = \sum_{i=0}^{7} c_i t^i \in K[t], \ c_7 \neq 0.$$  

We are going to describe explicitly cubic forms that vanish on $B_f$. Clearly, $u := xz^2 - y^3$ and $v := c_7x^2y + c_6x^2z + c_5xy^2 + c_4xyz + c_3xz^2 + c_2y^2z + c_1yz^2 + c_0z^3$ vanish on $B_f$. In order to find a third vanishing cubic form, let us define a polynomial $h(t) \in K[t]$ as a (non-zero) remainder with respect to division by $f(t)$:

$$t^9 - h(t) \in f(t)K[t], \ \deg(h) < \deg(f) = 7.$$  

We have

$$h(t) = \sum_{i=0}^{6} d_i t^i \in K[t].$$

For all roots $\alpha$ of $f$ we have

$$0 = 9\alpha - h(\alpha) = 9\alpha - \sum_{i=0}^{6} d_i \alpha^i.$$  

This implies that the cubic form $w = x^3 - d_6x^2z - d_5xyz - d_4x^2z - d_3xz^2 - d_2y^2z - d_1yz^2 - d_0z^3$ vanishes on $B_f$. Since $u, v, w$ have $x$-degree 1, 2, 3 respectively, they are linearly independent over $K_a$ and therefore constitute a basis of 3-dimensional $H_{B_f}$.

Now assume (till the end of this Section) that char$(K) \neq 3$. Since $C_{B_f}$ is the ramification curve for $\pi$, it follows that

$$g_B(C_{B_f}) = \left\{ (x : y : z), \begin{vmatrix} u_x & u_y & u_z \\ v_x & v_y & v_z \\ w_x & w_y & w_z \end{vmatrix} = 0 \right\} \subset \mathbb{P}^2$$

is a singular sextic which is $K$-birationally isomorphic to $C_{B_f}$. (See also [3] proposition 2 on p. 167.)

4. ANOTHER PROOF

The aim of this Section is to give a more elementary proof of Theorem[12] that formally does not refer to Lemma 2 of [3] Lemma 2 on pp. 161–162] (and therefore does not make use of the Smith theory. However, our arguments are based on ideas of [3] Ch. IX].) In order to do that, we just need to prove Lemma[13] under an additional assumption that the image of Gal$(K)$ in Perm$(B)$ is “very big”.

**Lemma 4.1.** Let $J(B)_2$ be the kernel of multiplication by 2 in $J(B)(K_a)$. Suppose that $G_B$ coincides either with Perm$(B)$ or with $A_7$. Then the Galois modules $J(B)_2$ and $Q_B$ are isomorphic.

---

¹This condition was inadvertently omitted in the Russian version [10].
Proof. Let \( g_0 : V(B) \to V(B) \) be the Geiser involution [2, p. 66–67], i.e., the biregular covering transformation of \( \pi \). Clearly, \( g_0 \) is defined over \( K \). This implies that if \( E \) is an irreducible \( K_a \)-curve on \( V(B) \) then \( E \) and \( g_0(E) \) have the same stabilizers in \( \text{Gal}(K) \). Clearly, different points \( b_1 \) and \( b_2 \) of \( B \) have different stabilizers in \( \text{Gal}(K) \). This implies that \( g_0(E_{b_1}) \neq E_{b_2} \), since the stabilizers of \( g_0(E_{b_1}) \) and \( E_{b_2} \) coincide with the stabilizers of \( b_1 \) and \( b_2 \) respectively. This implies that the lines

\[
\pi(E_{b_1}), \pi(E_{b_2}) \subset \mathbb{P}^2,
\]

which are bitangents to \( C_B \) [2, p. 68], do not coincide.

For each \( b \in B \) we write \( D_b \) for the effective degree 2 divisor on the plane quartic \( C_B \) such that \( 2D_b \) coincides with the intersection of \( C_B \) and \( \pi(E_b) \); it is well known that (the linear equivalence class of) \( D_b \) is a theta characteristic on \( C_B \). It is also clear that

\[
\sigma(D_b) = D_{\sigma(b)} \quad \forall \sigma \in \text{Gal}(K), \ b \in B.
\]

Clearly, if \( b_1 \neq b_2 \) then \( D_{b_1} \neq D_{b_2} \) and the divisors \( 2D_{b_1} \) and \( 2D_{b_2} \) are linearly equivalent. On the other hand, \( D_{b_1} \) and \( D_{b_2} \) are not linearly equivalent. Indeed, if \( D_{b_1} - D_{b_2} \) is the divisor of a rational function \( s \) then \( s \) is a non-constant rational function on \( C_B \) with, at most, two poles. This implies that either \( C_B \) is either a rational (if \( s \) has exactly one pole) or hyperelliptic (if \( s \) has exactly two poles). Since a smooth plane quartic is neither rational nor hyperelliptic, \( D_{b_1} - D_{b_2} \) is not a principal divisor.

Let \((\mathbb{Z}^B)^0\) be the free commutative group of all functions \( \phi : B \to \mathbb{Z} \) with \( \sum_{b \in B} \phi(b) = 0 \). Clearly, \((\mathbb{Z}^B)^0\) is provided with the natural structure of \( \text{Gal}(K) \)-module and there is a natural isomorphism of \( \text{Gal}(K) \)-modules

\[
(\mathbb{Z}^B)^0 / 2(\mathbb{Z}^B)^0 \cong Q_B.
\]

Let us consider the homomorphism of commutative groups \( r : (\mathbb{Z}^B)^0 \to \text{Pic}(C_B) \) that sends a function \( \phi \) to the linear equivalence class of \( \sum_{b \in B} \phi(b)D_b \). Clearly,

\[
 r((\mathbb{Z}^B)^0) \subset J(B)_2 \subset \text{Pic}(B)
\]

and therefore \( r \) kills \( 2 \cdot (\mathbb{Z}^B)^0 \). On the other hand, the image of \( r \) contains the (non-zero) linear equivalence class of \( D_{b_1} - D_{b_2} \). This implies that \( r \) is not identically zero and we get a non-zero homomorphism of \( \text{Gal}(K) \)-modules

\[
\bar{r} : Q_B \cong (\mathbb{Z}^B)^0 / 2(\mathbb{Z}^B)^0 \to J(B)_2.
\]

It is well-known that our assumptions on \( G_B \) imply that the \( G_B \)-module \( Q_B \) is (absolutely) simple and therefore \( Q_B \), viewed as Galois module, is also simple. This implies that \( \bar{r} \) is injective. Since the \( \mathbb{F}_2 \)-dimensions of both \( Q_B \) and \( J(B)_2 \) equal to 6 and therefore coincide, we conclude that \( \bar{r} \) is an isomorphism. \( \square \)

5. Added in translation

The following assertion is a natural generalization of Lemma 1.3:

**Proposition 5.1.** 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 7-element set that is a \( \text{Gal}(K) \)-orbit. Let us assume that the image \( G_B \) of \( \text{Gal}(K) \) in the group \( \text{Perm}(B) \) of all permutations of \( B \) coincides either with \( \text{Perm}(B) \cong S_7 \) or with the alternating group \( A_7 \). Then \( B \) is in general position.
Proof. Clearly, 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, 
$$\{P_1, P_2, P_3\} \subset \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\} = B.$$ 
Clearly, $D \cap E = \{P_1, P_2, P_3\}$. There exists $\sigma \in \text{Gal}(K)$ 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 $\sigma(D) \cap E = \{P_1, P_2, P_4\}$. In particular, $\sigma(D) \neq D$. 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, 
$$\{P_1, P_2, P_3, P_4, P_5, P_6\} = B \setminus \{P_7\}.$$ 
Clearly, $Y \cap E = B \setminus \{P_7\}$. 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 $\sigma \in \text{Gal}(K)$ such that $\sigma(P_1) = P_7$. Then $\sigma(P_2) = P_i$ for some positive integer $i \leq 6$. This implies that $\sigma(B \setminus \{P_2\}) = B \setminus \{P_i\}$ and the irreducible conic $\sigma(Y)$ contains $B \setminus \{P_i\}$. Clearly, $\sigma(Y) \cap E = B \setminus \{P_i\}$ contains $P_7$. In particular, $\sigma(Y) \neq Y$. However, both conics contain the 5-element set $B \setminus \{P_1, P_7\}$. Contradiction. □

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] M. Demazure, Surfaces de Del Pezzo II, III, IV, V. Springer Lecture Notes in Math. 777 (1980), 23–69.
[3] I. Dolgachev, D. Orlandi, Point sets in projective spaces and theta functions, Astérisque 165 (1986).
[4] I. Dolgachev, Classical Algebraic geometry. A modern view. Cambridge University Press, 2012. (Section 8.7)
[5] R. Hartshorne, Algebraic Geometry, GTM 52, Springer-Verlag, 1977.
[6] V. A. Iskovskikh, Minimal models of rational surfaces over arbitrary fields. Izv. Akad. Nauk SSSR Ser. Mat. 43 (1979), 19–43; Math. USSR-Izv. 14 (1980), 17–39.
[7] V. A. Iskovskikh, I.R. Shafarevich, Algebraic surfaces. Algebraic geometry, II, 127–262, Encyclopaedia Math. Sci., 35, Springer, Berlin, 1996.
[8] Yu. I. Manin, Cubic forms, second edition, North Holland, 1986.
[9] Yu. I. Manin, M. A. Tsfasman, Rational varieties: algebra, geometry, arithmetic. Uspekhi Mat. Nauk 41 (1986), no. 2(248), 43–94; Russian Math. Surveys 41 (1986), no. 2, 51–116.
[10] Yu. G. Zarhin, Hyperelliptic jacobians without complex multiplication. Math. Res. Letters 7 (2000), 123–132.
[11] 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 (Birkhäuser, 2001), pp. 473–490.
[12] Yu. G. Zarhin, Hyperelliptic jacobians without complex multiplication in positive characteristic. Math. Res. Letters 8 (2001), 429–435.
[13] Yu. G. Zarhin, Very simple 2-adic representations and hyperelliptic jacobians. Moscow Math. J. 2 (2002), issue 2, 403–431.
[14] 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.
[15] Yu. G. Zarhin, Non-supersingular hyperelliptic jacobians. Bull. Soc. Math. France 132 (2004), 617–634.
[16] Yu. G. Zarhin, Del Pezzo surfaces of degree 2 and jacobians without complex multiplication (Russian). Trudy St. Petersburg Mat. Obsch. 11 (2005), 81–91.

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

This reference was updated.
