TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 368, Number 5, May 2016, Pages 3651–3672
http://dx.doi.org/10.1090/tran/6579
Article electronically published on December 3, 2015

TWO-DIMENSIONAL FAMILIES OF HYPERELLIPTIC JACOBIANS WITH BIG MONODROMY

YURI G. ZARHIN

Abstract. Let K be a global field of characteristic different from 2 and $u(x) \in K[x]$ be an irreducible polynomial of even degree $2g \ge 6$ whose Galois group over K is either the full symmetric group $\mathbf{S}_{2g}$ or the alternating group $\mathbf{A}_{2g}$. We describe explicitly how to choose (infinitely many) pairs of distinct $t_1, t_2 \in K$ such that the g-dimensional Jacobian of a hyperelliptic curve $y^2 = (x-t_1)(x-t_2))u(x)$ has no nontrivial endomorphisms over an algebraic closure of K and has big monodromy.

1. Statements

As usual, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{C}$ stand for the ring of integers, the field of rational numbers and the field of complex numbers respectively. If ℓ is a prime, then we write $\mathbb{F}_\ell, \mathbb{Z}_\ell$ and $\mathbb{Q}_\ell$ for the ℓ-element (finite) field, the ring of ℓ-adic integers and field of ℓ-adic numbers respectively. If A is a finite set, then we write $\#(A)$ for the number of its elements.

If C is a commutative ring with 1, V a free C-module of finite rank and $e : V \times V \to C$ an alternating C-bilinear form, then we write

$$\mathrm{Sp}(V,e) \subset \mathrm{Gp}(V,e) \subset \mathrm{Aut}_C(V)$$

for the symplectic group

$$\mathrm{Sp}(V,e) = \{u \in \mathrm{Aut}_C(V) \mid e(ux,uy) = e(x,y) \ \forall\ x,y \in V\}$$

and the group of symplectic similitudes $\mathrm{Gp}(V,e)$ that consists of all automorphisms u of V such that there exists a *constant* $c = c(u) \in C^*$ such that

$$e(ux,uy) = c \cdot e(x,y) \ \forall\ x,y \in V.$$

Let K be a field of characteristic different from 2, let $\bar{K}$ be its algebraic closure and $\mathrm{Gal}(K) = \mathrm{Aut}(\bar{K}/K)$ its absolute Galois group. If $L \subset \bar{K}$ is a finite separable algebraic extension of K, then $\bar{K}$ is an algebraic closure of L and $\mathrm{Gal}(L) = \mathrm{Aut}(\bar{K}/L)$ is an open subgroup of finite index in $\mathrm{Gal}(K)$; actually, the index equals degree $[L:K]$ of the field extension L/K.

Let $n \ge 5$ be an integer, $f(x) \in K[x]$ a degree n polynomial *without multiple roots*, $\mathfrak{R}_f \subset \bar{K}$ the n-element set of its roots, $K(\mathfrak{R}_f) \subset \bar{K}$ the splitting field of $f(x)$ and $\mathrm{Gal}(f) = \mathrm{Gal}(K(\mathfrak{R}_f)/K)$ the Galois group of $f(x)$ over K. One may view $\mathrm{Gal}(f)$ as a certain group of permutations of $\mathfrak{R}_f$. Let $C_f : y^2 = f(x)$ be the corresponding hyperelliptic curve of genus $\lfloor (n-1)/2 \rfloor$. Let $J(C_f)$ be the Jacobian of C_f; it is an $\lfloor (n-1)/2 \rfloor$-dimensional abelian variety that is defined over K.

Received by the editors October 25, 2013 and, in revised form, July 12, 2014.
2010 *Mathematics Subject Classification.* Primary 14H40, 14K05, 11G30, 11G10.
This work was partially supported by a grant from the Simons Foundation (#246625).

Let X be an abelian variety that is defined over K. We write $\mathrm{End}(X)$ for the ring of all $\bar{K}$-endomorphisms of X. As usual, we write $\mathrm{End}^0(X)$ for the corresponding (finite-dimensional semisimple) $\mathbb{Q}$-algebra $\mathrm{End}(X) \otimes \mathbb{Q}$.

If m is a positive integer that is not divisible by $\mathrm{char}(K)$, then we write X_m for the kernel of multiplication by m in $X(\bar{K})$. It is well known that X_m is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $2\dim(X)$ that is a Galois submodule of $X(\bar{K})$: we write

$$\bar{\rho}_{m,X} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Z}/m\mathbb{Z}}(X_m)$$

for the corresponding structure homomorphism and

$$\tilde{G}_{m,X,K} \subset \mathrm{Aut}_{\mathbb{Z}/m\mathbb{Z}}(X_m)$$

for its image. A polarization λ on X that is defined over K gives rise to the Galois-equivariant alternating bilinear Riemann form

$$X_m \times X_m \to \mu_m$$

where μ_m is the cyclic group of all mth roots of unity in $\bar{K}$. Identifying (non-canonically) μ_m with $\mathbb{Z}/m\mathbb{Z}$, we may view the Riemann form as an alternating bilinear Riemann form

$$\bar{e}_{\lambda,m} : X_m \times X_m \to \mathbb{Z}/m\mathbb{Z}$$

such that

$$\bar{e}_{\lambda,m}(\sigma(x), \sigma(y)) = \bar{\chi}_m(\sigma)\bar{e}_{\lambda,m}(x, y)$$

for all $x, y \in X_m$ and $\sigma \in \mathrm{Gal}(K)$ where

$$\bar{\chi}_m = \bar{\chi}_{m,K} : \mathrm{Gal}(K) \to (\mathbb{Z}/m\mathbb{Z})^*$$

is the cyclotomic character that describes the Galois action on mth roots of unity. (This form is nondegenerate if and only if $\deg(\lambda)$ and m are relatively prime. In particular, if λ is a principal polarization, then $\bar{e}_{\lambda,m}$ is nondegenerate for all m.) This implies that

$$\tilde{G}_{m,X,K} \subset \mathrm{Gp}(X_m, \bar{e}_{\lambda,m}) \subset \mathrm{Aut}_{\mathbb{Z}/m\mathbb{Z}}(X_m).$$

Clearly, $\tilde{G}_{m,X,L} = \bar{\rho}_{m,X}(\mathrm{Gal}(K))$ is a subgroup of $\tilde{G}_{m,X,K}$ with index $\le [L : K]$.

If we choose a prime $\ell \ne \mathrm{char}(K)$, put $m = \ell^i$ and take the projective limit, then we get the Tate module $T_\ell(X)$ that is a free $\mathbb{Z}_\ell$-module of rank $2\dim(X)$ provided with the continuous Galois action (ℓ-adic representation)

$$\rho_{\ell,X} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(X))$$

and nondegenerate $\mathbb{Z}_\ell$-bilinear alternating Riemann form

$$e_{\lambda,\ell} : T_\ell(X) \times T_\ell(X) \to \mathbb{Z}_\ell$$

such that

$$e_{\lambda,\ell}(\sigma(x), \sigma(y)) = \chi_\ell(\sigma)e_\lambda(x, y)$$

for all $x, y \in T_\ell(X)$ and $\sigma \in \mathrm{Gal}(K)$ where

$$\chi_\ell : \mathrm{Gal}(K) \to \mathbb{Z}_\ell^* \subset \mathbb{Q}_\ell^*$$

is the cyclotomic character that describes the Galois action on ℓ-power roots of unity in $\bar{K}$. (This form is perfect if and only if $\deg(\lambda)$ is not divisible by ℓ.)

It follows that the image

$$G_{\ell,X,K} := \rho_{\ell,X}(\mathrm{Gal}(K)) \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(X))$$

sits in the group $\mathrm{Gp}(T_\ell(X), e_{\lambda,\ell})$ of symplectic similitudes, i.e.,

$$G_{\ell,X,K} \subset \mathrm{Gp}(T_\ell(X), e_{\lambda,\ell}) \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(X)).$$

Clearly, $G_{\ell,X,L} := \rho_{\ell,X}(\mathrm{Gal}(L))$ is a closed subgroup in $G_{\ell,X,K}$ with finite index $\le [L:K]$ and therefore is open in $G_{\ell,X,K}$.

In [48, Th. 5.4 on p. 38] the author proved the following statement.

Theorem 1.1. *Suppose that* $\mathrm{char}(K) = 0$ *and* $n = 2g + 2 \ge 12$ *is even. Assume also that* $f(x) = (x - t_1)(x - t_2)u(x)$ *where*

$$t_1, t_2 \in K,\ t_1 \ne t_2,\ u(x) \in K[x],\ \deg(u) = n - 2 = 2g$$

and $\mathrm{Gal}(u) = \mathbf{S}_{2g}$ *or* $\mathbf{A}_{2g}$. *Then* $\mathrm{End}(J(C_f)) = \mathbb{Z}$. *In particular,* $J(C_f)$ *is an absolutely simple abelian variety.*

The following statement follows easily from [48, Th. 8.3 on p. 49] applied to $t = t_1$ and $h(x) = (x - t_2)u(x)$ and an elementary substitution described in [48, Proof of Th. 5.4 on p. 38].

Theorem 1.2. *Suppose that* K *is a field that is finitely generated over* $\mathbb{Q}$ *and* $n = 2g + 2 \ge 12$ *is even. Assume also that* $f(x) = (x - t_1)(x - t_2)u(x)$ *with*

$$t_1, t_2 \in K,\ t_1 \ne t_2,\ u(x) \in K[x],\ \deg(u) = n - 2 = 2g$$

and $\mathrm{Gal}(u) = \mathbf{S}_{2g}$ *or* $\mathbf{A}_{2g}$. *Let* λ *be the canonical principal polarization on the Jacobian* $J(C_f)$. *Then the group* $G_{\ell,J(C_f),K}$ *is an open subgroup of finite index in the group* $\mathrm{Gp}(T_\ell(J(C_f)), e_{\lambda,\ell})$ *of symplectic similitudes.*

The aim of this note is, by imposing certain additional *arithmetic* conditions (inspired by [19]) on $f(x)$, to obtain the results about the groups $\tilde{G}_{\ell,J(C_f),K}$ for almost all ℓ when K is a finitely generated field. In a sense, our approach is a combination of methods of [48] and [19]. As a bonus, we were able to decrease the lower bound for g and cover the case when K has prime characteristic. Our main result is the following statement.

Theorem 1.3. *Let* $g \ge 3$ *be an integer. Let* K *be a discrete valuation field, let* $R \subset K$ *be the discrete valuation ring with maximal ideal* $\mathfrak{m}$ *and residue field* $k = R/\mathfrak{m}$ *of characteristic different from* 2. *(In particular,* $\mathrm{char}(K) \ne 2$.*) Let*

$$u(x) = \sum_{i=0}^{2g} a_i x^i \in K[x]$$

be a degree $2g$ *polynomial that enjoys the following properties.*

(i) *The polynomial* $u(x)$ *is irreducible over* K *and has no multiple roots, and its Galois group* $\mathrm{Gal}(u)$ *is either* $\mathbf{S}_{2g}$ *or* $\mathbf{A}_{2g}$.
(ii) *All the coefficients* a_i *lie in* R, *i.e.,* $u(x) \in R[x]$.
(iii) *Neither the leading coefficient* a_{2g} *nor the discriminant of* $u(x)$ *lies in* $\mathfrak{m}$. *In other words* $u(x)$ *modulo* $\mathfrak{m}$ *is a degree* $2g$ *polynomial over* k *without multiple roots.*

Suppose that t_1 *and* t_2 *are two distinct elements of* R *such that*

$$t_1 - t_2 \in \mathfrak{m},\ u(t_1) \notin \mathfrak{m},\ u(t_2) \notin \mathfrak{m}.$$

Then $\mathrm{End}(J(C_f)) = \mathbb{Z}$ *where* $f(x) = (x - t_1)(x - t_2)u(x)$. *In particular,* $J(C_f)$ *is an absolutely simple abelian variety.*

If, in addition, K *is a field that is finitely generated over its prime subfield, then:*

(i) *For all primes* $\ell \ne \mathrm{char}(K)$ *the group* $G_{\ell,J(C_f),K}$ *is an open subgroup of finite index in the group* $\mathrm{Gp}(T_\ell(J(C_f)), e_{\lambda,\ell})$.

(ii) *If* L/K *is a finite algebraic field extension, then for all but finitely many primes* ℓ *the group* $\tilde{G}_{\ell,J(C_f),L}$ *contains* $\mathrm{Sp}(J(C_f)_\ell, \bar{e}_{\lambda,\ell})$ *and the group* $G_{\ell,J(C_f),L}$ *contains* $\mathrm{Sp}(T_\ell(J(C_f)), e_{\lambda,\ell})$. *If, in addition,* $\mathrm{char}(K) = 0$, *then for all but finitely many primes* ℓ,

$$\tilde{G}_{\ell,J(C_f),L} = \mathrm{Gp}(J(C_f)_\ell, \bar{e}_{\lambda,\ell}),\ G_{\ell,J(C_f),L} = \mathrm{Gp}(T_\ell(J(C_f)), e_{\lambda,\ell}).$$

Remark 1.4. Suppose that $u(0) = a_0 \notin \mathfrak{m}$ (e.g., $a_0 = \pm 1$). Then any pair $\{t_1, t_2\}$ of distinct elements of $\mathfrak{m}$ satisfies the conditions of Theorem 1.3 (for given $u(x)$).

Example 1.5. Let $\mathcal{O}$ be a Dedekind ring with infinitely many maximal ideals and K its field of fractions with $\mathrm{char}(K) \ne 2$. (For example, K is a number field with ring of integers $\mathcal{O}$. Another example: $\mathcal{O}$ is the ring of regular functions on an absolutely irreducible smooth affine curve $\mathcal{C}$ over a field of characteristic different from 2 and K is the field of rational functions on $\mathcal{C}$.) Let $g > 1$ be an integer, and $u(x) = \sum_{i=0}^{2g} a_i x^i \in \mathcal{O}[x]$ a degree $2g$ polynomial that is irreducible over K. Pick any maximal ideal $\mathfrak{P}$ in $\mathcal{O}$ such that the characteristic of the residue field $\mathcal{O}/\mathfrak{P}$ is different from 2 and such that a_0, a_n and the discriminant of $f(x)$ are $\mathfrak{P}$-adic units. (This rules out only finitely many maximal ideals in $\mathcal{O}$.) Let us consider the discrete valuation ring R that is the localization $\mathcal{O}_\mathfrak{P}$ of $\mathcal{O}$ at $\mathfrak{P}$. Then the residue field k of R coincides with $\mathcal{O}/\mathfrak{P}$ and therefore has odd characteristic. Clearly, a_0, a_n and the discriminant of $f(x)$ are units in R. Let t_1, t_2 be distinct elements of $\mathfrak{P}$. Then they both lie in the maximal ideal of R. Now it's clear that if $g \ge 3$, then $\{K, R, u(x), t_1, t_2\}$ satisfy the conditions of Theorem 1.3.

For example, let $K = \mathbb{Q}, \mathcal{O} = \mathbb{Z}$ and $u(x) = x^{2g} - x - 1$. It is known [35, Remark 2 at the bottom of p. 43] that $u(x)$ is irreducible over $\mathbb{Q}$ and its Galois group is $\mathbf{S}_{2g}$. In order to figure out for which prime p the polynomial $u(x) \bmod p$ acquires multiple roots, we follow Serre's arguments [35]. So, let us consider the polynomial $\bar{u}(x) = x^{2g} - x - 1 \in \mathbb{F}_p[x]$ and assume that it has a multiple root, say α. Then α is also a root of the derivative $\bar{u}'(x) = 2gx^{2g-1} - 1 \in \mathbb{F}_p[x]$. It follows that p does *not* divide $2g$ and $\alpha \ne 0$. Clearly, α is a root of $2g\bar{u}(x) - x\bar{u}'(x) = (1 - 2g)x - 2g$. This implies that p does *not* divide $2g - 1$ and $\alpha = 2g/(1 - 2g) \in \mathbb{F}_p$. This implies that $(2g)^{2g}/(1 - 2g)]^{2g-1} - 1 = 0$ in $\mathbb{F}_p$; i.e., the integer $N(g) = (2g)^{2g} - (1 - 2g)^{2g-1}$ is divisible by p. In other words, the prime divisors of the discriminant of $u(x)$ are exactly the prime divisors of $N(g)$. (Clearly, any prime divisor of $2g(2g - 1)$ does not divide $N(g)$.) Now we take any odd prime p that does not divide $N(g)$ and pick any pair of *distinct* integers s_1, s_2, and put $t_1 = ps_1, t_2 = ps_2$. Then $\{\mathbb{Q}, \mathbb{Z}_{(p)}, x^{2g} - x - 1, t_1, t_2\}$ satisfy the conditions of Theorem 1.3. This implies that if we put $f(x) = (x^{2g} - x - 1)(x - t_1)(x - t_2)$, then the Jacobian $X = J(C_f)$ of the hyperelliptic curves $C_f : y^2 = f(x)$ is an absolutely simple g-dimensional abelian variety over $K = \mathbb{Q}$ that enjoys the following properties.

$\mathrm{End}(X) = \mathbb{Z}$; for all primes ℓ the group $G_{\ell,X,K}$ is an open subgroup of finite index in $\mathrm{Gp}(T_\ell(X), e_{\lambda,\ell})$. In addition, if L is a number field, then for all but finitely many primes ℓ,

$$G_{\ell,X,L} = \mathrm{Gp}(T_\ell(X), e_{\lambda,\ell}),\ \tilde{G}_{\ell,X,L} = \mathrm{Gp}(X_\ell, \bar{e}_{\lambda,\ell}).$$

Remark 1.6. Earlier Chris Hall [19] proved an analogue of Theorem 1.3: in his result $f(x)$ is required to be an irreducible polynomial of degree $n \ge 5$ over a number field K with coefficients in the ring of integers of K and Galois group $\mathbf{S}_n$ and such that modulo some odd prime it acquires exactly one multiple root and its multiplicity is 2. (His proof makes use of results of [42].) It was proven by Emmanuel Kowalski (in an appendix to [19]) that most polynomials enjoy this property. It would be interesting to produce explicit examples of such $f(x)$.[1] (For example, arguments of [35, p. 42, Remark 2] imply that $f(x) = x^n - x - 1$ enjoys this property.) However, Example 1.5 tells us how to produce plenty of explicit examples of $f(x)$ that satisfy the conditions of Theorem 1.3.

The next result tells us that distinct (unordered) pairs (t_1, t_2) with given $u(x)$ (as in Theorem 1.3) lead to nonisomorphic (over $\bar{K}$) Jacobians $J(C_f)$.

Theorem 1.7. *Let $g \ge 2$ be a positive integer, K a field of characteristic different from 2, $u(x) \in K[x]$ an irreducible polynomial of degree $2g$ and without multiple roots. Assume that $\mathrm{Gal}(u) = \mathbf{S}_{2g}$ or $\mathbf{A}_{2g}$. Let r be an even positive integer, and let B_1 and B_2 be two distinct r-element subsets of K. Let us put*

$$f_1(x) = u(x) \prod_{\alpha \in B_1} (x - \alpha) \in K[x], \ f_2(x) = u(x) \prod_{\alpha \in B_2} (x - \alpha) \in K[x].$$

Suppose that

$$\mathrm{End}(J(C_{f_1})) = \mathbb{Z}, \ \mathrm{End}(J(C_{f_2})) = \mathbb{Z}.$$

Then the Jacobians $J(C_{f_1})$ and $J(C_{f_2})$ are not isomorphic over $\bar{K}$.

The paper is organized as follows. In Section 2 we discuss the standard $(2g)$-dimensional permutational representation of the alternating group $\mathbf{A}_{2g}$ in characteristic 2. Section 3 deals with g-dimensional abelian varieties X such that the absolute Galois group of the ground field acts on X_2 through its quotient isomorphic to $\mathbf{A}_{2g}$ and the $\mathbf{A}_{2g}$-module X_2 is isomorphic to the permutational one. Examples of such X are provided by certain hyperelliptic Jacobians that are discussed in Section 5; among them are Jacobians that satisfy the conditions of Theorem 1.3. We prove Theorem 1.3 in Section 6. In Section 7 we prove auxiliary results about Galois groups of cyclotomic extensions. In Section 8 we prove Theorem 1.7. Section 9 contains (more or less straightforward) corollaries that tell us that the hyperelliptic Jacobians involved (and their self-products) satisfy the Tate, Hodge and Mumford-Tate conjectures.

2. Permutational representations of alternating groups

2.1. Recall [15] that 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 $\mathcal{G}$. In particular, if $\mathcal{G}$ is perfect and $\mathcal{G}_1 \twoheadrightarrow \mathcal{G}$ is a minimal cover, then $\mathcal{G}_1$ is also perfect. In addition, if r is a positive integer such that every subgroup in $\mathcal{G}$ of index dividing r coincides with $\mathcal{G}$, then the same is true for $\mathcal{G}_1$ [47, Remark 3.4]. Namely, every subgroup in $\mathcal{G}_1$ of index dividing r coincides with $\mathcal{G}_1$.

[1] *Added in proof*: Plenty of such examples have appeared in [50].

Lemma 2.2. *Let $m \ge 5$ be an integer, $\mathbf{A}_m$ the corresponding alternating group and $\mathcal{G}_1 \twoheadrightarrow \mathbf{A}_m$ a minimal cover. Then the only subgroup of index $< m$ in $\mathcal{G}_1$ is $\mathcal{G}_1$ itself.*

Proof. This is Lemma 2.2(i) of [48]. □

2.3. Let $g \ge 3$ be an integer. Then $2g \ge 6$ and $\mathbf{A}_{2g}$ is a simple nonabelian group.

Let B be a $2g$-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 $\mathbf{S}_{2g}$. We write $\mathrm{Alt}(B)$ for the only subgroup of index 2 in $\mathrm{Perm}(B)$. Every isomorphism $\mathrm{Perm}(B) \cong \mathbf{S}_{2g}$ induces an isomorphism between $\mathrm{Alt}(B)$ and the alternating group $\mathbf{A}_{2g}$. Let us consider the $2g$-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 nondegenerate and $\mathrm{Perm}(B)$-invariant.

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

Lemma 2.4. (i) *The centralizer $\mathrm{End}_{\mathrm{Alt}(B)}(\mathbb{F}_2^B)$ has $\mathbb{F}_2$-dimension 2.*

(ii) *Every proper nonzero $\mathrm{Alt}(B)$-invariant subspace in $\mathbb{F}_2^B$ has dimension 1 or $2g-1$. In particular, $\mathbb{F}_2^B$ does not contain a proper nonzero $\mathrm{Alt}(B)$-invariant even-dimensional subspace.*

Proof. This is Lemma 2.5 of [48]. (Since $\mathrm{Alt}(B)$ is doubly transitive, (i) follows from [25, Lemma 7.1].)

□

3. Abelian varieties

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

Recall that if X is an abelian variety of positive dimension over $\bar{F}$, then we write $\mathrm{End}(X)$ for the ring of all its $\bar{F}$-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 $\mathrm{End}_F^0(X)$ 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 $\mathrm{End}_F^0(X)$ are semisimple finite-dimensional $\mathbb{Q}$-algebras.

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

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

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

Theorem 3.1. *Let X be an abelian variety of positive dimension over a field K such that $\mathrm{End}^0(X)$ is a simple $\mathbb{Q}$-algebra, i.e., its center $\mathfrak{C}$ is a field. Suppose that K is a discrete valuation field with discrete valuation ring R and residue field k. Suppose that there exists a semiabelian group scheme $\mathcal{X}$ over $\mathrm{Spec}(R)$ whose generic fiber coincides with X and the identity component $\mathcal{X}_k^0$ of the closed fiber $\mathcal{X}_k$ has toric dimension one, i.e., is a commutative algebraic k-group that is an extension of an abelian variety by a one-dimensional algebraic torus. Then $\mathrm{End}(X) = \mathbb{Z}$.*

Proof of Theorem 3.1. Extending K, we may and will assume that all endomorphisms of X are defined over K. Removing from $\mathcal{X}$ all the irreducible components of $\mathcal{X}_k$ that do not pass through the identity element, we may and will assume that $\mathcal{X}_k = \mathcal{X}_k^0$, i.e., the closed fiber of $\mathcal{X}$ is connected. It is known ([26, Ch. IX, Cor. 1.4 on p. 130], [14, Ch. 1, Sect. 2, Prop. 2.7, p. 9] that every endomorphism of X extends uniquely to a certain endomorphism of the group scheme $\mathcal{X}/Spec(R)$. This gives us a ring homomorphism

$$\mathrm{End}(X) \to \mathrm{End}(\mathcal{X}/\mathrm{Spec}(R))$$

that sends 1 to 1. By composing this with the restriction homomorphism $\mathrm{End}(\mathcal{X}/\mathrm{Spec}(R)) \to \mathrm{End}(\mathcal{X}_k)$, we get a ring homomorphism $\mathrm{End}(X) \to \mathrm{End}(\mathcal{X}_k)$ that sends 1 to 1.

Let T be the one-dimensional torus in $\mathcal{X}_k$. Clearly, $\mathrm{End}(\mathrm{T}) = \mathbb{Z}$. On the other hand, every endomorphism of the algebraic k-group $\mathcal{X}_k$ leaves invariant T, so we get the restriction ring homomorphism $\mathrm{End}(\mathcal{X}_k) \to \mathrm{End}(\mathrm{T}) = \mathbb{Z}$ that sends 1 to 1. Taking the composition, we get the ring homomorphism

$$\mathrm{End}(X) \to \mathrm{End}(\mathrm{T}) = \mathbb{Z}$$

that sends 1 to 1. Extending the latter homomorphism by $\mathbb{Q}$-linearity, we get the homomorphism

$$\mathrm{End}^0(X) \to \mathbb{Q}$$

that sends 1 to 1. Since $\mathrm{End}^0(X)$ is a simple $\mathbb{Q}$-algebra, the latter homomorphism is an embedding and therefore $\mathrm{End}^0(X) = \mathbb{Q}$. This implies that $\mathrm{End}(X) = \mathbb{Z}$. □

Corollary 3.2. *Let X be an absolutely simple abelian variety of positive dimension over a field K. Suppose that K is a discrete valuation field with discrete valuation ring R and residue field k. Suppose that there exists a semiabelian group scheme $\mathcal{X}$ over* $\mathrm{Spec}(R)$ *whose generic fiber coincides with X and the identity component $\mathcal{X}_k^0$ of the closed fiber $\mathcal{X}_k$ has toric dimension one, i.e., $\mathcal{X}_k^0$ is a commutative algebraic k-group that is an extension of an abelian variety by a one-dimensional algebraic torus. Then* $\mathrm{End}(X) = \mathbb{Z}$.

Proof of Corollary 3.2. The absolute simplicity of X means that $\mathrm{End}^0(X)$ is a division algebra over $\mathbb{Q}$ and therefore is a simple $\mathbb{Q}$-algebra. □

Let n be a positive integer that is not divisible by $\mathrm{char}(F)$. Recall that if X is defined over F, then X_n is a Galois submodule in $X(\bar{F})$, all points of X_n are defined over a finite separable extension of F and 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 $\bar{\rho}_{n,X,F}(\mathrm{Gal}(F))$. We write $F(X_n)$ 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.

If F_1/F is a finite algebraic extension, then $F_1(X_n)$ coincides with the compositum $F_1F(X_n)$ of F_1 and $F(X_n)$.

Lemma 3.3. *Let F_1/F be a finite solvable Galois extension of fields. If $\tilde{G}_{n,X,F}$ is a simple nonabelian group, then F_1 and $F(X_n)$ are linearly disjoint over F and $\tilde{G}_{n,X,F_1} = \tilde{G}_{n,X,F}$.*

Proof. This is Lemma 3.2 of [48]. □

Now and until the end of this section we assume that $\mathrm{char}(F) \neq 2$. It is known [28] 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 [45, Sect. 1].

The field inclusion $F(X_2) \subset F(X_4)$ induces a natural surjection [45, Sect. 1]

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

Definition 3.4. We say that F is 2-*balanced* with respect to X if $\tau_{2,X}$ is a minimal cover. (See [10].)

Remark 3.5. Clearly, there always exists a subgroup $H \subset \tilde{G}_{4,X,F}$ such that the induced homomorphism $H \to \tilde{G}_{2,X,F}$ is surjective and a minimal cover. Let us put $L = F(X_4)^H$. Clearly,

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

and L is a maximal overfield of F that enjoys these properties. It is also clear that H and L can be chosen such that

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

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

and L is 2-*balanced* with respect to X ([10, Remark 2.3]; see also [11]).

We will need the following result from our previous work.

Lemma 3.6. *Assume that X_2 does not contain a proper nonzero $\tilde{G}_{2,X,F}$-invariant even-dimensional subspace 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. This is Lemma 3.4 of [46]. □

Theorem 3.7. *Let $g \geq 3$ be an integer and B a $2g$-element set. Let X be a g-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 the center $\mathfrak{C}$ of $\mathrm{End}^0(X)$ is a field, i.e., $\mathrm{End}^0(X)$ is a finite-dimensional simple $\mathbb{Q}$-algebra.*

Proof of Theorem 3.7. By Remark 3.5, we may and will assume that F is 2-*balanced* with respect to X, i.e., $\tau_{2,X} : \tilde{G}_{4,X,F} \twoheadrightarrow \tilde{G}_{2,X,F} = \mathbf{A}_{2g}$ is a minimal cover. In particular, $\tilde{G}_{4,X,F}$ is perfect, since $\mathbf{A}_{2g}$ is perfect. Since $\mathbf{A}_{2g}$ does not contain a subgroup of index $< 2g$ different from $\mathbf{A}_{2g}$, it follows from Lemma 2.2 that $\tilde{G}_{4,X,F}$ does not contain a proper subgroup of index $< 2g$ different from $\tilde{G}_{4,X,F}$. Now Lemmas 3.6 and 2.4 imply that $\mathrm{End}^0_F(X)$ is either $\mathbb{Q}$ or a quadratic field.

Recall that $\mathfrak{C}$ is the center of $\mathrm{End}^0(X)$. Suppose that $\mathfrak{C}$ is *not* a field. Then it is a direct sum

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

of number fields $\mathfrak{C}_1, \dots, \mathfrak{C}_r$ with $1 < r \le \dim(X) = g$. 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 the summands $\mathfrak{C}_i$'s. Since $\tilde{G}_{4,X,F}$ does not contain proper subgroups of index $\le g$, each $\mathfrak{C}_i$ is $\tilde{G}_{4,X,F}$-invariant. This implies that the r-dimensional $\mathbb{Q}$-subalgebra

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

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

Corollary 3.8. *Let $g \ge 3$ be an integer and B a $2g$-element set. Let X be a g-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 $\mathbb{F}_2^B$. Assume additionally that there exists a finite algebraic field extension E/F such that E is a discrete valuation field with discrete valuation ring R and residue field k such that the Néron model of X over $\mathrm{Spec}(R)$ is a semiabelian group scheme whose closed fiber has toric dimension 1. Then $\mathrm{End}(X) = \mathbb{Z}$.*

Proof. The result follows readily from Theorem 3.7 combined with Theorem 3.1. □

4. Abelian varieties with semistable reduction and toric dimension one

This section is a variation on a theme of [19] (see also [1]).

Let X be an abelian variety of positive dimension over a field K with polarization λ and let ℓ be a prime different from $\mathrm{char}(K)$. Let us consider the $2\dim(X)$-dimensional $\mathbb{Q}_\ell$-vector space

$$V_\ell(X) = T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

One may view $T_\ell(X)$ as a $\mathbb{Z}_\ell$-lattice of maximal rank; the Galois action on $T_\ell(X)$ extends by $\mathbb{Q}_\ell$-linearity to $V_\ell(X)$, and we may view $\rho_{\ell,X}$ as the ℓ-adic representation

$$\rho_{\ell,X} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(X)) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(X))$$

and its image $G_{\ell,X,K}$ as a compact ℓ-adic subgroup in $\mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(X))$ [32]. We write

$$\mathfrak{g}_{\ell,X} \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))$$

for the Lie algebra of $G_{\ell,X,K}$: it is a $\mathbb{Q}_\ell$-linear Lie subalgebra of $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))$ that would not change if one replaces K by its finite algebraic extension. On the other hand, extending $e_{\lambda,\ell}$ by $\mathbb{Q}_\ell$-linearity to $V_\ell(X)$ from $T_\ell(X)$, we obtain the nondegenerate alternating $\mathbb{Q}_\ell$-bilinear form

$$V_\ell(X) \times V_\ell(X) \to \mathbb{Q}_\ell,$$

which we continue to denote by $e_{\ell,\lambda}$. We have

$$G_{\ell,X,K} \subset \mathrm{Gp}(T_\ell(X), e_{\ell,\lambda}) \subset \mathrm{Gp}(V_\ell(X), e_{\ell,\lambda}) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(X)).$$

It is well known that the Lie algebra $\mathfrak{gp}(V_\ell(X), e_{\ell,\lambda})$ of the ℓ-adic Lie group $\mathrm{Gp}(V_\ell(X), e_{\ell,\lambda})$ coincides with the direct sum $\mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{sp}(V_\ell(X), e_{\ell,\lambda})$ where $\mathrm{Id} : V_\ell(X) \to V_\ell(X)$ is the identity map and $\mathfrak{sp}(V_\ell(X), e_{\ell,\lambda})$ is the Lie algebra of the ℓ-adic symplectic Lie group $\mathrm{Sp}(V_\ell(X), e_{\ell,\lambda})$. We have

$$\mathfrak{g}_{\ell,X} \subset \mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{sp}(V_\ell(X), e_{\ell,\lambda}) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X)).$$

Notice that the open compact subgroup $\mathrm{Gp}(T_\ell(X), e_{\ell,\lambda})$ of $\mathrm{Gp}(V_\ell(X), e_{\ell,\lambda})$ has the same Lie algebra $\mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{sp}(V_\ell(X), e_{\ell,\lambda})$ as $\mathrm{Gp}(V_\ell(X), e_{\ell,\lambda})$.

Now assume that K is finitely generated over its prime subfield and $\mathrm{End}(X) = \mathbb{Z}$. According to results of [13, 22, 40] (where the Tate conjecture for homomorphisms of abelian varieties and semisimplicity of Tate modules were proven), for every finite separable algebraic extension K_1 of K the $\mathrm{Gal}(K_1)$-module $V_\ell(X)$ is absolutely simple. We claim that for every open subgroup G_1 of finite index in $G_{\ell,X,K}$ the G_1-module $V_\ell(X)$ is absolutely simple. Indeed, the preimage $\rho_{\ell,X}^{-1}(G_1)$ is an open subgroup of finite index in $\mathrm{Gal}(K)$ and therefore coincides with $\mathrm{Gal}(K_1)$ for a certain finite separable algebraic extension K_1/K; in addition, $\rho_{\ell,X}(\mathrm{Gal}(K_1)) = G_1$. It follows that

$$\mathbb{Q}_\ell = \mathrm{End}_{\mathrm{Gal}(K_1)}(V_\ell(X)) = \mathrm{End}_{G_1}(V_\ell(X)),$$

and we are done if we know that the G_1-module $V_\ell(X)$ is semisimple. However, if G_1 is normal in $G_{\ell,X,K}$, then the (semi)simplicity of the $G_{\ell,X,K}$-module $V_\ell(X)$ implies the semisimplicity of the G_1-module $V_\ell(X)$, thanks to a theorem of Clifford [6, Sect, 49, Th. (49.2)]. In order to do the general case of not necessarily normal G_1, notice that every G_1 contains an open subgroup G_2 that is a normal (open) subgroup of finite index in $G_{\ell,X,K}$ that is the kernel of the natural continuous homomorphism from G to the group of permutations of the finite set $G_{\ell,X,K}/G_1$. We get that $V_\ell(X)$ is an absolutely simple G_2-module. Since G_1 contains G_2, it follows that the G_1-module $V_\ell(X)$ is also absolutely simple.

Applying Lemma 7.1 of [48] to $V = V_\ell(X), G = G_{\ell,X,K}, e = e_{\ell,\lambda}$, we conclude that there exists a semisimple $\mathbb{Q}_\ell$-Lie algebra

$$\mathfrak{g}^{\mathrm{ss}} = \mathfrak{g}_\ell^{\mathrm{ss}} \subset \mathfrak{sp}(V_\ell(X), e_{\ell,\lambda}) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))$$

such that either $\mathfrak{g}_{\ell,X} = \mathfrak{g}^{\mathrm{ss}}$ or $\mathfrak{g}_{\ell,X} = \mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{g}^{\mathrm{ss}}$. In addition,

$$\mathfrak{g}^{\mathrm{ss}} = \mathfrak{g}_\ell^{\mathrm{ss}} \subset \mathfrak{sp}(V_\ell(X), e_{\ell,\lambda}).$$

Since $\mathrm{End}(X) = \mathbb{Z}$, it follows from [41, Cor. 1.3.1] (see also [2, 3]) that the center of $\mathfrak{g}_{\ell,X}$ coincides with $\mathbb{Q}_\ell \mathrm{Id}$ and therefore

$$\mathfrak{g}_{\ell,X} = \mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{g}^{\mathrm{ss}} = \mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{g}_\ell^{\mathrm{ss}} \subset \mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{sp}(V_\ell(X), e_{\ell,\lambda}).$$

Clearly, the semisimple linear $\mathbb{Q}_\ell$-Lie algebra

$$\mathfrak{g}_\ell^{\mathrm{ss}} \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))$$

is absolutely irreducible.

Remark 4.1. Assume that $\mathfrak{g}_\ell^{\mathrm{ss}} = \mathfrak{sp}(V_\ell(X), e_{\ell,\lambda})$. Then the Lie algebra $\mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{g}_\ell^{\mathrm{ss}}$ of $G_{\ell,X,K}$ coincides with the Lie algebra $\mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{sp}(V_\ell(X), e_{\ell,\lambda})$ of compact $\mathrm{Gp}(T_\ell(X), e_{\ell,\lambda})$, and therefore $G_{\ell,X,K}$ is an open subgroup of finite index in $\mathrm{Gp}(T_\ell(X), e_{\ell,\lambda})$.

Remark 4.2. Suppose that the absolutely irreducible linear Lie algebra

$$\mathfrak{g}_{\ell,X} \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))$$

contains a linear operator $V_\ell(X) \to V_\ell(X)$ of rank one. Let us look at the classification (in characteristic zero) of absolutely irreducible linear Lie algebras with operator of rank one [18] (see also [5, Ch. 8, sect. 13, ex. 15]). The list consists of $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))$, the Lie algebra $\mathfrak{sl}(V_\ell(X))$ of all operators with zero trace, $\mathfrak{sp}(V_\ell(X))$ and $\mathbb{Q}_\ell\mathrm{Id} \oplus \mathfrak{sp}(V_\ell(X))$ where $\mathfrak{sp}(V_\ell(X))$ is the Lie algebra of the symplectic group of a certain nondegenerate alternating bilinear form on $V_\ell(X)$. Since

$$\mathbb{Q}_\ell\mathrm{Id} \subset \mathfrak{g}_{\ell,X} \subset \mathbb{Q}_\ell\mathrm{Id} \oplus \mathfrak{sp}(V_\ell(X), e_{\ell,\lambda}),$$

we conclude that $\mathfrak{g}_{\ell,X}$ coincides with $\mathbb{Q}_\ell\mathrm{Id}\oplus\mathfrak{sp}(V_\ell(X), e_{\ell,\lambda})$. By Remark 4.1, $G_{\ell,X,K}$ is an open subgroup of finite index in $\mathrm{Gp}(T_\ell(X), e_{\ell,\lambda})$.

Theorem 4.3. *Suppose that K is finitely generated over its prime subfield and* $\mathrm{End}(X) = \mathbb{Z}$. *Assume additionally that there exists a finite algebraic field extension E/K such that E is a discrete valuation field with discrete valuation ring R and residue field k such that the Néron model $\mathcal{X}$ of X over* $\mathrm{Spec}(R)$ *is a semiabelian group scheme whose closed fiber has toric dimension* 1. *Suppose that* $\mathrm{char}(k) \neq \ell$. *Then $G_{\ell,X,K}$ is an open subgroup of finite index in* $\mathrm{Gp}(T_\ell(X), e_{\ell,\lambda})$.

Proof. Replacing K by E, we may and will assume that $E = K$. So, K is the discrete valuation field with discrete valuation ring $\mathcal{O}$ and residue field k, and the Néron model $\mathcal{X}$ of X over $\mathcal{O}$ is a semiabelian scheme (with generic fiber X) such that the identity component of its closed fiber (over k) is an extension of a $(\dim(X) - 1)$-dimensional abelian variety by a one-dimensional torus.

Let us choose a *henselization* $\mathcal{O}^h \subset \bar{K}$ of $\mathcal{O}$ [4, Sect. 2.3]; it is a henselian discrete valuation ring containing $\mathcal{O}$ that has the same residue field k, and any uniformizer of $\mathcal{O}$ is also a uniformizer of $\mathcal{O}^h$. The field K^h of fractions of $\mathcal{O}^h$ is a discrete valuation field containing K. Since

$$K \subset K^h \subset \bar{K},$$

we may view $\mathrm{Gal}(K^h)$ as a (closed) subgroup of $\mathrm{Gal}(K)$. Let $\mathcal{I} \subset \mathrm{Gal}(K^h)$ be the corresponding inertia (sub)group [4, Sect. 2.3, Prop. 11]. We have

$$\mathcal{I} \subset \mathrm{Gal}(K^h) \subset \mathrm{Gal}(K).$$

It is known [4, Sect. 7.2, Th. 1 and Cor. 2] that the Néron model $\mathcal{X}^h$ of X over $\mathcal{O}^h$ is canonically isomorphic to $\mathcal{X}\otimes_{\mathcal{O}}\mathcal{O}^h$. In particular, X has semistable reduction over K^h, and the identity component of its closed fiber ${\mathcal{X}^h}_k$ is a commutative algebraic group over k that is an extension of a $(\dim(X) - 1)$-dimensional abelian variety by a one-dimensional torus; we denote this torus by T_0. One may identify the ℓ-adic Tate module $T_\ell(\mathrm{T}_0)$ of T_0 with a certain rank $\dim(\mathrm{T}_0)$ free $\mathbb{Z}_\ell$-submodule W of $T_\ell(X)$ that is called the *toric part* of $T_\ell(X)$ [17, Sect. 2.3]. (In our case W has rank 1.)

Let $T_\ell(X)^{\mathcal{I}}$ be the $\mathbb{Z}_\ell$-submodule of $\mathcal{I}$-invariants in $\mathrm{T}_\ell(X)$. By Grothendieck's criterion of semistable reduction [17, Prop. 3.5(iii) on p. 350], the orthogonal complement of $T_\ell(X)^{\mathcal{I}}$ in $T_\ell(X)$ with respect to $e_{\ell,\lambda}$ coincides with W. Since $e_{\ell,\lambda}$ is nondegenerate, the rank arguments imply that $T_\ell(X)^{\mathcal{I}}$ is a free $\mathbb{Z}_\ell$-module of rank $2\dim(X) - 1$. It follows easily that the $\mathbb{Q}_\ell$-vector subspace $V_\ell(X)^{\mathcal{I}}$ of $\mathcal{I}$-invariants

has codimension 1 in $V_\ell(X)$. It follows that there exists

$$\sigma \in \mathcal{I} \subset \mathrm{Gal}(K^h) \subset \mathrm{Gal}(K)$$

such that the subspace of σ-invariants in $V_\ell(X)$ has codimension 1. This implies that the linear operator

$$u := \rho_{\ell,X}(\sigma) - \mathrm{Id} : V_\ell(X) \to V_\ell(X)$$

has rank one. The other part of the same criterion of Grothendieck [17, Prop. 3.5(iv)] implies that $\rho_{\ell,X}(\sigma)$ is a unipotent linear operator in $V_\ell(X)$; more precisely,

$$[\rho_{\ell,X}(\sigma) - \mathrm{Id}]^2 = 0 \in \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X)),$$

since the reduction is semistable. Then the ℓ-adic logarithm $\log(\rho_{\ell,X}(\sigma))$ of $\rho_{\ell,X}(\sigma) \in G_{\ell,X,K}$ equals $\rho_{\ell,X}(\sigma) - \mathrm{Id}$ and therefore coincides with u. Since $\log(\rho_{\ell,X}(\sigma))$ lies in the Lie algebra $\mathfrak{g}_{\ell,X}$ of $G_{\ell,X,K}$, we conclude that u is the desired operator of rank one in $\mathfrak{g}_{\ell,X}$. Now Remark 4.2 implies that

$$\mathfrak{g}_{\ell,X} = \mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{sp}(V_\ell(X), e_{\ell,\lambda})$$

and $G_{\ell,X,K}$ is an open subgroup of finite index in $\mathrm{Gp}(T_\ell(X), e_{\ell,\lambda})$. □

Theorem 4.4. *We keep the notation and assumptions of Theorem* 4.3. *Then for all but finitely many primes ℓ the group $\tilde{G}_{\ell,X,K}$ contains* $\mathrm{Sp}(X_\ell, \bar{e}_{\lambda,\ell})$.

Proof. This is a result of [19] when K is a global field. The general case was done in [1]. The proof makes use of the classification of irreducible linear groups (over finite fields) generated by transvections [39]. □

Let K be a field that is finitely generated over its prime subfield. For each prime $\ell \neq \mathrm{char}(K)$ and positive integer j we write $K(\mu_{\ell^j})$ for the subfield of $\bar{K}$ obtained by adjoining to K all ℓ^jth roots of unity. It is well known that $K(\mu_{\ell^j})/K$ is an abelian field extension of degree dividing $(\ell-1)\ell^{j-1}$ and the cyclotomic character $\bar{\chi}_{\ell^j}$ factors through the embedding

$$\mathrm{Gal}(K(\mu_{\ell^j})/K) \hookrightarrow (\mathbb{Z}/\ell^j\mathbb{Z})^*.$$

We will use the following elementary statement that is well known, but we did not find a suitable reference. (It will be proven in Section 7.)

Theorem 4.5. *Let K be a field of characteristic zero that is finitely generated over $\mathbb{Q}$. Then for all but finitely many primes ℓ all the group embeddings* $\mathrm{Gal}(K(\mu_{\ell^j})/K) \hookrightarrow (\mathbb{Z}/\ell^j\mathbb{Z})^*$ *are isomorphisms.*

Corollary 4.6 (Corollary to Theorem 4.3)**.** *We keep the notation and assumptions of Theorem* 4.3. *Then for all but finitely many primes ℓ the group $G_{\ell,X,K}$ contains* $\mathrm{Sp}(T_\ell(X), e_{\ell,\lambda})$. *If, in addition,* $\mathrm{char}(K) = 0$, *then for all but finitely many primes ℓ the group $G_{\ell,X,K} = \mathrm{Gp}(T_\ell(X), e_{\ell,\lambda})$.*

Proof of Corollary 4.6. Let us assume that a prime $\ell \geq 5$ and $\deg(\lambda)$ is not divisible by ℓ. In particular, $\bar{e}_{\lambda,\ell}$ is nondegenerate and the finite group $\mathrm{Sp}(X_\ell, \bar{e}_{\lambda,\ell})$ is perfect, i.e., coincides with its own derived subgroup $[\mathrm{Sp}(X_\ell, \bar{e}_{\lambda,\ell}),\ \mathrm{Sp}(X_\ell, \bar{e}_{\lambda,\ell})]$. Using Theorem 4.4, we may and will assume (after removing finitely many primes) that $\tilde{G}_{\ell,X,K}$ contains $\mathrm{Sp}(X_\ell, \bar{e}_{\lambda,\ell})$.

Recall that $G_{\ell,X,K}$ is an open subgroup of finite index in $\mathrm{Gp}(T_\ell(X), e_{\ell,\lambda})$ and therefore is a *closed* subgroup in $\mathrm{Gp}(T_\ell(X), e_{\ell,\lambda})$. Following Serre [34], let us consider the closure G of the derived subgroup $[G_{\ell,X,K},\ G_{\ell,X,K}]$ of $G_{\ell,X,K}$ in

$\mathrm{Gp}(T_\ell(X), e_{\ell,\lambda})$. Since $G_{\ell,X,K}$ is closed in $\mathrm{Gp}(T_\ell(X), e_{\ell,\lambda})$, the group G is a subgroup of $G_{\ell,X,K}$. Clearly, G is also a closed subgroup of $\mathrm{Sp}(T_\ell(X), e_{\ell,\lambda})$ that maps surjectively on

$$[\mathrm{Sp}(X_\ell, \bar{e}_{\lambda,\ell}),\ \mathrm{Sp}(X_\ell, \bar{e}_{\lambda,\ell})] = \mathrm{Sp}(X_\ell, \bar{e}_{\lambda,\ell}).$$

It follows from a theorem of Serre [34] (see also [38, Th. 1.3]) that $G = \mathrm{Sp}(T_\ell(X), e_{\ell,\lambda})$. We conclude that $\mathrm{Sp}(T_\ell(X), e_{\ell,\lambda}) \subset G_{\ell,X,K}$. This proves the first assertion.

Now, assume additionally that $\mathrm{char}(K) = 0$. It follows from Theorem 4.5 that for all but finitely many primes ℓ the cyclotomic character $\chi_\ell : \mathrm{Gal}(K) \to \mathbb{Z}_\ell^*$ is surjective. This implies that the homomorphism

$$G_{\ell,X,K} \to \mathrm{Gp}(T_\ell(X), e_{\ell,\lambda})/\mathrm{Sp}(T_\ell(X), e_{\ell,\lambda}) = \mathbb{Z}_\ell^*$$

is also surjective for all but finitely many primes ℓ. In order to finish the proof, one has only to recall that we just proved that $\mathrm{Sp}(T_\ell(X), e_{\ell,\lambda}) \subset G_{\ell,X,K}$ for all but finitely many primes ℓ. □

Remark 4.7. It follows from Theorem 7.7 below that when $\mathrm{char}(K) = p > 0$ the index of the image $\bar{\chi}_\ell(\mathrm{Gal}(K))$ in $(\mathbb{Z}/\ell\mathbb{Z})^*$ is an unbounded function in ℓ. It follows that the function that assigns to a prime $\ell \neq p$ the index of $\tilde{G}_{\ell,X,K}$ in $\mathrm{Gp}(X_\ell, \bar{e}_{\lambda,\ell})$ is also unbounded. This, in turn, implies the unboundness of the function that assigns to a prime $\ell \neq p$ the index of $G_{\ell,X,K}$ in $\mathrm{Gp}(T_\ell(X), e_{\lambda,\ell})$.

Remark 4.8. It was stated without a proof in [19, Remark on p. 707] that if K is a global field of characteristic $p > 0$, then $\tilde{G}_{\ell,X,K}$ does *not* coincide with $\mathrm{Gp}(X_\ell, \bar{e}_{\lambda,\ell})$ for *infinitely* many primes ℓ.

Remarks 4.9. (i) Recall (see the proof of Theorem 4.3) that if a prime $\ell \neq \mathrm{char}(k)$, then

$$\mathfrak{g}_{\ell,X} = \mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{sp}(V_\ell(X), e_{\ell,\lambda}).$$

We claim that this equality (and therefore the conclusion of Theorem 4.3) holds for all $\ell \neq \mathrm{char}(K)$. Clearly, the only remaining case is

$$\mathrm{char}(K) = 0, \mathrm{char}(k) = p > 0, \ell = p.$$

In order to do that, let us choose a *prime* $q \neq p$. We know that

$$\mathfrak{g}_{q,X} = \mathbb{Q}_q \mathrm{Id} \oplus \mathfrak{sp}(V_q(X), e_{q,\lambda}).$$

Recall that for *all* primes ℓ,

$$\mathfrak{g}_{\ell,X} = \mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{g}_\ell^{\mathrm{ss}} \subset \mathbb{Q}_\ell \mathrm{Id} \oplus \mathfrak{sp}(V_\ell(X), e_{\ell,\lambda}),$$

where $\mathfrak{g}_\ell^{\mathrm{ss}}$ is an absolutely irreducible semisimple $\mathbb{Q}_\ell$-Lie algebra. Now the same arguments as in [44, Lemma 8.2 and its proof on pp. 426–427] prove that

$$\mathfrak{g}_{p,X} = \mathbb{Q}_p \mathrm{Id} \oplus \mathfrak{sp}(V_p(X), e_{p,\lambda})$$

provided we replace all 2's by q and all ℓ's by p.

(ii) The same arguments from invariant theory [20] as in [48, Sect. 9] prove that for every finite algebraic field extension K'/K and each self-product X^m of X, every ℓ-adic Tate class on X^m can be presented as a linear combination of products of divisor classes on X^m. In particular, the Tate conjecture holds true for all X^m in all codimensions. (In codimension one the Tate conjecture [36] for abelian varieties was proven by Tate himself over finite

fields [37], by the author [40] in characteristic > 2, by Faltings [12, 13] in characteristic 0, and by S. Mori [22] in characteristic 2 respectively.)

Assume additionally that $\mathrm{char}(K) = 0$ and therefore K is finitely generated over $\mathbb{Q}$, and fix an embedding $\bar{K} \subset \mathbb{C}$. Then the same arguments as in [44, Sect. 10] and [48, Sect. 10] (based on a theorem of Pijatetskij-Shapiro, Deligne and Borovoi [7,31]) prove that for each self-product X^m of X every Hodge class on X^m can be presented as a linear combination of products of divisor classes on X^m. In particular, the Hodge conjecture holds true for all X^m in all codimensions. In addition, the Mumford-Tate conjecture holds true for X. (See also [49].)

5. Points of order 2

5.1. Let K be a field of characteristic different from 2, and let $f(x) \in K[x]$ be a polynomial of *odd* degree $n \geq 5$ and without multiple roots. Let C_f be the hyperelliptic curve $y^2 = f(x)$ and $J(C_f)$ the Jacobian of C_f. The Galois module $J(C_f)_2$ of points of order 2 admits the following description.

Let $\mathbb{F}_2^{\mathfrak{R}_f}$ be the n-dimensional $\mathbb{F}_2$-vector space of functions $\varphi : \mathfrak{R}_f \to \mathbb{F}_2$ provided with the natural structure of a $\mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f)$-module. The canonical surjection

$$\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(K(\mathfrak{R}_f)/K) = \mathrm{Gal}(f)$$

provides $\mathbb{F}_2^{\mathfrak{R}_f}$ with the structure of a $\mathrm{Gal}(K)$-module. Let us consider the hyperplane

$$(\mathbb{F}_2^{\mathfrak{R}_f})^0 := \{\varphi : \mathfrak{R}_f \to \mathbb{F}_2 \mid \sum_{\alpha \in \mathfrak{R}_f} \varphi(\alpha) = 0\} \subset \mathbb{F}_2^{\mathfrak{R}_f}.$$

Clearly, $(\mathbb{F}_2^{\mathfrak{R}_f})^0$ is a Galois submodule in $\mathbb{F}_2^{\mathfrak{R}_f}$.

It is well known (see, for instance, [43]) that if n is odd, then the Galois modules $J(C_f)_2$ and $(\mathbb{F}_2^{\mathfrak{R}_f})^0$ are isomorphic. It follows that if $X = J(C_f)$, then $\tilde{G}_{2,X,K} = \mathrm{Gal}(f)$ and $K(J(C_f)_2) = K(\mathfrak{R}_f)$.

Lemma 5.2. *Suppose that $n = \deg(f)$ is odd and $f(x) = (x - t)h(x)$ with $t \in K$ and $h(x) \in K[x]$. Then $\tilde{G}_{2,J(C_f),K} \cong \mathrm{Gal}(h)$ and the Galois modules $J(C_f)_2$ and $\mathbb{F}_2^{\mathfrak{R}_h}$ are isomorphic.*

Proof. This is Lemma 5.1 of [48]. □

Corollary 5.3. *Suppose that $n = \deg(f) = 2g + 1$ is odd and $f(x) = (x - t)h(x)$ with $t \in K$ and $h(x) \in K[x]$. Assume also that $\mathrm{Gal}(h) = \mathrm{Alt}(\mathfrak{R}_h) \cong \mathbf{A}_{2g}$.*

Assume additionally that there exists a finite algebraic field extension E/K such that E is a discrete valuation field with discrete valuation ring R and residue field k such that the Néron model of $J(C_f)$ over $\mathrm{Spec}(R)$ is a semiabelian group scheme whose closed fiber has toric dimension 1. Then $\mathrm{End}(J(C_f)) = \mathbb{Z}$.

Proof of Corollary 5.3. Let us put $K = F$, $X = J(C_f)$ and $B = \mathfrak{R}_h$. Then the assertion is an immediate corollary of Lemma 5.2 and Corollary 3.8. □

Theorem 5.4. *Suppose that $n = 2g + 2 = \deg(f) \geq 8$ is even and that $f(x) = (x - t_1)(x - t_2)u(x)$ with*

$$t_1, t_2 \in K,\ t_1 \neq t_2,\ u(x) \in K[x],\ \deg(u) = n - 2.$$

Suppose that $\mathrm{Gal}(u) = \mathbf{S}_{2g}$ *or* $\mathbf{A}_{2g}$. *Assume additionally that there exists a finite algebraic field extension* E/K *such that* E *is a discrete valuation field with discrete valuation ring* R *and residue field* k *such that the Néron model of* $J(C_f)$ *over* $\mathrm{Spec}(R)$ *is a semiabelian group scheme whose closed fiber has toric dimension* 1. *Then* $\mathrm{End}(J(C_f)) = \mathbb{Z}$.

Proof. Replacing K if necessary by its suitable quadratic extension, we may and will assume that $\mathrm{Gal}(u) = \mathbf{A}_{2g}$. Let us put $h(x) = (x - t_2)u(x)$. We have $f(x) = (x - t_1)h(x)$. Let us consider the degree $(n-1)$ polynomials

$$h_1(x) = h(x + t_1) = (x + t_1 - t_2)u(x + t_1),\ h_2(x) = x^{n-1}h_1(1/x) \in K[x].$$

We have

$$\mathfrak{R}_{h_1} = \{\alpha - t_1 \mid \alpha \in \mathfrak{R}_h\} = \{\alpha - t_1 + t_2 \mid \alpha \in \mathfrak{R}_u\} \cup \{t_2 - t_1\},$$

$$\mathfrak{R}_{h_2} = \left\{\frac{1}{\alpha - t_1} \mid \alpha \in \mathfrak{R}_u\right\} \cup \left\{\frac{1}{t_2 - t_1}\right\}.$$

This implies that

$$K(\mathfrak{R}_{h_2}) = K(\mathfrak{R}_{h_1}) = K(\mathfrak{R}_u)$$

and

$$h_2(x) = \left(x - \frac{1}{t_2 - t_1}\right) v(x)$$

where $v(x) \in K[x]$ is a degree $(n-2)$ polynomial with $K(\mathfrak{R}_v) = K(\mathfrak{R}_u)$; in particular, $\mathrm{Gal}(v) = \mathrm{Gal}(u) = \mathbf{A}_{n-2}$. Again, the standard substitution

$$x_1 = 1/(x - t_1),\ y_1 = y/(x - t_1)^{g+1}$$

establishes a birational K-isomorphism between C_f and a hyperelliptic curve

$$C_{h_2} : y_1^2 = h_2(x_1).$$

Now the result follows from Corollary 5.3 applied to $h_2(x_1)$. □

6. Proof of main results

We keep the notation and assumptions of Theorem 1.3. In addition, let us put

$$X = J(C_f),\ S = \mathrm{Spec}(R).$$

Let us start to prove Theorem 1.3. First, notice that the equation $y^2 = f(x)$ defines a (semi)stable genus g curve over R whose generic fiber is smooth while its closed fiber is an irreducible reduced curve with one double point. More precisely, there is a semistable projective (flat) R-curve

$$\mathcal{C} := \mathrm{Proj}\ R[\mathbf{X}, \mathbf{Y}, \mathbf{Z}]/(F(\mathbf{X}, \mathbf{Y}, \mathbf{Z})) \to \mathrm{Spec}(R) = S$$

where

$$\begin{aligned} F(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) &= (\mathbf{Z}^{g+1})^2[((\mathbf{Y}/\mathbf{Z})^{g+1})^2 - f(\mathbf{X}/\mathbf{Z})] \\ &= \mathbf{Y}^2 - (\mathbf{X} - t_1\mathbf{Z})(\mathbf{X} - t_2\mathbf{Z})\mathbf{Z}^{2g}u(\mathbf{X}/\mathbf{Z}) \\ &= \mathbf{Y}^2 - (\mathbf{X} - t_1\mathbf{Z})(\mathbf{X} - t_2\mathbf{Z})\sum_{i=0}^{2g} a_i\mathbf{X}^i\mathbf{Z}^{2g-i} \in R[\mathbf{X}, \mathbf{Y}, \mathbf{Z}], \\ &\qquad \deg(\mathbf{X}) = \deg(\mathbf{Z}) = 1, \deg(\mathbf{Y}) = g + 1. \end{aligned}$$

The principal open (affine) subset $D_+(\mathbf{Z})$ of $\mathcal{C}$ is

$$\text{Spec } R[\mathbf{X}/\mathbf{Z}, \mathbf{Y}/\mathbf{Z}^{g+1}] = \text{Spec } R[x,y]/(y^2 - f(x))$$

with $x = \mathbf{X}/\mathbf{Z}, y = \mathbf{Y}/\mathbf{Z}^{g+1}$. The generic fiber of $\mathcal{C}$ coincides with the hyperelliptic curve C_f/K. Its closed fiber $\mathcal{C}_k$ is a singular (reduced) absolutely irreducible curve over the residue field k whose only singularity is an ordinary double point $(\bar{\beta} : 0 : 1)$ where

$$\bar{\beta} := t_1 \bmod m = t_2 \bmod m \in R/\mathfrak{m} = k.$$

The normalization of $\mathcal{C}_k$ is a (smooth projective) hyperelliptic curve of genus $g-1$ over k. This implies (see [4, Ch. 9, Example 8 on p. 246]) that $\text{Pic}^0_{\mathcal{C}_k/k}$ is a (connected) commutative algebraic k-group that is an extension of a $(g-1)$-dimensional abelian variety by a one-dimensional torus. On the other hand, $\text{Pic}^0_{\mathcal{C}/S}$ is a quasi-projective smooth separated S-group scheme [4, Th. 1 on p. 252] whose closed fiber coincides with $\text{Pic}^0_{\mathcal{C}_k/k}$ while the generic fiber is $J(C_f) = X$. In particular, $\text{Pic}^0_{\mathcal{C}/S}$ is a semiabelian scheme whose closed fiber has toric dimension one. Now let $\mathcal{X} \to S$ be the Néron model of X with closed fiber $\mathcal{X}_k$. The generic fibers of both $\mathcal{X}$ and $\text{Pic}^0_{\mathcal{C}/S}$ coincide with $X = J(C_f)$. Since $\text{Pic}^0_{\mathcal{C}/S}$ is semiabelian, it follows from [4, Ch. 7, Prop. 3 on p. 182] that the identity components of the closed fibers of $\mathcal{X}$ and $\text{Pic}^0_{\mathcal{C}/S}$ are isomorphic. This implies that (connected) $\text{Pic}^0_{\mathcal{C}_k/k}$ is isomorphic to the identity component $\mathcal{X}_k^0$ of $\mathcal{X}_k$; in particular, ${\mathcal{X}_k}^0$ has toric dimension one. Now Theorem 5.4 tells us that $\text{End}(J(C_f)) = \text{End}(X) = \mathbb{Z}$. This proves the first assertion of Theorem 1.3. The second assertion follows from Theorem 4.3 combined with Remark 4.9(i), while the third one follows from Corollary 4.6.

7. Cyclotomic extensions

Throughout this section, k is a field and $K \supset k$ its overfield that is finitely generated over k.

It seems that the following two lemmas are well known, but we did not find a suitable reference.

Lemma 7.1. *Let k' be the algebraic closure of k in K. Then $[k' : k] < \infty$, i.e., the field k' is a finite algebraic extension of k.*

Proof. The following elementary proof of Lemma 7.1 was suggested by the referee. (The original proof was based on a theorem of Emmy Noether ([9, Ch. IV, Sect. 4.2, Th. 4.14 on p. 127]) and used [9, Ch. IV, Sect. 4.4, Prop. 4.15 on p. 129 and Cor. 4.17 on p. 131].)

Let m be the transcendence degree of K over k. If $m = 0$, then K is algebraic over k and the assertion is trivial. So, we may assume that $m \ge 1$. Let $\{x_1, \dots, x_m\} \subset K$ be a transcendental basis of K over k and let $K_1 := k(x_1, \dots, x_m) \subset K$ be the corresponding purely transcendental extension of k. Since K is finitely generated over k and algebraic over K_1, the degree $[K : K_1]$ is finite. Let us consider the compositum $k'K_1 \subset K$ of k' and K_1. Since

$$K_1 \subset k'K_1 \subset K,$$

the field $k'K_1$ has finite degree over K_1 (and $[k'K_1 : K_1]$ divides $[K : K_1]$).

As algebraic extensions and purely transcendental extensions are linearly disjoint, $k'K_1$ is isomorphic to $k' \otimes_k K_1$ and hence the (finite) degree $[k'K_1 : K_1] = [k' : k]$. It follows that k'/k is also a finite algebraic field extension. □

Remark 7.2. The field K is finitely generated over k and therefore over k'. Suppose that k is perfect. Since k'/k is finite algebraic, k' is also perfect. Since the perfect (sub)field k' is algebraically closed in K, the field K is separable over k' (see [9, Appendix A1, Sect. A1.2 and Cor. A1.7 on p. 568]).

Lemma 7.3. *Suppose k is perfect. Let κ/k' be an algebraic field extension of finite degree. Then $K \otimes_{k'} \kappa$ is a field and the field extension $(K \otimes_{k'} \kappa)/K$ has degree $[\kappa : k']$. In particular, if κ/k' is a Galois extension, then $(K \otimes_{k'} \kappa)/K$ is also a Galois extension and the natural map*

$$\mathrm{Gal}(\kappa/k') \to \mathrm{Gal}((K \otimes_{k'} \kappa)/K),\ \sigma \mapsto \{x \otimes \beta \mapsto x \otimes \sigma(\beta)\}$$
$$\forall \sigma \in \mathrm{Gal}(\kappa/k'), x \in K, \beta \in \kappa$$

is an isomorphism of Galois groups.

Proof. By Remark 7.2, K is separable over k'. By Exercise A.1.2a and its solution in [9, pp. 568–569 and p. 749] (applied to $R = K$ and $S = \kappa$) the tensor product $K \otimes_{k'} \kappa$ is a domain and therefore is a field, since it is a finite-dimensional K-algebra whose dimension equals $[\kappa : k']$. □

Lemma 7.3 implies readily the following statement.

Corollary 7.4. *Suppose that k is perfect and let us fix an algebraic closure $\overline{k'}$ of k'. Then $K \otimes_{k'} \overline{k'}$ is a field that is a Galois extension of $K = K \otimes 1$ and the Galois group $\mathrm{Gal}((K \otimes_{k'} \overline{k'})/K)$ is canonically isomorphic to the absolute Galois group $\mathrm{Gal}(\overline{k'}) = \mathrm{Gal}(\overline{k'}/k')$ of k'.*

Proof of Theorem 4.5. The field K is finitely generated over $\mathbb{Q}$. It follows from Lemma 7.1 that the algebraic closure $\mathbb{Q}'$ of $\mathbb{Q}$ in K is an algebraic number field of finite degree over $\mathbb{Q}$. Let us put $k = \mathbb{Q}'$. Then k is algebraically closed in K. For all but finitely many primes ℓ the field extension $k/\mathbb{Q}$ is unramified at all prime divisors of ℓ. This implies that the ramification index of the field extension $k(\mu_{\ell^j})/k$ is at least $\varphi(\ell^j) = [\mathbb{Q}(\mu_{\ell^j}) : \mathbb{Q}]$ at all prime divisors of such ℓ. (Here φ is the Euler function.) This implies that $[k(\mu_{\ell^j}) : k] = [\mathbb{Q}(\mu_{\ell^j}) : \mathbb{Q}]$, i.e., k and $\mathbb{Q}(\mu_{\ell^j})$ are linearly disjoint over $\mathbb{Q}$. By Lemma 7.3, $K \otimes_k k(\mu_{\ell^j})$ is a field that is an extension of K of of degree $\varphi(\ell^j)$. It follows that the natural surjective homomorphism of $k(\mu_{\ell^j})$-algebras $K \otimes_k k(\mu_{\ell^j}) \to K(\mu_{\ell^j})$ is injective and therefore is a field isomorphism. In particular, $K(\mu_{\ell^j})$ is a degree $\varphi(\ell^j)$ Galois extension of K and

$$\mathrm{Gal}(K(\mu_{\ell^j})/K) = \mathrm{Gal}(k(\mu_{\ell^j})/k) = \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^j})/\mathbb{Q}) = (\mathbb{Z}/\ell^j\mathbb{Z})^*.$$

□

7.5. Now and until the end of Section 7 let us assume that k is the prime finite field $\mathbb{F}_p$ of characteristic p. It follows from Lemma 7.1 that k' is a finite field of characteristic p and therefore the number $q' = \#(k')$ of its elements is a power of p. For every prime $\ell \neq p$ we write $N_p(\ell)$ (resp. $N'(\ell)$), the index in $(\mathbb{Z}/\ell\mathbb{Z})^*$ of the cyclic multiplicative subgroup generated by $p \bmod \ell$ (resp. $q' \bmod \ell$). Clearly, $N_p(\ell)$ divides $N'(\ell)$.

The following assertion that is based on results of P. Moree [21] will be proven at the end of this section.

Lemma 7.6. *The function $\ell \mapsto N_p(\ell)$ is an unbounded function in ℓ.*

Theorem 7.7. (i) *For all primes $\ell \ne p$ the image*

$$\bar{\chi}_{\ell,K}(\mathrm{Gal}(K)) \subset (\mathbb{Z}/\ell\mathbb{Z})^*$$

is the cyclic multiplicative subgroup generated by $q' \bmod \ell$.

(ii) *Let $N_K(\ell)$ be the index $[(\mathbb{Z}/\ell\mathbb{Z})^* : \bar{\chi}_\ell(\mathrm{Gal}(K))]$. Then the function $\ell \mapsto N_K(\ell)$ is an unbounded function in ℓ.*

Proof of Theorem 7.7 (modulo Lemma 7.6). Since $k' \subset \bar{K}$, the algebraic closure of k' in $\bar{K}$ is an algebraically closed field and will be denoted by $\overline{k'}$. It follows from Corollary 7.4 that there is the natural continuous surjective group homomorphism of absolute Galois groups

$$\mathrm{rest} : \mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(k'),$$

where for each automorphism σ of $\bar{K}/K$ we write $\mathrm{rest}(\sigma)$ for its restriction to $\overline{k'}$. We need to distinguish between two cyclotomic characters:

$$\bar{\chi}_{\ell,K} : \mathrm{Gal}(K) \to (\mathbb{Z}/\ell\mathbb{Z})^*$$

and

$$\bar{\chi}_{\ell,k'} : \mathrm{Gal}(k') \to (\mathbb{Z}/\ell\mathbb{Z})^*$$

that define the action on ℓth roots of unity of $\mathrm{Gal}(K)$ and $\mathrm{Gal}(k')$ respectively. However, since all ℓth roots of unity of $\bar{K}$ lie in $\overline{k'}$,

$$\bar{\chi}_{\ell,K} = \bar{\chi}_{\ell,k'}\ \mathrm{rest} : \mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(k') \to (\mathbb{Z}/\ell\mathbb{Z})^*;$$

in particular, both cyclotomic characters have the same image in $(\mathbb{Z}/\ell\mathbb{Z})^*$. Since $\mathrm{Gal}(k')$ is generated (as the topological group) by the Frobenius automorphism that sends every element of $\overline{k'}$ (including all ℓth roots of unity) to its q'th power, the image

$$\bar{\chi}_{\ell,,k'}(\mathrm{Gal}(k')) \subset (\mathbb{Z}/\ell\mathbb{Z})^*$$

is the cyclic multiplicative subgroup generated by $q' \bmod \ell$. It follows that the image

$$\bar{\chi}_\ell(\mathrm{Gal}(K)) \subset (\mathbb{Z}/\ell\mathbb{Z})^*$$

is the cyclic multiplicative subgroup generated by $q' \bmod \ell$, i.e., we proved the first assertion of our theorem. In particular, $N_K(\ell)$ coincides with $N'(\ell)$. Recall that $N'(\ell)$ is a positive integer that is divisible by $N_p(\ell)$. It follows from Lemma 7.6 that the function

$$\ell \mapsto N'(\ell) = N_K(\ell)$$

is an unbounded function in ℓ. □

Proof of Lemma 7.6. Applying Lemma 4 of Section 2 in [21] (to $g = p$), we conclude that for every positive integer t the set of primes ℓ such that t divides $N_p(\ell)$ is infinite. (Actually, it is proven in [21] that this set of primes has a positive density.) In particular, for each t there is a prime $\ell \ne p$ with $N_p(\ell) \ge t$. This means that the function $\ell \mapsto N_p(\ell)$ is unbounded. □

8. Nonisomorphic hyperelliptic curves and Jacobians

We start to prove Theorem 1.7. Replacing K by its *perfectization*, we may and will assume that K is a perfect field.

It is well known ([16, Ch. 2, Sect. 3, pp. 253–255], [8, Ch. VIII, Sect. 3]) that the hyperelliptic curves C_{f_1} and C_{f_2} are isomorphic over $\bar{K}$ if and only if there exists a fractional linear transformation $T \in \mathrm{PGL}_2(\bar{K}) = \mathrm{Aut}(\mathbf{P}^1)$ that sends the branch points of the canonical double cover $C_{f_1} \to \mathbf{P}^1$ to the branch points of the canonical double cover $C_{f_2} \to \mathbf{P}^1$. If $\mathfrak{R} \subset \bar{K}$ is the set of roots of $u(x)$, then the corresponding sets of branch points are the disjoint unions $\mathfrak{R} \cup B_1$ and $\mathfrak{R} \cup B_2$ respectively.

Assume that $J(C_{f_1})$ and $J(C_{f_2})$ are isomorphic over $\bar{K}$. We need to get a contradiction. We know that $\mathrm{End}(J(C_{f_1})) = \mathbb{Z}$ and $\mathrm{End}(J(C_{f_2})) = \mathbb{Z}$. This implies that both Jacobians $J(C_{f_1})$ and $J(C_{f_2})$ have exactly one principal polarization, and therefore a $\bar{K}$-isomorphism of abelian varieties $J(C_{f_1}) \cong J(C_{f_2})$ respects the principal polarizations. Now the Torelli theorem implies that the hyperelliptic curves C_{f_1} and C_{f_2} are isomorphic over $\bar{K}$. Therefore there exists a fractional linear transformation $T \in \mathrm{PGL}_2(\bar{K}) = \mathrm{Aut}(\mathbf{P}^1)$ such that

$$T(\mathfrak{R} \cup B_1) = \mathfrak{R} \cup B_2.$$

Suppose that T is defined over K, i.e., lies in $\mathrm{PGL}_2(K)$. Then T commutes with the Galois action on $\bar{K}$ and therefore sends every Galois orbit in $\bar{K}$ onto another Galois orbit. This implies that T sends into itself the $2g$-element Galois orbit $\mathfrak{R}$; in addition, $T(B_1) = B_2$. Since

$$\mathrm{Alt}(\mathfrak{R}) \subset \mathrm{Gal}(u) \subset \mathrm{Perm}(\mathfrak{R})$$

and the only permutation of $\mathfrak{R}$ that commutes with all even permutations is the identity map, we conclude that T acts as the identity map on $\mathfrak{R}$. Since the number of elements in $\mathfrak{R}$ is greater than or equal to $2g \geq 4 > 3$, we conclude that T is the identity element of $\mathrm{PGL}_2(\bar{K})$ and therefore $B_2 = T(B_1) = B_1$, which is not the case. We obtained a contradiction but only under an additional assumption that T lies in $\mathrm{PGL}_2(K)$. Now assume that T does *not* lie in $\mathrm{PGL}_2(K)$. It follows from Hilbert's Theorem 90 that there is a Galois automorphism $\sigma \in \mathrm{Gal}(K)$ such that $\sigma(T) \neq T$. On the other hand, since both sets $\mathfrak{R} \cup B_1$ and $\mathfrak{R} \cup B_2$ are Galois-invariant,

$$\sigma(T)(\mathfrak{R} \cup B_1) = \mathfrak{R} \cup B_2.$$

If we put $U := T^{-1}\sigma(T) \in \mathrm{PGL}_2(\bar{K})$, then U does *not* coincide with the identity automorphism of $\mathbf{P}^1$ but $U(\mathfrak{R} \cup B_1) = \mathfrak{R} \cup B_1$. This implies that U gives rise to a nontrivial automorphism of C_{f_1} that is *not* the *hyperelliptic involution*. By functoriality, we obtain an automorphism of the abelian variety $J(C_{f_1})$ that is neither 1 nor -1. This gives us a contradiction, because

$$\mathrm{Aut}(J(C_{f_1})) = \mathrm{End}(J(C_{f_1}))^* = \mathbb{Z}^* = \{\pm 1\}.$$

This ends the proof of Theorem 1.7.

9. Concluding remarks

Let K and $f(x)$ be as in Theorem 1.3. Let us put $X = J(C_f)$. We know that $\mathrm{End}(X) = \mathbb{Z}$ and X has somewhere a semistable reduction with toric dimension one.

Now assume that K is finitely generated over its prime subfield and let ℓ be a prime different from $\mathrm{char}(K)$. It follows from arguments of Remark 4.9(ii) that for every finite algebraic field extension K'/K and each self-product X^m of X every ℓ-adic Tate class on X^m can be presented as a linear combination of products of divisor classes on X^m. In particular, the Tate conjecture holds true for all X^m in all codimensions.

Assume additionally that $\mathrm{char}(K) = 0$ and fix an embedding $\bar{K} \subset \mathbb{C}$. Then arguments of Remark 4.9(ii) imply that for each self-product X^m of X every Hodge class on X^m can be presented as a linear combination of products of divisor classes on X^m. In particular, the Hodge conjecture holds true for every X^m in all codimensions. In addition, the Mumford-Tate conjecture holds true for X.

Acknowledgements

The author is grateful to Chris Hall for useful discussions, Gregorz Banaszak and Wojciech Gajda for stimulating questions, and Boris Kunyavskii for help with references. His special thanks go to the referee, whose comments helped to improve the exposition.

This work was started during the author's stay at Max-Planck-Institut für Mathematik in September of 2013 and finished during the academic year 2013/2014 when the author was Erna and Jakob Michael Visiting Professor in the Department of Mathematics at the Weizmann Institute of Science. The hospitality and support of both institutes are gratefully acknowledged.

References

[1] Sara Arias-de-Reyna, Wojciech Gajda, and Sebastian Petersen, *Big monodromy theorem for abelian varieties over finitely generated fields*, J. Pure Appl. Algebra **217** (2013), no. 2, 218–229, DOI 10.1016/j.jpaa.2012.06.010. MR2969246

[2] Fedor Alekseivich Bogomolov, *Sur l'algébricité des représentations l-adiques* (French, with English summary), C. R. Acad. Sci. Paris Sér. A-B **290** (1980), no. 15, A701–A703. MR574307 (81c:14025)

[3] F. A. Bogomolov, *Points of finite order on abelian varieties* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **44** (1980), no. 4, 782–804, 973. MR587337 (81m:14031)

[4] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)

[5] N. Bourbaki, *Éléments de mathématique* (French), Fasc. XXXVIII: Groupes et algèbres de Lie. Chapitre VII: Sous-algèbres de Cartan, éléments réguliers. Chapitre VIII: Algèbres de Lie semi-simples déployées; Actualités Scientifiques et Industrielles, No. 1364, Hermann, Paris, 1975. MR0453824 (56 #12077)

[6] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, Vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962. MR0144979 (26 #2519)

[7] P. Deligne, *Hodge cycles on abelian varieties* (notes by J. S. Milne), in Hodge cycles, motives, and Shimura varieties, Lecture Notes in Math., vol. 900, Springer-Verlag, Berlin-New York, 1982, pp. 9–100.

[8] Igor Dolgachev and David Ortland, *Point sets in projective spaces and theta functions* (English, with French summary), Astérisque **165** (1988), 210 pp. (1989). MR1007155 (90i:14009)

[9] David Eisenbud, *Commutative algebra*, With a view toward algebraic geometry, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995. MR1322960 (97a:13001)

[10] Arsen Elkin and Yuri G. Zarhin, *Endomorphism algebras of hyperelliptic Jacobians and finite projective lines*, J. Ramanujan Math. Soc. **21** (2006), no. 2, 169–187. MR2244543 (2007m:14041)

[11] Arsen Elkin and Yuri G. Zarhin, *Endomorphism algebras of hyperelliptic Jacobians and finite projective lines. II*, J. Ramanujan Math. Soc. **25** (2010), no. 1, 1–23. MR2643388 (2011f:14048)

[12] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern* (German), Invent. Math. **73** (1983), no. 3, 349–366, DOI 10.1007/BF01388432. MR718935 (85g:11026a); Erratum, Invent. Math. **75** (1984), 381. MR0732554

[13] Gerd Faltings, Gisbert Wüstholz, Fritz Grunewald, Norbert Schappacher, and Ulrich Stuhler, *Rational points*, 2nd ed., papers from the seminar held at the Max-Planck-Institut für Mathematik, Bonn/Wuppertal, 1983/1984, Aspects of Mathematics, E6, Friedr. Vieweg & Sohn, Braunschweig, 1986. MR863887 (87m:11025)

[14] Gerd Faltings and Ching-Li Chai, *Degeneration of abelian varieties*, with an appendix by David Mumford, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 22, Springer-Verlag, Berlin, 1990. MR1083353 (92d:14036)

[15] Walter Feit and Jacques Tits, *Projective representations of minimum degree of group extensions*, Canad. J. Math. **30** (1978), no. 5, 1092–1102. MR0498824 (58 #16861)

[16] Phillip Griffiths and Joseph Harris, *Principles of algebraic geometry*, Pure and Applied Mathematics, Wiley-Interscience [John Wiley & Sons], New York, 1978. MR507725 (80b:14001)

[17] A. Grothendieck, *Modèles de Néron et monodromie*, Expose IX dans SGA7 I, Lecture Notes in Math. **288**, Springer Verlag, Berlin Heidelberg New York, 1972, 313–523.

[18] Victor W. Guillemin, Daniel Quillen, and Shlomo Sternberg, *The classification of the irreducible complex algebras of infinite type*, J. Analyse Math. **18** (1967), 107–112. MR0217130 (36 #221)

[19] Chris Hall, *An open-image theorem for a general class of abelian varieties*, with an appendix by Emmanuel Kowalski, Bull. Lond. Math. Soc. **43** (2011), no. 4, 703–711, DOI 10.1112/blms/bdr004. MR2820155 (2012f:11115)

[20] Roger Howe, *Remarks on classical invariant theory*, Trans. Amer. Math. Soc. **313** (1989), no. 2, 539–570, DOI 10.2307/2001418. MR986027 (90h:22015a); Erratum, Trans. Amer. Math. Soc. **318** (1990), 823. MR1019521

[21] Pieter Moree, *Asymptotically exact heuristics for (near) primitive roots. II*, Japan. J. Math. (N.S.) **29** (2003), no. 2, 143–157. MR2035537 (2004m:11188)

[22] Laurent Moret-Bailly, *Pinceaux de variétés abéliennes* (French, with English summary), Astérisque **129** (1985), 266. MR797982 (87j:14069)

[23] Brian Mortimer, *The modular permutation representations of the known doubly transitive groups*, Proc. London Math. Soc. (3) **41** (1980), no. 1, 1–20, DOI 10.1112/plms/s3-41.1.1. MR579714 (81f:20004)

[24] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970. MR0282985 (44 #219)

[25] Donald Passman, *Permutation groups*, W. A. Benjamin, Inc., New York-Amsterdam, 1968. MR0237627 (38 #5908)

[26] Michel Raynaud, *Faisceaux amples sur les schémas en groupes et les espaces homogènes* (French), Lecture Notes in Mathematics, Vol. 119, Springer-Verlag, Berlin-New York, 1970. MR0260758 (41 #5381)

[27] Kenneth A. Ribet, *Hodge classes on certain types of abelian varieties*, Amer. J. Math. **105** (1983), no. 2, 523–538, DOI 10.2307/2374267. MR701568 (85a:14030)

[28] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*, J. Pure Appl. Algebra **77** (1992), no. 3, 253–262, DOI 10.1016/0022-4049(92)90141-2. MR1154704 (93f:14022)

[29] J.-P. Serre, *Sur les groupes de Galois attachés aux groupes p-divisibles* (French), Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 118–131. MR0242839 (39 #4166)

[30] Jean-Pierre Serre, *Groupes algébriques associés aux modules de Hodge-Tate* (French), Journées de Géométrie Algébrique de Rennes. (Rennes, 1978), Astérisque, vol. 65, Soc. Math. France, Paris, 1979, pp. 155–188. MR563476 (81j:14027)

[31] Jean-Pierre Serre, *Représentations l-adiques* (French), Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), Japan Soc. Promotion Sci., Tokyo, 1977, pp. 177–193. MR0476753 (57 #16310)

[32] Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, with the collaboration of Willem Kuyk and John Labute, 2nd ed., Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. MR1043865 (91b:11071)

[33] Jean-Pierre Serre, *Lie algebras and Lie groups*, 1964 lectures given at Harvard University, 2nd ed., Lecture Notes in Mathematics, vol. 1500, Springer-Verlag, Berlin, 1992. MR1176100 (93h:17001)

[34] J.-P. Serre, *Lettre á Marie-France Vignéras*. in Œuvres. Collected papers. IV, 137, 2000, pp. 38–55.

[35] Jean-Pierre Serre, *Topics in Galois theory*, Lecture notes prepared by Henri Damon [Henri Darmon]; with a foreword by Darmon and the author, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992. MR1162313 (94d:12006)

[36] John T. Tate, *Algebraic cycles and poles of zeta functions*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 93–110. MR0225778 (37 #1371)

[37] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR0206004 (34 #5829)

[38] Adrian Vasiu, *Surjectivity criteria for p-adic representations. I*, Manuscripta Math. **112** (2003), no. 3, 325–355, DOI 10.1007/s00229-003-0402-4. MR2067042 (2005e:11157)

[39] A. E. Zalesskiĭ and V. N. Serežkin, *Linear groups generated by transvections* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **40** (1976), no. 1, 26–49, 221. MR0412295 (54 #421)

[40] Ju. G. Zarhin, *Abelian varieties in characteristic p* (Russian), Mat. Zametki **19** (1976), no. 3, 393–400. MR0422287 (54 #10278)

[41] Ju. G. Zarhin, *Torsion of abelian varieties in finite characteristic* (Russian), Mat. Zametki **22** (1977), no. 1, 3–11. MR0453757 (56 #12016)

[42] Yuri G. Zarhin, *Hyperelliptic Jacobians without complex multiplication*, Math. Res. Lett. **7** (2000), no. 1, 123–132, DOI 10.4310/MRL.2000.v7.n1.a11. MR1748293 (2001a:11097)

[43] Yuri G. Zarhin, *Hyperelliptic Jacobians and modular representations*, Moduli of abelian varieties (Texel Island, 1999), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 473–490. MR1827030 (2002b:11082)

[44] Yuri G. Zarhin, *Very simple 2-adic representations and hyperelliptic Jacobians*, Dedicated to Yuri I. Manin on the occasion of his 65th birthday, Mosc. Math. J. **2** (2002), no. 2, 403–431. MR1944511 (2003k:11098)

[45] Yuri G. Zarhin, *Homomorphisms of abelian varieties* (English, with English and French summaries), Arithmetic, geometry and coding theory (AGCT 2003), Sémin. Congr., vol. 11, Soc. Math. France, Paris, 2005, pp. 189–215. MR2182844 (2006k:14077)

[46] Yu. G. Zarhin, *Del Pezzo surfaces of degree 1 and Jacobians*, Math. Ann. **340** (2008), no. 2, 407–435, DOI 10.1007/s00208-007-0157-4. MR2368986 (2009g:14029)

[47] Yuri G. Zarhin, *Endomorphisms of superelliptic Jacobians*, Math. Z. **261** (2009), no. 3, 691–707, DOI 10.1007/s00209-008-0342-5. MR2471095

[48] Yuri G. Zarhin, *Families of absolutely simple hyperelliptic Jacobians*, Proc. Lond. Math. Soc. (3) **100** (2010), no. 1, 24–54, DOI 10.1112/plms/pdp020. MR2578467 (2011d:14055)

[49] Yuri G. Zarhin, *Hodge classes on certain hyperelliptic prymians*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 574, Amer. Math. Soc., Providence, RI, 2012, pp. 171–183, DOI 10.1090/conm/574/11432. MR2961409

[50] Yuri G. Zarhin, *Galois groups of Mori trinomials and hyperelliptic curves with big monodromy*, European J. Math., DOI 10.1007/s40879-015-0048-2.

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

Department of Mathematics, The Weizmann Institute of Science, P.O.B. 26, Rehovot 7610001, Israel

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