ABSOLUTELY SIMPLE PRYMIANS OF TRIGONAL CURVES

YURI G. ZARHIN

Dedicated To V. A. Iskovskikh on the occasion of his 70th birthday

1. Introduction

As usual, $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ denote the ring of integers, the field of rational numbers and the field of complex numbers respectively. Let us fix a primitive cubic root of unity $\zeta_3 = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$. Let $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ be the third cyclotomic field and $\mathbb{Z}[\zeta_3] = \mathbb{Z} + \mathbb{Z} \cdot \zeta_3$ its ring of integers. We write λ for the (principal) maximal ideal $(1 - \zeta_3) \cdot \mathbb{Z}[\zeta_3]$ of $\mathbb{Z}[\zeta_3]$.

It is known [11, Th. 5 on p. 176] (see also [5]) that for all positive integers m different from 2 there exists a m-dimensional complex abelian variety, whose endomorphism ring is $\mathbb{Z}[\zeta_3]$. Shimura's proof is purely complex-analytic and not constructive; roughly speaking it deals with points of the corresponding moduli space that do not belong to a countable union of subvarieties of positive codimension. In this paper we discuss a geometric approach to an explicit construction of those abelian varieties via jacobians, prymians and Galois theory.

In order to explain our approach, let us start with the following definitions. Let $f(x) \in \mathbb{C}[x]$ be a polynomial of degree $n \geq 4$ without multiple roots. Let $C_{f,3}$ be a smooth projective model of the smooth affine curve $y^3 = f(x)$. It is well known ([2], pp. 401-402, [15], Prop. 1 on p. 3359, [7], p. 148) that the genus $g(C_{f,3})$ of $C_{f,3}$ is $n-1$ if 3 does not divide n and $n-2$ if it does. In both cases $g(C_{f,3}) \geq 3$ is *not* congruent to 2 modulo 3.

The map $(x, y) \mapsto (x, \zeta_3 y)$ gives rise to a non-trivial birational automorphism $\delta_3 : C_{f,3} \to C_{f,3}$ of period 3. By functoriality, δ_3 induces the linear operator in the space of differentials of the first kind

$$\delta_3^* : \Omega^1(C_{f,3}) \to \Omega^1(C_{f,3}).$$

Its spectrum consists of eigenvalues ζ_3^{-1} and ζ_3; if 3 does not divide n then their multiplicities are $[n/3]$ and $[2n/3]$ respectively [17].

Let $J(C_{f,3})$ be the jacobian of $C_{f,3}$; it is an abelian variety, whose dimension equals $g(C_{f,3})$. We write $\mathrm{End}(J(C_{f,3}))$ for the ring of endomorphisms of $J(C_{f,3})$. By Albanese functoriality, δ_3 induces an automorphism of $J(C_{f,3})$ which we still denote by δ_3; it is known ([11], p. 149, [14], p. 448) that $\delta_3^2 + \delta_3 + 1 = 0$ in $\mathrm{End}(J(C_{f,3})$. This gives us an embedding

$$\mathbb{Z}[\zeta_3] \cong \mathbb{Z}[\delta_3] \subset \mathrm{End}(J(C_{f,3})), \ \zeta_3 \mapsto \delta_3$$

([7, p. 149], [14], [9, p. 448]).

If $f(x)$ is an odd polynomial of odd degree n then $C_{f,3}$ admits the involution

$$\delta_2 : C_{f,3} \to C_{f,3}, (x, y) \mapsto (-x, -y),$$

which commutes with δ_3. (It has exactly two fixed points if n is not divisible by 3.) By Albanese functoriality, δ_2 induces an automorphism of $J(C_{f,3})$ which we still denote by δ_2 and which (still) commutes with the automorphism δ_3 of $J(C_{f,3})$. We have $\delta_2^2 = 1$ in $\mathrm{End}(J(C_{f,3}))$.

Let K be a subfield of $\mathbb{C}$ that contains $\sqrt{-3}$ and all coefficients of $f(x)$, i.e.,

$$f(x) \subset K[x] \subset \mathbb{C}[x].$$

Let $\mathfrak{R}_f \subset \mathbb{C}$ be the set of roots of $f(x)$ and $K(\mathfrak{R}_f)$ the splitting field of $f(x)$ over K. Clearly, $K(\mathfrak{R}_f)$ is a finite Galois extension of K. We write $\mathrm{Gal}(f)$ for the (finite) Galois group $\mathrm{Gal}(K(\mathfrak{R}_f)/K)$. One may view $\mathrm{Gal}(f)$ as a certain permutation subgroup of the group $\mathrm{Perm}(\mathfrak{R}_f)$ of permutations of $\mathfrak{R}_f$. If we (choose an order on $\mathfrak{R}_f$, i.e.,) denote the roots of $f(x)$ by $\{\alpha_1, \dots, \alpha_n\}$ then we get a group isomorphism between $\mathrm{Perm}(\mathfrak{R}_f)$ and the full symmetric group $\mathbf{S}_n$ and $\mathrm{Gal}(f)$ becomes a certain subgroup of $\mathbf{S}_n$.

It is proven in [16, 19] that if $\mathrm{Gal}(f) = \mathbf{S}_n$ then

$$\mathrm{End}(J(C_{f,3})) = \mathbb{Z}[\delta_3] \cong \mathbb{Z}[\zeta_3].$$

In particular, this allowed us to construct explicitly g-dimensional principally polarized abelian varieties with endomorphism ring $\mathbb{Z}[\zeta_3]$ for all $g \ge 3$ under an assumption that 3 does not divide $g-2$: for example, if $f(x) = x^{g+1} - x - 1$ then $J(C_{f,3})$ is a g-dimensional principally polarized abelian variety with $\mathrm{End}(J(C_{f,3})) = \mathbb{Z}[\zeta_3]$. (It is known [10, p. 42] that the Galois group of the polynomial $x^n - x - 1$ over $\mathbb{Q}$ is $\mathbf{S}_n$ for all positive integers n.)

The aim of this paper is to provide an *explicit* construction of m-dimensional principally polarized abelian varieties, whose endomorphism ring is $\mathbb{Z}[\zeta_3]$ and $m \ge 5$ is an odd integer that is congruent to 2 modulo 3. We construct those abelian varieties (using odd $f(x)$ of degree $n = 2m+1$) as the anti-invariant part of $J(C_{f,3})$ (Prym variety) with respect to δ_2, assuming that $\mathrm{Gal}(f)$ coincides with the Weyl group $\mathbb{W}(\mathbb{D}_m)$ of the root system $\mathbb{D}_m$ in the following sense. Since $f(x)$ is odd and without multiple roots, there exist m distinct non-zero roots $\{\beta_1, \dots, \beta_m\}$ of $f(x)$ such that ($\beta_i \ne \pm\beta_j$ if $i \ne j$ and) $\mathfrak{R}_f$ coincides with the set $\{0\} \cup \{\pm\beta_1, \dots, \pm\beta_m\} \subset \bar{K}$. Then $\mathbb{W}(\mathbb{D}_m)$ may be defined as the group of permutations of $\mathfrak{R}_f$ of the form

$$0 \mapsto 0, \ \beta_i \mapsto \epsilon_i \beta_{s(i)}, \ -\beta_i \mapsto -\epsilon_i \beta_{s(i)}$$

where $s \in \mathbf{S}_m$ is an arbitrary permutation on m letters and signs $\epsilon_i = \pm 1$ satisfy the condition $\prod_{i=1}^m \epsilon_i = 1$. Let us consider the m-dimensional $\mathbb{F}_3$-vector space of *odd* functions

$$V_f^- := \{\phi : \mathfrak{R}_f \to \mathbb{F}_3 \mid \phi(-\alpha) = -\phi(\alpha) \ \forall \alpha \in \mathfrak{R}_f\}$$

provided with the natural structure of Galois module.

Our main result is the following statement.

Theorem 1.1. *Suppose that k is a nonnegative integer and $m = 6k+5 \ge 5$. Suppose that $n = 2m+1 = 12k+11$ and $f(x)$ is an odd polynomial of degree n without multiple roots. Then:*

(i) (1) (A) *$P(C_{f,3}) := (1-\delta_2)J(C_{f,3})$ is an m-dimensional δ_3-invariant abelian subvariety in $J(C_{f,3})$. In particular, the embedding $\mathbb{Z}[\delta_3] \subset \mathrm{End}(J(C_{f,3}))$ induces the embedding*

$$\mathbb{Z}[\zeta_3] \cong \mathbb{Z}[\delta_3] \hookrightarrow \mathrm{End}(P(C_{f,3})).$$

(B) *If one restrict the canonical principal polarization on $J(C_{f,3})$ to $P(C_{f,3})$ then the induced polarization is twice a principal polarization on $P(C_{f,3})$ and this principal polarization is δ_3-invariant.*

(C) *The principally polarized abelian variety $P(C_{f,3})$ is not isomorphic to the canonically polarized jacobian of a smooth projective curve.*

(2) *By functoriality, δ_3 induces the linear operator*

$$\delta_{3,P}^* : \Omega^1(P(C_{f,3})) \to \Omega^1(P(C_{f,3}))$$

in the space of differentials of the first kind on $P(C_{f,3})$. Its spectrum consists of eigenvalues ζ_3^{-1} of multiplicity $2k+1$ and ζ_3 of multiplicity $4k+4$.

(ii) *Suppose that K is a subfield of $\mathbb{C}$ that contains $\sqrt{-3}$ and all coefficients of $f(x)$. Then:*

(a) *The abelian variety $P(C_{f,3})$ and its automorphism δ_3 are defined over K. In addition, the Galois submodule $P(C_{f,3})^{\delta_3}$ of δ_3-invariants of $P(C_{f,3})(\bar{K})$ is canonically isomorphic to V_f^-.*

(b) *Assume additionally that* $\mathrm{Gal}(f)$ *coincides with* $\mathbb{W}(\mathbb{D}_m)$. *Then:*

(b1) $\mathrm{End}(P(C_{f,3})) = \mathbb{Z}[\zeta_3]$. *In particular, $P(C_{f,3})$ is an absolutely simple abelian variety.*

(b2) *The abelian variety $P(C_{f,3})$ is isomorphic neither to the jacobian of a smooth projective curve nor to a product of jacobians of smooth projective curves (even if one ignore polarizations).*

Example 1.2. Let $m = 5$ and $f(x) := x(x^{10} - x^2 - 1)$. One may check (see Example 2.3 below) that the Galois group of $f(x)$ over $K = \mathbb{Q}(\sqrt{-3})$ is $\mathbb{W}(\mathbb{D}_5)$. It follows that

$$\mathrm{End}(P(C_{f,3})) = \mathbb{Z}[\zeta_3].$$

Remark 1.3. If $m = 5$ then the 5-dimensional Prym varieties $P(C_{f,3})$ appear as intermediate jacobians of certain cubic threefolds [3]. (See also [20].)

Remark 1.4. A complete list of those (generalized) Prym varieties that are isomorphic, as principally polarized abelian varieties, to jacobians of smooth projective curves or to products of them was given by V.V. Shokurov [13, 14]. In the course of the proof of Theorem 1.1(i)(1)(C)) we use a different approach based on the study of the action of the period 3 automorphism on the differentials of the first kind [20].

The paper is organized as follows. In Section 2 we discuss permutation modules related to Galois groups of odd polynomials. In Section 3 we study trigonal jacobians and prymians and prove the main result.

I am grateful to V.V. Shokurov for useful discussions. My special thanks go to Dr. Arsen Elkin, who did computations with MAGMA related to Example 2.3.

2. Galois groups of odd polynomials and permutation modules

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

2.1. Galois groups of odd polynomials. Let $n = 12k + 11$ be a positive integer that is congruent to 11 modulo 12, $f(x) \in K[x]$ a degree n *odd* polynomial *without multiple roots* and with *non-zero* constant term. Let us put $m = 6k+5$. Then there exist m distinct non-zero roots $\{\beta_1,\dots,\beta_m\}$ of $f(x)$ such that the n-element set $\mathfrak{R}_f$ of roots of $f(x)$ coincides with $\{0\}\cup\{\pm\beta_1,\dots,\pm\beta_m\}\subset \bar{K}$ of all roots of $f(x)$. Clearly, $\mathfrak{R}_f$ is Galois-stable. We write $\mathrm{Perm}(\mathfrak{R}_f)$ for the group of permutations of the n-element set $\mathfrak{R}_f$. Let $\mathrm{Gal}(f)$ be the image of $\mathrm{Gal}(K)$ in $\mathrm{Perm}(\mathfrak{R}_f)$. If $K(\mathfrak{R}_f)$ is the splitting field of $f(x)$ obtained by adjoining to K all elements of $\mathfrak{R}_f$ then $K(\mathfrak{R}_f)/K$ is a finite Galois extension and $\mathrm{Gal}(f)$ is canonically isomorphic to the Galois group $\mathrm{Gal}(K(\mathfrak{R}_f)/K)$. Let $\mathrm{Perm}_0(\mathfrak{R}_f)$ be the subgroup of $\mathrm{Perm}(\mathfrak{R}_f)$ that consists of all permutations of the form

$$0\mapsto 0,\ \beta_i\mapsto \epsilon_i\beta_{s(i)},\ -\beta_i\mapsto -\epsilon_i\beta_{s(i)}$$

where $s\in \mathbf{S}_m$ is an arbitrary permutation on m letters and $\epsilon_i=\pm 1$. Clearly,

$$\mathrm{Gal}(f)\subset \mathrm{Perm}_0(\mathfrak{R}_f)\subset \mathrm{Perm}(\mathfrak{R}_f).$$

We write $\mathbb{W}(\mathbb{D}_m)$ for the index 2 subgroup of $\mathrm{Perm}_0(\mathfrak{R}_f)$, whose elements are characterized by the condition $\prod_{i=1}^m \epsilon_i=1$. We have

$$\mathbb{W}(\mathbb{D}_m)\subset \mathrm{Perm}_0(\mathfrak{R}_f)\subset \mathrm{Perm}(\mathfrak{R}_f).$$

Since 0 is a simple root of $f(x)$ we have $f(x)=x\cdot h(x)$ where $h(x)$ is an *even* polynomial of even degree $2m$, whose set of roots $\mathfrak{R}_h$ is $\{\pm\beta_1,\dots,\pm\beta_m\}$; in particular, $h(0)\ne 0$.

Remark 2.2. Clearly, $(\prod_{i=1}^m \beta_i)^2=-h(0)$ (recall that m is odd). It follows that $\mathrm{Gal}(f)=\mathrm{Gal}(h)\subset \mathbb{W}(\mathbb{D}_m)$ if and only if $-h(0)$ is a square in K.

Example 2.3. Let

$$m=5, h(x)=x^{10}-x^2-1\in\mathbb{Q}[x], f(x)=x\cdot h(x)=x(x^{10}-x^2-1).$$

Since $1=-h(0)$ is a square in $\mathbb{Q}$, the Galois group $\mathrm{Gal}(h/\mathbb{Q})$ of $h(x)$ over $\mathbb{Q}$ is a subgroup of $\mathbb{W}(\mathbb{D}_5)$. Using Magma [1], one obtains that the order of $\mathrm{Gal}(h/\mathbb{Q})$ is $2^4\cdot 5!$. Since the order of $\mathbb{W}(\mathbb{D}_5)$ is also $2^4\cdot 5!$, we conclude that $\mathrm{Gal}(h/\mathbb{Q})=\mathbb{W}(\mathbb{D}_5)$. One may check that the derived (sub)group $G_1:=(\mathbb{W}(\mathbb{D}_5),\mathbb{W}(\mathbb{D}_5))$ is a *perfect* (normal) subgroup of index 2 in $W(\mathbb{D}_5)$. It follows that the splitting field $\mathbb{Q}(\mathfrak{R}_h)$ of $h(x)$ over $\mathbb{Q}$ contains exactly one quadratic subfield. In order to determine this subfield, notice that if $\{\pm\beta_1,\dots,\pm\beta_5\}$ is the set of roots of $h(x)=x^{10}-x^2-1$ then $\{\beta_1^2,\dots\beta_5^2\}$ is the set of roots of x^5-x-1. Using Magma [1], one obtains that the discriminant of x^5-x-1 is 19×151 and therefore $\mathbb{Q}(\mathfrak{R}_h)$ contains $\mathbb{Q}(\sqrt{19\times 151})$. It follows that $\mathbb{Q}(\mathfrak{R}_h)$ does *not* contain $K=\mathbb{Q}(\sqrt{-3})$ and therefore $\mathbb{Q}(\mathfrak{R}_h)$ and K are linearly disjoint over $\mathbb{Q}$. This implies that the Galois group of $h(x)$ over K also coincides with $\mathbb{W}(\mathbb{D}_5)$ and therefore the Galois group of $f(x)$ over K also coincides with $\mathbb{W}(\mathbb{D}_5)$.

Definition 2.4. Let $\mathrm{Perm}(\mathfrak{R}_h)$ be the group of permutations of the $2m$-element set $\mathfrak{R}_h$. Let $\mathcal{G}$ be a permutation subgroup in $\mathbf{S}_m$. We write $2^m\cdot\mathcal{G}\subset \mathrm{Perm}(\mathfrak{R}_h)$ for the subgroup of all permutations of the form

$$(s;\epsilon_1,\dots,\epsilon_m):\beta_i\mapsto \epsilon_i\beta_{s(i)},\ -\beta_i\mapsto -\epsilon_i\beta_{s(i)}$$

where

$$s\in\mathcal{G},\ \epsilon_i=\pm 1.$$

We write $2^{m-1}\cdot\mathcal{G}$ for the index two subgroup in $2^m\cdot\mathcal{G}$, whose elements are characterized by the condition $\prod_{i=1}^m\epsilon_i=1$.

Example 2.5.

(i) The group $2^m \cdot \{1\}$ coincides with the group of all permutations of the form

$$\beta_i \mapsto \epsilon_i \beta_i, \ -\beta_i \mapsto -\epsilon_i \beta_i$$

where $\epsilon_i = \pm 1$ while $2^{m-1} \cdot \{1\}$ corresponds to its index 2 subgroup, whose elements are characterized by the condition $\prod_{i=1}^m \epsilon_i = 1$. The groups $2^m \cdot \{1\}$ and $2^{m-1} \cdot \{1\}$ are exponent 2 commutative groups of order 2^m and 2^{m-1} respectively.

(ii) Let us identify $\mathrm{Perm}(\mathfrak{R}_h)$ with the stabilizer of 0 in $\mathrm{Perm}(\mathfrak{R}_f)$. Then $2^m \cdot \mathbf{S}_m$ coincides with $\mathrm{Perm}_0(\mathfrak{R}_f)$ and $2^{m-1} \cdot \mathbf{S}_m$ coincides with $\mathbb{W}(\mathbb{D}_m)$.

Remark 2.6. Clearly, the natural map $(s; \epsilon_1, \dots, \epsilon_m) \mapsto s$ give rise to the surjective group homomorphisms

$$\kappa_h^0 : 2^m \cdot \mathcal{G} \twoheadrightarrow \mathcal{G}, \ \kappa_h : 2^{m-1} \cdot \mathcal{G} \twoheadrightarrow \mathcal{G},$$

whose kernels are $2^m \cdot \{1\}$ and $2^{m-1} \cdot \{1\}$ respectively.

Remarks 2.7. Suppose that there exists a permutation group $\mathcal{G} \subset \mathbf{S}_m$ such that $\mathrm{Gal}(h) = 2^{m-1} \cdot \mathcal{G}$. Then:

(i) The kernel of the surjective group homomorphism $\kappa_h : \mathrm{Gal}(h) = 2^{m-1} \cdot \mathcal{G} \twoheadrightarrow \mathcal{G}$ is the commutative (normal sub)group $2^{m-1} \cdot \{1\}$ of exponent 2.

(ii) Let G_1 be a *normal* subgroup in $\mathrm{Gal}(h)$ of *odd* index say, r. Then G_1 contains $2^{m-1} \cdot \{1\}$ and the surjectivity of κ_h implies that

$$\kappa_h(G_1) \cong G_1/(2^{m-1} \cdot \{1\})$$

is a normal subgroup of index r in $\mathcal{G}$. This implies that if $\mathcal{G}$ does not contain a normal subgroup of odd index (except $\mathcal{G}$ itself) then $\mathrm{Gal}(h)$ also does not contain a normal subgroup of odd index (except $\mathrm{Gal}(h)$ itself).

(iii) (1) If $\mathcal{G}$ is a transitive subgroup of $\mathbf{S}_m$ then $2^{m-1} \cdot \mathcal{G}$ is a transitive subgroup of $\mathrm{Perm}(\mathfrak{R}_h)$. This means that $\mathrm{Gal}(h)$ is a transitive subgroup of $\mathrm{Perm}(\mathfrak{R}_h)$, i.e., $h(x)$ is irreducible over K.

(2) Suppose that $\mathcal{G}$ is a doubly transitive subgroup of $\mathbf{S}_m$ and let $\mathcal{G}_1$ is the stabilizer of 1 in $\mathcal{G}$. Then $\mathcal{G}_1$ has exactly two orbits in $\{1, \dots, m\}$: namely, $\{1\}$ and the rest. Let $\mathrm{Gal}(h)_1$ be the stabilizer of β_1 in $\mathrm{Gal}(h)$. Then one may easily check that $\mathrm{Gal}(h)_1$ has exactly 3 orbits in $\mathfrak{R}_h$: namely, $\{\beta_1\}$, $\{-\beta_1\}$ and the rest.

2.8. Permutation modules. Let V_f be the $2m$-dimensional $\mathbb{F}_3$-vector space of functions

$$\phi : \mathfrak{R}_f \to \mathbb{F}_3, \ \sum_{\alpha \in \mathfrak{R}_f} \phi(\alpha) = 0.$$

The space V_f carries the natural structure of Galois module induced by the Galois action on $\mathfrak{R}_f$.

Let $\mathbb{F}_3^{\mathfrak{R}_h}$ be the $2m$-dimensional $\mathbb{F}_3$-vector space of all functions $\phi : \mathfrak{R}_h \to \mathbb{F}_3$. It carries the natural structure of Galois module. We write $1_{\mathfrak{R}_h}$ for the (Galois-invariant) constant function 1.

The map that assigns to a $\mathbb{F}_3$-valued function on $\mathfrak{R}_f$ its restriction to $\mathfrak{R}_h$ gives rise to the isomorphism $V_f \to \mathbb{F}_3^{\mathfrak{R}_h}$ of Galois modules. (One may extend a function ϕ on $\mathfrak{R}_h$ to $\mathfrak{R}_f = \{0\} \cup \mathfrak{R}_h$ by putting

$$\phi(0) := -\sum_{\alpha \in \mathfrak{R}_h} \phi(\alpha).)$$

The Galois module V_f splits into a direct sum of the Galois submodules of odd and even functions

$$V_f = V_f^- \oplus V_f^+$$

where

$$V_f^+ = \{\phi : \mathfrak{R}_f \to \mathbb{F}_3, \sum_{\alpha\in\mathfrak{R}_f} \phi(\alpha) = 0,\ \phi(\alpha) = \phi(-\alpha)\ \forall\alpha\},$$

$$V_f^- = \{\phi : \mathfrak{R}_f \to \mathbb{F}_3,\ \phi(\alpha) = -\phi(\alpha)\ \forall\alpha\}.$$

(The sum of values of an odd function is always zero.) Clearly, $\phi(0) = 0$ for all $\phi \in V_f^-$. It follows that

$$\dim_{\mathbb{F}_3}(V_f^-) = m.$$

Lemma 2.9. *Suppose that there exists a doubly transitive permutation group* $\mathcal{G} \subset \mathbf{S}_m$ *such that* $\mathrm{Gal}(h) = 2^{m-1} \cdot \mathcal{G}$. *Then* $\mathrm{End}_{\mathrm{Gal}(K)}(V_f^-) = \mathbb{F}_3$.

Proof. By Remark 2.7(iii)(1), $\mathrm{Gal}(h)$ acts transitively on $\mathfrak{R}_h$.

Let W_h^+ and W_h^- be the subspaces of even and odd functions respectively in $\mathbb{F}_3^{\mathfrak{R}_h}$. Clearly, they both are Galois submodules in $\mathbb{F}_3^{\mathfrak{R}_h}$ and

$$W_h^- \oplus W_h^+ = \mathbb{F}_3^{\mathfrak{R}_h}.$$

It is also clear that the Galois modules W_h^- and V_f^- are isomorphic. So, it suffices to check that

$$\mathrm{End}_{\mathrm{Gal}(K)}(W_h^-) = \mathbb{F}_3.$$

In order to do that, notice that $\#(\mathfrak{R}_h) = 2m = n - 1 = 12k + 10$ is *not* divisible by 3. This implies that the submodule $\mathbb{F}_3 \cdot 1_{\mathfrak{R}_h}$ of constant functions is a direct summand of W_h^+ and $\mathbb{F}_3^{\mathfrak{R}_h}$ splits into a direct sum of Galois modules

$$\mathbb{F}_3^{\mathfrak{R}_h} = W_h^- \oplus W_h^+ = W_h^- \oplus \mathbb{F}_3 \cdot 1_{\mathfrak{R}_h} \oplus W_h^{+,0}$$

where $W_h^{+,0}$ is the Galois (sub)module of even functions, whose sum of values is zero. Clearly,

$$\dim_{\mathbb{F}_3}\mathrm{End}_{\mathrm{Gal}(K)}(\mathbb{F}_3^{\mathfrak{R}_h}) \geq$$
$$\dim_{\mathbb{F}_3}\mathrm{End}_{\mathrm{Gal}(K)}(W_h^-) + \dim_{\mathbb{F}_3}\mathrm{End}_{\mathrm{Gal}(K)}(\mathbb{F}_3 \cdot 1_{\mathfrak{R}_h}) + \dim_{\mathbb{F}_3}\mathrm{End}_{\mathrm{Gal}(K)}(W_h^{+,0}) \geq$$
$$\dim_{\mathbb{F}_3}\mathrm{End}_{\mathrm{Gal}(K)}(W_h^-) + 1 + 1.$$

So, if we prove that $\dim_{\mathbb{F}_3}\mathrm{End}_{\mathrm{Gal}(K)}(\mathbb{F}_3^{\mathfrak{R}_h}) = 3$ then we are done. Since the image of $\mathrm{Gal}(K)$ in $\mathrm{Aut}_{\mathbb{F}_3}(\mathbb{F}_3^{\mathfrak{R}_h})$ coincides with

$$\mathrm{Gal}(h) \subset \mathrm{Perm}(\mathfrak{R}_h) \subset \mathrm{Aut}_{\mathbb{F}_3}(\mathbb{F}_3^{\mathfrak{R}_h}),$$

we have

$$\mathrm{End}_{\mathrm{Gal}(K)}(\mathbb{F}_3^{\mathfrak{R}_h}) = \mathrm{End}_{\mathrm{Gal}(h)}(\mathbb{F}_3^{\mathfrak{R}_h}).$$

So, in order to prove the Lemma, it suffices to check that

$$\dim_{\mathbb{F}_3}(\mathrm{End}_{\mathrm{Gal}(h)}(\mathbb{F}_3^{\mathfrak{R}_h})) = 3.$$

By Lemma 7.1 of [6], $\dim_{\mathbb{F}_3}(\mathrm{End}_{\mathrm{Gal}(h)}(\mathbb{F}_3^{\mathfrak{R}_h}))$ coincides with the number of orbits in $\mathfrak{R}_h$ of the stabilizer in $\mathrm{Gal}(h)$ of any root of $h(x)$. But the number of orbits is 3 (see Remark 2.7(iii)). This ends the proof. □

3. Cyclic covers, jacobians and prymians

If X is an abelian variety over $\bar{K}$ then we write $\mathrm{End}(X)$ for the ring of its $\bar{K}$-endomorphisms and $\mathrm{End}^0(X)$ for the corresponding $\mathbb{Q}$-algebra $\mathrm{End}(X)\otimes\mathbb{Q}$. If X is defined over K then we write $\mathrm{End}_K(X)$ for the ring of its K-endomorphisms.

As above $f(x) = x\cdot h(x)\in K[x]$ is an odd polynomial of degree $n = 2m+1 = 12k+11$ without multiple roots. We keep all the notation of the previous Section.

3.1. Trigonal curves. Hereafter we assume that K contains $\sqrt{-3}$. Let us consider (the smooth projective model of) the trigonal curve

$$C_{f,3} : y^3 = f(x)$$

of genus $n-1 = 12k+10$. The curve $C_{f,3}$ admits commuting periodic automorphisms

$$\delta_2 : (x, y)\mapsto(-x,-y)$$

and

$$\delta_3 : (x, y)\mapsto(x, \gamma y)$$

of period 2 and 3 respectively.

The regular map of curves

$$\pi : C_{f,3}\to\mathbb{P}^1,\ (x, y)\mapsto x$$

has degree 3 and ramifies exactly at 0, the $2m$-element set set $\{\alpha\mid\alpha\in\mathfrak{R}_f\}$ and ∞. (Notice that 3 does *not* divide $2m+1$.) Clearly, all branch points of π in $C_{f,3}$ are δ_3-invariant. By abuse of notation, we denote $\pi^{-1}(\infty)$ by ∞. Let us put

$$B = \pi^{-1}(\mathfrak{R}_f) = \{(\alpha, 0)\mid\alpha\in\mathfrak{R}_f\}\subset C(\bar{K}).$$

Clearly, all elements of B are δ_3-invariant. On the other hand, if $P = (\alpha, 0)\in B$ then $\delta_2(P) = (-\alpha, 0)\in B$.

The automorphism $\delta_2 : C_{f,3}\to C_{f,3}$ has exactly two fixed points, namely, $\pi^{-1}(0)$ and $\pi^{-1}(\infty)$. One may easily check that the quotient $\tilde{C}_{f,3} = C_{f,3}/(1,\delta_2)$ is a smooth (irreducible) projective curve (compare with Lemma 1.2, its proof and Corollary 1.3 in [20]) and $C_{f,3}\to\tilde{C}_{f,3}$ is a double covering that is ramified at exactly two points, namely the images of $\pi^{-1}(0)$ and $\pi^{-1}(\infty)$. The Hurwitz formula implies that the genus of $\tilde{C}_{f,3}$ is m.

Since

$$[n/3] = 4k+3,\ [2n/3] = 8k+7,$$

it follows from ([16], [17, Remarks 3.5 and 3.7]) that the $(n-1)$-dimensional $\bar{K}$-vector space $\Omega^1(C_{f,3})$ of differentials of the first kind on $C_{f,3}$ has a basis

$$\left\{x^i\frac{dx}{y},\ 0\le i\le 4k+2;\ x^j\frac{dx}{y^2},\ 0\le j\le 8k+6\right\}.$$

If

$$\delta_2^* : \Omega^1(C_{f,3})\to\Omega^1(C_{f,3}),\ \delta_3^* : \Omega^1(C_{f,3})\to\Omega^1(C_{f,3})$$

are the automorphisms induced by δ_2 and δ_3 respectively then

$$\delta_3^*(x^i\frac{dx}{y}) = \gamma^{-1}x^i\frac{dx}{y},\ \delta_3^*(x^j\frac{dx}{y^2}) = \gamma^{-2}x^j\frac{dx}{y^2} = \gamma x^j\frac{dx}{y^2},$$

$$\delta_2^*(x^i\frac{dx}{y}) = (-1)^i x^i\frac{dx}{y},\ \delta_2^*(x^j\frac{dx}{y^2}) = (-1)^{j+1}x^j\frac{dx}{y^2};$$

in particular, the basis consists of eigenvectors with respect to δ_2^* and δ_3^*. It follows that the subspace $\Omega^1(C_{f,3})^-$ of δ_2-anti-invariants is m-dimensional and admits a basis

$$\left\{x^{2i+1}\frac{dx}{y},\ 0 \le i \le 2k;\ x^{2j}\frac{dx}{y^2}\ 0 \le j \le 4k+3\right\}.$$

3.2. Trigonal jacobians. Let $J(C_{f,3})$ be the jacobian of $C_{f,3}$: it is a $(n-1)$-dimensional abelian variety that is defined over K. By Albanese functoriality, δ_2 and δ_3 induce the K-automorphisms of $J(C_{f,3})$ that we still denote by δ_2 and δ_3 respectively. We have

$$\delta_2^2 = 1,\ \delta_3^2 + \delta_3 + 1 = 0$$

where all the equalities hold in $\mathrm{End}(J(C_{f,3}))$. The latter equality gives rise to the embedding

$$\mathbb{Z}[\zeta_3] \hookrightarrow \mathrm{End}_K(J(C_{f,3})),\ \zeta_3 \mapsto \delta_3$$

of the cyclotomic ring $\mathbb{Z}[\mu_3]$ into the ring of K-endomorphisms of $J(C_{f,3})$.

Let $j : C_{f,3} \hookrightarrow J(C_{f,3})$ be canonical embedding of $C_{f,3}$ into its jacobian normalized by the condition $j(\infty) = 0$, i.e., j sends a point $P \in C_{f,3}(\bar{K})$ to the linear equivalence class of the divisor $(P) - (\infty)$. Clearly, j is δ_3-equivariant and δ_2-equivariant.

Let me remind the description of the Galois (sub)module $J(C_{f,3})^{\delta_3}$ of δ_3-invariants in $J(C_{f,3})(\bar{K})$. The Galois modules V_f and $J(C_{f,3})^{\delta_3}$ are canonically isomorphic [9] (see also [18]). Namely, let

$$\mathbb{Z}_B^0 = \{\sum_{P\in B} a_P(P) \mid a_P \in \mathbb{Z},\ \sum_{P\in B} a_P = 0\}$$

be the group of degree zero divisors on $C_{f,3}$ with support in B. The free commutative group $\mathbb{Z}_B^0$ carries the natural structure of Galois module. Clearly, the Galois module $\mathbb{Z}_B^0/3\mathbb{Z}_B^0$ is canonically isomorphic to V_f: a divisor $\sum_{P\in B} a_P(P)$ gives rise tho the function $\alpha \mapsto a_P \mod 3$ where $P = (\alpha, 0)$. Since B is δ_2-invariant, the map

$$D_2 : \sum_{P\in B} a_P(P) \mapsto \sum_{P\in B} a_P(\delta_2 P)$$

is an automorphism of of the Galois module $\mathbb{Z}_B^0$ that induces the automorphism of $\mathbb{Z}_B^0/3\mathbb{Z}_B^0 = V_f$ that sends a function $\alpha \to \phi(\alpha)$ to the function $\alpha \to \phi(-\alpha)$. (We still denote this automorphism of V_f by D_2.) Notice that

$$V_f^- = (1 - D_2)V_f,\ V_f^+ = (1 + D_2)V_f$$

(recall that V_f is the $\mathbb{F}_3$-vector space.) In other words, V_f^+ and V_f^- are eigenspaces of D_2 that correspond to eigenvalues 1 and -1 respectively.

Let us consider the natural map

$$\mathrm{cl} : \mathbb{Z}_B^0 \to J(C_{f,3})(\bar{K})$$

that sends a divisor $\sum_{P\in B} a_P(P)$ to (its linear equivalence class, i.e., to)

$$\sum_{P\in B} a_P j(P) \in J(C_{f,3})(\bar{K}).$$

It turns out that $\mathrm{cl}(\mathbb{Z}_B^0) = J(C_{f,3})^{\delta_3}$ and the kernel of cl coincides with $3 \cdot \mathbb{Z}_B^0$. This gives rise to the natural isomorphism of Galois module $\mathbb{Z}_B^0/3\mathbb{Z}_B^0$ and $J(C_{f,3})^{\delta_3}$ and we get the natural isomorphisms of Galois modules

$$\overline{\mathrm{cl}}: V_f = \mathbb{Z}_B^0/3\mathbb{Z}_B^0 \cong J(C_{f,3})^{\delta_3}.$$

Since δ_2 commutes with δ_3, the Galois submodule $J(C_{f,3})^{\delta_3}$ is δ_2-invariant. It follows from the explicit description of cl and D_2 that if $\overline{\mathrm{cl}}(\phi) = P \in J(C_{f,3})^{\delta_3}$ then $\delta_2 P$ is the image (under $\overline{\mathrm{cl}}$) of the function $\alpha \to \phi(-\alpha)$. In other words,

$$\overline{\mathrm{cl}}(D_2\phi) = \delta_2\overline{\mathrm{cl}}(\phi)\ \forall \phi \in V_f.$$

It follows that the restriction of $\overline{\mathrm{cl}}$ to V_f^- gives us the isomorphism of Galois modules

$$\overline{\mathrm{cl}}: V_f^- \cong \{P \in J(C_{f,3})^{\delta_3} \mid \delta_2 P = -P\}.$$

This implies that

$$\{P \in J(C_{f,3})^{\delta_3} \mid \delta_2 P = -P\} = \overline{\mathrm{cl}}(V_f^-) = \overline{\mathrm{cl}}((1-D_2)V_f) = (1-\delta_2)J(C_{f,3})^{\delta_3}.$$

3.3. Trigonal prymians. Let us consider the Prym variety

$$P(C_{f,3}) = (1-\delta_2)J(C_{f,3}) \subset J(C_{f,3}).$$

If one restrict the canonical principal polarization on $J(C_{f,3})$ to $P(C_{f,3})$ then the induced polarization is twice a principal polarization on $P(C_{f,3})$ [4, Sect. 3, Cor. 2]. Obviously, the principal polarization on $P(C_{f,3})$ is δ_3-invariant. It is also clear [4, Sect. 3, Cor. 2] that $P(C_{f,3})$ coincides with the identity component of the surjective map of jacobians $J(C_{f,3}) \to J(\tilde{C}_{f,3})$; in particular, it is a m-dimensional abelian variety that is defined over K. Clearly, the abelian subvariety $P(C_{f,3})$ is δ_3-invariant. Therefore we may and will consider δ_3 as the K-automorphism of $P(C_{f,3})$. Still $\delta_3^2+\delta_3+1=0$ in $\mathrm{End}(P(C_{f,3}))$. As above, this induces an embedding

$$\mathbb{Z}[\zeta_3] \hookrightarrow \mathrm{End}(P(C_{f,3})),\ \zeta_3 \mapsto \delta_3.$$

On the other hand, $1+\delta_2$ kills $P(C_{f,3})$, because

$$0 = 1-\delta_2^2 = (1+\delta_2)(1-\delta_2) \in \mathrm{End}(J(C_{f,3}))$$

and $P(C_{f,3})(\bar{K}) = (1-\delta_2)(J(C_{f,3}))$. This implies that

$$\delta_2 P = -P\ \forall P \in P(C_{f,3})(\bar{K}).$$

Let us consider the Galois (sub)module $P(C_{f,3})^{\delta_3}$ of δ_3-invariants in $P(C_{f,3})(\bar{K})$. Clearly,

$$P(C_{f,3})^{\delta_3} \subset \{P \in J(C_{f,3})^{\delta_3} \mid \delta_2 P = -P\}.$$

Since the latter group coincides with $(1-\delta_2)J(C_{f,3})^{\delta_3}$, we conclude that

$$P(C_{f,3})^{\delta_3} = \{P \in J(C_{f,3})^{\delta_3} \mid \delta_2 P = -P\}.$$

It follows that the Galois modules $P(C_{f,3})^{\delta_3}$ and V_f^- are canonically isomorphic.

Let us put

$$\mathcal{O} = \mathbb{Z}[\mu_3],\ \lambda = (1-\gamma)\mathcal{O},\ E = \mathcal{O}\otimes\mathbb{Q} = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}).$$

Then the residue field

$$\mathcal{O}/\lambda = \mathbb{F}_3.$$

Recall that we have the natural homomorphism

$$\mathcal{O} = \mathbb{Z}[\mu_3] \hookrightarrow \mathrm{End}_K(P(C_{f,3})), \zeta_3 \mapsto \delta_3.$$

This implies that

$$P(C_{f,3})^{\delta_3} = P(C_{f,3})_\lambda$$

and therefore the Galois modules $P(C_{f,3})_\lambda$ and V_f^- are canonically isomorphic. In particular,

$$\dim_{\mathbb{F}_3} P(C_{f,3})_\lambda = m.$$

On the other hand, it is well known [12, 8, 19] that $P(C_{f,3})_\lambda$ is a free $\mathcal{O}/\lambda$-module of rank $2\dim(P(C_{f,3}))/[E:\mathbb{Q}]$. Since $\mathcal{O}/\lambda = \mathbb{F}_3$ and $[E:\mathbb{Q}] = 2$, we get another proof of the equality $\dim(P(C_{f,3})) = m$. Notice that

$$\dim(P(C_{f,3})) = m = \dim_{\mathbb{F}_3}(\Omega^1(C_{f,3})^-).$$

Remark 3.4. Taking into account that $\dim(P(C_{f,3})) = m$ and applying Theorem 3.10 of [18] to

$$Y = J(C_{f,3}), Z = P(C_{f,3}), \delta = \delta_2, P(t) = 1 - t,$$

we obtain that $1 - \delta_2 : J(C_{f,3}) \twoheadrightarrow P(C_{f,3}) \subset J(C_{f,3})$ induces (on differentials of the first kind) an isomorphism

$$(1-\delta_2)^* : \Omega^1(P(C_{f,3})) \cong \Omega^1(C_{f,3})^- \subset \Omega^1(J(C_{f,3}))$$

and this isomorphism is δ_3-equivariant. It follows easily that δ_3 induces a linear operator in $\Omega^1(P(C_{f,3}))$, whose spectrum consists of eigenvalues γ^{-1} of multiplicity $2k+1$ and $\gamma = \gamma^{-2}$ of multiplicity $4k+4$. Clearly, the numbers $2k+1$ and $4k+4$ are relatively prime.

Theorem 3.5. *Assume that there exists a doubly transitive permutation group $\mathcal{G} \subset \mathbf{S}_m$ that enjoys the following properties:*

(i) *$\mathcal{G}$ does not contain a normal subgroup, whose index divides m (except $\mathcal{G}$ itself).*

(ii) $\mathrm{Gal}(h)$ *contains* $2^{m-1} \cdot \mathcal{G}$.

Then $\mathrm{End}(P(C_{f,3})) = \mathbb{Z}[\zeta_3]$. *In particular, $P(C_{f,3})$ is an absolutely simple abelian variety.*

Proof. Enlarging K if necessary, we may and will assume that $\mathrm{Gal}(h) = 2^{m-1} \cdot \mathcal{G}$. Identifying $\mathrm{Perm}(\mathfrak{R}_h)$ with the stabilizer of 0 in $\mathrm{Perm}(\mathfrak{R}_f)$, we obtain that

$$\mathrm{Gal}(f) = \mathrm{Gal}(h) = 2^{m-1} \cdot \mathcal{G}.$$

Since the Galois modules $P(C_{f,3})_\lambda$ and V_f^- are isomorphic, it follows from Lemma 2.9 that $\mathrm{End}_{\mathrm{Gal}(K)}(P(C_{f,3})_\lambda)^{\delta_3}) = \mathbb{F}_3$. Now Theorem 3.5 follows from Remark 3.4 and Theorem 3.12(ii)(2) of [19] applied to $X = P(C_{f,3}), E = \mathbb{Q}(\sqrt{-3}), \mathcal{O} = \mathbb{Z}[\mu_3], \lambda = (1-\gamma)\mathcal{O}$. □

Example 3.6. Let $m = 6k+5$ be a positive integer that is congruent to 5 modulo 6. Let L be the field of rational functions $\mathbb{C}(t_1, \dots, t_m)$ in m independent variables $t_1, \dots, t_m$ over $\mathbb{C}$. One may realized $2^m \cdot \mathbf{S}_m$ as the following group of (linear) automorphisms of L:

$$(s; \epsilon_1, \dots, \epsilon_m) : t_i \mapsto \epsilon_i t_{s(i)}, \ i = 1, \dots m$$

where

$$s \in \mathbf{S}_m, \ \epsilon_i = \pm 1.$$

Let K be the subfield of $2^m \cdot \mathbf{S}_m$-invariants in L. Clearly, L/K is a finite Galois extension with Galois group $2^m \cdot \mathbf{S}_m$. In particular, $\bar{L} = \bar{K}$. Since $m \geq 5$, the only normal subgroups in $\mathbf{S}_m$ are the subgroup $\{1\}$ of even index $m!$, the alternating (sub)group $\mathbf{A}_m$ of index 2 and $\mathbf{S}_m$ itself.

The even degree $2m$ polynomial

$$h(x) = \prod_{i=1}^{m}(x^2 - t_i^2) = \prod_{i=1}^{m}(x - t_i)\prod_{i=1}^{m}(x + t_i)$$

lies in $K[x]$ and its splitting field coincides with L. It follows that $\mathrm{Gal}(h) = 2^m \cdot \mathbf{S}_m$. Applying Theorem 3.5 to the odd degree $(2m+1)$ polynomial

$$f(x) := x \cdot h(x) = x \cdot \prod_{i=1}^{m}(x^2 - t_i^2),$$

we conclude that the endomorphism ring (over $\bar{L}$) of the m-dimensional prymian $P(C_{f,3})$ coincides with $\mathbb{Z}[\zeta_3]$.

Proof of Theorem 1.1. The assertions (i) (except (i)(1)(C)) and (ii)(a) are already proven in Subsection 3.3 and Remark 3.4. Since $\mathbf{S}_m$ is the doubly transitive permutation group that does not contain normal subgroups of odd index (except $\mathbf{S}_m$ itself) and $\mathbb{W}(\mathbb{D}_m) = 2^{m-1} \cdot \mathbf{S}_m$, the assertion (ii)(b1) follows from Theorem 3.5 applied to $\mathcal{G} = \mathbf{S}_m$.

In order to prove the assertion (i)(1)(C), notice that

$$3\cdot \mid (2k+1) - (4k+4) \mid = 6k + 9 > (6K+5) + 2 = m + 2 = \dim(P(C_{f,3})) + 2.$$

Now the assertion i)(1)(C follows from the assertion (i)(2) combined with the Theorem 1.1 of [20].

In order to prove the assertion (ii)(b2), notice that we already know (thanks to the assertion (ii)(b1)) that $\mathrm{End}(P(C_{f,3})) = \mathbb{Z}[\delta_3] \cong \mathbb{Z}[\zeta_3]$. This implies that $P(C_{f,3})$ is absolutely simple and has exactly one principal polarization, which is δ_3-invariant. So, if $P(C_{f,3})$ is isomorphic to the jacobian of a smooth curve then this isomorphism does respect the principal polarizations. Now the assertion (ii)(b2) follows from the assertion (i)(1)(C).

□

References

[1] W. Bosma, J. Cannon, C. Playoust, *The Magma Algebra System I: The User Language.* J. Symb. Comp. **24** (1997), 235–265; http://magma.maths.usyd.edu.au/magma/ .

[2] J. K. Koo, *On holomorphic differentials of some algebraic function field of one variable over C.* Bull. Austral. Math. Soc. **43** (1991), 399-405.

[3] K. Matsumoto, T. Terasoma, *Theta constants associated to cubic threefolds.* J. Algebraic Geom. **12** (2003), 741–775.

[4] D. Mumford, *Prym varieties* I. In: Contributions to Analysis, pp. 325–350. Academic Press 1974.

[5] Oort, F. *Endomorphism algebras of abelian varieties.* In: Algebraic geometry and commutative algebra, Vol. II, 469–502, Kinokuniya, Tokyo, 1988.

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

[7] B. Poonen, E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line.* J. reine angew. Math. **488** (1997), 141-188.

[8] Ribet, K.: Galois action on division points of Abelian varieties with real multiplications. Amer. J. Math. **98**, 751–804 (1976)

[9] E. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve.* Math. Ann. **310** (1998), 447–471; Erratum, Math. Ann. **339** (2007), 1.

[10] J.-P. Serre, Topics in Galois Theory. Jones and Bartlett Publishers, Boston-London (1992).

[11] Shimura, G. *On analytic families of polarized abelian varieties and automorphic functions.* Ann. of Math. (2) 78 1963 149–192.

[12] Shimura, G., Introduction to the arithmetic theory of automorphic functions. Princeton University Press, Princeton (1971).

[13] Shokurov, V. V., *Distinguishing Prymians from Jacobians*. Invent. Math. **65** (1981/82), no. 2, 209–219.

[14] Shokurov, V. V., Prym varieties: theory and applications. Izv. Akad. Nauk SSSR Ser. Mat. **47** (1983), no. 4, 785–855; Math. USSR-Izv. 23 (1984), no. 1, 83–147.

[15] C. Towse, *Weierstrass points on cyclic covers of the projective line*. Trans. AMS **348** (1996), 3355-3377.

[16] Yu. G. Zarhin, *Cyclic covers, their jacobians and endomorphisms*. J. reine angew. Math. **544** (2002), 91–110.

[17] Yu. G. Zarhin, *The endomorphism rings of jacobians of cyclic covers of the projective line*. Math. Proc. Cambridge Philos. Soc. **136** (2004), 257–267.

[18] Yu. G. Zarhin, *Endomorphism algebras of superelliptic Jacobians*. In: Geometric methods in algebra and number theory (F. Bogomolov, Yu. Tschinkel, eds), 339–362, Progr. Math., 235, Birkhäuser Boston, Boston, MA, 2005.

[19] Yu. G. Zarhin, *Endomorphisms of superelliptic jacobians*. Math. Z., DOI: 10.1007/s00209-008-0342-5; Erratum, DOI: 10.1007/s00209-008-0377-7 .

[20] Yu. G. Zarhin, *Cubic surfaces and cubic threefolds, jacobians and intermediate jacobians*. In: Algebra, Arithmetic and Geometry (Manin Festschrift), Progress in Math., Birkhäuser, 2008, to appear; arXiv:math/0610138v3 [math.AG] .

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

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

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