Max-Planck-Institut für Mathematik Bonn

Eigenvalues of Frobenius endomorphism of abelian varieties

by

Yuri G. Zarhin

Max-Planck-Institut für Mathematik
Preprint Series 2013 (57)

Eigenvalues of Frobenius endomorphism of abelian varieties

Yuri G. Zarhin

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

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

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

MPIM 13-57

EIGENVALUES OF FROBENIUS ENDOMORPHISM OF ABELIAN VARIETIES

YURI G. ZARHIN

Abstract. In this paper we discuss multiplicative relations between eigenvalues of Frobenius endomorphism of abelian varieties of small dimension over finite fields.

1. Introduction

There was a growing interest recently, in the study of multiplicative relations between eigenvalues of Frobenius endomorphism Fr_X of an abelian varietiy X over a finite field k. e.g, see [2, 1]. That is why I decided to return to this topic after a rather long break. Our main tool, as in [14, 15, 16, 5, 17], is the multiplicative group $\Gamma(X,k)$ generated by the set of R_X of eigenvalues of Fr_X . Assuming that k is *sufficiently large* with respect to X, i.e., $\Gamma(X,k)$ does *not* contain *nontrivial* roots of unity, we say that X is *neat* (see [17, Sect. 3] and Sect. 2 below) if it enjoys the following property.

If $e: R_X \to \mathbb{Z}$ is an integer-valued function such that

$$\prod_{\alpha\in R_X} \left(q^{-1}\alpha^2\right)^{e(\alpha)} = 1$$

then $e(\alpha)=e(q/\alpha)$ for all $\alpha \in R_X$. Here q is the number of elements of k. (Recall that $\alpha \mapsto q/\alpha$ is a permutation of R_X.)

Our main result is the following statement.

Theorem 1.1. *Suppose that $1 \le \dim(X) \le 3$ and k is sufficiently large with respect to X. Then X is not neat if and only it enjoys all of the following three properties.*

(i) *X is abslolutely simple, all endomorphisms of X are defined over k and its endomorphism algebra $\mathrm{End}^0(X)$ is a sextic CM field that is generated by Fr_X.*

(ii) *$\mathrm{End}^0(X)$ contains an imaginary quadratic subfield B that enjoys the following property. If*

$$\mathrm{Norm}: \mathrm{End}^0(X) \to B$$

is the norm map corresponding to the cubic field extension $\mathrm{End}^0(X)/B$ then

$$\mathrm{Norm}\left(q^{-1}\mathrm{Fr}_X^2\right)=1.$$

(iii) *X is almost ordinary, i.e. the set of slopes of its Newton polygon is $\{0,1/2,1\}$ and $\mathrm{length}(1/2)=2$.*

This work was partially supported by the Simons Foundation (grant #246625 to Yuri Zarkhin).

Remark 1.2. Let X and B satisfy the conditions (i)-(iii) of Theorem 1.1. Let us fix an embedding $B \subset \mathbb{C}$ of the imaginary quadratic field B into the field $\mathbb{C}$ of complex numbers. Let

$$\sigma_1, \sigma_2, \sigma_3 : \mathrm{End}^0(X) \hookrightarrow \mathbb{C}$$

the distinct embeddings of sextic $\mathrm{End}^0(X)$ to $\mathbb{C}$ that act as the identity map on B. Let us put

$$\alpha_1 = \sigma_1(\mathrm{Fr}_X),\ \alpha_2 = \sigma_2(\mathrm{Fr}_X),\ \alpha_3 = \sigma_3(\mathrm{Fr}_X).$$

Then $\alpha_1, \alpha_2, \alpha_3$ are distinct eigenvalues of Fr_X and

$$q^3 = (\alpha_1\alpha_2\alpha_3)^2.$$

Remark 1.3. See [17, Sect. 4] for examples of not neat abelian threefolds constructed by Hendrik Lenstra.

Acknowledgements. I am grateful to Hendrik Lenstra and Frans Oort for helpful discussions and to Igor Shparlinski for stimulating questions. This work was started during my stay at the Max-Planck-Institut für Mathematik (Bonn) in September 2013: I am grateful to the Institute for the hospitality and support.

2. Ranks of neat abelian varieties

As usual, ℓ is a prime different from p, $\mathbb{N}, \mathbb{Z}, \mathbb{Z}_\ell, \mathbb{Q}.\mathbb{C}, \mathbb{Q}_\ell$ stand for the set of positive integers, ring of integers, ring of ℓ-adic integers and the fields of rational, complex and ℓ-adic numbers respectively. If A is a finite set then we we write $\#(A)$ for number of its elements. We write $\mathrm{rk}(\Delta)$ for rank of a finitely generated commutative group Δ.

Throughout this paper k is a finite field of characteristic p that consists of q elements, $\bar{k}$ an algebraic closure of k and $\mathrm{Gal}(K) = \mathrm{Gal}(\bar{k}/k)$ the absolute Galois group of k. It is well known that the profinite group $\mathrm{Gal}(K)$ is procyclic and the *Frobenius automorphism*

$$\sigma_k : \bar{k} \to \bar{k},\ x \mapsto x^q$$

is a topological generator of $\mathrm{Gal}(k)$.

Let X be an abelian variety of positive dimension over k. We write $\mathrm{End}(X)$ for the ring of its k-endomorphisms and $\mathrm{End}^0(X)$ for the corresponding (finite-dimensional semisimple) $\mathbb{Q}$-algebra $\mathrm{End}(X) \otimes \mathbb{Q}$. We write $\mathrm{Fr}_X = \mathrm{Fr}_{X,k}$ for the Frobenius endomorphism of X. We have

$$\mathrm{Fr}_X \in \mathrm{End}(X) \subset \mathrm{End}^0(X).$$

By a theorem of Tate [12, Sect. 3, Th. 2 on p, 140], he $\mathbb{Q}$-subalgebra $\mathbb{Q}[\mathrm{Fr}_X]$ of $\mathrm{End}^0(X)$ generated by Fr_X coincides with the center of $\mathrm{End}^0(X)$. In particular, if $\mathrm{End}^0(X)$ is a field then $\mathrm{End}^0(X) = \mathbb{Q}[\mathrm{Fr}_X]$.

If ℓ is a prime different from p then we we write $T_\ell(X)$ for the $\mathbb{Z}_\ell$-Tate module of X and $V_\ell(X)$ for the corresponding $\mathbb{Q}_\ell$-vector space

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

It is well known [7] that $T_\ell(X)$ is a free $\mathbb{Z}_\ell$-module of rank $2\mathrm{dim}(X)$ that may be viewed as a $\mathbb{Z}_\ell$-lattice in the $\mathbb{Q}_\ell$-vector space $V_\ell(X)$ of dimension $2\mathrm{dim}(X)$.

By functoriality, $\mathrm{End}(X)$ and Fr_X acts on ($T_\ell(X)$ and) $V_\ell(X)$; it is well known that the action of Fr_X coincides with the action of σ_k. By a theorem of A. Weil

[7, Sect. 19 and Sect. 21], Fr_X acts on $V_\ell(X)$ as a semisimple linear operator, its characteristic polynomial

$$\mathbb{P}_X(t) = \mathbb{P}_{X,k}(t) = \det(t\mathrm{Id} - \mathrm{Fr}_X, V_\ell(X)) \in \mathbb{Z}_\ell[t]$$

lies in $\mathbb{Z}[t]$ and does not depend on a choice of ℓ. In addition, all eigenvalues of Fr_X (which are algebraic integers) have archimedean absolute value equal to $q^{1/2}$. This means that if

$$L = L_X \subset \mathbb{C}$$

is the splitting field of $\mathbb{P}_X(t)$ and

$$R_X = R_{X,k} \subset L$$

the set of roots of $P(t)$ then L is a finite Galois extension of $\mathbb{Q}$ such that for every field embedding $L \hookrightarrow \mathbb{C}$ we have $\mid \alpha \mid = q^{1/2}$ for all $\alpha \in R_X$. Let $\mathrm{Gal}(L/\mathbb{Q})$ be the Galois group of $L/\mathbb{Q}$. Clearly, R_X is a $\mathrm{Gal}(L/\mathbb{Q})$-invariant (finite) subset of L^*. It follows easily that if $\alpha \in R_X$ then $q/\alpha \in R_X$. Indeed, q/α is the *complex-conjugate* $\bar{\alpha}$ of α. We have

$$q^{-1}\alpha^2 = \frac{\alpha}{q/\alpha}.$$

Remark 2.1. Let $m(\alpha)$ be the multiplicity of the root α of $\mathbb{P}_X(t)$. Then

$$P_X(t) = \prod_{\alpha \in R_X} (t-\alpha)^{m(\alpha)} \in \mathbb{C}[t] \tag{1}$$

and

$$\mathrm{rk}(\mathrm{End}(X)) = \sum_{\alpha \in R_X} m(\alpha)^2 \tag{2}$$

(see [12, pp. 138–139], especially (4) and (5)). Let κ be a finite overfield of k of degree d and $X_\kappa = X \times_k \kappa$. Then $T_\ell(X_\kappa)$ and $V_\ell(X_\kappa)$ are canonically isomorphic to $T_\ell(X)$ and $V_\ell(X)$ respectively,

$$\mathrm{Fr}_{X_\kappa} = \mathrm{Fr}_X^d \subset \mathrm{End}(X) \subset \mathrm{End}(X_\kappa),$$

$$R_{X_\kappa} = \{\alpha^d \mid \alpha \in R_X\},\ \mathbb{P}_{X_\kappa}(t) = \prod_{\alpha \in R_X} (t-\alpha^d)^{m(\alpha)}.$$

Suppose that α/β is *not* a root of unity for every pair of *distinct* $\alpha, \beta \in R_X$. This implies that α^d and β^d are distinct roots of $\mathbb{P}_{X_\kappa}(t)$. It follows that for every $\alpha \in R_X$ the positive integer $m(\alpha)$ coincides with the multiplicity of root α^d of the polynomial $\mathbb{P}_{X_\kappa}(t)$. The formulas (1) and (2) applied to X_κ give us the equality $\mathrm{rk}(\mathrm{End}(X_\kappa)) = \mathrm{rk}(\mathrm{End}(X))$, which implies that $\mathrm{End}(X_\kappa) = \mathrm{End}(X)$, because the quotient $\mathrm{End}(X_\kappa)/\mathrm{End}(X)$ is torsion-free [11, Sect. 4, p. 501].

Remark 2.2. Let $\mathcal{O}_L$ be the ring of integers in L. Clearly, $R_X \subset \mathcal{O}_L$. It is also clear that $\mathfrak{B}$ is a maximal ideal in $\mathcal{O}_L$ such that $\mathrm{char}(\mathcal{O}_L/\mathfrak{B}) \ne p$ then all elements of R_X are $\mathfrak{B}$-adic units.

Remark 2.3. Notice that R_X is a $\mathrm{Gal}(L/\mathbb{Q})$-orbit if and only if $\mathbb{P}_X(t)$ is a power of an irreducible polynomial (over $\mathbb{Q}$), which means that X is isogenous over k to a simple abelian variety over k [12, Theorem 2(e)].

Example 2.4. By functoriality, $\mathrm{End}^0(X)$ and $\mathbb{Q}[\mathrm{Fr}_X]$ act on $V_\ell(X)$. This action extends by $\mathbb{Q}_\ell$-linearity to the embedding of $\mathbb{Q}_\ell$-algebras

$$\mathbb{Q}[\mathrm{Fr}_X]\otimes_{\mathbb{Q}}\mathbb{Q}_\ell \subset \mathrm{End}^0(X)\otimes_{\mathbb{Q}}\mathbb{Q}_\ell = \mathrm{End}(X)\otimes_{\mathbb{Q}}\mathbb{Q}_\ell \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X)).$$

Let us assume that $E=\mathbb{Q}[\mathrm{Fr}_X]$ is a field. (E.g., X is simple.) Then it is known [10] that $V_\ell(X)$ carries the natural structure of a free $E\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$-module and this module is free of rank $e=2\mathrm{dim}(X)/[E:\mathbb{Q}]$. It follows that

$$\mathbb{P}_X(t)=[\mathbb{P}_{X,\min}(t)]^e$$

where $\mathbb{P}_{X,\min}(t)$ is the minimal polynomial of the semisimple linear operator $\mathrm{Fr}_X : V_\ell(X)\to V_\ell(X)$. Clearly, $\mathbb{P}_{X,\min}(t)$ has integer coefficients, $\mathbb{P}_{X,\min}(\mathrm{Fr}_X)=0\in \mathrm{End}(X)$ and the natural homomorphism

$$\mathbb{Q}[t]/\mathbb{P}_{X,\min}(t)\mathbb{Q}[t]\to\mathbb{Q}[\mathrm{Fr}_X],\ t\mapsto \mathrm{Fr}_X+\mathbb{P}_{X,\min}(t)\mathbb{Q}[t]$$

is a field isomorphism. (In particular, $\mathbb{P}_{X,\min}(t)$ is irreducible over $\mathbb{Q}$.)

This implies that if we fix an embedding $E\subset\mathbb{C}$ then L_X is the normal closure of E over $\mathbb{Q}$ and R_X is the set of images of Fr_X ion $\mathbb{C}$ with respect to all field embeddings $E\hookrightarrow\mathbb{C}$; in addition, every eigenvalue $\alpha\in R_X$ has multiplicity e.

We write

$$\Gamma=\Gamma(X,k)$$

for the multiplicative subgroup of L^* generated by R_X. One may easily check, using Weil's results that Γ_X contains q and is a finitely genetated group of rank $\mathrm{rk}(\Gamma)\le\dim(X)+1$. Notice that the rank of Γ is $\dim(X)+1$ if and only if Γ is a free commutative group of rank $\dim(X)+1$ [16].

Remark 2.5. It follows from Remark 2.2 that if $\mathfrak{B}$ is a maximal ideal in $\mathcal{O}_L$ such that $\mathrm{char}(\mathcal{O}_L/\mathfrak{B})\ne p$ then all elements of $\Gamma(X.k)$ are $\mathfrak{B}$-adic units.

We write

$$\Gamma'=\Gamma(X,k)'$$

for the multiplicative subgroup of L^* generated by all the eigenvalues of $q^{-1}\mathrm{Fr}_X^2$. In other words, Γ' is the multiplicative (sub)group generated by

$$R'_X=\{q^{-1}\alpha^2\mid\alpha\in R_X\}.$$

Clearly, all the archimedean absolute values of all elements of Γ' are equal to 1.

One may easily check that

$$\mathrm{rk}(\Gamma')+1=\mathrm{rk}(\Gamma)$$

and Γ' and q generate a subgroup of finite index in Γ. We define the rank of X as $\mathrm{rk}(\Gamma')$ and denote by $\mathrm{rk}(X)$. Clearly,

$$0\le\mathrm{rk}(X)\le\dim(X).$$

It is known [17, Sect. 2.9 on p. 277 and Remark 2.9.2 on p. 278] that if Y is an abelian variety over k then

$$\max(\mathrm{rk}(X),\mathrm{rk}(Y))\le\mathrm{rk}(X\times Y)\le\mathrm{rk}(X\times Y).$$

Notice also that $\mathrm{rk}(X)$ does not depend on a field of definition of X and would not change if we replace X by an isogenous abelian variety. In addition, $\mathrm{rk}(X)=0$ if and only if X is a supersingular abelian variety [17, Sect. 2.0].

This implies the following *trivial* multiplicative relations between eigenvalues $\alpha, \beta, q/\alpha, q/\beta \in R_X$.

$$\alpha \cdot \frac{q}{\alpha} = q = \beta \cdot \frac{q}{\beta}. \tag{3}$$

Let us put

$$R'_X := \{q^{-1}\alpha^2 \mid \alpha \in R_X\}.$$

Clearly, all elements of R'_X have archimedean absolute value 1 with respect to all field embeddings $L \hookrightarrow \mathbb{C}$ and the map $\beta \mapsto \beta^{-1}$ is an involution of R'_X.

Assume that k is sufficiently large with respect to X, i.e., the multiplicative group $\Gamma(X, k)$ generated by k does not contain roots of unity (except 1). This implies (thanks to Remark 2.1) that all the endomorphisms of X are defined over k. On the other hand, the map

$$R_X \to R'_X, \ \alpha \mapsto \alpha' = q^{-1}\alpha^2$$

is a bijective map that sends q/α to $1/\alpha'$.

Suppose that there are an integer-valued function $e : R_X \to \mathbb{Z}$ and an integer M such that

$$\prod_{\alpha \in R_X} \alpha^{e(\alpha)} = q^M. \tag{4}$$

Since the archimedean absolute value of each α is $\sqrt{\alpha}$, we have

$$\frac{1}{2}\left(\sum_{\alpha \in R_X} e(\alpha)\right) = M$$

and therefore

$$2M = \sum_{\alpha \in R_X} e(\alpha), \ \prod_{\alpha \in R_X} \alpha^{2e(\alpha)} = q^{2M}.$$

This implies that

$$\prod_{\alpha \in R_X} (q^{-1}\alpha^2)^{e(\alpha)} = 1. \tag{5}$$

We may rewrite (5) as

$$\prod_{\beta \in R'_X} \beta^{e'(\beta)} = 1 \tag{5bis}$$

where $e'(\alpha^2/q) := e(\alpha)$.

Conversely, if (5bis) holds for some $e' : R'_X \to \mathbb{Z}$ then we have

$$\prod_{\alpha \in R_X} \alpha^{e(\alpha)} = q^M$$

with $e(\alpha) := 2e'(\alpha^2/q)$ and $M := \sum_{\beta \in R'_X} e'(\beta)$. We say that X is *neat* if it enjoys one of the following (obviously equivalent) equivalent conditions (we continue to assume that k is sufficiently large).

(i) Suppose an integer-valued function $e : R_X \to \mathbb{Z}$ and a positive integer M satisfy (3). Then $e(\alpha) = e(q/\alpha) \ \forall \alpha \in R_X$.

(ii) Suppose an integer-valued function $e' : R'_X \to \mathbb{Z}$ satisfies (4bis). Then $e'(\beta) = e'(1/\beta) \ \forall \beta \in R'_X$.

Remark 2.6. Let us consider the (sub)set $R_{X,ss}$ of $\alpha \in R_X$ such that $q^{-1}\alpha^2$ is a root of unity. (Here the subscript ss is short for supersingular.) Clearly, $\alpha \in R_{X,ss}$ if and only if $q\alpha^{-1} \in R_{X,ss}$. It is also clear that if $R_{X,ss}$ is non-empty then $1/2$ is a slope of X. (The converse is not true if $\dim(X) > 1$.)

Recall [17, Definition 2.3 on p. 276] that k is *sufficiently large* with respect tp X or just sufficiently large if $\Gamma(X, k)$ does not contain roots of unity different from 1. If m the order of the subgroup of roots of unity in $\Gamma(X, k)$ and κ/k is a finite algebraic field extension then κ is sufficiently large for X if and only if the degree $[\kappa : k]$ is divisible by m [17, p. 276]. In particular, if k is sufficiently large and $\beta \in R'_X$ is a root of unity then $\beta = 1$. Notice also that if $\mathrm{rk}(X) = \dim(X)$ then $\Gamma(X, k)$ is a free commutative group [16, Sect. 2.1], i.e., k is sufficiently large.

Lemma 2.7. *Suppose that k is sufficiently large with respect to X. If $R_{X,ss}$ is non-empty then the following conditions hold:*

(i) *q is a square.*
(ii) *$R_{X,ss}$ is either the singleton $\{\sqrt{q}\}$ or the singleton $\{-\sqrt{q}\}$. In both cases R'_X contains*

$$q^{-1}(\pm\sqrt{q})^2 = 1.$$

Proof. Let $\alpha \in R_{X,ss}$. Since the root of unity $q^{-1}\alpha^2$ lies in $\Gamma(X, k)$, we conclude that $\alpha^2 = q$. Since R_X is $\mathrm{Gal}(L/Q)$-stable, we conclude that if q is not a square then both $\sqrt{q}$ and $-\sqrt{q}$ lie in R_X and therefore

$$-1 = \frac{-\sqrt{q}}{\sqrt{q}} \in \Gamma(X, k),$$

which is not the case, because k is sufficiently large. Therefore q is a square and R_X is either the singleton $\{\sqrt{q}\}$ or the singleton $\{-\sqrt{q}\}$. □

Remark 2.8. Suppose that k is sufficiently large. Then if α_1 and α_2 are *distinct* elements of R_X then

$$\frac{\alpha_1}{\alpha_2} \neq \pm 1$$

and therefore $q^{-1}\alpha_1^2$ and $q^{-1}\alpha_2^2$ are *distinct* elements of R'_X. This implies that

$$\#(R_X) = \#(R'_X).$$

Till the end of this Section we assume that k is sufficiently large with respect to X.

In order to compute the rank of *neat* abelian varieties, let us consider the minimal polynomial $\mathbb{P}_{X,\min}(t)$ of the semisimple linear operator $\mathrm{Fr}_X : V_\ell(X) \to V_\ell(X)$. The set of roots of $\mathbb{P}_{X,\min}(t)$ coincides with one of $\mathbb{P}_X(t)$, i.e., with R_X; in addition, all the roots of $\mathbb{P}_X(t)$ are simple. It follows from Remark 2.3 that if X is simple or k-isogenous to a k-simple abelian variety then $\mathbb{P}_{X,\min}(t)$ is irreducible over $\mathbb{Q}$ and $\mathbb{P}_X(t) = [\mathbb{P}_{X,\min}(t)]^d$ for a certain positive integer d. In general case we have

$$\mathbb{P}_{X,\min}(t) = \prod_{\alpha \in R_X} (t - \alpha).$$

In particular,

$$\deg(\mathbb{P}_{X,\min}) = \#(R_X).$$

Example 2.9. Suppose X a supersingular abelian variety. According to Subsection 4.2, α^2/q is a root of unity for all $\alpha \in R_X$, i.e., $R_X = R_{X,ss}$. It follows from Lemma 2.7 that q is a square and R_X is either the singleton $\{-\sqrt{q}\}$ or the singleton $\{\sqrt{q}\}$. Then $\mathbb{P}_{X,\min}(t)$ is a linear polynomial that equals $t - \sqrt{q}$ or $t + \sqrt{q}$ respectively. This implies that that $\mathbb{P}_X(t) = (t \pm \sqrt{q})^{2\dim(X)}$ and R'_X is always the singleton $\{1\}$. It follows that X is neat.

Example 2.10. Suppose $R_{X,ss}$ is empty. This implies that $\alpha \neq q/\alpha$ for every $\alpha \in R_X$, the set R_X consists of even, say, $2d$ elements and one may choose d distinct elements $\alpha_1, \dots, \alpha_d$ of R_X such that

$$R_X = \{\alpha_1, \dots, \alpha_d;\ q/\alpha_1, \dots, q/\alpha_d\}.$$

If we put $\beta_i = q^{-1}\alpha_i^2$ then R'_X also consists of $2d$ (distinct) elements and coincides with

$$\{\beta_1, \dots, \beta_d;\ \beta_1^{-1}, \dots, \beta_d^{-1}\}.$$

In particular, $\mathrm{rk}(X) \leq d$. Now X is neat if and only if the set $\{\beta_1, \dots, \beta_d\}$ is multiplicatively independent, which means that

$$\mathrm{rk}(X) = d.$$

If this is the case then

$$\mathrm{rk}(X) = d = \frac{\#(R_X)}{2} = \frac{\deg(\mathbb{P}_{X,\min})}{2}.$$

Example 2.11. Suppose $R_{X,ss}$ is non- empty but does *not* coincide with the whole R_X. Let us denote by α_0 the only element of $R_{X,ss}$; as we have seen above, q is a square and $\alpha_0 = \pm\sqrt{q}$. This implies that if α is an element of R_X that is different from α_0 then $\alpha \neq q/\alpha$, the set $R_X \setminus \{\alpha_0\}$ consists of even, say, $2d$ elements and one may choose d distinct elements $\alpha_1, \dots, \alpha_d$ of $R_X \setminus \{\alpha_0\}$ such that

$$R_X = \{\alpha_0;\ \alpha_1, \dots, \alpha_d;\ q/\alpha_1, \dots, q/\alpha_d\}.$$

If we put $\beta_i = q^{-1}\alpha_i^2$ then $\beta_0 = 1$ R'_X consists of $(2d+1)$ (distinct) elements

$$\{1; \beta_1, \dots, \beta_d;\ \beta_1^{-1}, \dots, \beta_d^{-1}\}.$$

In particular, $\mathrm{rk}(X) \leq d$. Now X is neat if and only if the set $\{\beta_1, \dots, \beta_d\}$ is multiplicatively independent, which means that

$$\mathrm{rk}(X) = d.$$

. If this is the case then

$$\mathrm{rk}(X) = d = \frac{\#(R_X) - 1}{2} = \frac{\deg(\mathbb{P}_{X,\min}) - 1}{2}.$$

Example 2.12. Suppose that X is simple and $\mathrm{rk}(X) = 1$. It follows from Lemma 2.10 of [17] that R'_X consists of two elements say, β and β^{-1}. Clearly, β is not a root of unity. This implies easily that X is neat.

We will need the following elementary lemma.

Lemma 2.13. *Let p be a prime, B an imaginary quadratic field, T the set of maximal ideals in B that lie above p. Let $U_T \subset B^*$ be the multiplicative subgroup of T-units in B and U_T^1 the subgroup of T_B that consists of all $\gamma \in U_T$ such that the archimedean absolute value of γ is 1. If U_T^1 is infinite then p splits in B (i.e., $\#(T) = 2$), $\mathrm{rk}(U_T) = 2$ and $\mathrm{rk}(U_T^1) = 1$.*

Proof. By the generalized Dirichlet unit's theorem [3, Ch. V, Sect. 1], U_T is a finitely generated commutative group of rank $\#(T)$. Clearly, U_T contains an element p of infinite order. If $\#(T)=1$ then $\mathrm{rk}(U_T)=1$ and therefore for each

$$\gamma \in U_T^1 \subset U_T$$

a certain positive power of γ is a power of p. However, the archimedean absolute value of γ equals 1 and therefore γ must be a root of unity, which is not the case, since there are only finitely many roots of unity in B. So, $\#(T)=2$, i.e., p splits in B. In addition, U_T has rank 2. Since no power of p (except $1=p^0$) lies in U_T^1, we conclude that $\mathrm{rk}(U_T^1)<\mathrm{rk}(U_T)=2$. Since $\mathrm{rk}(U_T^1)\ge 1$, we conclude that $\mathrm{rk}(U_T^1)=1$. □

Corollary 2.14. *Let B be an imaginary quadratic subfield in L. Suppose that the intersection $\Gamma'(X,k)_B$ of B and $\Gamma'(X,k)$ is infinite. Then p splits in B and the infinite multiplicative group $\Gamma'(X,k)_B$ has rank 1.*

Proof. Notice that (in the notation of Lemma 2.13) $\Gamma'(X,k)_B$ is an infinite subgroup of U_T^1. In particular, U_T^1 is also infinite. Now Corollary follows readily from Lemma 2.13. □

Remark 2.15. Suppose that $g=\dim(X)>1$, k is sufficiently large with respect to X and X is simple. Then X is absolutely simple. In addition, if $\alpha\in R_X$ then $\alpha\ne q/\alpha$. (Indeed, otherwise, α is a square root of q and therefore X is supersingular [12]. Now the absolute simplicity of X implies that $\dim(X)=1$, which is not the case.) This implies that R_X has even cardinality say, $2m$ and one may choose m distinct elements $\{\alpha_1,\dots,\alpha_m\}$ of R_X such that the $2m$-element set R_X coincides with $\{\alpha_1,\dots,\alpha_m; q/\alpha_1,\dots,q/\alpha_m\}$. If we put $\beta_i=\alpha_i^2/q$ then R'_X coincides with the $2m$-element set $\{\beta_1,\dots,\beta_m;\beta_1^{-1},\dots,\beta_m^{-1})$ and

$$\mathrm{rk}(X)=\mathrm{rk}(\Gamma'(X,k)\le m.$$

Clearly, X is neat if and only if the set $\{\beta_1,\dots,\beta_m\}$ consists of multiplicatively independent elements, i.e., $\Gamma'(X,k)$ has rank m.

We have

$$\mathbb{P}_{X,\min}(t)=\prod_{i=1}^{m}(t-\alpha_i)(t=q/\alpha_i)$$

has degree $2m$. Since X is simple, there is a positive integer d such that $\mathbb{P}_X(t)=\mathbb{P}_{X,\min}(t)^d$. Comparing the degrees, we obtain that

$$2g=2\dim(X)=2md,\ g=md.$$

It follows that if $\mathrm{rk}(X)>g/2$ then $m>g/2$ and therefore $d=1$, i.e., $\mathbb{P}_X(t)$ has no multiple roots and therefore $\mathrm{End}^0(X)$ is a field.

3. Ranks of non-simple abelian varieties

The following assertion was proven in [17, pp. 273, 280–281].

Theorem 3.1. *Let X and Y be non-supersingular simple abelian varieties over k. If*

$$\mathrm{rk}(X\times Y)=\mathrm{rk}(X)+\mathrm{rk}(Y)-1$$

then there exists an imaginary quadratic field B enjoying the following properties.

0) *p splits in B;*

1) *The number fields* $E_X = \mathbb{Q}[\mathrm{Fr}_{X,k}]$ *and* $E_Y = \mathbb{Q}[\mathrm{Fr}_{Y,k}]$ *contain subfields isomorphic to* B*;*
2) $\mathrm{Norm}_{E_X/B}(q^{-1}\mathrm{Fr}_{X,k}^2)$ *and* $\mathrm{Norm}_{E_Y/B}(q^{-1}\mathrm{Fr}_{Y,k}^2)$ *are not roots of unity.*

Remark 3.2. There was a typo in the displayed formula for ranks in [17, Th. 2.12], see Sect. 8. It was also erroneously claimed (without a proof) in [17, Th. 2.12] that the conditions 0,1,2 are equivalent to the formula $\mathrm{rk}(X \times Y) = \mathrm{rk}(X) + \mathrm{rk}(Y) - 1$. Actually, the conditions 0),1),2) imply only the inequality $\mathrm{rk}(X \times Y) \le \mathrm{rk}(X) + \mathrm{rk}(Y) - 1$.

Proof of Theorem 3.1. Assertions 1 and 2 are proven in [17, pp. 280–281]. Assertion 0 is proven in [17, Remark 1.1.5 on p. 273]. (It also follows from Assertion 2 combined with Lemma 2.14).

□

Corollary 3.3 (Theorem 2.11 of [17])**.** *Assume that* $E = \mathrm{End}^0(X)$ *is a number field. Let* Y *be an ordinary elliptic curve over* k*. The equality* $\mathrm{rk}(\Gamma(X \times Y)) = \mathrm{rk}(\Gamma(X))$ *holds true if and only if* $\mathrm{End}^0 X$ *contains an imaginary quadratic subfield isomorphic to* $B = \mathrm{End}^0 Y$ *and* $\mathrm{Norm}_{E/B}(q^{-1}\mathrm{Fr}_{X,k}^2)$ *is not a root of unity.*

Proof. Since $\mathrm{rk}(Y) = 1$, we have

$$\mathrm{rk}(X) = \mathrm{rk}(X) + \mathrm{rk}(Y) - 1.$$

This implies that in one direction (if we are given that $\mathrm{rk}(\Gamma(X \times Y)) = \mathrm{rk}(\Gamma(X))$, i.e., $\mathrm{rk}(X \times Y) = \mathrm{rk}(X)$) our assertion follows from Theorem 3.1. Conversely, suppose that $B = \mathrm{End}^0 Y$ is isomorphic to a subfield of E and

$$\gamma := \mathrm{Norm}_{E/B}(q^{-1}\mathrm{Fr}_{X,k}^2) \in B$$

is *not* a root of unity. Let us fix an embedding $E \subset \mathbb{C}$. We have

$$\gamma \in B \subset E \subset L_X \subset \mathbb{C}.$$

By definition, γ is a product of elements of R'_X and therefore lies in $\Gamma'(X,k)$. In particular, in the notation of Lemma 2.14, $\gamma \in \Gamma'(X,k)_B$. On the other hand, $q^{-1}\mathrm{Fr}_{Y,k}^2 \subset B$ is also *not* a root of unity; in addition, it generates $\Gamma'(Y,k)$. Notice that (in the notation of Lemma 2.13) both γ and $q^{-1}\mathrm{Fr}_{Y,k}^2$ lie in U_T^1; in particular, U_T^1 is infinite. By Lemma 2.13, U_T^1 is a group of rank 1 and therefore the intersection of cyclic (sub)groups generated by γ and $q^{-1}\mathrm{Fr}_{Y,k}^2$ is an infinite cyclic group. This implies that the intersection of finitely generated groups $\Gamma'(X,k)$ and $\Gamma'(Y,k)$ is an infinite group. It follows that the rank of $\Gamma'(X \times Y, k) = \Gamma'(X,k)\Gamma'(Y,k)$ is strictly less than the sum

$$\mathrm{rk}(\Gamma'(X,k)) + \mathrm{rk}(\Gamma'(Y,k)) = \mathrm{rk}(\Gamma'(X,k)) + 1.$$

In other words, $\mathrm{rk}(X \times Y) < \mathrm{rk}(X) + 1$, i.e., $\mathrm{rk}(X \times Y) \le \mathrm{rk}(X)$. It follows that $\mathrm{rk}(X \times Y) = \mathrm{rk}(X)$ and we are done. □

4. Newton polygons

In order to define the Newton polygon of X, let us consider the ring $\mathcal{O}_L$ of integers in L and pick a maximal ideal $\mathfrak{P}$ in $\mathcal{O}_L$ such that the residue field $\mathcal{O}_L/\mathfrak{P}$ has characteristic p. The set S_p of such ideals consitutes a $\mathrm{Gal}(L/\mathbb{Q})$-orbit. Let

$$\mathrm{ord}_{\mathfrak{P}} : L^* \to \mathbb{Q}$$

be the discrete valuation map that corresponds to $\mathfrak{P}$ and normalized by the condition

$$\mathrm{ord}_{\mathfrak{P}}(q) = 1.$$

Then the set

$$\mathrm{Slp}_X = \mathrm{ord}_{\mathfrak{P}}(\mathfrak{R}_X) \subset \mathbb{Q}$$

is called the *set of slopes* of X. For each $c \in \mathrm{Slp}_X$ we write

$$\mathrm{length}(c) = \mathrm{length}_X(c)$$

for the number of roots α of $\mathbb{P}_X(t)$ (with multiplicities) such that

$$\mathrm{ord}_{\mathfrak{P}}(\alpha) = c.$$

By definition

$$\sum_{c \in \mathrm{Slp}_X} \mathrm{length}(c) = \deg(\mathbb{P}_X) = 2\mathrm{dim}(X). \tag{6}$$

Remark 4.1. It is well known that all slopes $c \in \mathrm{Slp}_X$ are rational numbers that lie between 0 and 1. In addition, if c is a slope then $1 - c$ is also a slope and $\mathrm{length}(c) = \mathrm{length}(1 - c)$. In addition, if $1/2$ is a slope then its length is even. Notice also that the rational number c can be presented as a fraction, whose denominator is a positive integer that does not exceed $2\mathrm{dim}(X)$ [15, p. 173].

Since $\mathbb{P}(t)$ has rational coefficients and $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on S_p, the set Slp_X and the function

$$\mathrm{length}_X : \mathrm{Slp}_p \to \mathbb{N}$$

do not depend on a choice of $\mathfrak{P}$. The *integrality property* of the Newton polygon [9, Sect. 9 and 21] means that $c \cdot \mathrm{length}_X(c)$ is a positive integer for each nonzero slope c. Suppose that a slope $c \ne 1/2$ is presented as the fraction in lowest terms, whose denominator is greater than $\mathrm{dim}(X)$. Then $\mathrm{length}(c) > \mathrm{dim}(X)$ and

$$\mathrm{length}(1 - c) = \mathrm{length}(c) > \mathrm{dim}(X),$$

which implies $\mathrm{length}(c) + \mathrm{length}(1 - c) > 2\mathrm{dim}(X)$ and we get a contradiction to (6). So, each slope $c \ne 1/2$ can be presented as a fraction, whose denominator does not exceed $\mathrm{dim}(X)$. It is also clear, that if the denominator of c in lowest terms is exactly $\mathrm{dim}(X)$ then

$$\mathrm{length}(c) = \mathrm{dim}(X) = \mathrm{length}(1 - c)$$

and $\mathrm{Slp}_X = \{c, 1 - c\}$.

Definition 4.2. An abelian variety X is called *ordinary* if $\mathrm{Slp}_X = \{0, 1\}$; it is called *supersingular* if $\mathrm{Slp}_X = \{1/2\}$. It is well known that X is supersingular if and only if R'_X consists of roots of unity, i.e., $q^{-1}\alpha^2$ is a root of unity for all $\alpha \in R_X$. (By the way, it follows immediately from Proposition 3.1.5 in [15, p. 172].)

X is called of *K3 type* [16] if Slp_X is either $\{0, 1/2, 1\}$ or $\{0, 1\}$ while (in both cases) $\mathrm{length}_X(0) = \mathrm{length}_X(1) = 1$. It is called *almost ordinary* [5] if

$$\mathrm{Slp}_X = \{0, 1/2, 1\}, \ \mathrm{length}_X(1/2) = 2.$$

Remark 4.3. Clearly, X is supersingular if and only if $\mathrm{rk}(X) = 0$. If X is a simple abelian variety of K3 type then $\mathrm{rk}(X) = \mathrm{dim}(X)$ [16]. If X is a simple almost ordinary then $\mathrm{rk}(X) = \mathrm{dim}(X)$ or $\mathrm{dim}(X) - 1$; if, in addition $\mathrm{dim}(X)$ is *even* then $\mathrm{rk}(X) = \mathrm{dim}(X)$ [5].

Theorem 4.4. *Let X be a simple abelian variety of positive dimension over k and $\mathbb{P}_X(t)$ is irreducible. Suppose there exists a rational number $c \ne 1/2$ such that* $\mathrm{Slp}_X = \{c, 1-c\}$. *(E.g., X is ordinary.) If* $\mathrm{rk}(X) = \dim(X) - 1$ *then* $\dim(X)$ *is even.*

Proof. Let us put $g = \dim(X)$ and

$$c' = 2c - 1 = -[2(1-c) - 1].$$

Clearly, $c' \ne 0$ and for all i the rational number $\mathrm{ord}_{\mathfrak{P}}(\alpha_i^2/q)$ is either c' or $-c'$. Let us define m_i by

$$\mathrm{ord}_{\mathfrak{P}}(\alpha_i^2/q) = m_i c'.$$

Clearly, $m_i = 1$ or -1. By Theorem 3.6(b) of [5] there are exist $\alpha_1, \dots, \alpha_g \in R_X$ and integers $n_1, \dots, n_g$ such that every n_i is either 1 or -1 and $\gamma = \prod_{i=1}^g (\alpha_i^2/q)^{n_i}$ is a root of unity. Pick $\mathfrak{P} \in S_p$. We have

$$0 = \mathrm{ord}_{\mathfrak{P}}(\gamma) = \sum_{i=1}^g n_i \mathrm{ord}_{\mathfrak{P}}\left(\alpha_i^2/q\right) = \sum_{i=1}^g n_i m_i c' = \left[\sum_{i=1}^g (\pm 1)\right] c'.$$

It follows that for a certain choice of signs $\sum_{i=1}^g (\pm 1) = 0$ and therefore g is even. □

Corollary 4.5. *Suppose that X is a simple abelian variety over k. Assume that* $1 \le \dim(X) \le 3$ *and k is sufficiently large with respect to X. If X is not neat then it is almost ordinary and* $\dim(X) = 3$.

Proof. The equality $\dim(X) = 3$ follows from Theorem 3.5 in [17]. Since X is not neat, $1 < \mathrm{rk}(X) < \dim(X) = 3$. This implies that $\mathrm{rk}(X) = 2$ and therefore $\deg(\mathbb{P}_{X,\min}) > 2 \cdot 2 = 4$. Since $\deg(\mathbb{P}_{X,\min})$ divides $\deg(\mathbb{P}_X) = 6$, we conclude that $\deg(\mathbb{P}_{X,\min}) = \deg(\mathbb{P}_X)$, i.e., $\mathbb{P}_X(t) = P_{X,\min}$ is irreducible over $\mathbb{Q}$. By Theorem 4.4, the Newton polygon of X has, at least, 3 distinct slopes. By Remark 4.1, all the slopes different from $1/2$ can be presented as fractions, whose denominator is strictly less than $\dim(X) = 3$. In other words, $\mathrm{Slp}_X = \{0, 1/2, 1\}$. In particular, $\mathrm{length}(1/2) = 2$ or 4. If $\mathrm{length}(1/2) = 4$ then $\mathrm{length}(0) = \mathrm{length}(1) = 1$ and X is of K3 type, which is not the case, since the rank of a simple abelian variety of K3 type equals its dimension [16]. Therefore $\mathrm{length}(1/2) = 2$ and $\mathrm{length}(0) = \mathrm{length}(1) = 2$, i.e., X is almost ordinary. □

5. Abelian Surfaces

The following statement should be known (at least, to experts) but I failed to find a reference.

Theorem 5.1. *Let L be a quartic CM field that contains an imaginary quadratic field B. Let S be a complex abelian surface provided with an embedding* $L \hookrightarrow \mathrm{End}^0(S)$. *Then S is isogenous to a square of an elliptic curve with complex multiplication. In particular, S is not simple.*

Proof. We may view L as a subfield of $\mathbb{C}$, Then $B = \mathbb{Q}(\sqrt{-d})$ where d is a positive integer. The field L contains the real quadratic subfield $\mathbb{Q}(\sqrt{r})$ where r is a square-free positive integer. Clearly,

$$L = \mathbb{Q} \oplus \mathbb{Q}\sqrt{-d} \oplus \mathbb{Q}\sqrt{r} \oplus \mathbb{Q}\sqrt{-rd}$$

is a Galois extension of $\mathbb{Q}$. This implies that L contains a second imaginary quadratic subfield $H := \mathbb{Q}(\sqrt{-rd})$. The natural map $B \otimes_{\mathbb{Q}} H \to L,\ b \otimes h \mapsto bh$ is a field isomorphism. In addition, the natural injective homomorphism

$$\mathrm{Gal}(B/\mathbb{Q}) \times \mathrm{Gal}(H/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(L/\mathbb{Q})$$

is surjective and therefore is a group isomorphism. Since $[L : \mathbb{Q}] = 2 \cdot 2$, it admits $2^2 = 4$ CM types Φ [7, ect. 22], [4]. Here is the list of all them. We have two CM types $\mathrm{Gal}(B/\mathbb{Q}) \otimes \tau_2$ indexed by $\tau_2 \in \mathrm{Gal}(H/\mathbb{Q})$ and two CM types $\tau_1 \otimes \mathrm{Gal}(H/\mathbb{Q})$ indexed by $\tau_1 \in \mathrm{Gal}(B/\mathbb{Q})$. They all have nontrivial automorphism groups

$$\mathrm{Aut}(\Phi) := \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \mid \sigma\Phi = \Phi\}.$$

Namely, $\mathrm{Aut}(\Phi) = \mathrm{Gal}(B/\mathbb{Q})$ for the former two CM types and $\mathrm{Aut}(\Phi) = \mathrm{Gal}(H/\mathbb{Q})$ for the latter two. Now the result follows from Theorem 3.5 of [4, p. 13] (applied to $F = l$.) □

Corollary 5.2. *There does not exist an abelian surface Y over a finite field k that enjoys the following properties.*

(i) *All endomorphisms of Y are defined over k.*
(ii) $\mathrm{End}^0(Y)$ *is a quartic CM field that contains an imaginary quadratic subfield.*

Proof. Assume that such Y does exist. Then it is absolutely simple. Replacing if necessary, k by its finite overfield and Y by a k-isogenous abelian variety, we may and will assume that Y can be *lifted* to an abelian variety A in characteristic zero such that there is an embedding $\mathrm{End}^0(Y) \hookrightarrow \mathrm{End}^0(A)$ [13, Sect. 3, Th. 2]. It follows that A is absolutely simple, which contradicts Theorem 5.1. The obtained contradiction proves Corollary. □

6. Proof of Theorem 1.1

Assume that X is *not* neat, k is sufficiently large and $1 \le \dim(X) \le 3$. According to [17, Th. 3.5 on p. 283], $\dim(X) = 3$ and one of the following two conditions holds.

(a) X is simple, $E = \mathrm{End}^0(X)$ is a number field that contains an imaginary quadratic subfield B such that $\mathrm{Norm}_{E/B}(q^{-1}\mathrm{Fr}_X^2)$ is a root of unity.
(b) X is isogenous over k to a product $Y \times Z$ of a *simple* abelian surface Y and an elliptic curve Z; $\mathrm{End}^0(Y)$ is a quartic CM-field containing an imaginary quiadratic subfield.

It follows from Corollary 5.2 that such an Y does not exist. Indeed, $\Gamma(X,k) = \Gamma(Y,k)\Gamma(Z,k)$; in particular, $\Gamma(Y,k)$ does not contain nontrivial roots of unity. Therefore all endomorphisms of Y are defined over k and therefore Y is absolutely simple. This contradicts to Corollary 5.2 and implies that the case (b) does not occur.

In the case (a), Corollary 4.5 implies that X is almost ordinary. Let us fix a field embedding $B \subset \mathbb{C}$ and let

$$\sigma_1, \sigma_2, \sigma_3 : E \hookrightarrow \mathbb{C}$$

be the list of field embedding $E \to \mathbb{C}$ that coincide with the identity map on B. Let us put

$$\alpha_1 = \sigma_1(\mathrm{Fr}_X) \in \mathbb{C},\ \alpha_2 = \sigma_2(\mathrm{Fr}_X) \in \mathbb{C}, \alpha_3 = \sigma_3(\alpha_3) \in \mathbb{C}.$$

Then

$$R_X = \{\alpha_1, \alpha_2, \alpha_3;\ q/\alpha_1, q/\alpha_2, q/\alpha_3\},$$
$$L = \mathbb{Q}(R_X) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = B(\alpha_1, \alpha_2, \alpha_3)$$

and the root of unity

$$\mathrm{Norm}_{E/B}\left(q^{-1}\mathrm{Fr}_X^2\right) = \prod_{i=1}^{3} \sigma_i \left(q^{-1}\mathrm{Fr}_X^2\right) = q^{-3} \prod_{i=1}^{3} \alpha_i^2 \in \Gamma(X, k).$$

Since $\Gamma(X, k)$ does *not* contain nontrivial roots of unity,

$$\mathrm{Norm}_{E/B}(q^{-1}\mathrm{Fr}_X^2) = 1.$$

(By the way, this gives us the relation

$$q^3 = \left(\prod_{i=1}^{3} \alpha_i\right)^2 .)$$

This ends the proof.

7. Abelian fourfolds

The following observation was inspired by results of Rutger Noot [8, Prop. 4.1 on p. 165 and p. 168] about the reduction type of abelian varieties of Mumford's type [6, Sect. 4].

Theorem 7.1. *Let X be an abelian fourfold over k. Suppose k is sufficiently large with respect to X, $\mathrm{rk}(X) = 3$ and X enjoys one of the following two properties.*

- *X is absolutely simple.*
- *X is isogenous over k to a product $X^{(3)} \times X^{(1)}$ of an (absolutely) simple abelian threefold $X^{(3)}$ and an ordinary elliptic curve $X^{(1)}$.*

Then one of the following two conditions holds.

(i) *there exist an imaginary quadratic field B and an embedding $B \hookrightarrow \mathrm{End}^0(X)$ that sends 1 to 1.*

(ii) *X is not simple and $X^{(3)}$ is an almost ordinary abelian threefold that is not neat and therefore satisfies the conditions of Theorem 1.1. In particular, $\mathrm{End}^0(X^{(3)})$ contains an imaginary quadratic subfield.*

Proof. If X is simple then

$$\mathrm{rk}(X) = 3 > 2 = \frac{\dim(X)}{2}.$$

By Remark 2.15, $\mathrm{End}^0(X)$ is a field. it follows from Theorem 3.6 of [5] that the condition (i) holds.

Now we may assume that $X = X^{(3)} \times X^{(1)}$. Since $X^{(1)}$ is an ordinary elliptic curve, $\mathrm{End}^0(X^{(1)})$ is an imaginary quadratic field and $\mathrm{rk}(X^{(1)}) = 1$. We have

$$\mathrm{rk}(X^{(3)}) \le \mathrm{rk}(X) = 3 \le \mathrm{rk}(X^{(3)}) + \mathrm{rk}(X^{(1)}) = \mathrm{rk}(X^{(3)}) + 1.$$

This implies that $\mathrm{rk}(X^{(3)}) = 2$ or 3. In both cases

$$\mathrm{rk}(X^{(3)}) > \frac{3}{2} = \frac{\dim(X^{(3)})}{2}.$$

Now Remark 2.15 implies that $\mathrm{End}^0(X^{(3)})$ is a field (recall that $X^{(3)}$ is simple). If $\mathrm{rk}(X^{(3)}) = 3$ then it follows from Corollary 3.3 (applied to $X = X^{(3)}$ and

$Y = X^{(1)}$) that there is a field embedding $\mathrm{End}^0(X^{(1)}) \hookrightarrow \mathrm{End}^0(X^{(3)})$ and therefore one may take as B the imaginary quadratic field $\mathrm{End}^0(X^{(1)})$, which implies that the condition (i) holds. If $\mathrm{rk}(X^{(3)}) = 2$ then $X^{(3)}$ is *not* neat. It follows from Theorem 1.1 that the condition (ii) holds. □

8. Corrigendum to [17]

- Page 274, Remark 2.1 The displayed formula should read
$$\mathrm{rk}(\Gamma) \le \lfloor \deg(\mathcal{P}_{\min})/2 \rfloor + 1.$$
The formula on last line should read $\lfloor \deg(\mathcal{P}_{\min})/2 \rfloor + 1$.
- Page 280, Theorem 2.12. The beginning of second sentence
The equality
$$\mathrm{rk}(\Gamma(X \times Y)) = \mathrm{rk}(X) + \mathrm{rk}(Y) - 1$$
holds true if and only if there exists an imaginary quadratic field B enjoying the following properties:
should read as follows.
If
$$\mathrm{rk}(X \times Y) = \mathrm{rk}(X) + \mathrm{rk}(Y) - 1$$
then there exists an imaginary quadratic field B that enjoys the following properties.
- Page 281, Remark 3.1, last line. The formula should read
$$\mathrm{rk}(\Gamma) = \lfloor \deg(\mathcal{P}_{\min})/2 \rfloor + 1.$$
- Page 284, line 8. $\alpha - 1$ should read α'^{-1}.

9. Corrigendum to [16]

- Pages 267, 269 (and throughout the text), $\angle$ and $\angle^*$ should read L and L^* respectively.
- Page 267, line -10: multiplicities should read multiplies.
- Page 271, Definition 3.4: ignore senseless **tenibk**.

References

[1] O. Ahmadi, I. Shparlinski, *On the distribution of number of points on algebraic curves in extensions of finie fields*. Math. Research Letters **17** (2010), 689–699.

[2] E. Kowalski, *The large sieve, monodromy and zeta functions of algebraic curves. II. Independence of the zeros*. IMRN (2008), Art. ID rnn 091, 1–57.

[3] S. Lang, Algebraic Numbers. Addison-Wesley Publishing Company, Reading, Mass., 1964.

[4] S. Lang, Complex Multiplication. Springer-Verlag, New York, 1983.

[5] H.W. Lenstra, Jr and Yu.G. Zarhin, *The Tate conjecture for almost ordinary abelian varieties over finite fields*. In: Advances in Number Theory, CNTA 91 Cinference Proceedings (F. Gouvea and N. Yui, eds.), Oxford University Press (1993), 179–194.

[6] D. Mumford, *A note of Shimura's paper "Discontinuous groups and abelian varieties"*. Math. Ann. **181** (1969), 345–351.

[7] D. Mumford, Abelian varieties, 2nd edition. Oxford University Press, 1974.

[8] R. Noot, *Abelian varieties with ℓ-adic Galois representation of Mumford's type*. J. reine angew. Math. **519** (2000), 155-169.

[9] F. Oort, *Abelian varieties over finite fields*, pp. 123–188. In: Higher-dimensional varieties over finite fields (D. Kaledin, Yu. Tschinkel, eds.), IOS Press, Amsterdam, 2008.

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

[11] J.-P. Serre, J. Tate, *Good reduction of abelian varieties.* Ann. Math. **88** (1968), 492–517.
[12] J.T. Tate, *Endomorphisms of abelian varieties over finite fields.* Invent. Math. **2** (1966), 134–144.
[13] J.T. Tate, *Classes d'isogénie de variétés abéliennes sur un corps fini* (d'après T. Honda), in Sém. Bourbaki 21, 1968/69, Exp. 352, Lecture Notes Math. 179, 1971, pp. 95–110.
[14] Yu.G. Zarhin, *Abelian varieties, ℓ-adic representations and SL_2.* Izvestiya AN SSSR ser. matem. **43** (1979) , 294–308 ; Math. USSR Izvestiya **14** (1980), 275–288.
[15] Yu.G. Zarhin, *Abelian varieties, ℓ-adic representations and Lie algebras. Rank independence on ℓ.* Invent. Math. **55** (1979), 165–176.
[16] Yu.G. Zarhin, *Abelian varieties of K3 type*, pp. 263–279. In: Séminaire de Théorie des Nombres, Paris, 1990-91 (S. David, ed.). Progress in Math. **108** (1993).
[17] Yu.G. Zarhin, *The Tate conjecture for non-simple abelian varieties over finite fields.* In: Algebra and Number Theory (G. Frey and J. Ritter, eds.), pp. 267–296. Walter de Gruyter, Berlin New York, 1994.

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

Department of Mathematics, The Weizmann Institute of Science, P.O.B. 26, Rehovot 7610001, Israel
E-mail address: `zarhin@math.psu.edu`