Séminaires & Congrès
11, 2005, p. 189–215

HOMOMORPHISMS OF ABELIAN VARIETIES

by

Yuri G. Zarhin

Abstract. — We study Galois properties of points of prime order on an abelian variety that imply the simplicity of its endomorphism algebra. Applications of these properties to hyperelliptic jacobians are discussed.

***Résumé* (Homomorphismes des variétés abéliennes).** — Nous étudions les propriétés galoisiennes des points d'ordre fini des variétés abéliennes qui impliquent la simplicité de leur algèbre d'endomorphismes. Nous discutons ceux-ci par rapport aux jacobiennes hyperelliptiques.

It is well-known that an abelian variety is (absolutely) simple or is isogenous to a self-product of an (absolutely) simple abelian variety if and only if the center of its endomorphism algebra is a field. In this paper we prove that the center is a field if the field of definition of points of prime order ℓ is "big enough".

The paper is organized as follows. In § 1 we discuss Galois properties of points of order ℓ on an abelian variety X that imply that its endomorphism algebra $\mathrm{End}^0(X)$ is a central simple algebra over the field of rational numbers. In § 2 we prove that similar Galois properties for two abelian varieties X and Y combined with the linear disjointness of the corresponding fields of definitions of points of order ℓ imply that X and Y are non-isogenous (and even $\mathrm{Hom}(X, Y) = 0$). In § 3 we give applications to endomorphism algebras of hyperelliptic jacobians. In § 4 we prove that if X admits multiplications by a number field E and the dimension of the centralizer of E in $\mathrm{End}^0(X)$ is "as large as possible" then X is an abelian variety of CM-type isogenous to a self-product of an absolutely simple abelian variety.

Throughout the paper we will freely use the following observation [**21**, p. 174]: if an abelian variety X is isogenous to a self-product Z^d of an abelian variety Z then a choice of an isogeny between X and Z^d defines an isomorphism between $\mathrm{End}^0(X)$ and the algebra $\mathrm{M}_d(\mathrm{End}^0(Z))$ of $d \times d$ matrices over $\mathrm{End}^0(Z)$. Since the center of

2000 ***Mathematics Subject Classification.*** — 14H40, 14K05.
Key words and phrases. — Hyperelliptic jacobians, homomorphisms of abelian varieties.

$\mathrm{End}^0(Z)$ coincides with the center of $\mathrm{M}_d(\mathrm{End}^0(Z))$, we get an isomorphism between the center of $\mathrm{End}^0(X)$ and the center of $\mathrm{End}^0(Z)$ (that does not depend on the choice of an isogeny). Also $\dim(X) = d \cdot \dim(Z)$; in particular, both d and $\dim(Z)$ divide $\dim(X)$.

1. Endomorphism algebras of abelian varieties

Throughout this paper K is a field. We write K_a for its algebraic closure and $\mathrm{Gal}(K)$ for the absolute Galois group $\mathrm{Gal}(K_a/K)$. We write ℓ for a prime different from $\mathrm{char}(K)$. If X is an abelian variety of positive dimension over K_a then we write $\mathrm{End}(X)$ for the ring of all its K_a-endomorphisms and $\mathrm{End}^0(X)$ for the corresponding $\mathbb{Q}$-algebra $\mathrm{End}(X) \otimes \mathbb{Q}$. If Y is (may be, another) abelian variety over K_a then we write $\mathrm{Hom}(X, Y)$ for the group of all K_a-homomorphisms from X to Y. It is well-known that $\mathrm{Hom}(X, Y) = 0$ if and only if $\mathrm{Hom}(Y, X) = 0$.

If n is a positive integer that is not divisible by $\mathrm{char}(K)$ then we write X_n for the kernel of multiplication by n in $X(K_a)$. It is well-known [**21**] that X_n is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2\dim(X)$. In particular, if $n = \ell$ is a prime then X_ℓ is an $\mathbb{F}_\ell$-vector space of dimension $2\dim(X)$.

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

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

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

$$\widetilde{G}_{\ell,X,K} \subset \mathrm{Aut}_{\mathbb{F}_\ell}(X_\ell)$$

of $\widetilde{G}_{\ell,X,K}$ in the $\mathbb{F}_\ell$-vector space X_ℓ.

Remark 1.1. — If $n = \ell^2$ then there is the natural surjective homomorphism

$$\tau_{\ell,X} : \widetilde{G}_{\ell^2,X,K} \twoheadrightarrow \widetilde{G}_{\ell,X,K}$$

corresponding to the field inclusion $K(X_\ell) \subset K(X_{\ell^2})$; clearly, its kernel is a finite ℓ-group. Clearly, every prime dividing $\#(\widetilde{G}_{\ell^2,X,K})$ either divides $\#(\widetilde{G}_{\ell,X,K})$ or is equal to ℓ. If A is a subgroup in $\widetilde{G}_{\ell^2,X,K}$ of index N then its image $\tau_{\ell,X}(A)$ in $\widetilde{G}_{\ell,X,K}$ is isomorphic to $A/A \bigcap \ker(\tau_{\ell,X})$. It follows easily that the index of $\tau_{\ell,X}(A)$ in $\widetilde{G}_{\ell,X,K}$ equals N/ℓ^j where ℓ^j is the index of $A \bigcap \ker(\tau_{\ell,X})$ in $\ker(\tau_{\ell,X})$. In particular, j is a nonnegative integer.

We write $\mathrm{End}_K(X)$ for the ring of all K-endomorphisms of X. We have

$$\mathbb{Z} = \mathbb{Z}\cdot 1_X \subset \mathrm{End}_K(X) \subset \mathrm{End}(X)$$

where 1_X is the identity automorphism of X. Since X is defined over K, one may associate with every $u \in \mathrm{End}(X)$ and $\sigma \in \mathrm{Gal}(K)$ an endomorphism ${}^{\sigma}u \in \mathrm{End}(X)$ such that ${}^{\sigma}u(x) = \sigma u(\sigma^{-1}x)$ for $x \in X(K_a)$ and we get the group homomorphism

$$\kappa_X : \mathrm{Gal}(K) \longrightarrow \mathrm{Aut}(\mathrm{End}(X)); \quad \kappa_X(\sigma)(u) = {}^{\sigma}u \quad \forall\, \sigma \in \mathrm{Gal}(K), u \in \mathrm{End}(X).$$

It is well-known that $\mathrm{End}_K(X)$ coincides with the subring of $\mathrm{Gal}(K)$-invariants in $\mathrm{End}(X)$, *i.e.*, $\mathrm{End}_K(X) = \{u \in \mathrm{End}(X) \mid {}^{\sigma}u = u \quad \forall\, \sigma \in \mathrm{Gal}(K)\}$. It is also well-known that $\mathrm{End}(X)$ (viewed as a group with respect to addition) is a free commutative group of finite rank and $\mathrm{End}_K(X)$ is its *pure* subgroup, *i.e.*, the quotient $\mathrm{End}(X)/\mathrm{End}_K(X)$ is also a free commutative group of finite rank. All endomorphisms of X are defined over a finite separable extension of K. More precisely [**31**], if $n \geqslant 3$ is a positive integer not divisible by $\mathrm{char}(K)$ then all the endomorphisms of X are defined over $K(X_n)$; in particular,

$$\mathrm{Gal}(K(X_n)) \subset \ker(\kappa_X) \subset \mathrm{Gal}(K).$$

This implies that if $\Gamma_K := \kappa_X(\mathrm{Gal}(K)) \subset \mathrm{Aut}(\mathrm{End}(X))$ then there exists a surjective homomorphism $\kappa_{X,n} : \widetilde{G}_{n,X} \twoheadrightarrow \Gamma_K$ such that the composition

$$\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(K(X_n)/K) = \widetilde{G}_{n,X} \xrightarrow{\kappa_{X,n}} \Gamma_K$$

coincides with κ_X and

$$\mathrm{End}_K(X) = \mathrm{End}(X)^{\Gamma_K}.$$

Clearly, $\mathrm{End}(X)$ leaves invariant the subgroup $X_\ell \subset X(K_a)$. It is well-known that $u \in \mathrm{End}(X)$ kills X_ℓ (*i.e.* $u(X_\ell) = 0$) if and only if $u \in \ell\cdot\mathrm{End}(X)$. This gives us a natural embedding

$$\mathrm{End}_K(X)\otimes\mathbb{Z}/\ell\mathbb{Z} \subset \mathrm{End}(X)\otimes\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathrm{End}_{\mathbb{F}_\ell}(X_\ell);$$

the image of $\mathrm{End}_K(X)\otimes\mathbb{Z}/\ell\mathbb{Z}$ lies in the centralizer of the Galois group, *i.e.*, we get an embedding

$$\mathrm{End}_K(X)\otimes\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathrm{End}_{\mathrm{Gal}(K)}(X_\ell) = \mathrm{End}_{\widetilde{G}_{\ell,X,K}}(X_\ell).$$

The next easy assertion seems to be well-known (compare with Prop. 3 and its proof on pp. 107–108 in [**19**]) but quite useful.

Lemma 1.2. — *If* $\mathrm{End}_{\widetilde{G}_{\ell,X,K}}(X_\ell) = \mathbb{F}_\ell$ *then* $\mathrm{End}_K(X) = \mathbb{Z}$.

Proof. — It follows that the $\mathbb{F}_\ell$-dimension of $\mathrm{End}_K(X)\otimes\mathbb{Z}/\ell\mathbb{Z}$ does not exceed 1. This means that the rank of the free commutative group $\mathrm{End}_K(X)$ does not exceed 1 and therefore is 1. Since $\mathbb{Z}\cdot 1_X \subset \mathrm{End}_K(X)$, it follows easily that $\mathrm{End}_K(X) = \mathbb{Z}\cdot 1_X = \mathbb{Z}$. □

Lemma 1.3. — *If* $\mathrm{End}_{\widetilde{G}_{\ell,X,K}}(X_\ell)$ *is a field then* $\mathrm{End}_K(X)$ *has no zero divisors, i.e.,* $\mathrm{End}_K(X)\otimes\mathbb{Q}$ *is a division algebra over* $\mathbb{Q}$.

Proof. — It follows that $\mathrm{End}_K(X)\otimes\mathbb{Z}/\ell\mathbb{Z}$ is also a field and therefore has no zero divisors. Suppose that u,v are non-zero elements of $\mathrm{End}_K(X)$ with $uv=0$. Dividing (if possible) u and v by suitable powers of ℓ in $\mathrm{End}_K(X)$, we may assume that both u and v do not lie in $\ell\,\mathrm{End}_K(X)$ and induce non-zero elements in $\mathrm{End}_K(X)\otimes\mathbb{Z}/\ell\mathbb{Z}$ with zero product. Contradiction. □

Let us put $\mathrm{End}^0(X) := \mathrm{End}(X)\otimes\mathbb{Q}$. Then $\mathrm{End}^0(X)$ is a semisimple finite-dimensional $\mathbb{Q}$-algebra [**21**, §21]. Clearly, the natural map $\mathrm{Aut}(\mathrm{End}(X))\to\mathrm{Aut}(\mathrm{End}^0(X))$ is an embedding. This allows us to view κ_X as a homomorphism

$$\kappa_X:\mathrm{Gal}(K)\longrightarrow\mathrm{Aut}(\mathrm{End}(X))\subset\mathrm{Aut}(\mathrm{End}^0(X)),$$

whose image coincides with $\Gamma_K\subset\mathrm{Aut}(\mathrm{End}(X))\subset\mathrm{Aut}(\mathrm{End}^0(X))$; the subalgebra $\mathrm{End}^0(X)^{\Gamma_K}$ of Γ_K-invariants coincides with $\mathrm{End}_K(X)\otimes\mathbb{Q}$.

Remark 1.4

(i) Let us split the semisimple $\mathbb{Q}$-algebra $\mathrm{End}^0(X)$ into a finite direct product $\mathrm{End}^0(X)=\prod_{s\in\mathcal{I}}D_s$ of simple $\mathbb{Q}$-algebras D_s. (Here $\mathcal{I}$ is identified with the set of minimal two-sided ideals in $\mathrm{End}^0(X)$.) Let e_s be the identity element of D_s. One may view e_s as an idempotent in $\mathrm{End}^0(X)$. Clearly,

$$1_X=\sum_{s\in\mathcal{I}}e_s\in\mathrm{End}^0(X),\quad e_se_t=0\ \forall\, s\neq t.$$

There exists a positive integer N such that all $N\cdot e_s$ lie in $\mathrm{End}(X)$. We write X_s for the image $X_s:=(Ne_s)(X)$; it is an abelian subvariety in X of positive dimension. Clearly, the sum map

$$\pi_X:\prod_s X_s\longrightarrow X,\quad (x_s)\longmapsto\sum_s x_s$$

is an isogeny. It is also clear that the intersection $D_s\bigcap\mathrm{End}(X)$ leaves $X_s\subset X$ invariant. This gives us a natural identification $D_s\cong\mathrm{End}^0(X_s)$. One may easily check that each X_s is isogenous to a self-product of (absolutely) simple abelian variety. Clearly, if $s\neq t$ then $\mathrm{Hom}(X_s,X_t)=0$.

(ii) We write C_s for the center of D_s. Then C_s coincides with the center of $\mathrm{End}^0(X_s)$ and is therefore either a totally real number field of degree dividing $\dim(X_s)$ or a CM-field of degree dividing $2\dim(X_s)$ [**21**, p. 202]; the center C of $\mathrm{End}^0(X)$ coincides with $\prod_{s\in\mathcal{I}}C_s=\oplus_{s\in S}C_s$.

(iii) All the sets

$$\{e_s\mid s\in\mathcal{I}\}\subset\oplus_{s\in\mathcal{I}}\mathbb{Q}\cdot e_s\subset\oplus_{s\in\mathcal{I}}C_s=C$$

are stable under the Galois action $\mathrm{Gal}(K) \xrightarrow{\kappa_X} \mathrm{Aut}(\mathrm{End}^0(X))$. In particular, there is a continuous homomorphism from $\mathrm{Gal}(K)$ to the group $\mathrm{Perm}(\mathcal{I})$ of permutations of $\mathcal{I}$ such that its kernel contains $\ker(\kappa_X)$ and

$$e_{\sigma(s)} = \kappa_X(\sigma)(e_s) = {}^{\sigma}e_s,\ {}^{\sigma}(C_s) = C_{\sigma(s)},\ {}^{\sigma}(D_s) = D_{\sigma(s)} \quad \forall\, \sigma \in \mathrm{Gal}(K), s \in \mathcal{I}.$$

It follows that $X_{\sigma(s)} = Ne_{\sigma(s)}(X) = \sigma(Ne_s(X)) = \sigma(X_s)$; in particular, abelian subvarieties X_s and $X_{\sigma(s)}$ have the same dimension and $u \mapsto {}^{\sigma}u$ gives rise to an isomorphism of $\mathbb{Q}$-algebras $\mathrm{End}^0(X_{\sigma(s)}) \cong \mathrm{End}^0(X_s)$.

(iv) If J is a non-empty Galois-invariant subset in $\mathcal{J}$ then the sum $\sum_{s\in J} Ne_s$ is Galois-invariant and therefore lies in $\mathrm{End}_K(X)$. If J' is another Galois-invariant subset of $\mathcal{I}$ that does not meet J then $\sum_{s\in J} Ne_s$ also lies in $\mathrm{End}_K(X)$ and $\sum_{s\in J} Ne_s \sum_{s\in J'} Ne_s = 0$. Assume that $\mathrm{End}_K(X)$ has no zero divisors. It follows that $\mathcal{I}$ must consist of one Galois orbit; in particular, all X_s have the same dimension equal to $\dim(X)/\#(\mathcal{I})$. In addition, if $t \in \mathcal{I}$, $\mathrm{Gal}(K)_t$ is the stabilizer of t in $\mathrm{Gal}(K)$ and F_t is the subfield of $\mathrm{Gal}(K)_t$-invariants in the separable closure of K then it follows easily that $\mathrm{Gal}(K)_t$ is an open subgroup of index $\#(\mathcal{I})$ in $\mathrm{Gal}(K)$, the field extension F_t/K is separable of degree $\#(\mathcal{I})$ and $\prod_{s\in S} X_s$ is isomorphic over K_a to the Weil restriction $\mathrm{Res}_{F_t/K}(X_t)$. This implies that X is isogenous over K_a to $\mathrm{Res}_{F_t/K}(X_t)$.

Theorem 1.5. — *Suppose that ℓ is a prime, K is a field of characteristic $\neq \ell$. Suppose that X is an abelian variety of positive dimension g defined over K. Assume that $\widetilde{G}_{\ell,X,K}$ contains a subgroup $\mathcal{G}$ such $\mathrm{End}_{\mathcal{G}}(X_\ell)$ is a field.*

Then one of the following conditions holds:

(a) *The center of $\mathrm{End}^0(X)$ is a field. In other words, $\mathrm{End}^0(X)$ is a simple $\mathbb{Q}$-algebra.*

(b)

(i) *The prime ℓ is odd;*

(ii) *there exist a positive integer $r > 1$ dividing g, a field F with*

$$K \subset K(X_\ell)^{\mathcal{G}} =: L \subset F \subset K(X_\ell), \quad [F : L] = r$$

and a g/r-dimensional abelian variety Y over F such that $\mathrm{End}^0(Y)$ is a simple $\mathbb{Q}$-algebra, the $\mathbb{Q}$-algebra $\mathrm{End}^0(X)$ is isomorphic to the direct sum of r copies of $\mathrm{End}^0(Y)$ and the Weil restriction $\mathrm{Res}_{F/L}(Y)$ is isogenous over K_a to X. In particular, X is isogenous over K_a to a product of g/r-dimensional abelian varieties. In addition, $\mathcal{G}$ contains a subgroup of index r;

(c)

(i) *The prime $\ell = 2$;*

(ii) *there exist a positive integer $r > 1$ dividing g, fields L and F with*

$$K \subset K(X_4)^{\mathcal{G}} \subset L \subset F \subset K(X_4), \quad [F : L] = r$$

and a g/r-dimensional abelian variety Y over F such that $\mathrm{End}^0(Y)$ is a simple $\mathbb{Q}$-algebra, the $\mathbb{Q}$-algebra $\mathrm{End}^0(X)$ is isomorphic to the direct sum of r copies of $\mathrm{End}^0(Y)$ and the Weil restriction $\mathrm{Res}_{F/L}(Y)$ is isogenous over K_a to X. In particular, X is isogenous over K_a to a product of g/r-dimensional abelian varieties.In addition, there exists a nonnegative integer j such that 2^j divides r and $\mathcal{G}$ contains a subgroup of index $r/2^j > 1$.

Proof. — We will use notations of Remark 1.4. Let us put $n = \ell$ if ℓ is odd and $n = 4$ if $\ell = 2$. Replacing K by $K(X_\ell)^{\mathcal{G}}$, we may and will assume that

$$\widetilde{G}_{\ell,X,K} = \mathcal{G}.$$

If ℓ is odd then let us put $L = K$ and $H := \mathrm{Gal}(K(X_\ell)/K) = \mathcal{G} = \mathrm{Gal}(L(X_\ell)/L)$.

If $\ell = 2$ then we choose a subgroup $\mathcal{H} \subset \widetilde{G}_{4,X,K}$ of smallest possible order such that $\tau_{2,X}(\mathcal{H}) = \widetilde{G}_{2,X,K} = \mathcal{G}$ and put $L := K(X_4)^{\mathcal{H}} \subset K(X_4)$. It follows easily that $L(X_4) = K(X_4)$ and $\mathrm{Gal}(L(X_2)/L) = \mathrm{Gal}(K(X_2)/K)$, *i.e.*,

$$\mathcal{H} = \widetilde{G}_{4,X,L}, \quad \widetilde{G}_{2,X,L} = \mathcal{G}.$$

The minimality property of $\mathcal{H}$ combined with Remark 1.1 implies that if $H \subset \widetilde{G}_{4,X,L}$ is a subgroup of index $r > 1$ then $\tau_{2,X}(H)$ has index $r/2^j > 1$ in $\widetilde{G}_{2,X,L}$ for some nonnegative index j.

In light of Lemma 1.3, $\mathrm{End}_L(X)$ has no zero divisors. It follows from Remark 1.4(iv) that $\mathrm{Gal}(L)$ acts on $\mathcal{I}$ transitively. Let us put $r = \#(\mathcal{I})$. If $r = 1$ then $\mathcal{I}$ is a singleton and $\mathcal{I} = \{s\}, X = X_s, \mathrm{End}^0(X) = D_s, C = C_s$. This means that assertion (a) of Theorem 1.5 holds true.

Further we assume that $r > 1$. Let us choose $t \in \mathcal{I}$ and put $Y := X_t$. If $F := F_t$ is the subfield of $\mathrm{Gal}(L)_t$-invariants in the separable closure of K then it follows from Remark 1.4(iv) that F_t/L is a separable degree r extension, Y is defined over F and X is isogenous over $L_a = K_a$ to $\mathrm{Res}_{F/L}(Y)$.

Recall (Remark 1.4(iii)) that $\ker(\kappa_X)$ acts trivially on $\mathcal{I}$. It follows that $\mathrm{Gal}(L(X_n))$ acts trivially on $\mathcal{I}$. This implies that $\mathrm{Gal}(L(X_n))$ lies in $\mathrm{Gal}(L)_t$. Recall that $\mathrm{Gal}(L)_t$ is an open subgroup of index r in $\mathrm{Gal}(L)$ and $\mathrm{Gal}(L(X_n))$ is a normal open subgroup in $\mathrm{Gal}(L)$. It follows that $H := \mathrm{Gal}(L)_t/\mathrm{Gal}(L(X_n))$ is a subgroup of index r in

$$\mathrm{Gal}(L)/\mathrm{Gal}(L(X_n)) = \mathrm{Gal}(L(X_n)/L) = \widetilde{G}_{n,X,L}.$$

If ℓ is odd then $n = \ell$ and $\widetilde{G}_{n,X,L} = \widetilde{G}_{\ell,X,L} = \mathcal{G}$ contains a subgroup of index $r > 1$. It follows from Remark 1.4 that assertion (b) of Theorem 1.5 holds true.

If $\ell = 2$ then $n = 4$ and $\widetilde{G}_{n,X,L} = \widetilde{G}_{4,X,L}$ contains a subgroup H of index $r > 1$. But in this case we know (see the very beginning of this proof) that $\widetilde{G}_{2,X,L} = \mathcal{G}$ and $\tau_{2,X}(H)$ has index $r/2^j > 1$ in $\widetilde{G}_{2,X,L}$ for some nonnegative integer j. It follows from Remark 1.4 that assertion (c) of Theorem 1.5 holds true. ☐

Before stating our next result, recall that a *perfect* finite group $\mathcal{G}$ with center $\mathcal{Z}$ is called *quasi-simple* if the quotient $\mathcal{G}/\mathcal{Z}$ is a simple nonabelian group. Let H be a non-central normal subgroup in quasi-simple $\mathcal{G}$. Then the image of H in simple $\mathcal{G}/\mathcal{Z}$ is a non-trivial normal subgroup and therefore coincides with $\mathcal{G}/\mathcal{Z}$. This means that $\mathcal{G} = \mathcal{Z}H$. Since $\mathcal{G}$ is perfect, $\mathcal{G} = [\mathcal{G},\mathcal{G}] = [H,H] \subset H$. It follows that $\mathcal{G} = H$. In other words, every proper normal subgroup in a quasi-simple group is central.

Theorem 1.6. — *Suppose that ℓ is a prime, K is a field of characteristic different from ℓ. Suppose that X is an abelian variety of positive dimension g defined over K. Let us assume that $\widetilde{G}_{\ell,X,K}$ contains a subgroup $\mathcal{G}$ that enjoys the following properties:*

(i) $\mathrm{End}_{\mathcal{G}}(X_\ell) = \mathbb{F}_\ell$;

(ii) *The group $\mathcal{G}$ does not contain a subgroup of index* 2.

(iii) *The only normal subgroup in $\mathcal{G}$ of index dividing g is $\mathcal{G}$ itself.*

Then one of the following two conditions (a) and (b) holds:

(a) *There exists a positive integer $r > 2$ such that:*

(a0) *r divides g and X is isogenous over K_a to a product of g/r-dimensional abelian varieties;*

(a1) *If ℓ is odd then $\mathcal{G}$ contains a subgroup of index r;*

(a2) *If $\ell = 2$ then there exists a nonnegative integer j such that $\mathcal{G}$ contains a subgroup of index $r/2^j > 1$.*

(b)

(b1) *The center of* $\mathrm{End}^0(X)$ *coincides with* $\mathbb{Q}$. *In other words,* $\mathrm{End}^0(X)$ *is a matrix algebra either over $\mathbb{Q}$ or over a quaternion $\mathbb{Q}$-algebra.*

(b2) *If $\mathcal{G}$ is perfect and* $\mathrm{End}^0(X)$ *is a matrix algebra over a quaternion $\mathbb{Q}$-algebra $\mathbb{H}$ then $\mathbb{H}$ is unramified at every prime not dividing $\#(\mathcal{G})$.*

(b3) *Let $\mathcal{Z}$ be the center of $\mathcal{G}$. Suppose that $\mathcal{G}$ is quasi-simple, i.e. it is perfect and the quotient $\mathcal{G}/\mathcal{Z}$ is a simple group. If* $\mathrm{End}^0(X) \neq \mathbb{Q}$ *then there exist a perfect finite (multiplicative) subgroup* $\Pi \subset \mathrm{End}^0(X)^*$ *and a surjective homomorphism* $\Pi \twoheadrightarrow \mathcal{G}/\mathcal{Z}$ *such that every prime dividing* $\#(\Pi)$ *also divides* $\#(\mathcal{G})$.

Proof. — Let us assume that the center C of $\mathrm{End}^0(X)$ is not a field. Applying Theorem 1.5, we conclude that the condition (a) holds.

Assume now that the center C of $\mathrm{End}^0(X)$ is a field. We need to prove (b). Let us define n and L as in the beginning of the proof of Theorem 1.5. We have

$$\mathcal{G} = \widetilde{G}_{\ell,X,L}, \quad \mathrm{End}_{\widetilde{G}_{\ell,X,L}}(X_\ell) = \mathbb{F}_\ell.$$

In addition, if $\ell = 2$ and $H \subset \widetilde{G}_{4,X,L}$ is a subgroup of index $r > 1$ then $\tau_{2,X}(H)$ has index $r/2^j > 1$ in $\widetilde{G}_{2,X,L} = \mathcal{G}$ for some nonnegative integer j. This implies that the only normal subgroup in $\widetilde{G}_{n,X,L} = \widetilde{G}_{4,X,L}$ of index dividing g is $\widetilde{G}_{n,X,L}$ itself. It is also clear that $\widetilde{G}_{n,X,L}$ does not contain a subgroup of index 2. It follows from Remark 1.1 that if $\mathcal{G}$ is perfect then $\widetilde{G}_{4,X,L}$ is also perfect and every prime dividing $\#(\widetilde{G}_{4,X,L})$

must divide $\#(\mathcal{G})$, because (thanks to a celebrated theorem of Feit-Thompson) $\#(\mathcal{G})$ must be even. (If ℓ is odd then $n = \ell$ and $\widetilde{G}_{n,X,L} = \mathcal{G}$.)

It follows from Lemma 1.2 that $\mathrm{End}_L(X) = \mathbb{Z}$ and therefore $\mathrm{End}_L(X) \otimes \mathbb{Q} = \mathbb{Q}$. Recall that $\mathrm{End}_L(X) \otimes \mathbb{Q} = \mathrm{End}^0(X)^{\mathrm{Gal}(L)}$ and $\kappa_X : \mathrm{Gal}(L) \to \mathrm{Aut}(\mathrm{End}^0(X))$ kills $\mathrm{Gal}(L(X_n))$. This gives rise to the homomorphism

$$\kappa_{X,n} : \widetilde{G}_{n,X,L} = \mathrm{Gal}(L(X_n)/L) = \mathrm{Gal}(L)/\,\mathrm{Gal}(L(X_n)) \longrightarrow \mathrm{Aut}(\mathrm{End}^0(X))$$

with $\kappa_{X,n}(\widetilde{G}_{n,X,L}) = \kappa_X(\mathrm{Gal}(L)) \subset \mathrm{Aut}(\mathrm{End}^0(X))$ and $\mathrm{End}^0(X)^{\widetilde{G}_{n,X,L}} = \mathbb{Q}$. Clearly, the action of $\widetilde{G}_{n,X,L}$ on $\mathrm{End}^0(X)$ leaves invariant the center C and therefore defines a homomorphism $\widetilde{G}_{n,X,L} \to \mathrm{Aut}(C)$ with $C^{\widetilde{G}_{n,X,L}} = \mathbb{Q}$. It follows that $C/\mathbb{Q}$ is a Galois extension and the corresponding map

$$\widetilde{G}_{n,X,L} \longrightarrow \mathrm{Aut}(C) = \mathrm{Gal}(C/\mathbb{Q})$$

is surjective. Recall that C is either a totally real number field of degree dividing g or a purely imaginary quadratic extension of a totally real number field C^+ where $[C^+ : \mathbb{Q}]$ divides g . In the case of totally real C let us put $C^+ := C$. Clearly, in both cases C^+ is the largest totally real subfield of C and therefore the action of $\widetilde{G}_{n,X,L}$ leaves C^+ stable, *i.e.* $C^+/\mathbb{Q}$ is also a Galois extension. Let us put $r := [C^+ : \mathbb{Q}]$. It is known [**21**, p. 202] that r divides g. Clearly, the Galois group $\mathrm{Gal}(C^+/\mathbb{Q})$ has order r and we have a surjective homomorphism (composition)

$$\widetilde{G}_{n,X,L} \twoheadrightarrow \mathrm{Gal}(C/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(C^+/\mathbb{Q})$$

of $\widetilde{G}_{n,X,L}$ onto order r group $\mathrm{Gal}(C^+/\mathbb{Q})$. Clearly, its kernel is a normal subgroup of index r in $\widetilde{G}_{n,X,L}$. This contradicts our assumption if $r > 1$. Hence $r = 1$, *i.e.* $C^+ = \mathbb{Q}$. It follows that either $C = \mathbb{Q}$ or C is an imaginary quadratic field and $\mathrm{Gal}(C/\mathbb{Q})$ is a group of order 2. In the latter case we get the surjective homomorphism from $\widetilde{G}_{n,X,L}$ onto $\mathrm{Gal}(C/\mathbb{Q})$, whose kernel is a subgroup of order 2 in $\widetilde{G}_{n,X,L}$, which does not exist. This proves that $C = \mathbb{Q}$. It follows from Albert's classification [**21**, p. 202] that $\mathrm{End}^0(X)$ is either a matrix algebra $\mathbb{Q}$ or a matrix algebra $\mathrm{M}_d(\mathbb{H})$ where $\mathbb{H}$ is a quaternion $\mathbb{Q}$-algebra. This proves assertion (b1) of Theorem 1.6.

Assume, in addition, that $\mathcal{G}$ is perfect. Then, as we have already seen, $\widetilde{G}_{n,X,L}$ is also perfect. This implies that $\Gamma := \kappa_{X,n}(\widetilde{G}_{n,X,L})$ is a finite perfect subgroup of $\mathrm{Aut}(\mathrm{End}^0(X))$ and every prime dividing $\#(\Gamma)$ must divide $\#(\widetilde{G}_{n,X,L})$ and therefore divides $\#(\mathcal{G})$. Clearly,

$$\mathbb{Q} = \mathrm{End}^0(X)^{\Gamma}. \tag{1}$$

Assume that $\mathrm{End}^0(X) \neq \mathbb{Q}$. Then $\Gamma \neq \{1\}$. Since $\mathrm{End}^0(X)$ is a central simple $\mathbb{Q}$-algebra, all its automorphisms are inner, *i.e.*, $\mathrm{Aut}(\mathrm{End}^0(X)) = \mathrm{End}^0(X)^*/\mathbb{Q}^*$. Let $\Delta \twoheadrightarrow \Gamma$ be the universal central extension of Γ. It is well-known that Δ is a finite perfect group and the set of prime divisors of $\#(\Delta)$ coincides with the set of prime divisors of $\#(\Gamma)$. The universality property implies that the inclusion map $\Gamma \subset \mathrm{End}^0(X)^*/\mathbb{Q}^*$ lifts (uniquely) to a homomorphism $\pi : \Delta \to \mathrm{End}^0(X)^*$. The equality (1) means that the centralizer of $\pi(\Delta)$ in $\mathrm{End}^0(X)$ coincides with $\mathbb{Q}$ and therefore $\ker(\pi)$ does not coincide with Δ. It follows that the image Γ_0 of $\ker(\pi)$ in Γ does not coincide with the whole Γ. It also follows that if $\mathbb{Q}[\Delta]$ is the group $\mathbb{Q}$-algebra of Δ then π induces the $\mathbb{Q}$-algebra homomorphism $\pi : \mathbb{Q}[\Delta] \to \mathrm{End}^0(X)$ such that the centralizer of the image $\pi(\mathbb{Q}[\Delta])$ in $\mathrm{End}^0(X)$ coincides with $\mathbb{Q}$.

I claim that $\pi(\mathbb{Q}[\Delta]) = \mathrm{End}^0(X)$ and therefore $\mathrm{End}^0(X)$ is isomorphic to a direct summand of $\mathbb{Q}[\Delta]$. This claim follows easily from the next lemma that will be proven later in this section.

Lemma 1.7. — *Let E be a field of characteristic zero, T a semisimple finite-dimensional E-algebra, S a finite-dimensional central simple E-algebra, $\beta : T \to S$ an E-algebra homomorphism that sends 1 to 1. Suppose that the centralizer of the image $\beta(T)$ in S coincides with the center E. Then β is surjective, i.e. $\beta(T) = S$.*

In order to prove (b2), let us assume that $\mathrm{End}^0(X) = \mathrm{M}_d(\mathbb{H})$ where $\mathbb{H}$ is a quaternion $\mathbb{Q}$-algebra. Then $\mathrm{M}_d(\mathbb{H})$ is isomorphic to a direct summand of $\mathbb{Q}[\Delta]$. On the other hand, it is well-known that if q is a prime not dividing $\#(\Delta)$ then $\mathbb{Q}_q[\Delta] = \mathbb{Q}[\Delta] \otimes_{\mathbb{Q}} \mathbb{Q}_q$ is a direct sum of matrix algebras over (commutative) fields. It follows that $\mathrm{M}_d(\mathbb{H}) \otimes_{\mathbb{Q}} \mathbb{Q}_q$ also splits. This proves the assertion (b2).

In order to prove (b3), let us assume that $\mathcal{G}$ is a quasi-simple finite group with center $\mathcal{Z}$. Let us put $\Pi := \pi(\Delta) \subset \mathrm{End}^0(X)^*$. We are going to construct a surjective homomorphism $\Pi \twoheadrightarrow \mathcal{G}/\mathcal{Z}$. In order to do that, it suffices to construct a surjective homomorphism $\Gamma \twoheadrightarrow \mathcal{G}/\mathcal{Z}$. Recall that there are surjective homomorphisms

$$\tau : \widetilde{G}_{n,X,L} \longrightarrow\!\!\!\!\!\rightarrow \widetilde{G}_{\ell,X,L} = \mathcal{G}, \quad \kappa_{X,n} : \widetilde{G}_{n,X,L} \longrightarrow\!\!\!\!\!\rightarrow \Gamma.$$

(If ℓ is odd then τ is the identity map; if $\ell = 2$ then $\tau = \tau_{2,X}$.) Let H_0 be the kernel of $\kappa_{X,n} : \widetilde{G}_{n,X,L} \twoheadrightarrow \Gamma$. Clearly,

$$\widetilde{G}_{n,X,L}/H_0 \cong \Gamma. \tag{2}$$

Since $\Gamma \neq \{1\}$, we have $H_0 \neq \widetilde{G}_{n,X,L}$. It follows that $\tau(H_0) \neq \mathcal{G}$. The surjectivity of $\tau : \widetilde{G}_{n,X,L} \twoheadrightarrow \mathcal{G}$ implies that $\tau(H_0)$ is normal in $\mathcal{G}$ and therefore lies in the center $\mathcal{Z}$. This gives us the surjective homomorphisms

$$\widetilde{G}_{n,X,L}/H_0 \longrightarrow\!\!\!\!\!\rightarrow \tau(\widetilde{G}_{n,X,L})/\tau(H_0) = \mathcal{G}/\tau(H_0) \longrightarrow\!\!\!\!\!\rightarrow \mathcal{G}/\mathcal{Z},$$

whose composition is a surjective homomorphism $\widetilde{G}_{n,X,L}/H_0 \twoheadrightarrow \mathcal{G}/\mathcal{Z}$. Using (2), we get the desired surjective homomorphism $\Gamma \twoheadrightarrow \mathcal{G}/\mathcal{Z}$. □

Proof of Lemma 1.7. — Replacing E by its algebraic closure E_a and tensoring T and S by E_a, we may and will assume that E is algebraically closed. Then $S = \mathrm{M}_n(E)$ for some positive integer n. Clearly, $\beta(T)$ is a direct sum of say, b matrix algebras over E and the center of $\beta(T)$ is isomorphic to a direct sum of b copies of E. In particular, if $b > 1$ then the centralizer of $\beta(T)$ in S contains the b-dimensional center of $\beta(T)$ which gives us the contradiction. So, $b = 1$ and $\beta(T) \cong \mathrm{M}_k(E)$ for some positive integer k. Clearly, $k \leqslant n$; if the equality holds then we are done. Assume that $k < n$: we need to get a contradiction. So, we have

$$1 \in E \subset \beta(T) \cong \mathrm{M}_k(E) \hookrightarrow \mathrm{M}_n(E) = S.$$

This provides E^n with a structure of faithful $\beta(T)$-module in such a way that E^n does not contain a non-zero submodule with trivial (zero) action of $\beta(T)$. Since $\beta(T) \cong \mathrm{M}_k(E)$, the $\beta(T)$-module E^n splits into a direct sum of say, e copies of a simple faithful $\beta(T)$-module W with $\dim_E(W) = k$. Clearly, $e = n/k > 1$. It follows easily that the centralizer of $\beta(T)$ in $S = \mathrm{M}_n(E)$ coincides with

$$\mathrm{End}_{\beta(T)}(W^e) = \mathrm{M}_e(\mathrm{End}_{\beta(T)}(W)) = \mathrm{M}_e(E)$$

and has E-dimension $e^2 > 1$. Contradiction. □

Corollary 1.8. — *Suppose that ℓ is a prime, K is a field of characteristic different from ℓ. Suppose that X is an abelian variety of positive dimension g defined over K. Let us assume that $\widetilde{G}_{\ell,X,K}$ contains a perfect subgroup $\mathcal{G}$ that enjoys the following properties:*

(a) $\mathrm{End}_{\mathcal{G}}(X_\ell) = \mathbb{F}_\ell$*;*

(b) *The only subgroup of index dividing g in $\mathcal{G}$ is $\mathcal{G}$ itself.*

If g is odd then either $\mathrm{End}^0(X)$ *is a matrix algebra over $\mathbb{Q}$ or $p = \mathrm{char}(K) > 0$ and* $\mathrm{End}^0(X)$ *is a matrix algebra $\mathrm{M}_d(\mathbb{H}_p)$ over a quaternion $\mathbb{Q}$-algebra $\mathbb{H}_p$ that is ramified exactly at p and ∞ and $d > 1$. In particular, if* $\mathrm{char}(K)$ *does not divide $\#(\mathcal{G})$ then* $\mathrm{End}^0(X)$ *is a matrix algebra over $\mathbb{Q}$.*

Proof of Corollary 1.8. — Let us assume that $\mathrm{End}^0(X)$ is *not* isomorphic to a matrix algebra over $\mathbb{Q}$. Then $\mathrm{End}^0(X)$ is (isomorphic to) a matrix algebra $\mathrm{M}_d(\mathbb{H})$ over a quaternion $\mathbb{Q}$-algebra $\mathbb{H}$. This means that there exists an absolutely simple abelian variety Y over K_a such that X is isogenous to Y^d and $\mathrm{End}^0(Y) = \mathbb{H}$. Clearly, $\dim(Y)$ is odd. It follows from Albert's classification [**21**, p. 202] that $p := \mathrm{char}(K_a) = \mathrm{char}(K) > 0$. By Lemma 4.3 of [**23**], if there exists a prime $q \neq p$ such that $\mathbb{H}$ is unramified at q then $4 = \dim_{\mathbb{Q}} \mathbb{H}$ divides $2\dim(Y)$. Since $\dim(Y)$ is odd, $2\dim(Y)$ is not divisible by 4 and therefore $\mathbb{H}$ is unramified at all primes different from p. It follows from the theorem of Hasse-Brauer-Noether that $\mathbb{H} \cong \mathbb{H}_p$.

Now, assume that $d = 1$, *i.e.* $\mathrm{End}^0(X) = \mathbb{H}_p$. We know that $\mathrm{End}^0(X)^* = \mathbb{H}_p^*$ contains a nontrivial finite perfect group Π. But this contradicts to the following elementary statement, whose proof will be given later in this section.

Lemma 1.9. — *Every finite subgroup in $\mathbb{H}_p^*$ is solvable.*

Hence $\mathrm{End}^0(X) \neq \mathbb{H}_p$, *i.e.* $d > 1$.

Assume now that p does *not* divide $\#(\mathcal{G})$. It follows from Theorem 1.6 that $\mathbb{H}$ is unramified at p. This implies that $\mathbb{H}$ can be ramified only at ∞ which could not be the case. The obtained contradiction proves that $\mathrm{End}^0(X)$ is a matrix algebra over $\mathbb{Q}$. □

Proof of Lemma 1.9. — If $p \neq 2$ then $\mathbb{H}_p^* \subset (\mathbb{H}_p \otimes_{\mathbb{Q}} \mathbb{Q}_2)^* \cong \mathrm{GL}(2, \mathbb{Q}_2)$ and if $p = 2$ then $\mathbb{H}_2^* \subset (\mathbb{H}_2 \otimes_{\mathbb{Q}} \mathbb{Q}_3)^* \cong \mathrm{GL}(2, \mathbb{Q}_3)$. Since every finite subgroup in $\mathrm{GL}(2, \mathbb{Q}_2)$ (resp. $\mathrm{GL}(2, \mathbb{Q}_3)$) is conjugate to a finite subgroup in $\mathrm{GL}(2, \mathbb{Z}_2)$ (resp. $\mathrm{GL}(2, \mathbb{Z}_3)$), it suffices to check that every finite subgroup in $\mathrm{GL}(2, \mathbb{Z}_2)$ and $\mathrm{GL}(2, \mathbb{Z}_3)$ is solvable.

Recall that both $\mathrm{GL}(2, \mathbb{F}_2)$ and $\mathrm{GL}(2, \mathbb{F}_3)$ are solvable and use the Minkowski-Serre lemma ([**28**, pp. 124–125]; see also [**32**]). This lemma asserts, in particular, that if q is an odd prime then the kernel of the reduction map $\mathrm{GL}(n, \mathbb{Z}_q) \to \mathrm{GL}(n, \mathbb{F}_q)$ does not contain nontrivial elements of finite order and that all periodic elements in the kernel of the reduction map $\mathrm{GL}(n, \mathbb{Z}_2) \to \mathrm{GL}(n, \mathbb{F}_2)$ have order 1 or 2.

Indeed, every finite subgroup $\Pi \subset \mathrm{GL}(2, \mathbb{Z}_3)$ maps injectively in $\mathrm{GL}(2, \mathbb{F}_3)$ and therefore is solvable. If $\Pi \subset \mathrm{GL}(2, \mathbb{Z}_2)$ is a finite subgroup then the kernel of the reduction map $\Pi \to \mathrm{GL}(2, \mathbb{F}_2)$ consists of elements of order 1 or 2 and therefore is an elementary commutative 2-group. Since the image of the reduction map is solvable, we conclude that Π is solvable. □

Corollary 1.10. — *Suppose that ℓ is a prime, K is a field of characteristic different from ℓ. Suppose that X is an abelian variety of dimension g defined over K. Let us put $g' = \max(2, g)$. Let us assume that $\widetilde{G}_{\ell,X,K}$ contains a perfect subgroup $\mathcal{G}$ that enjoys the following properties:*

(a) $\mathrm{End}_{\mathcal{G}}(X_\ell) = \mathbb{F}_\ell$;

(b) *The only subgroup of index dividing g in $\mathcal{G}$ is $\mathcal{G}$ itself.*

(c) *If $\mathcal{Z}$ is the center of $\mathcal{G}$ then $\mathcal{G}/\mathcal{Z}$ is a simple nonabelian group.*

Suppose that $\mathrm{End}^0(X) \cong \mathrm{M}_d(\mathbb{Q})$ *with $d > 1$. Then there exist a perfect finite subgroup $\Pi \subset \mathrm{GL}(d, \mathbb{Z})$ and a surjective homomorphism $\Pi \twoheadrightarrow \mathcal{G}/\mathcal{Z}$ such that every prime dividing $\#(\Pi)$ also divides $\#(\mathcal{G})$.*

Proof of Corollary 1.10. — Clearly, $\mathrm{End}^0(X)^* = \mathrm{GL}(n, \mathbb{Q})$. One has only to recall that every finite subgroup in $\mathrm{GL}(n, \mathbb{Q})$ is conjugate to a finite subgroup in $\mathrm{GL}(n, \mathbb{Z})$ and apply Theorem 1.6(iii). □

2. Homomorphisms of abelian varieties

Theorem 2.1. — *Let ℓ be a prime, K a field of characteristic different from ℓ, X and Y abelian varieties of positive dimension defined over K. Suppose that the following conditions hold:*

(i) *The extensions $K(X_\ell)$ and $K(Y_\ell)$ are linearly disjoint over K.*

(ii) $\mathrm{End}_{\widetilde{G}_{\ell,X,K}}(X_\ell) = \mathbb{F}_\ell$.

(iii) *The centralizer of $\widetilde{G}_{\ell,Y,K}$ in $\mathrm{End}_{\mathbb{F}_\ell}(Y_\ell)$ is a field.*

Then either $\mathrm{Hom}(X, Y) = 0, \mathrm{Hom}(Y, X) = 0$ *or* $\mathrm{char}(K) > 0$ *and both abelian varieties X and Y are supersingular.*

Remark 2.2. — Theorem 2.1 was proven in [**43**] under an addititional assumption that the Galois modules X_ℓ and Y_ℓ are simple.

In order to prove Theorem 2.1, we need first to discuss the notion of Tate module. Recall [**21, 29, 47**] that this is a $\mathbb{Z}_\ell$-module $T_\ell(X)$ defined as the projective limit of Galois modules X_{ℓ^m}. It is well-known that $T_\ell(X)$ is a free $\mathbb{Z}_\ell$-module of rank $2\dim(X)$ provided with the continuous action

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

There is the natural isomorphism of Galois modules

$$X_\ell = T_\ell(X)/\ell T_\ell(X), \tag{3}$$

so one may view $\widetilde{\rho}_{\ell,X}$ as the reduction of $\rho_{\ell,X}$ modulo ℓ. Let us put

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

it is a $2\dim(X)$-dimensional $\mathbb{Q}_\ell$-vector space. The group $T_\ell(X)$ is naturally identified with the $\mathbb{Z}_\ell$-lattice in $V_\ell(X)$ and the inclusion $\mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(X)) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(X))$ allows us to view $V_\ell(X)$ as representation of $\mathrm{Gal}(K)$ over $\mathbb{Q}_\ell$. Let Y be (may be, another) abelian variety of positive dimension defined over K. Recall [**21**, § 19] that $\mathrm{Hom}(X,Y)$ is a free commutative group of finite rank. Since X and Y are defined over K, one may associate with every $u \in \mathrm{Hom}(X,Y)$ and $\sigma \in \mathrm{Gal}(K)$ an endomorphism ${}^\sigma u \in \mathrm{Hom}(X,Y)$ such that

$${}^\sigma u(x) = \sigma u(\sigma^{-1}x) \quad \forall\, x \in X(K_a)$$

and we get the group homomorphism

$$\kappa_{X,Y} : \mathrm{Gal}(K) \to \mathrm{Aut}(\mathrm{Hom}(X,Y)); \quad \kappa_{X,Y}(\sigma)(u) = {}^\sigma u \;\forall\, \sigma \in \mathrm{Gal}(K), u \in \mathrm{Hom}(X,Y),$$

which provides the finite-dimensional $\mathbb{Q}_\ell$-vector space $\mathrm{Hom}(X,Y)\otimes\mathbb{Q}_\ell$ with the natural structure of Galois module.

There is a natural structure of Galois module on the $\mathbb{Q}_\ell$-vector space

$$\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), V_\ell(Y))$$

induced by the Galois actions on $V_\ell(X)$ and $V_\ell(Y)$. On the other hand, there is a natural embedding of Galois modules [**21**, § 19],

$$\mathrm{Hom}(X,Y)\otimes\mathbb{Q}_\ell \subset \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), V_\ell(Y)),$$

whose image must be a $\mathrm{Gal}(K)$-invariant $\mathbb{Q}_\ell$-vector subspace. It is also clear that $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(X), T_\ell(Y))$ is a Galois-invariant $\mathbb{Z}_\ell$-lattice in $\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), V_\ell(Y))$. The equality (3) gives rise to a natural isomorphism of Galois modules

$$\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(X), T_\ell(Y)) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell/\ell\mathbb{Z}_\ell = \mathrm{Hom}_{\mathbb{F}_\ell}(X_\ell, Y_\ell). \tag{4}$$

Proof of Theorem 2.1. — Let $K(X_\ell, Y_\ell)$ be the compositum of the fields $K(X_\ell)$ and $K(Y_\ell)$. The linear disjointness of $K(X_\ell)$ and $K(Y_\ell)$ means that

$$\mathrm{Gal}(K(X_\ell, Y_\ell)/K) = \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K).$$

Let $X_\ell^* = \mathrm{Hom}_{\mathbb{F}_\ell}(X_\ell, \mathbb{F}_\ell)$ be the dual of X_ℓ and $\overline{\rho}^*_{n,X,K} : \mathrm{Gal}(K) \to \mathrm{Aut}(X_\ell^*)$ the dual of $\overline{\rho}_{n,X,K}$. One may easily check that $\ker(\overline{\rho}^*_{n,X,K}) = \ker(\overline{\rho}_{n,X,K})$ and therefore we have an isomorphism of the images

$$\widetilde{G}^*_{\ell,X,K} := \overline{\rho}^*_{n,X,K}(\mathrm{Gal}(K)) \cong \overline{\rho}_{n,X,K}(\mathrm{Gal}(K))) = \widetilde{G}_{\ell,X,K}.$$

One may also easily check that the centralizer of $\mathrm{Gal}(K)$ in $\mathrm{End}_{\mathbb{F}_\ell}(X_\ell^*)$ still coincides with $\mathbb{F}_\ell$. It follows that if A_1 is the $\mathbb{F}_\ell$-subalgebra in $\mathrm{End}_{\mathbb{F}_\ell}(X_\ell^*)$ generated by $\widetilde{G}^*_{\ell,X,K}$ then its centralizer in $\mathrm{End}_{\mathbb{F}_\ell}(X_\ell^*)$ coincides with $\mathbb{F}_\ell$. Let us consider the Galois module $W_1 = \mathrm{Hom}_{\mathbb{F}_\ell}(X_\ell, Y_\ell) = X_\ell^* \otimes_{\mathbb{F}_\ell} Y_\ell$ and denote by τ the homomorphism $\mathrm{Gal}(K) \to \mathrm{Aut}(W_1)$ that defines the Galois module structure on W_1. One may easily check that τ factors through $\mathrm{Gal}(K(X_\ell, Y_\ell)/K)$ and the image of τ coincides with the image of

$$\widetilde{G}^*_{\ell,X,K} \times \widetilde{G}_{\ell,X,Y} \subset \mathrm{Aut}(X_\ell^*) \times \mathrm{Aut}(Y_\ell) \longrightarrow \mathrm{Aut}(X_\ell^* \otimes_{\mathbb{F}_\ell} Y_\ell) = \mathrm{Aut}(W_1).$$

Let A_2 be the $\mathbb{F}_\ell$-subalgebra in $\mathrm{End}_{\mathbb{F}_\ell}(Y_\ell)$ generated by $\widetilde{G}_{\ell,Y,K}$. Recall that the centralizer of $\mathrm{Gal}(K)$ in $\mathrm{End}_{\mathbb{F}_\ell}(Y_\ell)$ is a field, say $\mathbb{F}$. Clearly, the centralizer of A_2 in $\mathrm{End}_{\mathbb{F}_\ell}(Y_\ell)$ coincides with $\mathbb{F}$. One may easily check that the subalgebra of $\mathrm{End}_{\mathbb{F}_\ell}(W_1)$ generated by the image of $\mathrm{Gal}(K)$ coincides with

$$A_1 \otimes_{\mathbb{F}_\ell} A_2 \subset \mathrm{End}_{\mathbb{F}_\ell}(X_\ell^*) \otimes_{\mathbb{F}_\ell} \mathrm{End}_{\mathbb{F}_\ell}(Y_\ell) = \mathrm{End}_F(X_\ell^* \otimes_{\mathbb{F}_\ell} Y_\ell) = \mathrm{End}_{\mathbb{F}_\ell}(W_1).$$

It follows from Lemma (10.37) on p. 252 of [**3**] that the centralizer of $A_1 \otimes_{\mathbb{F}_\ell} A_2$ in $\mathrm{End}_F(X_\ell^* \otimes_{\mathbb{F}_\ell} Y_\ell)$ coincides with $\mathbb{F}_\ell \otimes_{\mathbb{F}_\ell} \mathbb{F} = \mathbb{F}$. This implies that the centralizer of $\mathrm{Gal}(K)$ in $\mathrm{End}_F(X_\ell^* \otimes_{\mathbb{F}_\ell} Y_\ell) = \mathrm{End}_{\mathbb{F}_\ell}(W_1)$ is the field $\mathbb{F}$.

Let us consider the $\mathbb{Q}_\ell$-vector space $V_1 = \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), V_\ell(Y))$ and the free $\mathbb{Z}_\ell$-module $T_1 = \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(X), T_\ell(Y))$ provided with the natural structure of Galois modules. Clearly, T_1 is a Galois-stable $\mathbb{Z}_\ell$-lattice in V_1. By (4), there is a natural isomorphism of Galois modules $W_1 = T_1/\ell T_1$. Let us denote by D_1 the centralizer of $\mathrm{Gal}(K)$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_1)$. Clearly, D_1 is a finite-dimensional $\mathbb{Q}_\ell$-algebra. Therefore in order to prove that D_1 is a division algebra, it suffices to check that D_1 has no zero divisors.

Suppose that D_1 has zero divisors, *i.e.* there are non-zero $u, v \in D_1$ with $uv = 0$. We have $u, v \subset D_1 \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_1)$. Multiplying u and v by proper powers of ℓ, we may and will assume that $u(T_1) \subset T_1, v(T_1) \subset T_1$ but $u(T_1)$ is *not* contained in ℓT_1 and $v(T_1)$ is *not* contained in ℓT_1. This means that u and v induce *non-zero* endomorphisms $\overline{u}, \overline{v} \in \mathrm{End}(W_1)$ that commute with $\mathrm{Gal}(K)$ and $\overline{uv} = 0$. Since both $\overline{u}$ and $\overline{v}$ are non-zero elements of the field $\mathbb{F}$, we get a contradiction that proves that D_1 has no zero divisors and therefore is a division algebra.

End of the proof of Theorem 2.1. — We may and will assume that K is finitely generated over its prime subfield (replacing K by its suitable subfield). Then the conjecture of Tate [**34**] (proven by the author in characteristic > 2 [**36, 37**], Faltings in characteristic zero [**5, 6**] and Mori in characteristic 2 [**17**]) asserts that the natural representation of $\mathrm{Gal}(K)$ in $V_\ell(Z)$ is completely reducible for any abelian variety Z over K. In particular, the natural representations of $\mathrm{Gal}(K)$ in $V_\ell(X)$ and $V_\ell(Y)$ are completely reducible. It follows easily that the dual Galois representation in $\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), \mathbb{Q}_\ell)$ is also completely reducible. Since $\mathbb{Q}_\ell$ has characteristic zero, it follows from a theorem of Chevalley [**1**, p. 88] that the Galois representation in the tensor product $\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} V_\ell(Y) = \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), V_\ell(Y)) =: V_1$ is completely reducible. The complete reducibility implies easily that V_1 is an irreducible Galois representation, because the centralizer is a division algebra. Recall that $\mathrm{Hom}(X, Y) \otimes \mathbb{Q}_\ell$ is a Galois-invariant subspace in $\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), V_\ell(Y)) = V_1$. The irreducibility of V_1 implies that either $\mathrm{Hom}(X, Y) \otimes \mathbb{Q}_\ell = 0$ or $\mathrm{Hom}(X, Y) \otimes \mathbb{Q}_\ell = V_1$.

If $\mathrm{Hom}(X, Y) \otimes \mathbb{Q}_\ell = 0$ then $\mathrm{Hom}(X, Y) = 0$ and therefore $\mathrm{Hom}(Y, X) = 0$.

If $\mathrm{Hom}(X, Y) \otimes \mathbb{Q}_\ell = V_1$ then the rank of the free commutative group $\mathrm{Hom}(X, Y)$ coincides with the dimension of the $\mathbb{Q}_\ell$-vector space V_1. Clearly, V_1 has dimension $4 \dim(X) \dim(Y)$. It is proven in proposition 3.3 of [**43**] that if A and B are abelian varieties over an algebraically closed field $\mathcal{K}$ and the rank of $\mathrm{Hom}(A, B)$ equals $4 \dim(A) \dim(B)$ then $\mathrm{char}(\mathcal{K}) > 0$ and both A and B are supersingular abelian varieties. Applying this result to X and Y, we conclude that $\mathrm{char}(K) = \mathrm{char}(K_a) > 0$ and both X and Y are supersingular abelian varieties. □

3. Hyperelliptic jacobians

In this section we deal with the case of $\ell = 2$. Suppose that $\mathrm{char}(K) \neq 2$. Let $f(x) \in K[x]$ be a polynomial of degree $n \geqslant 3$ without multiple roots. Let $\mathfrak{R}_f \subset K_a$ be the set of roots of f. Clearly, $\mathfrak{R}_f$ consists of n elements. Let $K(\mathfrak{R}_f) \subset K_a$ be the splitting field of f. Clearly, $K(\mathfrak{R}_f)/K$ is a Galois extension and we write $\mathrm{Gal}(f)$ for its Galois group $\mathrm{Gal}(K(\mathfrak{R}_f)/K)$. By definition, $\mathrm{Gal}(K(\mathfrak{R}_f)/K)$ permutes elements of $\mathfrak{R}_f$; further we identify $\mathrm{Gal}(f)$ with the corresponding subgroup of $\mathrm{Perm}(\mathfrak{R}_f)$ where $\mathrm{Perm}(\mathfrak{R}_f)$ is the group of permutations of $\mathfrak{R}_f$.

We write $\mathbb{F}_2^{\mathfrak{R}_f}$ for the n-dimensional $\mathbb{F}_2$-vector space of maps $h : \mathfrak{R}_f \to \mathbb{F}_2$. The space $\mathbb{F}_2^{\mathfrak{R}_f}$ is provided with a natural action of $\mathrm{Perm}(\mathfrak{R}_f)$ defined as follows. Each $s \in \mathrm{Perm}(\mathfrak{R}_f)$ sends a map $h : \mathfrak{R}_f \to \mathbb{F}_2$ to $sh : \alpha \mapsto h(s^{-1}(\alpha))$. The permutation module $\mathbb{F}_2^{\mathfrak{R}_f}$ contains the $\mathrm{Perm}(\mathfrak{R}_f)$-stable hyperplane

$$(\mathbb{F}_2^{\mathfrak{R}_f})^0 = \Big\{h : \mathfrak{R}_f \to \mathbb{F}_2 \mid \textstyle\sum_{\alpha \in \mathfrak{R}_f} h(\alpha) = 0\Big\}$$

and the $\mathrm{Perm}(\mathfrak{R}_f)$-invariant line $\mathbb{F}_2 \cdot 1_{\mathfrak{R}_f}$ where $1_{\mathfrak{R}_f}$ is the constant function 1. Clearly, $(\mathbb{F}_2^{\mathfrak{R}_f})^0$ contains $\mathbb{F}_2 \cdot 1_{\mathfrak{R}_f}$ if and only if n is even.

If n is even then let us define the $\mathrm{Gal}(f)$-module $Q_{\mathfrak{R}_f} := (\mathbb{F}_2^{\mathfrak{R}_f})^0/(\mathbb{F}_2 \cdot 1_{\mathfrak{R}_f})$. If n is odd then let us put $Q_{\mathfrak{R}_f} := (\mathbb{F}_2^{\mathfrak{R}_f})^0$. If $n \neq 4$ the natural representation of $\mathrm{Gal}(f)$ is faithful, because in this case the natural homomorphism $\mathrm{Perm}(\mathfrak{R}_f) \to \mathrm{Aut}_{\mathbb{F}_2}(Q_{\mathfrak{R}_f})$ is injective.

Remark 3.1. — It is known [**15**, Satz 4], that $\mathrm{End}_{\mathrm{Gal}(f)}(Q_{\mathfrak{R}_f}) = \mathbb{F}_2$ if either n is odd and $\mathrm{Gal}(f)$ acts doubly transitively on $\mathfrak{R}_f$ or n is even and $\mathrm{Gal}(f)$ acts 3-transitively on $\mathfrak{R}_f$.

The canonical surjection $\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(K(\mathfrak{R}_f)/K) = \mathrm{Gal}(f)$ provides $Q_{\mathfrak{R}_f}$ with a natural structure of $\mathrm{Gal}(K)$-module. Let C_f be the hyperelliptic curve $y^2 = f(x)$ and $J(C_F)$ its jacobian. It is well-known that $J(C_F)$ is a $[(n-1)/2]$-dimensional abelian variety defined over K. It is also well-known that the $\mathrm{Gal}(K)$-modules $J(C_f)_2$ and $Q_{\mathfrak{R}_f}$ are isomorphic (see for instance [**25, 27, 39**]). It follows that if $n \neq 4$ then

$$\mathrm{Gal}(f) = \widetilde{G}_{2,J(C_f)}.$$

It follows from Remark 3.1 that if either n is odd and $\mathrm{Gal}(f)$ acts doubly transitively on $\mathfrak{R}_f$ or n is even and $\mathrm{Gal}(f)$ acts 3-transitively on $\mathfrak{R}_f$ then

$$\mathrm{End}_{\widetilde{G}_{2,J(C_f)}}(J(C_f)_2)) = \mathbb{F}_2.$$

It is also clear that $K(J(C_f)_2)) \subset K(\mathfrak{R}_f)$. (The equality holds if $n \neq 4$.)

The next assertion follows immediately from Theorem 1.6, Corollaries 1.8 and 1.10 (applied to $X = J(C_f), \ell = 2, \mathcal{G} = \mathrm{Gal}(f)$).

Theorem 3.2. — *Let K be a field of characteristic different from 2, let $n \geqslant 5$ be an integer, $g = [(n-1)/2]$ and $f(x) \in K[x]$ a polynomial of degree n. Suppose that either n is odd and* $\mathrm{Gal}(f)$ *acts doubly transitively on $\mathfrak{R}_f$ or n is even and* $\mathrm{Gal}(f)$ *acts 3-transitively on $\mathfrak{R}_f$. Assume also that* $\mathrm{Gal}(f)$ *is a simple nonabelian group that does not contain a subgroup of index dividing g except* $\mathrm{Gal}(f)$ *itself. If g is odd then* $\mathrm{End}^0(J(C_f))$ *enjoys one of the following properties:*

(i) $\mathrm{End}^0(J(C_f))$ *is isomorphic to the matrix algebra* $\mathrm{M}_d(\mathbb{Q})$ *where d divides g. If $d > 1$ there exist a finite perfect group* $\Pi \subset \mathrm{GL}(d,\mathbb{Z})$ *and a surjective homomorphism* $\Pi \twoheadrightarrow \mathrm{Gal}(f)$ *such that every prime dividing* $\#(\Pi)$ *also divides* $\#(\mathrm{Gal}(f))$.

(ii) $p := \mathrm{char}(K)$ *is a prime dividing* $\#(\mathrm{Gal}(f))$ *and* $\mathrm{End}^0(J(C_f))$ *is isomorphic to the matrix algebra* $\mathrm{M}_d(\mathbb{H}_p)$ *where $d > 1$ divides g.*

Example 3.3. — Suppose that $n = 5$ and $\mathrm{Gal}(f)$ is the alternating group $\mathbb{A}_5$ acting doubly transitively on $\mathfrak{R}_f$. Clearly, $g = 2$ and $\mathrm{Gal}(f)$ is a simple nonabelian group without subgroups of index 2. Applying Theorem 3.2, we conclude that $\mathrm{End}^0(J(C_f))$ is either $\mathbb{Q}$ or $\mathrm{M}_2(\mathbb{Q})$ or $\mathrm{M}_2(\mathbb{H})$ where $\mathbb{H}$ is a quaternion $\mathbb{Q}$-algebra unramified outside $\{\infty, 2, 3, 5\}$; in addition $\mathbb{H} \cong \mathbb{H}_p$ if $p := \mathrm{char}(K) > 0$. Suppose that $\mathrm{End}(J(C_f)) \neq \mathbb{Z}$ and therefore $\mathrm{End}^0(J(C_f)) \neq \mathbb{Q}$. If $\mathrm{End}^0(J(C_f)) = \mathrm{M}_2(\mathbb{Q})$ then $\mathrm{GL}(2,\mathbb{Q}) = \mathrm{M}_2(\mathbb{Q})^*$ contains a finite group, whose order divides 5, which is not the case. This implies that $\mathrm{End}^0(J(C_f)) = \mathrm{M}_2(\mathbb{H})$. This means that $J(C_f)$ is supersingular and therefore $p := \mathrm{char}(K) > 0$. This implies that $p = 3$ or $p = 5$.

We conclude that either $\mathrm{End}(J(C_f) = \mathbb{Z}$ or $\mathrm{char}(K) \in \{3, 5\}$ and $J(C_f)$ is a supersingular abelian varietiy. In fact, it is known [**46**] that if $\mathrm{char}(K) = 5$ then $\mathrm{End}(J(C_f) = \mathbb{Z}$. On the other hand, one may find a supersingular $J(C_f)$ in characteristic 3 [**46**].

Example 3.3 is a special case of the following general result proven by the author [**38, 42, 46**]. *Suppose that* $n \geqslant 5$ *and* $\mathrm{Gal}(f)$ *is the alternating group* $\mathbb{A}_n$ *acting on* $\mathfrak{R}_f$. *If* $\mathrm{char}(K) = 3$ *we assume additionally that* $n \geqslant 7$. *Then* $\mathrm{End}(J(C_f) = \mathbb{Z}$.

We refer the reader to [**18, 19, 11, 12, 16, 13, 38, 40, 42, 41, 44, 45**] for a discussion of other known results about, and examples of, hyperelliptic jacobians without complex multiplication.

Corollary 3.4. — *Suppose that* $n = 7$ *and* $\mathrm{Gal}(f) = \mathrm{SL}_3(\mathbb{F}_2) \cong \mathrm{PSL}_2(\mathbb{F}_7)$ *acts doubly transitively on* $\mathfrak{R}_f$. *Then* $\mathrm{End}^0(J(C_f)) = \mathbb{Q}$ *and therefore* $\mathrm{End}(J(C_f)) = \mathbb{Z}$.

Proof. — We have $g = \dim(J(C_f)) = 3$. Since $\mathrm{PSL}_2(\mathbb{F}_7)$ is a simple nonabelian group it does not contain a subgroup of index 3. So, we may apply Theorem 3.2. We obtain that if $\mathrm{End}^0(J(C_f)) \neq \mathbb{Q}$ then either $\mathrm{End}^0(J(C_f)) = \mathrm{M}_3(\mathbb{Q})$ and there exist a finite perfect group $\Pi \subset \mathrm{GL}(3, \mathbb{Z})$ and a surjective homomorphism $\Pi \twoheadrightarrow \mathrm{Gal}(f) = \mathrm{PSL}_2(\mathbb{F}_7)$ or $\mathrm{End}^0(J(C_f)) = \mathrm{M}_3(\mathbb{H}_p)$ where $p = \mathrm{char}(K)$ is either 3 or 7. The case of $\mathrm{End}^0(J(C_f)) = \mathrm{M}_3(\mathbb{H}_p)$ means that $J(C_f)$ is supersingular, which is not true ([**46**], Th. 3.1). Hence $\mathrm{End}^0(J(C_f)) = \mathrm{M}_3(\mathbb{Q})$ and $\mathrm{GL}(3, \mathbb{Z})$ contains a finite group of order dividing 7. It follows that $\mathrm{GL}(3, \mathbb{Z})$ contains an element of order dividing 7, which is not true. The obtained contradiction proves that $\mathrm{End}^0(J(C_f)) = \mathbb{Q}$ and therefore $\mathrm{End}(J(C_f)) = \mathbb{Z}$. □

Corollary 3.5. — *Suppose that* $n = 11$ *and* $\mathrm{Gal}(f) = \mathrm{PSL}_2(\mathbb{F}_{11})$ *acts doubly transitively on* $\mathfrak{R}_f$. *Then* $\mathrm{End}^0(J(C_f)) = \mathbb{Q}$ *and therefore* $\mathrm{End}(J(C_f)) = \mathbb{Z}$.

Proof. — We have $g = \dim(J(C_f)) = 5$. It is known [**2**] that $\mathrm{PSL}_2(\mathbb{F}_{11})$ is a simple nonabelian subgroup not containing a subgroup of index 5. So, we may apply Theorem 3.2. We obtain that if $\mathrm{End}^0(J(C_f)) \neq \mathbb{Q}$ then either $\mathrm{End}^0(J(C_f)) = \mathrm{M}_5(\mathbb{Q})$ and there exist a finite perfect group $\Pi \subset \mathrm{GL}(5, \mathbb{Z})$ and a surjective homomorphism $\Pi \twoheadrightarrow \mathrm{Gal}(f) = \mathrm{PSL}_2(\mathbb{F}_{11})$ or $\mathrm{End}^0(J(C_f)) = \mathrm{M}_5(\mathbb{H}_p)$ where $p = \mathrm{char}(K)$ is either 3 or 5 or 11.

Assume that $\mathrm{End}^0(J(C_f)) = \mathrm{M}_5(\mathbb{Q})$. Then $\mathrm{GL}(5, \mathbb{Z})$ contains a finite group, whose order is divisible by 11. It follows that $\mathrm{GL}(5, \mathbb{Z})$ contains an element of order 11, which is not true. Hence $\mathrm{End}^0(J(C_f)) \neq \mathrm{M}_5(\mathbb{Q})$

Assume that $\mathrm{End}^0(J(C_f)) = \mathrm{M}_5(\mathbb{H}_p)$ where p is either 3 or 5 or 11. This implies that $J(C_f)$ is a supersingular abelian variety.

Notice that every homomorphism from simple $\mathrm{PSL}_2(\mathbb{F}_{11})$ to $\mathrm{GL}(4,\mathbb{F}_2)$ is trivial, because 11 divides $\#(\mathrm{PSL}_2(\mathbb{F}_{11}))$ but $\#(\mathrm{GL}(4,\mathbb{F}_2))$ is *not* divisible by 11. Since $4 = g-1$, it follows from Theorem 3.3 of [**46**] (applied to $g = 5, X = J(C_f), G = \mathrm{Gal}(f) = \mathrm{PSL}_2(\mathbb{F}_{11})$) that there exists a central extension $\pi_1 : G_1 \to \mathrm{PSL}_2(\mathbb{F}_{11})$ such that G_1 is perfect, $\ker(\pi_1)$ is a cyclic group of order 1 or 2 and $\mathrm{M}_5(\mathbb{H}_p)$ is a direct summand of the group $\mathbb{Q}$-algebra $\mathbb{Q}[G_1]$. It follows easily that $G_1 = \mathrm{PSL}_2(\mathbb{F}_{11})$ or $\mathrm{SL}_2(\mathbb{F}_{11})$. It is known [**10, 7**] that $\mathbb{Q}[\mathrm{PSL}_2(\mathbb{F}_{11})]$ is a direct sum of matrix algebras over fields. Hence $G_1 = \mathrm{SL}_2(\mathbb{F}_{11})$ and the direct summand $\mathrm{M}_5(\mathbb{H}_p)$ corresponds to a faithful ordinary irreducible character χ of $\mathrm{SL}_2(\mathbb{F}_{11})$ with degree 10 and $\mathbb{Q}(\chi) = \mathbb{Q}$. This implies that in notations of [**4**, § 38], $\chi = \theta_j$ where j is an odd integer such that $1 \leqslant j \leqslant (11-1)/2 = 5$ and either $6j$ is divisible by $11+1 = 12$ or $4j$ is divisible by 12 ([**7**], Th. 6.2 on p. 285). This implies that $j = 3$ and $\chi = \theta_3$. However, the direct summand attached to θ_3 is ramified at 2 ([**10**, the case (c) on p. 4]; [**7**, theorem 6.1(iii) on p. 284]). Since $p \neq 2$, we get a contradiction which proves that $J(C_f)$ is not supersingular. This implies that $\mathrm{End}^0(J(C_f)) = \mathbb{Q}$ and therefore $\mathrm{End}(J(C_f)) = \mathbb{Z}$. □

Corollary 3.6. — *Suppose that* $n = 12$ *and* $\mathrm{Gal}(f)$ *is the Mathieu group* $\mathbf{M}_{11}$ *acting* 3*-transitively on* $\mathfrak{R}_f$. *Then* $\mathrm{End}(J(C_f)) = \mathbb{Z}$.

Proof. — Let α be a root of $f(x)$ and $K_1 = K(\alpha)$. Clearly, the stabilizer of α in $\mathrm{Gal}(f) = \mathbf{M}_{11}$ is $\mathrm{PSL}_2(\mathbb{F}_{11})$ acting doubly transitively on the roots of $f_1(x) = f(x)/(x-\alpha) \in K_1[x]$. Let us put $h(x) = f_1(x+\alpha) \in K_1[x], h(x) = x^{11}h(1/x) \in K_1[x]$. Clearly, $\deg(h_1) = 11$ and $\mathrm{Gal}(h_1) = \mathrm{PSL}_2(\mathbb{F}_{11})$ acts doubly transitively on the roots of h_1. By Corollary 3.5, $\mathrm{End}(J(C_{h_1})) = \mathbb{Z}$. On the other hand, the standard substitution $x_1 = 1/(x-\alpha), y_1 = y/(x-\alpha)^6$ establishes a birational isomorphism between C_f and $C_{h_1} : y_1^2 = h_1(x_1)$. This implies that $J(C_f) \cong J(C_{h_1})$ and therefore $\mathrm{End}(J(C_f)) = \mathbb{Z}$. □

In characteristic zero the assertions of Corollaries 3.4, 3.5 and 3.6 were earlier proven in [**46, 39**].

Corollary 3.7. — *Suppose that* $\deg(f) = n$ *where* $n = 22, 23$ *or* 24 *and* $\mathrm{Gal}(f)$ *is the corresponding (at least)* 3*-transitive Mathieu group* $\mathbf{M}_n \subset \mathrm{Perm}(\mathfrak{R}_f) \cong \mathbf{S}_n$. *Then* $\mathrm{End}(J(C_f)) = \mathbb{Z}$.

Proof. — First, assume that $n = 23$ or 24. We have $g = \dim(J(C_f)) = 11$. It is known that both $\mathbf{M}_{23}$ and $\mathbf{M}_{24}$ do not contain a subgroup of index 11 [**2**]. So, we may apply Theorem 3.2 and obtain that if $\mathrm{End}(J(C_f) \neq \mathbb{Z}$ then $\mathrm{End}^0(J(C_f)) \neq \mathbb{Q}$ and one of the following conditions holds:

(i) $\mathrm{End}^0(J(C_f)) = \mathrm{M}_{11}(\mathbb{Q})$ and there exist a finite perfect group $\Pi \subset \mathrm{GL}(11,\mathbb{Z})$ and a surjective homomorphism $\Pi \twoheadrightarrow \mathrm{Gal}(f) = \mathbf{M}_n$;

(ii) $p = \mathrm{char}(K) \in \{3,5,7,11,23\}$ and $\mathrm{End}^0(J(C_f)) = \mathrm{M}_{11}(\mathbb{H}_p)$.

Assume that the condition (i) holds. Then $\operatorname{End}^0(J(C_f)) = \mathrm{M}_{11}(\mathbb{Q})$ and $\mathrm{GL}(11,\mathbb{Z})$ contains a finite group, whose order is divisible by 23. It follows that $\mathrm{GL}(11,\mathbb{Z})$ contains an element of order 23, which is not true. The obtained contradiction proves that the condition (i) is not fulfilled.

Hence the condition (ii) holds. Then $p = \operatorname{char}(K) \in \{3,5,7,11,23\}$ and there exist a finite perfect subgroup $\Pi \subset \operatorname{End}^0(J(C_f))^* = \mathrm{GL}(11,\mathbb{H}_p)$ and a surjective homomorphism $\pi : \Pi \twoheadrightarrow \mathbf{M}_n$. Replacing Π by a suitable subgroup, we may and will assume that no proper subgroup of Π maps onto $\mathbf{M}_n$. By tensoring $\mathbb{H}_p$ to the field of complex numbers (over $\mathbb{Q}$), we obtain an embedding

$$\Pi \subset \mathrm{GL}(11,\mathbb{H}_p) \subset \mathrm{GL}(22,\mathbb{C}).$$

In particular, the (perfect) group Π admits a non-trivial projective 22-dimensional representation over $\mathbb{C}$. Recall that $\mathbf{M}_n$ has Schur's multiplier 1 (since $n = 23$ or 24) [**2**] and therefore all its projective representations are (obtained from) linear representations. Also, all nontrivial linear representations of $\mathbf{M}_{24}$ have dimension $\geqslant 23$, because the smallest dimension of a nontrivial linear representation of $\mathbf{M}_{24}$ is 23. It follows from results of Feit–Tits [**8**] that Π cannot have a non-trivial projective representation of dimension < 23. This implies that $n \neq 24$, *i.e.* $n = 23$.

Recall that 22 is the smallest possible dimension of a nontrivial representation of $\mathbf{M}_{23}$ in characteristic zero, because its every irreducible representation in characteristic zero has dimension $\geqslant 22$ [**2**]. It follows from a theorem of Feit–Tits ([**8**], pp. 1 and § 4; see also [**14**]) that the projective representation

$$\Pi \longrightarrow \mathrm{GL}(11,\mathbb{H}_p)/\mathbb{Q}^* \subset \mathrm{GL}(22,\mathbb{C})/\mathbb{C}^*$$

factors through $\ker(\pi)$. This means that $\ker(\pi)$ lies in $\mathbb{Q}^*$ and therefore Π is a central extension of $\mathbf{M}_{23}$. Now the perfectness of Π implies that π is an isomorphism, *i.e.* $\Pi \cong \mathbf{M}_{23}$.

Let us consider the natural homomorphism $\mathbb{Q}[\mathbf{M}_{23}] \cong \mathbb{Q}[\Pi] \to \mathrm{M}_{11}(\mathbb{H}_p)$ induced by the inclusion $\Delta \subset \mathrm{M}_{11}(\mathbb{H}_p)^*$. It is surjective, because otherwise one may construct a (complex) nontrivial representation of $\mathbf{M}_{23}$ of dimension < 22. This implies that $\mathrm{M}_{11}(\mathbb{H}_p)$ is isomorphic to a direct summand of $\mathbb{Q}[\mathbf{M}_{23}]$. But this is not true, since Schur indices of all irreducible representations of $\mathbf{M}_{23}$ are equal to 1 [**7**, § 7] and therefore $\mathbb{Q}[\mathbf{M}_{23}]$ splits into a direct sum of matrix algebras over fields. The obtained contradiction proves that the condition (ii) is not fulfilled. So, $\operatorname{End}(J(C_f) = \mathbb{Z}$.

Now let $n = 22$. Then $g = 10$. It is known that $\mathbf{M}_{22}$ is a simple nonabelian group not containing a subgroup of index 10 [**2**]. Let us assume that $\operatorname{End}^0(J(C_f)) \neq \mathbb{Q}$. Applying Theorem 1.6, we conclude that there exists a positive integer d dividing 10 such that either $d > 1$ and $\operatorname{End}^0(J(C_f) = \mathrm{M}_d(\mathbb{Q})$ or $\operatorname{End}^0(J(C_f)) = \mathrm{M}_d(\mathbb{H})$ where H is a quaternion $\mathbb{Q}$-algebra unramified outside ∞ and the prime divisors of $\#(\mathbf{M}_{22})$. In addition, there exist a finite perfect subgroup $\Pi \subset \operatorname{End}^0(J(C_f))^*$ and a surjective homomorphism $\pi : \Pi \twoheadrightarrow \mathbf{M}_{22}$. Replacing Π by a suitable subgroup, we may and will assume (without losing the perfectness) that no proper subgroup of Π maps onto $\mathbf{M}_n$.

By Lemma 3.13 on pp. 200–201 of [**41**], every homomorphism from Π to $\mathrm{PSL}(10,\mathbb{R})$ is trivial. The perfectness of Π implies that every homomorphism from Π to $\mathrm{PGL}(10,\mathbb{R})$ is trivial. Since $\mathrm{M}_d(\mathbb{Q})^* = \mathrm{GL}(d,\mathbb{Q}) \subset \mathrm{GL}(10,\mathbb{R})$, we conclude that $\mathrm{End}^0(J(C_f)) \neq \mathrm{M}_d(\mathbb{Q})$ and therefore $\mathrm{End}^0(J(C_f)) = \mathrm{M}_d(\mathbb{H})$.

If $d = 10$ then $p := \mathrm{char}(K) > 0$ and $J(C_f)$ is a supersingular abelian variety.

Assume that $d \neq 10$, *i.e.* $d = 1, 2$ or 5. If H is unramified at ∞ then there exists an embedding $\mathbb{H} \hookrightarrow \mathrm{M}_2(\mathbb{R})$. This gives us the embeddings

$$\Pi \subset \mathrm{M}_d(\mathbb{H})^* \longrightarrow \mathrm{M}_{2d}(\mathbb{R})^* = \mathrm{GL}(2d,\mathbb{R}) \subset \mathrm{GL}(10,\mathbb{R})$$

and therefore there is a nontrivial homomorphism from Π to $\mathrm{PGL}(10,\mathbb{R})$. The obtained contradiction proves that $\mathbb{H}$ is ramified at ∞.

There exists an embedding $\mathbb{H} \hookrightarrow \mathrm{M}_4(\mathbb{Q}) \subset \mathrm{M}_4(\mathbb{R})$. This implies that if $d = 1$ or 2 then there are embeddings

$$\Pi \subset \mathrm{M}_d(\mathbb{H})^* \longrightarrow \mathrm{M}_{4d}(\mathbb{R})^* = \mathrm{GL}(4d,\mathbb{R}) \subset \mathrm{GL}(10,\mathbb{R})$$

and therefore there is a nontrivial homomorphism from Π to $\mathrm{PGL}(10,\mathbb{R})$. The obtained contradiction proves that $d = 5$. This means that there exists an abelian surface Y over K_a such that $J(C_f)$ is isogenous to Y^5 and $\mathrm{End}^0(Y) = \mathbb{H}$. However, there do not exist abelian surfaces, whose endomorphism algebra is a definite quaternion algebra over $\mathbb{Q}$. This result is well-known in characteristic zero (see, for instance [**24**]); the positive characteristic case was done by Oort [**23**, Lemma 4.5 on p. 490]. Hence $d \neq 5$. This implies that $d = 10$ and $J(C_f)$ is a supersingular abelian variety.

Since $\mathbf{M}_{22}$ is a simple group and $11 \mid \#(\mathbf{M}_{22})$, every homomorphism from $\mathbf{M}_{22}$ to $\mathrm{GL}(9,\mathbb{F}_2)$ is trivial, because $\#(\mathrm{GL}(9,\mathbb{F}_2))$ is not divisible by 11. Since $9 = g - 1$, it follows from Theorem 3.3 of [**46**] (applied to $g = 10, X = J(C_f), G = \mathrm{Gal}(f) = \mathbf{M}_{22}$) that there exists a central extension $\pi_1 : G_1 \to \mathbf{M}_{22}$ such that G_1 is perfect, $\ker(\pi_1)$ is a cyclic group of order 1 or 2 and there exists a faithful 20-dimensional absolutely irreducible representation of G_1 in characteristic zero. However, such a central extension with 20-dimensional irreducible representation does not exist [**2**]. □

Combining Corollary 3.7 with previous author's results [**39, 42**] concerning small Mathieu groups, we obtain the following statement.

Theorem 3.8. — *Suppose that* $n \in \{11, 12, 22, 23, 24\}$ *and* $\mathrm{Gal}(f)$ *is the corresponding Mathieu group* $\mathbf{M}_n \subset \mathrm{Perm}(\mathfrak{R}_f) \cong \mathbf{S}_n$. *Then* $\mathrm{End}(J(C_f)) = \mathbb{Z}$.

In characteristic zero the assertion of Theorem 3.8 was earlier proven in [**39, 41**].

Theorem 3.9. — *Suppose that* $n = 15$ *and* $\mathrm{Gal}(f)$ *is the alternating group* $\mathbb{A}_7$ *acting doubly transitively on* $\mathfrak{R}_f$. *Then either* $\mathrm{End}(J(C_f)) = \mathbb{Z}$ *or* $J(C_f)$ *is isogenous over* K_a *to a product of elliptic curves.*

Proof. — We have $g = 7$. Unfortunately, A_7 has a subgroup of index 7. However, A_7 is simple nonabelian and does not have a normal subgroup of index 7. Applying

Theorem 1.6 to $X = J(C_f), g = 7, \ell = 2, \mathcal{G} = \mathrm{Gal}(f) = \mathbb{A}_7$, we obtain that either $J(C_f)$ is isogenous to a product of elliptic curves (case (a)) or $\mathrm{End}^0(J(C_f))$ is a central simple $\mathbb{Q}$-algebra (case (b)). If $\mathrm{End}^0(J(C_f))$ is a matrix algebra over $\mathbb{Q}$ then either $\mathrm{End}^0(J(C_f)) = \mathbb{Q}$ (*i.e.*, $\mathrm{End}(J(C_f)) = \mathbb{Z}$) or $\mathrm{End}^0(J(C_f)) = \mathrm{M}_7(\mathbb{Q})$ (*i.e.*, $J(C_f)$ is isogenous to the 7th power of an elliptic curve without complex multiplication).

If the central simple $\mathbb{Q}$-algebra $\mathrm{End}^0(J(C_f))$ is not a matrix algebra over $\mathbb{Q}$ then there exists a quaternion $\mathbb{Q}$-algebra $\mathbb{H}$ such that either $\mathrm{End}^0(J(C_f)) = \mathbb{H}$ or $\mathrm{End}^0(J(C_f)) = \mathrm{M}_7(\mathbb{H})$. If $\mathrm{End}^0(J(C_f)) = \mathrm{M}_7(\mathbb{H})$ then $J(C_f)$ is a supersingular abelian variety and therefore is isogenous to a product of elliptic curves.

Let us assume that $\mathrm{End}^0(J(C_f)) = \mathbb{H}$. We need to arrive to a contradiction. Since $7 = \dim(J(C_f))$ is odd, $p = \mathrm{char}(K) > 0$. The same arguments as in the proof of Corollary 1.8 tell us that $\mathbb{H} = \mathbb{H}_p$. By Theorem 1.6(b3), there exist a perfect finite group $\Pi \subset \mathrm{End}^0(J(C_f))^* = \mathbb{H}_p^*$ and a surjective homomorphism $\Pi \twoheadrightarrow \mathbb{A}_7$. But Lemma 1.9 asserts that every finite subgroup in $\mathbb{H}_p^*$ is solvable. The obtained contradiction proves that $\mathrm{End}^0(J(C_f)) \neq \mathbb{H}$. □

Theorem 3.10. — *Suppose that* $n = q + 1$ *where* $q \geqslant 5$ *is a prime power that is congruent to* ± 3 *modulo* 8. *Suppose that* $\mathrm{Gal}(f) = \mathrm{PSL}_2(\mathbb{F}_q)$ *acts doubly transitively on* $\mathfrak{R}_f$ *(where* $\mathfrak{R}_f$ *is identified with the projective line* $\mathbb{P}^1(\mathbb{F}_q)$*). Then* $\mathrm{End}^0(J(C_f))$ *is a simple* $\mathbb{Q}$*-algebra, i.e.* $J(C_f)$ *is either absolutely simple or isogenous to a power of an absolutely simple abelian variety.*

Proof. — Since $n = q + 1$ is even, $g = (q-1)/2$. It is known [**20**] that the $\mathrm{Gal}(f) = \mathrm{PSL}_2(\mathbb{F}_q)$-module $Q_{\mathfrak{R}_f}$ is simple and the centralizer of $\mathrm{PSL}_2(\mathbb{F}_q)$ in $\mathrm{End}_{\mathbb{F}_2}(Q_{\mathfrak{R}_f})$ is the field $\mathbb{F}_4$. On the other hand, $\mathrm{PSL}_2(\mathbb{F}_q)$ is a simple nonabelian group: we need to inspect its subgroups. The following statement will be proven later in this section.

Lemma 3.11. — *Let* $q \geqslant 5$ *be a power of an odd prime. Then* $\mathrm{PSL}_2(\mathbb{F}_q)$ *does not contain a subgroup of index dividing* $(q-1)/2$ *except* $\mathrm{PSL}_2(\mathbb{F}_q)$ *itself.*

Recall that $\widetilde{G}_{2,J(C_f)} = \mathrm{Gal}(f) = \mathrm{PSL}_2(\mathbb{F}_q)$. Now Theorem 3.10 follows readily from Theorem 1.5 combined with Lemma 3.11. □

Proof of Lemma 3.11. — Since $\mathrm{PSL}_2(\mathbb{F}_q)$ is a simple nonabelian subgroup, it does not contain a subgroup of index $\leqslant 4$ except $\mathrm{PSL}_2(\mathbb{F}_q)$ itself. This implies that in the course of the proof we may assume that $(q-1)/2 \geqslant 5$, *i.e.*, $q \geqslant 11$.

Recall that $\#(\mathrm{PSL}_2(\mathbb{F}_q)) = (q+1)q(q-1)/2$. Let $H \neq \mathrm{PSL}_2(\mathbb{F}_q)$ be a subgroup in $\mathrm{PSL}_2(\mathbb{F}_q)$. The list of subgroups in $\mathrm{PSL}_2(\mathbb{F}_q)$ given in [**33**, theorem 6.25 on p. 412] tells us that $\#(H)$ divides either $q \pm 1$ or $q(q-1)/2$ or 60 or $(b+1)b(b-1)$ where $b < q$ is a positive integer such that q is an integral power of b. This implies that if the index of H is a divisor of $(q-1)/2$ then either

(1) $(q+1)q$ divides 60, or

(2) $(q+1)q(q-1)/2 \leqslant \frac{q-1}{2}(\sqrt{q}+1)\sqrt{q}(\sqrt{q}-1) = \frac{q-1}{2}(q-1)\sqrt{q}$.

In the case (1) we have $q = 5$ which contradicts our assumption that $q \geqslant 11$. So, the case (2) holds. Clearly, $(q+1)\sqrt{q} \leqslant (q-1)$ which is obviously not true. □

Theorem 3.12. — *Let K be a field of characteristic different from 2. Suppose that $f(x)$ and $h(x)$ are polynomials in $K[x]$ enjoying the following properties:*

(i) $\deg(f) \geqslant 3$ *and the Galois group* $\mathrm{Gal}(f)$ *acts doubly transitively on the set* $\mathfrak{R}_f$ *of roots of f. If* $\deg(f)$ *is even then this action is 3-transitive;*

(ii) $\deg(h) \geqslant 3$ *and the Galois group* $\mathrm{Gal}(h)$ *acts doubly transitively on the set* $\mathfrak{R}_h$ *of roots of h. If* $\deg(h)$ *is even then this action is 3-transitive;*

(iii) *The splitting fields $K(\mathfrak{R}_f)$ of f and $K(\mathfrak{R}_h)$ of h are linearly disjoint over K.*

Let $J(C_f)$ be the jacobian of the hyperelliptic curve $C_f : y^2 = f(x)$ and $J(C_h)$ be the jacobian of the hyperelliptic curve $C_h : y^2 = h(x)$. Then either $\mathrm{Hom}(J(C_f), J(C_h)) = 0$, $\mathrm{Hom}(J(C_h), J(C_f)) = 0$ *or* $\mathrm{char}(K) > 0$ *and both $J(C_f)$ and $J(C_h)$ are supersingular abelian varieties.*

Proof. — Let us put $X = J(C_f), Y = J(C_h)$. The transitivity properties imply that $\mathrm{End}_{\widetilde{G}_{2,X}}(X_2) = \mathbb{F}_2$ and $\mathrm{End}_{\widetilde{G}_{2,Y}}(Y_2) = \mathbb{F}_2$. The linear disjointness of $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ implies that the fields $K(X_2) = K((J(C_f)_2) \subset K(\mathfrak{R}_f)$ and $K(Y_2) = K((J(C_h)_2) \subset K(\mathfrak{R}_h)$ are also linearly disjoint over K. Now the assertion follows readily from Theorem 2.1 with $\ell = 2$. □

4. Abelian varieties with multiplications

Let E be a number field. Let (X, i) be a pair consisting of an abelian variety X of positive dimension over K_a and an embedding $i : E \hookrightarrow \mathrm{End}^0(X)$. Here $1 \in E$ must go to 1_X. It is well known [**26**] that the degree $[E : \mathbb{Q}]$ divides $2\dim(X)$, *i.e.*

$$d = d_X := \frac{2\dim(X)}{[E : \mathbb{Q}]}$$

is a positive integer. Let us denote by $\mathrm{End}^0(X, i)$ the centralizer of $i(E)$ in $\mathrm{End}^0(X)$. Clearly, $i(E)$ lies in the center of the finite-dimensional $\mathbb{Q}$-algebra $\mathrm{End}^0(X, i)$. It follows that $\mathrm{End}^0(X, i)$ carries a natural structure of finite-dimensional E-algebra. If Y is (possibly) another abelian variety over K_a and $j : E \hookrightarrow \mathrm{End}^0(Y)$ is an embedding that sends 1 to the identity automorphism of Y then we write

$$\mathrm{Hom}^0((X, i), (Y, j)) = \{u \in \mathrm{Hom}^0(X, Y) \mid ui(c) = j(c)u \ \forall\, c \in E\}.$$

Clearly, $\mathrm{End}^0(X, i) = \mathrm{Hom}^0((X, i), (X, i))$. If m is a positive integer then we write $i^{(m)}$ for the composition $E \hookrightarrow \mathrm{End}^0(X) \subset \mathrm{End}^0(X^m)$ of i and the diagonal inclusion $\mathrm{End}^0(X) \subset \mathrm{End}^0(X^m) = \mathrm{M}_m(\mathrm{End}^0(X))$. Clearly,

$$\mathrm{End}^0(X^m, i^{(m)}) = \mathrm{M}_m(\mathrm{End}^0(X, i)) \subset \mathrm{M}_m(\mathrm{End}^0(X)) = \mathrm{End}^0(X^m).$$

Remark 4.1. — The E-algebra $\mathrm{End}^0(X,i)$ is semisimple. Indeed, in notations of Remark 1.4 $\mathrm{End}^0(X)=\prod_{s\in\mathcal{I}} D_s$ where all $D_s=\mathrm{End}^0(X_s)$ are simple $\mathbb{Q}$-algebras. If $\mathrm{pr}_s:\mathrm{End}^0(X)\twoheadrightarrow D_s$ is the corresponding projection map and $D_{s,E}$ is the centralizer of $\mathrm{pr}_s\, i(E)$ in D_s then one may easily check that $\mathrm{End}^0(X,i)=\prod_{s\in\mathcal{I}} D_{s,E}$. Clearly, $\mathrm{pr}_s\, i(E)\cong E$ is a simple $\mathbb{Q}$-algebra. It follows from Theorem 4.3.2 on p. 104 of [**9**] that $D_{s,E}$ is also a *simple* $\mathbb{Q}$-algebra. This implies that $D_{s,E}$ is a *simple* E-algebra and therefore $\mathrm{End}^0(X,i)$ is a semisimple E-algebra. We write i_s for the composition $\mathrm{pr}_s\, i:E\hookrightarrow\mathrm{End}^0(X)\twoheadrightarrow D_s\cong\mathrm{End}^0(X_s)$. Clearly, $D_{s,E}=\mathrm{End}^0(X_s,i_s)$ and

$$\mathrm{End}^0(X,i)=\prod_{s\in\mathcal{I}}\mathrm{End}^0(X_s,i_s). \tag{5}$$

It follows that $\mathrm{End}^0(X,i)$ is a simple E-algebra if and only if $\mathrm{End}^0(X)$ is a simple $\mathbb{Q}$-algebra, *i.e.*, X is isogenous to a self-product of (absolutely) simple abelian variety.

Theorem 4.2

(i) $\dim_E(\mathrm{End}^0((X,i))\leqslant 4\cdot\dim(X)^2/[E:\mathbb{Q}]^2$;

(ii) *Suppose that* $\dim_E(\mathrm{End}^0((X,i))=4\cdot\dim(X)^2/[E:\mathbb{Q}]^2$. *Then:*

(a) *X is isogenous to a self-product of an (absolutely) simple abelian variety. Also* $\mathrm{End}^0((X,i)$ *is a central simple E-algebra, i.e., E coincides with the center of* $\mathrm{End}^0((X,i)$. *In addition, X is an abelian variety of CM-type.*

(b) *There exist an abelian variety Z, a positive integer m, an isogeny ψ : $Z^m\to X$ and an embedding $k:E\hookrightarrow\mathrm{End}^0(Z)$ that sends 1 to 1_Z such that:*

(1) $\mathrm{End}^0(Z,k)$ *is a central division algebra over E of dimension* $(2\dim(Z)/[E:\mathbb{Q}])^2$ *and* $\psi\in\mathrm{Hom}^0((Z^r,k^{(m)}),(X,i))$.

(2) *If* $\mathrm{char}(K_a)=0$ *then E contains a CM subfield and* $2\dim(Z)=[E:\mathbb{Q}]$. *In particular,* $[E:\mathbb{Q}]$ *is even.*

(3) *If E does not contain a CM-field (e.g., E is a totally real number field) then* $\mathrm{char}(K_a)>0$ *and X is a supersingular abelian variety.*

Proof. — Recall that $d=2\dim(X)/[E:\mathbb{Q}]$. First, assume that X is isogenous to a self-product of an absolutely simple abelian variety, *i.e.*, $\mathrm{End}^0(X,i)$ is a simple E-algebra. We need to prove that

$$N:=\dim_E(\mathrm{End}^0(X,i))\leqslant d^2.$$

Let C be the center of $\mathrm{End}^0(X)$. Let E' be the center of $\mathrm{End}^0(X,i)$. Clearly,

$$C\subset E'\subset\mathrm{End}^0(X,i)\subset\mathrm{End}^0(X).$$

Let us put $e=[E':E]$. Then $\mathrm{End}^0(X,i)$ is a *central* simple E'-algebra of dimension N/e. Then there exists a central division E'-algebra D such that $\mathrm{End}^0(X,i)$ is isomorphic to the matrix algebra $\mathrm{M}_m(D)$ of size m for some positive integer m. Dimension arguments imply that

$$m^2\dim_{E'}(D)=\frac{N}{e},\quad \dim_{E'}(D)=\frac{N}{em^2}.$$

Since $\dim_{E'}(D)$ is a square,

$$\frac{N}{e} = N_1^2, \quad N = eN_1^2, \quad \dim_{E'}(D) = \left(\frac{N_1}{m}\right)^2$$

for some positive integer N_1. Clearly, m divides N_1.

Clearly, D contains a (maximal) field extension L/E' of degree $(N_1)/m$ and $\mathrm{End}^0(X,i) \cong \mathrm{M}_m(D)$ contains every field extension T/L of degree m. This implies that

$$\mathrm{End}^0(X) \supset \mathrm{End}^0(X,i) \supset T$$

and the number field T has degree $[T:\mathbb{Q}] = [E':\mathbb{Q}]\cdot\frac{N_1}{m}\cdot m = [E:\mathbb{Q}]eN_1$. But $[T:\mathbb{Q}]$ must divide $2\dim(X)$ (see [**30**, proposition 2 on p. 36]); if the equality holds then X is an abelian variety of CM-type. This implies that eN_1 divides $d = 2\dim(X)/[E:\mathbb{Q}]$. It follows that $(eN_1)^2$ divides d^2; if the equality holds then $[T:\mathbb{Q}] = 2\dim(X)$ and therefore X is an abelian variety of CM-type. But $(eN_1)^2 = e^2N_1^2 = e(eN_1^2) = eN = e\cdot\dim_E(\mathrm{End}^0(X,i))$. This implies that $\dim_E(\mathrm{End}^0(X,i)) \leqslant d^2/e \leqslant d^2$, which proves (i).

Assume now that $\dim_E(\mathrm{End}^0(X,i)) = d^2$. Then $e=1$ and

$$(eN_1)^2 = r^2, N_1 = d,\ [T:\mathbb{Q}] = [E:\mathbb{Q}]eN_1 = [E:\mathbb{Q}]d = 2\dim(X);$$

in particular, X is an abelian variety of CM-type. In addition, since $e=1$, we have $E' = E$, *i.e.* $\mathrm{End}^0(X,i)$ is a *central* simple E-algebra. We also have $C \subset E$ and

$$\dim_E(D) = \dim_{E'}(D) = \left(\frac{N_1}{m}\right)^2 = \left(\frac{d}{m}\right)^2.$$

Since E is the center of D, it is also the center of the matrix algebra $\mathrm{M}_m(D)$. Clearly, there exist an abelian variety Z over K_a, an embedding $j: D \hookrightarrow \mathrm{End}^0(Z)$ and an isogeny $\psi: Z^m \to X$ such that the induced isomorphism

$$\psi_*: \mathrm{End}^0(Z^m) \cong \mathrm{End}^0(X),\ u \longmapsto \psi u \psi^{-1}$$

maps $j(\mathrm{M}_m(D)) := \mathrm{M}_m(j(D)) \subset \mathrm{M}_m(\mathrm{End}^0(Z)) = \mathrm{End}^0(Z^m)$ onto $\mathrm{End}^0(X,i)$. Since E is the center of $\mathrm{M}_m(D)$ and $i(E)$ is the center of $\mathrm{End}^0(X,i)$, the isomorphism ψ_* maps $j(E) \subset j(\mathrm{M}_m(D)) = \mathrm{M}_m(j(D)) \subset \mathrm{End}^0(Z^m)$ onto $i(E) \subset \mathrm{End}^0(X)$. In other words, $\psi_* j(E) = i(E)$. It follows that there exists an automorphism σ of the field E such that $i = \psi_* j\sigma$ on E. It follows easily that if we put $k := j\sigma : E \hookrightarrow \mathrm{End}^0(Z)$ then $\psi \in \mathrm{Hom}((Z^m, k^{(m)}), (X,\psi))$.

Clearly, $k(E) = j(E)$ and therefore $j(D) \subset \mathrm{End}^0(Z,k)$. Since $\mathrm{M}_m(\mathrm{End}^0(Z,k)) \cong \mathrm{End}^0(X,i) \cong \mathrm{M}_m(D)$, the dimension arguments imply that $j(D) = \mathrm{End}^0(Z,k)$ and therefore $\mathrm{End}^0(Z,k) \cong D$ is a division algebra. Clearly,

$$\dim(Z) = \frac{\dim(X)}{m}, \quad \dim_E(D) = \left(\frac{d}{m}\right)^2 = \left(\frac{2\dim(X)}{[E:\mathbb{Q}]m}\right)^2 = \left(\frac{2\dim(Z)}{[E:\mathbb{Q}]}\right)^2.$$

Let B be an absolutely *simple* abelian variety over K_a such that X is isogenous to a self-product B^r of B where the positive integer $r = \dim(X)/\dim(B)$. Then $\mathrm{End}^0(B)$ is a central division algebra over C; we define a positive integer g_0 by $\dim_C(\mathrm{End}^0(B)) = g_0^2$. Since $\mathrm{End}^0(X)$ contains a field of degree $2\dim(X)$, it follows from Propositions 3 and 4 on pp. 36–37 in [**30**] (applied to $A = X$, $K = C$, $g = g_0$, $m = \dim(B)$, $f = [C : \mathbb{Q}]$) that $2\dim(B) = [C : \mathbb{Q}] \cdot g_0$. Let T_0 be a maximal subfield in the g_0^2-dimensional central division algebra $\mathrm{End}^0(B)$. Well-known properties of maximal subfields of division algebras imply that T_0 contains the center C and $[T_0 : C] = g_0$. It follows that $[T_0 : \mathbb{Q}] = [C : \mathbb{Q}][T_0 : C] = [C : \mathbb{Q}] \cdot g_0 = 2\dim(B)$ and therefore $\mathrm{End}^0(B)$ contains a field of degree $2\dim(B)$. This implies that B is an absolutely simple abelian variety of CM-type; in terminology of [**22**], B is an absolutely simple abelian variety with *sufficiently many complex multiplications*.

Assume now that $\mathrm{char}(K_a) = 0$. We need to check that $2\dim(Z) = [E : \mathbb{Q}]$ and E contains a CM-field. Indeed, since D is a division algebra, it follows from Albert's classification [**21, 23**] that $\dim_{\mathbb{Q}}(D)$ divides $2\dim(Z) = 2\dim(X)/m = [E : \mathbb{Q}]d/m$. On the other hand, $\dim_{\mathbb{Q}}(D) = [E : \mathbb{Q}] \dim_E(D) = [E : \mathbb{Q}]\,(d/m)^2$. Since m divides d, we conclude that $d/m = 1$, *i.e.*, $\dim_E(D) = 1, D = E, 2\dim(Z) = [E : \mathbb{Q}]$. In other words, $\mathrm{End}^0(Z)$ contains the field E of degree $2\dim(Z)$. It follows from Theorem 1 on p. 40 in [**30**] (applied to $F = E$) that E contains a CM-field.

Now let us drop the assumption about $\mathrm{char}(K_a)$ and assume instead that E does *not* contain a CM subfield. It follows that $\mathrm{char}(K) > 0$. Since C lies in E, it is totally real. Since B is an absolutely simple abelian variety with *sufficiently many complex multiplications* it is isogenous to an absolutely simple abelian variety W defined over a finite field [**22**] and $\mathrm{End}^0(B) \cong \mathrm{End}^0(W)$. In particular, the center of $\mathrm{End}^0(W)$ is isomorphic to C and therefore is a totally real number field. It follows from the Honda–Tate theory [**35**] that W is a supersingular elliptic curve and therefore B is also a supersingular elliptic curve. Since X is isogenous to B^r, it is a supersingular abelian variety.

Now let us consider the case of arbitrary X. Applying the already proven case of Theorem 4.2(i) to each X_s, we conclude that

$$\dim_E(\mathrm{End}^0(X_s, i)) \leqslant \left(\frac{2\dim(X_s)}{[E : \mathbb{Q}]}\right)^2.$$

Applying (5), we conclude that

$$\begin{aligned}\dim_E(\mathrm{End}^0(X, i)) &= \sum_{s\in\mathcal{I}} \dim_E(\mathrm{End}^0(X_s, i_s)) \\ &\leqslant \sum_{s\in\mathcal{I}} \left(\frac{2\dim(X_s)}{[E : \mathbb{Q}]}\right)^2 \leqslant \frac{(2\sum_{s\in\mathcal{I}} \dim(X_s))^2}{[E : \mathbb{Q}]^2} = \frac{(2\dim(X))^2}{[E : \mathbb{Q}]^2}.\end{aligned}$$

It follows that if the equality $\dim_E(\mathrm{End}^0(X, i)) = (2\dim(X))^2/[E : \mathbb{Q}]^2$ holds then the set $\mathcal{I}$ of indices s is a singleton, *i.e.* $X = X_s$ is isogenous to a self-product of an absolutely simple abelian variety. ◻

5. Corrigendum to [46]

Page 629, proof of Lemma 6.1 (i). First, the Hasse–Witt/Cartier–Manin matrix of the hyperelliptic curve C is $M^{(1/3)}$. (The exponent was inadvertently distorted.) Second, the jacobian $J(C)$ is a *supersingular* abelian surface if and only if $MM^{(3)} = 0$. (The product was mistakenly transposed.) Clearly,

$$\det(MM^{(3)}) = \det(M)\det(M)^3 = \det(M)^4 = (a_1a_5)^4.$$

Hence, if $MM^{(3)} = 0$ then $a_1 = 0$, because $a_5 \neq 0$. Suppose that $a_1 = 0$. Then

$$M = \begin{pmatrix} a_2 & 0 \\ a_5 & 0 \end{pmatrix}, \quad M^{(3)} = \begin{pmatrix} a_2^3 & 0 \\ a_5^3 & 0 \end{pmatrix}, \quad MM^{(3)} = \begin{pmatrix} a_2^4 & 0 \\ a_5a_2^3 & 0 \end{pmatrix}.$$

We conclude that $MM^{(3)} = 0$ if and only if $a_1 = a_2 = 0$. It follows that $J(C)$ is a supersingular abelian surface if and only if $a_1 = a_2 = 0$. Since $M \neq 0$, the jacobian $J(C)$ is not isomorphic to a product of two supersingular elliptic curves.

References

[1] C. Chevalley – *Théorie des groupes de Lie,* tome III, Hermann, Paris, 1954.

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

[3] Ch.W. Curtis & I. Reiner – *Methods of Representation Theory,* Vol. I, John Wiley & Sons, New York, Chichester, Brisbane, Toronto, 1981.

[4] L. Dornhoff – *Group Representation Theory,* Part A, Marcel Dekker, Inc., New York, 1972.

[5] G. Faltings – Endlichkeitssätze für abelsche Variaetäten über Zählkorpern, *Invent. Math.* **73** (1983), p. 349–366.

[6] ______, Complements to Mordell, Chapter VI, in *Rational points* (G. Faltings, G. Wustholz et al., eds.), Aspects of Mathematics, vol. E6, Friedr. Vieweg & Sohn, Braunschweig, 3rd ed., 1992.

[7] W. Feit – The computations of some Schur indices, *Israel J. Math.* **46** (1983), p. 274–300.

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

[9] I.N. Herstein – *Noncommutative rings*, John Wiley and Sons, 1968.

[10] G. Janusz – Simple components of $\mathbb{Q}[\mathrm{SL}(2, q)]$, *Comm. Algebra* **1** (1974), p. 1–22.

[11] N. Katz – Monodromy of families of curves: applications of some results of Davenport-Lewis, in *Séminaire de Théorie des Nombres (Paris, 1979-80)* (M.-J. Bertin, ed.), Progress in Math., vol. 12, Birkhäuser, Boston-Basel-Stuttgart, 1981, p. 171–195.

[12] ______, Affine cohomological transforms, perversity, and monodromy, *J. Amer. Math. Soc.* **6** (1993), p. 149–222.

[13] N. Katz & P. Sarnak – *Random matrices, Frobenius eigenvalues and Monodromy*, American Mathematical Society, Providence, RI, 1999.

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

[15] M. Klemm – Über die Reduktion von Permutationsmoduln, *Math. Z.* **143** (1975), p. 113–117.

[16] D. Masser – Specialization of some hyperelliptic jacobians, in *Number Theory in Progress,* vol. I (K. Györy, H. Iwaniec & J. Urbanowicz, eds.), de Gruyter, Berlin-New York, 1999, p. 293–307.

[17] L. Moret-Bailly – *Pinceaux de variétés abéliennes*, Astérisque, vol. 129, Société Mathématique de France, 1985.

[18] Sh. Mori – The endomorphism rings of some abelian varieties, *Japan. J. Math. (N.S.)* **2** (1976), p. 109–130.

[19] ______, The endomorphism rings of some abelian varieties. II, *Japan. J. Math. (N.S.)* **3** (1977), p. 105–109.

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

[21] D. Mumford – *Abelian varieties*, 2nd ed., Oxford University Press, 1974.

[22] F. Oort – The isogeny class of a CM-abelian variety is defined over a finite extension of the prime field, *J. Pure Appl. Algebra* **3** (1973), p. 399–408.

[23] ______, Endomorphism algebras of abelian varieties, in *Algebraic Geometry and Commutative Algebra in Honor of M. Nagata* (H. Hijikata et al., eds.), vol. II, Kinokuniya Cy, Tokyo, 1988, p. 469–502.

[24] F. Oort & Yu.G. Zarhin – Endomorphism algebras of complex tori, *Math. Ann.* **303** (1995), p. 11–29.

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

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

[27] E. Schaefer – Computing a Selmer group of a Jacobian using functions on the curve, *Math. Ann.* **310** (1998), p. 447–471.

[28] J.-P. Serre – *Lie groups and Lie algebras*, 2nd ed., Lect. Notes in Math., vol. 1500, Springer, 1992.

[29] ______, *Abelian ℓ-adic representations and elliptic curves*, 3rd ed., AK Peters, Wellesley, 1998.

[30] G. Shimura – *Abelian varieties with complex multiplication and modular functions*, Princeton University Press, Princeton, 1997.

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

[32] A. Silverberg & Yu.G. Zarhin – Variations on a theme of Minkowski and Serre, *J. Pure Appl. Algebra* **111** (1996), p. 285–302.

[33] M. Suzuki – *Group Theory I*, Springer Verlag, New York, 1982.

[34] J. Tate – Endomorphisms of Abelian varieties over finite fields, *Invent. Math.* **2** (1966), p. 134–144.

[35] ______, Classes d'isogénie des variétés abéliennes sur un corps fini, in *Séminaire Bourbaki 1968/69*, Lect. Notes in Math., vol. 179, Springer, 1971, Exp. 352; Russian translation in *Matematika* **14** (1970), no. 6, p. 129–137.

[36] Yu.G. Zarhin – Endomorphisms of Abelian varieties over fields of finite characteristic, *Izv. Akad. Nauk SSSR Ser. Mat.* **39** (1975), p. 272–277, *Math. USSR Izv.* **9** (1975), p. 255–260.

[37] ______, Abelian varieties in characteristic P, *Mat. Zametki* **19** (1976), p. 393–400, *Math. Notes* **19** (1976), p. 240–244.

[38] ______, Hyperelliptic jacobians without complex multiplication, *Math. Res. Lett.* **7** (2000), p. 123–132.

[39] ______, Hyperelliptic jacobians and modular representations, in *Moduli of abelian varieties* (C. Faber, G. van der Geer & F. Oort, eds.), Progress in Math., vol. 195, Birkhäuser, 2001, p. 473–490.

[40] ______, Hyperelliptic jacobians without complex multiplication in positive characteristic, *Math. Res. Lett.* **8** (2001), p. 429–435.

[41] ______, Hyperelliptic Jacobians without Complex Multiplication, Doubly Transitive Permutation Groups and Projective Representations, in *Algebraic Number Theory and Algebraic Geometry (Parshin Festschrift)*, Contemp. Math., vol. 300, American Mathematical Society, 2002, p. 195–210.

[42] ______, Very simple 2-adic representations and hyperelliptic jacobians, *Moscow Math. J.* **2** (2002), no. 2, p. 403–431.

[43] ______, Homomorphisms of hyperelliptic jacobians, in *Number Theory, Algebra, and Algebraic Geometry (Shafarevich Festschrift)*, Trudy Mat. Inst. Steklov., vol. 241, 2003, Proc. Steklov Inst. Math., vol. 241, 2003, p. 79-92, p. 90–104.

[44] ______, Hyperelliptic jacobians and simple groups $\mathrm{U}_3(2^m)$, *Proc. Amer. Math. Soc.* **131** (2003), p. 95–102.

[45] ______, Hyperelliptic jacobians without complex multiplication and Steinberg representations in positive characteristic, arXiv: `math.NT/0301177`, 2003.

[46] ______, Non-supersingular hyperelliptic jacobians, *Bull. Soc. math. France* **132** (2004), p. 617–634.

[47] Yu.G. Zarhin & A.N. Parshin – Finiteness problems in Diophantine geometry, Amer. Math. Soc. Transl. (2), vol. 143, American Mathematical Society, 1989, p. 35–102.

Yu.G. Zarhin, Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA • *E-mail :* `zarhin@math.psu.edu`