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

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

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,

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

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*

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