ENDOMORPHISM ALGEBRAS OF ABELIAN VARIETIES WITH SPECIAL REFERENCE TO SUPERELLIPTIC JACOBIANS

YURI G. ZARHIN

Abstract. This is (mostly) a survey article. We use an information about Galois properties of points of small order on an abelian variety in order to describe its endomorphism algebra over an algebraic closure of the ground field. We discuss in detail applications to jacobians of cyclic covers of the projective line.

2000 Math. Subj. Class: Primary 14H40; Secondary 14K05, 11G30, 11G10

Key words and phrases: *abelian varieties, superelliptic jacobians, doubly transitive permutation groups*

1. Definitions and statements

Throughout this paper K is a field and K_a its algebraic closure. We write $K^{\mathrm{sep}} \subset K_a$ for the separable algebraic closure of K in K_a and $\mathrm{Gal}(K)$ for the absolute Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K) = \mathrm{Aut}(K_a/K)$. Throughout the paper ℓ is a prime different from $\mathrm{char}(K)$. If A is a finite set then we write $|A|$ for its cardinality. For every abelian varieties X and Y over K_a we write $\mathrm{Hom}(X,Y)$ for the group of all K_a-homomorphisms from X to Y.

If X is an abelian variety of positive dimension over K then $\mathrm{End}_K(X)$ and $\mathrm{End}(X)$ stand for the rings of all its K-endomorphisms and K_a-endomorphisms respectively. It is known [11] that all endomorphisms of X are defined over K^{sep}.

The ring $\mathrm{End}_K(X)$ is a subring of $\mathrm{End}(X)$ and they both have the same identity element (automorphism), which we denote by 1_X. We write $\mathrm{End}^0_K(X)$ and $\mathrm{End}^0(X)$ for the corresponding $\mathbb{Q}$-algebras $\mathrm{End}_K(X)\otimes\mathbb{Q}$ and $\mathrm{End}(X)\otimes\mathbb{Q}$; they both are semisimple finite-dimensional algebras over the field $\mathbb{Q}$ of rational numbers. We have

$$\mathbb{Q}\cdot 1_X \subset \mathrm{End}^0_K(X) \subset \mathrm{End}^0(X).$$

The aim of this paper is to explain how one may obtain some information about the structure of $\mathrm{End}^0(X)$ in certain favorable circumstances, knowing only the Galois properties of certain points of prime order and the "multiplicities" of the action of a certain endomorphism field on the differentials of the first kind on X. One may view this paper as an exposition of ideas that were developed in [38] and [44, 45] and applied to *superelliptic* jacobians and prymians [37, 38, 36, 46, 47]. We also use this opportunity to correct inaccuracies in the statements of Theorems 1.1(ii), 3.12(ii), 5.2(ii) and Remark 3.2 of [44] and fill gaps in the proof of Theorem 3.12(ii) [44, p. 702] in [44, p. 697]). (See also [45] for the corrected version of [44].) We also fill a gap in the proof of [38, Theorem 4.2,(i) and (ii)(a)] (caused by

Partially supported by Simons Foundation Collaboration grant # 585711.

Part of this work was done in May-June 2018 at the Max-Planck-Institut für Mathematik (Bonn, Germany), whose hospitality and support are gratefully acknowledged.

improper use of [7, Theorem 4.3.2] in [38, Remark 4.1]), see below Theorems 5.1 and 5.4 and their proofs (Section 5).

Here is a couple of sample results that deal with jacobians $J(C_{f,p})$ of (smooth projective models of) superelliptic curves

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

Hereafter p is a prime and we assume that $\operatorname{char}(K) \neq p$ while $f(x) \in K[x]$ is a separable polymomial of degree $n \geq 3$. We write $\mathbb{Z}[\zeta_p]$ for the ring of integers in the pth cyclotomic field $\mathbb{Q}(\zeta_p)$. (When $p = 2$ we have $\mathbb{Z}[\zeta_p] = \mathbb{Z}$ and $C_{f,2}$ becomes the hyperelliptic curve $y^2 = f(x)$.) The choice of a primitive pth root of unity in K_a gives rise to a natural ring embedding

$$\mathbb{Z}[\zeta_p] \hookrightarrow \operatorname{End}(J(C_{f,p}))$$

(see [18, 15] and Section 8 below). If p does *not* divide n then the dimension of $J(C_{f,p})$ is $(n-1)(p-1)/2$; otherwise it is $(n-2)(p-1)/2$.

Theorem 1.1 (see Th. 2.1 of [27], Th. 2.1 of [37] and Th. 3.8 of [38])**.** *Let us assume that* $\operatorname{char}(K) \neq 2$ *and* $f(x) \in K[x]$ *is an irreducible polynomial of degree* $n \geq 5$*, whose Galois group* $\operatorname{Gal}(f)$ *over* K *enjoys one of the following two properties.*

- $\operatorname{char}(K) \neq 3$ *and* $\operatorname{Gal}(f)$ *is either the full symmetric group* $\mathbf{S}_n$ *or the alternating group* $\mathbf{A}_n$*;*
- $n \in \{11, 12, 22, 23, 24\}$ *and* $\operatorname{Gal}(f)$ *is isomorphic to the corresponding Mathieu group* $\mathbf{M}_n$*.*

Let $C_{f,2} : y^2 = f(x)$ *be the corresponding hyperelliptic curve of genus* $[(n-1)/2]$ *over* K *and* $J(C_{f,2})$ *its jacobian, which is a* $[(n-1)/2]$*-dimensional abelian variety over* K*.*

Then $\operatorname{End}(J(C_{f,2})) = \mathbb{Z}$*. In particular,* $J(C_{f,2})$ *is absolutely simple.*

Theorem 1.2 (see Th. 1.1 of [36])**.** *Let us assume that* $\operatorname{char}(K) = 0$ *and* $f(x) \in K[x]$ *is an irreducible polynomial of degree* $n \geq 5$*, whose Galois group* $\operatorname{Gal}(f)$ *over* K *is either the full symmetric group* $\mathbf{S}_n$ *or the alternating group* $\mathbf{A}_n$*. Let* p *be an odd prime,* $C_{f,p}$ *the corresponding superelliptic curve over* K *and* $J(C_{f,p})$ *its jacobian, which is an abelian variety over* K*.*

Then $\operatorname{End}(J(C_{f,p})) = \mathbb{Z}[\zeta_p]$*. In particular,* $J(C_{f,p})$ *is absolutely simple.*

Theorem 1.3 (see Th. 1.1 of [44], Th. 1.1 of [45] and Theorem 8.7 below)**.** [1] *Suppose that* K *has characteristic zero,* $n \geq 4$ *and* p *is an odd prime that does not divide* n*. Assume also that either* $n = p + 1$ *or* p *does not divide* $n - 1$*.*

Suppose that K *contains a primitive* p*th root of unity and* $\operatorname{Gal}(f)$ *is a doubly transitive permuation group (on the set of roots of* $f(x)$*) that does not contain a proper normal subgroup, whose index divides* $n - 1$*.*

Then $\operatorname{End}(J(C_{f,p})) = \mathbb{Z}[\zeta_p]$*. In particular,* $J(C_{f,p})$ *is absolutely simple.*

The paper is organized as follows. Section 2 contains basic definitions and reviews elementary results concerning the structure of $\operatorname{End}^0(X)$ and $\operatorname{End}^0_K(X)$ under certain assumptions on the Galois properties of the group X_ℓ of points of prime order ℓ on X related to the image $\tilde{G}_{\ell,X,K}$ of the Galois group in $\operatorname{Aut}(X_\ell)$. These results are generalized in Section 3 when X admits multiplications from the ring $\mathcal{O}$ of integers in a number field E and X_ℓ is replaced by the group X_λ of points on X that are

[1] In Th. 1.1 of [44] the assertion (ii)(a) actually is not proven and should be ignored.

killed by multiplication from a maximal ideal $\lambda \subset \mathcal{O}$. (The results of Section 2 correspond to the case $\mathcal{O} = \mathbb{Z}, E = \mathbb{Q}, \lambda = \ell\mathbb{Z}$.) In order to prove the results of Section 3, we need to use results from the theory of (central semi)simple algebras over fields, which are discussed in Section 4. We prove the assertions of Section 3 in Section 5. In Section 6 the Lie algebra $\mathrm{Lie}(X)$ of X (which is the dual of the space of differentials of the first kind) enters the picture: assuming that $\mathrm{char}(K) = 0$, we discuss the action of E on $\mathrm{Lie}(X)$, which allows us to extend the results of Section 3. We are going to apply these results to superelliptic (hypergeometric) jacobians $J(C_{f,q})$ of curves $C_{f,q}$ and their natural abelian subvarieties $J^{(f,q)}$, which are provided with the action of the qth cyclotomic field $E = \mathbb{Q}(\zeta_q)$ where q is a prime power. (Here $C_{f,q}$ is the smooth projective module of the affine curve $y^q = f(x)$ where $f(x)$ is a polynomial without multiple roots.) In order to do this, we need to discuss certain constructions related to permutation groups and permutation modules, which is done in Section 7. Section 8 contains results about endomorphism algebras of $J^{(f,q)}$. Section 9 contains auxiliary results about the structure of the Galois module $J_\lambda^{(f,q)}$ where λ is the maximal ideal of the qth cyclotomic ring $\mathbb{Z}[\zeta_q]$ generated by $(1-\zeta_q)$.

Acknowledgements. I am deeply grateful to Jiangwei Xue, who had read the first version of the manuscript and made numerous valuable comments and suggestions that helped to improve the exposition. Part of this work was done in June 2017 during my stay at Steklov Mathematical Institute (Russian Academy of Sciences, Moscow), whose hospitality is gratefully acknowledged.

2. Definitions and first statements

2.1. We write $C_{K,X}$ and C_X for the centers of $\mathrm{End}_K^0(X)$ and $\mathrm{End}^0(X)$. Both $C_{K,X}$ and C_X are isomorphic to direct sums of number fields; each of those fields is either totally real or CM. It is well known that X is K-isogenous to a self-product of a K-simple abelian variety Z_K (respectively, is isogenous over K_a to a self-product of an absolutely simple abelian variety Z over K_a) if and only if $C_{K,X}$ (respectfully, C_X) is a field. If this is the case then there is a canonical isomorphism between the fields $C_{K,X}$ and C_{K,Z_K} (respectfully between the fields C_X and C_Z). In addition, C_X is a field if and only if $\mathrm{End}^0(X)$ is a simple $\mathbb{Q}$-algebra. In general, the semisimple $\mathbb{Q}$-algebra $\mathrm{End}^0(X)$ splits into a finite direct sum

$$\mathrm{End}^0(X) = \sum_{s \in \mathcal{I}(X)} D_s$$

of simple $\mathbb{Q}$-algebras D_s. (Here the finite nonempty set $\mathcal{I}(X)$ is identified with the set of (nonzero) minimal two-sided ideals in $\mathrm{End}^0(X)$.) Let e_s be the identity element of $D_s \subset \mathrm{End}^0(X)$. We have

$$1_X = \sum_{s \in \mathcal{I}(X)} e_s \in \mathrm{End}^0(X),\ e_s^2 = e_s,\ e_s e_t = 0\ \forall s \neq t.$$

Let us choose a positive integer N such that all $Ne_s \in \mathrm{End}(X)$ and consider

$$X_s := (Ne_s)(X) \subset X,$$

which is an abelian subvariety of X that is defined over K_a.

The following assertion is contained in [38, Remark 1.4 on pp. 192-193].

Lemma 2.2. (i) *The $\mathbb{Q}$-algebras D_s and $\mathrm{End}^0(X_s)$ are isomorphic. In particular, $\mathrm{End}^0(X_s)$ is a simple $\mathbb{Q}$-algebra, i.e., X_s is isogenous over K_a to a self-product of simple abelian variety over K_a.*

(ii) $\mathrm{Hom}(X_s, X_t) = \{0\}$ *for each* $s \ne t$ *.*

(iii) *The natural K_a-homomorphism of abelian varieties*

$$\Pi_X : \prod_{s\in\mathcal{I}(X)} X_s \to X,\ \{x_s\}_{s\in\mathcal{I}(X)} \mapsto \sum_{s\in\mathcal{I}(X)} x_s$$

is an isogeny.

2.3. Since X is defined over K, each $\sigma \in \mathrm{Gal}(K)$ and $u \in \mathrm{End}(X)$ give rise to ${}^{\sigma}u \in \mathrm{End}(X)$ such that

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

This gives us a continuous group homomorphism [22]

$$\kappa_{X,K} : \mathrm{Gal}(K) \to \mathrm{Aut}(\mathrm{End}(X)),\ k_X(\sigma)(u) ={}^{\sigma} u\ \forall \sigma \in \mathrm{Gal}(K), u \in \mathrm{End}(X)$$

with finite image. (Here $\mathrm{Aut}(\mathrm{End}(X))$ is provided with discrete topology). If L/K is a finite separable algebraic field extension with $L \subset K^{\mathrm{sep}}$ then $\mathrm{Gal}(L)$ is an open subgroup of finite index in $\mathrm{Gal}(K)$ and the restriction of $\kappa_{X,K}$ to $\mathrm{Gal}(L)$ coincides with

$$\kappa_{X,L} : \mathrm{Gal}(L) \to \mathrm{Aut}(\mathrm{End}(X)).$$

It is well known that $\mathrm{End}_L(X)$ coincides with the subring $\mathrm{End}(X)^{\mathrm{Gal}(L)}$ of $\mathrm{Gal}(L)$-invariants, i.e.,

$$\mathrm{End}_L(X) = \{u \in \mathrm{End}(X) \mid^{\sigma} u = u\ \forall \sigma \in \mathrm{Gal}(L)\}.$$

In particular,

$$\mathrm{End}_K(X) = \mathrm{End}(X)^{\mathrm{Gal}(K)} = \{u \in \mathrm{End}(X) \mid^{\sigma} u = u\ \forall \sigma \in \mathrm{Gal}(K)\}.$$

The kernel $\ker(\kappa_{X,K})$ is a closed normal subgroup of finite index in $\mathrm{Gal}(K)$ and therefore is open, i.e. coincides with the Galois (sub)group $\mathrm{Gal}(\mathcal{F}_{X,K})$ of a certain overfield $\mathcal{F}_{X,K} \supset K$ such that $\mathcal{F}_{X,K} \subset K^{\mathrm{sep}}$ and $\mathcal{F}_{X,K}/K$ is a finite Galois extension. Clearly, $\mathrm{End}_L(X) = \mathrm{End}(X)$ (i.e., all endomorphisms of X are defined over L) if and only if $L \supset \mathcal{F}_{X,K}$. In general, $\mathcal{F}_{X,L}$ coincides with the compositum $\mathcal{F}_{X,K}L$ of $\mathcal{F}_{X,K}$ and L in K^{sep}.

The following assertion is contained in [38, Remark 1.4 on pp. 192-193].

Lemma 2.4. *The finite subset $\{Ne_s \mid s \in \mathcal{I}(X)\}$ of $\mathrm{End}(X)$ is $\mathrm{Gal}(K)$-stable. If $\mathrm{End}_K(X)$ has no zero divisors then the action of $\mathrm{Gal}(K)$ on $\mathcal{I}(X)$ is transitive and*

$$\dim(X_s) = \dim(X)/|\mathcal{I}(X)|,$$

which does not depend on a choice of $s \in \mathcal{I}(X)$.

Corollary 2.5. *If $\mathrm{End}^0_K(X)$ is a number field then the action of $\mathrm{Gal}(K)$ on $\mathcal{I}(X)$ is transitive and $|\mathcal{I}(X)|$ divides $\dim(X)$.*

Proof. Since $\mathrm{End}^0_K(X)$ is a number field, $\mathrm{End}_K(X)$ is an order in this field and therefore has no zero divisors. So, we may apply Lemma 2.4 and get the desired transitivity and the equality $\dim(X_s) = \dim(X)/|\mathcal{I}(X)|$. Since all three numbers $\dim(X_s), \dim(X)$ and $|\mathcal{I}(X)|$ are nonzero integers, we conclude that $|\mathcal{I}(X)|$ divides $\dim(X)$. □

Theorem 2.6. *Let F/K be a finite Galois field extension such that $F \subset K^{\mathrm{sep}}$ and all endomorphisms of X are defined over F. If $\mathrm{End}_K^0(X)$ is a number field and $\mathrm{Gal}(F/K)$ does not contain a proper subgroup, whose index divides $\dim(X)$ then $\mathcal{I}(X)$ is a singleton, i.e., $\mathrm{End}^0(X)$ is a simple $\mathbb{Q}$-algebra.*

Proof. Since all endomorphisms of X are defined over F,

$$F \supset \mathcal{F}_{X,K},\ \mathrm{Gal}(F) \subset \mathrm{Gal}(\mathcal{F}_{X,K})$$

and $\kappa_{X,K} : \mathrm{Gal}(K) \to \mathrm{Aut}(\mathrm{End}(X))$ factors through the quotient $\mathrm{Gal}(K)/\mathrm{Gal}(F) = \mathrm{Gal}(F/K)$. This implies that the action of $\mathrm{Gal}(K)$ on $\mathcal{I}(X)$ also factors through $\mathrm{Gal}(F/K)$. By Corollary 2.5 $\mathrm{Gal}(K)$ acts transitively on $\mathcal{I}(X)$ and therefore the corresponding $\mathrm{Gal}(F/K)$-action on $\mathcal{I}(X)$ is also transitive. This implies that $\mathrm{Gal}(F/K)$ has a subgroup of index $|\mathcal{I}(X)|$. By Corollary 2.5, $|\mathcal{I}(X)|$ divides $\dim(X)$ and therefore this subgroup must coincide with the whole $\mathrm{Gal}(F/K)$, i.e., $\mathcal{I}(X)$ is a singleton. □

Let X_ℓ be the kernel of multiplication by ℓ in $X(K_a)$. It is well known [11, 14] that X_ℓ is a $\mathrm{Gal}(K)$-invariant subgroup of $X(K^{\mathrm{sep}})$, which is (as a group) a $2\dim(X)$-dimensional vector space over the prime finite field $\mathbb{F}_\ell$ of characteristic ℓ. This gives rise to the natural continuous group homomorphism

$$\tilde{\rho}_{\ell,X,K} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{F}_\ell}(X_\ell),$$

whose image we denote by $\tilde{G}_{\ell,X,K}$. By definition, we get the surjective continuous homomorphism

$$\tilde{\rho}_{\ell,X,K} : \mathrm{Gal}(K) \twoheadrightarrow \tilde{G}_{\ell,X,K} \subset \mathrm{Aut}_{\mathbb{F}_\ell}(X_\ell).$$

One may view the vector space X_ℓ as (faithful) $\tilde{G}_{\ell,X,K}$-module.

The next well known lemma goes back to K. Ribet [17] and S. Mori [10].

Lemma 2.7. *(* [38, Lemma 1.2 on p. 191]*) If the centralizer*

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

then

$$\mathrm{End}_K(X) = \mathbb{Z},\ \mathrm{End}_K^0(X) = \mathbb{Q}.$$

The next statement follows readily from [38, Th. 1.5 on pp. 193–194].

Theorem 2.8. *Let us assume that $\mathrm{End}_{\tilde{G}_{\ell,X,K}}(X_\ell)$ is a field. Suppose that $\tilde{G}_{\ell,X,K}$ does not contain a proper subgroup, whose index divides $\dim(X)$. Then $\mathrm{End}^0(X)$ is a simple $\mathbb{Q}$-algebra.*

The following assertion is an immediate corollary of Theorem 2.8 and [38, Th. 1.6 on pp. 195].

Theorem 2.9. *Let us assume that*

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

Suppose that $\tilde{G}_{\ell,X,K}$ does contain neither a proper subgroup with index dividing $\dim(X)$ nor a normal subgroup of index 2. Then $\mathrm{End}^0(X)$ is a central simple $\mathbb{Q}$-algebra.

3. Abelian varieties with multiplication

In this section we discuss analogues of results of Section 1 when the endomorphism algebra of an abelian variety contains a given number field.

3.1. Let E be a number field and

$$i : E \hookrightarrow \mathrm{End}^0_K(X) \subset \mathrm{End}^0(X)$$

be a $\mathbb{Q}$-algebra embedding such that $i(1) = 1_X$. It is known [21, Prop. 2 on p. 36]) that the degree $[E : \mathbb{Q}]$ divides $2\mathrm{dim}(X)$. Let us put

$$d_{X,E} = \frac{2\mathrm{dim}(X)}{[E : \mathbb{Q}]}.$$

We write $\mathrm{End}^0(X, i)$ for the centralizer of $i(E)$ in $\mathrm{End}^0(X)$ and $\mathrm{End}^0_K(X, i)$ for the centralizer of $i(E)$ in $\mathrm{End}^0_K(X)$. We have

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

We write $i(E)C_X$ for the compositum of $i(E)$ and C_X in $\mathrm{End}^0(X)$. In other words, $i(E)C_X$ is the image of the homomorphism of $\mathbb{Q}$-algebras

$$i \otimes \mathrm{id}_{C_X} : E \otimes_{\mathbb{Q}} C_X \to \mathrm{End}^0(X),\ e \otimes c \mapsto i(e)c.$$

Clearly $E \otimes_{\mathbb{Q}} C_X$ is a direct sum of fields, each of which contains a subfield isomorphic to E. This implies that $i(E)C_X$ is a direct sum of fields, each of which contains a subfield isomorphic to E. (In addition, each such a field contains a subfield isomorphic to C_X if the latter is a field.)

Clearly, $i(E)C_X$ commutes with $i(E)$ and therefore lies in $\mathrm{End}^0(X, i)$ and even in its center.

The next three assertions will be proven in in Section 5.

The first one is a corollary of standard facts about centralizers and bicentralizers of semisimple subalgebras of semisimple algebras. (See Theorem 4.1 below.)

Theorem 3.2. *$\mathrm{End}^0(X, i)$ is a finite-dimensional semisimple $\mathbb{Q}$-algebra, whose center coincides with $i(E)C_X$.*

The next two statements deal with the E-dimension of $\mathrm{End}^0(X, i)$.

Theorem 3.3. *Let us consider $\mathrm{End}^0(X, i)$ as an E-algebra. Then the E-algebra $\mathrm{End}^0(X, i)$ is semisimple and*

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

Theorem 3.4. *Suppose that*

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

Then E contains C_X and therefore C_X is a field. In addition, $\mathrm{End}^0(X, i)$ is a central simple E-algebra and X is an abelian variety of CM type over K_a. In particular, X is isogenous over K_a to a self-product of an absolutely simple abelian variety of CM type over K_a.

Example 3.5. Let $E=\mathbb{Q}$. Then $\mathrm{End}^0(X,i)=\mathrm{End}^0(X)$. We have

$$\dim_{\mathbb{Q}}(\mathrm{End}^0(X))\le (2g)^2;$$

the equalty holds if and only if $\mathrm{char}(K_a)>0$ and X is isogenous over K_a to a self-product of a supersingular elliptic curve [27].

3.6. Let $\mathcal{O}$ be the ring of integers in E. If λ is a maximal ideal in $\mathcal{O}$ then we write $k(\lambda)$ for its (finite) residue field $\mathcal{O}/\lambda$. For all but finitely many λ

$$\mathrm{char}(k(\lambda))\ne \mathrm{char}(K).$$

Let us assume that

$$i(\mathcal{O})\subset \mathrm{End}_K(X).$$

Then the center of $\mathrm{End}_K(X,i)$ contains $i(\mathcal{O})$ and $\mathrm{End}_K(X,i)$ becomes an $i(\mathcal{O})\cong\mathcal{O}$-algebra. Notice that $\mathcal{O}$ is a Dedekind ring and the $\mathcal{O}$-module $\mathrm{End}_K(X)$ is finitely generated torsion-free. Therefore $\mathrm{End}_K(X)$ is isomorphic (as an $\mathcal{O}$-module) to a direct sum of finitely many nonzero ideals of $\mathcal{O}$. Let us assume that $\mathrm{char}(k(\lambda))\ne \mathrm{char}(K)$ and consider

$$X_\lambda=\{x\in X(K_a)\mid i(u)x=0\ \forall u\in\lambda\subset\mathcal{O}\}\subset X(K_a).$$

It is known [16] that X_λ is a $\mathrm{Gal}(K)$-invariant finite subgroup of $X(K^{\mathrm{sep}})$ that carries the natural structure of $d_{X,E}$-dimensional vector space over $k(\lambda)$. The Galois action on X_λ induces the continuous group homomorphism

$$\bar\rho_{\lambda,X,K}:\mathrm{Gal}(K)\to \mathrm{Aut}_{k(\lambda)}(X_\lambda),$$

whose image we denote by $\tilde G_{\lambda,X,K}$. As above (in the case of $E=\mathbb{Q},\mathcal{O}=\mathbb{Z},\lambda=\ell\mathbb{Z})$), we get the surjective continuous group homomorphism

$$\bar\rho_{\lambda,X}=\bar\rho_{\lambda,X,K}:\mathrm{Gal}(K)\twoheadrightarrow \tilde G_{\lambda,X,K}\subset \mathrm{Aut}_{k(\lambda)}(X_\lambda).$$

If $K'\subset K^{\mathrm{sep}}$ is an overfield of K then $\bar\rho_{\lambda,X,K'}$ coincides with the restriction of $\bar\rho_{\lambda,X,K}$ to $\mathrm{Gal}(K')\subset\mathrm{Gal}(K)$.

Let $K(X_\lambda)\subset K^{\mathrm{sep}}$ be the field of definition of all points of X_λ. Then the subgroup $\mathrm{Gal}(K(X_\lambda))$ of $\mathrm{Gal}(K)$ coincides with $\ker(\bar\rho_{\lambda,X,K})$, $K(X_\lambda)/K$ is a finite Galois extension and $\bar\rho_{\lambda,X,K}$ induces the canonical isomorphism

$$\mathrm{Gal}(K(X_\lambda)/K)=\mathrm{Gal}(K)/\mathrm{Gal}(K(X_\lambda))\cong \tilde G_{\lambda,X,K}\subset\mathrm{Aut}_{k(\lambda)}(X_\lambda).$$

3.7. We will need the following result related to the notion of minimal covers of groups [8].

Lemma 3.8. *Let F/K be a finite Galois field extension and let L/K be a Galois field extension such that*

$$K\subset L\subset F.$$

Then there exists an overfield $\mathcal{K}$ of K that is a subfield of F and enjoys the following properties.

(i) $K\subset\mathcal{K}\subset F$.

(ii) *Let $\phi_{\mathcal{K},L}$ be the restriction of the natural surjective group homomorphism $\mathrm{Gal}(F/K)\twoheadrightarrow\mathrm{Gal}(L/K)$ to $\mathrm{Gal}(F/\mathcal{K})\subset\mathrm{Gal}(F/K)$. Then the group homomorphism $\phi_{\mathcal{K},L}:\mathrm{Gal}(F/\mathcal{K})\to\mathrm{Gal}(L/K)$ is surjective.*

(iii) *$\mathcal{K}$ is maximal among the fields that satisfy (i) and (ii).*

Proof. Clearly, $\mathcal{K}=K$ satisfies (i) and (ii). The existence of maximal $\mathcal{K}$ follows from the finiteness of the set of intermediate fields that satisfy (i). □

Remark 3.9. (i) The maximality of $\mathcal{K}$ in Lemma 3.8 means that surjective $\phi_{\mathcal{K},L} : \mathrm{Gal}(F/\mathcal{K}) \to \mathrm{Gal}(L/K)$ is a *minimal cover* in a sense of [8], i.e., if H is a subgroup of $\mathrm{Gal}(F/\mathcal{K})$ that maps *onto* $\mathrm{Gal}(L/K)$ then $H = \mathrm{Gal}(F/\mathcal{K})$. Indeed, the subfield F^H of F enjoys the properties (i–ii) and contains $F^{\mathrm{Gal}(F/\mathcal{K})} = \mathcal{K}$. In light of the maximality of $\mathcal{K}$, we have $F^H = \mathcal{K}$ and therefore $\mathrm{Gal}(F/\mathcal{K}) = H$. (Such a $\mathcal{K}$ is not necessarily unique.)

ii) Suppose that H is a subgroup in $\mathrm{Gal}(F/\mathcal{K})$ of index $d > 1$. By (i), the index $d' := (\mathrm{Gal}(L/K) : \phi_{\mathcal{K},L}(H)) > 1$. I claim that d' divides d. Indeed, if $\phi = \phi_{\mathcal{K},L}$ then

$$d = \frac{|\mathrm{Gal}(F/\mathcal{K})|}{|H|} = \frac{|\ker(\phi)| \cdot |\mathrm{Gal}(L/K)|}{|\ker(\phi)\bigcap H||\phi(H)|} =$$

$$\frac{|\ker(\phi)|}{|\ker(\phi)\bigcap H|} \cdot \frac{|\mathrm{Gal}(L/K)|}{|\phi(H)|} = \frac{|\ker(\phi)|}{|\ker(\phi)\bigcap H|} \cdot d'.$$

Since $\ker(\phi)\bigcap H$ is a subgroup of $\ker(\phi)$, Lagrange's theorem tells us that $|\ker(\phi)\bigcap H|$ divides $|\ker(\phi)|$ and therefore d' divides d.

This implies that if $d > 1$ is an integer such that $\mathrm{Gal}(L/K)$ does *not* contain a proper subgroup of index dividing d then $\mathrm{Gal}(F/\mathcal{K})$ also does *not* contain a proper subgroup of index dividing d.

Remark 3.10. Let K, L, F be as in Lemma 3.8. Suppose that $\mathcal{T}$ is a field that is an overfield of K and a subfield of F. Since the field extension L/K is Galois, the field extension $\mathcal{T}L/\mathcal{T}$ is also Galois. Hereafter $\mathcal{T}L$ is the compositum of $\mathcal{T}$ and L, which is a subfield of F with

$$[\mathcal{T}L : K] \le [\mathcal{T} : K][L : K]; \tag{1}$$

the equality holds if and only if $\mathcal{T}$ and L are **linearly disjoint** over K.

The assertion that $\mathcal{T}$ enjoys the property (ii) of Lemma 3.8 means that $\mathcal{T}$ and L are **linearly disjoint** over K. Indeed, suppose that $\mathcal{T}$ and L are **linearly disjoint** over K. Then

$$[\mathcal{T}L : K] = [\mathcal{T} : K][L : K].$$

Since

$$[\mathcal{T}L : K] = [\mathcal{T}L : \mathcal{T}][\mathcal{T} : K],$$

we conclude that $[\mathcal{T}L : \mathcal{T}] = [L : K]$ and therefore the natural injective group homomorphism ("restriction" to L)

$$\mathrm{res}_L : \mathrm{Gal}(\mathcal{T}L/\mathcal{T}) \to \mathrm{Gal}(L/K)$$

is a map between two finite groups of the same order $[L : K]$ and therefore is an isomorphism. Notice that res_L coincides with the restriction to $\mathrm{Gal}(\mathcal{T}L/\mathcal{T}) \subset \mathrm{Gal}(F/K)$ of $\phi_{\mathcal{T},L} : \mathrm{Gal}(F/\mathcal{T}) \to \mathrm{Gal}(L/K)$. This implies that $\phi_{\mathcal{T},L}$ is surjective, i.e., $\mathcal{T}$ enjoys the property (ii) of Lemma 3.8.

Conversely, let us assume that $\phi_{\mathcal{T},L}$ is *surjective*. Notice that $\phi_{\mathcal{T},L}$ factors through $\mathrm{Gal}(F/\mathcal{T}) \twoheadrightarrow \mathrm{Gal}(\mathcal{T}L/\mathcal{T})$ and therefore the surjectiveness of $\phi_{\mathcal{T},L}$ implies (actually, is equivalent to) the surjectiveness of

$$\mathrm{res}_L : \mathrm{Gal}(\mathcal{T}L/\mathcal{T}) \to \mathrm{Gal}(L/K),$$

which, in turn, implies the inequality $[\mathcal{T}L : \mathcal{T}] \ge [L : K]$. This implies that

$$[\mathcal{T}L : K] = [\mathcal{T}L : [\mathcal{T}][\mathcal{T} : K] \ge [L : K][\mathcal{T} : K],$$

which tells us in light of (1) that

$$[\mathcal{T}L : K] = [L : K][\mathcal{T} : K],$$

i.e., $\mathcal{T}$ and L are linearly disjoint over K.

This means that $\mathcal{T}$ enjoys the properties (i)-(iii) of Lemma 3.8 if and only if it is *maximal* among overfields of K that lie in F and are linearly disjoint with L over K.

Remark 3.11. Let us apply Lemma 3.8 and Remark 3.9 to $L = K(X_\lambda)$ and choose as $F \subset K^{\mathrm{sep}}$ any finite Galois extension of K that contains both $K(X_\lambda)$ and $\mathcal{F}_{X,K}$; in particular, all endomorphisms of X are defined over F. We have

$$\mathrm{Gal}(L/K) = \mathrm{Gal}(K(X_\lambda)/K) = \tilde{G}_{\lambda,X,K}.$$

Clearly, $\bar{\rho}_{\lambda,X,K}$ factors through $\mathrm{Gal}(K)/\mathrm{Gal}(F) = \mathrm{Gal}(F/K)$, and for each overfield $K' \subset F$ of K the image

$$\tilde{G}_{\lambda,X,K'} = \bar{\rho}_{\lambda,X,K}(\mathrm{Gal}(K'))$$

coincides with the image of

$$\mathrm{Gal}(F/K') \to \mathrm{Gal}(K(X_\lambda)/K') = \tilde{G}_{\lambda,X,K'} \subset \tilde{G}_{\lambda,X,K} \subset \mathrm{Aut}_{k(\lambda)}(X_\lambda).$$

Now if we take as K' a field $\mathcal{K}$ that enjoys the properties (i)-(iii) of Lemma 3.8 then

$$\tilde{G}_{\lambda,X,\mathcal{K}} = \tilde{G}_{\lambda,X,K} \subset \mathrm{Aut}_{k(\lambda)}(X_\lambda)$$

and the surjective group homomorphism

$$\phi_{\mathcal{K}} : \mathrm{Gal}(F/\mathcal{K}) \to \mathrm{Gal}(L/K) = \tilde{G}_{\lambda,X,K}$$

is a *minimal cover*. In particular,

$$\mathrm{End}_{\tilde{G}_{\lambda,X,K}}(X_\lambda) = \mathrm{End}_{\tilde{G}_{\lambda,X,\mathcal{K}}}(X_\lambda).$$

In addition, if $d > 1$ is a positive integer such that $\tilde{G}_{\lambda,X,K}$ does *not* contain a proper subgroup, whose index divides d then $\mathrm{Gal}(F/\mathcal{K})$ also does *not* contain a proper subgroup, whose index divides d. Notice also that since all the endomorphisms of X are defined over F, i,e., $\kappa_{X,K}$ kills $\mathrm{Gal}(F)$, there is the natural homomorphism

$$\mathrm{Gal}(F/K) = \mathrm{Gal}(K)/\mathrm{Gal}(F) \to \mathrm{Aut}(\mathrm{End}(X,i))$$

induced by $\kappa_{X,K}$ such that

$$\mathrm{End}_{K'}(X,i) = \mathrm{End}(X,i)^{\mathrm{Gal}(F/K')}$$

for all fields K' with $K \subset K' \subset F$, including $K' = \mathcal{K}$ or K.

Lemma 3.12. *(*[44, Lemma 3.8 on p. 700]*]) If the centralizer*

$$\mathrm{End}_{\tilde{G}_{\lambda,X,K}}(X_\lambda) = k(\lambda)$$

then $\mathrm{End}_K(X,i) = i(\mathcal{O})$.

Since the natural $\mathbb{Q}$-algebra homomorphisms

$$\mathcal{O} \otimes \mathbb{Q} \to E, \ i(\mathcal{O}) \otimes \mathbb{Q} \to i(E)$$

are obvious isomorphisms, Lemma 3.12 implies the following assertion.

Corollary 3.13. *If the centralizer*

$$\mathrm{End}_{\tilde{G}_{\lambda,X,K}}(X_\lambda)=k(\lambda)$$

then $\mathrm{End}^0_K(X,i)=i(E)$.

Theorem 3.14. *Let us assume that*

$$\mathrm{End}_{\tilde{G}_{\lambda,X,K}}(X_\lambda)=k(\lambda).$$

Suppose that $\tilde{G}_{\lambda,X,K}$ *does not contain a proper subgroup, whose index divides* $d_{X,E}$. *Then:*

(i) $\mathrm{End}^0(X)$ *is a simple* $\mathbb{Q}$*-algebra;*
(ii) $i(E)$ *contains* C_X, *i.e., the center* $i(E)C_X$ *of* $\mathrm{End}^0(X,i)$ *coincides with* $i(E)$*;*
(iii) $\mathrm{End}^0(X,i)$ *is a central simple* $i(E)$*-algebra.*

We prove Theorem 3.14 in Section 5.

4. Semisimple subalgebras of semisimple algebras

This section contains auxiliary results about semisimple algebras over fields that will be used in the proof of Theorems 3.2, 3.3 and 3.4 in Section 5. All associative algebras, subalgebras and rings are assumed to have 1. Let k be a field, $\mathcal{A}$ a finite-dimensional central simple k-algebra. We write $\mathrm{End}(\mathcal{A})$ for the ring of endomorphisms of the additive abelian group A and $\mathrm{End}_k(\mathcal{A})$ for the k-algebra of endomorphisms of the k-vector space $\mathcal{A}$. We have

$$k\cdot \mathrm{id}_{\mathcal{A}}\subset \mathrm{End}_k(\mathcal{A})\subset \mathrm{End}(\mathcal{A})$$

where $\mathrm{id}_{\mathcal{A}}$ is the identity endomorphism of $\mathcal{A}$. One may view $\mathrm{End}_k(\mathcal{A})$ as the centralizer of $k\cdot \mathrm{id}_{\mathcal{A}}$ in $\mathrm{End}(\mathcal{A})$. We write $\mathcal{A}^{\mathrm{opp}}$ for the opposite algebra of $\mathcal{A}$; it is well known that $\mathcal{A}^{\mathrm{opp}}$ is also simple central over k and the natural k-algebra homomorphism

$$\mathcal{A}\otimes_k \mathcal{A}^{\mathrm{opp}}\to \mathrm{End}_k(\mathcal{A}),\ u\otimes v\mapsto \{x\mapsto uxv\ \forall\ x\in \mathcal{A}\}$$

is an isomorphism of (central simple k-algebras). Further we will identify $\mathcal{A}\otimes_k\mathcal{A}^{\mathrm{opp}}$ with $\mathrm{End}_k(\mathcal{A})$ via this isomorphism and

$$\mathcal{A}=\mathcal{A}\otimes 1,\ \mathcal{A}^{\mathrm{opp}}=1\otimes\mathcal{A}^{\mathrm{opp}}$$

with corresponding k-subalgebras of $\mathrm{End}_k(\mathcal{A})$. It is well known that the centralizer of $\mathcal{A}\otimes 1$ (resp. of $1\otimes\mathcal{A}^{\mathrm{opp}}$) in $\mathrm{End}(\mathcal{A})$ actually lies in $\mathrm{End}_k(\mathcal{A})$ (because both subalgebras contain $k\otimes 1=1\otimes k=k\cdot\mathrm{id}_{\mathcal{A}}$) and coincides with $1\otimes\mathcal{A}^{\mathrm{opp}}$ (resp. with $\mathcal{A}\otimes 1$).

Let $\mathcal{B}$ be a k-subalgebra of $\mathcal{A}$. Let $\mathcal{Z}_{\mathcal{A}}(\mathcal{B})$ be the centralizer of $\mathcal{B}$ in $\mathcal{A}$. Clearly, $\mathcal{Z}_{\mathcal{A}}(\mathcal{B})$ is a k-subalgebra of $\mathcal{A}$; in addition, $\mathcal{B}$ lies in the *double centralizer* of B, i.e., in the centralizer $\mathcal{Z}_{\mathcal{A}}(\mathcal{Z}_{\mathcal{A}}(\mathcal{B}))$ of $\mathcal{Z}_{\mathcal{A}}(\mathcal{B})$. It is also clear that the center of $\mathcal{B}$ lies in the center of $\mathcal{Z}_{\mathcal{A}}(\mathcal{B})$. The following assertion is well known in the case of simple $\mathcal{B}$.

Theorem 4.1. *Suppose that* $\mathcal{B}$ *is a semisimple* k*-algebra. Then* $\mathcal{Z}_{\mathcal{A}}(\mathcal{B})$ *is also a semisimple* k*-algebra. In addition, the centralizer of* $\mathcal{Z}_{\mathcal{A}}(\mathcal{B})$ *in* $\mathcal{A}$ *coincides with* $\mathcal{B}$*, i.e.,* $\mathcal{B}$ *coincides with its own double centralizer in* $\mathcal{A}$.

In particular, the centers of $\mathcal{B}$ *and* $\mathcal{Z}_{\mathcal{B}}(\mathcal{A})$ *do coincide.*

If, in addition, $\mathcal{B}$ *is commutative then the center of* $\mathcal{Z}_{\mathcal{A}}(\mathcal{B})$ *coincides with* $\mathcal{B}$.

Proof. The tensor product $\mathcal{B}\otimes_k \mathcal{A}^{\mathrm{opp}}$ is a *semisimple* k-algebra, because $\mathcal{A}^{\mathrm{opp}}$ is central simple and $\mathcal{B}$ is simple. The algebra

$$\mathcal{Z}_{\mathcal{A}}(\mathcal{B})=\mathcal{Z}_{\mathcal{A}}(\mathcal{B})\otimes 1\subset A\otimes_k \mathcal{A}^{\mathrm{opp}}=\mathrm{End}_k(\mathcal{A})$$

coincides with the centralizer of the *semisimple* algebra

$$\mathcal{B}\otimes_k \mathcal{A}^{\mathrm{opp}}\subset \mathcal{A}\otimes_k \mathcal{A}^{\mathrm{opp}}=\mathrm{End}_k(\mathcal{A}),$$

i.e., it is the endomorphism algebra of the *semisimple* $\mathcal{B}\otimes_k \mathcal{A}^{\mathrm{opp}}$-module $\mathcal{A}$ and therefore is semisimple. By the Jacobson density theorem, the double centralizer of

$$\mathcal{B}\otimes_k \mathcal{A}^{\mathrm{opp}}\subset \mathcal{A}\otimes_k \mathcal{A}^{\mathrm{opp}}=\mathrm{End}_k(\mathcal{A})$$

coincides with $\mathcal{B}\otimes_k \mathcal{A}^{\mathrm{opp}}$. On the other hand, if $\mathcal{C}$ is the double centralizer of $\mathcal{B}$ in $\mathcal{A}$ then $\mathcal{C}$ contains $\mathcal{B}$ and $\mathcal{C}\otimes_k \mathcal{A}^{\mathrm{opp}}$ lies in the double centralizer of $\mathcal{B}\otimes_k \mathcal{A}^{\mathrm{opp}}$, i.e.,

$$\mathcal{C}\otimes_k \mathcal{A}^{\mathrm{opp}}\subset \mathcal{B}\otimes_{\mathcal{A}}^{\mathrm{opp}} .$$

This implies that $\mathcal{C}\subset\mathcal{B}$ and therefore $\mathcal{C}=\mathcal{B}$. □

Theorem 4.2. *Let $\mathcal{B}$ be a simple k-subalgebra of $\mathcal{A}$.*

Then its centralizer $\mathcal{Z}_{\mathcal{A}}(\mathcal{B})$ is also a simple k-algebra. In addition,

$$\dim_k(\mathcal{B})\cdot\dim_k(\mathcal{Z}_{\mathcal{A}}(\mathcal{B}))=\dim_k(\mathcal{A}).$$

Proof. This is a special case of Theorem 4.3.2 on p. 104 of [7] □

4.3. Iy is well known that $\dim_k(\mathcal{A})$ is a square. Let us put

$$d=d_{\mathcal{A}}:=\sqrt{\dim_k(\mathcal{A})}.$$

Let k_0 be a subfield of k such that k/k_0 is a finite algebraic *separable* field extension. Let $\bar{k}_0$ be an algebraic closure of k_0. We write Σ_k for the $[k:k_0]$-element set of k_0-linear field embeddings $k\hookrightarrow\bar{k}_0$. It is well known that the canonical homomorphism of semisimple commutative $\bar{k}_0$-algebras

$$k\otimes_{k_0}\bar{k}_0\to\oplus_{\sigma\in\Sigma_k}k\otimes_{k,\sigma}\bar{k}_0$$

is an isomorphism. Notice also that each $k\otimes_{k,\sigma}\bar{k}_0$ is canonically isomorphic to $\bar{k}_0$. This implies easily that the canonical homomorphism of semisimple $\bar{k}_0$-algebras

$$\mathcal{A}\otimes_{k_0}\bar{k}_0\to\oplus_{\sigma\in\Sigma_k}\mathcal{A}\otimes_{k,\sigma}\bar{k}_0$$

is an isomorphism. In addition, each $\mathcal{A}\otimes_{k,\sigma}\bar{k}_0$ is isomorphic to the matrix algebra $\mathrm{M}_d(\bar{k}_0)$ of size d over $\bar{k}_0$. This implies that $\mathcal{A}\otimes_{k_0}\bar{k}_0$ is isomorphic to a direct sum of $[k:k_0]$ copies of $\mathrm{M}_d(\bar{k}_0)$.

Remark 4.4. Suppose that $\mathrm{char}(k_0)=0$ and provide $\mathcal{A}$ with the structure of the (reductive) k_0-Lie algebra, defining

$$[u,v]=uv-vu\ \forall u,v\in\mathcal{A}.$$

Then $[k:k_0]d_{\mathcal{A}}$ is the rank $\mathrm{rk}(\mathcal{A}/k_0)$ of the reductive k_0-Lie algebra $\mathcal{A}$. Indeed, the rank of the k_0-Lie algebra $\mathcal{A}$ coincides with the rank of the $\bar{k}_0$-Lie algebra $\mathcal{A}\otimes_{k_0}\bar{k}_0$ while the latter equals $[k:k_0]$ times the rank of $\mathrm{M}_d(\bar{k}_0)$. It remains to recall that the rank of $\mathrm{M}_d(\bar{k}_0)$ over $\bar{k}_0$ equals $d=d_{\mathcal{A}}$.

Theorem 4.5. *Let $\mathcal{E}$ be a subfield of $\mathcal{A}$ such that $\mathcal{E} \supset k_0$. (In particular, $\mathcal{A}$ and $\mathcal{E}$ have the same multiplicative identity* 1*.) Let $k\mathcal{E} \subset \mathcal{A}$ be the image of the natural k-algebra homomorphism*

$$\mathcal{E} \otimes_{k_0} k \to \mathcal{A},\ u \otimes c \mapsto uc = cu\ \forall u \in \mathcal{E}, c \in k.$$

and $\mathcal{Z}_{\mathcal{A}}(\mathcal{E}) \subset \mathcal{A}$ the centralizer of $\mathcal{E}$ in $\mathcal{A}$.

Then $\mathcal{E}, k\mathcal{E}$ and $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ enjoy the following properties.

(0) *The degree $[\mathcal{E} : k_0]$ divides $\mathrm{rk}(\mathcal{A}/k_0) = [k : k_0]d_{\mathcal{A}}$. In addition, if $k\mathcal{E}$ is a field then $[k\mathcal{E} : k_0]$ divides $[k : k_0]d_{\mathcal{A}}$, the degree $[k\mathcal{E} : k]$ divides $d_{\mathcal{A}}$ and $[k\mathcal{E} : \mathcal{E}]$ divides $[k : k_0]d_{\mathcal{A}}/[\mathcal{E} : k_0]$.*

(i) *$k\mathcal{E}$ is a commutative semisimple k-algebra.*

(ii) *$\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ is a semisimple k-algebra that coincides with the centralizer of $k\mathcal{E}$ in $\mathcal{A}$.*

(iii) *The center of $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ coincides with $k\mathcal{E}$. The centralizer of $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ in $\mathcal{A}$ coincides with $k\mathcal{E}$.*

(iv) *$\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ is a simple k-algebra if and only if $k\mathcal{E}$ is a field. (E.g., if $\mathcal{E}$ contains k.)*

(v) *If $\mathrm{char}(k_0) = 0$ then*

$$\dim_{\mathcal{E}}(\mathcal{Z}_{\mathcal{A}}(\mathcal{E})) \le \left(\frac{d_{\mathcal{A}}[k : k_0]}{[\mathcal{E} : k_0]}\right)^2.$$

(vi) *If $\mathrm{char}(k_0) = 0$ then the equality*

$$\dim_{\mathcal{E}}(\mathcal{Z}_{\mathcal{A}}(\mathcal{E})) = \left(\frac{d_{\mathcal{A}}[k : k_0]}{[\mathcal{E} : k_0]}\right)^2$$

holds if and only if $\mathcal{E}$ contains k_0.

Example 4.6. If $\mathcal{E} = k$ then $[\mathcal{E} : k_0] = [k : k_0]$ and $\mathcal{Z}_{\mathcal{A}}(\mathcal{E}) = \mathcal{A}$. Then

$$\dim_k(\mathcal{Z}_{\mathcal{A}}(\mathcal{E})) = d_{\mathcal{A}}^2 = \left(\frac{d_{\mathcal{A}}[k : k_0]}{[k : k_0]}\right)^2 = \left(\frac{d_{\mathcal{A}}[k : k_0]}{[\mathcal{E} : k_0]}\right)^2.$$

Remark 4.7. If $\mathrm{char}(k_0) = 0$ then the ranks of the k_0-Lie algebra $\mathcal{A}$ and its subalgebra $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ coincide. Indeed, it suffices to check that $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ contains a Cartan subalgebra of $\mathcal{A}$. In order to do that, notice that $\mathcal{E}/k_0$ is a finite separable field extension and therefore there is $u \in \mathcal{E}$ that generates $\mathcal{E}$ over k_0. Clearly, u is semisimple and the centralizer of u in $\mathcal{A}$ coincides with the centralizer of $\mathcal{E}$, i.e., with $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$. Since u is semisimple, there is a Cartan subalgebra $\mathfrak{h}$ of $\mathcal{A}$ that contains u. Since $\mathfrak{h}$ is commutative, it commutes with its own element u and therefore lies in $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$. This ends the proof.

Proof of Theorem 4.5. Since k/k_0 is separable, $\mathcal{E} \otimes_{k_0} k$ is isomorphic to a direct sum of fields. The same is true for its quotient $k\mathcal{E}$, which proves (i). Since k is is the center of $\mathcal{A}$ and $k\mathcal{E}$ is generated by k and $\mathcal{E}$, the centralizer of semisimple k-akgebra $k\mathcal{E}$ coincides with the centralizer of $\mathcal{E}$. Now (ii) follows from Theorem 4.1. Since $k\mathcal{E}$ is commutative, (iii) follows from (ii), thanks to Theorem 4.1, and (iv) follows from (ii) and (iii).

Let us prove (v) and (vi). Recall that $\mathcal{Z}_{\mathcal{A}}(\mathcal{E}) = \mathcal{Z}_{\mathcal{A}}(k\mathcal{E})$.

First, assume that $k\mathcal{E}$ is a field. Then

$$[k\mathcal{E} : k] \cdot [k : k_0] = [k\mathcal{E} : k_0] = [k\mathcal{E} : \mathcal{E}] \cdot [\mathcal{E} : k_0],\ [\mathcal{E} : k_0] \le [k\mathcal{E} : k_0]$$

and therefore

$$\frac{[k\mathcal{E}:\mathcal{E}]}{[k\mathcal{E}:k_0]^2}=\frac{1}{[\mathcal{E}:k_0][k\mathcal{E}:k_0]}\le\frac{1}{[\mathcal{E}:k_0]^2}; \tag{2}$$

the equality holds if and only if $[k\mathcal{E}:k_0]=[\mathcal{E}:k_0]$, i.e., $k\mathcal{E}=\mathcal{E}$, which means that $\mathcal{E}$ contains k.

By Theorem 4.2,

$$\dim_k(\mathcal{Z}_{\mathcal{A}}(\mathcal{E}))=\dim_k(\mathcal{Z}_{\mathcal{A}}(k\mathcal{E}))=\frac{\dim_k(\mathcal{A})}{[k\mathcal{E}:k]}=\frac{d_{\mathcal{A}}^2}{[k\mathcal{E}:k]}.$$

This implies that the $k\mathcal{E}$-dimension of $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ is given by the formula

$$\dim_{k\mathcal{E}}(\mathcal{Z}_{\mathcal{A}}(\mathcal{E}))=\frac{\dim_{k\mathcal{E}}(\mathcal{Z}_{\mathcal{A}}(\mathcal{E}))}{[k\mathcal{E}:k]}=\frac{d_{\mathcal{A}}^2}{[k\mathcal{E}:k][k\mathcal{E}:k]}=\frac{d_{\mathcal{A}}^2}{[k\mathcal{E}:k]^2}.$$

It follows that the $\mathcal{E}$-dimension of $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ is given by the formula

$$\dim_{\mathcal{E}}(\mathcal{Z}_{\mathcal{A}}(\mathcal{E}))=[k\mathcal{E}:\mathcal{E}]\cdot\dim_{k\mathcal{E}}(\mathcal{Z}_{\mathcal{A}}(\mathcal{E}))=\frac{[k\mathcal{E}:\mathcal{E}]}{[k\mathcal{E}:k]^2}\cdot d_{\mathcal{A}}^2=$$

$$\frac{[k\mathcal{E}:\mathcal{E}]}{[k\mathcal{E}:k]^2[k:k_0]^2}\cdot[k:k_0]^2d_{\mathcal{A}}^2=\frac{[k\mathcal{E}:\mathcal{E}]}{[k\mathcal{E}:k_0]^2}\cdot([k:k_0]d_{\mathcal{A}})^2\le$$

$$\frac{1}{[\mathcal{E}:k_0]^2}\cdot([k:k_0]d_{\mathcal{A}})^2;$$

in light of (2), the equality holds if and only if $\mathcal{E}$ contains k.

Now suppose that $k\mathcal{E}$ is *not* a field and let us split semisimple $k\mathcal{E}$ into a finite direct sum

$$k\mathcal{E}=\oplus_{j\in J}F_j$$

of fields F_j. Here the set of indices J is finite nonempty but *not* a singleton. We write e_j for the idenity element of $F_j\subset k\mathcal{E}$. Clearly,

$$e_j^2=e_j,\ \sum_{j\in J}e_j=1\in\mathcal{A},\ e_je_{j'}=0\ \forall j\ne j'. \tag{3}$$

The map

$$i_j:\mathcal{E}\to F_j,\ u\mapsto e_ju=e_jue_j$$

is a field embedding. Let us put

$$\mathcal{A}_j=e_j\mathcal{Z}_{\mathcal{A}}(\mathcal{E})=e_j\mathcal{Z}_{\mathcal{A}}(\mathcal{E})e_j\subset\mathcal{Z}_{\mathcal{A}}(\mathcal{E})\subset\mathcal{A}.$$

Clearly, $\mathcal{A}_j$ is a central simple F_j-algebra and

$$\mathcal{Z}_{\mathcal{A}}(\mathcal{E})=\oplus_{j\in J}\mathcal{A}_j.$$

The field embedding $i_j:\mathcal{E}\to F_j$ allows us to view $\mathcal{A}_j$ as $\mathcal{E}$-algebra. Clearly,

$$\dim_{\mathcal{E}}(\mathcal{Z}_{\mathcal{A}}(\mathcal{E}))=\sum_{j\in J}\dim_{\mathcal{E}}(\mathcal{A}_j).$$

Let us put

$$d_j:=\sqrt{\dim_{F_j}(\mathcal{A}_j)};$$

all d_j are positive integers.

Applying Remark 4.3 to F_j (instead of k) and $\mathcal{A}_j$ (instead of $\mathcal{A}$), we conclude that the rank $\mathrm{rk}(\mathcal{A}_j)$ of k_0-Lie algebra $\mathcal{A}_j$ is $[F_j:k_0]d_j$. This implies that the rank of the reductive k_0-Lie subalgebra $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ of $\mathcal{A}$ is $\sum_{j\in J}[F_j:k_0]d_j$. Remarks 4.3 and 4.7 imply that

$$\sum_{j\in J}[F_j:k_0]d_j=[k:k_0]d_{\mathcal{A}}.$$

Applying the already proven case of (v) to F_j (instead of k), $\mathcal{A}_j$ (instead of $\mathcal{A}$) and the field $i_j(E)$, we conclude that

$$\dim_{\mathcal{E}}(\mathcal{A}_j)=\dim_{i_j(\mathcal{E})}(\mathcal{A}_j)\le\frac{([F_j:k_0]d_j)^2}{[i_j(\mathcal{E}):k_0]^2}=\frac{([F_j:k_0]d_j)^2}{[\mathcal{E}:k_0]^2}.$$

This implies that

$$\dim_{\mathcal{E}}(\mathcal{Z}_{\mathcal{A}}(\mathcal{E}))=\sum_{j\in J}\dim_{\mathcal{E}}(\mathcal{A}_j)\le\frac{\sum_{j\in J}([F_j:k_0]d_j)^2}{[\mathcal{E}:k_0]^2}.$$

Since J is *not* a singleton and all d_j are positive,

$$\sum_{j\in J}([F_j:k_0]d_j)^2<\left(\sum_{j\in J}[F_j:k_0]d_j\right)^2=(d_{\mathcal{A}}[k:k_0])^2.$$

This implies that

$$\dim_{\mathcal{E}}(\mathcal{Z}_{\mathcal{A}}(\mathcal{E}))<\frac{(d_{\mathcal{A}}[k:k_0])^2}{[\mathcal{E}:k_0]^2},$$

which ends the proof of (v) and (vi).

It remains to prove (0). First assume that $k\mathcal{E}$ is a field. Then $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ is a central simple $k\mathcal{E}$-algebra. Then the rank of k_0-Lie algebra $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ equals $[k\mathcal{E}:k_0]\cdot\mathbf{d}$ where the positive integer

$$\mathbf{d}:=\sqrt{\dim_{k\mathcal{E}}(\mathcal{Z}_{\mathcal{A}}(\mathcal{E}))}.$$

By Remark 4.7, the ranks of $\mathcal{A}$ and $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ do coincide and therefore the rank of k_0-Lie algebra $\mathcal{A}$ is divisible by $[k\mathcal{E}:k_0]$. This means that $[k:k_0]d_{\mathcal{A}}$ is divisible by $[k\mathcal{E}:k_0]$, $[k:k_0]d_{\mathcal{A}}$ is divisible by $[k\mathcal{E}:k_0]$. Since $[k\mathcal{E}:k_0]=[k\mathcal{E}:\mathcal{E}][\mathcal{E}:k_0]$, $[k\mathcal{E}:k]$ divides $]d_{\mathcal{A}}$ and $[k\mathcal{E}:\mathcal{E}]$ divides $[k:k_0]d_{\mathcal{A}}/[\mathcal{E}:k_0]$. In addition, $[k\mathcal{E}:\mathcal{E}]$ divides $[k:k_0]d_{\mathcal{A}}/[\mathcal{E}:k_0]$.

Now let us do the general case when (in the notation above) $k\mathcal{E}$ is a direct sum $\oplus_{j\in J}F_j$ of overfields $F_j\supset E$ and $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ is a direct sum $\oplus_{j\in J}\mathcal{A}_j$ of central simple F_j-algebras $\mathcal{A}_j$. Then the rank of k_0-Lie algebra $\mathcal{A}_j$ equals $[F_j:k_0]\cdot\mathbf{d}_j$ where the positive integer

$$\mathbf{d}_j=\sqrt{\dim_{F_j}(\mathcal{A}_j)}.$$

Since $[F_j:k_0]$ is divisible by $[\mathcal{E}:k_0]$, the rank of $\mathcal{A}_j$ is also divisible by $[\mathcal{E}:k_0]$. Since the rank of $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ is the sum of the ranks of $\mathcal{A}_j$, it is also divisible by $[\mathcal{E}:k_0]$. By Remark 4.7, the ranks of $\mathcal{A}$ and $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ do coincide and therefore the rank of k_0-Lie algebra $\mathcal{A}$ is divisible by $[\mathcal{E}:k_0]$. □

4.8. We write $\mathrm{Aut}_{k_0}(\mathcal{A})$ for the automorphism group of the (associative) k_0-algebra $\mathcal{A}$. Let G be a group and

$$\rho:G\to\mathrm{Aut}_{k_0}(\mathcal{A})$$

be a group homomorphism. Clearly, k_0 lies in the subalgebra $\mathcal{A}^G$ of G-invariants of $\mathcal{A}$. It is also clear that G leaves stable the center k, i.e., ρ induces the group homomorphism

$$\rho_k:G\to\mathrm{Aut}(k/k_0)$$

where $\mathrm{Aut}(k/k_0)$ is the (finite) automorphism group of the field extension k/k_0.

Theorem 4.9. *Suppose that $\mathcal{E}$ is a field that lies in $\mathcal{A}^G$ and contains k_0. Then $\mathcal{E}$ and $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ enjoy the following properties.*

(i) *The field $\mathcal{E}$ is a finite algebraic extension of k_0 and the degree $[\mathcal{E}:k_0]$ divides $\mathrm{rk}(\mathcal{A}/k_0)=[k:k_0]d_{\mathcal{A}}$.*

(ii) *The subalgebras $k\mathcal{E}$ and $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ of $\mathcal{A}$ are G-stable.*

(iii) *Let us assume that (in the notation above) $k\mathcal{E}$ is a finite direct sum $\oplus_{j\in J}F_j$ of overfields $F_j\supset\mathcal{E}$ and $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ is a finite direct sum $\oplus_{j\in J}\mathcal{A}_j$ of central simple F_j-algebras $\mathcal{A}_j=e_j\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$. Then there is a group homomorphism*
$$\rho_J: G\to \mathrm{Perm}(J)$$
of G into the group $\mathrm{Perm}(J)$ of permutations of J such that if $\rho_J(j)=j'$ then
$$\rho(g)(F_j)=F_{j'}, \rho(g)(\mathcal{A}_j)=\mathcal{A}_{j'}\ \forall g\in G.$$

(iiibis) *If $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})^G=\mathcal{E}$ then the action of G on J is transitive; in particular, for each $j,j'\in J$ there is a k_0-linear field isomorphism $F_j\cong F_{j'}$ that extends to an isomorphism of k_0-algebras $\mathcal{A}_j\cong\mathcal{A}_{j'}$. In particular, positive integers*
$$\mathbf{e}_{\mathcal{E}}=[F_j:\mathcal{E}],\ \mathbf{d}_{\mathcal{E}}=\sqrt{\dim_{F_j}(\mathcal{A}_j)}$$
do not depend on a choice of j and
$$[k:k_0]d_{\mathcal{A}}=|J|\mathbf{e}_{\mathcal{E}}\mathbf{d}_{\mathcal{E}}[\mathcal{E}:k_0].$$
Here $|J|$ is the cardinality of J.

(iv) *If $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})^G=\mathcal{E}$ and G does not contain a proper subgroup with finite index dividing $([k:k_0]d_{\mathcal{A}})/[\mathcal{E}:k_0]$ then J is a singleton, $k\mathcal{E}$ is a field and $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})$ is a central simple $k\mathcal{E}$-algebra.*

(v) *If $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})^G=\mathcal{E}$ and $k\mathcal{E}$ is a field then $k\mathcal{E}/\mathcal{E}$ is a finite Galois field extension, whose degree $[k\mathcal{E}:\mathcal{E}]$ divides $([k:k_0]d_{\mathcal{A}})/[\mathcal{E}:k_0]$. In addition, ρ_k induces the surjective group homomorphism*
$$\rho_{k\mathcal{E}}: G\twoheadrightarrow \mathrm{Gal}(k\mathcal{E}/\mathcal{E}).$$
In particular, if G does not admit a proper normal subgroup with finite index dividing $([k:k_0]d_{\mathcal{A}})/[\mathcal{E}:k_0]$ then $k\mathcal{E}=\mathcal{E}$, i.e., $\mathcal{E}$ contains k.

Proof. (i) follows from the inclusion $k_0\subset\mathcal{E}$ and Theorem 4.5(0).

(ii) is obvious.

Let us prove (iii). The set $\{\mathcal{A}_j\mid j\in J\}$ is the set of (nonzero) minimal two-sided ideals of $\mathcal{A}$. Therefore G permutes elements of this set, i.e, there is the group homomorphism
$$\rho_J: G\to \mathrm{Perm}(J)$$
of G into the group $\mathrm{Perm}(J)$ of permutations of J such that if $g\in G$ and $\rho_J(g)(j)=j'$ then $\rho(g)(\mathcal{A}_j)=\mathcal{A}_{j'}$. Since F_j (resp. $F_{j'}$) is the center of $\mathcal{A}_j$ (resp. of $\mathcal{A}_{j'}$) with identity element e_j (resp. $e_{j'}$),
$$\rho(g)(F_j)=F_{j'},\ \rho(g)(e_j)=e_{j'}. \tag{4}$$

Let us prove (iiibis). We need to check the transitivity of the G-action on J. Notice that for each nonempty G-invariant subset $T\subset J$ the sum $e_T=\sum_{j\in T}e_j$ is a nonzero element of $\mathcal{A}$ that is G-invariant, thanks to(4). This implies that e_T is a nonzero element of $\mathcal{Z}_{\mathcal{A}}(\mathcal{E})^G=\mathcal{E}$. If the action onf G on J is *not* transitive then J

is not a singleton and there exist two disjoint G-orbits $T_1, T_2 \subset J$. It follows from (3) that $e_{T_1}e_{T_2} = 0$. Since both factors are nonzero elements of the *field* $\mathcal{E}$, we get a desired contradiction that proves the transitivity. This proves (iiibis).

(iv) follows readily from the transitivity of the G-action on J.

Let us prove (v). So, $k\mathcal{E}$ be a field. Then $k\mathcal{E}/\mathcal{E}$ is a finite algebraic field extension and it follows from Theorem 4.5(0) that $[k\mathcal{E} : \mathcal{E}]$ divides $([k : k_0]d_{\mathcal{A}})/[\mathcal{E} : k_0]$. Clearly, $k\mathcal{E}$ is G-stable and the subfield $(k\mathcal{E})^G$ of its G-invariants coincides with $\mathcal{E}$. This gives us the natural group homomorphism

$$\rho_{k\mathcal{E}} : G \to \mathrm{Aut}(k\mathcal{E}/\mathcal{E}),$$

whose image $H := \rho_{k\mathcal{E}}(G) \subset \mathrm{Aut}(k\mathcal{E}/\mathcal{E})$ is a finite group (whose order does not exceed $[k\mathcal{E} : \mathcal{E}]$. Since the subfield of H-invariants

$$(k\mathcal{E})^H = (k\mathcal{E})^G = \mathcal{E},$$

the order of H coincides with $[k\mathcal{E} : \mathcal{E}]$, the field extension $k\mathcal{E}/\mathcal{E}$ is Galois with Galois group H. Since the group homomorphism $\rho_{k\mathcal{E}} : G \to H$ is surjective, its kernel $\ker(\rho_{k\mathcal{E}})$ is a normal subgroup in G of index $[k\mathcal{E} : \mathcal{E}]$. This implies that $\ker(\rho_{k\mathcal{E}})$ is a normal subgroup of G, whose index divides $([k : k_0]d_{\mathcal{A}})/[E : k_0]$. Therefore, if G does not admit a proper normal subgroup with finite index dividing $([k : k_0]d_{\mathcal{A}})/[E : k_0]$ then $G = \ker(\rho_{k\mathcal{E}})$ and therefore $[k\mathcal{E} : \mathcal{E}] = 1$, i.e., $k\mathcal{E} = \mathcal{E}$, which means that $\mathcal{E}$ contains k.

□

4.10. In this subsection we assume that $\mathfrak{A}$ is a semisimple finite-dimensional algebra over a field k_0 of characteristic zero. Then $\mathfrak{A}$ splits into a finite direct sum

$$\mathfrak{A} = \oplus_{s \in \mathfrak{I}(\mathfrak{A})}\mathcal{A}_s$$

of simple k_0-algebras $\mathcal{A}_s$. (Here the finite nonempty set $\mathfrak{I}(\mathfrak{A})$ is identified with the set of (nonzero) minimal two-sided ideals in $\mathfrak{A}$.)

Example 4.11. If $k_0 = \mathbb{Q}$ and $\mathfrak{A} = \mathrm{End}^0(X)$ then $\mathfrak{I}(\mathrm{End}^0(X)) = \mathcal{I}(X)$.

Let G be a group and

$$\rho : G \to \mathrm{Aut}_{k_0}(\mathfrak{A})$$

be a group homomorphism. Clearly, ρ induces the action of G on $\mathfrak{I}(\mathfrak{A})$ such that

$$\rho(g)\mathcal{A}_s = \mathcal{A}_{gs} \ \forall g \in G, \ s \in \mathfrak{I}(\mathfrak{A}).$$

Let $\mathcal{E}$ be a subfield of $\mathfrak{A}$ that contains k_0 and lies in the subalgebra $\mathfrak{A}^G$ of G-invariants. Then the centralizer $\mathcal{Z}_{\mathfrak{A}}(\mathcal{E})$ of $\mathcal{E}$ in $\mathfrak{A}$ is G-stable.

Lemma 4.12. *Let us assume that the subalgebra $\mathcal{Z}_{\mathfrak{A}}(\mathcal{E})^G$ of G-invariants of $\mathcal{Z}_{\mathfrak{A}}(\mathcal{E})$ is a field. Then the action of G on $\mathfrak{I}(\mathfrak{A})$ is transitive. In particular, simple k_0-algebras $\mathcal{A}_s$ and $\mathcal{A}_t$ are isomorphic for each pair $s, t \in \mathcal{I}(\mathfrak{A})$.*

Proof. We use the same idea as in the proof of Theorem 4.9(iii). Let

$$e_s \in \mathcal{A}_t \subset \sum_{t \in \mathfrak{I}(\mathfrak{A})} \mathcal{A}_t = \mathfrak{A}$$

be the identity element of $\mathcal{A}_s$. Clearly, e_s lies in the center of $\mathfrak{A}$ and

$$\rho(g)e_s = e_{gs} \ \forall g \in G, \ s \in \mathcal{I}(\mathfrak{A}).$$

It is also clear that $e_se_t = 0$ for distinct elements s and t of $\mathcal{I}(\mathfrak{A})$. Notice that for each nonempty G-invariant subset $T \subset \mathfrak{I}(\mathfrak{A})$ the sum $e_T = \sum_{t \in T} e_t$ is a nonzero *central* element of $\mathfrak{A}$ that is G-invariant. This implies that e_T is a nonzero element of $\mathcal{Z}_{\mathfrak{A}}(E)^G$. If the action on G on $\mathcal{I}(\mathfrak{A})$ is *not* transitive then J there exist two disjoint G-orbits $T_1, T_2 \subset \mathfrak{I}(\mathfrak{A})$. Clearly, $e_{T_1} e_{T_2} = 0$. Since both factors are nonzero elements of the *field* $\mathcal{Z}_{\mathfrak{A}}(E)^G$, we get a desired contradiction that proves the transitivity. □

Corollary 4.13. *We keep the notation and assumptions of Lemma 4.12. Suppose that K_a is an algebraically closed field of characteristic* 0 *that contains k_0 and we are given a nonempty family $\{\mathcal{M}_\tau \mid \tau \in \Sigma\}$ of finite-dimensional K_a-vector spaces $\mathcal{M}_\tau$ that enjoy the following properties.*

(i) *Not all $\mathcal{M}_\tau = \{0\}$.*

(ii) *For each $\tau \in \Sigma$ we are given a homomorphism of k_0-algebras*

$$\mathcal{Z}_{\mathfrak{A}}(\mathcal{E}) \to \mathrm{End}_{K_a}(\mathcal{M}_\tau)$$

that sends 1 *to the identity automorphism of $\mathcal{M}_\tau$.*

If the largest common divisor of all $\dim_{K_a}(\mathcal{M}_\tau)$ is 1 *then $\mathcal{Z}_{\mathfrak{A}}(\mathcal{E})$ is a finite-dimensional semisimple commutative $\mathcal{E}$-algebra, which is either a field or isomorphic to a direct sum of finitely many copies of the same field.*

Proof. Applying Lemma 4.12 to the semisimple $\mathcal{E}$-algebra $\mathcal{Z}_{\mathfrak{A}}(\mathcal{E})$ (instead of the k_0-algebra $\mathfrak{A}$), we obtain that $\mathcal{Z}_{\mathfrak{A}}(\mathcal{E})$ is isomorphic to a direct sum of copies of a certain finite-dimensional simple $\mathcal{E}$-algebra say, $\mathcal{B}$. The center F of $\mathcal{B}$ is an overfield of $\mathcal{E}$ and the field extension $F/\mathcal{E}$ is finite algebraic. As usual,

$$d_{\mathcal{B}} = \sqrt{\dim_F(\mathcal{B})}$$

is a positive integer. This implies that the tensor product $\mathcal{B} \otimes_{k_0} K_a$ is isomorphic as a K_a-algebra to a direct sum of $[\mathcal{E} : k_0]$ copies of the matrix algebra $\mathrm{M}_{d_{\mathcal{B}}}(K_a)$ of size $d_{\mathcal{B}}$ over K_a. This implies that $\mathcal{Z}_{\mathfrak{A}}\mathcal{E}) \otimes_{k_0} K_a$ is isomorphic as a K_a-algebra to a direct sum of copies of $\mathrm{M}_{d_{\mathcal{B}}}(K_a)$. On the other hand, each $\mathcal{M}_\tau$ carries the natural structure of $\mathcal{Z}_{\mathfrak{A}}\mathcal{E}) \otimes_{k_0} K_a$-module. Since the K_a-dimension of every finite-dimensional $\mathrm{M}_{d_{\mathcal{B}}}(K_a)$-module is divisible by $d_{\mathcal{B}}$, all $\dim_{K_a}(\mathcal{M}_\tau)$ are divisible by $d_{\mathcal{B}}$. This implies that $d_{\mathcal{B}} = 1$, i.e., $\mathcal{B} = F$ is a field. □

5. Abelian varieties and centralizers

In this section we are going to prove Theorems 3.2, 3.3 and 3.4. We will use Theorem 4.5 in order to prove Theorem 5.1 below that is a special case of these Theorems. Later we deduce from Theorem 5.1 the general case.

Theorem 5.1. *Suppose that Y is a positive-dimensional abelian variety over K_a that enjoys the following equivalent properties.*

(a) $\mathrm{End}^0(Y)$ *is a simple $\mathbb{Q}$-algebra.*

(b) *The center C_Y of* $\mathrm{End}^0(Y)$ *is a number field and* $\mathrm{End}^0(Y)$ *is a central simple algebra over C_Y.*

(c) *There exists a simple abelian variety Z over K_a such that Y is isogenous over K_a to a self-product of Z.*

Let E be a number field and $i : E \hookrightarrow \mathrm{End}^0(Y)$ be a $\mathbb{Q}$-algebra embedding. Then the E-algebra $\mathrm{End}^0(Y, i)$ *enjoys the following properties.*

(i) $\mathrm{End}^0(Y, i)$ *is semisimple.*

(ii) $\mathrm{End}^0(Y,i)$ *is simple if and only if* $i(E)C_Y$ *is a field* [2] *. (E.g.,* $C_Y \subset E$ *or* $E \subset C_Y$ *or number fields* E *and* C_Y *are linearly disjoint over* $\mathbb{Q}$*.) If this is the case then* $\mathrm{End}^0(Y,i)$ *is a central simple algebra over the field* $i(E)C_Y$*.*

(iii)

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

(iv) *The equality*

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

holds if and only if

$$\dim_{C_Y}(\mathrm{End}^0(Y)) = \left(\frac{2\dim(Y)}{[C_Y:\mathbb{Q}]}\right)^2$$

and E *contains* C_Y*.*

Remark 5.2. (i) Suppose that Y satisfies the equivalent conditions (a),(b),(c) of Theorem 5.1. This means that there are a simple abelian variety Z over K_a and a positive integer r such that Y is isogenous to Z^r over K_a. In addition, $\mathrm{End}^0(Z)$ is a central division C_Y-algebra and $\mathrm{End}^0(Y)$ is isomorphic to the matrix algebra $\mathrm{M}_r(\mathrm{End}^0(Z))$ of size r over $\mathrm{End}^0(Z)$; in particular, fields C_Y and C_Z are isomorphic. We have

$$\dim(Y) = r\cdot\dim(Z),\ \dim_{C_Y}(\mathrm{End}^0(Y)) = r^2\dim_{C_Z}(\mathrm{End}^0(Z)).$$

Recall that the number

$$d(Z) := \sqrt{\dim_{C_Z}(\mathrm{End}^0(Z))}$$

is a positive integer.

It follows from Albert's classification [14, Sect. 21] that $d(Z)\cdot[C_Z:\mathbb{Q}]$ divides $2\dim(Z)$. This implies that

$$r\cdot d(Z)\cdot[C_Z:\mathbb{Q}] = \sqrt{\dim_{C_Y}(\mathrm{End}^0(Y))}\cdot[C_Z:\mathbb{Q}],$$

which divides $2r\cdot\dim(Z) = 2\dim(Y)$. Now if we put

$$k_0 = \mathbb{Q},\ k = C_Y,\ \mathcal{A} = \mathrm{End}^0(Y)$$

then

$$[k:k_0] = [C_Y:\mathbb{Q}] = [C_Z:\mathbb{Q}],\ d_{\mathcal{A}} = \sqrt{\dim_{C_Y}(\mathrm{End}^0(Y))} = r\cdot d(Z)$$

and

$$[k:k_0]d_{\mathcal{A}} = [C_Y:\mathbb{Q}]r\cdot d(Z) = [C_Z:\mathbb{Q}]r\cdot d(Z),$$

which divides $r\cdot 2\dim(Z) = 2\dim(Y)$. In particular,

$$[k:k_0]d_{\mathcal{A}} \le 2\dim(Y);$$

the equality holds if and only if

$$d(Z)\cdot[C_Z:\mathbb{Q}] = 2\dim(Z).$$

[2] Last sentences of [38, Remark 4.1] and [44, Remark 3.1] wrongly assert the simplicity of $\mathrm{End}^0(Y,i)$ without assuming that $i(E)C_Y$ is a field. The mistake was caused by improper use of [7, Theorem 4.3.2 on p. 104].

Notice that this equality is equivalent to

$$\dim_{C_Z}(\mathrm{End}^0(Z)) = \left(\frac{2\dim(Z)}{[C_Z:\mathbb{Q}]}\right)^2,$$

which, in turn, is equivalent to

$$\dim_{C_Y}(\mathrm{End}^0(Y)) = \left(\frac{2\dim(Y)}{[C_Y:\mathbb{Q}]}\right)^2. \tag{5}$$

(ii) Now assume that (5) holds. We have

$$r\cdot d(Z) = \frac{2\dim(Y)}{[C_Y:\mathbb{Q}]}.$$

Let E be a subfield of $\mathrm{End}^0(Y)$ that contains C_Y and $i: E \hookrightarrow \mathrm{End}^0(Y)$ be the inclusion map. It follows from Theorems 4.1 and 4.2 applied to $\mathcal{E} = i(E)$ that $\mathrm{End}^0(Y,i)$ is a central simple E-algebra and

$$\dim_{C_Y}(\mathrm{End}^0(Y)) = [E:C_Y]\cdot \dim_{C_Y}(\mathrm{End}^0(Y,i)).$$

This implies that

$$\dim_E(\mathrm{End}^0(Y,i)) = \frac{\dim_{C_Y}(\mathrm{End}^0(Y,i))}{[E:C_Y]} = \frac{\dim_{C_Y}(\mathrm{End}^0(Y))}{[E:C_Y]^2} =$$

$$\frac{(2\dim(Y))^2}{[C_Y:\mathbb{Q}]^2[E:C_Y]^2} = \left(\frac{2\dim(Y)}{[E:\mathbb{Q}]}\right)^2.$$

(iii) For example, let F be a (maximal) subfield of $\mathrm{End}^0(Z)$ such that

$$C_Z \subset F,\ [F:C_Z] = d(Z)$$

and let L/C_Z be a degree r field extension that is linearly disjoint with F. Then $E := F\otimes_{C_Z} L$ is an overfield of C_Z and

$$[E:\mathbb{Q}] = [E:C_Z]\cdot[C_Z:\mathbb{Q}] = [F:C_Z]\cdot[L:C_Z]\cdot[C_Z:\mathbb{Q}] = r\cdot d(Z)\cdot[C_Z:\mathbb{Q}] =$$

$$\frac{2\dim(Y)}{[C_Y:\mathbb{Q}]}\cdot[C_Y:\mathbb{Q}] = 2\dim(Y).$$

Let us fix an embedding

$$i_0 : L \hookrightarrow \mathrm{M}_r(C_Y) \subset \mathrm{M}_r(\mathrm{End}^0(Z))$$

that sends 1 to 1. Then

$$E = F\otimes_{C_Z} L \to \mathrm{M}_r(\mathrm{End}^0(Z)),\ f\otimes l \mapsto f\cdot i_0(l)$$

is a C_Z-algebra homomorphism that sends 1 to 1. Since E is a field, this homomorphism is an embedding. It follows that $\mathrm{M}_r(\mathrm{End}^0(Z))$ contains a number field of degree $2\dim(Y)$. Since $\mathrm{M}_r(\mathrm{End}^0(Z)) \cong \mathrm{End}^0(Y)$, the algebra $\mathrm{End}^0(Y)$ contains a number field of degree $2\dim(Y)$, i.e., Y is an abelian variety of CM type over K_a.

Proof of Theorem 5.1. Assertions (i) and (ii) follow from Theorems 4.2 and 4.1.

In order to prove (iii) and (iv) let us put (as in Remark 5.2(i))

$$k_0 = \mathbb{Q},\ k = C_Y,\ \mathcal{A} = \mathrm{End}^0(Y).$$

Then

$$[k:k_0] = [C_Y:\mathbb{Q}] = [C_Z:\mathbb{Q}], d_{\mathcal{A}} = \sqrt{\dim_{C_Y}(\mathrm{End}^0(Y))} = r\cdot d(Z)$$

and according to Remark 5.2(i)

$$[k:k_0]d_{\mathcal{A}} \le 2\mathrm{dim}(Y).$$

Now the desired result follows from Theorem 4.5(v,vi). □

5.3. Let X be an arbitrary positive-dimensional abelian variety over K_a. In this subsection we use the notation of Subsection 2.1.

Let E be a number field and $i: E \hookrightarrow \mathrm{End}^0(X)$ be a $\mathbb{Q}$-algebra embedding that sends 1 to 1_X. Then the E-algebra $\mathrm{End}^0(X,i)$ enjoys the following properties. Let $s \in \mathcal{I}(X)$ and

$$\mathrm{pr}_s : \mathrm{End}^0(X) = \sum_{s\in\mathcal{I}(X)} D_s \twoheadrightarrow D_s$$

be the corresponding projection map. Clearly, $\mathrm{pr}_s i(E) \cong E$. We write $D_{s,E}$ for the centralizer of $\mathrm{pr}_s i(E)$ in D_s. One may easily check that $\mathrm{End}^0(X,i) = \prod_{s\in\mathcal{I}(X)} D_{s,E}$. We write i_s for the composition $\mathrm{pr}_s i : E \hookrightarrow \mathrm{End}^0(X) \twoheadrightarrow D_s = \mathrm{End}^0(X_s)$. Clearly,

$$i_s(1) = e_s = 1_{X_s},\ D_{s,E} = \mathrm{End}^0(X_s, i_s),\ \mathrm{End}^0(X,i) = \oplus_{s\in\mathcal{I}(X)}\mathrm{End}^0(X_s,i_s).$$

In particular, the ratio

$$d_{X_s,E} = \frac{2\mathrm{dim}(X_s)}{[E:\mathbb{Q}]}$$

is a positive integer, i.e., $[E:\mathbb{Q}]$ divides $2\mathrm{dim}(X_s)$.

Theorem 5.4. *Suppose that X is a positive-dimensional abelian variety over K_a.*

Let E be a number field and $i: E \hookrightarrow \mathrm{End}^0(X)$ be a $\mathbb{Q}$-algebra embedding that sends 1 to 1_X. Then the E-algebra $\mathrm{End}^0(X,i)$ enjoys the following properties.

(i) $\mathrm{End}^0(X,i)$ *is a semisimple.*

(ii) $\mathrm{End}^0(X,i)$ *is simple if and only if C_X is a field and $i(E)C_X$ is a field. If this is the case then* $\mathrm{End}^0(X,i)$ *is a central simple algebra over the field $i(E)C_X$.*

(iii)

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

(iv) *the equality*

$$\mathrm{dim}_E(\mathrm{End}^0(X,i)) = \left(\frac{2\mathrm{dim}(X)}{[E:\mathbb{Q}]}\right)^2$$

holds if and only if C_X is a field,

$$\mathrm{dim}_{C_X}(\mathrm{End}^0(X)) = \left(\frac{2\mathrm{dim}(X)}{[C_X:\mathbb{Q}]}\right)^2$$

and E contains C_X.

Proof. We use the notation of Section 5.3. Applying Theorem 5.1(i) to each (X_s, i_s), we obtain that $\mathrm{End}^0(X_s,i_s)$ are semisimple E-algebras. This implies that their direct sum $\mathrm{End}^0(X,i)$ is also semisimple; if it simple then $\mathcal{I}(X)$ is a singleton, i.e. C_X is a field. This proves (i) while (ii) follows readily from Theorem 5.1(ii).

Let us prove (iii) and (iv). If $\mathcal{I}$ is a singleton then the desired result is contained in Theorem 5.1. Now assume that $\mathcal{I}$ is *not* a singleton. Applying Theorem 5.1(iii) to each (X_s, i_s), we obtain that

$$\dim_E(\mathrm{End}^0(X_s, i_s)) \le \frac{(2\dim(X_s))^2}{[E:\mathbb{Q}]^2},$$

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

Since $\mathcal{I}$ is *not* a singleton and all $\dim(X_s)$ are positive,

$$\sum_{s\in\mathcal{I}} \frac{(2\dim(X_s))^2}{[E:\mathbb{Q}]^2} < \frac{(\sum_{s\in\mathcal{I}} 2\dim(X_s))^2}{[E:\mathbb{Q}]^2} = \left(\frac{2\dim(X)}{[E:\mathbb{Q}]}\right)^2.$$

This ends the proof. □

Proof of Theorems 3.2, 3.3 and 3.4. Theorems 5.1 and 5.4 combined with Remark 5.2 imply readily Theorems 3.2, 3.3 and 3.4. □

Proof of Theorem 3.14. Let us choose fields F and $\mathcal{K} \subset F$ as in Remark 3.11. Then

$$k(\lambda) = \mathrm{End}_{\tilde{G}_{\lambda,X,K}}(X_\lambda) = \mathrm{End}_{\tilde{G}_{\lambda,X,\mathcal{K}}}(X_\lambda).$$

It follows from Lemma 3.12 that $\mathrm{End}_{\mathcal{K}}(X, i) = i(\mathcal{O})$ and therefore $\mathrm{End}^0_{\mathcal{K}}(X, i) = i(E)$. By Remark 3.11, $\mathrm{Gal}(F/\mathcal{K})$ acts on $\mathrm{End}(X, i)$ in such a way that

$$\mathrm{End}(X, i)^{\mathrm{Gal}(F/\mathcal{K})} = \mathrm{End}_{\mathcal{K}}(X, i) = i(O).$$

Extending the action of $\mathrm{Gal}(F/\mathcal{K})$ by $\mathbb{Q}$-linearity on $\mathrm{End}(X, i) \otimes \mathbb{Q}$, we get the group homomorphism

$$\mathrm{Gal}(F/\mathcal{K}) \to \mathrm{Aut}_{\mathbb{Q}}(\mathrm{End}(X, i) \otimes \mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(\mathrm{End}^0(X, i))$$

such that the subalgebra of $\mathrm{Gal}(F/\mathcal{K})$-invariants

$$(\mathrm{End}^0(X, i))^{\mathrm{Gal}(F/\mathcal{K})} = (\mathrm{End}(X, i))^{\mathrm{Gal}(F/\mathcal{K})} \otimes \mathbb{Q} = i(\mathcal{O}) \otimes \mathbb{Q} = i(E)$$

is a field. Applying Example 4.11 and Lemma 4.12 to $k_0 = \mathbb{Q}, G = \mathrm{Gal}(F/\mathcal{K})$ and $\mathfrak{A} = \mathrm{End}^0(X)$, we conclude that $\mathrm{Gal}(F/\mathcal{K})$ acts transitively on $\mathcal{I}(X)$. This implies that all the X_s's are Galois-conjugate abelian subvarieties of X. In particular, $\dim(X_s)$ does not depend on s and

$$\dim(X) = |\mathcal{I}(X)| \cdot \dim(X_s).$$

On the other hand, the results of Section 5.3 tell us that $[E:\mathbb{Q}]$ divides $2\dim(X_s)$. This implies that $2\dim(X)$ is divisible by $|\mathcal{I}(X)|[E:\mathbb{Q}]$ and therefore $|\mathcal{I}(X)|$ divides the ratio

$$\frac{2\dim(X)}{[E:\mathbb{Q}]} = d_{X,E}.$$

The transitivity of the action of $\mathrm{Gal}(F/\mathcal{K})$ on $\mathcal{I}(X)$ implies that the stabilizer $\mathrm{Gal}(F/\mathcal{K})_s$ of any s is a subgroup in $\mathrm{Gal}(F/\mathcal{K})$, whose index divides $d_{X,E}$. However, the conditions of Theorem 3.14 imposed on $\tilde{G}_{\lambda,X,K}$ combined with Remark 3.11 imply that such a subgroup must coincide with the whole group $\mathrm{Gal}(F/\mathcal{K})$, i.e., $\mathcal{I}(X)$ is a singleton and $\mathrm{End}^0(X)$ is a simple $\mathbb{Q}$-algebra. In particular, the center C_X is a field.

By Remark 5.2(i) applied to $Y = X$, the product $[C_X : \mathbb{Q}]d_{\mathrm{End}^0(X)}$ divides $2\mathrm{dim}(Y)$. Applying Theorem 4.9(iiibis and iv) to

$$k_0 = \mathbb{Q}, k = C_X, \mathcal{A} = \mathrm{End}^0(X),\ G = \mathrm{Gal}(F/\mathcal{K})$$

$\mathcal{E} = i(E)$ and its centralizer $\mathcal{Z}_{\mathcal{A}}(i(E)) = \mathrm{End}^0(X, i)$, we conclude that $\mathrm{End}^0(X, i)$ is a central simple $i(E)$-algebra provided that the only subgroup of $\mathrm{Gal}(F/\mathcal{K})$, whose index divides $M = [C_X : \mathbb{Q}]d_{\mathrm{End}^0(X)}/[i(E) : \mathbb{Q}]$ is the whole $\mathrm{Gal}(F/\mathcal{K})$. However, M obviously divides $d_{X,E}$ and we have already seen that the only subgroup of $\mathrm{Gal}(F/\mathcal{K})$, whose index divides $d_{X,E}$ is the whole $\mathrm{Gal}(F/\mathcal{K})$. This ends the proof. □

6. Tangent spaces

The aim of this section is to obtain an additional information about endomorphiam algebras of abelian varieties X with multiplications by a number field E, using the action of E on the Lie algebra of X.

Throughout this section K is a field of characteristic 0.

6.1. Let E be a number field and Σ_E be the set of field embeddings $\tau : E \hookrightarrow K_a$. To each $\tau \in \Sigma_K$ corresponds the natural surjective K_a-algebra homomorphism

$$\pi_\tau : E \otimes_{\mathbb{Q}} K_a \twoheadrightarrow E \otimes_{E,\tau} K_a =: K_{a,\tau} = K_a.$$

Taking the direct sum of all π_τ's, we get the canonical isomorphiam of K_a-algebras

$$\Pi : E \otimes_{\mathbb{Q}} K_a \cong \oplus_{\tau\in\Sigma_E} K_{a,\tau}.$$

Remark 6.2. Suppose that $\tau(E) \subset K$ for all $\tau \in \Sigma_K$. (E.g., this condition holds if E is normal over $\mathbb{Q}$ and K contains a subfield isomorphic to E.) Then to each $\tau \in \Sigma_K$ corresponds the natural surjective K-algebra homomorphism

$$\pi_{\tau,K} : E \otimes_{\mathbb{Q}} K \twoheadrightarrow E \otimes_{E,\tau} K =: K_\tau = K.$$

Taking the direct sum of all $\pi_{\tau,K}$'s, we get the canonical isomorphism of K-algebras

$$\Pi_K : E \otimes_{\mathbb{Q}} K \cong \oplus_{\tau\in\Sigma_E} K_\tau.$$

If $\mathcal{M}$ is any $E \otimes_{\mathbb{Q}} K_a$-module then we write for each $\tau \in \Sigma_K$

$$M_\tau = \{x \in \mathcal{M} \mid u(x) = \tau(u)x\ \forall u \in E = E \otimes 1 \subset E \otimes_{\mathbb{Q}} K_a\}.$$

Clearly, $M_\tau = K_{a,\tau}\mathcal{M}$ is an $E \otimes_{\mathbb{Q}} K_a$-submodule of $\mathcal{M}$ and

$$\mathcal{M} = \oplus_{\tau\in\Sigma_K} M_\tau.$$

In particular, if $\mathcal{M}$ viewed as a vector space over $K_a = 1 \otimes K_a$ has finite dimension then

$$\dim_{K_a}(\mathcal{M}) = \sum_{\tau\in\Sigma_K} \dim_{K_a}(M_\tau).$$

6.3. Let V_K be a smooth absolutely irreducible quasiprojective variety over K and $V = V \times_K K_a$ the correspomding variety over the algebraic closure K_a of K. The Galois group $\mathrm{Gal}(K)$ acts naturally on $V_K(K_a) = V(K_a)$; the set of fixed points of this action coincides with $V_K(K)$. Further we identify $V_K(K_a)$ with its bijective image in $V(K_a)$.

Let P be a K-point of V_K, which we also view as K_a-point of V. We write $\mathbf{t}_P(V)$ for the tangent K_a-vector space to V at P and $\mathbf{t}_P(V_K)$ for the tangent K-vector space to V_K at P. The natural K_a-linear map [6, Remark 6.3(iii) on p. 147]

$$\mathbf{t}_P(V) \to \mathbf{t}_P(V_K) \otimes_K K_a$$

is an isomorphism of K_a-vector spaces [6, Remark 6.12(iii) on p. 152]. The Galois group $\mathrm{Gal}(K)$ acts by semi-linear automorphisms on $\mathbf{t}_P(V)$ and the corresponding K-vector subspace of $\mathrm{Gal}(K)$-invariants

$$\mathbf{t}_P(V)^{\mathrm{Gal}(K)} = \mathbf{t}_P(V_K) \otimes 1 = \mathbf{t}_P(V_K).$$

Let Z be a smooth closed K_a-subvariety of V such that $P \in Z(K_a)$. Then the induced map of the K_a-vector tangent spaces $\mathbf{t}_P(Z) \to \mathbf{t}_P(V)$ is an embedding and we identify $\mathbf{t}_P(Z)$ with its image in $\mathbf{t}_P(V)$. For each $\sigma \in \mathrm{Gal}(K)$ the K_a-vector subspace

$$\sigma(\mathbf{t}_P(Z)) \subset \mathbf{t}_P(V)$$

coincides with the tangent space to the closed smooth subvariety $\sigma Z \subset V$ at $P \in (\sigma Z)(K_a) = \sigma(Z(K_a))$. (This assertion follows readily from the classical explicit description of the tangent space [6, Example 6.5 on p. 148].)

6.4. Let X be a positive-dimensional abelian variety over K_a that is defined over K. This means that there exists an abelian scheme X_K over K such that $X = X_K \times_K K_a$. Let

$$\mathbf{o} \in X_K(K) \subset X_K(K_a) = X(K_a)$$

be the zero of the group law on X_K. Let us put

$$\mathrm{Lie}(X) = \mathbf{t}_{\mathbf{o}}(X),\ \mathrm{Lie}_K(X) = \mathbf{t}_{\mathbf{o}}(X_K).$$

By definition, $\mathrm{Lie}(X)$ (resp. $\mathrm{Lie}_K(X)$) is a $\dim(X)$-dimensional vector space over K_a (resp. over K) and there is the natural identification of K_a-vector spaces

$$\mathrm{Lie}(X) = \mathrm{Lie}_K(X) \otimes_K K_a.$$

If $Z \subset K_a$ is an abelian K_a-subvariety of X then $Z(K_a)$ contains $\mathbf{o}$ and we consider the K_a-vector subspace.

$$\mathrm{Lie}(Z) := \mathbf{t}_{\mathbf{o}}(Z) \subset \mathbf{t}_{\mathbf{o}}(X) = \mathrm{Lie}(X).$$

For each $\sigma \in \mathrm{Gal}(K)$ we have the abelian K_a-subvariety σZ and

$$\mathrm{Lie}(\sigma Z) = \sigma(\mathrm{Lie}(Z)) \subset \mathrm{Lie}_K(X) \otimes_K K_a = \mathrm{Lie}(X).$$

By functoriality, $\mathrm{Lie}(X)$ (resp. $\mathrm{Lie}_K(X)$) carries the natural structure of $\mathrm{End}(X) \otimes K_a = \mathrm{End}^0(X) \otimes_{\mathbb{Q}} K_a$-module (resp. of $\mathrm{End}_K(X_K) \otimes K = \mathrm{End}^0_K(X_K) \otimes_{\mathbb{Q}} K$-module.)

Let

$$i : E \hookrightarrow \mathrm{End}^0(X)$$

be a $\mathbb{Q}$-algebra embedding that sends 1 to 1_X.

In particular, $\mathrm{Lie}(X)$ becomes the $E \otimes_{\mathbb{Q}} K_a$-module. Let us consider the K_a-vector subspace

$$\mathrm{Lie}(X)_\tau = \{z \in \mathrm{Lie}(X) \mid i(e)z = \tau(e)z\ \forall e \in E\} \subset \mathrm{Lie}(X),\ n_\tau(X, i) = \dim_{K_a}(\mathrm{Lie}(X)_\tau).$$

Clearly,

$$\mathrm{Lie}(X) = \oplus_{\tau \in \Sigma_E} \mathrm{Lie}(X)_\tau,\ \dim(X) = \dim_{K_a}(\mathrm{Lie}(X)) = \sum_{\tau \in \Sigma_E} n_\tau(X, i).$$

We write $n_{X,i}$ for the greatest common divisor of all $n_\tau(X,i)$. Clearly, $n_{X,i}$ is a positive integer dividing $\dim(X)$. The subspace $\mathrm{Lie}(X)_\tau$ is $\mathrm{End}^0(X,i)$-invariant and carries the natural structure of $\mathrm{End}^0(X,i)\otimes_{\mathbb{Q}} K_a$-module.

From now on we assume that

$$i(E)\subset \mathrm{End}^0_K(X_K).$$

Theorem 6.5. *Suppose that* $\mathrm{char}(K)=0$. *If* $\mathrm{End}^0_K(X,i)$ *is a number field and* $n_{X,i}=1$ *then* $\mathrm{End}^0(X,i)$ *is a semisimple commutative E-algebra and all its simple components are mutually isomorphic number fields.*

Proof. Let us put

$$k_0=\mathbb{Q}, \mathfrak{A}=\mathrm{End}^0(X), G=\mathrm{Gal}(K), \Sigma=\Sigma_K, \mathcal{M}_\tau=\mathrm{Lie}(X)_\tau.$$

Applying Lemma 4.12 and Corollary 4.13 to $\mathcal{E}=i(E)$, and

$$\mathcal{Z}_{\mathfrak{A}}(\mathcal{E})=\mathrm{End}^0(X,i), \quad \mathcal{Z}_{\mathfrak{A}}(\mathcal{E})^G=\mathrm{End}^0_K(X,i),$$

we obtain the desired result. □

Corollary 6.6. *Suppose that*

$$\mathrm{char}(K)=0,\ i(\mathcal{O})\subset \mathrm{End}_K(X),\ n_{X,i}=1.$$

Let us assume that there exists a maximal ideal λ of $\mathcal{O}$ such that

$$\mathrm{End}_{\tilde{G}_{\lambda,X,K}}(X_\lambda)=k(\lambda)$$

then $\mathrm{End}^0(X,i)$ *is a semisimple commutative E-algebra and all its simple components are mutually isomorphic number fields.*

Proof. By Corollary 3.13, the condition on the centralizer implies that $\mathrm{End}^0_K(X,i)=i(E)\cong E$ is a number field. Now the result follows from Theorem 6.5. □

6.7. We continue our study of certain subspaces of $\mathrm{Lie}(X)$. If $\tau\in\Sigma_E$ and $\sigma\in\mathrm{Gal}(K)$ then their composition

$$\sigma\tau: E\hookrightarrow K_a$$

also lies in Σ_E and

$$\sigma(\mathrm{Lie}(X)_\tau)=\mathrm{Lie}(X)_{\sigma\tau}\subset\mathrm{Lie}(X).$$

In particular,

$$n_\tau(X,i)=\dim_{K_a}(\mathrm{Lie}(X)_\tau)=\dim_{K_a}(\mathrm{Lie}(X)_{\sigma\tau})=n_{\sigma\tau}(X,i),$$

i.e.,

$$n_\tau(X,i)=n_{\sigma\tau}(X,i)\ \forall\tau\in\Sigma_E,\sigma\in\mathrm{Gal}(K).$$

In addition, suppose that $Z\subset X$ is an abelian K_a-subvariety of X such $\mathrm{Lie}(Z)$ is E-invariant (i.e., is a $E\otimes_{\mathbb{Q}}K_a$-submodule of $\mathrm{Lie}(X)$). Then $\mathrm{Lie}(\sigma Z)$ is also E-invariant and

$$\sigma(\mathrm{Lie}(Z)_\tau)=\mathrm{Lie}(\sigma Z)_{\sigma\tau}.$$

In particular, if $\tau(E)\subset K$ then $\sigma\tau=\tau$ and therefore

$$\sigma(\mathrm{Lie}(Z)_\tau)=\mathrm{Lie}(\sigma Z)_\tau$$

and

$$\dim_{K_a}(\mathrm{Lie}(\sigma Z)_\tau)=\dim_{K_a}(\mathrm{Lie}(Z)_\tau).$$

Now we use the notation of Subsections 2.1 and 5.3. Recall that $X_s \subset X$ is a positive dimensional abelian K_a-subvariety of X for all $s \in \mathcal{I}(X)$. Since $\mathrm{char}(K) = 0$, the isogeny Π_X (see Lemma 2.2) induces an isomorphism of K_a-vector spaces

$$\mathrm{Lie}(X) = \oplus_{s\in\mathcal{I}(X)}\mathrm{Lie}(X_s)$$

while each subspace $\mathrm{Lie}(X_s) \subset \mathrm{Lie}(X)$ is E-invariant and $\mathrm{End}^0(X,i)$-invariant in light of results of Subsection 5.3. In addition, the action of E on $\mathrm{Lie}(X_s) \subset \mathrm{Lie}(X)$ induced by i coincides with the action of E induced by $i_s : E \hookrightarrow \mathrm{End}^0(X_s)$. This implies that

$$\dim_{K_a}(\mathrm{Lie}(X_s)_\tau) = n_\tau(X_s, i_s)\ \forall s \in \mathcal{I}(X), \tau \in \Sigma_E.$$

It is also clear that

$$\sigma(\mathrm{Lie}(X_s)) = \mathrm{Lie}(\sigma(X_s)) = \mathrm{Lie}(X_{\sigma(s)})\ \forall \sigma \in \mathrm{Gal}(K), s \in \mathcal{I}(X).$$

So, if

$$\tau(E) \subset K\ \forall \tau \in \Sigma_E \tag{6}$$

and the action of $\mathrm{Gal}(K)$ on $\mathcal{I}(X)$ is transitive then $\dim_{K_a}(\mathrm{Lie}(X_s)_\tau)$ does *not* depend on a choice of s and

$$n_\tau(X,i) = \dim_{K_a}(\mathrm{Lie}(X)_\tau) = |\mathcal{I}(X)|\dim_{K_a}(\mathrm{Lie}(X_s)_\tau.$$

This implies that if (6) holds and the Galois action on $\mathcal{I}(X)$ is transitive then $n_\tau(X,i)$ is divisible by $|\mathcal{I}(X)|$ for all $\tau \in \Sigma_E$. It follows that $n_{X,i}$ is divisible by $|\mathcal{I}(X)|$.

Lemma 6.8. *Suppose that* $\mathrm{char}(K) = 0$ *and* $\tau(E) \subset K$ *for all* $\tau \in \Sigma_E$. *If* $\mathrm{End}^0_K(X,i)$ *is a number field and* $n_{X,i} = 1$ *then* $\mathcal{I}(X)$ *is a singleton, i.e.,* $X = X_s$, C_X *is a number field and* $\mathrm{End}^0(X)$ *is simple* $\mathbb{Q}$*-algebra, which is a central simple algebra over* C_X.

Proof. If $\mathrm{End}^0_K(X,i)$ is a number field then $\mathrm{Gal}(K)$ acts on $\mathcal{I}(X)$ transitively. By results of Subsection 6.7, $n_{X,i}$ is divisible by $|\mathcal{I}(X)|$. Since $n_{X,i} = 1$, $\mathcal{I}(X)$ is a singleton, i.e., $X = X_s$ and $\mathrm{End}^0(X) = \mathrm{End}^0(X_s)$ is a simple $\mathbb{Q}$-algebra. □

Remark 6.9. Lemma 6.8 is a generalization of ([44, Th. 3.12(i)], [45, Th. 3.12(i)]).

Theorem 6.10. *Suppose that*

$$\mathrm{char}(K) = 0,\ \mathrm{End}^0_K(X,i) = i(E),\ n_{X,i} = 1,\ \tau(E) \subset K\ \forall\ \tau \in \Sigma_E.$$

Then $\mathrm{End}^0(X,i)$ *is a number field containing* E *and the degree* $[\mathrm{End}^0(X,i) : i(E)]$ *divides* $d_{X,E}$.

Proof. Let us put $k_0 = \mathbb{Q}$. By Lemma 6.8, $\mathcal{A} := \mathrm{End}^0(X)$ is a central simple algebra over the number field $k := C_X$. Let us apply Theorem 4.9 to $G = \mathrm{Gal}(K)$, the field $\mathcal{E} = i(E)$ and

$$\mathcal{Z}_{\mathcal{A}}(E) = \mathrm{End}^0(X,i),\ \mathcal{Z}_{\mathcal{A}}(E)^G = \mathrm{End}^0_K(X,i) = i(E).$$

By Theorem 6.5, $\mathrm{End}^0(X,i)$ (in the notation of Theorem 4.9) is a direct sum of fields

$$\mathrm{End}^0(X,i) = \oplus_{j\in J}F_j$$

where all F_j's are mutually isomorphic number fields. By Theorem 4.9(iii, iiibis), there is a *transitive* action

$$\rho_J : \mathrm{Gal}(K) \to \mathrm{Perm}(J)$$

of $\mathrm{Gal}(K)$ on J such that if $\rho_J(\sigma)j = j'$ then $\sigma(F_j) = F_{j'}$. Let $e_j \in F_j \in \mathrm{End}^0(X, i)$ be the identity element of F_j. Clearly,

$$\sum_{j\in J} e_j = 1 \in \mathrm{End}^0(X),\ e_j^2 = e_j^2,\ e_j e_{j'} = 0\ \forall j \neq j'.$$

This implies that the set $\{e_j \mid j \in J\}$ is $\mathrm{Gal}(K)$-invariant and the action of $\mathrm{Gal}(K)$ on this set is transitive. Let us put

$$\mathrm{Lie}(X)^{(j)} = e_j \mathrm{Lie}(X) \subset \mathrm{Lie}(X).$$

Clearly, each $\mathrm{Lie}(X)^{(j)}$ is a $E \otimes_{\mathbb{Q}} K_a$-sumbodule of $\mathrm{Lie}(X)$ and

$$\mathrm{Lie}(X) = \oplus_{j\in J} \mathrm{Lie}(X)^{(j)}.$$

In addition, $\mathrm{Gal}(K)$ acts transitively on the set $\{\mathrm{Lie}(X)^{(j)} \mid j \in J\}$. Since $\tau(E) \subset K$ for each $\tau \in \Sigma_E$, $\dim_{K_a}(\mathrm{Lie}(X)^{(j)}_{\tau})$ does *not* depend on a choice of $j \in J$. This implies that

$$n_\tau(X, i) = \dim_{K_a}(\mathrm{Lie}(X)_\tau) = |J| \dim_{K_a}(\mathrm{Lie}(X)^{(j)}_{\tau});$$

in particular, all $n_\tau(X, i)$ are divisible by $|J|$. This implies that $n_{X,i}$ is divisible by $|J|$. Since $n_{X,i} = 1$, J is a singleton, i.e., $\mathrm{End}^0(X, i) = F_j$ is a (number) field.

It remains to prove that $[F_j : E]$ divides $d_{X,E}$. Indeed, since F_j is a subfield of $\mathrm{End}^0(X)$, its degree $[F_j : \mathbb{Q}]$ divides $2\dim(X)$ and therefore

$$[F_j : E] = \frac{[F_j : \mathbb{Q}]}{[E : \mathbb{Q}]}$$

divides

$$\frac{2\dim(X)}{[E : \mathbb{Q}]} = d_{X,E}.$$

□

Theorem 6.11. *Suppose that*

$$\mathrm{char}(K) = 0,\ i(\mathcal{O}) \subset \mathrm{End}_K(X),\ n_{X,i} = 1,\ \tau(E) \subset K\ \forall\ \tau \in \Sigma_E.$$

Let us assume that there exists a maximal ideal λ of $\mathcal{O}$ such that

$$\mathrm{End}_{\tilde{G}_{\lambda,X,K}}(X_\lambda) = k(\lambda)$$

and $\tilde{G}_{\lambda,X,K}$ does not contain a proper normal subgroup with index dividing $d_{X,E}$.

Then $\mathrm{End}^0(X, i) = i(E) \cong E$.

Proof. By Corollary 3.13, the condition on the centralizer implies that

$$\left[\mathrm{End}^0(X, i)\right]^{\mathrm{Gal}(K)} = \mathrm{End}^0_K(X, i) = i(E).$$

Applying Theorem 6.10, we conclude that $\mathrm{End}^0(X, i)$ is a field containing E and $\left[\mathrm{End}^0(X, i) : E\right]$ divides $d_{X,E}$. By Remark 3.11, there exist a finite Galois extension F/K and an overfield $\mathcal{K}$ of K that is a subfield of F that enjoys the following properties.

(i)
$$\mathrm{End}_{\tilde{G}_{\lambda,X,\mathcal{K}}}(X_\lambda)=\mathrm{End}_{\tilde{G}_{\lambda,X,K}}(X_\lambda)=k(\lambda)$$
and
$$\tilde{G}_{\lambda,X,\mathcal{K}}=\tilde{G}_{\lambda,X,K}\subset \mathrm{Aut}_{k(\lambda)}(X_\lambda).$$
This implies that $\mathrm{End}^0_{\mathcal{K}}(X,i)=i(E)$.

(ii) There is a surjective group homomorphism
$$\mathrm{Gal}(F/\mathcal{K})\twoheadrightarrow \tilde{G}_{\lambda,X,\mathcal{K}}=\tilde{G}_{\lambda,X,K},$$
which is a *minimal cover*. In particular, $\mathrm{Gal}(F/\mathcal{K})$ also does *not* contain a proper normal subgroup with index dividing $d_{X,E}$.

(iii) The homomorphism
$$\kappa_{X,\mathcal{K}}:\mathrm{Gal}(\mathcal{K})\to \mathrm{Aut}(\mathrm{End}^0(X))=\mathrm{Aut}_{\mathbb{Q}}(\mathrm{End}^0(X))$$
factors through
$$\mathrm{Gal}(\mathcal{K})\twoheadrightarrow \mathrm{Gal}(F/\mathcal{K}).$$
Since $\mathrm{End}^0(X,i)$ is a $\mathrm{Gal}(K)$-stable subalgebra of $\mathrm{End}^0(X)$, there is a group homomorphism
$$\kappa:\mathrm{Gal}(F/\mathcal{K})\to \mathrm{Aut}_{\mathbb{Q}}(\mathrm{End}^0(X,i)),$$
such that the subalgebra $\left[\mathrm{End}^0(X,i)\right]^{\mathrm{Gal}(F/\mathcal{K})}$ of $\mathrm{Gal}(F/\mathcal{K})$-invariants coincides with
$$\left[\mathrm{End}^0(X,i)\right]^{\mathrm{Gal}(\mathcal{K})}=\mathrm{End}^0_{\mathcal{K}}(X,i)=i(E).$$

Let Γ be the image of
$$\kappa:\mathrm{Gal}(F/\mathcal{K})\to \mathrm{Aut}\left(\mathrm{End}^0(X,i)/i(E)\right).$$
Clearly,
$$\left[\mathrm{End}^0(X,i)\right]^{\Gamma}=i(E)$$
and Galois theory tells us that $|\Gamma|=\left[\mathrm{End}^0(X,i):i(E)\right]$. This implies that $\ker(\kappa)$ is a subgroup of index $\left[\mathrm{End}^0(X,i):i(E)\right]$ in $\mathrm{Gal}(F/\mathcal{K})$. This implies that the index of $\ker(\kappa)$ in $\mathrm{Gal}(F/\mathcal{K})$ divides $d_{X,E}$ and therefore $\mathrm{Gal}(F/\mathcal{K})=\ker(\kappa)$, i.e., Γ is the trivial group of order 1 and
$$i(E)=\left[\mathrm{End}^0(X,i)\right]^{\Gamma}=\mathrm{End}^0(X,i).$$
□

Remark 6.12. Theorem 6.11 is a generalization of ([44, Th. 3.12(ii)] [3] , [45, Th. 3.12(ii)]).

[3] The assertion (ii)(a) of [44, Th. 3.12(ii)] is wrong without additional assumptions.

7. Doubly Transitive Permutation Groups and Permutational Modules

In order to apply our results to endomorphism algebras of superelliptic jacobians, we need to discuss modular representations that correspond to permutation groups.

Let T be a finite nonempty set, $n=|T|$ and $\mathrm{Perm}(T)\cong \mathbf{S}_n$ the group of permutations of T. We write $\mathrm{Alt}(T)\cong \mathbf{A}_n$ for the only (normal) subgroup of index 2 in $\mathrm{Perm}(T)$.

Let ℓ be a prime. One may attach to T the following natural linear representations of $\mathrm{Perm}(T)$ over $\mathbb{F}_\ell$. In what follows we assume that

$$n\ge 3.$$

First, let us consider the space $\mathbb{F}_\ell^T$ of all functions $\phi: T\to \mathbb{F}_\ell$. The action of $\mathrm{Perm}(T)$ on T gives rise to the faithful n-dimensional linear representation

$$\mathrm{Perm}(T)\to \mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_\ell^T).$$

More precisely, each $g\in \mathrm{Perm}(T)$ sends a function $\phi: T\to \mathbb{F}_\ell$ to the function

$$[g]\phi: t\mapsto \phi(g^{-1}t)\ \forall t\in T.$$

The representation space $\mathbb{F}_\ell^T$ contains the invariant line $\mathbb{F}_\ell\cdot 1_T$ of constant functions (where 1_T is the constant function 1) and the invariant $(n-1)$-dimensional hyperplane of functions with zero "integral"

$$(\mathbb{F}_\ell^T)^0=\{\phi: T\to\mathbb{F}_\ell\mid \sum_{t\in T}\phi(t)=0\}\subset \mathbb{F}_\ell^T.$$

Clearly,

$$\mathbb{F}_\ell\cdot 1_T=(\mathbb{F}_\ell^T)^{\mathrm{Perm}(T)},$$

i.e., $\mathbb{F}_\ell\cdot 1_T$ is the subspace of $\mathrm{Perm}(T)$-invariants in $\mathbb{F}_\ell^T$.

If ℓ does not divide n then

$$\mathbb{F}_\ell^T=\mathbb{F}_\ell\cdot 1_T\oplus(\mathbb{F}_\ell^T)^0.$$

This implies that if ℓ does *not* divide n then $(\mathbb{F}_\ell^T)^0$ is a *faithful* $\mathrm{Perm}(T)$-module.

If ℓ divides n then $\mathbb{F}_\ell\cdot 1_T\subset(\mathbb{F}_\ell^T)^0$ and we may get the *heart* of the permutational representation [13]

$$(\mathbb{F}_\ell^T)^{00}=(\mathbb{F}_\ell^T)^0/(\mathbb{F}_\ell\cdot 1_T),$$

which also carries the natural structure of $(n-2)$-dimensional representation space

$$\mathrm{Perm}(T)\to \mathrm{Aut}_{\mathbb{F}_\ell}((\mathbb{F}_\ell^T)^{00}).$$

We may also consider the quotient

$$(\mathbb{F}_\ell^T)_0=\mathbb{F}_\ell^T/(\mathbb{F}_\ell\cdot 1_T),$$

which is also provided with the natural structure of $(n-1)$-dimensional representation space

$$\mathrm{Perm}(T)\to \mathrm{Aut}_{\mathbb{F}_\ell}((\mathbb{F}_\ell^T)_0)$$

[25]. If ℓ does not divide n then the $\mathrm{Perm}(T)$-modules $(\mathbb{F}_\ell^T)^0$ and $(\mathbb{F}_\ell^T)_0$ are canonically isomorphic. If ℓ divides n then

$$(\mathbb{F}_\ell^T)_0=\mathbb{F}_\ell^T/(F_\ell\cdot 1_T)\supset(\mathbb{F}_\ell^T)^0/(F_\ell\cdot 1_T)=(\mathbb{F}_\ell^T)^{00},$$

i.e., $(\mathbb{F}_\ell^T)_0$ contains a $\mathrm{Perm}(T)$-invariant hyperplane that is isomorphic as $\mathrm{Perm}(T)$-module to $(\mathbb{F}_\ell^T)^{00}$.

Lemma 7.1. *Suppose that*

$$n \ge 4,\ \ell > 2,\ \ell \mid n.$$

Then both $\mathrm{Perm}(T)$*-modules* $(\mathbb{F}_\ell^T)^{00}$ *and* $(\mathbb{F}_\ell^T)_0$ *are faithful.*

Proof. Since $(\mathbb{F}_\ell^T)^{00}$ is isomorphic to a submodule of $(\mathbb{F}_\ell^T)_0$, it suffices to check the faithfulness of $Perm(T)$-module $(\mathbb{F}_\ell^T)^{00}$. Let g be a non-identity permutation of T. The there is $t \in T$ such that $s = g(t) \ne t$. Let $u := g^{-1}(t)$. Clearly, $u \ne t$. No matter whether u coincides with s or not, there exists $\phi \in (\mathbb{F}_\ell^T)^0$ such that $\phi(s) = \phi(u) = 1, \phi(t) = 0$. (Here we use that $|T| = n > 3$.) Then

$$[g]\phi(s) = \phi(t) = 0,\ [g]\phi(t) = \phi(u) = 1.$$

This implies that the function $[g]\phi - \phi$ takes values -1 at s and 1 at t. In particular, it is *not* a constant function. This implies that the image of ϕ in $(\mathbb{F}_\ell^T)^0/\mathbb{F}_\ell \cdot 1_T) = (\mathbb{F}_\ell^T)^{00}$ is *not* g-invariant. This implies that the action of $\mathrm{Perm}(T)$ on $(\mathbb{F}_\ell^T)^{00}$ is faithful. □

Lemma 7.2. *Suppose that*

$$n \ge 5,\ \ell = 2,\ 2 \mid n.$$

Then both $\mathrm{Perm}(T)$*-modules* $(\mathbb{F}_2^T)^{00}$ *and* $(\mathbb{F}_2^T)_0$ *are faithful.*

Proof. Since $(\mathbb{F}_2^T)^{00}$ is isomorphic to a submodule of $(\mathbb{F}_2^T)_0$, it suffices to check the faithfulness of $\mathrm{Perm}(T)$-module $(\mathbb{F}_2^T)^{00}$. Since $\mathrm{Alt}(T)$ is a subgroup of $\mathrm{Perm}(T)$, $(\mathbb{F}_2^T)^{00}$ carries the natural structure of the $\mathrm{Alt}(T)$ -module and it is known [13] that this module is simple. Since $\dim_{\mathbb{F}_2}((\mathbb{F}_2^T)^{00}) = n - 2 \ge 5 - 2 > 1$, the corresponding homomorphism $\mathrm{Alt}(T) \to \mathrm{Aut}_{\mathbb{F}_2}((\mathbb{F}_2^T)^{00})$ is nontrivial. Since $\mathrm{Alt}(T) \cong \mathbf{A}_n$ is simple (recall that $n \ge 5$), this homomorphism must be injective. Since $\mathbf{A}_n$ is the only normal subgroup of $\mathbf{S}_n \cong \mathrm{Perm}(T)$ (except the trivial one and $\mathbf{S}_n$ itself), we conclude that the group homomorphism $\mathrm{Perm}(T) \to \mathrm{Aut}_{\mathbb{F}_2}((\mathbb{F}_2^T)^{00})$ is injective, i.e., $(\mathbb{F}_2^T)^{00}$ is a faithful $\mathrm{Perm}(T)$-module. □

Remark 7.3. The only missing cases not covered by Lemmas 7.1 and 7.2 correspond to $n = \ell = 3$ and $n = 4, \ell = 2$. In both cases the $\mathrm{Perm}(T)$-module $(\mathbb{F}_2^T)^{00}$ is *not* faithful.

Let $\mathcal{G} \subset \mathrm{Perm}(T)$ be a permutation (sub)group. We may view $\mathbb{F}_\ell^T, (\mathbb{F}_\ell^T)^0, (\mathbb{F}_\ell^T)^{00}, (\mathbb{F}_\ell^T)_0$ as $\mathbb{F}_\ell$-linear representations of $\mathcal{G}$. One may easily check that the $\mathbb{F}_\ell$-dimension of the subspace $(\mathbb{F}_\ell^T)^{\mathcal{G}}$ of $\mathcal{G}$-invariants equals the number of $\mathcal{G}$-orbits in T. In particular, $(\mathbb{F}_\ell^T)^{\mathcal{G}} = F_\ell \cdot 1_T$ if and only if G is transitive.

The following statement is contained in [9, Satz 4 and Satz 11]. (In the notation of [9],

$$p = \ell, K = \mathbb{F}_\ell, \Omega = T, M^1 = (\mathbb{F}_\ell^T)_0, M = (\mathbb{F}_\ell^T)^{00}.\ )$$

Lemma 7.4. (i) *Suppose that ℓ does not divide n and $\mathcal{G}$ acts transitively on T. Then* $\mathrm{End}_{\mathcal{G}}((\mathbb{F}_\ell^T)^0) = \mathbb{F}_\ell$ *if and only if $\mathcal{G}$ is doubly transitive.*

(ii) *Suppose that ℓ divides n. If $\mathcal{G}$ is 3-transitive then*

$$\mathrm{End}_{\mathcal{G}}((\mathbb{F}_\ell^T)^{00}) = \mathbb{F}_\ell.$$

(iii) *Suppose that $n \ge 4$, $\mathcal{G}$ acts transitively on T and ℓ divides n. Suppose that* $\mathrm{End}_{\mathcal{G}}((\mathbb{F}_\ell^T)^{00})$ *is a field. Then either $\ell = 2$ and n is congruent to* 2 *modulo* 4 *or $\mathcal{G}$ is doubly transitive.*

Actually, one may remove the transitivity condition in Lemma 7.4(a).

Corollary 7.5. *Suppose that ℓ does not divide n. Then $\mathrm{End}_{\mathcal{G}}((\mathbb{F}_\ell^T)^0)=\mathbb{F}_\ell$ if and only if $\mathcal{G}$ is doubly transitive.*

Proof. Recall that $n \ge 3$. In light of Lemma 7.4(a), we need to check only the transitivity of $\mathcal{G}$ if $\mathrm{End}_{\mathcal{G}}((\mathbb{F}_\ell^T)^0)=\mathbb{F}_\ell$.

Suppose that $\mathcal{G}$ is *not* transitive, i.e., one may split T into a disjoint union $T=T_1 \cup T_2$ of two nonempty $\mathcal{G}$-stable subsets T_1 and T_2. If we put $n_i=|T_i|$ then $n_1+n_2=n$ and both $n_i \ge 1$. Since ℓ does *not* divide n, it does not divide, at least, one of n_i. We may assume that ℓ does *not* divide n_1. Let us consider $u \in \mathrm{End}_{\mathcal{G}}((\mathbb{F}_\ell^T)^0)$ that is defined as follows. For each $\phi \in (\mathbb{F}_\ell^T)^0$ the function $u(\phi)$ takes the value $n_1\left(\sum_{t\in T_2}\phi(t)\right)$ at every point of T_2 and takes the value $-n_2\left(\sum_{t\in T_2}\phi(t)\right)$ at every point of T_1. Clearly, the image of u is the one-dimension subspace of $(\mathbb{F}_\ell^T)^0$ that is generated by the function

$$\psi: T \to \mathbb{F}_\ell,\ \psi(t_2)=n_1\ \forall t_2 \in T_2,\ \psi(t_1)=-n_2\ \forall t_1 \in T_1.$$

Since $\dim_{\mathbb{F}_\ell}((\mathbb{F}_\ell^T)^0)>1$, u is *not* a scalar and we get a desired contradiction. □

The following assertion is a special case of [13, Lemma 2 on p. 3].

Lemma 7.6. *Suppose that $\ell \mid n$, $\mathcal{G}$ is transitive and the $\mathcal{G}$-module $(\mathbb{F}_\ell^T)^{00}$ is simple. Then the list of $\mathcal{G}$ -invariant subspaces of $\mathbb{F}_\ell^T$ consists of $\{0\}, \mathbb{F}_\ell^T, \mathbb{F}_\ell\cdot 1_T, (\mathbb{F}_\ell^T)^0$.*

This lemma implies readily the following corollary.

Corollary 7.7. *Suppose that $\ell \mid n$, $\mathcal{G}$ is transitive and the $\mathcal{G}$-module $(\mathbb{F}_\ell^T)^{00}$ is simple. Then the list of $\mathcal{G}$ -invariant subspaces of $(\mathbb{F}_\ell^T)_0$ consists of $\{0\}, (\mathbb{F}_\ell^T)^{00}, \mathbb{F}_\ell^T)_0$.*

Theorem 7.8. *Suppose that $\ell \mid n$, $\mathcal{G}$ is transitive and the $\mathcal{G}$-module $(\mathbb{F}_\ell^T)^{00}$ is absolutely simple. Then*

$$\mathrm{End}_{\mathcal{G}}\left(\left(\mathbb{F}_\ell^T\right)_0\right)=\mathbb{F}_\ell.$$

Proof. The absolute simplicity of $(\mathbb{F}_\ell^T)^{00}$ implies that

$$\mathrm{End}_{\mathcal{G}}((\mathbb{F}_\ell^T)^{00})=\mathbb{F}_\ell.$$

Let

$$u \in \mathrm{End}_{\mathcal{G}}((\mathbb{F}_\ell^T)_0).$$

We need to prove that $u \in \mathbb{F}_\ell$, i.e., u is a scalar. Then $u((\mathbb{F}_\ell^T)^{00}) \subset (\mathbb{F}_\ell^T)_0$ is a $\mathcal{G}$-invariant subspace of $(\mathbb{F}_\ell^T)_0$ of dimension $\le n-2$. It follows from Corollary 7.7 that $u((\mathbb{F}_\ell^T)^{00}) \subset (\mathbb{F}_\ell^T)^{00}$. Since $\mathrm{End}_{\mathcal{G}}((\mathbb{F}_\ell^T)^{00})=\mathbb{F}_\ell$, there is $a \in \mathbb{F}_\ell$ such that the restriction of u to $(\mathbb{F}_\ell^T)^{00}$ coincides with multiplication by a, i.e., $(u-a)((\mathbb{F}_\ell^T)^{00})=\{0\}$. Since $(\mathbb{F}_\ell^T)^{00}$ has codimension 1 in $(\mathbb{F}_\ell^T)_0$, the image $W:=(u-a)((\mathbb{F}_\ell^T)_0)$ has dimension ≤ 1. Since W is obviously $\mathcal{G}$-stable, it follows from from Corollary 7.7 that $W=\{0\}$, i.e., $u-a=0$, which in turn means that $u=a$, i.e., is a scalar. This ends the proof. □

Example 7.9. Suppose that $\ell \mid n$ and $n \ge 5$. If $\mathcal{G}=\mathrm{Perm}(T)$ or $\mathrm{Alt}(T)$ then $\mathcal{G}$ is transitive and the $\mathcal{G}$-module $(\mathbb{F}_\ell^T)^{00}$ is absolutely simple [13]. By Theorem 7.8,

$$\mathrm{End}_{\mathcal{G}}\left(\left(\mathbb{F}_\ell^T\right)_0\right)=\mathbb{F}_\ell.$$

This assertion is actually contained in Lemma 3.7 of [25, p. 339].

8. Superelliptic jacobians

The aim of this section is to apply results of Section 6 to endomorphism algebras of superelliptic jacobians, using group-theoretic constructions of Section 7.

Let p be a prime, r a positive integer, $q = p^r$ and $\zeta_q \in \mathbb{C}$ be a primitive qth root of unity, $E := \mathbb{Q}(\zeta_q) \subset \mathbb{C}$ the qth cyclotomic field and $\mathcal{O} := \mathbb{Z}[\zeta_q]$ the ring of integers in $\mathbb{Q}(\zeta_q) = E$.

Let us assume that $\mathrm{char}(K) \ne p$ and K contains a primitive qth root of unity ζ. Let $f(x) \in K[x]$ be a polynomial of degree $n \ge 3$ without multiple roots, $\mathfrak{R}_f \subset K_a$ the (n-element) set of roots of f and $K(\mathfrak{R}_f) \subset K_a$ the splitting field of f. We write $\mathrm{Gal}(f) = \mathrm{Gal}(f/K)$ for the Galois group $\mathrm{Gal}(K(\mathfrak{R}_f)/K)$ of f; it permutes the roots of f and may be viewed as a certain permutation group of $\mathfrak{R}_f$, i.e., as a subgroup of the group $\mathrm{Perm}(\mathfrak{R}_f) \cong \mathbf{S}_n$ of permutations of $\mathfrak{R}_f$. (The transitivity of $\mathrm{Gal}(f)$ is equivalent to the irreducibility of $f(x)$.) There is the canonical surjection

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

In particular, we may view $\mathrm{Gal}(f)$-modules

$$\mathbb{F}_p^{\mathfrak{R}_f}, (\mathbb{F}_p^{\mathfrak{R}_f})^0, (\mathbb{F}_p^{\mathfrak{R}_f})^{00}, (\mathbb{F}_p^{\mathfrak{R}_f})_0$$

as $\mathrm{Gal}(K)$-modules.

Let $C_{f,q}$ be a smooth projective model of the smooth affine K-curve $y^q = f(x)$. The map $(x, y) \mapsto (x, \zeta y)$ gives rise to a non-trivial birational K-automorphism $\delta_q : C_{f,q} \to C_{f,q}$ of period q. The jacobian $J(C_{f,q})$ of $C_{f,q}$ is an abelian variety that is defined over K. By Albanese functoriality, δ_q induces an automorphism of $J(C_{f,q})$ which we still denote by δ_p. It is known ([15, p. 149], [18, p. 458], [39, 42],[25, Lemma 2.6]) that δ_q satisfies

$$\mathcal{P}_q(\delta_q) = 0 \in \mathrm{End}(J(C_{f,q}))$$

where the polynomial

$$\mathcal{P}_q(t) = \frac{t^q - 1}{t - 1} = t^{q-1} + \cdots + 1 \in \mathbb{Z}[t].$$

Notice that

$$\mathcal{P}(t) = \prod_{j=1}^{r} \Phi_{p^j}(t)$$

where $\Phi_{p^j}(t) \in \mathbb{Z}[t]$ is the p^jth cyclotomic polynomial of degree $(p-1)p^{j-1}$.

Let us consider the abelian K-subvariety $J^{(f,q)}$ of $J(C_{f,q})$ defined as follows.

$$J^{(f,q)} = \mathcal{P}_{q/p}(\delta_q)((C_{f,q})) \subset J(C_{f,q}).$$

It is known [39, 44, 42, 25] that $J^{(f,q)}$ is positive-dimensional and $J(C_{f,q})$ is K-isogenous to a product $\prod_{j=1}^{r} J^{(f,p^j)}$. E.g., if $q = p$ (i.e, $r = 1$) then $J(C_{f,p}) = J^{(f,p)}$. (See also [24].)

Clearly, $J^{(f,q)}$ is δ_q-invariant and

$$\Phi_q(\delta_q)(J^{f,q}) = \{0\}.$$

This gives rise to the embedding

$$\imath : \mathbb{Z}[\zeta_q] \to \mathrm{End}_K(J^{(f,q)})$$

that sends 1 to $1_{J^{(f,q)}}$ and ζ_q to the restriction of δ_q to $J^{(f,q)}$.

Extending i by $\mathbb{Q}$-linearity to the $\mathbb{Q}$-algebra embedding

$$i : E = \mathbb{Q}(\zeta_q) \hookrightarrow \mathrm{End}_K^0(J^{(f,q)}),$$

which we continue to denote by i. Recall that

$$[E : \mathbb{Q}] = [\mathbb{Q}(\zeta_q) : \mathbb{Q}] = (p-1)p^{r-1}.$$

The dimension of $J^{(f,q)}$ and $d_{J^{(f,q)},E}$ are as follows [15, 18, 39, 42, 44, 25].

(i) If p does *not* divide n then

$$2\mathrm{dim}\left(J^{f,q}\right) = (n-1)(p^r - p^{r-1}),\ d_{J^{(f,q)},E} = n-1.$$

(ii) If q divides n then

$$2\mathrm{dim}\left(J^{(f,q)}\right) = (n-2)(p^r - p^{r-1}),\ d_{J^{f,q},E} = n-2.$$

(These equalities follow from (i) combined with [39, Remark 4.3 on p. 352]).

(iii) If p divides n but q does *not* divide n then [25]

$$2\mathrm{dim}\left(J^{(f,q)}\right) = (n-1)(p^r - p^{r-1}),\ d_{J^{(f,q)},E} = n-1.$$

Let λ be the maximal principal ideal $(1-\zeta_q)\mathbb{Z}[\zeta_q]$ in $Z[\zeta_q] = \mathcal{O}$. Its residue field $k(\lambda) = \mathbb{F}_p$.

Here is an explicit description of the Galois module $J_\lambda^{f,q}$ [15, 18, 39, 42, 44, 25].

(0) If (n,p) is neither $(3,3)$ nor $(4,2)$ then

$$\tilde{G}_{\lambda,J^{(f,q)},K} \cong \mathrm{Gal}(f).$$

(i) If p does *not* divide n then $J_\lambda^{(f,q)}$ is isomorphic to $(\mathbb{F}_p^{\mathfrak{R}_f})^0$ [39, Lemma 4.11]. (When $p=q$ this assertion was proven in [18].)

(ii) If q divides n then $J_\lambda^{(f,q)}$ is isomorphic to $(\mathbb{F}_p^{\mathfrak{R}_f})^{00}$, see Theorem 9.1 below. (When $q=p$ this assertion was proven in [15]).

(iii) If p divides n but q does *not* divide n then $J_\lambda^{(f,q)}$ is isomorphic to $(\mathbb{F}_p^{\mathfrak{R}_f})_0$ [25]. [4]

The results of Section 7 imply readily the following statement.

Lemma 8.1. *Suppose that (n,p) is neither $(3,3)$ nor $(4,2)$. Then the following conditions hold.*

(A) *The group $\tilde{G}_{\lambda,J^{(f,q)},K}$ is isomorphic to* $\mathrm{Gal}(f)$.

(B) *If p does not divide n and* $\mathrm{Gal}(f)$ *is doubly transitive then*

$$\mathrm{End}_{\tilde{G}_{\lambda,J^{(f,q)},K}}(J_\lambda^{(f,q)}) = \mathbb{F}_p.$$

(C) *If q divides n and either* $\mathrm{Gal}(f)$ *is 3-transitive or*

$$\mathrm{End}_{\mathrm{Gal}(f)}((\mathbb{F}_p^{\mathfrak{R}_f})^{00}) = \mathbb{F}_p$$

then

$$\mathrm{End}_{\tilde{G}_{\lambda,J^{(f,q)},K}}(J_\lambda^{(f,q)}) = \mathbb{F}_p.$$

[4] J. Xue [25] assumed that $\mathrm{char}(K) = 0$. However, all his arguments related to the computation of $\dim\left(J^{(f,q)}\right)$ and $J_\lambda^{(f,q)}$ work under a weaker assumption that $\mathrm{char}(K) \ne p$.

(D) *Suppose that p divides n but q does not divide n. Assume also that* $\mathrm{Gal}(f)$ *is transitive (i.e., $f(x)$ is irreducible over K) and the* $\mathrm{Gal}(f)$*-module* $(\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ *is absolutely simple. Then*

$$\mathrm{End}_{\tilde{G}_{\lambda,J^{(f,q)},K}}(J_\lambda^{(f,q)}) = \mathbb{F}_p.$$

Now let us assume that $\mathrm{char}(K) = 0$. Here are the explicit formulas for $n_{J^{(f,q)},i}$. Let

$$n = kq + c,\ k, c \in \mathbb{Z}_+,\ 0 \le c < q.$$

(i) Suppose that p does *not* divide n, i.e., $c \ge 1$. Then $n_{J^{(f,q)},i}$ are as follows [44, 45, Sections 4 and 5, especially, Remark 4.1 and Lemma 5.1].
   (1) if $n = kq + 1$ (i.e., $c = 1$) then $n_{J^{(f,q)},i} = k$.
   (2) If p is odd and $n-1$ is *not* divisible by q (i.e., $c > 1$) then $n_{J^{(f,q)},i} = 1$.
   (3) If $p = 2 < q$ and $n-1$ is *not* divisible by q (i.e., $c > 1$) then $n_{J^{(f,q)},i} = 1$ or 2. In addition, if either k is odd or $c < q/2$ then $n_{J^{(f,q)},i} = 1$.

(ii) Suppose that q divides n. Then $c = 0$ and

$$n - 1 = (k-1)q + (q-1).$$

Using [39, Remark 4.3 on p. 352], and (i), we obtain the following results similar to (i), replacing n by $n-1$, $n-1$ by $n-2$, k by $k-1$ and c by $q-1$ respectively.
   (1) If p is odd then $(n-2)$ is *not* divisible by q and $n_{J^{(f,q)},i} = 1$.
   (2) If $p = 2 < q$ then $n-2$ is *not* divisible by q and $n_{J^{(f,q)},i} = 1$ or 2. In addition, if $k-1$ is odd (i.e., k is even) then $n_{J^{(f,q)},i} = 1$.

(iii) If $n \ge 5$, p divides n but q does *not* divide n then $n_{J^{(f,q)},i} = 1$ [25, Prop. 2.2 and Remark 2.3].

Remark 8.2. The case of $n = 3$ is discussed in [42, 26]; see also [17].

Theorem 8.3. *Suppose that $n \ge 4$ and* $\mathrm{char}(K) = 0$*. If $p \mid n$ then we assume additionally that $n \ge 5$.*

If $\mathrm{End}^0(J^{(f,q)}, i)$ *coincides with* $i(\mathbb{Q}(\zeta_q)) = \mathbb{Q}[\delta_q]$ *then*

$$\mathrm{End}^0(J^{(f,q)}) = \mathbb{Q}[\delta_q] \cong \mathbb{Q}(\zeta_q),\ \mathrm{End}(J^{(f,q)}) = \mathbb{Z}[\delta_q] \cong \mathbb{Z}[\zeta_q].$$

Proof. (i) Suppose that p does *not* divide n. Then the result is proven in [39, Theorem 4.16].

(ii) Suppose that $q \mid n$. This case follows from (i), thanks to Remark 4.3 of [39].

(iii) Suppose that $p \mid n$ but q does *not* divide n. Then the result is proven in [25, Cor. 4.4]

□

Theorem 8.4. *Suppose that $n \ge 4$ and (n, p) is not $(4, 2)$. Assume also that there is a a subgroup*

$$\mathcal{G} \subset \mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f)$$

such that one of the following three conditions holds.

(i) *The prime p does not divide n, $\mathcal{G}$ is doubly transitive and does not contain a subgroup, whose index divides $(n-1)$ except $\mathcal{G}$ itself.*

(ii) *The prime power q divides n, $\mathcal{G}$ does not contain a proper subgroup, whose index divides $(n-2)$. In addition, either $\mathcal{G}$ is 3-transitive or*

$$\mathrm{End}_{\mathcal{G}}((\mathbb{F}_p^{\mathfrak{R}_f})^{00}) = \mathbb{F}_p.$$

(iii) *The prime p divides n but q does not divide n. The group $\mathcal{G}$ is transitive and does not contain a proper proper subgroup, whose index divides $(n-1)$. In addition, assume that (at least) one of the following two conditions holds.*

(A3) *The group $\mathcal{G}$ is transitive and the $\mathcal{G}$-module $(\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ is absolutely simple.*

(B3) *The centralizer $\mathrm{End}_{\mathcal{G}}\left((\mathbb{F}_p^{\mathfrak{R}_f})_0\right) = \mathbb{F}_p$.*

Then

$$\tilde{G}_{\lambda, J^{(f,q)}, K} \cong \mathrm{Gal}(f), \ \mathrm{End}_{\tilde{G}_{\lambda, J^{(f,q)}, K}}(J_\lambda^{(f,q)}) = \mathbb{F}_p,$$

$\mathrm{End}^0(J^{(f,q)})$ *is a simple $\mathbb{Q}$-algebra, whose center is a subfield of $\mathbb{Q}[\delta_q]$, and the centralizer* $\mathrm{End}^0(J^{(f,q)}, i)$ *of* $\mathbb{Q}[\delta_q]$ *in* $\mathrm{End}^0(J^{(f,q)})$ *is a central simple $\mathbb{Q}[\delta_q]$-algebra.*

Remark 8.5. By Theorem 7.8, the condition (A3) of Theorem 8.4 implies the condition (B3).

Proof of Theorem 8.4. Replacing K by its overfield $K(\mathfrak{R}_f)^{\mathcal{G}}$, we may and will assume that $\mathrm{Gal}(f) = \mathcal{G}$. it follows from Lemma 8.1 that

$$\mathrm{End}_{\tilde{G}_{\lambda, J^{(f,q)}, K}}(J_\lambda^{(f,q)}) = \mathbb{F}_p.$$

Now the desired result follows from Theorems 3.14. □

Remark 8.6. Suppose that $q = 2$, i.e.

$$\mathbb{Z}[\zeta_q] = \mathbb{Z}, \mathbb{Q}[\zeta_q] = \mathbb{Q}, \mathbb{Q}[\delta_q] = \mathbb{Q}.$$

In this case $C_{f,2}$ is a hyperelliptic curve of genus $[(n-1)/2]$, and

$$J(C_{f,2}) = J^{(f,2)}, \quad \left[\frac{n-1}{2}\right] = \dim(J(C_{f,2})) = \dim\left(J^{(f,2)}\right).$$

Applying Theorem 2.9 (instead of Theorems 3.14), we can do slightly better. Namely, we obtain that $\mathrm{End}^0(J(C_{f,2}))$ is a central simple $\mathbb{Q}$-algebra if there is a subgroup $\mathcal{G}$ of $\mathrm{Gal}(f)$ that enjoys the following properties.

- $\mathcal{G}$ contains neither a normal subgroup of index 2 nor a proper subgroup of index dividing $[(n-1)/2]$.
- One of the following two conditions holds.
  (1) n is odd and $\mathcal{G}$ is 2-transitive
  (2) n is even and either $\mathcal{G}$ is 3-transitive or

$$\mathrm{End}_{\mathcal{G}}((\mathbb{F}_p^{\mathfrak{R}_f})^{00}) = \mathbb{F}_p.$$

It follows from Albert's classification [14, Sect. 21] that the central simple $\mathbb{Q}$-algebra $\mathrm{End}^0(J(C_{f,2}))$ is isomorphic either to a matrix algebra over $\mathbb{Q}$ or to a matrix algebra over a quaternion $\mathbb{Q}$-algebra. See [27, 28, 29, 37, 30, 3, 4, 5, 31, 38, 33, 40] for other results about endomorphism algebras of hyperelliptic jacobians.

Theorem 8.7. *Let us assume that*

$$\mathrm{char}(K) = 0, n \geq 4, q > 2.$$

If $p \mid n$ then we assume additionally that $n \geq 5$.

Suppose that there is a subgroup

$$\mathcal{G} \subset \mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f)$$

such that (at least) one of the following three conditions holds.

(i) *The prime p does not divide n, $\mathcal{G}$ is doubly transitive and does not contain a proper normal subgroup, whose index divides $(n-1)$. Assume additionally that*

$$n = kq + c, \quad k, c \in \mathbb{Z}_+,\ 0 \le c < q.$$

where integers p, k and c enjoy (at least) one of the following three properties.

(A1) $n = q + 1$, *i.e.,* $k = 1, c = 1$.

(B1) p *is odd and* $c > 1$ *(i.e.,* q *does not divide* $n - 1$*).*

(C1) $p = 2 < q, c > 1$ *and either* k *is odd or* $c < q/2$.

(ii) *The prime power q divides n, $\mathcal{G}$ does not contain a proper normal subgroup, whose index divides $(n-2)$. We also assume that p and k enjoy (at least) one of the following three properties.*

(A2) p *is odd.*

(B2) $p = 2 < q$ *and* k *is even.*

(C2) *Either* $\mathcal{G}$ *is* 3*-transitive or*

$$\mathrm{End}_{\mathcal{G}}\left((\mathbb{F}_p^{\mathfrak{R}_f})^{00}\right) = \mathbb{F}_p.$$

(iii) *The prime p divides n but q does not divide n. The group $\mathcal{G}$ does not contain a proper normal subgroup, whose index divides $(n-1)$.*

In addition, assume that (at least) one of the following two conditions holds.

(A3) *The group $\mathcal{G}$ is transitive and the $\mathcal{G}$-module $(\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ is absolutely simple.*

(B3) *The centralizer* $\mathrm{End}_{\mathcal{G}}\left((\mathbb{F}_p^{\mathfrak{R}_f})_0\right) = \mathbb{F}_p$.

Then

$$\mathrm{End}^0(J^{(f,q)}) = \mathbb{Q}[\delta_q] \cong \mathbb{Q}(\zeta_q),\ \mathrm{End}(J^{(f,q)}) = \mathbb{Z}[\delta_q] \cong \mathbb{Z}[\zeta_q].$$

Proof. Clearly, (n,p) is neither $(3,3)$ nor $(4,2)$. Notice that our conditions on n and q imply that $n_{J^{(f,q)},E} = 1$. Second, Theorem 8.4 implies that

$$\tilde{G}_{\lambda, J^{(f,q)},K} \cong \mathrm{Gal}(f),\ \mathrm{End}_{\tilde{G}_{\lambda, J^{(f,q)},K}}(J_\lambda^{f,q}) = \mathbb{F}_p.$$

Now Theorem 6.11 implies that the centralizer $\mathrm{End}^0(J^{(f,q)}, i)$ coincides with $\mathbb{Q}[\delta_q] = i(\mathbb{Q}(\zeta_q))$. Now the desired result follows from Theorem 8.3. □

Remark 8.8. Suppose that $\mathrm{char}(K) = 0$, $n \ge 5$ and $\mathrm{Gal}(f)$ coincides either with the full symmetric group $\mathrm{Perm}(\mathfrak{R}_f) \cong \mathbf{S}_n$ or the alternating group $\mathrm{Alt}(\mathfrak{R}_f) \cong \mathbf{A}_n$. Then

$$\mathrm{End}^0(J^{(f,q)}) = \mathbb{Q}[\delta_q] \cong \mathbb{Q}(\zeta_q),\ \mathrm{End}(J^{(f,q)}) = \mathbb{Z}[\delta_q] \cong \mathbb{Z}[\zeta_q]$$

without any additional conditions on n and q. The case when either p does *not* divide n or $q \mid n$ was done in [39], the case when $p \mid n$ but q does *not* divide n was done in [25]. The proofs in [39] are based on the notion of a *very simple* representation that was introduced in [28], see also [40].

Remark 8.9. Theorem 8.7 is a generalization of ([44, Th. 5.2] [5] , [45, Th. 5.2]).

9. δ_q-invariant divisors on superelliptic curves

The aim of this section is to construct an isomorphism between the Galois modules $J_\lambda^{(f,q)}$ and $(\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ when q divides n. (The existence of such an isomorphism was stated and used in Section 8.)

Suppose that $n = \deg(f)$ is divisible by q, i.e, there is a positive integer m such that

$$n = mq.$$

We write $B = B_f$ for the set

$$B = \{(\alpha, 0) \mid \alpha \in \mathfrak{R}_f\} \subset C_{f,q}(K_a).$$

The set B consists of δ_q-invariant points of $C_{f,q}(K_a)$. Clearly, $C_{f,q}(K_a)$ contains an affine curve

$$(C_{f,q})_0(K_a) = \{(a,b) \in K_a^2 \mid f(a,b) = 0\}.$$

The complement $C_{f,q}(K_a) \backslash (C_{f,q})_0(K_a)$ is a finite *nonempty set*; we call its elements *infinite points* of $C_{f,q}$. The rational function $x \in K_a(C_{f,q})$ defines a finite cover $\pi : C_{f,q} \to \mathbb{P}^1$ of degree q. The set of branch points contains B and sits in the (disjoint) union of B and the (finite) set of infinite points of $C_{f,q}$; π sends the latter set to the *infinite point* ∞ of $\mathbb{P}^1(K_a)$. Clearly, y is a *local parameter* at every $P \in B$ and $\mathrm{ord}_P(x - x(P)) = q$. If $\tilde{\infty}$ is any infinite point of C then both $\mathrm{ord}_{\tilde{\infty}}(x)$ and $\mathrm{ord}_{\tilde{\infty}}(y)$ are *negative integers* such that $n \cdot \mathrm{ord}_{\tilde{\infty}}(x) = q \cdot \mathrm{ord}_{\tilde{\infty}}(y)$, i.e.,

$$\mathrm{ord}_{\tilde{\infty}}(y) = m \cdot \mathrm{ord}_{\tilde{\infty}}(x).$$

It follows easily from the previous remark that if $\beta \in K_a$ then the rational function $(x - \beta) \in K_a(C_{f,q})$ has a pole at $\tilde{\infty}$, whose order does *not* depend on β, including the cases $\beta = 0$ and $\beta = \alpha \in \mathfrak{R}_f$.

The main result of this section is the following statement.

Theorem 9.1. *Suppose that $n = \deg(f)$ is divisible by $q = p^r$.*

Then the $\mathrm{Gal}(K)$*-modules $J_\lambda^{(f,q)}$ and $(\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ are isomorphic.*

In the course of the proof of Theorem 9.1 we will use the following assertion that will be proven at the end of this section.

Lemma 9.2. *Let $D = \sum_{P \in B} a_P(P)$ be a degree zero divisor with support in B. Then the linear equivalence class of $p^{r-1}D$ is zero if and only if there exists an integer j such that all integers a_P's are congruent to j modulo p.*

Proof of Theorem 9.1 (modulo Lemma 9.2). The map $P \to x(P)$ establishes a Galois-equivariant bijection between B and $\mathfrak{R}_f$. So, it suffices to check that the Galois modules $J_\lambda^{(f,q)}$ and $(\mathbb{F}_p^B)^{00}$ are isomorphic. Notice that

$$J_\lambda^{(f,q)} = \{x \in J^{(f,q)}(K_a) \mid \delta_q(x) = x\} \subset J^{(f,q)}(K_a) =$$

$$\mathcal{P}_{q/p}(\delta_q)((J(C_{f,q})(K_a)) = \left(1 + \delta_q + \cdots + \delta_q^{p^{r-1}-1}\right)(J(C_{f,q})(K_a)).$$

Since $B \subset C_{f,q}(K_a)$ consists of δ_q-invariant points, the linear equivalence class of every degree zero divisor $D = \sum_{P \in B} a_P(P)$ is a δ_q-invariant point of $J(C_{f,q})(K_a)$.

[5] In Th. 5.2 of [44] the assertion (ii)(a) is actually not proven and should be ignored.

This implies that that the linear equivalence class of $p^{r-1}D = \sum_{P\in B} p^{r-1}a_P(P)$ lies in

$$\{x \in J^{(f,q)}(K_a) \mid \delta_q(x) = x\} = J_\lambda^{(f,q)} \subset J^{(f,q)}(K_a) \subset J(C_{f,q})(K_a).$$

Let us consider the following Galois-equivariant homomorphism of $\mathbb{F}_p$-vector spaces

$$\Psi : (\mathbb{F}_p^B)^0 \to J_\lambda^{(f,q)}.$$

Let $\phi : B \to \mathbb{F}_p$ be a function with $\sum_{b\in B}\phi(b) = 0$. We may "lift" ϕ to a map $P \to a_P \in \mathbb{Z}$ in such a may that

$$b_P \bmod p = \phi(P)\ \forall P \in B,\ \sum_{P\in P} a_P = 0.$$

Then $D = \sum_P a_P(P)$ is a degree zero divisor on $C_{f,q}$ with support in B. We define $\Psi(\phi) \in J_\lambda^{(f,q)}$ as the linear equivalence class of $p^{r-1}D$. First, notice that our map is well-defined. Indeed, if $P \mapsto a_P$ lifts the zero function then all a_P are divisible by p and therefore all the coefficients of $p^{r-1}D$ are divisible by $p \cdot p^{r-1} = q$. It follows from by Lemma 9.2 that the class of $p^{r-1}D$ is zero. This proves that Ψ is well-defined. Clearly, Φ is a group homomorphism and therefore is a $\mathbb{F}_p$-linear map. It follows from the same Lemma that $\phi \in \ker(\Psi)$ if and only if there exists $j \in \mathbb{Z}$ such that all (the corresponding) a_P's are congruent to j modulo p. This means that

$$\phi(P) = j \bmod p\ \forall P \in B,$$

i.e., ϕ is a constant function. In other words, $\ker(\Psi) = \mathbb{F}_p \cdot 1_B$. Therefore Φ induces a Galois-equivariant embedding of $\mathbb{F}_p$-vector spaces

$$(\mathbb{F}_p^B)^{00} = (\mathbb{F}_p^B)^0/(\mathbb{F}_p \cdot 1_B) \hookrightarrow J_\lambda^{(f,q)}.$$

This embedding is actually an isomorphism, since

$$\dim_{\mathbb{F}_p}((\mathbb{F}_p^B)^{00}) = n - 2 = \dim_{\mathbb{F}_p}(J_\lambda^{(f,q)}).$$

□

It remains to prove Lemma 9.2. We will need the following two assertions that characterize *principal divisors* with support in B.

Lemma 9.3. *Let $D = \sum_{P\in B} a_P(P)$ be a divisor on $C_{f,q}$ with support in B. Then D is principal if and only if there exist a divisor $D_1 = \sum_{P\in B} b_P(P)$ on $C_{f,q}$ with support in B and a nonnegative integer $j < q$ such that m divides* $\deg(D_1) = \sum_{P\in B} b_P$ *and*

$$D = q\sum_{B\in B} b_P(P) - \frac{\sum_{P\in B} b_P}{m}\left(\sum_{P\in B}(P)\right).$$

Corollary 9.4. *Let Q be a point of B. Then a divisor $D = \sum_{P\in B} a_P(P)$ with support in B is principal if and only if there is a degree zero divisor D_0 with support in B and an integer j such that*

$$D = qD_0 + j\left(\left(\sum_{P\in B}(P)\right) - n(Q)\right). \tag{7}$$

In addition, all integers a_P's are divisible by p^{r-1} if and only if j is divisible by p^{r-1}.

Proof of Lemma 9.3. Suppose $D = \mathrm{div}(h)$ where $h \in K_a(C_{f,q})$ is a *nonzero* rational function on C_f. Since D is δ_q-invariant, $\delta_q^* h = h\delta_q$ coincides with $c \cdot h$ for some nonzrero $c \in K_a$. The δ_q-invariance of the splitting

$$K_a(C_{f,q}) = \oplus_{j=0}^{q-1} y^j \cdot K_a(x)$$

implies that $h(x) = y^j \cdot u(x)$ for some nonzero rational function $u(x) \in K_a(x)$ and a nonnegative integer $j \leq q-1$. It follows that all "finite" zeros and poles of $u(x)$ lie in B. i.e., there exists an integer-valued function $P \mapsto b_P$ on B such that $u(x)$ coincides up to multiplication by a nonzero constant to $\prod_{P\in B}(x - x(P))^{b_P}$. Recall that the zero divisor of y is $\sum_{P\in B}(P)$ while the set of its poles coincides with the set of infinite points of C_f and if $\tilde{\infty}$ is such a point then

$$\mathrm{ord}_{\tilde{\infty}}(u) = (\sum_{P\in B} b_P)\mathrm{ord}_{\tilde{\infty}}(x) = \frac{\sum_{P\in B} b_P}{m} \cdot \mathrm{ord}_{\tilde{\infty}}(y).$$

Since $h(x) = y^j u(x)$ has neither zeros nor poles at infinite points of $C_{f,q}$,

$$\frac{\sum_{P\in B} b_P}{m} + j = 0.$$

On the other hand, for each $P \in B$,

$$a_P = \mathrm{ord}_P(h) = j + \mathrm{ord}_P(u) = j + qb_P.$$

This implies that

$$D = \sum_{P\in B} a_P(P) = q\sum_{P\in B} b_P(P) + j\sum_{P\in B}(P) = q\sum_{P\in B} b_P(P) - \frac{\sum_{P\in B} b_P}{m}(\sum_{P\in B}(P)).$$

Conversely, suppose that there is a divisor $\sum_{P\in B} b_P(P)$ on C_f with support in B such that m divides $\left(\sum_{P\in B} b_P\right)$ and

$$D = q\sum_{P\in B} b_P(P) - \frac{\sum_{P\in B} b_P}{m}\left(\sum_{P\in B}(P)\right).$$

Clearly, $\deg(D) = 0$. Let us put

$$j := -\frac{\sum_{P\in B} b_P}{m}.$$

Let us consider the (nonzero) rational function

$$h = y^j \prod_{P\in B}(x - x(P))^{b_P} \in K_a(C_f).$$

Clearly h has neither zeros nor poles at infinite points of C_f, because

$$\mathrm{ord}_{\tilde{\infty}}(h) = j\mathrm{ord}_{\tilde{\infty}}(y) + (\sum_{P\in B} b_P)\mathrm{ord}_{\tilde{\infty}}(x) = (mj + \sum_{P\in B} b_P)\mathrm{ord}_{\tilde{\infty}}(x) = 0\cdot\mathrm{ord}_{\tilde{\infty}}(x) = 0.$$

This implies that the support of $\mathrm{div}(h)$ lies in B. For each $P \in B$

$$\mathrm{ord}_P(h) = j + qb_P = a_P.$$

This implies that $D = \mathrm{div}(h)$, i.e., D is *principal*. □

Proof of Corollary 9.4. Clearly, $n(Q)-\sum_{P\in B}(P)$ is the divisor of the rational function $(x-x(Q))^m/y$ and $q((P)-(Q))$ is the divisor of the rational function $(x-x(P))/(x-x(Q))$. This implies that a divisor D of the form (7) is principal.

Conversely, suppose that a divisor $D=\sum_{P\in B}a_P(P)$ with support in B is principal. Let $\sum_{P\in B}b_P(P)$ and j be as in Lemma 9.3 and its proof, i.e.,

$$j=-\frac{\sum_{P\in B}b_P}{m}\in\mathbb{Z},\ D=q\sum_{P\in B}b_P(P)+j\left(\sum_{P\in B}(P)\right).$$

Let us put

$$D_0=(\sum_{P\in B}b_P(P))-(\sum_{P\in B}b_P)(Q)=(\sum_{P\in B}b_P(P))+jm(Q).$$

Clearly, D_0 is a degree zero divisor with support in B and

$$D=q\sum_{P\in B}b_P(P)-q(\sum_{P\in B}b_P)(Q)+q(\sum_{P\in B}b_P)(Q)+j\left(\sum_{P\in B}(P)\right)=$$

$$qD_0-qjm(Q)+j\left(\sum_{P\in B}(P)\right)=qD_0-jn(Q)+j\left(\sum_{P\in B}(P)\right)=qD_0+j\left(\left(\sum_{P\in B}(P)\right)-n(Q)\right).$$

In order to prove the second assertion of Corollary, notice that both $q=p^r$ and $n=qm=p^rm$ are divisible by p^{r-1} and therefore all the coefficients of D are divisible by p^{r-1} if and only if all the coefficients of $j\left(\sum_{P\in B}(P)\right)$ are divisible by p^{r-1} as well. All the coefficients of $j\left(\sum_{P\in B}(P)\right)$ are equal to j and therefore are divisible by p^{r-1} if and only if j is divisible by p^{r-1}. □

Proof of Lemma 9.2. Let us fix a point $Q\in B$.

Suppose that the class of $p^{r-1}D$ is zero. By Corollary 9.4 (applied to $p^{r-1}D$), there exist a a degree zero divisor $D_0=\sum P\in Bb_P(P)$ and an integer $j_0=j_0(Q)\in\mathbb{Z}$ such that

$$p^{r-1}D=p^rD_0+p^{r-1}j_0\left(\left(\sum_{P\in B}(P)\right)-n(Q)\right).$$

This means that

$$p^{r-1}a_Q=p^rb_Q+p^{r-1}j_0(Q)\cdot(1-n),\ p^{r-1}a_P=p^rb_P+p^{r-1}j_0(Q)\ \forall P\in B\setminus\{Q\}.$$

The first equality implies that $(1-n)j_0(Q)$ is congruent to a_Q modulo p, which means that $j_0(Q)$ is congruent to a_Q modulo p (since $p\mid n$). The second equality implies that a_P is congruent to $j_0(Q)$ modulo P, i.e., a_P is congruent to a_Q for all $P\in B\setminus\{Q\}$. Since a_Q is obviously congruent to itself modulo p, we obtain that a_P is congruent to a_Q modulo p for each $P,Q\in B$. Now we may put $j=a_Q$.

Conversely, suppose that $D=\sum_{P\in B}a_P(P)$ is a degree zero divisor with support in B such that all a_P are congruent modulo p to a certain fixed (independent on P) integer $\mathbf{j}$. Then

$$p^{r-1}D=p^{r-1}\mathbf{j}\left(\sum_{P\in B}(P)\right)+p^{r-1}p\left(\sum_{P\in B}\frac{(a_P-\mathbf{j})}{p}(P)\right)=$$

$$p^{r-1}\mathbf{j}\left(\sum_{P\in B}(P)\right)+p^r\left(\sum_{P\in B}b_P(P)\right)$$

where $b_P = (a_P - \mathbf{j})/p$. Clearly,

$$\sum_{P\in B} b_P = \sum_{P\in B} \frac{(a_P - \mathbf{j})}{p} = \frac{1}{p}\left(\sum_{P\in B}(a_P - \mathbf{j})\right) = \frac{1}{p} n\,(-\mathbf{j}) = -p^{r-1}m\mathbf{j}.$$

This implies that

$$p^{r-1}D = p^{r-1}\mathbf{j}\left(\left(\sum_{P\in B}(P)\right) - n(Q)\right) + p^{r-1}\mathbf{j}n(Q) + p^r\left(\sum_{P\in B} b_P(P)\right) =$$

$$p^{r-1}\mathbf{j}\left(\left(\sum_{P\in B}(P)\right) - n(Q)\right) + p^r D_0$$

where Q is any point of B and

$$D_0 = p^{r-1}\mathbf{j}m(Q) + \left(\sum_{P\in B} b_P(P)\right).$$

Since $\deg(D) = 0$, the degree of D_0 is also zero. It follows from Corollary 9.4 that the class of $p^{r-1}D$ is 0. □

References

[1] E. Artin, Geometric Algebra. Interscience Publishers, New York, 1957.

[2] J. D. Dixon, B. Mortimer, Permutation Groups. Springer, New York Berlin Heidelberg, 1996.

[3] A. Elkin, *Hyperelliptic jacobians with real multiplication*. J. Number Theory **117** (2006), 53–86.

[4] A. Elkin, Yu. G. Zarhin, *Endomorphism algebras of hyperelliptic jacobians and finite projective lines*. J. Ramanujan Math. Soc. **21** (2006), 169–187.

[5] A. Elkin and Yu. G. Zarhin, *Endomorphism algebras of hyperelliptic Jacobians and finite projective lines*. II, J. Ramanujan Math. Soc. **25** (2010), 1–23.

[6] U. Görtz, T. Wedhorn, Algebraic Geometry I. Vieweg+Teubner Verlag, Wiesbaden, 2010.

[7] I. N. Herstein, Noncommutative rings. The Mathematical Association of America/John Wiley and Sons, 1968.

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

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

[10] Sh. Mori, *The endomorphism rings of some abelian varieties II*. Japan. J. Math. **3** (1997), 105–109

[11] S. Lang, Abelian varieties, 2nd edn. Springer Verlag, New York, 1983.

[12] S. Lang, Algebra. 3rd edn. Addison-Wesley, Reading, MA, 1993.

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

[14] D. Mumford, Abelian varieties. 2nd edn. Oxford University Press, London (1974).

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

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

[17] K. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*. Ann. Math. (2) **101** (1975), 555–562.

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

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

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

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

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

[23] B.L. van der Waerden, Algebra I. Achte Auflage. Springer, Berlin Heidelberg New York, 1971.

[24] H. Wang, J. Xue, Ch. F. Yu, *Fixed points and homology of superelliptic jacobians*. Math. Z. **278** (2014), 169–189.

[25] J. Xue, *Endomorphism algebras af Jacobians of certain superelliptic curves*. J. Number Theory **131** (2011), 332–342.

[26] J. Xue, Ch.-F. Yu, *Endomorphism algebras of factors of certain hypergeometric Jacobians*.Trans. Amer. Math. Soc. 367 (2015), no. 11, 8071–8106.

[27] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Res. Letters **7** (2000), 123–132.

[28] Yu. G. Zarhin, *Hyperelliptic jacobians and modular representations*. In: Moduli of abelian varieties (C. Faber, G. van der Geer, F. Oort, editors). Progress in Math. **195** (2001), 473–490. Birkhäuser, Boston.

[29] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication in positive characteristic*. Math. Res. Letters **8** (2001), 429–435.

[30] Yu. G. Zarhin, *Very simple* 2*-adic representations and hyperelliptic jacobians*. Moscow Math. J. **2** (2002), issue 2, 403-431.

[31] Yu. G. Zarhin, *Hyperelliptic jacobians without Complex Multiplication, Doubly Transitive Permutation Groups and Projective Representations*. Contemp. Math. **300** (2002), 195–210.

[32] Yu. G. Zarhin, *Endomorphism rings of certain jacobians in finite characteristic*. Matem. Sbornik **193** (2002), issue 8, 39–48; Sbornik Math. **193** (8) (2002), 1139-1149.

[33] Yu. G. Zarhin, *Hyperelliptic jacobians and simple groups* $\mathrm{U}_3(2^m)$. Proc. AMS **131** (2003), 95–102.

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

[35] Yu. G. Zarhin, *Homomorphisms of hyperelliptic jacobians*. In: Number Theory, Algebra, Algebraic Geometry (Shafarevich Festschrift). Proceedings of the Steklov Institute of Math. **241** (2003), 79–92.

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

[37] Yu. G. Zarhin, *Non-supersingular hyperelliptic jacobians*. Bull. Soc. Math. France **132** (2004), 617–634.

[38] Yu. G. Zarhin, *Homomorphisms of abelian varieties*. In: Arithmetic, Geometry and Coding Theory (AGCT 2003) (Y. Aubry, G. Lachaud, editors). Séminaires et Congrès **11** (2005), 189–215.

[39] Yu. G. Zarhin, *Endomorphism algebras of superelliptic Jacobians*. In: Geometric methods in Algebra and Number Theory (F. Bogomolov, Yu. Tschinkel, editors). Progress in Math. **235** (2005), 339–362. Birkhäuser, Boston Basel Berlin.

[40] Yu. G. Zarhin, *Very simple representations: variations on a theme of Clifford*, pp. 151–168. In: Progress in Galois Theory (H. Voelklein, T. Shaska, eds.), Springer Science+Business Media , Inc., 2005.

[41] Yu. G. Zarhin, *Del Pezzo surfaces of degree* 2 *and jacobians without complex multiplication*. Trudy St. Petersburg Mat. Obsch. **11** (2005), 81–91; AMS Translations - Series 2, vol. **218** (2006), 67–75.

[42] Yu. G. Zarhin, *Superelliptic jacobians*, pp. 363-390. In: "Diophantine Geometry" Proceedings (U. Zannier, ed.), Edizioni Della Normali, Pisa, 2007.

[43] Yu.G. Zarhin, *Non–isogenous superelliptic jacobians*. Math. Z. **253** (2006), 537–554.

[44] Yu.G. Zarhin, *Endomorphisms of superelliptic jacobians*. Math. Z. **261** (2009), 691–707, 709.

[45] Yu.G. Zarhin, *Endomorphisms of superelliptic jacobians*. arXiv:math/0605028v6 [math.AG].

[46] Yu.G. Zarhin, *Absolutely simple Prymians of trigonal curves*. Trudy Steklov Math. Inst. **264** (2009), 212–223; English translation: Proceedings of the Steklov Institute of Math. **264** (2009), 204–215.

[47] Yu.G. Zarhin, *Hodge classes on certain hyperelliptic prymians*. In: Arithmetic, Geometry, Cryptography and Coding Theory (AGCT 2011) (Y.Aubry, Ch. Ritzenthaler, A. Zykin, eds.), Contemporary Math. **574** (2012), 171–183.

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA
E-mail address: zarhin@math.psu.edu