Mathematics
Research
Reports

Yuri G. Zarhin

On matrices of endomorphisms of abelian varieties

Volume 1 (2020), p. 55-68.

<http://mrr.centre-mersenne.org/item/MRR_2020__1__55_0>

𝕄athematics ℝesearch ℝeports
Volume 1 (2020), 55–68

On matrices of endomorphisms of abelian varieties

Yuri G. Zarhin

(Recommended by Linus Kramer)

Abstract. We study endomorphisms of abelian varieties and their action on the ℓ-adic Tate modules. We prove that for every endomorphism one may choose a basis of each $\mathbb{Q}_\ell$-Tate module such that the corresponding matrix has rational entries and does not depend on ℓ.

1. Introduction

Let X be an abelian variety of positive dimension g over an algebraically closed field K of arbitrary characteristic. We write $\mathrm{End}(X)$ for the endomorphism ring of X and $\mathrm{End}^0(X)$ for the corresponding $\mathbb{Q}$-algebra

$$\mathrm{End}^0(X) := \mathrm{End}(X) \otimes \mathbb{Q},$$

which is a finite-dimensional semisimple algebra over $\mathbb{Q}$. If n is any integer, then we write $n_X \in \mathrm{End}(X)$ for multiplication by n in X, which is an isogeny if $n \neq 0$. For example, 1_X is the identity automorphism of X.

One may view $\mathrm{End}(X) = \mathrm{End}(X) \otimes 1$ as an *order* in $\mathrm{End}^0(X)$. Let $\ell \neq \mathrm{char}(K)$ be a prime and $T_\ell(X)$ be the ℓ-adic Tate module of X, which is a free $\mathbb{Z}_\ell$-module of rank $2g$ [6]. We write $V_\ell(X)$ for the corresponding $\mathbb{Q}_\ell$-vector space

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

of dimension $2g$.

By functoriality, there is the natural injective ring homomorphism (see [6])

$$\mathrm{End}(X) \to \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(X)), u \mapsto u_\ell$$

that extends by $\mathbb{Z}_\ell$-linearity to the injective $\mathbb{Z}_\ell$-algebra homomorphism

$$\mathrm{End}(X) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(X)),\ u \mapsto u_\ell$$

and extends by $\mathbb{Q}_\ell$-linearity to the injective $\mathbb{Q}_\ell$-algebra homomorphism

$$\mathrm{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathrm{End}(X) \otimes \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X)),\ u \mapsto u_\ell$$

(see [9, 6]).

If $u \in \mathrm{End}^0(X)$, then let us consider the monic characteristic polynomial of degree $2g$

$$\mathcal{P}_u(t) := \det(t\mathrm{Id} - u_\ell, V_\ell(X)) \in \mathbb{Q}_\ell[t]$$

of $u_\ell \in \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))$. (Here $\mathrm{Id} : V_\ell(X) \to V_\ell(X)$ is the identity map.) A classical result of Weil [6, Sect. 19, Th. 4 on p. 180 and Definition on p. 182] asserts that if $u \in \mathrm{End}(X)$, then $\mathcal{P}_u(t)$ lies in $\mathbb{Z}[t]$ and does not depend on the choice of ℓ. It readily follows that if $u \in \mathrm{End}^0(X)$, then $\mathcal{P}_u(t)$ lies in $\mathbb{Q}[t]$ and does not depend on the choice of ℓ.

Received February 1, 2020; accepted May 25, 2020.
2020 *Mathematics Subject Classification.* 14K05,16K20.
Keywords. Abelian varieties, Tate modules, Semisimple algebras.
Acknowledgements. The author was partially supported by Simons Foundation Collaboration grant # 585711. Part of this work was done in December 2019 - January 2020 during his stay at the Weizmann Institute of Science Department of Mathematics, whose hospitality and support are gratefully acknowledged.

The aim of this note is to prove the following assertion.

Theorem 1.1. *Let X be an abelian variety of positive dimension g over an algebraically closed field K of arbitrary characteristic. Let $u \in \mathrm{End}^0(X)$. Then there exists a square matrix $M(u)$ of size $2g$ with entries in $\mathbb{Q}$ that enjoys the following property.*

If ℓ is any prime $\neq \mathrm{char}(K)$, then there is a basis of the $2g$-dimensional $\mathbb{Q}_\ell$-vector space $V_\ell(X)$ such that the corresponding matrix of $u_\ell \in \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))$ coincides with $M(u)$.

Remark 1.2. In the case of characteristic 0, the assertion of Theorem 1.1 reduces to the case of $K = \mathbb{C}$ where it is obvious; in addition, if $u \in \mathrm{End}(X)$, then one may chose bases in the free $\mathbb{Z}_\ell$-modules $T_\ell(X)$ in such a way that the corresponding matrices $M(u)$ have entries in $\mathbb{Z}$ and do not depend on the choice of ℓ.

Examples 1.3. (i) Let E be a subfield of $\mathrm{End}^0(X)$ that contains 1_X. Then E is a number field; let d be its degree over $\mathbb{Q}$. The natural $\mathbb{Q}_\ell$-algebra homomorphism

$$E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \to \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X)),\ u \mapsto u_\ell \tag{1.1}$$

is injective [9, 6] and endows $V_\ell(X)$ with the structure of a faithful $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module. It is known [8] that this module is *free* and its rank is

$$h := \frac{2g}{d}$$

(in particular, $d \mid 2g$). Let us choose an h-element basis

$$\{z_1, \ldots, z_h\} \subset V_\ell(X)$$

of the $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module $V_\ell(X)$. Also, choose a d-element basis

$$B_E = \{\alpha_1, \ldots, \alpha_d\} \subset E \tag{1.2}$$

of the $\mathbb{Q}$-vector space E. Then the d-element set

$$B_{E,\ell} := \{\alpha_1 = \alpha_1 \otimes 1, \ldots, \alpha_d = \alpha_d \otimes 1\} \subset E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \tag{1.3}$$

is a basis of the d-dimensional $\mathbb{Q}_\ell$-vector space $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. It follows that the $2g(= dh)$-element set

$$B_{E,\ell,X} := \{\alpha_{i,\ell} z_j \mid 1 \le i \le d,\ 1 \le j \le h\} \subset V_\ell(X) \tag{1.4}$$

is a basis of the $\mathbb{Q}_\ell$-vector space $V_\ell(X)$. (Here $\alpha_{i,\ell} \in \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))$ is the image of

$$\alpha_i = \alpha_i \otimes 1 \in E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$$

under the injective homomorphism (1.1).) Now assume that

$$u \in E = E \otimes 1 \subset E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell,$$

and let $M_0(u)$ be the matrix of the $\mathbb{Q}$-linear map

$$\mathrm{mult}_u : E \to E,\ w \mapsto uw \ \text{ for all } w \in E$$

with respect to B_E (1.2). Clearly, $M_0(u)$ coincides with the matrix of the $\mathbb{Q}_\ell$-linear map

$$E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \to E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell,\ w \mapsto uw$$

with respect to $B_{E,\ell}$ (1.3). It follows that the matrix $M(u)$ of u_ℓ w.r.t. $B_{E,\ell,X}$ (1.4) is the block diagonal matrix, whose all diagonal entries coincide with $M_0(u)$. In particular, all entries of $M(u)$ are rational numbers and $M(u)$ does not depend on the choice of ℓ. Notice that we use the same basis $B_{E,\ell,X}$ for all $u \in E$.

(ii) Let m be a positive integer and let us consider the abelian variety $Y = X^m$. Then $\mathrm{End}^0(Y) = \mathrm{Mat}_m(\mathrm{End}^0(X))$ and there is the natural embedding

$$\mathrm{Mat}_m(E) \subset \mathrm{Mat}_m(\mathrm{End}^0(X)) = \mathrm{End}^0(Y).$$

We also have

$$V_\ell(Y) = \bigoplus_{i=1}^m V_\ell(X),\ \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(Y)) = \mathrm{Mat}_m(\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))).$$

The basis $B_{E,\ell,X}$ of $V_\ell(X)$ gives rise to the obvious basis $B^{(m)}_{E,\ell,X}$ of the $\mathbb{Q}_\ell$-vector space $\bigoplus_{i=1}^m V_\ell(X) = V_\ell(Y)$ that enjoys the following properties. If

$$u = \left(u_{ij}\right)_{i,j=1}^m \in \mathrm{Mat}_m(E) \subset \mathrm{Mat}_m(\mathrm{End}^0(X)) = \mathrm{End}^0(Y),$$

then the matrix of $u_\ell \in \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(Y))$ w.r.t. $B^{(m)}_{E,\ell,X}$ coincides with the block matrix $\left(M(u_{ij})\right)_{i,j=1}^m$. In particular, all its entries lie in $\mathbb{Q}$ and do not depend on the choice of ℓ.

The paper is organized as follows. In Section 2 we discuss the plan of the proof of Theorem 1.1. In particular, we obtain that Theorem 1.1 follows from certain auxiliary assertions about endomorphism subalgebras of abelian varieties (Theorems 2.1 and 2.2) and about elements of finite-dimensional semisimple algebras in characteristic 0 (Theorem 2.4). The results about endomorphism subalgebras are proven in Section 3. The assertion about semisimple algebras is proven in Section 4.

Acknowledgements. I am grateful to Fei Xu for interesting stimulating questions about endomorphisms of abelian varieties and useful comments to the preliminary version of the paper. My special thanks go to the referee, whose thoughtful comments helped to improve the exposition.

2. Endomorphism subalgebras of abelian varieties: statements

In the course of the proof of Theorem 1.1, we will use the following assertions.

Theorem 2.1. *Let D be a finite-dimensional $\mathbb{Q}$-algebra with identity element 1_D and let W be a positive-dimensional abelian variety over K endowed with a $\mathbb{Q}$-algebra embedding $\tau : D \hookrightarrow \mathrm{End}^0(W)$ that sends 1_D to 1_W. Suppose that $r \ge 2$ is an integer and D splits into a direct sum $D = \bigoplus_{i=1}^r D_i$ of r nonzero finite-dimensional $\mathbb{Q}$-algebras D_i. We will identify D_i's with the corresponding two-sided ideals in D. Then for all $i = 1,\dots,r$ there exist positive-dimensional abelian subvarieties $W_i \subset W$ and $\mathbb{Q}$-algebra embeddings $\tau_i : D_i \hookrightarrow \mathrm{End}^0(W_i)$ that send 1_{D_i} to 1_{W_i} and enjoy the following properties.*

(i) *The homomorphism of abelian varieties*

$$S : \prod_{i=1}^r W_i \to W,\ \{w_i\}_{i=1}^r \mapsto \sum_{i=1}^r w_i$$

is an isogeny.

(ii) *For each $u = \sum_{i=1}^r u_i \in D$ with $u_i \in D_i$, for every i we have*

$$\{\tau_i(u_i)\}_{i=1}^r \in \bigoplus_{i=1}^r \mathrm{End}^0(W_i) \subset \mathrm{End}^0\left(\prod_{i=1}^r W_i\right),$$

$$S \circ \left(\{\tau_i(u_i)\}_{i=1}^r\right) \circ S^{-1} = \tau(u) \in \mathrm{End}^0(W).$$

Theorem 2.2. *Let E be a number field, m a positive integer, $\mathrm{Mat}_m(E)$ the matrix algebra of size m over E, and Z an abelian variety of positive dimension over K endowed with a $\mathbb{Q}$-algebra embedding $\widetilde{\kappa} : \mathrm{Mat}_m(E) \hookrightarrow \mathrm{End}^0(Z)$ that sends the identity matrix $\mathrm{Id}_m \in \mathrm{Mat}_m(E)$ to 1_Z.*

Then there are a positive-dimensional abelian variety X over K, a $\mathbb{Q}$-algebra embedding $\kappa : E \hookrightarrow \mathrm{End}^0(X)$ that sends 1 to 1_X, and an isogeny of abelian varieties $\psi : X^m \to Z$ that enjoy the following properties.

Let $\mathrm{Mat}_m(\kappa) : \mathrm{Mat}_m(E) \hookrightarrow \mathrm{Mat}_m(\mathrm{End}^0(X)) = \mathrm{End}^0(X^m)$ *be the natural $\mathbb{Q}$-algebra embedding that sends a matrix $\left(a_{ij}\right)_{i,j=1}^m \in \mathrm{Mat}_m(E)$ to*

$$\left(\kappa(a_{ij})\right)_{i,j=1}^m \in \mathrm{Mat}_m(\mathrm{End}^0(X)) = \mathrm{End}^0(X^m).$$

Then

$$\widetilde{\kappa}(u) = \psi \circ \mathrm{Mat}_m(\kappa)(u) \circ \psi^{-1} \text{ for every } u \in \mathrm{Mat}_m(E). \tag{2.1}$$

Remark 2.3. Notice that in the notation of Theorem 2.2, ψ induces (by functoriality of Tate modules) the isomorphism

$$\psi_\ell : V_\ell(X^m) \cong V_\ell(Z)$$

of $\mathbb{Q}_\ell$-vector spaces. Thus $\psi_\ell\left(B^{(m)}_{E,\ell,X}\right)$ is a basis of the $\mathbb{Q}_\ell$-vector space $V_\ell(Z)$. It follows from (2.1) combined with Example 1.3(ii) that for each $u \in \mathrm{Mat}_m(E)$ there exists a square matrix $M(u)$ of size $2\dim(Z)$ with rational entries that enjoys the following property. For each prime $\ell \neq \mathrm{char}(K)$ the matrix of $\widetilde{\kappa}(u)_\ell$ with respect to $\psi_\ell\left(B^{(m)}_{E,\ell,X}\right)$ coincides with $M(u)$.

In light of Theorem 2.1, Theorem 2.2, and Remark 2.3, Theorem 1.1 is an immediate corollary of the following assertion applied to the semisimple $\mathbb{Q}$-algebra $\mathrm{End}^0(X)$.

Theorem 2.4. *Let D be a finite-dimensional semisimple algebra over $\mathbb{Q}$. Then every element of D is contained in a subalgebra of D with the same identity element that is isomorphic to a direct sum of matrix algebras over number fields.*

We prove Theorem 2.4 in Section 4. Theorems 2.1 and 2.2 will be proven in Section 3.

3. Endomorphism subalgebras of abelian varieties: proofs

Results of this section (Lemma 3.1 and Theorem 3.2) and their proofs are rather straightforward (and boring). However, we need them in order to prove Theorem 2.1.

Throughout this section, let D be a finite-dimensional $\mathbb{Q}$-algebra with the identity element 1_D and W a positive-dimensional abelian variety over K endowed with a $\mathbb{Q}$-algebra embedding

$$\tau : D \hookrightarrow \mathrm{End}^0(W)$$

that sends 1_D to 1_W.

Lemma 3.1. *Let u_1, u_2 be two conjugate elements of D, i.e., there exists $s \in D^*$ such that*

$$u_2 = s u_1 s^{-1}.$$

Let N be a positive integer such that all three elements

$$N\tau(u_1) = \tau(Nu_1), N\tau(u_2) = \tau(Nu_2), N\tau(s) = \tau(Ns) \in \mathrm{End}^0(W)$$

actually lie in $\mathrm{End}(W)$. *Let us consider abelian subvarieties*

$$W_1 := \tau(Nu_1)(W) \subset W,\ W_2 := \tau(Nu_2)(W) \subset W$$

of W. Then

$$\tau(Ns)(W_1) = W_2.$$

In addition, the restriction

$$\tau(Ns)\big|_{W_1} : W_1 \to W_2$$

is an isogeny of abelian varieties.

Proof. Renaming Nu_1, Nu_2, Ns by u_1, u_2, s respectively, we may and will assume that

$$\tau(u_1), \tau(u_2), \tau(s) \in \mathrm{End}(W),\ N = 1.$$

Since s in invertible in D, the endomorphism

$$\tau(s) : W \to W$$

is invertible in $\mathrm{End}^0(W)$ and therefore is an isogeny. This means that

$$\tau(s)(W) = W, \tag{3.1}$$

and there is a positive integer r such that multiplication by r annihilates $\ker(\tau(s))$. Furthermore, the equality $u_2 = su_1s^{-1}$ means that $u_2s = su_1$ and therefore

$$\tau(u_2)\tau(s) = \tau(s)\tau(u_1).$$

Combining it with (3.1) and the definition of W_1 and W_2, we obtain that

$$W_2 = \tau(u_2)(W) = \tau(u_2)\tau(s)(W) = \tau(s)\tau(u_1)(W) = \tau(s)W_1,$$

i.e.,

$$W_2 = \tau(s)W_1.$$

This means that the restriction

$$\tau(s)\big|_{W_1} : W_1 \to W_2,\ w_1 \mapsto s(w_1)$$

is a surjective morphism of abelian varieties. Since its kernel $\ker(\tau(s)\big|_{W_1}$ is a group subscheme of $\ker(\tau(s))$, it is also annihilated by multiplication by r. This implies that $\tau(s)\big|_{W_1}$ is an isogeny. □

The following assertion contains Theorem 2.1.

Theorem 3.2. *Suppose that $r \ge 2$ is an integer and D splits into a direct sum*

$$D = \bigoplus_{i=1}^{r} D_i$$

of r nonzero finite-dimensional $\mathbb{Q}$-algebras D_i. We will identify D_i's with the corresponding two-sided ideals in D. Let us consider the subrings

$$O_i := \{u_i \in D_i \subset D \mid \tau(u_i) \in \mathrm{End}(W)\}$$

of D_i $(1 \le i \le r)$.

Let $e_i := 1_{D_i}$ be the identity element of D_i viewed as a nonzero central idempotent in D. Let N be a positive integer such that $Ne_i \in O_i$ for all i, i.e., all $\tau(Ne_i) = N\tau(e_1)$ lie in $\mathrm{End}(W)$. *(Such an N always exists.) Let us consider abelian subvarieties $W_i := \tau(Ne_i)(W) \subset W$ of W.*

Then:

(i) (a) *The natural $\mathbb{Q}$-algebra homomorphisms*

$$O_i \otimes \mathbb{Q} \to D_i,\ u_i \otimes c \mapsto c \cdot u_i$$

are isomorphisms for $i = 1, \ldots, r$.

(b) *For each*

$$i, j \in \{1, \ldots, r\},\ i \neq j$$

and $w_i \in W_i, w_j \in W_j$

$$\tau(Ne_i)(w_i) = Nw_i, \tau(Ne_j)(w_i) = 0. \tag{3.2}$$

(ii) *The natural morphisms of abelian varieties*

$$S:\prod_{i=1}^{r}W_i\to W,\ \{w_i\}_{i=1}^{r}\mapsto\sum_{i=1}^{r}w_i,\ P:W\to\prod_{i=1}^{r}W_i,\ w\mapsto\{\tau(Ne_i)(w_i)\}_{i=1}^{r} \tag{3.3}$$

are isogenies such that

$$P\circ S=N_W,\ S\circ P=N_{\widetilde{W}}\ \ \textit{where}\ \widetilde{W}:=\prod_{i=1}^{r}W_i. \tag{3.4}$$

In particular, $\sum_{i=1}^{r}W_i=\left\{\sum_{i=1}^{r}w_i\mid w_i\in W_i\ \textit{for all}\ i\right\}$ *coincides with* W.

(iii) *For each* $u_i\in O_i$ *and* $u_j\in O_j$ *with* $i\neq j$

$$\tau(u_i)(W_i)\subset W_i,\tau(u_j)(W_i)=\{0\},\ \tau(u_i)(W_j)=\{0\},\tau(u_j)(W_j)\subset W_j. \tag{3.5}$$

(iv) *There exist* $\mathbb{Q}$*-algebra embeddings*

$$\tau_i:D_i\to\mathrm{End}^0(W_i)$$

that enjoy the following properties.

(c) $\tau_i(e_i)=1_{W_i}$.

(d) *If* $u_i\in O_i\subset D_i$, *then* $\tau_i(u_i)\in\mathrm{End}(W_i)$ *and*

$$\tau_i(u_i)(w_i)=\tau(u_i)(w_i)\in W_i\ \textit{for any}\ w_i\in W_i.$$

(e) *For each*

$$u=\sum_{i=1}^{r}u_i\in D\ \ \textit{with}\ u_i\in D_i\ \ \textit{for any}\ i$$

we have

$$\{\tau_i(u_i)\}_{i=1}^{r}\in\bigoplus_{i=1}^{r}\mathrm{End}^0(W_i)\subset\mathrm{End}^0\left(\prod_{i=1}^{r}W_i\right)=\mathrm{End}^0(\widetilde{W})$$

and

$$S\circ\left(\{\tau_i(u_i)\}_{i=1}^{r}\right)\circ S^{-1}=\tau(u)\in\mathrm{End}^0(W).$$

Remark 3.3. (i) The rings O_i do not have to have the identity elements.

(ii) The abelian subvarieties W_i do not depend on the choice of N.

Proof of Theorem 3.2. Proof of (i). Since $\mathrm{End}(W)$ is a free $\mathbb{Z}$-module of finite rank and τ is a ring embedding, O_i is also a free $\mathbb{Z}$-module of finite rank that generates the finite-dimensional $\mathbb{Q}$-vector space D_i. This implies that $O_i\otimes\mathbb{Q}\to D_i$ is an isomorphism, which proves (a).

Clearly,

$$\sum_{i=1}^{r}e_i=1_D,\ e_i^2=e_i\ \text{ for every } i,\text{ and } e_ie_j=0\ \text{ if } i\neq j.$$

This implies that

$$\tau(Ne_i)^2=N\cdot\tau(Ne_i),\ \sum_{i=1}^{r}\tau(Ne_i)=N\cdot 1_W=N_W, \tag{3.6}$$
$$\tau(Ne_i)\tau(Ne_j)=0_W\ \text{ if } i\neq j.$$

Let

$$i,j\in\{1,\dots,r\},\ w_i\in W_i,w_j\in W_j.$$

Then there exist

$$\widetilde{w}_i,\widetilde{w}_j\in W\text{ such that } w_i=\tau(Ne_i)(\widetilde{w}_i),w_j=\tau(Ne_j)(\widetilde{w}_j).$$

This implies that

$$\tau(Ne_i)(w_i)=\tau(Ne_i)^2(\widetilde{w}_i)=N\tau(Ne_i)(\widetilde{w}_i)=Nw_i.$$

Furthermore, if $i \neq j$, then

$$\tau(Ne_i)(w_j) = \tau(Ne_i)\tau(Ne_j)(\widetilde{w}_j) = 0 \in W$$

in light of (3.6). This proves (b).

Proof of (ii). Recall that for each $w \in W$

$$\tau(Ne_i)(w) \in W_i \text{ where } i \in \{1, \ldots, r\}.$$

This implies that

$$S \circ P(w) = S(\tau(Ne_1)(w), \tau(Ne_2)(w), \ldots, \tau(Ne_r)(w)) = \sum_{i=1}^{r} \tau(Ne_i)(w) =$$

$$\tau(N \cdot 1_D)(w) = \tau(N(\sum_{i=1}^{r} e_i))w = Nw.$$

This proves that

$$S \circ P = N_W. \tag{3.7}$$

Furthermore, let $w_i \in W_i$ for every $i \in \{1, \ldots, r\}$. Thanks to (3.6),

$$P \circ S(w_1, w_2, \ldots, w_r) = P\left(\sum_{i=1}^{r} w_i\right) =$$

$$\left(\sum_{i=1}^{r} \tau(Ne_1)(w_i), \sum_{i=1}^{r} \tau(Ne_2)(w_i), \ldots, \sum_{i=1}^{r} \tau(Ne_r)(w_i)\right) =$$

$$(\tau(Nu_1)(w_1), \tau(Nu_2)(w_2), \ldots, \tau(Nu_r)(w_r)) =$$

$$(Nw_1, Nw_2, \ldots, Nw_r) = N \cdot (w_1, w_2, \ldots, w_r).$$

This proves that

$$P \circ S = N_{\widetilde{W}}. \tag{3.8}$$

Combining (3.7) and (3.8), we obtain that both S and P are isogenies. This proves (ii).

Proof of (iii). Let $u_i \in O_i \subset D_i$. Then

$$u_i = e_i u_i = e_i u_i e_i.$$

This implies that

$$\tau(Nu_i) = N\tau(u_i) = \tau(Ne_i)\tau(u_i) \in \mathrm{End}(W)$$

and therefore

$$\tau(Nu_i)(W) = \tau(Ne_i)\tau(u_i)(W) \subset \tau(Ne_i)(W) = W_i,$$

i.e.,

$$N\tau(u_i)(W) \subset W_i.$$

Clearly, $\tau(u_i)(W)$ is an abelian subvariety of W and therefore coincides with $N\tau(u_i)(W)$. This implies that

$$\tau(u_i)(W) = N\tau(u_i)(W) \subset W_i.$$

In particular,

$$\tau(u_i)(W) \subset W_i \text{ for every } i.$$

Furthermore, if $i \neq j$, then

$$0 = u_i e_j, 0_W = \tau(Nu_i e_j) = \tau(u_i)\tau(Ne_j)$$

and therefore

$$\tau(Nu_i)(W_j) = \{0\}.$$

Again, $\tau(u_i)(W_j)$ is an abelian subvariety of W and therefore coincides with

$$N\tau(u_i)(W_j) = \tau(Nu_i)(W_j) = \{0\}.$$

Hence, $\tau(u_i)(W_j) = \{0\}$. This ends the proof of (3.5) and (iii).

Proof of (iv). Now (3.5) allows us to define the ring homomorphisms

$$\tau_i : O_i \to \mathrm{End}(W_i),\ u_i \mapsto \{w_i \mapsto \tau(u_i)(w_i) \in W_i \text{ for any } w_i \in W_i\} \text{ for any } u_i \in O_i.$$

It follows from the previously proved property (i) that τ_i extend to $\mathbb{Q}$-algebra homomorphisms

$$D_i = O_i \otimes \mathbb{Q} \to \mathrm{End}(W_i) \otimes \mathbb{Q} = \mathrm{End}^0(W_i),$$

which we continue to denote by τ_i. Also, it follows from (i) that $\tau_i(Ne_i) = N_{W_i}$ and therefore

$$\tau_i(e_i) = \frac{1}{N}\tau_i(Ne_i) = \frac{1}{N}N_{W_i} = 1_{W_i}.$$

This proves (c). Property (d) follows from the very definition of τ_i. Let us prove that

$$\tau_i : D_i \to \mathrm{End}^0(W_i)$$

is an *embedding*. Suppose that $u_i \in D_i$ satisfies $\tau_i(u_i) = 0$. Replacing u_i by mu_i for sufficiently divisible positive integer m, we may and will assume that $u_i \in O_i$. Then

$$\{0\} = \tau_i(u_i)(W_i) = \tau(u_i)(W_i).$$

Furthermore, if $i \neq j$, then $\tau(u_i)(W_j) = 0$. It follows that $\tau(u_i)$ annihilates

$$W_i + \sum_{j\neq i} W_j = \sum_{j=1}^{r} W_j = W,$$

because the *isogeny* S is *surjective*. This implies that $\tau(u_i) = 0_W$. Since τ is injective, $u_i = 0$, i.e., τ_i is an embedding.

Let us prove (e). Replacing

$$u = (u_1, \ldots, u_i, \ldots, u_r) = \sum_{i=1}^{r} u_i \in \bigoplus_{i=1}^{r} D_i = D$$

by $mu = (mu_1, \ldots mu_i, \ldots, mu_r)$ for sufficiently divisible positive integer m, we may and will assume that all $u_i \in O_i$. Let us check that in $\mathrm{Hom}(\prod_{i=1}^{r} W_i, W) = \mathrm{Hom}(\widetilde{W}, W)$ we have

$$S \circ (\tau_1(u_1), \ldots \tau_i(u_i), \ldots \tau_r(u_r)) = \tau(u) \circ S. \tag{3.9}$$

So, let $(w_1, \ldots w_i, \ldots, w_r) \in \prod_{i=1}^{r} W_i$. Then

$$(\tau_1(u_1), \ldots \tau_i(u_i), \ldots, \tau_r(u_r))(w_1, \ldots w_i, \ldots, w_r) =$$
$$(\tau_1(u_1)(w_1), \ldots \tau_i(u_i)(w_i), \ldots, \tau_r(u_r)(w_r)) \in \prod_{i=1}^{r} W_i,$$

$$S \circ ((\tau_1(u_1), \ldots, \tau_i(u_i), \ldots, \tau_r(u_r))(w_1, \ldots w_i, \ldots w_r)) =$$
$$S(\tau(u_1)(w_1), \ldots, \tau(u_i)(w_i), \ldots, \tau(u_r)(w_r)) = \sum_{i=1}^{r} \tau(u_i)(w_i).$$

Furthermore, $S(w_1, \ldots, w_i, \ldots, w_r) = \sum_{i=1}^{r} w_i$; in addition, thanks to (iii),

$$\tau(u_i)(w_j) = 0 \text{ if } i \neq j.$$

This implies that

$$\tau(u) \circ S(w_1, \ldots, w_i, \ldots, w_r) = \tau(u)\left(\sum_{i=1}^{r} w_i\right) = \left(\sum_{i=1}^{r} \tau(u_i)\right)\left(\sum_{j=1}^{r} w_j\right) =$$
$$\sum_{i=1}^{r} \tau(u_i)(w_i) = S \circ (\tau_1(u_1)(w_1), \ldots, \tau_i(u_i)(w_i), \ldots, \tau_r(u_r)(w_r)).$$

This proves (3.9). Multiplying both sides of (3.9) by S^{-1} from the right, we get the desired equality

$$S\circ(\tau_1(u_1),\dots\tau_i(u_i),\dots,\tau_r(u_r))\circ S^{-1}=\tau(u)$$

in $\mathrm{End}^0(W)$. □

Proof of Theorem 2.2. We write $e_{ij}\in \mathrm{Mat}_m(E)$ for the matrix, whose only nonzero entry is 1 at the intersection of ith row and jth column, $i,j\in\{1,\dots,m\}$. We have

$$e_{ii}^2=e_{ii},\ \sum_{i=1}^m e_{ii}=\mathrm{Id}_m,\ e_{ii}e_{jj}=0\ \text{ if } i\neq j.$$

In addition, if $i\neq j$, then the monomial matrix

$$s_{ij}=s_{ji}\in \mathrm{GL}(m,\mathbb{Q})\subset \mathrm{Mat}_m(E)$$

attached to the *transposition* $(i\,j)$ satisfies

$$s_{ij}=\mathrm{Id}_m-(e_{ii}+e_{jj})+(e_{ij}+e_{ji})\in \mathrm{GL}(m,\mathbb{Q}),\ s_{ij}^2=\mathrm{Id}_m,$$

$$s_{ij}e_{ii}s_{ij}^{-1}=e_{jj}. \tag{3.10}$$

There is a positive integer N such that

$$N\widetilde{\kappa}(e_{ij})\in \mathrm{End}(Z)\ \text{ for all } i,j=1,\dots m.$$

Let us consider the nonzero abelian subvarieties

$$Z_i:=\widetilde{\kappa}(Ne_{ii})(Z)\subset Z.$$

It follows from (3.10) combined with Lemma 3.1 that there are isogenies of abelian varieties

$$P_{ij}:=\widetilde{\kappa}(Ns_{ij})\big|_{Z_i}: Z_i\to Z_j,\ z_i\mapsto \widetilde{\kappa}(Ns_{ij})(z_i),$$

Since

$$s_{ij}^2=\mathrm{Id}_m,\ \widetilde{\kappa}(s_{ij})^2=1_Z,$$

we get

$$P_{ji}\circ P_{ij}=N^2_{Z_i}.$$

They give rise to the product-isogenies

$$\mathbf{P}:=\prod_{i=1}^m P_{1i}: Z_1^m\to\prod_{i=1}^m Z_i,\ \mu:=\prod_{i=1}^m P_{i1}:\prod_{i=1}^m Z_i\to Z_1^m$$

such that

$$\mu\circ\mathbf{P}=N^2_{Z_1^m},\ \mathbf{P}\circ\mu=N^2_{\widetilde{Z}}\ \text{ where } \widetilde{Z}:=\prod_{i=1}^m Z_i.$$

Applying Theorem 3.2 to the subalgebra of diagonal matrices

$$D=\bigoplus_{i=1}^m E\cdot e_{ii}\subset \mathrm{Mat}_m(E),$$

$$r=m,\ D_i=E\cdot e_{ii},\ e_i:=e_{ii}$$

and

$$W:=Z,\ \tau: D\hookrightarrow \mathrm{End}^0(Z),\ u\mapsto\widetilde{\kappa}(u),$$

we obtain that the morphism of abelian varieties

$$S:\widetilde{Z}=\prod_{i=1}^m Z_i\to Z,\ \{z_i\}_{i=1}^m\mapsto\sum_{i=1}^r z_i \tag{3.11}$$

is an isogeny. In addition, we get the $\mathbb{Q}$-algebra embeddings

$$\tau_i: E\cdot e_{ii}=D_i\hookrightarrow \mathrm{End}^0(Z_i)$$

that send e_{ii} to 1_{Z_i} and such that for every collection $u_i \in D_i$ $(1 \le i \le m)$

$$\sum_{i=1}^{m} \tau_i(u_i) \in \bigoplus_{i=1}^{m} \mathrm{End}^0(Z_i) \subset \mathrm{End}^0\left(\prod_{i=1}^{m} Z_i\right) = \mathrm{End}^0(\widetilde{Z}),$$

$$S \circ \left(\sum_{i=1}^{m} \tau_i(u_i)\right) \circ S^{-1} = \widetilde{\kappa}\left(\sum_{i=1}^{m} u_i\right) \in \mathrm{End}^0(Z).$$

This implies that

$$S^{-1} \circ \widetilde{\kappa}\left(\sum_{i=1}^{m} u_i\right) \circ S = \sum_{i=1}^{m} \tau_i(u_i) \in \bigoplus_{i=1}^{m} \mathrm{End}^0(Z_i) \subset \mathrm{End}^0\left(\prod_{i=1}^{m} Z_i\right).$$

In particular, for each $j \in \{1, \dots, m\}$

$$S^{-1} \circ \widetilde{\kappa}(e_{jj}) \circ S = \tau_j(e_{jj}) = 1_{Z_j} \in \mathrm{End}^0(Z_j) \subset \bigoplus_{i=1}^{m} \mathrm{End}^0(Z_i) \subset \mathrm{End}^0\left(\prod_{i=1}^{m} Z_i\right).$$

Let us write

$$X := Z_1, \quad \psi := \mathbf{P} \circ S : X^m = Z_1^m \to \prod_{i=1}^{m} Z_i \to Z.$$

In order to define κ, let us consider

$$O := \{u \in E \mid \widetilde{\kappa}(u) \in \mathrm{End}(Z)\}.$$

Clearly, O is an order in E and the natural $\mathbb{Q}$-algebra homomorphism

$$O \otimes \mathbb{Q} \to E, \ u \otimes a \mapsto au$$

is an isomorphism. In addition, for each nonzero $u \in O$ the selfmap of Z

$$\widetilde{\kappa}(u) : Z \to Z$$

is an isogeny. Since E is the center of $\mathrm{Mat}_m(E)$, every $u \in O$ commutes with all e_{ij} and s_{ij}. In particular, for all $u \in O$

$$\widetilde{\kappa}(u)(Z_i) = \widetilde{\kappa}(u)\widetilde{\kappa}(Ne_{ii})(Z) = \widetilde{\kappa}(uNe_{ii})(Z) = \widetilde{\kappa}(Ne_{ii}u)(Z) \subset \widetilde{\kappa}(Ne_{ii})(Z) = Z_i$$

and the diagrams

$$\begin{array}{ccc} Z_1 & \xrightarrow{\tau_1(u)} & Z_1 \\ {\scriptstyle P_{1i}}\downarrow & & \downarrow{\scriptstyle P_{1i}} \\ Z_i & \xrightarrow{\tau_i(u)} & Z_i \end{array}, \qquad \begin{array}{ccc} Z_i & \xrightarrow{\tau_i(u)} & Z_i \\ {\scriptstyle P_{i1}}\downarrow & & \downarrow{\scriptstyle P_{i1}} \\ Z_1 & \xrightarrow{\tau_1(u)} & Z_1 \end{array} \tag{3.12}$$

are commutative. This gives rise to the ring homomorphisms

$$\tau_i : O \to \mathrm{End}(Z_i), \ u \mapsto \{z_i \mapsto \widetilde{\kappa}(u)(z_i) \text{ for all } z_i \in Z_i\} \text{ for all } u \in O,$$

which are obviously injective, and extend them by $\mathbb{Q}$-linearity to the injective $\mathbb{Q}$-algebra homomorphisms $E \to \mathrm{End}^0(Z_i)$, which we continue to denote by τ_i. Let us write

$$\kappa := \tau_1 : E \hookrightarrow \mathrm{End}^0(X = Z_1).$$

□

4. Linear Algebra

Definition 4.1. Let k be a field and $\mathscr{C}$ be a finite-dimensional k-algebra with identity element $1_{\mathscr{C}}$. We say that $\mathscr{C}$ is splittable over k if it is isomorphic to a direct sum of matrix algebras over fields that are finite algebraic separable extensions of k.

Examples 4.2.
(i) If $\mathscr{C}$ is a field that is a finite algebraic separable extension of k, then it is splittable over k.
(ii) If $\mathscr{C}_1$ and $\mathscr{C}_2$ are splittable over k, then their direct sum $\mathscr{C}_1 \bigoplus \mathscr{C}_2$ is also splittable over k.
(iii) If $\mathscr{C}$ is splittable over k, then for all positive integers d the matrix algebra $\mathrm{Mat}_d(\mathscr{C})$ is also splittable over k.
(iv) Let L/k be a finite algebraic separable field extension of k. If $\mathscr{C}$ is splittable over k then
$$\mathscr{C}_L = \mathscr{C} \otimes_k L$$
is splittable over k and over L.
(v) Suppose that E is an overfield of k and $\mathscr{C}$ is a finite-dimensional splittable E-algebra. If E/k is a finite separable field extension, then $\mathscr{C}$ is splittable over k as well.

Clearly, Theorem 2.4 is a special case of the following assertion.

Theorem 4.3. *Let k be a field of characteristic zero, $\mathscr{A}$ a nonzero semisimple finite-dimensional k-algebra with identity element $1_{\mathscr{A}}$, and f an element of $\mathscr{A}$. Then there exists a k-subalgebra $\mathscr{C}$ of $\mathscr{A}$ that contains $1_{\mathscr{A}}$ and f, and is splittable over k.*

We will need the following lemma that will be proven at the end of this section.

Lemma 4.4. *Let $\mathscr{A}$ be a nonzero finite-dimensional algebra over a field k with identity element $1_{\mathscr{A}}$. Let $\mathcal{V}$ be a nonzero finite-dimensional k-vector space that is a faithful semisimple $\mathscr{A}$-module. Assume additionally that every simple $\mathscr{A}$-submodule M of $\mathcal{V}$ is absolutely simple, i.e., the centralizer $\mathrm{End}_{\mathscr{A}}(M)$ of $\mathscr{A}$ in $\mathrm{End}_k(M)$ coincides with $k \cdot 1_M$ where $1_M : M \to M$ is the identity map.*

Then $\mathscr{A}$ is isomorphic to a direct sum of matrix algebras over k.

Proof of Theorem 4.3. Induction by $\dim_k(\mathscr{A})$.

Step 0. If $\dim_k(\mathscr{A}) = 1$, then $\mathscr{A} = k \cdot 1_{\mathscr{A}} \cong k$ is obviously splittable over k.

Now assume that $d := \dim_k(\mathscr{A}) > 1$ and the assertion of Theorem 4.3 holds true for all semisimple algebras of dimension $< d$ over any field of characteristic 0.

Step 1. Suppose that the k-algebra $\mathscr{A}$ is not simple, i.e., it splits into a direct sum
$$\mathscr{A} = \mathscr{A}_1 \bigoplus \mathscr{A}_2$$
of two nonzero semisimple k-algebras $\mathscr{A}_1$ and $\mathscr{A}_2$. Clearly, both $\dim_k(\mathscr{A}_1)$ and $\dim_k(\mathscr{A}_2)$ are strictly less than d. There are elements
$$f_1 \in \mathscr{A}_1,\ f_2 \in \mathscr{A}_2$$
such that $f = f_1 + f_2$. Applying the induction assumption to both $(\mathscr{A}_1, f_1)$ and $(\mathscr{A}_2, f_2)$, we obtain that there are splittable over k subalgebras
$$\mathscr{C}_1 \subset \mathscr{A}_1,\ \mathscr{C}_2 \subset \mathscr{A}_2$$
such that
$$1_{\mathscr{A}_1}, f_1 \in \mathscr{C}_1,\ 1_{\mathscr{A}_2}, f_2 \in \mathscr{C}_2.$$
Now the direct sum
$$\mathscr{C} = \mathscr{C}_1 \bigoplus \mathscr{C}_2 \subset \mathscr{A}_1 \bigoplus \mathscr{A}_2 = \mathscr{A}$$

is splittable over k and contains $1_{\mathscr{A}_1} + 1_{\mathscr{A}_2} = 1_{\mathscr{A}}$ and $f_1 + f_2 = f$.

So, in the course of the proof, we may and will assume that $\mathscr{A}$ is a simple k-algebra.

Step 2. Let E be the center of the simple k-algebra $\mathscr{A}$. Then E is a field that is a finite algebraic extension of k. Clearly, $\mathscr{A}$ carries the natural structure of central simple E-algebra. If $E \ne k$, then

$$\dim_E(\mathscr{A}) < \dim_k(\mathscr{A})$$

and the induction assumption implies that there is a splittable over E subalgebra $\mathscr{C} \subset \mathscr{A}$ that contains both $1_{\mathscr{A}}$ and f. Since E/k is finite algebraic, $\mathscr{C}$ is splittable over k as well.

So, in the course of the proof, we may and will assume that $E = k$, i.e., $\mathscr{A}$ is a central simple k-algebra.

Step 3. So, $\mathscr{A}$ is a *central simple* k-algebra of finite k-dimension $d > 1$. Recall that $d = m^2$ where $m > 1$ is an integer. Then $\mathscr{A}$ carries the natural structure of an m^2-dimensional k-Lie algebra with brackets

$$[u, v] := uv - vu \text{ for } u, v \in \mathscr{A}.$$

The center of the k-Lie algebra $\mathscr{A}$ coincides with $k \cdot 1_{\mathscr{A}}$. Let us consider the k-linear *reduced trace map* (see [7])

$$\mathrm{tr}_{\mathscr{A}} : \mathscr{A} \to k.$$

Recall (see [7]) that

$$\mathrm{tr}_{\mathscr{A}}(uv) = \mathrm{tr}_{\mathscr{A}}(vu) \text{ for } u, v \in \mathscr{A}; \mathrm{tr}_{\mathscr{A}}(\alpha) = m\alpha \text{ for } \alpha \in k = k \cdot 1_{\mathscr{A}}.$$

This implies that

$$\mathrm{tr}_{\mathscr{A}}([u, v]) = \mathrm{tr}_{\mathscr{A}}(uv) - \mathrm{tr}_{\mathscr{A}}(vu) = 0,$$

and therefore one may view $\mathrm{tr}_{\mathscr{A}}$ as a homomorphism of k-Lie algebras (here k is viewed as the Lie algebra with zero brackets operation). It follows that the k-Lie algebra $\mathscr{A}$ splits into a direct sum

$$\mathscr{A} = k \cdot 1_{\mathscr{A}} \bigoplus \mathrm{sl}(\mathscr{A})$$

of its center $k \cdot 1_{\mathscr{A}}$ and the nonzero $(m^2 - 1)$-dimensional k-Lie algebra $\mathrm{sl}(\mathscr{A}) := \ker(\mathrm{tr}_{\mathscr{A}})$; in addition, $\mathrm{sl}(\mathscr{A})$ contains the derived k-Lie subalgebra $[\mathscr{A}, \mathscr{A}]$ of $\mathscr{A}$. It is known that $[\mathscr{A}, \mathscr{A}]$ is an absolutely simple k-Lie algebra of type A_{m-1} over k, (see [4, Ch. X, Sect. 3]). This implies that

$$\dim_k([\mathscr{A}, \mathscr{A}]) = m^2 - 1 = \dim_k(\mathrm{sl}(\mathscr{A})).$$

Since $[\mathscr{A}, \mathscr{A}] \subset \mathrm{sl}(\mathscr{A})$, we have $[\mathscr{A}, \mathscr{A}] = \mathrm{sl}(\mathscr{A})$, and therefore

$$\mathscr{A} = k \cdot 1_{\mathscr{A}} \bigoplus \mathrm{sl}(\mathscr{A}) = k \cdot 1_{\mathscr{A}} \bigoplus [\mathscr{A}, \mathscr{A}]$$

is a reductive k-Lie algebra, whose center is $k \cdot 1_{\mathscr{A}}$ and the semisimple part is $\mathrm{sl}(\mathscr{A})$.

Since $\mathrm{char}(k) = 0$,

$$\mathrm{tr}_{\mathscr{A}}(1) = m \ne 0 \text{ in } k.$$

Replacing f by $f - \frac{\mathrm{tr}_{\mathscr{A}}(f)}{m} 1_{\mathscr{A}}$, we may and will assume that f lies in the (semi)simple Lie algebra $\mathrm{sl}(\mathscr{A})$.

Step 4. Since f is an element of the semisimple k-Lie algebra $\mathrm{sl}(\mathscr{A})$, it can be presented as the sum

$$f = f_s + f_n$$

of commuting semisimple f_s and nilpotent f_n, (see [1, Sect. 6, n 3, Th. 3]). Let us consider the natural faithful representation of $\mathrm{sl}(\mathscr{A})$ in the finite-dimensional k-vector space $\mathscr{A}$

$$\mathrm{sl}(\mathscr{A}) \to \mathrm{End}_k(\mathscr{A}),\ u \mapsto \{z \mapsto uz\} \text{ for all } z \in \mathscr{A} \text{ and for all } u \in \mathrm{sl}(\mathscr{A}).$$

Then $f_s \in \mathrm{sl}(\mathscr{A})$ acts on $\mathscr{A}$ as a semisimple operator with zero trace and $f_n \in \mathrm{sl}(\mathscr{A})$ acts on $\mathscr{A}$ as a nilpotent operator.

Step 5. Suppose that $f_s \neq 0$. Then the subalgebra $k[f_s]$ of $\mathscr{A}$ generated by f_s and $1_{\mathscr{A}}$ is a semisimple commutative k-subalgebra that contains $k\cdot 1_{\mathscr{A}}$ as a proper k-subalgebra. The centralizer $\mathcal{Z}_{f_s}$ of semisimple $k[f_s]$ in semisimple $\mathscr{A}$ is a *semisimple* k-subalgebra ([3, Th. 4.3.2], [10, Th. 4.1]) that contains both f_s and f_n and therefore contains $f_s + f_n = f$. Clearly, $\mathcal{Z}_{f_s}$ does not coincide with the whole $\mathscr{A}$, since f_s does not belong to the center $k\cdot 1_{\mathscr{A}}$. This implies that

$$\dim_k(\mathcal{Z}_{f_s}) < \dim_k(\mathscr{A}) = d.$$

The induction assumption applied to $\mathcal{Z}_{f_s}$ proves the desired assertion. So, we may and will assume that $f_s = 0$, i.e., $f = f_n$ is a nonzero *nilpotent* element.

Step 6. So, f is a nonzero nilpotent element. By Jacobson-Morozov theorem [2, Ch. 8, Sect. 11, Prop. 2], there is a Lie k-subalgebra $\mathfrak{g}$ of $\mathrm{sl}(\mathscr{A})$ that contains f and is isomorphic to $\mathrm{sl}(2,k)$. Let $\mathscr{C} \subset \mathscr{A}$ be the associative k-subalgebra of $\mathscr{A}$ generated by $\mathfrak{g}$ and $1_{\mathscr{A}}$. Clearly,

$$f \in \mathfrak{g} \subset \mathscr{C} \subset \mathscr{A}.$$

Let us consider the natural faithful action of $\mathscr{C}$ on the k-vector space $\mathcal{V} := \mathscr{A}$ induced by multiplication in $\mathscr{A}$. Clearly, a k-vector subspace $\mathcal{W}$ of $\mathcal{V}$ is a $\mathscr{C}$-submodule (resp. a simple $\mathscr{C}$-submodule) if and only if it is a $\mathfrak{g}$-submodule (resp. a simple $\mathfrak{g}$-submodule). In addition, if $\mathcal{W}$ is a $\mathscr{C}$-submodule, then the centralizer

$$\mathrm{End}_{\mathscr{C}}(\mathcal{W}) = \mathrm{End}_{\mathfrak{g}}(\mathcal{W}).$$

Recall [2, Ch. VII, Sect. 1, Prop. 3 and Th. 1] that every $\mathrm{sl}(2,k)$-module of finite k-dimension is semisimple; in addition, if $\mathcal{W}$ is a simple $\mathrm{sl}(2,k)$-module of finite k-dimension, then it is absolutely simple, ibid. This implies that $\mathcal{V}$ is a semisimple $\mathscr{C}$-module and all of its simple submodules are absolutely simple. It follows from Lemma 4.4 that $\mathscr{C}$ is a direct sum of matrix algebras over k and therefore is splittable. This ends the proof of Theorem 4.3. □

Proof of Lemma 4.4. We may and will identify $\mathscr{A}$ with its isomorphic image in $\mathrm{End}_k(\mathcal{V})$. The semisimplicity and faithfullness of $\mathcal{V}$ combined with [5, Ch. XVII, Sect. 4, Prop. 4.7] imply that $\mathscr{A}$ is a finite-dimensional semisimple k-algebra. Let us consider the centralizer

$$\mathscr{B} := \mathrm{End}_{\mathscr{A}}(\mathcal{V}) \subset \mathrm{End}_k(\mathcal{V})$$

of $\mathscr{A}$ in $\mathrm{End}_k(\mathcal{V})$. The semisimplicity of $\mathcal{V}$ and absolute simplicity of all its simple $\mathscr{A}$-submodules combined with [5, Ch. XVII, Sect. 1, Prop. 1.2] imply that there are a positive integer s and s positive integers $d_1,\dots,d_s$ such that the k-algebra

$$\mathscr{B} \cong \bigoplus_{i=1}^{s} \mathrm{Mat}_{d_i}(k).$$

In particular, $\mathscr{B}$ is semisimple and therefore the faithful $\mathscr{B}$-module $\mathcal{V}$ is semisimple. Let

$$p_i : \bigoplus_{i=1}^{s} \mathrm{Mat}_{d_i}(k) \twoheadrightarrow \mathrm{Mat}_{d_i}(k)$$

be the (surjective) projection map to the ith summand. Recall that the coordinate k-vector space k^{d_i} endowed with the natural action of $\mathrm{Mat}_{d_i}(k)$ is the only (up to an isomorphism) simple $\mathrm{Mat}_{d_i}(k)$-module and this module is absolutely simple. Using p_i, one may endow k^{d_i} with the natural structure of $\bigoplus_{i=1}^{s}\mathrm{Mat}_{d_i}(k)$-module and this module, which we denote by M_i, is an absolutely simple $\bigoplus_{i=1}^{s}\mathrm{Mat}_{d_i}(k)$-module. Clearly, every simple $\bigoplus_{i=1}^{s}\mathrm{Mat}_{d_i}(k)$-module is isomorphic to one of M_i; in particular, each simple $\bigoplus_{i=1}^{s}\mathrm{Mat}_{d_i}(k)$-module is absolutely simple. This means that each simple $\mathscr{B}$-module is absolutely simple. Recall that the $\mathscr{B}$-module $\mathscr{V}$ is semisimple and therefore is isomorphic to a direct sum of simple $\mathscr{B}$-modules, each of which is absolutely simple. It follows from [5, Ch. XVII, Sect. 1, Prop. 1.2] that the centralizer $\mathrm{End}_{\mathscr{B}}(\mathscr{V})$ of $\mathscr{B}$ in $\mathrm{End}_k(\mathscr{V})$ is isomorphic to a direct sum of matrix algebras over k. By Jacobson's density theorem [5, Ch. XVII, Sect. 3, Th. 3.2], our $\mathscr{A}$ coincides with $\mathrm{End}_{\mathscr{B}}(\mathscr{V})$ and therefore is isomorphic to a direct sum of matrix algebras over k. This ends the proof.

□

References

[1] N. Bourbaki, *Éléments de mathématique. Fasc. XXVI. Groupes et algèbres de Lie. Chapitre I: Algèbres de Lie*, Seconde édition. Actualités Scientifiques et Industrielles, No. 1285, Hermann, Paris, 1971, 146 pages.

[2] ———, *Éléments de mathématique. Fasc. XXXVIII: Groupes et algèbres de Lie. Chapitre VII: Sous-algèbres de Cartan, éléments réguliers. Chapitre VIII: Algèbres de Lie semi-simples déployées*, Actualités Scientifiques et Industrielles, No. 1364. Hermann, Paris, 1975, 271 pages.

[3] I. N. Herstein, *Noncommutative rings*, Carus Mathematical Monographs, vol. 15, Mathematical Association of America, Washington, DC, 1994, Reprint of the 1968 original, xii+202 pages.

[4] N. Jacobson, *Lie algebras*, Dover Publications, Inc., New York, 1979, Republication of the 1962 original, ix+331 pages.

[5] S. Lang, *Algebra*, second ed., Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1984, xv+714 pages.

[6] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Oxford University Press, 1974, viii+279 pages.

[7] I. Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003, Corrected reprint of the 1975 original, xiv+395 pages.

[8] K. A. Ribet, "Galois action on division points of Abelian varieties with real multiplications", *Amer. J. Math.* **98** (1976), no. 3, p. 751-804.

[9] J. Tate, "Endomorphisms of abelian varieties over finite fields", *Invent. Math.* **2** (1966), p. 134-144.

[10] Y. G. Zarhin, "Endomorphism algebras of abelian varieties with special reference to superelliptic Jacobians", in *Geometry, algebra, number theory, and their information technology applications*, Springer Proc. Math. Stat., vol. 251, Springer, Cham, 2018 (A. Akbary S. Gun, eds.), p. 477-528.

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