Endomorphism rings of Abelian varieties and their representations

Peter Bruin
14 and 29 October 2009

1. Introduction

These are notes of two talks with the aim of giving some basic properties of the endomorphism ring of an Abelian variety A and its representations on certain linear objects associated to A. The results can be found in § 5.1 of Shimura's book [1], but presented in a completely different way.

For completeness, we state some definitions. An *Abelian variety* over a field k is a proper, smooth, connected group variety over k. A basic result from the theory of Abelian varieties is that every Abelian variety is commutative (and projective, but we will not use this.) A *homomorphism* between Abelian varieties A and B is a morphism $A \to B$ of varieties over k that is compatible with the group structure. The set $\operatorname{Hom}(A, B)$ of all homomorphisms from A to B is an Abelian group, and the group $\operatorname{End} A$ of all endomorphisms of A is a ring. An *isogeny* between Abelian varieties is a surjective homomorphism with finite kernel. An Abelian variety A is *simple* if it has exactly two Abelian subvarieties (namely 0 and A).

Fact 1.1. *If A and B are Abelian varieties over a field, then $\operatorname{Hom}(A, B)$ is finite free as an Abelian group.*

Note that $\operatorname{End} A$ can be non-commutative and can have zero divisors; for example, if A is a product of an elliptic curve with itself, then A contains the ring $\operatorname{Mat}_2(\mathbf{Z})$.

Below we will only be concerned with what $\operatorname{End} A$ looks like after tensoring with $\mathbf{Q}$. We start by introducing the right setting for this.

2. The category $\mathbf{Q} \otimes \mathcal{A}(k)$

Let $\mathcal{A}(k)$ denote the category of all Abelian varieties over k. This is an additive category: if A and B are Abelian varieties, $\operatorname{Hom}(A, B)$ has the structure of an Abelian group, composition is bilinear, and the category $\mathcal{A}(k)$ has finite direct products which also function as finite direct sums.

We let $\mathbf{Q} \otimes \mathcal{A}(k)$ denote the same category but with $\operatorname{Hom}(A, B)$ replaced by $\mathbf{Q} \otimes \operatorname{Hom}(A, B)$ for all objects A and B of $\mathcal{A}(k)$ (and extending the $\mathbf{Z}$-bilinear composition maps

$$\operatorname{Hom}(B, C) \times \operatorname{Hom}(A, B) \xrightarrow{\circ} \operatorname{Hom}(A, C)$$

to $\mathbf{Q}$-bilinear maps). The canonical functor

$$\mathcal{A}(k) \to \mathbf{Q} \otimes \mathcal{A}(k)$$

is sometimes denoted by

$$A \mapsto \mathbf{Q} \otimes A;$$

we will use the empty notation for it and instead keep writing $\mathbf{Q} \otimes \operatorname{End}$ for endomorphism rings in $\mathbf{Q} \otimes \mathcal{A}(k)$. This is the "universal functor of $\mathcal{A}(k)$ into a $\mathbf{Q}$-linear category." It has the effect of making all isogenies into isomorphisms.

Fact 2.1. *The category $\mathbf{Q} \otimes \mathcal{A}(k)$ is a semi-simple Abelian category. In other words, morphisms have kernels and cokernels satisfying certain properties, and every Abelian variety is isogenous to a direct product (or direct sum, which is the same) of simple Abelian varieties.*

3. Linear objects associated to an Abelian variety

We start with the case of Abelian varieties over the complex numbers. In this case we may view an Abelian variety A as a compact complex Lie group, and we have

$$\begin{aligned} \mathrm{T}_0 A &= \text{tangent space at the identity element} \\ \mathrm{T}_0^* A &= \text{cotangent space at the identity element} \\ \mathrm{H}_1(A, \mathbf{Z}) &= \text{first homology group} \\ \mathrm{H}^1(A, \mathbf{Z}) &= \text{first cohomology group} \end{aligned}$$

The $\mathbf{C}$-vector spaces $\mathrm{T}_0 A$ and $\mathrm{T}_0^* A$ have $\mathbf{C}$-dimension equal to $\dim A$, whereas $\mathrm{H}_1(A, \mathbf{Z})$ and $\mathrm{H}^1(A, \mathbf{Z})$ are free Abelian groups of rank equal to $2 \dim A$. In fact, $\mathrm{H}_1(A, \mathbf{Z})$ can be identified with a lattice in $\mathrm{T}_0 A$, namely the kernel of the *exponential map*, which is a canonical surjective homomorphism

$$\exp\colon \mathrm{T}_0 A \to A$$

of complex Lie groups. Instead of

$$\mathrm{H}_1(\ \ , \mathbf{Z})\colon \mathcal{A}(\mathbf{C}) \to \{\text{finite free Abelian groups}\}$$

we can also take homology with rational coefficients to obtain a functor

$$\mathrm{H}_1(\ \ , \mathbf{Q})\colon \mathcal{A}(\mathbf{C}) \to \{\text{finite-dimensional } \mathbf{Q}\text{-vector spaces}\}.$$

This functor extends uniquely to a $\mathbf{Q}$-linear functor

$$\mathrm{H}_1(\ \ , \mathbf{Q})\colon \mathbf{Q} \otimes \mathcal{A}(\mathbf{C}) \to \{\text{finite-dimensional } \mathbf{Q}\text{-vector spaces}\}.$$

For an Abelian variety A over an arbitrary base field k, the tangent space $\mathrm{T}_0 A$ and the cotangent space $\mathrm{T}_0^* A$ are still defined; they are k-vector spaces of dimension equal to the dimension of k. However, the classical (co)homology groups $\mathrm{H}_1(A, \mathbf{Z})$ and $\mathrm{H}^1(A, \mathbf{Z})$ are no longer defined. As an analogue of the cohomology group, we can take *l-adic étale cohomology* (for l a prime number not divisible by the characteristic of k); we will not go into this. A suitable analogue of the homology group is the *Tate module*

$$\mathrm{T}_l A = \varprojlim_n A[l^n](\bar{k})$$

where $\bar{k}$ is some fixed algebraic closure of k and the projective limit is taken with respect to the maps

$$l\colon A[l^{n+1}](\bar{k}) \to A[l^n](\bar{k}).$$

If k has characteristic zero, then the functor T_0 extends uniquely to a $\mathbf{Q}$-linear functor

$$\mathrm{T}_0\colon \mathbf{Q} \otimes \mathcal{A}(k) \to \{\text{finite-dimensional } k\text{-vector spaces}\}.$$

In particular, this extended functor T_0 gives ring homomorphisms

$$\mathbf{Q} \otimes \operatorname{End} A \to \operatorname{End}_k \mathrm{T}_0 A.$$

For an arbitrary base field k and for any prime number l not divisible by the characteristic of k, we compose the functor

$$\mathrm{T}_l\colon \mathcal{A}(k) \to \{\text{finite free } \mathbf{Z}_l\text{-modules}\}$$

with the canonical functor

$$\begin{aligned} \{\text{finite free } \mathbf{Z}_l\text{-modules}\} &\to \{\text{finite-dimensional } \mathbf{Q}_l\text{-vector spaces}\} \\ M &\mapsto \mathbf{Q}_l \otimes_{\mathbf{Z}_l} M = \mathbf{Q} \otimes_{\mathbf{Z}} M. \end{aligned}$$

The result factors via $\mathbf{Q} \otimes \mathcal{A}(k)$ by the universal property of the latter category; therefore we obtain a functor

$$\mathrm{V}_l\colon \mathbf{Q} \otimes \mathcal{A}(k) \to \{\text{finite-dimensional } \mathbf{Q}_l\text{-vector spaces}\}.$$

More concretely, for any Abelian variety A over k, the ring homomorphism

$$\mathrm{T}_l\colon \operatorname{End} A \to \operatorname{End}_{\mathbf{Z}_l} \mathrm{T}_l A$$

given by functoriality of T_l can be extended to a $\mathbf{Q}$-algebra homomorphism

$$\mathrm{V}_l\colon \mathbf{Q} \otimes \operatorname{End} A \to \operatorname{End}_{\mathbf{Q}_l} \mathrm{V}_l A.$$

For $a \in \mathbf{Q} \otimes \operatorname{End} A$, let $\chi(a)$ denote the characteristic polynomial of the endomorphism $\mathrm{V}_l a$ of $\mathrm{V}_l A$. It is known that this is a polynomial with coefficients in $\mathbf{Z}$ that does not depend on the choice of l.

4. Some algebra

Let K be a field. An *algebra* over K is a ring R with a homomorphism from K into the centre $\mathrm{Z}(R)$ of R; for the purpose of this talk, we will require all algebras to be finite-dimensional over K. A K-algebra is *simple* if it has exactly two two-sided ideals, and *semi-simple* if it is a product of simple K-algebras. A K-algebra R is *central* if the ring homomorphism $K \to \mathrm{Z}(R)$ is an isomorphism.

Example. If n is a positive integer, $\mathrm{Mat}_n(K)$ is a central simple K-algebra for any field K. The division algebra of Hamilton quaternions is a central simple algebra over the real numbers. If R is a simple algebra over K, then $\mathrm{Z}(R)$ is an extension field of K (it is a finite K-algebra that is a domain, since a zero divisor would generate a non-trivial two-sided ideal of R), so R is a central simple algebra over $\mathrm{Z}(R)$.

Fact 4.1. *If R is a central simple K-algebra and L is an extension field of K, then $L \otimes_K R$ is a central simple L-algebra.*

Corollary 4.2. *If R is a semi-simple K-algebra and L is a separable extension of K, then $L \otimes_K R$ is a semi-simple L-algebra.*

Proof. It suffices to prove the claim for in the case where R is a simple K-algebra. Then R is central over $\mathrm{Z}(R)$, and
$$L \otimes_K R \cong (L \otimes_K \mathrm{Z}(R)) \otimes_{\mathrm{Z}(R)} R.$$
By assumption $L \otimes_K \mathrm{Z}(R)$ is a product of extension fields of $\mathrm{Z}(R)$. The above fact now implies that $L \otimes_K R$ is a product of central simple algebras over these fields. □

Fact 4.3. *If R is a central simple K-algebra, and K^{sep} is a separable closure of K, there exists an isomorphism*
$$\iota \colon K^{\mathrm{sep}} \otimes_K R \xrightarrow{\sim} \mathrm{Mat}_n(K^{\mathrm{sep}})$$
of K^{sep}-algebras for some positive integer n. In particular, we have
$$[R : K] = n^2.$$
The function
$$K^{\mathrm{sep}} \otimes_K R \to \{\text{monic polynomials of degree } n \text{ over } K^{\mathrm{sep}}\}$$
sending r to the characteristic polynomial of $\iota(r)$ is independent of the choice of ι and induces a function
$$\chi^{\mathrm{red}}_{R/K} \colon R \to \{\text{monic polynomials of degree } n \text{ over } K\}.$$

If R is a simple algebra over K (not necessarily central), we define
$$[R : K]^{\mathrm{red}} = [R : \mathrm{Z}(R)]^{1/2}[\mathrm{Z}(R) : R]$$
and for $r \in R$ we define
$$\chi^{\mathrm{red}}_{R/K}(r) = \mathrm{N}_{\mathrm{Z}(R)[X]/K[X]}\bigl(\chi^{\mathrm{red}}_{R/\mathrm{Z}(R)}(r)\bigr).$$
Finally, if R is any semi-simple algebra over K, with decomposition
$$R \cong R_1 \times \cdots \times R_s$$
into simple K-algebras, we write
$$[R : K]^{\mathrm{red}} = \sum_{i=1}^{s} [R_i : K]^{\mathrm{red}}$$
and for $r \in R$, with components $r_i \in R_i$, we write
$$\chi^{\mathrm{red}}_{R/K}(r) = \prod_{i=1}^{s} \chi^{\mathrm{red}}_{R_i/K}(r_i).$$
The integer $[R : K]^{\mathrm{red}}$ is called the *reduced degree* of R. For every $r \in R$, the polynomial $\chi^{\mathrm{red}}_{R/K}(r)$ is called the *reduced characteristic polynomial* of r; it is a polynomial of degree $[R : K]^{\mathrm{red}}$. If R is commutative, then $[R : K]^{\mathrm{red}}$ and $\chi^{\mathrm{red}}_{R/K}(r)$ are equal to $[R : K]$ and the usual characteristic polynomial $\chi_{R/K}$, respectively.

We will be interested in commutative semi-simple subalgebras of a semi-simple K-algebra R. The set of such subalgebras is partially ordered under inclusion, and contains maximal elements (K is an element, and every chain of commutative semi-simple subalgebras of R is stationary because R has finite dimension over K).

Fact 4.4. *Let R be a semi-simple K-algebra, and let E be a commutative semi-simple subalgebra of R. Then*

$$[E : K] \leq [R : K]^{\mathrm{red}},$$

with equality if and only if E is a maximal commutative semi-simple subalgebras of R.

Let us now look at representations of simple algebras. For our applications it will suffice to take $\mathbf{Q}$ as the base field. Let R be a simple $\mathbf{Q}$-algebra, let K be its centre, and write

$$[R : K] = n^2.$$

Consider a field F of characteristic 0 and an F-linear representation of R, i.e. an finite-dimensional F-vector space V together with a $\mathbf{Q}$-algebra homomorphism

$$R \to \operatorname{End}_F V.$$

Choose an algebraically closed field $\bar{F}$ containing F. We write

$$V_{\bar{F}} = \bar{F} \otimes_F V$$

and consider it as a $\bar{F}$-linear representation of the $\bar{F}$-algebra

$$\begin{aligned} \bar{F} \otimes_{\mathbf{Q}} R &\cong \bar{F} \otimes_{\mathbf{Q}} K \otimes_K R \\ &\cong \Big(\prod_{j: K \to \bar{F}} \bar{F} \Big) \otimes_K R \\ &\cong \prod_{j: K \to \bar{F}} (\bar{F} \underset{K}{{}_j\otimes} R) \\ &\cong \prod_{j: K \to \bar{F}} \operatorname{Mat}_n(\bar{F}). \end{aligned}$$

In the last step, we have chosen an isomorphism $\bar{F} \underset{K}{{}_j\otimes} R \xrightarrow{\sim} \operatorname{Mat}_n(\bar{F})$ for every j; this is possible by Fact 4.3.

The only finite-dimensional $\bar{F}$-linear representations of $\operatorname{Mat}_n(\bar{F})$ are finite direct sums of the standard representation $\bar{F}^n$, so that we can write

$$V_{\bar{F}} \cong \bigoplus_{j: K \to \bar{F}} (\bar{F}^n)^{m_j}.$$

From this formula we see that the characteristic polynomial of an element $r \in R$ equals

$$\chi_V(r) = \prod_{j: K \to \bar{F}} j(\chi^{\mathrm{red}}_{R/K}(r))^{m_j}$$

The coefficients of this polynomial lie in the intersection of F and the normal closure of K in $\bar{F}$ (the compositum of the images of all the j.)

We will now deduce some useful results from this discussion.

Lemma 4.5. *Let R be a semi-simple $\mathbf{Q}$-algebra, and let V be a finite-dimensional faithful representation of R over a field F of characteristic 0. Then*

$$\dim_F V \geq [R : \mathbf{Q}]^{\mathrm{red}}.$$

If equality holds, then we have

$$\chi_V(r) = \chi^{\mathrm{red}}_{R/\mathbf{Q}}(r)$$

for all $r \in R$.

Proof. It suffices to prove the lemma in the case where R is simple. Let K denote the centre of R. In the notation of the above discussion, the fact that V is faithful means that all the m_j are positive integers. This implies

$$\begin{aligned}\dim_F V &= \dim_{\bar F} V_{\bar F}\\ &= n \sum_{j:K\to\bar F} m_j\\ &\geq n[K:\mathbf{Q}]\\ &= [R:\mathbf{Q}]^{\mathrm{red}},\end{aligned}$$

with equality if and only if all m_j are equal to 1. In this case, we have

$$\begin{aligned}\chi_V(r) &= \prod_{j:K\to\bar F} j(\chi^{\mathrm{red}}_{R/K}(r))\\ &= \mathrm{N}_{K[X]/\mathbf{Q}[X]}\bigl(\chi^{\mathrm{red}}_{R/K}(r)\bigr),\end{aligned}$$

which by definition equals $\chi^{\mathrm{red}}_{R/\mathbf{Q}}(r)$. □

Lemma 4.6. *Let R be a semi-simple $\mathbf{Q}$-algebra, let V be a finite-dimensional faithful representation of R over a field F of characteristic 0, and let E be a commutative semi-simple subalgebra of R. Then*

$$[E:\mathbf{Q}] \leq [R:\mathbf{Q}]^{\mathrm{red}} \leq \dim_F V.$$

If equality holds, then

$$\chi_V(r) = \chi_{E/\mathbf{Q}}(r)$$

for all $r \in E$, and the commutant of E inside R is equal to E.

Proof. The first inequality is Fact 4.4, and the second inequality follows from Lemma 4.5. The claim about the characteristic polynomial follows from Lemma 4.5 applied to V viewed as a representation of E. To prove that the commutant of E equals E when $[E:\mathbf{Q}] = \dim_F V$, we view V as a representation of the semi-simple F-algebra $F\otimes_{\mathbf{Q}} R$. Then V is also a representation of the commutative semi-simple F-algebra $F\otimes_{\mathbf{Q}} E$. We decompose the latter algebra as a product of extension fields of F, say

$$F\otimes_{\mathbf{Q}} E \cong K_1\times\cdots\times K_d,$$

and consider the corresponding decomposition

$$V = V_1\oplus\cdots\oplus V_d$$

of V. The commutant E' of E contains E (since E is commutative) and has a decomposition

$$F\otimes_{\mathbf{Q}} E' \cong K'_1\times\cdots\times K'_d,$$

where K'_i is a K_i-algebra acting K_i-linearly on V_i for each i. Now let us assume that the inequality $[E:\mathbf{Q}] \leq \dim_F V$ is an equality. Then V_i is one-dimensional over K_i for each i, and therefore $K'_i = K_i$ for each i. This implies that $E' = E$. □

5. Endomorphism rings

Let A be an Abelian variety. There is (up to isogeny) a decomposition

$$A \sim A_1^{h_1} \times \cdots \times A_s^{h_s}$$

into simple Abelian varieties, where the A_i are pairwise non-isogenous. Since there are no non-trivial homomorphisms between non-isogenous simple Abelian varieties, the above decomposition gives an isomorphism

$$\mathbf{Q} \otimes \operatorname{End} A \cong \operatorname{Mat}_{h_1}(\mathbf{Q} \otimes \operatorname{End} A_1) \times \cdots \times \operatorname{Mat}_{h_s}(\mathbf{Q} \otimes \operatorname{End} A_s).$$

Furthermore, each $\mathbf{Q} \otimes \operatorname{End} A_i$ is a division algebra over $\mathbf{Q}$. Since for any division algebra R over $\mathbf{Q}$ and any $n \geq 1$ the ring $\operatorname{Mat}_n(R)$ is a simple $\mathbf{Q}$-algebra, we see that $\mathbf{Q} \otimes \operatorname{End} A$ is a semi-simple $\mathbf{Q}$-algebra. By Lemma 4.5 and the existence of faithful (l-adic) representations of dimension equal to $2 \dim A$, we see that

$$[\mathbf{Q} \otimes \operatorname{End} A : \mathbf{Q}]^{\mathrm{red}} \leq 2 \dim A.$$

Theorem 5.1. *Let A be an Abelian variety over a field. The following are equivalent:*

(1) $\mathbf{Q} \otimes \operatorname{End} A$ *contains a commutative semi-simple* $\mathbf{Q}$*-algebra of degree* $2 \dim A$*;*
(2) $[\mathbf{Q} \otimes \operatorname{End} A : \mathbf{Q}]^{\mathrm{red}} = 2 \dim A$*;*
(3) $\mathbf{Q} \otimes \operatorname{End} A_i$ *contains a commutative semi-simple* $\mathbf{Q}$*-algebra of degree* $2 \dim A_i$ *for each* i*;*
(4) $[\mathbf{Q} \otimes \operatorname{End} A_i : \mathbf{Q}]^{\mathrm{red}} = 2 \dim A_i$ *for each* i*.*

Proof. The equivalences (1) $\Leftrightarrow$ (2) and (3) $\Leftrightarrow$ (4) follow from Fact 4.4. The equivalence (2) $\Leftrightarrow$ (4) follows from the identities

$$\dim A = \sum_{i=1}^{s} h_i \dim A_i$$

and

$$[\mathbf{Q} \otimes \operatorname{End} A : \mathbf{Q}]^{\mathrm{red}} = \sum_{i=1}^{s} h_i [\mathbf{Q} \otimes \operatorname{End} A_i : \mathbf{Q}]^{\mathrm{red}}$$

together with the fact that $[\mathbf{Q} \otimes \operatorname{End} A_i : \mathbf{Q}]^{\mathrm{red}} \leq 2 \dim A_i$ for each i. □

Note that "commutative semi-simple $\mathbf{Q}$-algebra" is synonymous with "product of number fields". Furthermore, if the equivalent conditions of the theorem hold, then

$$\chi(r) = \chi^{\mathrm{red}}_{\mathbf{Q} \otimes \operatorname{End}(A)/\mathbf{Q}}(r) \quad \text{for all } r \in \mathbf{Q} \otimes \operatorname{End} A,$$

and if E is a commutative semi-simple subalgebra of dimension $2 \dim A$ in $\mathbf{Q} \otimes \operatorname{End} A$, then

$$\chi(r) = \chi_{E/\mathbf{Q}}(r) \quad \text{for all } r \in E.$$

We now restrict ourselves to the case where A is an Abelian variety over a field k of characteristic 0. Then A together with its endomorphisms can be defined over some finitely generated extension of $\mathbf{Q}$, which in turn can be embedded into $\mathbf{C}$. We consider the set $A(\mathbf{C})$ of complex points of A as a complex Lie group. For each of the simple factors A_i of A (over k), we then have a representation

$$\mathbf{Q} \otimes \operatorname{End} A_i \to \mathbf{Q} \otimes \operatorname{End} A_i(\mathbf{C}) \to \operatorname{End}_{\mathbf{Q}} \mathrm{H}_0(A_i(\mathbf{C}), \mathbf{Q}).$$

This makes $\mathrm{H}_0(A_i(\mathbf{C}), \mathbf{Q})$ into a vector space over the division algebra $\mathbf{Q} \otimes \operatorname{End} A_i$, and we have

$$\begin{aligned} 2 \dim A_i &= \dim_{\mathbf{Q}} \mathrm{H}_0(A_i(\mathbf{C}), \mathbf{Q}) \\ &= [\mathbf{Q} \otimes \operatorname{End} A_i : \mathbf{Q}] \dim_{\mathbf{Q} \otimes \operatorname{End} A_i} \mathrm{H}_0(A_i(\mathbf{C}), \mathbf{Q}). \end{aligned}$$

Comparing this with Theorem 5.1, we see that $\mathbf{Q} \otimes \operatorname{End} A$ contains a commutative semi-simple subalgebra of degree $2 \dim A$ if and only if for each i the inequality

$$[\mathbf{Q} \otimes \operatorname{End} A_i : \mathbf{Q}] \geq [\mathbf{Q} \otimes \operatorname{End} A_i : \mathbf{Q}]^{\mathrm{red}}$$

is an equality and if $\mathrm{H}_0(A_i(\mathbf{C}), \mathbf{Q})$ is one-dimensional over $\mathbf{Q} \otimes \operatorname{End} A_i$. This is the case if and only if $\mathbf{Q} \otimes \operatorname{End} A_i$ is a field of degree $2 \dim A_i$ over $\mathbf{Q}$. We have therefore proved the following.

Theorem 5.2. *Let A be an Abelian variety over a field of characteristic 0. The following are equivalent:*

(1) $\mathbf{Q} \otimes \operatorname{End} A$ *contains a commutative semi-simple* $\mathbf{Q}$*-algebra of degree* $2 \dim A$*;*

(2) the division algebra $\mathbf{Q} \otimes \operatorname{End} A_i$ *is a field of degree* $2 \dim A_i$ *over* $\mathbf{Q}$ *for each of the simple factors* A_i *of* A*.*

One special case is worth describing separately. Suppose A is an Abelian variety over a field of characteristic 0 such that $\mathbf{Q} \otimes \operatorname{End} A$ contains a field F of degree $2 \dim A$ over $\mathbf{Q}$. Then A is isogenous to B^h for some simple Abelian variety B and some positive integer h. The $\mathbf{Q}$-algebra $\mathbf{Q} \otimes \operatorname{End} B$ is a field K of degree $2 \dim B$ over $\mathbf{Q}$, and we have $\operatorname{End} A = \operatorname{Mat}_h(\mathbf{Q} \otimes \operatorname{End} B)$.

References

[1] Gorō Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions.* Princeton University Press, Princeton, NJ, 1998.