Structure of Endomorphism Algebras of Abelian Varieties

(Alexander Unger, Number Theory Seminar 2005, University of Sydney)

Throughout these notes, X, Y, Z will always denote abelian varieties defined over a field k and all morphisms are assumed to be defined over k as well. We make no further assumptions on the field k. However, in the last two sections we shall investigate the case when $\mathrm{char}(k) = 0$, respectively when k is a finite field, more precisely.

1. Isogenies

Definition 1. *A morphism $f : X \to Y$ of abelian varieties is called* isogeny *if it is surjective and* $\ker(f)$ *is finite. In this case we write $X \sim Y$.*

In Prop. 4 we will see that being isogenous is an equivalence relation.

We have the following nice characterisation of isogenies:

Proposition 2. *For a morphism $f : X \to Y$ of abelian varieties, the following are equivalent:*

(i) *f is an isogeny*
(ii) $\dim X = \dim Y$ *and f is surjective*
(iii) $\dim X = \dim Y$ *and* $\ker(f)$ *is finite*
(iv) *f is finite, flat and surjective.*

Proof. [Mi], Prop. 6.1 □

Here, "$\ker(f)$ is finite" means $\ker(f)(\bar{k})$ is finite or, respectively, $\ker(f)$ has finite rank as a group scheme.

Every isogeny induces an inclusion of function fields $k(Y) \hookrightarrow k(X)$ and we define the *degree of f* to be $\deg(f) = [k(X) : k(Y)]$. The degree is multiplicative and $\deg(f) = \mathrm{rank}(\ker(f))$ (rank as a group scheme).

An important example is the multiplicationby an integer $n \neq 0$:: $[n]_X : X \to X$, $x \mapsto nx$. We write $X[n] := \ker[n]_X$.

Proposition 3. *$[n]_X$ is an isogeny of degree n^{2g} ($g = \dim X$). If* $(\mathrm{char}(k), n) = 1$ *then $[n]_X$ is separable and we have $X[n](k^{sep}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.*

Proof. [MvG], Prop. 5.9, Cor. 5.11 □

Proposition 4. *Let $f : X \to Y$ be an isogeny of degree n, then there exists an isogeny $f' : Y \to X$ such that $f \circ f' = [n]_Y$ and $f' \circ f = [n]_X$.*

Proof. [MvG], Prop. 5.12 □

2. Structure of Endomorphism Algebras

Let X, Y be abelian varieties. Since Y is a commutative group variety, it followws that $\mathrm{Hom}(X, Y)$ is an abelian group. It is torsion free since $0 = nf = [n]_Y f = f[n]_X$ implies $f = 0$ because $[n]_X$ is surjective.

Put

$$\mathrm{Hom}^0(X, Y) = \mathrm{Hom}(X, Y) \otimes_{\mathbb{Z}} \mathbb{Q}$$

and

$$\mathrm{End}^0(X) = \mathrm{Hom}^0(X, X).$$

We define the *category of abelian varieties over k up to isogeny* to be the category with abelian varieties over k as objects and $\mathrm{Hom}^0(X, Y)$ as morphisms from X to Y. Note that by Prop. 4 two abelian varieties are isomorphic in this category if and only if they are isogenous. Furthermore, if $X \sim Y$ then $\mathrm{End}^0(X) \cong \mathrm{End}^0(Y)$.

We are interested in the structure of $\mathrm{End}^0(X)$ which is naturally a $\mathbb{Q}$-algebra.

First we want to find out more about the structure of an abelian variety.

Definition 5. *A* simple abelian variety *is an abelian variety that contains no proper abelian subvariety.*

Theorem 6. *Every abelian variety is isogenous to a product $X_1^{n_1} \times \cdots \times X_k^{n_k}$ where the X_i are simple abelian varieties which are pairwise non-isogenous. The n_i and the isogeny type of the X_i are uniquely determined.*

Proof. (sketch) It is sufficient to prove that whenever Y is an abelian subvariety of X, there exists an abelian subvariety Z of X such that $X \sim Y \times Z$.

Let i be the inclusion $Y \hookrightarrow X$ and let D be an ample and effective divisor on X. Then we know that

$$\varphi_D : X \to X^\vee, \quad x \mapsto [t_x^* D - D]$$

is an isogeny. Let Z be the connected component of the kernel containing 0 of the composition

$$i^\vee \circ \varphi_D : X \to X^\vee \to Y^\vee.$$

Then Z is an abelian variety and the map $f : Z \times Y \to X, (z, y) \mapsto z + y$, is an isogeny.

To see that it is injective, note, that $\ker(f) = Y \cap Z$ is contained in the kernel of $\varphi_{D_{|Y}}$ and thus finite since $D|_Y$ is ample. For surjectivity, see [Mi], Prop. 9.1.

The theorem now follows by induction after the dimension. $\square$

Corollary 7. *Let X be as above, then we have*

$$\mathrm{End}^0(X) \cong M_{n_1}(\mathrm{End}^0(X_1)) \times \cdots \times M_{n_k}(\mathrm{End}^0(X_k))$$

Proof. Note, that $\mathrm{Hom}(X_i, X_j) = 0$ for $i \neq j$. By restriction $f \in \mathrm{End}^0(X)$ maps a component X_i to $X_i^{n_i}$. The intersection of each X_i with the image of X_i is an abelian subvariety, so must be either 0 or equal to X_i since X_i is simple. Therefore the image of X_i is of the form $X_i^{m_i}$. Because X_i is simple we must have $m_i = 0$ or 1. Hence, we get the above decomposition. $\square$

Next we want to show that the dimension of $\mathrm{End}^0(X)$ as a $\mathbb{Q}$-algebra is finite.

Given $f \in \mathrm{Hom}(X, Y)$ we obtain maps $X[n](k^{\mathrm{sep}}) \to Y[n](k^{\mathrm{sep}})$ for all $n \in \mathbb{Z}$. Since f is a group homomorphism, we get a map $T_l f$ between the Tate-modules $T_l X$ and $T_l Y$.

Remark: With respect to the induced maps $[l]_X : X[l^{n+1}] \to X[l^n]$ the Tate-module is defined as

$$T_l X = \varprojlim X[l^n](k_{\mathrm{sep}}).$$

If $(l, \mathrm{char}(k)) = 1$ then $T_l X \cong \mathbb{Z}_l^{2g}$ where $g = \dim X$. In this case $T_l X$ and $T_l Y$ are naturally $\mathbb{Z}_l$-modules and $T_l f$ is $\mathbb{Z}_l$-linear.

Theorem 8. *For* $(l, \mathrm{char}(k)) = 1$ *the map*

$$\mathrm{Hom}(X, Y) \otimes \mathbb{Z}_l \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l X, T_l Y)$$

is injective. Therefore $\mathrm{Hom}(X, Y)$ *is a free abelian group of finite rank, and*

$$\mathrm{rank}_{\mathbb{Z}} \mathrm{Hom}(X, Y) \leq 4(\dim X)(\dim Y)$$

Proof. [Mu], Thm. 19.3 □

If X is a simple abelian variety, every non-zero endomorphism is an isogeny. This follows from the fact, that the image of an endomorphism f of X is an abelian subvariety, so $\mathrm{im}(f) = X$ since $f \neq 0$ and therefore, f is surjective, hence an isogeny.

However that means, that every $f \in \mathrm{End}^0(X)$ (with an inverse $\frac{1}{\deg f} f'$, where f' is as in Prop. 4) and hence, $\mathrm{End}^0(X)$ is a division algebra (i. e. a finite-dimensional skew field over $\mathbb{Q}$). It is in particular a simple $\mathbb{Q}$-algebra.

Corollary 9. *For every abelian variety* X *the endomorphism algebra* $\mathrm{End}^0(X)$ *is a semi-simple finite-dimensional* $\mathbb{Q}$*-algebra.*

Proof. By Thm. 8 $\dim_{\mathbb{Q}} \mathrm{End}^0(X) < \infty$. Now let $X \sim X_1^{n_1} \times \cdots \times X_k^{n_k}$ as in Thm. 6. Then each $\mathrm{End}^0(X_i)$ is simple. By Wedderburn's first structure theorem, a finite-dimensional k-algebra is simple if and only if it is isomorphic to a matrix ring over a skew field. Hence, the $M_n(\mathrm{End}^0(X_i))$ are simple and by Cor. 7, $\mathrm{End}^0(X)$ is semi-simple. □

From now on X shall always be a simple abelian variety, unless otherwise stated. We want to continue with the study of the center of the division algebra $\mathrm{End}^0(X)$. First we need the notion of norm and trace. For the following facts, see [Co2] and [Co3].

Let A be a finite-dimensional division algebra over a field k with center K. Let furthermore F be a field such that $k \subseteq F \subseteq A$. If F is a maximal commutative subfield of A, then $K \subseteq F$ and we have (with $n = \dim_K A$)

$$A \otimes_K F \cong M_n(F).$$

In particular,

$$[A : K] = [F : K]^2$$

and so A has quadratic degree over its center. Let λ denote the canonical map $A \to A \otimes_K F$, take an isomorphism $\mu : A \otimes_K F \to M_n(F)$ and consider the map

$$\mu \circ \lambda : A \to A \otimes_K F \to M_n(F)$$

Definition 10. *With the notation as above we define for $a \in A$ the* reduced norm

$$\mathrm{N}^0(a) = \det(\mu\lambda(a))$$

and the reduced trace

$$\mathrm{tr}^0(a) = \mathrm{tr}(\mu\lambda(a))$$

First we have to show that this is well-defined:

- Let μ' be another isomorphism $A \otimes_K F \cong M_n(F)$, then $\mu' \circ \mu$ is an automorphism of $M_n(F)$. By the Skolem-Noether theorem, $\mu' \circ \mu$ is inner. Therefore, $\mu\lambda(a)$ and $\mu'\lambda(a)$ are conjugate and hence have the same determinant and trace.
- If L is an extension of F, we get $A \otimes_K L \cong (A \otimes_K F) \otimes_F L \cong M_n(L)$ and hence a representation of A in L which clearly gives the same reduced norm and trace for A. Thus, if we take another maximal subfield F' of A, we obtain the same reduced norm and trace since we can take a representation in an extension L of both F and F' where the two norms and traces agree. Hence, the definition is independent of the choice of F.

Let E/K be a galois closure of F. One can show that $\mathrm{Gal}(E/K)$ fixes $\mathrm{N}^0(a)$ and $\mathrm{tr}^0(a)$ and therefore $\mathrm{N}^0(a), \mathrm{tr}^0(a) \in K$.

The reduced norm and trace have the following (universal) property which is actually the reason for the name 'reduced' norm and trace:

Lemma 11. *Every norm form* N *on A over k (that is a multiplicative polynomial function $\mathrm{N} : A \to k$, i.e for all $a, b \in A$, $\mathrm{N}(a)$ is a polynomial in any basis of A and $\mathrm{N}(ab) = \mathrm{N}(a)\mathrm{N}(b)$) is of the form*

$$\mathrm{N} = (\mathrm{N}_{K/k}\mathrm{N}^0)^r$$

for some $r \in \mathbb{N}$.
Every trace form tr *on A over k (that is an additive function $\mathrm{tr} : A \to k$ with the property $\mathrm{tr}(ab) = \mathrm{tr}(ba)$) is of the form*

$$\mathrm{tr} = s \cdot \mathrm{tr}_{K/k}\mathrm{tr}^0$$

for some $s \in \mathbb{N}$.
Moreover, if $[A : K] = d^2$, then N^0 is homogeneous of degree d.

Proof. [Mu], §19 ∎

Corollary 12. *Let X be a simple abelian variety of dimension g, K the center of $\mathrm{End}^0(X)$, $[\mathrm{End}^0(X) : K] = d^2$ and $[K : \mathbb{Q}] = e$. Then $de|2g$.*

Proof. Define for $f \in \mathrm{End}^0(X)$ the *norm* and *trace*

$$\mathrm{N}(f) = \det(T_l)f, \qquad \mathrm{tr}(f) = \mathrm{tr}(T_l f).$$

One can prove that the characteristic polynomial of $T_l f$ has rational coefficients and therefore, N defines a norm form over $\mathbb{Q}$. By the last lemma, for some $r \in \mathbb{N}$

$$\mathrm{N}(f) = (\mathrm{N}_{K/\mathbb{Q}}\mathrm{N}^0(f))^r.$$

Now, $\mathrm{N}(f)$ is homogeneous of degree $2g$ and $\mathrm{N}_{K/\mathbb{Q}}\mathrm{N}^0(f)$ is homogeneous of degree de. Hence $de|2g$. □

Proposition 13. *Let all notations be as above. If $\mathrm{End}^0(X)$ contains a subfield F of degree $2g$ over $\mathbb{Q}$, then $de = 2g$.*

Proof. [Sh], §5, Prop. 3 and 4 □

3. The Rosati-involution

We shall now introduce an involution on $\mathrm{End}^0(X)$ that will give use more information about the center K.

Let D be an ample and effective divisor on X. That is if and only if the map

$$\varphi_D : X \to X^\vee, \quad x \mapsto [t_x^* D - D]$$

is an isogeny. Let $f \in \mathrm{End}^0(X)$, put

$$f^\dagger = (\varphi_D' \circ f^\vee \circ \varphi_D) \otimes \frac{1}{\deg \varphi_D},$$

where φ_D' is as in Prop. 4.

One can easily verify that $f^{\dagger\dagger} = f$ and $(fg)^\dagger = g^\dagger f^\dagger$. That means, $f \mapsto f^\dagger$ is an anti-involution on $\mathrm{End}^0(X)$, the so called *Rosati-involution.*

Theorem 14. *(*Positivity of the Rosati-involution*)*
The form $(f, g) \mapsto \mathrm{tr}(fg^\dagger)$ is positive definite. In particular, $\mathrm{tr}(ff^\dagger) > 0$ for all $f \in \mathrm{End}^0(X) \setminus \{0\}$.

Proof. This is a deep and absolutely non-trivial fact! It can be found e.g. in [Mu], Theorem 21.1. □

Remark: The trace that we mean in this theorem is the l-adic trace defined in the proof of Cor. 12. However, we know that all trace forms are just positive multiples of the reduced trace. Therefore, it doesn't really matter which trace we use for this statement.

We should also note that on the center K of $\mathrm{End}^0(X)$ each trace form is a (positive) multiple of the standard trace $\mathrm{tr}_{K/\mathbb{Q}}$. Analogously, any norm form coincides on K with a power of the standard norm $\mathrm{N}_{K/\mathbb{Q}}$.

In the following we will always denote the center of $\mathrm{End}^0(X)$ by K. If $f \in K$, then for arbitrary $g \in \mathrm{End}^0(X)$ we have

$$f^\dagger g = f^\dagger g^{\dagger\dagger} = (g^\dagger f)^\dagger = (fg^\dagger)^\dagger \ = g^{\dagger\dagger} f^\dagger = g f^\dagger$$

i.e. the involution maps the center to itself. We denote the set of fixed elements under the involution by

$$K_0 = \{x \in K | x^\dagger = x\}.$$

Lemma 15. *K_0 is a totally real algebraic number field and if † is not the identity on K, then K is an imaginary quadratic extension of K_0, i.e. K is a* CM-field.

Theorem 16. *(*Approximation Theorem*)*
Let $K/\mathbb{Q}$ be a field extension and $|\cdot|_1, \ldots, |\cdot|_n$ pairwise non-equivalent valuations on K over $\mathbb{Q}$. Then for all $\varepsilon > 0$ and all $a_1, \ldots, a_n \in K_i$ (where K_i is the completion of K at $|\cdot|_i$) there is an $x \in K$ such that

$$|x - a_i|_i < \varepsilon \quad \textit{for all } i = 1, \ldots, n.$$

Proof. see for example [Co2], Prop. 8.2.5 □

Proof. (of Lemma 15) Let $\sigma_1, \ldots \sigma_r : K_0 \hookrightarrow \mathbb{R}$ be the real embeddings of K_0 and (in complex conjugate pairs) $\sigma_{r+1}, \bar{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \bar{\sigma}_{r+s} : K_0 \hookrightarrow \mathbb{C}$ all the complex embeddings of K_0.

By the approximation theorem (for the absolute values $|\sigma_i(\cdot)|$, where $| \quad |$ is the standard absolute value on $\mathbb{C}$) for all $\varepsilon > 0$ there is an $x \in K_0$ such that

$$|\sigma_j(x)| < \varepsilon, \quad \forall j = 1, \ldots, r+s-1 \quad \text{and} \quad |\sigma_{r+s}(x) - i| < \varepsilon.$$

(i. e. $\sigma_j(x) \approx 0$ for all $j = 1, \ldots, r+s-1$ and $\sigma_{r+s}(x) \approx i$)

Then (for a positive p) we get

$$\frac{1}{p}\mathrm{tr}(xx^\dagger) = \frac{1}{p}\mathrm{tr}(x^2) = \mathrm{tr}_{K_0/\mathbb{Q}}(x^2) = \sum_{j=1}^{r} \sigma_j(x^2) + 2\sum_{k=1}^{s} \mathrm{Re}\ \sigma_{r+k}(x^2).$$

All terms in this sum are ≈ 0 except the last one which is ≈ -2 since $\sigma_{r+s}(x^2) \approx -1$. Therefore $\mathrm{tr}(xx^\dagger) < 0$ which contradicts the positivity of the Rosati-involution, unless $s = 0$. Then, all embeddings of K_0 are real and hence, K_0 is totally real.

Now we see that the condition that K is a CM-field is equivalent to the condition that K is a totally complex field.
Assume this is false, then there is a real embedding $\tau_1 : K \hookrightarrow \mathbb{R}$ from which we obtain another real embedding $\tau_2 : K \hookrightarrow \mathbb{R}$ by $\tau_2(y) = \tau_1(y^\dagger)$. These two embeddings are different since the Rosati-involution was assumed not to be the identity on K. Let $\tau_3, \ldots, \tau_m : K \hookrightarrow \mathbb{C}$ be all the other embeddings of K.

Again by the approximation theorem, for all $\varepsilon > 0$ there is an $x \in K$ such that

$$|\tau_1(x) + 1| < \varepsilon, \quad |\tau_2(x) - 1| < \varepsilon \quad \text{and} \quad |\tau_j(x)| < \varepsilon \quad \forall j = 3, \ldots, m.$$

(i. e. $\tau_1(x) \approx -1$, $\tau_2(x) \approx 1$ and $\tau_j(x) \approx 0$ for all $j \neq 1, 2$)

Then (for a positive q) we get

$$\frac{1}{q}\mathrm{tr}(xx^\dagger) = \mathrm{tr}_{K/\mathbb{Q}}(xx^\dagger) = \sum_{j=1}^{m} \tau_j(xx^\dagger) \approx \tau_1(xx^\dagger) + \tau_2(xx^\dagger).$$

Clearly, $xx^\dagger \in K_0$ and so $\tau_1(xx^\dagger) = \tau_2(xx^\dagger)$. Therefore

$$\frac{1}{q}\mathrm{tr}(xx^\dagger) \approx 2\tau_1(xx^\dagger) = 2\tau_1(x)\tau_1(x^\dagger) = 2\tau_1(x)\tau_2(x) \approx -2.$$

This again contradicts the positivity of the Rosati-involution and hence, K must be totally complex. □

4. The Classification Theorem

Now we can write down the complete classification of endomorphism algebras of simple abelian varieties. There are four different types.

If the Rosati-involution is the identity on the center K we know that K is a totally real number field. In this case, $\mathrm{End}^0(X)$ can only have rank 1 or 4 over its center K.

Together with the fact that a non-trivial rcentral simple algebra over the reals is either a matrix algebra or the standard quaternion algebra $\mathbb{H}$ we obtain the first three types:

TYPE I: $\mathrm{End}^0(X) = K = K_0$ is a totally real algebraic number field and the Rosati-involution is the identity.

TYPE II: $K = K_0$ is a totally real algebraic number field and $\mathrm{End}^0(X)$ is a quaternion algebra such that for every embedding $\sigma : K \hookrightarrow \mathbb{R}$

$$\mathbb{R} \otimes_{K,\sigma} \mathrm{End}^0(X) \cong M_2(\mathbb{R})$$

as $\mathbb{R}$-algebras.

TYPE III: $K = K_0$ is a totally real algebraic number field and $\mathrm{End}^0(X)$ is a quaternion algebra such that for every embedding $\sigma : K \hookrightarrow \mathbb{R}$

$$\mathbb{R} \otimes_{K,\sigma} \mathrm{End}^0(X) \cong \mathbb{H}$$

as $\mathbb{R}$-algebras.

What can we say about the Rosati-involution in the last two cases? For any involution * on a division algebra A over $\mathbb{R}$ we have trivially for all $a \in A$:

$$a^2 - (a + a^*)a + a^*a = 0.$$

We also know that

$$a^2 - (\mathrm{tr}^0 a)a + \mathrm{N}^0(a) = 0.$$

Therefore, we must have for all $a \in A$:

$$a + a^* = \mathrm{tr}^0 a \quad \Leftrightarrow \quad a^* = \mathrm{tr}^0 a - a.$$

So, in case II the Rosati-involution corresponds to the involution

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = (\mathrm{tr} M)I - M$$

and in case III it corresponds to the quaternion conjugation

$$a + bi + cj + dk \mapsto \overline{a + bi + cj + dk} = a - bi - cj - dk.$$

Remark: In literatur it's often said that the Rosati-involution is conjugate to the standard involution by the Skolem-Noether theorem. However, here we have identity! (which is not true for higher dimension, e. g. $M_n(k)$)

Now we consider the case when the Rosati-involution is not the identity on K. We know that $\mathrm{End}^0(X)$ is split by a maximal subfield, in particular by $\mathbb{C}$. Together with Lemma 15 we get:

TYPE IV: K is a CM-field over K_0, i. e. an imaginary quadratic extension of the totally real field K_0, and $\mathrm{End}^0(X)$ is a division algebra such that for every embedding $\sigma : K \hookrightarrow \mathbb{C}$

$$\mathbb{R} \otimes_{K,\sigma} \mathrm{End}^0(X) \cong M_d(\mathbb{C})$$

as $\mathbb{C}$-algebras, where $d^2 = [\mathrm{End}^0(X) : K]$.

By the Skolem-Noether theorem the Rosati-involution is conjugate to the standard involution on $M_d(\mathbb{C})$

$$A = (a_{ij}) \mapsto (\overline{a_{ji}}) = \bar{A}^t =: A^*.$$

We will be interested in abelian varieties of type IV, which we will call abelian varieties *with complex multiplication (by K).*

5. Abelian Varietites in Characteristic 0

In the following two parts I want to give some important examples.

Let X be an abelian variety defined in characteristic 0. We know that over $\mathbb{C}$, X is a complex torus:

$$X \cong V/\Lambda$$

where V is a complex vector space of dimension $g = \dim X$ and Λ is a lattice in V.

Now an endomorphism f of X corresponds to a $\mathbb{C}$-linear map $F_f : V \to V$ with $F_f(\Lambda) \subseteq \Lambda$. So, we obtain the *analytic representation of* $\mathrm{End}^0(X)$:

$$S_a : \mathrm{End}^0(X) \to M_g(\mathbb{C}), \quad f \mapsto F_f$$

Furthermore, a $\mathbb{C}$-linear map $F : V \to V$ that leaves the lattice invariant corresponds to a map $\Lambda \to \Lambda$ of $\mathbb{Z}$-modules and so we obtain the *rational representation of* $\mathrm{End}^0(X)$:

$$S_r : \mathrm{End}^0(X) \to M_{2g}(\mathbb{Q}), \quad f \otimes 1 \mapsto (S_a f)_{|\Lambda}$$

If X is simple then $\mathrm{End}^0(X)$ is a division algebra and we know that every rational representation is divisible by $[\mathrm{End}^0(X) : \mathbb{Q}]$ (see [Co2], Prop. 7.1.4).
Hence, with the same notations as before, we have in characteristic 0

$$d^2 e | 2g,$$

not only $de|2g$ as stated in Cor. 12.

However, if $\mathrm{End}^0(X)$ contains a subfield of degree $2g$ over $\mathbb{Q}$, then $de = 2g$ by Prop. 13, so that we must have $d = 1$ which means that $\mathrm{End}^0(X) = K$ is a field.

In particular, in characteristic 0 there are no elliptic curves with a quaternion algebra as endomorphism algebra (they contain a subfield of degree 2 over $\mathbb{Q}$).

5.1. **Elliptic Curves without Complex Multiplication.** For elliptic curves the following fact is known.

Theorem 17. *If an elliptic curve E (over $\mathbb{C}$) has complex multiplication (say, by F) then the j-invariant $j(E)$ is an algebraic integer.*

Proof: [Si2], Thm. II.6.1 □

Remark: One can show that $\mathbb{Q}(j(E))$ is the Hilbert class field (i.e. the maximal abelian extension) of F.

For $j \neq 0, 1728$ we know that the elliptic curve given by

$$E : y^2 + xy = x^3 - \frac{36}{j - 1728} x - \frac{1}{j - 1728}$$

has j-invariant $j(E) = j$.

Choose j algebraic, but not integral, or transcendental over $\mathbb{Q}$, then $\mathrm{End}^0(E) = \mathbb{Q}$ by Thm. 16 and the above statement.

5.2. **Complex Multiplication.** We can very easily construct elliptic curves with a given totally complex field as endomorphism algebra: Let K be an imaginary quadratic extension of $\mathbb{Q}$, so $K = \mathbb{Q}(\sqrt{-m})$ for some $m \in \mathbb{N}$. Then its ring of integers $\mathscr{O}_K$ is a lattice in $\mathbb{C} \cong K \otimes_{\mathbb{Q}} \mathbb{R}$ and so

$$E = (K \otimes_{\mathbb{Q}} \mathbb{R}) / \mathscr{O}_K$$

is an elliptic curve.

Clearly we have for all $\alpha \in \mathscr{O}_K$: $\alpha \mathscr{O}_K \subseteq \mathscr{O}_K$ and by the above discussion we get

$$\mathscr{O}_K \subseteq \mathrm{End}(E) \quad \Rightarrow \quad K \subseteq \mathrm{End}^0(E).$$

By the classification theorem and the fact that quaternion algebras do not occur as endomorphism algebras of elliptic curves in char0, we must then have

$$K = \mathrm{End}^0(E).$$

So we have constructed an elliptic curve whose endomorphism ring is the given CM-field. We want to generalize that.

Clearly, we can define a complex torus in higher dimension as above. However, this need not be an abelian variety since we need that $K \otimes_{\mathbb{Q}} \mathbb{R}$ possesses a non-degenerate Riemann form. Furthermore, we shall think more about the complex structure of the real vector space $K \otimes_{\mathbb{Q}} \mathbb{R}$.

Definition 18. *Let K be a CM-field, $2g = [K : \mathbb{Q}]$. A* CM-type Φ for K *is a set $\Phi = \{\sigma_1, \ldots \sigma_g\}$ of distinct embeddings $\sigma_j : K \hookrightarrow \mathbb{C}$ such that $\sigma_i \neq \bar{\sigma}_j$ for $i \neq j$.*

We can also say that a CM-type is a set of representatives for the action of $Gal(K/K_0)$ on $\mathrm{Hom}_{\mathbb{Q}-\mathrm{algebras}}(K, \mathbb{C})$.

Lemma 19. *There is a bijection*

$$\left\{ \begin{array}{c} \textit{complex structures on } K \otimes_{\mathbb{Q}} \mathbb{R}, \textit{ i.e.} \\ \mathbb{R}\textit{-algebra homomorphisms } \mathbb{C} \to K \otimes_{\mathbb{Q}} \mathbb{R} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{CM-types} \\ \Phi \textit{ for } K \end{array} \right\}$$

Proof. see Robert's talk last semester □

For a given CM-type (K, Φ) we define

$$X(K, \Phi) = (K \otimes \mathbb{R})/\mathscr{O}_K$$

where $K \otimes_{\mathbb{Q}} \mathbb{R}$ carries the complex structure given by Φ.

Theorem 20. *$X(K, \Phi)$ is an abelian variety.*

Proof. Since $X(K, \Phi)$ is a complex torus it is sufficient to show that $K \otimes \mathbb{R}$ possesses a non-degenerate Riemann form, i.e. an $\mathbb{R}$-bilinear alternating form E that is integral on the lattice and such that the form $(x, y) \mapsto E(ix, y)$ is symmetric and positive definite.

We have a 1-1-correspondence between $\mathbb{R}$-bilinear alternating forms E on $K \otimes \mathbb{R}$ and Hermitian forms H on $K \otimes_{\mathbb{Q}} \mathbb{R}$ via

$$H(x, y) = E(ix, y) + iE(x, y) \quad (E(x, y) = \mathrm{Im}H, \text{ resp.})$$

where $(x, y) \mapsto E(ix, y)$ is positive definite if and only if H is positive definite (since $E(x, x) = 0$). The fact that E is $\mathbb{Z}$-valued on the lattice corresponds to the fact that $\mathrm{Im}H$ is integral on the lattice.

So, we need to find a positive Hermitian form H on $K \otimes_{\mathbb{Q}} \mathbb{R}$ such that $\mathrm{Im}H$ is integral on the lattice.

Let $K = K_0(\alpha)$ with α purely imaginary, i. e. $\alpha^2 \in K_0$ and for all $\tau : K_0 \hookrightarrow \mathbb{R}$, $\tau(\alpha^2) < 0$. By the approximation theorem there exists an $\eta \in K_0$ such that for all $\varepsilon > 0$ and all $\sigma_j \in \Phi$

$$\left|\sigma_j(\eta) - \frac{\sigma_j(\alpha}{i}\right| < \epsilon,$$

i.e. that $\sigma_j(\eta)$ and $\frac{\sigma_j(\alpha)}{i}$ have the same sign and so

$$\frac{\sigma_j(\eta\alpha)}{i} > 0.$$

Furthermore, there is an $N \in \mathbb{N}$ such that $N\eta\alpha \in \mathscr{O}_K$.

Proof. That's a basic fact for number fields: let K be a number field and $\alpha \in K$. Then there's an $N \in \mathbb{N}$ such that $N\alpha \in \mathscr{O}_K$:
consider the minimal polynomial of α:

$$P(x) = \mathrm{Min}(\alpha) = x^n + \sum_{j=0}^{n-1} a_j x^j \quad \in \mathbb{Q}[x].$$

Let $a_j = \frac{r_j}{s_j}$ ($r_j, s_j \in \mathbb{Z}$ and wlog $s_j > 0$) and $s_j = \prod_{p \text{ prime}} p^{\varepsilon_p(s_j)}$ be the decomposition of s_j into primes. Let $\varepsilon_p = \max_{1 \le j < n}\{\varepsilon_p(s_j)\}$ and put

$$N = \prod_{p \text{ prime}} p^{\varepsilon_p}.$$

Then we have

$$\begin{aligned} 0 = N^n P(\alpha) &= N^n\alpha^n + \sum_{j=0}^{n-1} r_j \frac{N^n}{s_j}\alpha^j = (N\alpha)^n + \sum_{j=0}^{n-1} r_j \frac{N^{n-j}}{s_j}(N\alpha)^j \\ &= (N\alpha)^n + \sum_{j=0}^{n-1} r_j \Big(\prod_{p \text{ prime}} p^{(n-j)\varepsilon_p - \varepsilon_p(s_j)}\Big)(N\alpha)^j \end{aligned}$$

Because of $n - j \ge 1$ and the choice of ε_p we have $(n-j)\varepsilon_p - \varepsilon_p(s_j) \ge 0$ and therefore

$$\gamma_j := r_j \prod_{p \text{ prime}} p^{(n-j)\varepsilon_p - \varepsilon_p(s_j)} \quad \in \mathbb{Z}.$$

Hence $Q(x) = x^n + \sum_{j=0}^{n-1} \gamma_j x^j \ \in \mathbb{Z}[x]$ and $Q(N\alpha) = 0$, i. e. $N\alpha$ is integral over $\mathbb{Z}$ which proves our claim. $\square$

Now let $\gamma := N\eta\alpha$. Then $K = K_0(\gamma)$ and $\beta_j := \frac{\sigma_j(\gamma)}{i} > 0$.
We define

$$H(x, y) = 2\sum_{j=1}^{g} \beta_j \sigma_j(x)\overline{\sigma_j(y)}.$$

This clearly defines a positive definite Hermitian form an $K \otimes_{\mathbb{Q}} \mathbb{R}$ and it remains to show that $\mathrm{Im}H$ is integral on $\mathscr{O}_K$.

Let $x, y \in \mathscr{O}_K$:

$$\begin{aligned}\mathrm{Im}H(x,y) = -\mathrm{Re}(iH(x,y)) &= -2\mathrm{Re}\sum_{j=1}^{g} i\beta_j\sigma_j(x)\overline{\sigma_j(y)} \\ &= -2\mathrm{Re}\sum_{j=1}^{g}\sigma_j(\gamma)\sigma_j(x)\sigma_j(\bar{y}) = -2\mathrm{Re}\sum_{j=1}^{g}\sigma_j(\gamma x\bar{y}) \\ &= -\sum_{j=1}^{g}(\sigma_j(\gamma x\bar{y}) + \bar{\sigma}_j(\gamma x\bar{y})) = -\mathrm{tr}_{K/\mathbb{Q}}(\gamma x\bar{y}) \quad \in \mathbb{Z},\end{aligned}$$

since $\gamma x\bar{y} \in \mathscr{O}_K$.

This shows that there is a non-degenerate Riemann form on $X(K,\Phi)$ which therefore is an abelian variety. □

Remarks:

(i) In general $X(K,\Phi)$ is not simple! We should be interested in a characterisation of CM-Types that tells us when $X(K,\Phi)$ is simple.

(ii) We say, $X(K,\Phi)$ is an abelian variety *of CM-type* (K,Φ). One can give a more general definition of an abelian variety of CM-type (K,Φ) and it is possible to show that such an abelian variety is isogenous to $X(K,\Phi)$.

(iii) The abelian varieties $X(K,\Phi_1)$ and $X(K,\Phi_2)$ are isogenous $\Leftrightarrow$ $\Phi_1 = \Phi_2$, i.e. we have 2^g isogeny classes of abelian varieties with CM by K.

6. Abelian Varieties over Finite Fields

Let X be an abelian variety defined over a finite field $\mathbb{F}_q$, $q = p^r$, p prime. We have the *Frobenius endomorphism* $\pi : X \to X$ which in projective coordinates is just the map $[x_0 : ... : x_n] \mapsto [x_0^q : ... : x_n^q]$. Note that this is well-defined since X is defined over $\mathbb{F}_q$. Also π is defined over $\mathbb{F}_q$.

Denote by P_π the characteristic polynomial of π (defined as the characteristic polynomial of $T_l\pi$). We know that P_π is monic and of degree $2g$ ($g = \dim X$) with integer coefficients and $P_\pi(\pi) = 0$. That means that π is an algebraic integer.

Clearly, π commutes with all endomorphisms f of X that are defined over $\mathbb{F}_q$. So

$$\mathbb{Q}[\pi] \subseteq \mathrm{center}(\mathrm{End}^0_{\mathbb{F}_q}(X))$$

where $\mathbb{Q}[\pi] = \mathbb{Z}[T]/(P_\pi(T)) \otimes_{\mathbb{Z}} \mathbb{Q}$ (a product of fields).

Theorem 21. (Tate) *Let X, Y be abelian varieties defined over a field k and $V_lX = T_lX \otimes_{\mathbb{Z}} \mathbb{Q}_l$. Denote by $\mathrm{Hom}_{\mathbb{Q}_l}(V_lX, V_lY)^\Gamma$ all homomorphisms $V_lX \to V_lY$ that commute with the action of $\Gamma = Gal(k^{sep}/k)$. Then the map*

$$\mathrm{Hom}(X,Y) \otimes_{\mathbb{Z}} \mathbb{Q}_l \to \mathrm{Hom}_{\mathbb{Q}_l}(V_lX, V_lY)^\Gamma$$

is injective. If k is finite then the latter map is bijective.

Proof. [Ta] □

Remark: This map is also bijective for number fields (Faltings) and many function fields in char$p$ (Zarkhin).

Corollary 22. center$(\mathrm{End}^0_{\mathbb{F}_q}(X)) = \mathbb{Q}[\pi]$.

Proof. Tate proofs in his article [Ta] that the image of center$(\mathrm{End}^0_{\mathbb{F}_q}(X))$ in $\mathrm{End}_{\mathbb{Q}_l}(V_lX)^\Gamma$ is equal to those elements in $\mathrm{Aut}(V_lX)$ that are defined by elements of Γ. However, finite fields are perfect, so $\Gamma = Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ which is topologically generated by the Frobenius that corresponds to the Frobenius endomorphism on X. That means that center$(\mathrm{End}^0_{\mathbb{F}_q}(X))$ is generated by π. □

Theorem 23. *(Riemann hypothesis) All roots of P_π have absolute value $q^{1/2}$.*

Proof. [Mi], 14.1 - 14.4 □

This leads to the following definition:

Definition 24. *A* Weil-q-integer *is an algebraic integer $\pi \in \mathbb{C}$ such that for all embeddings $\sigma : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$*

$$|\sigma(\pi)| = (\sigma(\pi))\overline{(\sigma(\pi))} = q^{1/2}.$$

Two Weil-q-integers π, π' are said to be conjugate *if there exists a $\sigma : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$ such that $\sigma(\pi) = \pi'$, i. e. they are conjugate as algebraic numbers.*
This is obviously equivalent to: there exists an isomorphism $\mathbb{Q}(\pi) \to \mathbb{Q}(\pi')$ that maps π to π'.

Hence, the Frobenius endomorphism of an abelian variety over $\mathbb{F}_q$ is a Weil-q-integer. We want to find out when the Frobenius endomorphisms of two abelian varieties X, Y over $\mathbb{F}_q$ are conjugate as Weil-q-integers.

Let $f : X \to Y$ be an isogeny defined over $\mathbb{F}_q$. Then we get an isomorphism

$$\mathrm{End}^0_{\mathbb{F}_q}(X) \to \mathrm{End}^0_{\mathbb{F}_q}(Y), \quad \phi \otimes 1 \mapsto (f \circ \phi \circ f') \otimes \frac{1}{\deg f}$$

(where f' is as in Prop. 4)

Clearly, that isomorphism maps π_X to π_Y since $f \circ \pi_X = \pi_Y \circ f$ and $ff' = [\deg f]$. By Cor. 22, if X and Y are *simple* we get an isomorphism between fields

$$\mathbb{Q}(\pi_X) \to \mathbb{Q}(\pi_Y) \quad \text{with} \quad \pi_X \mapsto \pi_Y,$$

i. e. π_X and π_Y are conjugate Weil-q-integers.

Hence, we get a map

$$\left\{ \begin{array}{c} \mathbb{F}_q\text{-isogeny classes of simple} \\ \text{abelian varieties over } \mathbb{F}_q \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{conjugacy classes of} \\ \text{Weil-}q\text{-integers} \end{array} \right\}$$

Theorem 25. (Honda) *This map is bijective.*

Proof. [Ho] □

If P_π is irreducible (so X has to be simple) then by Cor. 22 we have

$$2g = \deg P_\pi = [\mathbb{Q}(\pi) : \mathbb{Q}] = [\mathrm{center}(\mathrm{End}^0_{\mathbb{F}_q}(X)) : \mathbb{Q}] =: e.$$

However, $de|2g$, where $d^2 = [\mathrm{End}^0_{\mathbb{F}_q}(X) : \mathrm{center}(\mathrm{End}^0_{\mathbb{F}_q}(X))]$, and hence $d = 1$, i. e.

$$\mathrm{End}^0_{\mathbb{F}_q}(X) = \mathbb{Q}(\pi).$$

Example 26. *(supersingular elliptic curves)*

Let π_1 be a root of the polynomial $X^2 + p$. Then π_1 is a Weil-p-integer and by Honda's theorem, π_1 is the Frobenius of some elliptic curve E. Since $X^2 + p$ is irreducible (over $\mathbb{Q}$), we have

$$\mathrm{End}^0_{\mathbb{F}_p}(E) = \mathbb{Q}(\pi_1).$$

Recall: An elliptic curve is *supersingular* if and only if for all $n \in \mathbb{N}$, which is equivalent to $p|\mathrm{tr}(\pi_E)$.

So our elliptic curve E is supersingular and its endomorphism algebra over $\mathbb{F}_q$ is an imaginary quadratic field.

Now consider E over $\mathbb{F}_{p^2}$. Its Frobenius is clearly $\pi_2 = \pi_1^2$. What is P_{π_2}? We know that the roots of P_{π_2} are exactly the eigenvalues of $T_l\pi_2 = (T_l\pi_1)^2$. Hence, the roots of P_{π_2} are the squares of the roots of P_{π_1}: $(+i\sqrt{p})^2 = -p$ and $(-i\sqrt{p})^2 = -p$. Therefore, we have $P_{\pi_2}(X) = (X + p)^2$. In particular, $\pi_2 \in \mathbb{Q}$ and hence

$$\mathrm{center}(\mathrm{End}^0_{\mathbb{F}_{p^2}}(E)) = \mathbb{Q}.$$

However, $\pi_1 \notin \mathbb{Q}$ and therefore $\mathrm{End}^0_{\mathbb{F}_{p^2}}(E) \neq \mathbb{Q}$. By the classification theorem, $\mathrm{End}^0_{\mathbb{F}_{p^2}}(E)$ must then be a quaternion algebra.

Assume there are endomorphism not defined over $\mathbb{F}_{p^2}$. Then by the Galois action $\dim_{\mathbb{Q}} \mathrm{End}^0_{\mathbb{F}_p}(E) > \dim_{\mathbb{Q}} \mathrm{End}^0_{\mathbb{F}_{p^2}}(E)$ what contradicts the fact that de divides $2g = 2$. Therefore, all endomorphisms of E are already defined over $\mathbb{F}_{p^2}$.

Let us make this example a bit more explicit.

Consider the elliptic curve over $\mathbb{F}_p$ defined by

$$E : y^2 = x^3 + x$$

When is an elliptic curve supersingular? We have the criterion:
$E : y^2 = f(x)$ is supersingular $\iff$ the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ is 0.

Hence, in our case

$$\begin{aligned}(x^3 + x)^{(p-1)/2} &= \sum_{j=0}^{(p-1)/2} \binom{(p-1)/2}{j} x^{3((p-1)/2-j)} x^j \\ &= \sum_{j=0}^{(p-1)/2} \binom{(p-1)/2}{j} x^{\frac{3}{2}(p-1)-2j}\end{aligned}$$

and we get a $(p-1)$-st power of x if $j = (p-1)/4$. Therefore the coefficient of x^{p-1} is 0 if and only if $p \equiv 3 \pmod 4$ (and $\binom{(p-1)/2}{(p-1)/4}$ otherwise).

So, from now on let p be of the form $4k+3$.

Consider the map $[i] : E \to E$, $(x, y) \mapsto (-x, iy)$, where i is a root of $X^2 + 1$. Clearly, $[i]$ is defined over $\mathbb{F}_p \iff i \in \mathbb{F}_p \iff X^2 = -1$ has a solution in $\mathbb{F}_p$ $\iff \left(\frac{-1}{p}\right) = 1$.

However, by the quadratic reciprocity law,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{(4k+3-1)/2} = (-1)^{2k+1} = -1.$$

Therefore, $[i]$ is not defined over $\mathbb{F}_p$.

Let π be the Frobenius of E and its characteristic polynomial

$$P_\pi(X) = X^2 + \mathrm{tr}(\pi)X + p.$$

Since E is supersingular, $p | \mathrm{tr}(\pi)$, hence $\mathrm{tr}(\pi) = pt$ for some integer t. However,

$$|\mathrm{tr}(\pi)| = |\pi + \bar{\pi}| \leq |\pi| + |\bar{\pi}| = 2|\pi| = 2\sqrt{p}$$

and therefore

$$p|t| \leq 2\sqrt{p} \quad \Rightarrow \quad \sqrt{p}|t| \leq 2.$$

If $p > 3$ this can only be the case if $t = 0$, i.e. the characteristic polynomial of π is $X^2 + p$. So, we are in the same situation as above.

With Honda's theorem we see that this elliptic curve is the only supersingular curve up to $\mathbb{F}_p$-isogeny when $p = 4k+3$, $k \geq 1$.

Furthermore, we have

$$\mathrm{End}^0_{\mathbb{F}_p}(E) = \mathbb{Q}(\pi).$$

and $\mathrm{End}^0_{\mathbb{F}_{p^2}}(E) = \mathrm{End}^0_{\bar{\mathbb{F}}}(E)$ is the quaternion algebra generated by π and $[i]$.

References

[BiL] Birkenhake, C., Lange, H., *Complex Abelian Varieties*, Grundlehren d. mathematischen Wissenschaften (302), Springer (2004)

[Co2] Cohn, P. M., *Algebra, Volume 2*, John Wiley & Sons Ltd. (1989)

[Co3] Cohn, P. M., *Algebra, Volume 3*, John Wiley & Sons Ltd. (1991)

[Ho] Honda, T., *Isogeny Classes of Abelian Varieties over Finite Fields* Journal of the Mathematical Society of Japan 20, 83-95 (1968)

[Mi] Milne, J. S., *Abelian Varieties*, lecture notes on `http://www.jmilne.org/math` (1998)

[Mu] Mumford, D., *Abelian Varieties*, Oxford University Press (1970)

[MvG] Moonen, B., van der Geer, G., *Abelian Varieties* (preliminary version 2005 on `http://staff.science.uva.nl/bmoonen/boek/BookAV.htm`)

[Ne] Neukirch, J., *Algebraische Zahlentheorie*, Springer (1992)

[Sh] Shimura, G., *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press (1998)

[Si] Silverman, J. H., *The Arithmetic of Elliptic Curves*, Springer (1986)

[Si2] Silverman, J. H., *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer (1986)

[Ta] Tate, J., *Endomorphisms of Abelian Varieties over Finite Fields* Inventiones Mathematicae 2, 134-144 (1966)