Computing Endomorphism Rings of Jacobians

Lectures by: John Voight
Notes by: Ross Paterson

These notes were taken live during lectures at the CMI-HIMR Computational Number Theory summer school held at the University of Bristol in June 2019. In particular, any mistakes are the fault of the transcriber and not of the lecturer. Remarks in red were not written on the board, and were often added later by the transcriber.

Lecture List

Contents

1 Course Outline

We will look at computing endomorphism rings of jacobians

1. /$\mathbb{F}_q$
2. /$\mathbb{C}$
3. /$\mathbb{Q}$
4. Classification

Lecture 1: Endomorphisms over $\mathbb{F}_q$

Why should we care about endomorphism rings? Well if we want to understand an object we should try too understand its symmetries. Specifically these impact on rational points, Mordell-Weil ranks and more but its also a lot of fun.

Let F be a perfect field, F^{al} and $\mathrm{Gal}_F := \mathrm{Gal}(F^{\mathrm{al}}/F)$. Let A be an abelian variety over F, with multiplication law $m : A \times A \to A$, identity $e : \operatorname{spec} F \to A$ and inversion $i : A \to A$, satisfying group laws.

If $K \supseteq F$ then write $A_K := A \times_F \operatorname{spec} K$ and write $A^{\mathrm{al}} = A \times_F F^{\mathrm{al}}$,

Definition 1.1. *A **homomorphism** of abelian varieties $\phi : A \to A'$ is a morphism of abelian varieties (over F) respecting m, e, i and m', e', i'. e.g. for m*

$$\begin{array}{ccc} A \times A & \xrightarrow{m} & A \\ \downarrow{\scriptstyle \phi\times\phi} & & \downarrow{\scriptstyle \phi} \\ A' \times A' & \xrightarrow{m'} & A' \end{array}$$

*An **isogeny** is a homomorphism such that ϕ is surjective and $\dim A = \dim A'$*

Definition 1.2. *The **degree** of an isogeny is*

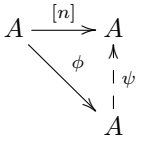
$$\deg \phi = [F(A) : F(A')]$$

Remark 1.3. *If $\mathrm{char}(F) \nmid \deg \phi$ then $\deg \phi = \#(\ker \phi)(F^{\mathrm{al}})$.*

Example 1. $\deg([n]_A : A \to A) = n^{2 \dim A}$.

Lemma 1.4. *If $\phi : A \to A'$ is an isogeny with degree $n = \deg \phi$, then there is an isogeny $\psi : A' \to A$ such that $\phi \circ \psi = [n]_{A'}$ and $\psi \circ \phi = [n]_A$.*

Sketch. $\ker \phi \subset A[n]$ so we have a commutative diagram:



□

If there is some isogeny $\psi : A \to A'$ then we write $A \sim A'$.

Definition 1.5. *A is **simple** (over F) if $A \nsim A_1 \times A_2$ nontrivially, i.e. for $\dim A_1, \dim A_2 \geq 1$. Say A is **geometrically simple** if A^{al} is simple.*

Lemma 1.6. *There is a unique isogenous representation $A \sim A_1^{n_1} \times \ldots A_t^{n_t}$ with each A_i simple, pairwise nonisogenous and $n_i \in \mathbb{Z}_{\geq 1}$.*

2 Finite Fields

Let $F = \mathbb{F}_q$ and $p = \text{char}(F)$. Let $\pi = \text{Frob}_q : A \to A$ be the q power Frobenius. Let

$$C_A(T) = C(T) := \det\left(1 - \text{Frob}_q^* T \mid H^1_{et}(A^{\text{al}}, \mathbb{Q}_\ell)\right) \quad \ell \nmid q$$

which we will call the characteristic polynomial (charpoly) of Frobenius, the correct term is probably reciprocal characteristic polynomial but we're clocking back to the 90's and calling it this. Then we have some properties

- $\deg C(T) = 2g = 2 \dim A$
- $C(T) \in 1 + T\mathbb{Z}[T]$ (independent of ℓ)
- $\#A(\mathbb{F}_q) = C(1)$.
- Factoring $C(T) := \prod_{i=1}^{2g}(1 - z_i T)$ with $|z_i|_{\mathbb{C}} = \sqrt{q}$.
- $q^g T^{2g} c\left(\frac{1}{qT}\right) = C(T)$ so can order roots $z_i z_{2g+1-i} = q$ for $i = 1, \ldots, g$
- $C(T) = \det\left(1 - \text{Frob} T \mid T_\ell(A)\right)$ for $T_\ell(A) = \varprojlim_n A[\ell^n]$ and $\ell \neq p$.

Example 2. *$g = 1$, $A = E$ an elliptic curve then $C(T) = 1 - aT + qT^2$ and*

$$\#E(\mathbb{F}_q) = q + 1 - a = c(1).$$

(If X is a nice curve, then this polynomial is the L-polynomial of the jacobian as in Andrew Sutherlands course.)

Theorem 2.1 (Tate)**.** *TFAE*

(i) *A' is isogenous to a subabelian variety of A,*

(ii) *$C'(T) := C_{A'}(T) \mid C(T)$ in $\mathbb{Q}[T]$.*

Corollary 2.2. *$A \sim A' \iff C(T) = C'(T)$*

Example 3. $C_A(T) = (1 + 5T^2)(1 - 2T + 5T^2) \Rightarrow A \sim E_1 \times E_2$.

Let $\mathcal{O} = \text{End}(A) := \text{Hom}(A, A)$, $\mathcal{O}$ is a ring with $\mathbb{Z} \subset \mathcal{O}$.
Let $B := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = \text{End}(A)_{\mathbb{Q}}$ the **Endomorphism Algebra**
From $\varphi \in \mathcal{O}$ an isogeny we know that we have ψ such that $\varphi\psi = n \in \mathcal{O}$ so $\varphi^{-1} = \psi/n$. Note that B is well defined on the isogeny class of A, and $\text{End}(A) \cong \mathbb{Z}^r$ for $r \geq 1$ as abelian groups. If we look at the isogenous product of simple abelian varieties

$$\begin{aligned} A \sim A_1^{n_1} \times \cdots \times A_t^{n_t} \Rightarrow B &= M_{n_1}(\text{End}(A_1)_{\mathbb{Q}}) \times \cdots \times M_{n_t}(\text{End}(A_t)_{\mathbb{Q}}) \\ &= M_{n_1}(B_1) \times \ldots M_{n_t}(B_t) \end{aligned}$$

where the B_i are division algebras over $\mathbb{Q}$ and this is thus a semisimple $\mathbb{Q}$-algebra.

Theorem 2.3 (Tate)**.** *Let $\pi = \text{Frob}_q \in \mathcal{O}$*

(a) *$Z(B) = \mathbb{Q}[\pi]$,*

(b) $B = \mathbb{Q}[\pi]$ *if and only if* $B = Z(B)$ *if and only if* $C(T)$ *is seperable (i.e. has no multiple roots),*

(c)

$$\begin{aligned}\mathbb{Q}[\pi] = \mathbb{Q} &\iff C(T) = \text{Power of linear polynomial} \\ &\iff B \cong M_g(B_1), \quad B_1 = \text{ Quaternion algebra over } \mathbb{Q}, \mathrm{Ram}(B_1) = \{p, \infty\} \\ &\iff A \sim E^g \in \text{ supersingular.}\end{aligned}$$

Recall $C(T) = \det(1 - \pi T \mid V) = \prod_{i=1}^{2g}(1 - z_i T)$.

Definition 2.4. $C^{\otimes 2}(T) = \det\left(1 - \pi^{\otimes 2} T \mid V \otimes V\right) = \prod_{i,j=1}^{(2g)^2}(1 - z_i z_j T) \in 1 + T\mathbb{Z}[T]$.

Factor $C^{\otimes 2} = h(T)\prod_i \Phi_{k_i}(qT) \in \mathbb{Q}[T]$, where Φ_{k_i} is the k_ith cyclotomic polynomial, so the minimal polynomial of a primitive k_ith root of unity.

Lemma 2.5 (Tate)**.** *We can show that*

(a)

$$\mathrm{rk}_{\mathbb{Z}}\,\mathcal{O} = \dim_{\mathbb{Q}} B = \#\{i : k_i = 1\}$$

More generally, $\mathrm{rk}_{\mathbb{Z}}\,\mathrm{End}(A_{\mathbb{F}_{q^r}}) = \sum_{k_i \mid r}\varphi(k_i)$*, where* φ *is here the Euler totient function.*

(b) Let $K = LCM\{k_i\}$*. Then* $\mathbb{F}_{q^K}$ *is the minimal field extension of* $\mathbb{F}_q$ *such that all endomorphisms of* A *are defined. i.e. such that* $\mathrm{End}(A^{\mathrm{al}}) = \mathrm{End}(A_{\mathbb{F}_{q^K}})$.

Example 4. $q = 5$*,* $C(T) = 1 - 2T^2 + 25T^4$*,* $g = 2$*. A is simple over* $\mathbb{F}_5$.

$$\begin{aligned}C^{\otimes 2}(T) &= (1 - 5T)^4(1 + 5T)^4(1 - 2T + 25T)^2(1 + 2T + 25T^2)^2 \\ &= \Phi_1(5T)^4\Phi_2(5T)^4 h(T)\end{aligned}$$

so $k_1 = \ldots k_4 = 1$ *and* $k_5, \ldots, k_8 = 2$ *and so* $K = 2$.

$$\begin{aligned}&\mathrm{rk}(\mathrm{End}(A)) = 4 && B = \mathbb{Q}[\pi] \cong \mathbb{Q}[T]/\langle C(T)\rangle \\ &\mathrm{rk}(\mathrm{End}(A_{\mathbb{F}_{25}})) = 8 && \mathrm{End}(A^{\mathrm{al}}) \text{ is defined over } \mathbb{F}_{25}\end{aligned}$$

Definition 2.6.

$$C^{(r)}(T) = \det(1 - \pi^r T \mid V) = \prod_{i=1}^{2g}(1 - z_i^r T)$$

for $r \geq 1$

Example 5. $C^{(2)}(T) = (1 - 2T + 25T^2)^2$ *and so* $A_{\mathbb{F}_25} \sim E^2$*,* $\#E(\mathbb{F}_25) = 25 - 2 + 1 = 24$.
$\mathrm{End}(A_{\mathbb{F}_25})_{\mathbb{Q}} \cong M_2(K)$ *for* $K = \mathbb{Q}[T]/(1 - 2T + 25T^2) \cong \mathbb{Q}(\sqrt{-24})$

Theorem 2.7 (Tate Conjecture for Abelian Varieties)**.** *The cyclic class map is an isomorphism*

$$\mathrm{Corr}(A, A) \otimes \mathbb{Q}_\ell \to (H^1_{et}(A^{\mathrm{al}}, \mathbb{Q}_\ell)^{\otimes 2}(1))^{\mathrm{Gal}_{\mathbb{F}_q}}$$

where Frob_q *acts by* $q^{-1}\mathrm{Frob}q$ *as we have a Tate twist.*

$$\mathrm{End}(A) \cong \mathrm{Corr}(A, , A^\vee)$$

$$\dim B = \dim \mathrm{Corr}(A, A)_{\mathbb{Q}}$$

Moreover,

$$\begin{aligned}
\dim_{\mathbb{Q}} B &= \dim_{\mathbb{Q}_\ell}(\mathrm{Corr}(A, A) \otimes \mathbb{Q}_\ell) \\
&= \dim_{\mathbb{Q}_\ell}(\text{Fixed subspace of } H^{\otimes 2}(1) \text{ under } \mathrm{Frob}_q) \\
&= \dim_{\mathbb{Q}_\ell}(\text{Fixed subspace of } H^{\otimes 2} \text{ where } \mathrm{Frob}_q \text{ acts by } q) \\
&= \#\{(i, j) : z_i z_j = q\} \\
&= \#\{i : k_i = 1\}
\end{aligned}$$

Lecture 2: Endomorphisms over $\mathbb{C}$

3 Endomorphisms over $\mathbb{C}$

Let $A/\mathbb{C}$ be an abelian variety with $g = \dim A$. Let $T_0(A)$ be the tangent space of A at O. Then $T_0(A) \cong \mathbb{C}^g$ is a Lie group, so has an exponential map

$$\exp : T_0(A) \to A(\mathbb{C})$$

which is in fact surjective. Let $\Lambda = \ker \exp$, then $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$, and further $A(\mathbb{C})[n] = \frac{1}{n}\Lambda/\Lambda$.

$$T_\ell A = \varprojlim_n A[\ell^n] \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathbb{Z}_\ell^{2g}.$$

Alternatively

$$\begin{aligned}
A(\mathbb{C}) &\cong \widetilde{A(\mathbb{C})}/\pi_1(A) \\
&\cong \mathbb{C}^g/\Lambda
\end{aligned}$$

where $\Lambda \cong H_1(A, \mathbb{Z})$. Now, let $V := \mathbb{C}^g$ and choose a $\mathbb{Z}$-basis $\{\lambda_i\}_{i=1}^{2g}$ for Λ. Then $\Pi := (\lambda_{ij})_{i,j} \in \mathrm{Mat}_{g \times 2g}(\mathbb{C})$, is the **big period matrix**. A change of basis of $\mathbb{C}^g$ acts by $P\Pi$ for $P \in \mathrm{GL}_g(\mathbb{C})$, so $\Pi = (P_1 \ P_2)$,

$$P_2^{-1}\Pi = (\Omega \ 1_g)$$

for $\Omega \in \mathrm{GL}_g(\mathbb{C})$ which we call the **small period matrix**. Let $X/\mathbb{C}$ be a nice curve, and $\omega_1, \ldots, \omega_g \in H^0(X, \Omega^1)$ be a $\mathbb{C}$-basis of holomorphic 1-forms on X.

Example 6. *If $X : y^2 = f(x)$ with $f(x)$ squarefree and $\deg(f) \in \{2g + 1, 2g + 2\}$, then*

$$\omega_i = x^{i-1}\frac{dx}{y}.$$

The set $X(\mathbb{C})$ is a compact (connected) Reimann surface. Let $\alpha_1, beta_1, \ldots, \alpha_g, \beta_g$ be a $\mathbb{Z}$-basis of $H_1(X, \mathbb{Z})$ that is **symplectic**, i.e. α_i intersects β_i with (oriented) intersection 1, α_i does not intersect β_j for $i \neq j$. So the intersection form is

$$\begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix}$$

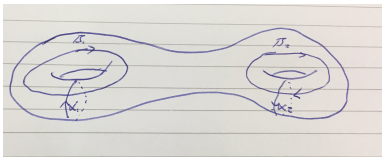


Figure 1: Example of symplectic basis on a genus 2 surface

The integration pairing

$$\begin{aligned}\Omega^1 \times H_1(X,\mathbb{Z}) &\to \mathbb{C}\\ (\omega,\nu) &\mapsto \int_\nu \omega\end{aligned}$$

is nondegenerate. This gives an injection $H_1(X,\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{C}}(\Omega^1,\mathbb{C})$. Let

$$\Lambda := \left\{ \left(\int_\nu \omega_j \right)^T : \nu \in H_1(X,\mathbb{Z}) \right\} \subset \mathbb{C}^g$$

Let $\mathrm{Jac}\, X := \mathrm{Hom}_{\mathbb{C}}(\Omega^1,\mathbb{C})/H_1(X,\mathbb{Z}) \cong \mathbb{C}^g/\Lambda$ be the Jacobian. It has big period matrix $\Pi = (P_1\ P_2)$ where

$$\begin{aligned}P_1 &= \left(\int_{\alpha_i} \omega_j \right)_{i,j}\\ P_2 &= \left(\int_{\beta_i} \omega_j \right)_{i,j}\end{aligned}$$

Example 7. $X : y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1$, `LMFDB:262144.d.324288.1`
$A : -\mathrm{Jac}\, X$, *then* $\Pi = \begin{pmatrix} 0.33 - 0.008i & \dots \\ -0.89 - 1.4i & \dots \end{pmatrix} \in \mathrm{Mat}_{2\times 4}(\mathbb{C})$.

Cutting open X along paths α_i, β_j and applying Greens theorem we find

Definition 3.1. $\Pi \in \mathrm{Mat}_{g\times 2g}(\mathbb{C})$ *is a* ***Riemann matrix****, if there is a skew-symmetric (alternating)* $E \in M_{2g}(\mathbb{Z})_{\mathrm{alt}}$, $\det E \neq 0$ *such that*

1. $\Pi E^{-1} \Pi^T = 0$*; and*
2. $\sqrt{-1}\Pi E^{-1}\Pi^*$ *is a positive definite hermitian form.*

where A^* *is the conjugate transpost of* A.
We say E *is a* ***Polarisation*** *on* Π.

Theorem 3.2 (Riemann-Poincaré)**.** $\mathbb{C}^g/\Pi\mathbb{Z}^{2g}$ *is an abelian variety if and only if* Π *is a Riemann matrix for some* E.

Proposition 3.3. *If* E *realises* Π *as a Riemann matrix, then* $E_{\mathbb{R}} : V \times V \to \mathbb{R}$ *defines*

$$\begin{aligned}H : V \times V &\to \mathbb{C}\\ H(x,y) &= E_{\mathbb{R}}(\sqrt{-1}x, y) + \sqrt{-1}E_{\mathbb{R}}(x,y)\end{aligned}$$

which is a positive definite, hermitian form and conversely.

Question 1. *How do we read off the endomorphism algebra from the period matrices?*

$\mathrm{End}(A)$ can be thought of in two ways, identifying $A = \mathbb{C}^g/\Lambda$:

- First, $\mathrm{End}(A) = \{M \in M_g(\mathbb{C}) : M\Lambda \subset \Lambda\} \subset M_g(\mathbb{C})$, i.e. the homotheties. So $M\Pi = \Pi R$ where $R \in M_{2g}(\mathbb{Z})$ since landing in Λ means you have a $\mathbb{Z}$-linear combination of the basis. Note that oen of M or R uniquely determines the other. M is called the (co)**tangent representation**. If $\alpha \in \mathrm{End}(A)$, then $[\alpha] \circlearrowleft H^0(X, \Omega^1)^\vee$.
- Second, we view $\Lambda = \mathbb{Z}^{2g} \subset \mathbb{R}^{2g}$ equipped with a **complex structure**, a map $J : \mathbb{R}^{2g} \to \mathbb{R}^{2g}$ such that $J^2 = -1$ induced by multiplication by i on $\mathbb{C}^g$.

Example 8. *$g = 1$, $\Pi = (P_1 \ P_2)$, $\Lambda = \mathbb{Z}\tau_1 + \mathbb{Z}\tau_2$ and $i\begin{pmatrix}\tau_1\\ \tau_2\end{pmatrix} = J\begin{pmatrix}\tau_1\\ \tau_2\end{pmatrix}$. Then* $\mathrm{End}(A) \cong \{R \in M_{2g}(\mathbb{Z}) \mid RJ = JR\}$
$\subset M_{2g}(\mathbb{Z})$.

$$H_1(X, \mathbb{Z}) \circlearrowleft ([\alpha] = R) \Rightarrow 0 \to \mathrm{End}(A) \to M_{2g}(\mathbb{Z})$$

So $\mathrm{End}(A) \cong \mathbb{Z}^r$ for $r \leq (2g)^2$. Note that $RJ = JR$ is a linear condition on $R \in M_{2g}(\mathbb{Z})$. LLL tells us that we can find short integer candidates.

Example 9. *Continuing 7 we have* $J = \begin{pmatrix} -0.25 & -0.19 & \dots \\ \cdots & \cdots & \cdots \\ \vdots & \ddots & \ddots \end{pmatrix}$ *and $J^2 = -1$. There are then 16 equations in 16 unknowns. Find the integer kernel spanned by 4 matrices (see exercises).*

$$M \approx \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix} -\frac{1}{2} - \frac{i}{2} & \dots \\ \frac{\sqrt{2}}{2} - i & \dots \end{pmatrix}$$

If X is defined over $F \subset \mathbb{C}$ with $[F : \mathbb{Q}] < \infty$ and we choose an F-basis for $H^0(X, \Omega^1)$ then $M, R \leftrightarrow \alpha \in \mathrm{End}(\mathrm{Jac}\, X)$ is defined over $K \supset F$ if and only if $M \in M_g(K)$. This tells us that $\mathrm{End}(A) = \mathbb{Z}$. If we let $K = \mathbb{Q}(\zeta_8)$ then $\mathrm{End}(A_K) \stackrel{?}{=} \mathbb{Z}\langle\alpha, \beta\rangle \subseteq B$, $\mathrm{disc}(B) = 6$ with $\alpha^2 = 3$, $\beta^2 + \beta + 1 = 0$, $\alpha\beta + \overline{\beta}\alpha = 3$ and $\overline{\beta} = 1 + \beta$. We will explain the question mark tomorrow.

Lecture 3: Endomorphisms over $\mathbb{Q}$

4 Number Fields

We're going to talk about endomorphism rings of Jacobians over number fields today, which will involve patching together the previous two lectures.

Let F be a number field and $F^{\mathrm{al}} \subset \mathbb{C}$ algebraic closure. Let X/F be a nice curve of genus $g \geq 1$. Let $A := \mathrm{Jac}\, X$ be the jacobian of X. Write X^{al} and A^{al} for the base changes to F^{al} as before. By "compute the endomorphism ring of A" we mean: Give as output,

- A (minimal) finite Galois extension $K \subseteq F$ such that $\mathrm{End}(A_K) = \mathrm{End}(A^{\mathrm{al}})$ (End is finitely generated and we can extend by each generator to obtain finite extension),
- A $\mathbb{Z}$-basis for $\mathrm{End}(A_K)$; and

- The multiplication table and $\mathrm{Gal}(K/F)$-action on basis.

Example 10. *Remember our running example:*
$X : y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1$. *Let* $K = \mathbb{Q}(\zeta_8)$ $\mathrm{End}(A_K) = \mathcal{O} \subset B$, $\mathcal{O}$ *maximal order in* B *a quaternion algebra with* $\mathrm{disc}(B) = 6$.

Theorem 4.1 (Lombardo)**.** *There exists a deterministic algorithm algorithm to compute the endomorphism ring.*

Proof. (1) By resolving singularities of $\mathrm{Sym}^g X$, embed

$$A \to \mathbb{P}^N$$

(2) $\mathrm{End}(A^{\mathrm{al}})$ is defined over $K = F(A[3])$.

(3) By *night*, try all rational maps $A - - \succ A$ over K. (Hey theres only countably many...), gives us a "lower bound".

(4) By *day*, compute an "upper bound" by creeping up (approximating to finite precision) on the isomorphism

$$\mathrm{End}(A_K) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathrm{End}_{\mathrm{Gal}(F^{\mathrm{al}}/K)} T_\ell(A_K)$$

Eventually (at *sunset*) ((3)) and ((4)) agree. □

Notation: Let K be such that $\mathrm{End}(A^{\mathrm{al}}) = \mathrm{End}(A_K)$ and let

$$A_K \sim A_1^{n_1} \times \cdots \times A_t^{n_t}$$

Let $B_i = \mathrm{End}(A_i)_{\mathbb{Q}}$, a division algebra, and $L_i = Z(B_i)$.

$$\dim_{L_i} B_i = e_i^2$$

for some $e_i \in \mathbb{Z}_{\geq 1}$. Then

$$\mathrm{End}(A_K)_{\mathbb{Q}} \cong M_{n_1}(B_1) \times \cdots \times M_{n_t}(B_t)$$

$\dim_{\mathbb{Q}}(B_i) = [L_i : \mathbb{Q}]e_i^2$. Thus

$$\dim_{\mathbb{Q}}(\mathrm{End}(A_K)_{\mathbb{Q}}) = \sum_{i=1}^{t} n_i^2 e_i^2 [L_i : \mathbb{Q}].$$

4.1 Better Days (Upper Bounds)

Let $\mathfrak{p}$ be a prime of good reduction for X and let $\mathbb{F}_{\mathfrak{p}}$ be its residue field. Specialisation gives an injective ring homomorphism

$$\mathrm{End}(A^{\mathrm{al}}) \subseteq \mathrm{End}(A_{\mathbb{F}_{\mathfrak{p}}^{\mathrm{al}}})$$

where $A_{\mathbb{F}_{\mathfrak{p}}^{\mathrm{al}}}$ is the reduction of A over $\mathbb{F}_{\mathfrak{p}}^{\mathrm{al}}$. This inclusion is rarely strict.

Let $k_{\mathfrak{p}}$ be such that $\mathrm{End}(A_{\mathbb{F}_{\mathfrak{p}}^{\mathrm{al}}})$ is defined over $\mathbb{F}_{\mathfrak{p}^{k_{\mathfrak{p}}}}$.

Proposition 4.2. *(a) For all* $i = 1, \ldots, t$ *there exists* $g_{\mathfrak{p},i}(T) \in 1 + T\mathbb{Z}[T]$ *such that*

$$C_{\mathfrak{p}}^{(k_{\mathfrak{p}})}(T) = g_{\mathfrak{p},1}(T)^{e_1} \ldots g_{\mathfrak{p},t}(T)^{e_t}$$

(b) Factor $C_{\mathfrak{p}}^{(k_{\mathfrak{p}})}(T) = \prod_{i=1}^{t} h_{\mathfrak{p},i}(T)^{m_{\mathfrak{p},i}}$*, then*

$$2\sum_{i=1}^{t} e_i n_i^2 \dim A_i = \sum_{i=1}^{t} e_i^2 n_i^2 \deg g_{\mathfrak{p},i} \leq \dim_{\mathbb{Q}}(\mathrm{End}(A_{\overline{\mathbb{F}_p}})_{\mathbb{Q}})$$

with equality on the end if and only if $g_{\mathfrak{p},i}(T)$ *are seperable and pairwise coprime. (See exercise sheet.)*

Corollary 4.3. *(a)) If equality holds in* ((b)) *then* $t \leq t_{\mathfrak{p}}$*.*

(b)) If equality holds in ((b)) *and* $t = t_{\mathfrak{p}}$ *then*

$$\{(e_i n_i, n_i \dim A_i)\}_{i=1}^{t} = \left\{(m_{\mathfrak{p},i}, \frac{1}{2} m_{\mathfrak{p},i} \deg h_{\mathfrak{p},i})\right\}_{i=1}^{t_{\mathfrak{p}}}$$

Example 11. $C_5^{(2)}(T) = (1 - 2T + 25T^2)^2$ *in our usual example,* $t \leq t_5 = 1$*.*

Proposition 4.4 (Zywina)**.** *There is a set* S *of primes of positive density such that* $t = t_{\mathfrak{p}}$ *and equality holds in* ((b))*. Assuming Mumford-Tate conjecture for* A*. (We do not go into detail on this conjecture, but essentially it says that certain things seen in the hodge theory can be viewed via the Galois representation theory.)*

Lemma 4.5. *Given the multiset* $\{e_i n_i\}_i$*, the set* S *is effectively computable.*

Remark 4.6. *We can guess* $\{e_i n_i\}_i$*.*

Lemma 4.7. *If* $\mathfrak{p} \in S$ *then* $L_i \hookrightarrow \mathbb{Q}[T]/(g_{\mathfrak{p},i}(T)) = M_{\mathfrak{p},i}$

Proposition 4.8 (Zywina)**.** *For any* $\mathfrak{q} \in S$*, for all* $\mathfrak{p} \in S$ *outside of a set of density zero, we have "*$L_i = M_{\mathfrak{p},i} \cap M_{\mathfrak{q},i}$*". i.e. If* $M' \hookrightarrow M_{\mathfrak{p},i}$ *and* $M' \hookrightarrow M_{\mathfrak{q},i}$ *then* $M' \hookrightarrow L_i$ *.*

Example 12.

$$\begin{aligned} C_7(T) &= 1 + 6T^2 + 49T^4 & k_7 &= 2 \\ C_7^{(2)}(T) &= (1 + 6T + 49T^2)^2 \\ M_5 &= \mathbb{Q}(\sqrt{-24}) \\ M_7 &= \mathbb{Q}(\sqrt{-40}) \end{aligned}$$

So in particular $L = \mathbb{Q}$*. Hence* $\dim_{\mathbb{Q}} \mathrm{End}(A)_{\mathbb{Q}} = \dim_{\mathbb{Q}} B = (e_1 n_1)^2 [L_1 : \mathbb{Q}] = 2^2 \cdot 1 = 4$

4.2 Better Nights (Lower Bounds)

Recall from our numberical calculations that we obtain candidate endomorphisms α and matrices $M \in M_g(K)$ and $R \in M_{2g}(\mathbb{Z})$. We compute a "certificate" that α is an endomorphism. Let $P_0 \in X(F)$. Then we have the Abel-Jacobi map

$$X \xhookrightarrow{AJ} A \xrightarrow{\alpha} A \overset{\text{mum}}{\dashrightarrow} \mathrm{Sym}^g(X)$$

where AJ sends $P \mapsto [P] - [P_0]$, and the Mumford map mum is given by $[D] \mapsto \{Q_1, \ldots, Q_g\}$ where $[D] = [Q_1 + \cdots + Q_g - gP_0]$.

Let $D \supseteq \{(P, Q_i) : P \in X\}$ be the Zariski closure of the graph of α,

Theorem 4.9 (Costa-Mascot-Sijsling-Voight)**.** *There is a deterministic algorithm that, given $M \in M_g(K)$, returns:*

- `true` *if $M \leftrightarrow \alpha \in \mathrm{End}(A_K)$ with divisor D and $\alpha(AJ(X)) \not\subseteq 1$ bad locus of* mum*.*
- *(Not quite sure yet, at the moment just returns false for undecided)*

Lecture 4: Classification

We begin by finishing up from last time. F was a number field and X/F a nice curve, with $A := \mathrm{Jac}\, X$ and $M \in M_g(K)$ a candidate endomorphism $\leftrightarrow \alpha \in \mathrm{End}(A_K)$

Theorem 4.10 (Costa-Mascot-Sijsling-Voight)**.** *There exists a deterministic algorithm to certify $M \leftrightarrow \alpha$ with divisor D.*

Proof. Suppose that $P_0 \in X(F)$ is not a Weierstrass point, choose x a uniformizer at P_0. We compute:

$$\alpha([\tilde{P}_0 - P_0]) = [\tilde{Q}_1, \ldots, \tilde{Q}_g - gP_0]$$

where $P_0 \in X(F[[x]])$ is the formal expansion (this you should think of the local ring at P_0). □

In the exercises you get to carry this out: Solve a differential equation formally

$$\sum_{i=1}^{g} x_j^*(\omega_i) = \alpha^*(\omega_i),$$

for $x_j := x(\tilde{Q}_j)$.

Now we begin todays lecture!

5 Classification of Endomorphisms

Let F be a field and A/F an abelian variety, then up to isogeny we know

$$A \sim A_1^{n_1} \times \cdots \times A_t^{n_t}$$

where A_i are simple, so

$$\mathrm{End}(A)_{\mathbb{Q}} \cong M_{n_1}(B_1) \times \cdots \times M_{n_t}(B_t)$$

with $B_i := \mathrm{End}(A_i)_{\mathbb{Q}}$ which is a (finite-dimensional (as the Tate module is finitely generated)) division ($\mathbb{Q}$-)algebra. From now on A is simple so that $B = \mathrm{End}(A)_{\mathbb{Q}}$ is a division algebra (and hence simple, i.e. no nontrivial 2-sided algebras). Let $L := Z(B)$ be the centre, a number field. B is a **central** L-algebra, and we call such things CSA's.

If B' is a CSA over L and L'/L a field extension then $B \otimes_L L'$ is again a CSA.

Question 2. *Which CSA's can turn up for endomorphism rings of abelian varieties?*

We will turn out to have some extra involution structure which will restrict the possible choices.

Let $F \subset \mathbb{R}$ be a dubfield and B a finite-dimensional F-algebra. B acts on itself by left multiplication: $\forall \alpha \in B$ define the map

$$\begin{aligned} \lambda_\alpha : B &\to B \\ x &\mapsto \alpha x \end{aligned}$$

which is F linear. Define $\operatorname{Tr}_{B/F} \alpha - \operatorname{Tr} \lambda_\alpha$.

Definition 5.1. *An **involution** $\bar{\cdot} : B \to B$ is a F-linear map such that*

(i) $\overline{1} = 1$*;*

(ii) $\overline{\overline{\alpha}} = \alpha$ *for all* $\alpha \in B$

(iii) $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$ *for all* $\alpha, \beta \in B$*.*

*An involution is **positive** if* $\operatorname{Tr}(\alpha\overline{\alpha}) \geq 0$ *for all* $\alpha \in B$*.*

Remark 5.2. *$\bar{\cdot}$ is positive if and only if if is positive on $B \otimes_F \mathbb{R} = B_{\mathbb{R}}$.*

Example 13. $\mathrm{id} : \mathbb{R} \to \mathbb{R}$ *is positive since* $\operatorname{Tr}(x^2) = x^2 \geq 0$.
Complex conjugation $\bar{\cdot} : \mathbb{C} \to \mathbb{C}$ *since* $\operatorname{Tr}(z\overline{z}) = 2\left|z\right|^2 \geq 0$.

Example 14. *Let* $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ *be Hamiltons quaternions. Then the involution* $\mathbb{H} \to \mathbb{H}$ *given by*

$$\alpha \mapsto 2t - \alpha$$

where $\alpha = t + xi + yj + zij$*, is positive since* $\overline{\alpha}\alpha = \alpha\overline{\alpha} = t^2 + x^2 + y^2 + z^2 \geq 0$*, so that* $\operatorname{Tr}(\alpha\overline{\alpha}) = 4(t^2 + x^2 + y^2 + z^2) \geq 0$.

Example 15. *Let* $D = \mathbb{R}, \mathbb{C}, \mathbb{H}$ *and* $\bar{\cdot}$ *the involution choice above. Let* $B = M_n(D)$ *and define*

$$\begin{aligned} * : B &\to B \\ \alpha &\mapsto \overline{\alpha}^T \end{aligned}$$

the conjugate transpose map. If $\alpha = (a_{i,j})_{i,j=1..n}$ *then*

$$\operatorname{Tr}(\alpha^*\alpha) = n(\dim_{\mathbb{R}}(D)) \sum_{i,j=1}^{n} \overline{a_{i,j}} a_{i,j}$$

So that $*$ is positive.

Theorem 5.3 (Frobenius-Wedderburn)**.** *A simple $\mathbb{R}$-algebra is isomorphic to $M_n(D)$ for one of $D = \mathbb{R}, \mathbb{C}, \mathbb{H}$.*

Proposition 5.4. *Let $B \cong M_n(D)$ and $*$ the conjugate transpose map. Let $\cdot^\dagger : B \to B$ be another positive involution on B. Then there is $\mu \in B^\times$ with $\mu^* = \mu$ such that all eigenvalues of λ_μ are positive and*

$$\alpha^\dagger = \mu^{-1}\alpha^*\mu$$

for all $\alpha \in B$ and conversely.

Returning to endomorphism rings we have

Theorem 5.5. *B has a positive involution.*

Proof over $\mathbb{C}$: Let $A(\mathbb{C}) \cong V/\Lambda$. We say $f : V \to \mathbb{C}$ is a **$\mathbb{C}$-antilinear functional** if

$$f(x + x') = f(x) + f(x')$$
$$f(ax) = \overline{a} f(x)$$

for all $x, x' \in V, \alpha \in \mathbb{C}$. Write $f \in \mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C}) =: V^*$. Now

$$\Lambda^* := \{f \in V^* \mid \mathrm{Im}\, f(\Lambda) \subset \mathbb{Z}\}$$
$$A^\vee := V^*/\Lambda^*$$
$$(A^v ee)^\vee \cong A$$

Let $H : V \times V \to \mathbb{C}$ be a polarisation on A, a positive definite hermitian form on V, such that $E := \mathrm{Im}\, H(\Lambda) \subset \mathbb{Z}$ gives a $\mathbb{C}$-linear map $\lambda : V \to V^*$ via $x \mapsto H(x, -)$. $\lambda(\Lambda) \subset \Lambda^*$ so $\lambda : A \to A^\vee$ is an isogeny. In general $A^\vee := \underline{\mathrm{Pic}}^0(A)$.
A new definition of polarisation: Isogeny $\lambda A \to A^\vee$, for $\phi \in \mathrm{End}(A)$ define $\phi^\dagger \in \mathrm{End}(A)_\mathbb{Q}$ by $\phi^\dagger := \lambda^{-1}\phi^\vee\lambda$. Consider

$$\begin{array}{ccc} A & \xrightarrow{\lambda} & A^\vee \\ & & \downarrow{\scriptstyle \phi^\vee} \\ A & \xrightarrow{\lambda} & A^\vee \end{array}$$

altering this we have

$$\begin{array}{ccc} A & \xrightarrow{\lambda} & A^\vee \\ \downarrow{\scriptstyle \phi^\dagger} & & \downarrow{\scriptstyle \phi^\vee} \\ A & \xleftarrow[\lambda^{-1}]{} & A^\vee \end{array}$$

extend $\mathbb{Q}$-linearly to B and then $\cdot^\dagger : B \to B$ is an involution that depends on λ. We have: $H(\phi x, y) = H(x, \phi^\dagger y)$, i.e. $\phi^\dagger$ is the adjoint of ϕ. B acts faithfully on V. If $r \in \mathbb{R}$ is an eigenvalue of $\phi^\dagger\phi$ on B then for x an eigenvector on V, by duality we get

$$rH(x, x) = H(rx, x) = H(\phi^\dagger\phi x, x) = H(\phi x, \phi x) > 0.$$

So in particular $r = \frac{H(\phi x, \phi x)}{H(x,x)} > 0$ and thus $\mathrm{Tr}(\phi^\dagger\phi) \in \mathbb{R}_{>0}$. □

Let $K := Z(B)$ and $F = K^{\langle\dagger\rangle}$ be the fixed field for the involution $\dagger$.

Lemma 5.6. *F is a totally real number field and either $K = F$ or K is a CM-field.*

Theorem 5.7 (Albert)**.** *Let $n = [F : \mathbb{Q}]$, then F is one of*

I. (real multiplication) $B = K = F$ and $\dagger = \mathrm{id}$

II. (quaternion multiplication by matrices) $K = F$, B is a (division-) quaternion algebra over F such that
$$B \otimes_\mathbb{Q} \mathbb{R} \cong M_2(\mathbb{R})^n$$

III. (quaternion multiplication by Hamiltons quaternions) $K = F$, B is a (division-) quaternion algebra over F such that
$$B \otimes_\mathbb{Q} \mathbb{R} \cong \mathbb{H}^n$$

Type	$\mathbf{B} \otimes_{\mathbb{Q}} \mathbb{R}$	Constraints
I.	$\mathbb{R}^n$	$n \mid g$
II.	$M_2(\mathbb{R})^n$	$2n \mid g$
III.	$\mathbb{H}^n$	$2n \mid g$
IV.	$M_d(\mathbb{C})^n$	$nd^2 \mid g$

Table 1: What further is known ($\mathrm{char}(F) = 0,\ g = \dim A,\ n = [F : \mathbb{Q}]$)

IV. (CM) $K \supseteq F$ *and* $B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_d(\mathbb{C})^n$ *for some* $d \in \mathbb{Z}_{\geq 1}$.

We summarise what further is known with Table.

Example 16. $\mathrm{End}(A_{\mathbb{Q}(i)})_{\mathbb{Q}} \cong \mathbb{H}$ *for* A *in isogeny class with LMFDB label* 4096.b.65536.

Definition 5.8. *A* ***Weil*** q***-number*** *is* $\pi \in \mathbb{Q}^{\mathrm{al}} \subset \mathbb{C}$ *such that* $|\pi_i|_{\mathbb{C}} = \sqrt{q}$ *for all conjugates* π_i.

Theorem 5.9 (Honda-Tate)**.** *There is a bijection*

$$\{\text{Simple abelian varieties over } \mathbb{F}_q\}/\text{isogeny} \leftrightarrow \{\text{Weil q-numbers }\}/\text{Galois conjugacy}$$

Given by $A \mapsto$ *root of* $C_A(T)$. *For* A, *let* $B = \mathrm{End}(A)_{\mathbb{Q}}$.

1. $Z(B) = \mathbb{Q}(\pi) =: L$
2. $2 \dim A = 2g = e[L : \mathbb{Q}]$
3. B *splits at every non-archimedean* $v \nmid p = \mathrm{char}\, \mathbb{F}_q$.
4. B *ramifies at every* v *real.*
5. $\mathrm{inv}_v(B) = \frac{v(\pi)}{v(q)}[L_v : \mathbb{Q}_p] \mod \mathbb{Z}$ *for* $v \mid p$.
6. $C_A(T) = m_A(T)^e$, *for* e *the least common denominator of* $m_v(B)$ *for all places* v, *where* m_A *is the minimal polynomial of* $\pi = \mathrm{Frob}_q$.

Example 17. $1 - \sqrt{q}T$, q *a square and* $\pi = \sqrt{q}$ *is a Weil q-number.* $L = \mathbb{Q}(\pi) = \mathbb{Q}$. $\mathrm{inv}_\infty(B) = \frac{1}{2}$ *and* $\mathrm{inv}_p(B) = \frac{1}{2}$. *Thus* $e = 2$ *and we have a supersingular elliptic curve.*