Restrictions on endomorphism algebras of abelian varieties

Pip Goodman

27th April 2022

Why might we expect restrictions on $\mathrm{End}(A)$ from the G_K-modules $A[\ell]$?

Theorem (Faltings' Isogeny Theorem)

The natural map

$$\mathrm{End}_K(A) \otimes \mathbb{Z}_\ell \to \mathrm{End}(T_\ell(A))^{G_K}$$

is an isomorphism.

Thus given the action of G_K on $A[\ell]$ one should not expect to say any more than $\mathrm{End}_K(A) \otimes \mathbb{Z}_\ell$. In fact, in general, $A[\ell]$ doesn't tell us much about $\mathrm{End}(A)$.

Example

1. $f(x) = (x+1)(x^4 + x^3 + x^2 + x + 1)$, has $\mathrm{End}^0(J_f) \cong \mathbb{Q}$.
2. $f(x) = x(x^4 + x^3 + x^2 + x + 1)$, has $\mathrm{End}^0(J_f) \cong \mathbb{Q} \times \mathbb{Q}$.
3. $f(x) = (x-1)(x^4 + x^3 + x^2 + x + 1)$, has $\mathrm{End}^0(J_f) \cong \mathbb{Q}(\zeta_5)$.

Why might we expect restrictions on $\mathrm{End}(A)$ from the G_K-modules $A[\ell]$?

Theorem (Faltings' Isogeny Theorem)

The natural map

$$\mathrm{End}_K(A) \otimes \mathbb{Z}_\ell \to \mathrm{End}(T_\ell(A))^{G_K}$$

is an isomorphism.

Thus given the action of G_K on $A[\ell]$ one should not expect to say any more than $\mathrm{End}_K(A) \otimes \mathbb{Z}_\ell$. In fact, in general, $A[\ell]$ doesn't tell us much about $\mathrm{End}(A)$.

Example

1. $f(x) = (x+1)(x^4+x^3+x^2+x+1)$, has $\mathrm{End}^0(J_f) \cong \mathbb{Q}$.
2. $f(x) = x(x^4+x^3+x^2+x+1)$, has $\mathrm{End}^0(J_f) \cong \mathbb{Q} \times \mathbb{Q}$.
3. $f(x) = (x-1)(x^4+x^3+x^2+x+1)$, has $\mathrm{End}^0(J_f) \cong \mathbb{Q}(\zeta_5)$.

Why might we expect restrictions on $\mathrm{End}(A)$ from the G_K-modules $A[\ell]$?

Theorem (Faltings' Isogeny Theorem)

The natural map

$$\mathrm{End}_K(A) \otimes \mathbb{Z}_\ell \to \mathrm{End}(T_\ell(A))^{G_K}$$

is an isomorphism.

Thus given the action of G_K on $A[\ell]$ one should not expect to say any more than $\mathrm{End}_K(A) \otimes \mathbb{Z}_\ell$. In fact, in general, $A[\ell]$ doesn't tell us much about $\mathrm{End}(A)$.

Example

1. $f(x) = (x+1)(x^4 + x^3 + x^2 + x + 1)$, has $\mathrm{End}^0(J_f) \cong \mathbb{Q}$.
2. $f(x) = x(x^4 + x^3 + x^2 + x + 1)$, has $\mathrm{End}^0(J_f) \cong \mathbb{Q} \times \mathbb{Q}$.
3. $f(x) = (x-1)(x^4 + x^3 + x^2 + x + 1)$, has $\mathrm{End}^0(J_f) \cong \mathbb{Q}(\zeta_5)$.

Links to Inverse Galois Theory

Theorem (Serre '72)

Let E/K be an elliptic curve with $\mathrm{End}(E) \cong \mathbb{Z}$. Then for all but finitely many primes ℓ, we have $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$.

Theorem (Hall '08)

Let $f(x) \in K[x]$ be a squareefree polynomial of degree $2g+1$. Suppose $\mathrm{End}(J_f) \cong \mathbb{Z}$, and modulo some prime q, f has a root of multiplicity two. Then for all but finitely many primes ℓ, we have $\mathrm{Gal}(K(J_f[\ell])/K) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.

Theorem (Zarhin '00)

Let $f \in K[x]$ be a polynomial of degree $n \geq 5$ with Galois group containing A_n. Then J_f has trivial endomorphism ring.

Remark

To prove this result, it suffices to prove it for A_n.

Links to Inverse Galois Theory

Theorem (Serre '72)

Let E/K be an elliptic curve with $\mathrm{End}(E) \cong \mathbb{Z}$. Then for all but finitely many primes ℓ, we have $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$.

Theorem (Hall '08)

Let $f(x) \in K[x]$ be a squareefree polynomial of degree $2g+1$. Suppose $\mathrm{End}(J_f) \cong \mathbb{Z}$, and modulo some prime q, f has a root of multiplicity two. Then for all but finitely many primes ℓ, we have $\mathrm{Gal}(K(J_f[\ell])/K) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.

Theorem (Zarhin '00)

Let $f \in K[x]$ be a polynomial of degree $n \geq 5$ with Galois group containing A_n. Then J_f has trivial endomorphism ring.

Remark

To prove this result, it suffices to prove it for A_n.

Theorem (Zarhin '00)

Let $f \in K[x]$ be a polynomial of degree $n \geq 5$ with Galois group containing A_n. Then J_f has trivial endomorphism ring.

For a rough outline of the proof, we'll need the following properties of $\mathrm{End}(A)$:

- $\mathrm{End}(A)$ is a free $\mathbb{Z}$-module of rank $< 4g^2$.
- G_K acts on $\mathrm{End}(A)$ by conjugation.
- $\mathrm{End}(A) \otimes \mathbb{Z}/2\mathbb{Z}$ may be viewed as a subalgebra of $\mathrm{End}(A[2])$.

What can we say for smaller Galois groups ?

Zarhin has done a lot of work on this for large insoluble Galois groups. For example, we have the following :

Theorem (Elkin, Zarhin '06,'08)

Suppose $n = q + 1$*, where* $q \geq 5$ *is a prime power congruent to* ± 3 *or* 7 *modulo* 8*. Suppose that* $f(x) \in K[x]$ *is irreducible, has degree* n *and* $\mathrm{Gal}(f) \cong \mathrm{PSL}_2(\mathbb{F}_q)$*. Then one of the following holds :*

1. $\mathrm{End}^0(J_f) = \mathbb{Q}$ *or a quadratic field.*
2. $q \equiv 3 \mod 4$ *and* $\mathrm{End}^0(J_f) \cong M_g(\mathbb{Q}(\sqrt{-q}))$*.*

A result of Lombardo

Theorem (Lombardo '19)

Let $f \in K[x]$ be an irreducible degree 5 polynomial. Then $\mathrm{End}^0(J_f)$ is a division algebra.

Improvements in genus 2

Theorem (G. '21)

Let $f(x) \in K[x]$ be a polynomial of degree 5 or 6, with $\mathrm{Gal}(f)$ containing an element of order 5. Then one of the following holds :

1. $\mathrm{End}(J_f) \cong \mathbb{Z}$.
2. $\mathrm{End}(J_f) \cong \mathbb{Z}\left[\frac{1+r\sqrt{D}}{2}\right]$*, where* $D \equiv 5 \mod 8$*,* $D > 0$ *and* $2 \nmid r$*.*
3. $\mathrm{End}(J_f) \cong R$*, where* R *is a 2-maximal order in a degree 4 CM field, which is totally inert at 2.*

Remark

Specifying $\mathrm{Gal}(f)$, we can give more information on $\mathrm{End}(J_f)$.

Higher genus

Theorem (G.'21)

Let A/K be an abelian variety of dimension g, with $\mathrm{Gal}(K(A[\ell]/K)$ containing an element of prime order $p = 2g+1$, and g satisfying some additional conditions. Then one of the following holds :

1. $\mathrm{End}^0(A)$ *is a number field, with restrictions on the primes above ℓ ;*
2. $\mathrm{End}^0(A) \cong M_a(F)$ *where $F \subsetneq \mathbb{Q}(\zeta_p)$ is a CM field and $a = \frac{2g}{[F:\mathbb{Q}]}$.*

Satisfied by $g = 1, 2, 3, 5, 6, 9, 11, 14, 18, 23, 26, 29, 30, 33, 35, 39, 41, \ldots$

Restrictions on the endomorphism field

Definition (Endomorphism field)

Let A/K be an abelian variety of dimension g. Denote by L/K the minimal extension over which all endomorphisms of A are defined.
E.g. $E : y^2 = x^3 - 2$ has $g = 1$ and $L = \mathbb{Q}(\zeta_3)$.

Theorem (G.'21)

Suppose $p = 2g + 1$ *is a prime divisor of* $[L : K]$*. Then* $\mathrm{End}^0(A) \cong M_a(F)$ *where* $F \subsetneq \mathbb{Q}(\zeta_p)$ *is a CM field and* $a = \frac{2g}{[F:\mathbb{Q}]}$*.*

Sketch of the proof

Proof sketch

1. First prove $A \sim B^n$ over $\bar{K}$ for some absolutely simple abelian variety B and an integer $n > 1$.
2. Then observe that $\mathrm{Gal}(L/K)$ acts faithfully on $\mathrm{End}^0(B^n) \cong M_n(D)$ by automorphisms, where $D \cong \mathrm{End}^0(B)$ is a finite dimensional division algebra (over $\mathbb{Q}$) satisfying $[D : \mathbb{Q}]n \leq 2g = p - 1$.
3. The Skolem-Noether Theorem then tells us we have a faithful representation

$$\rho : \mathrm{Gal}(L/K) \to \mathrm{PGL}_n(D).$$

4. This restricts D to be a subfield of $\mathbb{Q}(\zeta_p)$ and $[D : \mathbb{Q}]n = p - 1$. Which in turn implies B has CM by a proper subfield of $\mathbb{Q}(\zeta_p)$.

What do the examples say ?

Example

Jacobians with trivial endomorphism rings are quite common, so let's see some non trivial examples.

$\mathrm{Gal}(f)$	$\mathrm{End}(J_f)$	$f(x)$
F_5	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	$x^5 + 10x^3 + 20x + 5$
F_5	$\mathbb{Z}[\zeta_5]$	$x^5 - 2$
D_5	$\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$	$x^5 - 19x^4 + 107x^3 + 95x^2 + 88x - 16$
F_5	R	$52x^5 + 104x^4 + 104x^3 + 52x^2 + 12x + 1$

where R is the maximal order of the CM number field with defining polynomial $x^4 + x^3 + 2x^2 - 4x + 3$. We note that this field is cyclic, ramified only at 13, and 2 generates a maximal ideal.

Note also, when $\mathrm{Gal}(f) \cong F_5$ and J_f is of CM type, $\mathrm{End}^0(J_f)$ is isomorphic to the unique degree 4 extension of $\mathbb{Q}$ contained in $\mathbb{Q}(f)$.

What do the examples say ?

Example

Jacobians with trivial endomorphism rings are quite common, so let's see some non trivial examples.

$\mathrm{Gal}(f)$	$\mathrm{End}(J_f)$	$f(x)$
F_5	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	$x^5 + 10x^3 + 20x + 5$
F_5	$\mathbb{Z}[\zeta_5]$	$x^5 - 2$
D_5	$\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$	$x^5 - 19x^4 + 107x^3 + 95x^2 + 88x - 16$
F_5	R	$52x^5 + 104x^4 + 104x^3 + 52x^2 + 12x + 1$

where R is the maximal order of the CM number field with defining polynomial $x^4 + x^3 + 2x^2 - 4x + 3$. We note that this field is cyclic, ramified only at 13, and 2 generates a maximal ideal.

Note also, when $\mathrm{Gal}(f) \cong F_5$ and J_f is of CM type, $\mathrm{End}^0(J_f)$ is isomorphic to the unique degree 4 extension of $\mathbb{Q}$ contained in $\mathbb{Q}(f)$.

Missing examples

Example

For $A/\mathbb{Q}$ of dimension two and $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \supseteq C_5$ soluble, we have the following table :

	$\mathbb{Z}$	RM	CM
F_5	✓	✓	✓
D_5	✓	✓	?
C_5	✓	?	?

Missing examples

Example

For $A/\mathbb{Q}$ of dimension two and $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \supseteq C_5$ soluble, we have the following table :

	$\mathbb{Z}$	RM	CM
F_5	✓	✓	✓
D_5	✓	✓	?
C_5	✓	?	?

Ruling out the CM cases

Suppose A has CM. Then CM theory tells us that $\mathrm{Gal}(L/\mathbb{Q}) \cong C_4$.
We now look to understand $L \cap \mathbb{Q}(A[2])$.
A theorem of Silverberg tells us that $L \subseteq \mathbb{Q}(A[m])$ for $m \geq 3$.
This rules out the C_5 case.

A specialisation of Silverberg's theorem for $A[2]$

The D_5 CM case is ruled out by the following :

Theorem (G.'22)

Suppose $E = \mathrm{End}^0(A)$ is a (finite) Galois extension of $\mathbb{Q}$ and $L \not\subseteq K(A[2])$. The following hold :

- $\mathrm{Gal}(E/\mathbb{Q})$ *has a non-trivial normal elementary abelian 2-subgroup ;*
- *if* $\mathrm{End}(A)$ *is 2-maximal in* E*, then* 2 *is wildly ramified in* $E/\mathbb{Q}$*.*

In particular, if $E/\mathbb{Q}$ is Galois, $\mathrm{End}(A)$ is a 2-maximal order and 2 is not wildly ramified, then $L \subseteq K(A[2])$.

Corollary (G.'22)

Let $A\colon y^2 = f(x)$ be an elliptic curve defined over a number field with a real embedding. If $\mathrm{Gal}(f) \cong C_3$, then $\mathrm{End}(A) \cong \mathbb{Z}$.

Example (Silverman II)

The condition that $\mathrm{End}(A)$ is 2-maximal cannot be removed. Indeed, the elliptic curve $y^2 = (x+2)(x^2-2x-11)$ has CM by $\mathbb{Z}[\sqrt{-3}]$ and its 2-torsion field is $\mathbb{Q}(\sqrt{3})$. Likewise $y^2 = x^3 - x = x(x-1)(x+1)$ has CM by $\mathbb{Z}[i]$ and shows we can't remove the wild ramification condition.

Theorem (G.'22)

Let $A/\mathbb{Q}$ be an abelian variety of dimension $g \geq 1$ with $p = 2g + 1$ prime. Suppose $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \cong C_p$. Then either

- $\mathrm{End}^0(A) \subsetneq \mathbb{Q}(\zeta_p)$ *; or*
- $p \in \{7, 11, 19, 43, 67, 163\}$ *and* $\mathrm{End}^0(A) \cong M_g(\mathbb{Q}(\sqrt{-p}))$*.*

In particular there are only finitely many possibilities for $\mathrm{End}^0(A)$.

Corollary (G.'22)

Let $A/\mathbb{Q}$ be an abelian surface. Suppose $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \cong C_5$. Then either $\mathrm{End}(A) = \mathbb{Z}$ or $\mathrm{End}^0_{\overline{\mathbb{Q}}}(A) = \mathrm{End}^0(A) = \mathbb{Q}(\sqrt{5})$.

Theorem (G.'22)

Let $A/\mathbb{Q}$ be an abelian variety of dimension $g \geq 1$ with $p = 2g+1$ prime. Suppose $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \cong C_p$. Then either

- $\mathrm{End}^0(A) \subsetneq \mathbb{Q}(\zeta_p)$ *; or*
- $p \in \{7, 11, 19, 43, 67, 163\}$ *and* $\mathrm{End}^0(A) \cong M_g(\mathbb{Q}(\sqrt{-p}))$.

In particular there are only finitely many possibilities for $\mathrm{End}^0(A)$.

Corollary (G.'22)

Let $A/\mathbb{Q}$ be an abelian surface. Suppose $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \cong C_5$. Then either $\mathrm{End}(A) = \mathbb{Z}$ or $\mathrm{End}^0_{\mathbb{Q}}(A) = \mathrm{End}^0(A) = \mathbb{Q}(\sqrt{5})$.

Example (Wilson '00)

For $f(x) = x(x^5 - 4x^4 + 2x^3 + 5x^2 - 2x - 1)$ has $\mathrm{End}_{\mathbb{Q}}(J_f) = \mathrm{End}(J_f) \cong \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ and $\mathrm{Gal}(f) \cong C_5$.

Sketch of the proof

Let $E = \mathrm{End}^0_{\mathbb{Q}}(A)$. Recall $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q}) \cong C_p$.

- By Class Field Theory $\mathbb{Q}(A[2])/\mathbb{Q}$ is ramified at some odd prime q (for example by Kronecker-Weber and $[\mathbb{Q}(\zeta_{2^n}) : \mathbb{Q}] = 2^{n-1}$).
- Néron-Ogg-Shafarevich tells us the image of I_q on $T_\ell(A)$ for any ℓ contains an element of order p.
- Take a suitable ℓ satisfying $\langle \ell \rangle = \mathbb{Z}/p\mathbb{Z}^*$ and apply our earlier theorem.
- We find E is a field.
- $E \otimes \mathbb{Q}_\ell = \prod_{\lambda|\ell} E_\lambda$ induces a $G_{\mathbb{Q}}$-equivariant splitting $V_\ell = \prod_{\lambda|\ell} V_\lambda$.
- Each V_λ has E_λ dimension $\frac{2g}{[E:\mathbb{Q}]}$.
- For λ outside a finite set, consider the action of I_q on V_λ, and take the trace of our element of order p.
- This gives $[\mathbb{Q}(\zeta_p) \cap E : \mathbb{Q}] = [E : \mathbb{Q}]$ and hence $E \subseteq \mathbb{Q}(\zeta_p)$.
- The rest follows from a close study of the endomorphism field $L/\mathbb{Q}$.

Thanks for listening !