Endomorphism fields of abelian varieties

Notes by Tony Feng
for a talk by Kiran Kedlaya

June 14, 2016

1 Introduction

(This is joint work with R. Guralnick.)

Let A/K be an abelian variety of dimension g over a number field K. Define the *endomorphism field* of K to be "the" minimal field extension L of K such that

$$\mathrm{End}(A_L) \cong \mathrm{End}(A_{\overline{K}}).$$

Then L/K is a finite Galois extension.

Example 1.1. If E is a CM elliptic curve $K/\mathbb{Q}$ then L is an imaginary quadratic field.

Question. For fixed g, how large can $[L : K]$ be?

Theorem 1.2 (Silverberg '92)**.** *The degree* $[L : K]$ *divides* $2\prod_p p^{r(g,p)}$ *where* $r(g,p) = \sum_{i=0}^{\infty} \lfloor \frac{2g}{(p-1)p^i} \rfloor$.

Proof. For each prime $\ell \geq 3$, $\mathrm{Gal}(L/K)$ can be identified with a subquotient of $\mathrm{GSp}(2s, \mathbb{F}_\ell)$ via the action of Γ in ℓ-torsion points. The claimed bound then results from taking the gcd over ℓ. □

This looks like Minkowski's method for bounding the order of a finite subgroup of $\mathrm{GL}(n, \mathbb{Q})$. The method is to reduce mod $\mathbb{F}_\ell$ and take the gcd in a similar sense. The conclusion is that the order divides

$$\prod_p p^{\lfloor \frac{n}{p-1} \rfloor + \lfloor \frac{n}{(p-1)p} \rfloor + \ldots}$$

but for $p = 2$, the direct GCD gives the wrong answer, because one must add in archimedean considerations.

Comparison of bounds. We compare Silverberg's bound with the LCM of $[L : K]$ over all A, K.

g	Silverberg bound	Optimal bound
1	$2^4 \times 3$	2
2	$2^8 \times 3^2 \times 5$	$2^4 \times 3$
3	$2^{11} \times 3^4 \times 5 \times 7$	$2^6 \times 3^3 \times 7$

It's not surprising that there's an issue at 2. However, Silverberg's bound is also off by factors of 3 and 5, but at least in the $g = 3$ case is right for $p = 7$. This was the starting point for our project.

2 Where do these bounds come from?

2.1 The optimal bound for $g = 2$

For $g = 1$, the optimal bound is easy (either the curve has CM or not).

For $g = 2$, one enumerates all the options for $\mathrm{Gal}(L/K)$ for abelian surfaces. In joint work with Fité-Rotger-K.-Sutherland, we did this by the classification of Sato-Tate groups of abelian surfaces.

Conjecture 2.1 (Sato-Tate)**.** *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Setting*

$$a_p := \mathrm{Tr}\,\mathrm{Frob}_p = p + 1 - \#E(\mathbb{F}_p),$$

the distribution of $\frac{a_p}{\sqrt{p}} \in [-2, 2]$ is the distribution of the trace of a random matrix in SU(2)*.*

For A an abelian variety over K, we can define a compact Lie group $ST(A)$ for which one expects an analogous equidistribution statement for the characteristic polynomials of Frobenius. The recipe for this is essentially written in Serre's paper in the Motives volume, and is written somewhat more explicitly in my first paper with Bonaszak.

The group $ST(A)$ is defined in terms of Hodge cycles. If you know the Mumford-Tate conjecture for A, then you can express it in terms of ℓ-adic Galois representations.

The group of connected components of $ST(A)$ surjects onto $\mathrm{Gal}(L/K)$, and is an isomorphism if $g \leq 3$.

Unfortunately, this classification seems to be hard for $g \geq 3$. Instead, we use another interpretation of the group of connected components of $ST(A)$.

3 Results

3.1 Strategy

$ST(A)$ arises as a compact form of a certain reductive algebraic group over $\mathbb{Q}$, called the *algebraic Sato-Tate group* $AST(A)$. In particular, the group of connected components of $ST(A)$ and $AST(A)$ coincide.

Plan. Use a form of the Minkowski method for $AST(A)$, plus Archimedean considerations.

We described Minkowski's method for finite groups, but it turns out to work pretty well for algebraic groups. You look for integral models, and reduce modulo primes. So what we have to do is

- realize $AST(A) \subset \mathrm{Sp}(2g)_{\mathbb{Q}}$ over $\mathbb{Z}[1/N]$.
- reduce mod ℓ for $\ell \gg 0$.
- realize the component group as a subquotient of $\mathrm{Sp}(2g, \mathbb{F}_\ell)$.
- look very closely at extreme cases (occurring when the connected part is as small as possible).

3.2 Statement of results

Theorem 3.1 (G-K)**.** *For A an abelian variety of dimension g with endomorphism field L, $[L : K]$ divides $\prod p^{r'(g,p)}$ where*

$$r'(g,p) = \sum_{i=0}^{\infty} \begin{cases} r(g,p) - g - 1 & p = 2 \\ \max\{0, r(g,p) - 1\} & p = \textit{Fermat prime} \\ r(g,p) & \textit{otherwise}. \end{cases}$$

and this is the best possible.

3.3 Why the discrepancy for Fermat primes?

To extremize the power of p in $[L : K]$, you are forced to take A to be a twist of a power of a CM abelian variety. We can find an exact sequence

$$1 \to G_1 \to \pi_0(AST(A)) \to G_2 \to 0$$

where G_1 is the component group of $AST(A) \cap AST(A)^\circ \cdot Z$. So the point is to separate into the part that commutes with the connected component and the part that doesn't. The analysis of G_2 is combinatorial, while the G_1 is something in the domain of Minkowski's method.

To beat the bound $r(g,p)$ the point is that there is not enough room in G_1 unless $AST(A)^\circ$ is abelian. This forces you into CM situations. In particular, $A_{\overline{K}} \sim A_0^?$ where A_0 has CM in some subfield of $\mathbb{Q}(\zeta_p)$. In order to match this bound exactly, the subfield must be a *proper* subfield. (The reason is that we're looking inside PGL instead of GL, so the center doesn't contribute.)

The reason Fermat primes arise is that they are precisely the primes for which there is no CM subfield of $\mathbb{Q}(\zeta_p)$ which is proper.

For $p = 2$, a similar issue occurs.