

RESEARCH

Open Access



Endomorphism fields of abelian varieties

Robert Guralnick¹ and Kiran S. Kedlaya^{2*} 

*Correspondence:
kedlaya@ucsd.edu

²Department of Mathematics,
University of California, San
Diego, 9500 Gilman Drive #0112,
La Jolla, CA 92093, USA
Full list of author information is
available at the end of the article

Abstract

We give a sharp divisibility bound, in terms of g , for the degree of the field extension required to realize the endomorphisms of an abelian variety of dimension g over an arbitrary number field; this refines a result of Silverberg. This follows from a stronger result giving the same bound for the order of the component group of the Sato–Tate group of the abelian variety, which had been proved for abelian surfaces by Fité–Kedlaya–Rotger–Sutherland. The proof uses Minkowski’s reduction method, but with some care required in the extremal cases when p equals 2 or a Fermat prime.

1 Introduction

For A an abelian variety over a field K , the *endomorphism field* of A is the minimal algebraic extension L of K such that $\text{End}(A_L) = \text{End}(A_{\bar{L}})$. The purpose of this paper is to establish a bound on the degree $[L : K]$ in terms of the dimension of A ; more precisely, we compute the LCM of all possible degrees as A, K vary while $\dim_K A$ remains fixed.

Before stating our result, we state a prior result of Silverberg [8] which already contains many of the main ideas. For g a positive integer and p a prime, define

$$r(g, p) := \sum_{i=0}^{\infty} \left\lfloor \frac{2g}{(p-1)p^i} \right\rfloor.$$

Theorem 1.1 (Silverberg) *For A an abelian variety of dimension g over a number field K , the endomorphism field of A is a finite Galois extension of K of degree dividing $2 \times \prod_p p^{r(g,p)}$.*

The proof [8, Theorem 4.1] is elegantly simple: one verifies that for each prime $\ell > 2$, the Galois group of the endomorphism field extension is isomorphic (via its action on ℓ -torsion points) to a subquotient of the group $\text{Sp}(2g, \mathbb{F}_\ell)$. The bound is then obtained by taking the greatest common divisor of the orders of these finite groups. This echoes the method used by Minkowski to bound the order of a finite group of integer matrices (as exposed in [3]); we will return to this analogy a bit later.

From this proof, it is not clear whether one should expect the bound of Theorem 1.1 to be sharp. However, a moment’s thought shows that it is not sharp for $g = 1$: the bound is $2^4 \times 3$ but the optimal bound is obviously 2, with the worst case being an elliptic curve whose CM field is not contained in K . More seriously, for $g = 2$, the bound of Theorem 1.1 is $2^8 \times 3^2 \times 5$, but (as will be explained shortly) the work of Fité–Kedlaya–Rotger–Sutherland [2] implies that the optimal bound is $2^4 \times 3$. This raises the question

© The Author(s) 2017. This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

of identifying the discrepancy between Theorem 1.1 and the optimal bound, and this is achieved by our main result.

Theorem 1.2 *For A an abelian variety of dimension $g > 0$ over a number field K , the degree over K of the endomorphism field of A divides*

$$\prod_p p^{r'(g,p)}, \quad r'(g,p) := \begin{cases} r(g,p) - g - 1 & \text{if } p = 2; \\ \max\{0, r(g,p) - 1\} & \text{if } p \text{ is a Fermat prime}; \\ r(g,p) & \text{otherwise.} \end{cases}$$

Moreover, for fixed g, p (but varying over all K), this value of $r'(g, p)$ is best possible.

To give one more example, for $g = 3$, the bound from Theorem 1.1 is $2^{11} \times 3^4 \times 5 \times 7$ whereas the optimal bound is $2^6 \times 3^3 \times 7$. It is easy to see that the factor of 7 is necessary, e.g., by considering twists of the Klein quartic (see [5, §4]).

As in [2], our approach uses the relationship between the endomorphism field L of A and the Sato–Tate group of A ; the latter is a compact Lie group whose component group subjects canonically onto $\text{Gal}(L/K)$, and the bound we ultimately prove is for the order of the component group (see Theorem 5.4). The Sato–Tate group is constructed as a compact form of a certain linear algebraic group over \mathbb{Q} , the *algebraic Sato–Tate group*, which allows us to bound the order of the component group using a variant of Minkowski’s method. One key point is that the extremal cases occur for CM abelian varieties, for which the connected part of the algebraic Sato–Tate group is a torus which splits over a CM field; what distinguishes a Fermat prime p in this context is that $\mathbb{Q}(\mu_p)$ contains no proper subfield which is CM. (For $p = 2$, the same statement about $\mathbb{Q}(\mu_4)$ plays an analogous role.)

To prove that Theorem 1.2 is sharp, we use the relationship between twisting of abelian varieties and Sato–Tate groups; this reduces the problem to exhibiting abelian varieties admitting actions by large finite groups, which we achieve using CM abelian varieties and the same wreath product construction as in Minkowski’s theorem. Note that the fields of definition of the resulting abelian varieties are controlled by class groups of abelian number fields, so we are unable to establish lower bounds over any fixed number field.

To conclude this introduction, we comment on the subtler problem of giving bounds by size, rather than divisibility. As described in [3, §6], results of Weisfeiler and Feit can be combined with the classification of finite simple groups to show that for $n > 10$, the largest finite subgroups of $\text{GL}(n, \mathbb{Q})$ have order $2^n n!$ (and are unique up to conjugacy). For abelian varieties of sufficiently large dimension g , one would expect that the largest possible endomorphism field extension, and the largest possible component group of the Sato–Tate group, are obtained by twisting a power of an elliptic curve with j -invariant 0 using an automorphism group of order $6^g g!$ (note that these examples already occur over \mathbb{Q}). For the endomorphism field, this expectation has been confirmed by work of Rémond [6]; it is highly likely that a similar analysis applies to the component group (because the cases where the two differ tend not to have enough CM to trouble the bounds), but this would require some additional argument.

2 Group schemes

We start with some notation. Our notation choices are not entirely typical; they are made to help us distinguish between groups and group schemes.

Definition 2.1 For G a group scheme (over some base), we write G_X for the base extension of G to the base scheme X , and $G(X)$ for the group of X -valued points of G . We say that G is *pointful over X* if $G(X)$ occupies a Zariski-dense subset of G . By convention, all group schemes we consider will be smooth; the standard linear groups will be considered as schemes over \mathbb{Z} , and we will write $GL(n, X)$ instead of $GL(n)(X)$ and so on.

For G a group scheme over a connected base, let G° denote the identity connected component, and write $\pi_0(G) := G/G^\circ$ for the group of connected components, viewed as a finite group scheme over the same base. If G is pointful, then so are both G° and G/G° .

For L/K a finite extension of fields and G a group scheme over $\text{Spec } L$, write $\text{Res}_K^L G$ for the Weil restriction of scalars of G to $\text{Spec } K$.

Example 2.2 For n a positive integer, the n -torsion subscheme of the multiplicative group over \mathbb{Q} is the group scheme $\text{Spec } \mathbb{Q}[x]/(x^n - 1)$ which is obviously defined over \mathbb{Q} . However, it is only pointful for $n = 1, 2$.

Definition 2.3 For G a group scheme, let $\text{Out}(G)$ be the group scheme of outer automorphisms of G , i.e., the cokernel of the map $G \rightarrow \text{Aut}(G)$ induced by conjugation. Note that for G a group scheme over a field k which is not algebraically closed, an element of $\text{Aut}(G)(k)$ may map trivially to $\text{Out}(G)(k)$ even though it does not come from the image of $G(k)$; that is, the scheme-theoretic notion of an outer automorphism disagrees with the group-theoretic notion because the latter is not stable under base extension.

3 Minkowski’s method

We next formulate our version of Minkowski’s reduction method. We implicitly follow [3], but see also [7] for another detailed treatment (both considering only finite groups).

Throughout Sect. 3, let G be a group scheme over a number field K .

Definition 3.1 By convention G is a scheme of finite type over K , so it can be extended to a group scheme over $\mathfrak{o}_K[1/N]$ for some positive integer N . In particular, it makes sense to form the base extension of G to $\mathbb{F}_q := \mathfrak{o}_K/\mathfrak{q}$ for all but finitely many prime ideals \mathfrak{q} of \mathfrak{o}_K .

Let H be a finite pointful subquotient group scheme of G . By the previous paragraph, $H(K)$ is isomorphic to a subquotient of $G(\mathbb{F}_q)$ for all but finitely many \mathfrak{q} ; in particular, for each prime p , any p -Sylow subgroup of $H(K)$ is isomorphic to a subquotient of a p -Sylow subgroup of $G(\mathbb{F}_q)$ for all but finitely many \mathfrak{q} .

To translate this into a numerical bound, define the nonnegative integers $r(G, p)$ by the formula

$$\prod_p p^{r(G,p)} = \sup_S \left\{ \gcd \#G(\mathbb{F}_q) \right\}$$

where S runs over all cofinite sets of prime ideals of \mathfrak{o}_K . Then the preceding discussion implies that H has order dividing $\prod_p p^{r(G,p)}$; in particular, this bound applies to the component group of any pointful subgroup scheme of G .

We collect some remarks related to this construction.

Remark 3.2 Suppose that there exists a finite pointful subquotient group scheme H of G such that the p -part of $\#H$ equals the upper bound $p^{r(G,p)}$. Let P be a p -Sylow subgroup of H ; then for infinitely many q , P has the same cardinality as a p -Sylow subgroup of $G(\mathbb{F}_q)$, so by Sylow’s theorem the two must be isomorphic. That is, the isomorphism type of P is uniquely determined by G .

Remark 3.3 Let H be a pointful subgroup scheme of G . Then $\#\pi_0(H)$ divides $\prod_p p^{r(G,p)-\delta(G,p)}$ for

$$\prod_p p^{\delta(G,p)} = \inf_S \left\{ \gcd_{q \in S} \#H^\circ(\mathbb{F}_q) \right\}.$$

Remark 3.4 In light of Wedderburn’s theorem, for any number field K and any twisted form G of $\mathrm{GL}(n)_K$ one has $r(G, p) = r(\mathrm{GL}(n)_K, p)$.

Remark 3.5 For each prime p , the group $C_p \wr S_{\lfloor n/(p-1) \rfloor}$ embeds into $\mathrm{GL}(n, \mathbb{Q})$, as then do its p -Sylow subgroups. The original theorem of Minkowski asserts that the conjugates of the latter are the largest possible p -subgroups of $\mathrm{GL}(n, \mathbb{Q})$. However, if we compare this to the values

$$\begin{aligned} r(\mathrm{GL}(n)_{\mathbb{Q}}, p) &= \left\lfloor \frac{n}{p-1} \right\rfloor + \left\lfloor \frac{n}{p(p-1)} \right\rfloor + \left\lfloor \frac{n}{p^2(p-1)} \right\rfloor + \dots \quad (p > 2) \\ r(\mathrm{GL}(n)_{\mathbb{Q}}, 2) &= n + 2 \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \dots, \end{aligned}$$

we see that the Minkowski bound is only sharp for $p > 2$; for $p = 2$, the Minkowski bound is too large by $\lfloor \frac{n}{2} \rfloor$, and one must supplement using some extra analysis involving quadratic forms over finite fields [3, §5]. For this reason, we do not know whether the example $C_p \wr S_{\lfloor n/(p-1) \rfloor}$ is optimal also for subquotients when $p = 2$.

Remark 3.6 For K a number field, the Chebotarev density theorem implies that $r(\mathrm{GL}(n)_K, p)$ depends only on $K \cap \mathbb{Q}(\mu_{p^\infty})$. For

$$\begin{aligned} m(K, p) &:= \min\{m \geq 1 : K \cap \mathbb{Q}(\mu_{p^m}) = K \cap \mathbb{Q}(\mu_{p^\infty})\} \\ t(K, p) &:= [\mathbb{Q}(\mu_{p^{m(K,p)}}) : K \cap \mathbb{Q}(\mu_{p^{m(K,p)}})], \end{aligned}$$

for $p > 2$ we have

$$r(\mathrm{GL}(n)_K, p) = m(K, p) \left\lfloor \frac{n}{t(K, p)} \right\rfloor + \left\lfloor \frac{n}{pt(K, p)} \right\rfloor + \left\lfloor \frac{n}{p^2t(K, p)} \right\rfloor + \dots \tag{3.1}$$

and this bound is again optimal (see [3, §5.3] for a detailed discussion).

For $p = 2$, the situation depends crucially on whether $\mathbb{Q}(\zeta_4) \subseteq K$. If so, then $t(K, 2) = 1$,

$$r(\mathrm{GL}(n)_K, 2) = m(K, 2)n + \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \dots, \tag{3.2}$$

and this bound is optimal, achieved by $C_{2^{m(K,2)}} \wr S_n$. If not, the situation is more complicated; we limit ourselves to observing that for $K = \mathbb{Q}(\sqrt{-2})$ we have $r(\mathrm{GL}(n)_K, 2) = r(\mathrm{GL}(n)_{\mathbb{Q}}, 2)$, while for $K = \mathbb{Q}(\sqrt{2})$ we have $r(\mathrm{GL}(n)_K, 2) = r(\mathrm{GL}(n)_{\mathbb{Q}}, 2) + \lfloor \frac{n}{2} \rfloor$.

Remark 3.7 Although we do not need this for our main result, we note in passing the following corollary of Remark 3.6 (which only affects the prime $p = 2$): the optimal divisibility bound for the order of a finite subgroup of $\mathrm{Sp}(2g, \mathbb{Q})$ is $2^{r(\mathrm{GL}(g)_{\mathbb{Q}(i), 2})} \prod_{p>2} p^{r(\mathrm{GL}(2g), p)}$. This comes down to the fact that any irreducible finite subgroup of $\mathrm{Sp}(2g, \mathbb{Q})$ is centralized by some totally imaginary number field [4, Lemma 2.3].

Remark 3.8 It is natural to use Minkowski’s method as a starting point for bounding the order of finite subgroups of any reductive group over any field. This has been discussed extensively by Serre [7].

4 Comparison of Minkowski bounds

For our purposes, it will be important to compare the Minkowski bounds for various group/subgroup pairs. The key points will be to identify discrepancies for $p = 2$, and to isolate cases for $p > 2$ where the bound for the subgroup matches that of the full group.

Remark 4.1 A trivial but useful observation along these lines is that for $n \geq 1, p > 2, d > 1$,

$$r(\mathrm{GL}(dn)_{\mathbb{Q}}, p) > r(\mathrm{GL}(n)_{\mathbb{Q}}, p) \quad \text{whenever } r(\mathrm{GL}(dn)_{\mathbb{Q}}, p) > 0.$$

A slightly less trivial observation is that for $n \geq 1$,

$$r(\mathrm{GL}(n)_{\mathbb{Q}(i)}, 2) > r(\mathrm{GL}(n)_{\mathbb{Q}}, 2).$$

Lemma 4.2 *Let K be a number field of degree d over \mathbb{Q} . For each integer $n \geq 1$ and each odd prime p ,*

$$r(\mathrm{GL}(dn)_{\mathbb{Q}}, p) \geq r(\mathrm{GL}(n)_K, p) + r(S_d, p);$$

moreover, if $n > 1$ and $m(K, p) > 1$, or if $d \geq p(p - 1)$, then the inequality is strict.

Proof There is nothing to check when $d = 1$, so we may assume $d \geq 2$. Put $m = m(K, p), t = t(K, p)$; then the desired inequality is

$$\left\lfloor \frac{dn}{p-1} \right\rfloor + \left\lfloor \frac{dn}{p(p-1)} \right\rfloor + \dots \geq m \left\lfloor \frac{n}{t} \right\rfloor + \left\lfloor \frac{n}{pt} \right\rfloor + \dots + \left\lfloor \frac{d}{p} \right\rfloor + \left\lfloor \frac{d}{p^2} \right\rfloor + \dots.$$

From the equality $dt = p^{m-1}(p - 1)$, we see that $\frac{d}{p-1}$ equals $\frac{1}{t}$ times the integer p^{m-1} which is no less than m (and strictly greater than m if $m > 1$). Consequently, by writing the difference between the two sides as

$$\left\lfloor \frac{dn}{p-1} \right\rfloor - m \left\lfloor \frac{n}{t} \right\rfloor + \left\lfloor \frac{dn}{p(p-1)} \right\rfloor - \left\lfloor \frac{n}{pt} \right\rfloor + \dots + \left\lfloor \frac{d}{p} \right\rfloor + \left\lfloor \frac{d}{p^2} \right\rfloor + \dots,$$

we see that this difference does not decrease if we increase n by 1 (and strictly increases if $m > 1$). If $n = 1$, then the desired inequality becomes $r(\mathrm{GL}(d)_{\mathbb{Q}}, p) \geq r(S_d, p)$, which holds because S_d embeds into $\mathrm{GL}(d, \mathbb{Q})$; this equality is strict whenever $d \geq p(p - 1)$. This proves the claim. □

Corollary 4.3 *For K a number field of degree d , for $p > 2$ we have*

$$r(\mathrm{GL}(dn)_{\mathbb{Q}}, p) \geq r(\mathrm{Aut}(K/\mathbb{Q}) \times \mathrm{Res}_{\mathbb{Q}}^K \mathrm{GL}(n)_K, p). \tag{4.1}$$

Moreover, if $K \not\subseteq \mathbb{Q}(\mu_p), K$ is not the degree- p subextension of $\mathbb{Q}(\mu_{p^2})$, and $r(\mathrm{GL}(dn)_{\mathbb{Q}}, p) \neq 0$, then the equality is strict.

Proof The inequality (4.1) holds because $\text{Aut}(K/\mathbb{Q}) \times \text{Res}_{\mathbb{Q}}^K \text{GL}(n)_K$ embeds into $\text{GL}(dn)_{\mathbb{Q}}$. We thus only need to obtain a contradiction assuming that $K \not\subseteq \mathbb{Q}(\mu_p)$, K is not the degree- p subextension of $\mathbb{Q}(\mu_{p^2})$, $r(\text{GL}(dn)_{\mathbb{Q}}, p) > 0$, and equality holds in (4.1).

Note that (4.1) also follows from Lemma 4.2, so equality must also hold in the latter. By Remark 3.6, if $K' := K \cap \mathbb{Q}(\mu_{p^\infty})$ has degree $d' \neq d$, then $r(\text{GL}(n)_K, p) = r(\text{GL}(n)_{K'}, p)$; we then get the strict inequality by applying Lemma 4.2 to the field K' and invoking Remark 4.1 (using the condition that $r(\text{GL}(dn)_{\mathbb{Q}}, p) > 0$). We must therefore have $K = K'$ and hence $K \subseteq \mathbb{Q}(\mu_{p^\infty})$; since we assumed $K \not\subseteq \mathbb{Q}(\mu_p)$, this implies that $m(K, p) > 1$. To have equality in Lemma 4.2, we must then have $n = 1$ and $d < p(p - 1)$.

Since $m(K, p) > 1$, K must contain the degree- p subextension of $\mathbb{Q}(\mu_{p^2})$, necessarily strictly by hypothesis; hence d/p is an integer strictly greater than 1. By the bound on d , we cannot then have $\mathbb{Q}(\mu_p) \subseteq K$, so $r(\text{GL}(1)_K, p) = 0$. Meanwhile, K is an abelian extension of \mathbb{Q} , so $r(\text{Aut}(K/\mathbb{Q}), p) = 1$. However, since $d \geq 2p$, $r(\text{GL}(d)_{\mathbb{Q}}, p) \geq 2$, yielding the desired contradiction. \square

Corollary 4.4 *For any integers $n, d > 1$, for each odd prime p for which $r(\text{GL}(nd)_{\mathbb{Q}}, p) > 0$, we have*

$$r(\text{GL}(dn)_{\mathbb{Q}}, p) > r(\text{GL}(n)_{\mathbb{Q}}, p) + r(S_d, p).$$

Proof We first reduce to the case where d is even. Namely, we may do this by replacing d with $2 \lfloor \frac{d}{2} \rfloor$ except if d is odd, $r(\text{GL}(dn)_{\mathbb{Q}}, p) > 0$, and $r(\text{GL}((d - 1)n)_{\mathbb{Q}}, p) = 0$. This implies $(d - 1)n < p - 1 \leq dn$, which implies on one hand that $n < p - 1$ and $r(\text{GL}(n)_{\mathbb{Q}}, p) = 0$, and on the other hand that $d - 1 < p - 1$ and so $r(S_d, p) = 0$; this yields the claimed inequality.

For any number field K of even degree d , by Lemma 4.2 we have

$$r(\text{GL}(dn)_{\mathbb{Q}}, p) \geq r(\text{GL}(n)_K, p) + r(S_d, p) \geq r(\text{GL}(n)_{\mathbb{Q}}, p) + r(S_d, p),$$

so it suffices to confirm that both equalities cannot hold simultaneously. Since we are free to choose K , we take it to contain the quadratic subfield of $\mathbb{Q}(\mu_p)$; then by Remark 3.6, we have $r(\text{GL}(n)_K, p) > r(\text{GL}(n)_{\mathbb{Q}}, p)$ unless both quantities equal zero. It thus suffices to rule out the equality $r(\text{GL}(dn)_{\mathbb{Q}}, p) = r(S_d, p)$; since $r(\text{GL}(d)_{\mathbb{Q}}, p) \geq r(S_d, p)$, this follows from Remark 4.1. \square

For $p = 2$, we have the following analogue of Corollary 4.3.

Remark 4.5 For K/F an extension of number fields of degree d , we obviously have

$$r(\text{GL}(dn)_F, 2) \geq r(\text{Aut}(K/F) \times \text{Res}_F^K \text{GL}(n)_K, 2).$$

In case $F = \mathbb{Q}(i)$, one can show using Remark 3.2 that equality holds only when $d = 1$; however, we will not need this.

For $p = 2$, we have the following analogue of Corollary 4.4.

Lemma 4.6 *For any integers $n, d > 1$ such that $g = dn/2$ is an integer,*

$$r(\text{GL}(g)_{\mathbb{Q}(i)}, 2) \geq r(\text{GL}(n)_{\mathbb{Q}}, 2) + r(S_d, 2)$$

with equality only for $(n, d) = (2, 2)$.

Proof We are claiming that

$$dn + \left\lfloor \frac{dn}{4} \right\rfloor + \left\lfloor \frac{dn}{8} \right\rfloor + \cdots \geq n + 2 \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \cdots + \left\lfloor \frac{d}{2} \right\rfloor + \left\lfloor \frac{d}{4} \right\rfloor + \cdots$$

with equality only for $(n, d) = (2, 2)$. For $d = 2$, this inequality becomes $n \geq \lfloor \frac{n}{2} \rfloor + 1$; for $n = 2$, it becomes $2d \geq 4$. It thus remains to check the cases where $n, d \geq 3$.

We may write the difference between the two sides as

$$(d - 1)n + \left(\left\lfloor \frac{dn}{4} \right\rfloor - \left\lfloor \frac{d}{2} \right\rfloor \right) + \left(\left\lfloor \frac{dn}{8} \right\rfloor - \left\lfloor \frac{d}{4} \right\rfloor \right) + \cdots - 2 \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{4} \right\rfloor - \cdots;$$

in particular, for $n \geq 2$ fixed, this difference increases if we increase d by 2. Using the previous paragraph, we deduce the claim when d is even. For d odd, we may argue that

$$\begin{aligned} r(\mathrm{GL}(g)_{\mathbb{Q}(i)}, 2) &\geq r(\mathrm{GL}(g - n/2)_{\mathbb{Q}(i)}, 2) \geq r(\mathrm{GL}(n)_{\mathbb{Q}}, 2) + r(S_{d-1}, 2) \\ &= r(\mathrm{GL}(n)_{\mathbb{Q}}, 2) + r(S_d, 2) \end{aligned}$$

with strict inequality if $n > 2$. □

5 Abelian varieties and Sato–Tate groups

We now specialize to the cases of interest for abelian varieties.

Definition 5.1 For A an abelian variety over a number field K , let $\mathrm{AST}(A)$ denote the algebraic Sato–Tate group of A in the sense of [1, Definition 9.5]. The key properties that we need are the following.

- The group scheme $\mathrm{AST}(A)$ is a pointful subgroup scheme of $\mathrm{Sp}(2g)_{\mathbb{Q}}$ whose connected part is reductive. The connected part is closely related to the Mumford–Tate group of A .
- There exists a torus $T \subset \mathrm{AST}(A)_{\mathbb{C}}^{\circ}$ which acts on \mathbb{C}^{2g} with weights $1, -1$ each with multiplicity g . In particular, the fixed space of $\mathrm{AST}(A)$ is the zero subspace.
- The component group $\pi_0(A)$ surjects onto $\mathrm{Gal}(L/K)$ for L the endomorphism field of A ; this map is a bijection whenever the Mumford–Tate group is completely explained by endomorphisms (which holds in all cases when $g \leq 3$ but can fail for $g \geq 4$, as originally shown by Mumford). Moreover, for K' a finite extension of K , $\mathrm{AST}(A_{K'})$ is the inverse image of $\mathrm{Gal}(LK'/K') \subseteq \mathrm{Gal}(L/K)$ in $\mathrm{AST}(A)$.
- Any decomposition of \mathbb{Q}^{2g} into indecomposable $\mathrm{AST}(A)$ -modules corresponds to a product-up-to-isogeny decomposition of A .
- The group $\mathrm{AST}(A)$ is a torus if and only if A is isogenous to a product of abelian varieties with CM defined over K .

Example 5.2 Put

$$M_1 := \mathbb{Q}(i), M_2 := \mathbb{Q}(\sqrt{-2}), M_3 := \mathbb{Q}(\sqrt{-3}), M_4 := \mathbb{Q}(\sqrt{-6})$$

and let K be the compositum of these four fields. Let A be the product of four elliptic curves E_1, \dots, E_4 with CM by M_1, \dots, M_4 , respectively. Then $\mathrm{AST}(A)$ is a torus of dimension 3.

Remark 5.3 The Sato–Tate group of A , as studied for abelian surfaces in [2], is a maximal compact subgroup of $\mathrm{AST}(A, \mathbb{C})$; it therefore has the same component group as $\mathrm{AST}(A)$. On one hand, this means that the argument using algebraic Sato–Tate groups in the proof of Theorem 5.4 directly applies also to the component groups of Sato–Tate groups; on

the other hand, the conclusion of Theorem 5.4 in the case $g = 2$ is a consequence of [2, Theorem 4.3], which will save a bit of case analysis.

We prove the upper bound assertion of Theorem 1.2 by establishing the following result.

Theorem 5.4 *For A an abelian variety of dimension g over a number field K , the component group of the algebraic Sato–Tate group of A (or equivalently, the Sato–Tate group of A) has order dividing $\prod_p p^{r'(g,p)}$.*

Proof Put $G = \text{AST}(A)$. It suffices to check the claimed divisibility for the p -part of $\#\pi_0(G)$; this is immediate from Remark 3.5 (applied with $n = 2g$) unless $p = 2$ or p is a Fermat prime. In light of Remark 5.3, we may assume further that $g \geq 3$.

Note that for any fixed p , $r'(g, p)$ is superadditive in g ; we may thus reduce to the case where A is indecomposable, which as noted above implies that G acts indecomposably on $V = \mathbb{Q}^{2g}$. Using Corollary 4.4 and Lemma 4.6, we may also deduce the claim in case G° does not act isotypically on V (the exceptional case of Lemma 4.6 cannot occur for $g \geq 3$). We may thus assume hereafter that G° acts isotypically on V .

Let W be an irreducible G° -representation occurring in V , and put

$$D := \text{End}_{G^\circ}(W), \quad M := \text{End}_{G^\circ}(V), \quad F := Z(D) = Z(M).$$

By Schur’s lemma, D is a division algebra, M is a matrix ring over D , and $T := \text{image}(G^\circ \rightarrow M^\times)$ is a torus which splits over F . If we define $H := \ker(G \rightarrow \text{Out}(G^\circ))$, we obtain an induced injective morphism $H/G^\circ \hookrightarrow M^\times/T$. Meanwhile, since V is G° -isotypical, G/H acts faithfully on the set of isomorphism classes of G° -constituents of $W \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$; this implies that the map $G \rightarrow \text{Aut}(F/\mathbb{Q})$ induces an injective morphism $G/H \hookrightarrow \text{Aut}(F/\mathbb{Q})$.

Define the following positive integers:

$$\begin{aligned} a &:= [F : \mathbb{Q}]; \\ b &:= \text{rank}_F D = \text{the } G^\circ\text{-multiplicity of } W \otimes_F \overline{F}; \\ c &:= \text{rank}_D M = \text{the } G^\circ\text{-multiplicity of } W \text{ in } V; \\ d &:= \frac{2g}{abc} = \text{the } \overline{\mathbb{Q}}\text{-dimension of a } G^\circ\text{-constituent of } V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}. \end{aligned}$$

In this notation, G/H injects into S_a while H/G° injects into a subgroup of a twisted form of $\text{GL}(bc)_F$. In light of Remark 3.4, it follows that the p -adic valuation of $\#\pi_0(G)$ is at most

$$r(\text{Aut}(F/\mathbb{Q}), p) + r(\text{GL}(bc)_F, p) \leq r(\text{GL}(abc)_{\mathbb{Q}}, p). \tag{5.1}$$

If $d > 1$, then Remark 4.1 immediately yields the desired bound (even for $p = 2$). We may thus assume hereafter that $d = 1$, which implies that G° is abelian and hence a torus. In this case, F must be totally imaginary; it is in fact the CM field associated to the unique simple isogeny factor of A .

If $p > 2$ is a Fermat prime, then the only way to violate the desired bound would be to have equality in (5.1), which can only occur if $F \subseteq \mathbb{Q}(\mu_p)$ in light of Corollary 4.3 (the degree- p subextension of $\mathbb{Q}(\mu_{p^2})$ cannot be a compositum of CM fields because its degree is odd). Since F is totally imaginary, this would force $F = \mathbb{Q}(\mu_p)$. However, under these conditions, we may invoke Remark 3.3: the reduction of G° itself always has order divisible by p , yielding exactly the correct bound.

If $p = 2$ and $F \cap \mathbb{Q}(\mu_{2^\infty}) = \mathbb{Q}$, then $r(\mathrm{GL}(n)_F, 2) = r(\mathrm{GL}(n)_{\mathbb{Q}}, 2)$ (see Remark 3.6) and so we may invoke Lemma 4.6 to deduce the desired result (again assuming that $g \geq 3$). If instead $\mathbb{Q}(\mu_4) \subseteq F$, then Remark 4.5 gives a valuation bound which is only off by 2, and again this discrepancy is accounted for by Remark 3.3 (the reduction of G° itself always has order divisible by 4). Otherwise, $F' := F \cap \mathbb{Q}(\mu_8)$ must equal one of $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$. In case $F' = \mathbb{Q}(\sqrt{-2})$, Remark 3.6 implies that $r(\mathrm{GL}(n)_{F'}, 2) = r(\mathrm{GL}(n)_{\mathbb{Q}}, 2)$; we thus obtain an upper bound of

$$r(\mathrm{Aut}(F'/\mathbb{Q}), 2) + r(\mathrm{GL}(abc/2)_{F'}, 2) = 1 + r(\mathrm{GL}(g)_{\mathbb{Q}}, 2)$$

and again Lemma 4.6 settles the question (for $g \geq 3$).

In case $F' = \mathbb{Q}(\sqrt{2})$, we must argue a bit more carefully. Since F' is Galois and totally real, we must have $F' \neq F$ and $r(\mathrm{Aut}(F/\mathbb{Q}), 2) = 1 + r(\mathrm{Aut}(F/F'), 2)$. By Remark 3.6, we have

$$r(\mathrm{GL}(n)_F, 2) = r(\mathrm{GL}(n)_{F'}, 2) = r(\mathrm{GL}(n)_{\mathbb{Q}}, 2) + \left\lfloor \frac{n}{2} \right\rfloor.$$

Note finally that the reduction of G° always has order divisible by 2. From (5.1), we now obtain an upper bound of

$$r(\mathrm{Aut}(F/F'), 2) + r(\mathrm{GL}(bc)_{\mathbb{Q}}, 2) + \left\lfloor \frac{bc}{2} \right\rfloor$$

which by Lemma 4.6 (and the fact that $a \geq 4$) is itself bounded above by

$$r(\mathrm{GL}(g)_{\mathbb{Q}}, 2) + \left\lfloor \frac{g}{a} \right\rfloor \leq r(\mathrm{GL}(g)_{\mathbb{Q}}, 2) + \left\lfloor \frac{g}{4} \right\rfloor.$$

This gives the desired bound once more. □

6 Lower bounds

To conclude, we establish the lower bound assertion of Theorem 1.2 by twisting powers of CM abelian varieties.

Definition 6.1 We briefly recall [2, Definition 2.20]. Let A be an abelian variety over a number field K , let L/K be a finite Galois extension, and let $f : \mathrm{Gal}(L/K) \rightarrow \mathrm{Aut}(A_L)$ be a 1-cocycle. Then there exists an abelian variety A^f over K equipped with an isomorphism $A_L^f \cong A_L$ such that the action of $\tau \in G_K$ on $A^f(\bar{K}) \cong A_L^f(\bar{K})$ corresponds to the action of $f(\tau)\tau$ on $A(\bar{K}) \cong A_L(\bar{K})$. The isomorphism $A_L^f \cong A_L$ induces an isomorphism $\mathrm{End}(A_L^f) \cong \mathrm{End}(A_L)$ in which corresponding elements $\alpha \in \mathrm{End}(A_L^f)$, $\beta \in \mathrm{End}(A_L)$ satisfy the relation

$$\tau(\alpha) = f(\tau)\tau(\beta)f(\tau)^{-1}. \tag{6.1}$$

We use the twisting setup in the following setting.

Definition 6.2 Fix a prime p and a positive integer m . Let A_0 be an abelian variety of dimension g_0 over some number field K , such that A_0 has complex multiplication by the ring of integers \mathfrak{o}_M of a subfield M of $\mathbb{Q}(\mu_{p^m})$; put $d = [\mathbb{Q}(\mu_{p^m}) : M]$. (Note that we cannot hope to fix the field K , because its degree over \mathbb{Q} is related to the class number of M .) Let $G_0 \subseteq \mathrm{GL}(d, M)$ be a subgroup of order p^m stable under $\mathrm{Gal}(M/\mathbb{Q})$ and identify G_0 with a subgroup of $\mathrm{Aut}(A_{0, KM}^d)$. Put $A_1 = A_0^{dn}$ for some positive integer n ; then $G_1 = G_0 \wr S_n$ may be identified with a subgroup of $\mathrm{Aut}(A_{1, KM})$ stable under $\mathrm{Gal}(KM/K)$. Let G be the image of G_1 under the map $\mathrm{GL}(dn, M) \rightarrow \mathrm{PGL}(dn, M)$.

Choose an S_n -extension L_0/K linearly disjoint from KM , so that L_0M/KM is again an S_n -extension. Note that for a “generic” C_{p^m} -extension L_1/L_0M , the Galois closure L_2 of L_1 over M will have Galois group $G_0 \wr S_n$. Using class field theory, we may further ensure that L_2 is also Galois over K and that there exists a 1-cocycle $f : \text{Gal}(L_2/K) \rightarrow \text{Aut}(A_{1,L_2})$ whose restriction to $\text{Gal}(L_2/KM)$ is the preceding identification of the latter with $G_0 \wr S_n \subseteq \text{Aut}(A_{1,KM})$.

Put $A = A_1^f$ and let L be the endomorphism field of A . Then $KM \subseteq L$ and (6.1) implies the existence of a surjective morphism from $\text{Gal}(L/KM)$ to G , but not in general to G_1 .

Theorem 6.3 *For each prime p , there exists an abelian variety A of dimension g over some number field K such that the p -part of $[L : K]$ is at least $p^{r_{g,p}}$.*

Proof Suppose first that $p - 1$ is not a power of 2 (i.e., p is odd and not a Fermat prime). Then there exists a subfield M of $\mathbb{Q}(\mu_p)$ whose index ℓ is an odd prime divisor of $p - 1$. Applying Definition 6.2 with $m = 1$, $n = \lfloor \frac{g}{p-1} \rfloor$ then yields the desired result; note that in this case, there is no harm to take K to contain M , which simplifies the analysis somewhat.

Suppose next that p is a Fermat prime; we may assume that $r_{g,p} \geq 1$. The previous construction breaks down because $p - 1$ admits no odd prime divisor, so we can only apply Definition 6.2 with $m = 1$, $M = \mathbb{Q}(\mu_p)$, $n = \lfloor \frac{g}{p-1} \rfloor$. Note that we now lose one factor of p to the quotient map $G_1 \rightarrow G$, so again we get the desired result.

Suppose finally that $p = 2$. Apply Definition 6.2 with $m = 2$, $M = \mathbb{Q}(i)$, $n = g$; note that in this case we may even take $K = \mathbb{Q}$. This time, we lose two factors of 2 to the quotient map $G_1 \rightarrow G$, but gain one back from the extension M/\mathbb{Q} . This proves the claim once more. \square

Author details

¹Department of Mathematics, University of Southern California, 3620 S. Vermont Ave., KAP 104, Los Angeles, CA 90089-2532, USA, ²Department of Mathematics, University of California, San Diego, 9500 Gilman Drive #0112, La Jolla, CA 92093, USA.

Acknowledgements

Thanks to Francisc Fité, Gaël Rémond, Jean-Pierre Serre, Alice Silverberg, and Andrew Sutherland for feedback. Guralnick was partially supported by NSF Grants DMS-1302886 and DMS-1600056. Kedlaya was supported by NSF Grant DMS-1501214 and UC San Diego (Warschawski Professorship).

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 21 April 2017 Accepted: 7 July 2017

Published online: 06 November 2017

References

1. Banaszak, G., Kedlaya, K.S.: An algebraic Sato–Tate group and Sato–Tate conjecture. *Indiana Univ. Math. J.* **64**, 245–274 (2015)
2. Fité, F., Kedlaya, K.S., Rotger, V., Sutherland, A.V.: Sato–Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.* **148**, 1390–1442 (2012)
3. Guralnick, R. M., Lorenz, M.: Orders of finite groups of matrices. In: *Groups, Rings and Algebras: Proceedings of a Conference in Honor of Donald S. Passman*, Contemporary Math, vol. 420, pp. 141–162 (2006)
4. Kirschmer, M.: Finite symplectic matrix groups. *Exp. Math.* **20**, 217–228 (2011)
5. Poonen, B., Schaefer, E.F., Stoll, M.: Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$. *Duke Math. J.* **137**, 103–158 (2007)
6. Rémond, G.: Degré de définitions des endomorphismes d’une variété abélienne, preprint <https://www-fourier.ujf-grenoble.fr/~remond/>
7. Serre, J.-P.: Bounds for the Orders of the Finite Subgroups of $G(k)$, in *Group Representation Theory*. EPFL Press, Lausanne (2007)
8. Silverberg, A.: Fields of definition for homomorphisms of abelian varieties. *J. Pure Appl. Algebra* **77**, 253–262 (1992)