ESSENTIAL DIMENSION OF ABELIAN VARIETIES OVER NUMBER FIELDS

PATRICK BROSNAN AND RAMESH SREEKANTAN

ABSTRACT. We affirmatively answer a conjecture in the preprint "Essential dimension and algebraic stacks," proving that the essential dimension of an abelian variety over a number field is infinite.

Let k be a field and let Fields_k denote the category whose objects are field extensions L/k and whose morphisms are inclusions $L \hookrightarrow M$ of fields. Let $F : \mathrm{Fields}_k \to \mathrm{Sets}$ be a covariant functor. A *field of definition* for an element $a \in F(L)$ is a subfield M of L over k such that $a \in \mathrm{im}(F(M) \to F(L))$. The *essential dimension* of $a \in F(L)$ is $\mathrm{ed}\, a := \inf\{\mathrm{trdeg}_k M \,|\, M \text{ is a field of definition for } a\}$. The essential dimension of the functor F is $\mathrm{ed} F := \sup\{\mathrm{ed}\, a \,|\, L \in \mathrm{Fields}_k, a \in F(L)\}$.

If G is an algebraic group over k, we write $\mathrm{ed}\, G$ for the essential dimension of the functor $L \mapsto H^1_{\mathrm{fppf}}(L, G)$. That is $\mathrm{ed}\, G$ is the essential dimension of the functor sending a field L to the set of isomorphism classes of G-torsors over L. The notion of essential dimension of a finite group was introduced by J. Buhler and Z. Reichstein. The definition of the essential dimension of a functor is a generalization given later by A. Merkurjev. In [3] (which the reader could consult for further background), a notion of essential dimension for algebraic stacks was introduced. In the terminology of that paper, $\mathrm{ed}\, G$ is the essential dimension of the stack $\mathscr{B}G$.

The purpose of this paper is to generalize the following result.

Theorem 1 (Corollary 10.4 [3])**.** *Let E be an elliptic curve over a number field k. Assume that there is at least one prime $\mathfrak{p}$ of k where E has semistable bad reduction. Then* $\mathrm{ed}\, E = +\infty$.

Note that another equivalent way of stating the theorem is to say that $\mathrm{ed}\, E = +\infty$ for all elliptic curves E such that $j(E) \in \overline{\mathbb{Q}} \setminus \{\text{algebraic integers}\}$. The result was proved by showing that Tate curves have infinite essential dimension. However, this method does not apply to elliptic curves with integral j invariants. Nonetheless, Conjecture 10.5 of [3] guesses that $\mathrm{ed}\, E = +\infty$ for all elliptic curves over number fields. This conjecture is answered by the following.

Theorem 2. *Let A be an abelian variety over a number field k. Then* $\mathrm{ed}\, A = +\infty$.

Note that if A is an abelian variety over $\mathbb{C}$, then $\mathrm{ed}\, A = 2 \dim A$. This is the main result of [2].

The theorem is an easy consequence of the following result whose formulation does not involve essential dimension. To state it, for a positive integer m, let μ_m denote the group scheme of m-th roots of unity; and, for a rational prime l, let μ_{l^∞} denote the union $\cup_{n \in \mathbb{Z}_+} \mu_{l^n}$.

Theorem 3. *Let A be an abelian variety over a number field k. Then there is an odd prime ℓ and an algebraic field extension L/k such that*

(1) $\mathbb{Q}_\ell/\mathbb{Z}_\ell \subset A(L)$.
(2) $1 < |\mu_{\ell^\infty}(L)| < \infty$.

In the first section, we derive Theorem 2 from Theorem 3. The technique used is a result of M. Florence concerning the essential dimension of $\mathbb{Z}/\ell^n$. In the section 2, we prove Theorem 3. Here the main results used are those of Bogomolov and Serre on the action of the absolute Galois group $\mathrm{Gal}(k)$ on the Tate module $T_\ell A$.

Remark 4. The recent preprint [7] of Karpenko and Merkurjev provides another way to show that the essential dimension of an abelian variety over a number field is infinite. To be precise, by generalizing the results of that paper slightly, one can use them to compute the essential dimension of the group scheme $A[n]$ of n-torsion points of an abelian variety. In fact, using this idea one can show that the essential dimension of an abelian variety over a p-adic field is also infinite. However, the present proof of Theorem 2 is shorter than a proof using [7] would be and we hope that Theorem 3 is independently interesting.

Acknowledgments. It is a pleasure to thank Z. Reichstein and A. Vistoli for useful conversations. We are also extremely grateful to N. Fakhruddin. After seeing a primitive version of this paper proving Theorems 2 and 3 for elliptic curves (using Serre's results on Galois representations for ordinary elliptic curves and the theory of complex multiplication for elliptic curves with CM), he pointed out that Bogomolov's results could be applied to prove the same results for abelian varieties.

1. Theorem 3 implies Theorem 2

As mentioned above, we will use the following result [6, Theorem 4.1] of M. Florence.

Theorem 5. *Let ℓ be an odd prime and r a positive integer. Let $L/\mathbb{Q}$ be a field such that $|\mu_{\ell^\infty}(L)| = \ell^r < \infty$. Then, for any positive integer k,*

$$\mathrm{ed}_L\, \mathbb{Z}/\ell^k = \max\{1, k-r\}.$$

Corollary 6. *Let A be an abelian variety over a field L of characteristic 0. Let ℓ be an odd prime and suppose that the statements in the conclusion of Theorem 3 are satisfied; i.e:*

(1) $\mathbb{Q}_\ell/\mathbb{Z}_\ell \subset A(L)$.
(2) $1 < |\mu_{\ell^\infty}(L)| < \infty$.

Then $\mathrm{ed} A = +\infty$.

Proof. Since L satisfies (2), $\mathrm{ed}_L\, \mathbb{Z}/\ell^n \to \infty$ as $n \to \infty$. By (1), there is an injection $(\mathbb{Z}/\ell^n)_L \to A$. Therefore, by [1, Theorem 6.19], $\mathrm{ed} A \geq \mathrm{ed}_L\, \mathbb{Z}/\ell^n - \dim A$ for all n. Letting n tend to ∞, we see that $\mathrm{ed} A = +\infty$. □

Proof of Theorem 2 assuming Theorem 3. Let A be our abelian variety over a number field k. Using Theorem 3 and Corollary 6, we can find a field extension L/k such that $\mathrm{ed} A_L = +\infty$. This implies that $\mathrm{ed} A = +\infty$ (by [1, Proposition 1.5].)

2. Galois representations and the proof of Theorem 3

Before proving Theorem 3, we fix some (standard) notation. We write $G := \mathrm{Gal}(\overline{k}/k)$ for the absolute Galois group of the number field k. For a rational prime ℓ, we write $T_\ell A$ for the Tate-module $\varprojlim A[\ell^n]$ of the abelian variety A. We write $V_\ell A$ for $T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. For an integer n, we write $\mathbb{Z}/n(1)$ for μ_n, and for $j \in \mathbb{Z}$, $\mathbb{Z}/n(j)$ for $\mu_n^{\otimes j}$. We write $\mathbb{Z}_\ell(j) := \varprojlim \mathbb{Z}/l^m(j)$.

For any prime $\mathfrak{p}$ of k where A has good reduction, write $T_\mathfrak{p}$ for the corresponding Frobenius torus [4, Definition 3.1 and p. 326]. By [4, Proposition 3.2], $T_\mathfrak{p}$ contains a rank 1 torus $D \cong \mathbb{G}_m$ such that, for every rational prime $\ell \notin \mathfrak{p}$, $D(\mathbb{Q}_\ell) \subset \mathrm{Gl}(V_\ell A)$ is the set of homotheties (i.e. scalar matrices).

Lemma 7. *Let $\mathfrak{p}$ be a prime of k such that the reduction $A/\mathfrak{p}$ of A at $\mathfrak{p}$ is good but not supersingular. Then the rank of $T_\mathfrak{p}$ is strictly greater than 1.*

Proof. This follows directly from [4, Proposition 3.3]. □

The following proposition was suggested to us by N. Fakhruddin.

Proposition 8. *Let V be an n-dimensional vector space over a field F, and let T be an F-split torus in $\mathrm{Gl}_n(V)$ of rank at least 2 containing the homotheties. Then there is a non-zero vector $v \in V$ and a rank 1 subtorus S of T such that*

(1) *S fixes v;*
(2) *the determinant map $\det : S \to \mathbb{G}_m$ is surjective.*

Proof. First note that it suffices to prove the proposition when T is rank 2. Pick a basis $e_1, \dots, e_d$ for V. Then we can assume that the injection $T \to \mathrm{Gl}(V)$ is given by $(\lambda, \mu) \mapsto T(\lambda, \mu)$ where $T(\lambda, \mu) e_i = \lambda \mu^{r_i} e_i$ for some integers r_i with $(r_1, \dots, r_d) = 1$.

Now, each e_i is fixed by the group T_i of matrices of the form $T(\mu^{-r_i}, \mu)$. We have

$$\det T(\mu^{-r_i}, \mu) = \mu^{-nr_i + \sum_{j=1}^n r_j}.$$

This determinant is trivial if and only if $nr_i = \sum_{j=1}^n r_j$, and this can happen for all i only if all the r_i are the same. However, since T has rank at least 2, at least two of the r_i must differ. Thus, we can set v equal to one of the e_i and $S = T_i$. □

Proof of Theorem 3. Let A be our abelian variety over a number field k. We can find a prime $\mathfrak{p}$ in k such that A has good reduction at $\mathfrak{p}$ but $A/\mathfrak{p}$ is not supersingular. (This is well-known if $\dim A = 1$: the case where A has CM is standard and otherwise it follows from the exercise on page IV-13 of [8]. When $\dim A > 1$ it can be proved by adapting the exercise as Ogus does in Corollary 2.8 of his notes in [5].) Thus the Frobenius torus $T_\mathfrak{p}$ has rank at least 2. Using Tchebotarev density, it is easy to see that $T_\mathfrak{p} \otimes \mathbb{Q}_\ell$ is a split torus for all rational primes ℓ in a set of positive density. Thus, we can find an odd rational prime ℓ such that $\ell \not| \mathfrak{p}$ and $T_\mathfrak{p} \otimes \mathbb{Q}_\ell$ is split. Now, set $F = k(\zeta_\ell)$ where ζ_ℓ is a primitive ℓ-th root of unity. Note that $T_\mathfrak{p}$ is the Frobenius torus for A_F as Frobenius tori are invariant under finite extension of the ground field.

Now, using Proposition 8, we can can find a rank 1 subtorus $S \subset T_\mathfrak{p}$ and a vector $v \in T_\ell A_F$ such that S fixes v and $\det : S \to \mathbb{G}_m$ is surjective. Let $\rho : \mathrm{Gal}(F) \to \mathrm{Aut}(V_\ell A_F)$ denote the Galois representation on the Tate module and let $H = \{g \in \mathrm{Gal}(F) \,|\, \rho(g)v = v\}$. By the theorem of Bogomolov [4, Theorem B] (and the fact that S fixes v), it follows that the

$$\mathrm{Lie}(S) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \subset \mathrm{Lie}(\rho(H))$$

where $\mathrm{Lie}(S)$ denotes the Lie algebra of S as an algebraic group and $\mathrm{Lie}(\rho(H))$ denotes the Lie algebra as an ℓ-adic group. Therefore the intersection of $S(\mathbb{Q}_\ell)$ with $\rho(H)$ contains an open neighborhood of the identity in $S(\mathbb{Q}_\ell)$. In particular, $\det(H)$ contains an open subset of the identity in $\mathbb{Q}_\ell^*$. Set $L := \overline{F}^H$. Then, from the fact that v is fixed by H, it follows that $\mathbb{Q}_\ell/\mathbb{Z}_\ell \subset A(L)$. On the other hand, since $\wedge^{2\dim A} T_\ell A \cong \mathbb{Z}_\ell(\dim A)$, the fact that $\det(H)$ contains an open subset of the identity in $\mathbb{Q}_\ell^*$ implies that $\mu_{\ell^\infty}(L)$ is finite. This completes the proof of Theorem 3.

REFERENCES

[1] Grégory Berhuy and Giordano Favi. Essential dimension: a functorial point of view (after A. Merkurjev). *Doc. Math.*, 8:279–330 (electronic), 2003.

[2] P. Brosnan. The essential dimension of a g-dimensional complex abelian variety is $2g$. To appear in Transformation Groups, “online first” DOI: 10.1007/s00031-006-0045-0.

[3] Patrick Brosnan, Zinovy Reichstein, and Angelo Vistoli. Essential dimension and algebraic stacks. arXiv.org:math/0701903.

[4] Wên Chên Chi. l-adic and λ-adic representations associated to abelian varieties defined over number fields. *Amer. J. Math.*, 114(2):315–353, 1992.

[5] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yen Shih. *Hodge cycles, motives, and Shimura varieties*, volume 900 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1982.

[6] Mathieu Florence. On the essential dimension of cyclic p-groups. To appear in Inventiones Mathematicae, “online first” DOI:10.1007/s00222-007-0079-5.

[7] Nikita Karpenko and Alexander Merkurjev. Essential dimension of finite p-groups. Linear Algebraic Groups and Related Structure preprint server: 278.

[8] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

(Brosnan) DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF BRITISH COLUMBIA, 1984 MATHEMATICS ROAD, VANCOUVER, B.C., CANADA V6T 1Z2

(Sreekantan) SCHOOL OF MATHEMATICS TATA INSTITUTE OF FUNDAMENTAL RESEARCH, 1 HOMI BHABHA ROAD, COLABA, MUMBAI 400 005, INDIA

E-mail address, Brosnan: brosnan@math.ubc.ca

E-mail address, Sreekantan: ramesh@math.tifr.res.in