Bartel, A. (2015) Simplicity of twists of abelian varieties. *Acta Arithmetica*, 171(1), pp. 15-22. (doi:10.4064/aa171-1-2)

This is the author's final accepted version.

There may be differences between this version and the published version. You are advised to consult the publisher's version if you wish to cite from it.

http://eprints.gla.ac.uk/149654/

Deposited on: 08 January 2019

Enlighten – Research publications by members of the University of Glasgow
http://eprints.gla.ac.uk

SIMPLICITY OF TWISTS OF ABELIAN VARIETIES

ALEX BARTEL

Abstract. We give some easy necessary and sufficient criteria for twists of abelian varieties by Artin representations to be simple.

1. Introduction

Let A/k be an abelian variety over a field, let $R \leq \mathrm{End}(A)$ be a commutative ring of endomorphisms of A (here and in the sequel, we regard the abelian varieties as schemes *over a base*, and this is also the category in which our morphisms will live; in particular, $\mathrm{End}(A)$ denotes endomorphisms of A defined over k; the same remark applies to statements like "A is principally polarised", etc.), and let K/k be a finite Galois extension with Galois group G. Let Γ be an $R[G]$-module, together with an isomorphism $\psi : R^n \to \Gamma$ for some n. Attached to this data is the so-called twist of A by Γ, denoted by $B = \Gamma \otimes_R A$, which is an abelian variety over k with the property that the base change $B_K = B \times_k K$ is isomorphic to $(A_K)^n$.

As soon as $n > 1$, B is, by its very definition, never absolutely simple. But it can be simple over k, and to know when this is the case is important for some applications, see e.g. [4]. If A' is a proper abelian subvariety of A, then $\Gamma \otimes_R A'$ is a proper abelian subvariety of $\Gamma \otimes_R A$. Similarly, if $\Gamma' \leq \Gamma$ is an R-free $R[G]$-submodule of strictly smaller R-rank, then $\Gamma' \otimes_R A$ is isogenous to a proper abelian subvariety of $\Gamma \otimes_R A$. The purpose of this note is to point out that, under some mild additional hypotheses (and in particular over number fields in the generic case, when $\mathrm{End}_{\bar{k}}(A) \cong \mathbb{Z}$), these are the only two ways in which B can fail to be simple.

As a concrete example, we mention the following generalisation of Howe's analysis [4]:

Theorem 1.1. *Let A/k be a simple abelian variety of dimension 1 or 2 over a number field, let p be an odd prime number and let K/k be a Galois extension with Galois group G of order p. If A is not absolutely simple or not principally polarised, assume that $p > 3$. Let I be the augmentation ideal in $\mathbb{Z}[G]$, i.e. the kernel of the map $\mathbb{Z}[G] \to \mathbb{Z}$, $g \mapsto 1\ \forall g \in G$. Then $I \otimes_{\mathbb{Z}} A$ is simple if and only if $\mathrm{End}(A) \otimes \mathbb{Q}$ does not contain the quadratic subfield of $\mathbb{Q}(\mu_p)$.*

Remark 1.2. If $p = 2$, then $I \otimes_{\mathbb{Z}} A$ is a quadratic twist of A, and so also simple if A is. Since, for all p, $I \otimes \mathbb{Q}$ is the unique non-trivial irreducible $\mathbb{Q}[G]$-module, the theorem completely deals with simplicity of those twists of elliptic curves and of principally polarised absolutely simple abelian surfaces that are trivialised by a cyclic prime degree extension.

Remark 1.3. By computing the endomorphism ring of $I \otimes \mathbb{Q}$ as a $\mathbb{Q}[G]$-module, Howe [4] showed part of one implication in the case $\dim(A) = 1$:

This research is partly supported by a research fellowship from the Royal Commission for the Exhibition of 1851.

he proved that if E/k is a non-CM elliptic curve, then $I \otimes_{\mathbb{Z}} E$ is simple. In the proof of the theorem that we present, one does not need to know the endomorphism ring of $I \otimes \mathbb{Q}$ to deduce the result for elliptic curves; one does, however, need to know it to prove the statement for abelian surfaces.

The same technique yields uniform statements for higher dimensional abelian varieties, where the restriction on p depends on the dimension of the variety:

Theorem 1.4. *Fix an integer d. There exists an integer p_0 such that for all number fields k, all simple abelian varieties A/k of dimension d, all primes $p > p_0$, and all Galois extensions K/k with cyclic Galois group G of order p, the twist $I \otimes_{\mathbb{Z}} A$ is simple if and only if $\mathrm{End}(A) \otimes \mathbb{Q}$ does not contain a subfield of $\mathbb{Q}(\mu_p)$ other than $\mathbb{Q}$. Here, I is, as in Theorem 1.1, the augmentation ideal in $\mathbb{Z}[G]$.*

Similarly concrete results can be obtained for twists by other representations, and we give several more examples in the same vein in the last section.

Acknowledgements. I would like to thank Barinder Banwait for bringing Howe's paper to my attention, which motivated this work. Many thanks are due to Victor Rotger for very helpful email correspondence. I gratefully acknowledge the financial support by the Royal Commission for the Exhibition of 1851.

2. Endomorphisms of twists of abelian varieties

In this section we begin by recalling (see [9, §III.1.3]) the definition of a twist of an abelian variety by an Artin representation, and then give sufficient conditions for the endomorphism ring of such a twist to be an integral domain, equivalently for the twist to be simple. We strongly recommend [6] for a very thorough treatment of twists of abelian varieties, and, more generally, of commutative algebraic groups.

Let Y/k be an abelian variety, and K/k a finite Galois extension with Galois group G. A K/k-form of Y is a pair (X, f), where X/k is an abelian variety, and $f : Y_K \to X_K$ is an isomorphism, defined over K. There is an obvious notion of isomorphism between such pairs, and the set of isomorphism classes of K/k-forms of Y is in bijection with the pointed set $H^1(G, \mathrm{Aut}\, Y_K)$, where the G-action on $\mathrm{Aut}_K Y$ is given by[1] $\phi^\sigma = \sigma \circ \phi \circ \sigma^{-1}$ for $\sigma \in G$ and $\phi \in \mathrm{Aut}(Y_K)$. The bijection is given by assigning to a K/k-form (X, f) the cocycle represented by $\sigma \mapsto f^{-1} f^\sigma$, where, as before, f^σ is defined to be $\sigma \circ f \circ \sigma^{-1}$.

Now, suppose that A/k is an abelian variety, and $R \le \mathrm{End}(A)$ a commutative ring. With K/k and G as above, let Γ be an $R[G]$-module, together with an R-module isomorphism $\psi : R^n \to \Gamma$ for some $n \in \mathbb{N}$. Then the map $a_\Gamma : \sigma \mapsto \psi^{-1}\psi^\sigma = \psi^{-1} \circ \sigma \circ \psi \in \mathrm{GL}_n(R) \le \mathrm{Aut}_K A^n$ defines a cocycle in $H^1(G, \mathrm{Aut}(A_K)^n)$. Indeed, note that since G acts trivially on automorphisms of A^n that are defined over k, as is the case for $\mathrm{GL}_n(R) \le \mathrm{Aut}(A_K)^n$,

[1] we adhere to the common convention that the superscript for the action is written on the right, even though this is actually a left action

1-cocycles whose image lies in $\mathrm{GL}_n(R)$ are simply group homomorphisms. The twist B of A by Γ, written $B = \Gamma \otimes_R A$ is, by definition, the K/k-form of A^n corresponding to the cocycle a_Γ.

We now come to the endomorphism ring of B. Our aim is to find criteria for B to be simple, equivalently for $\mathrm{End}(B)$ to be a division ring. In theory, one can easily describe $\mathrm{End}(B)$ in terms of the G-module structure of $\mathrm{End}_K(A)$ and $\mathrm{End}_R(\Gamma)$:

Lemma 2.1. *There is an isomorphism*

$$\mathrm{End}(\Gamma \otimes_R A) \xrightarrow{\sim} (\mathrm{End}_R(\Gamma) \otimes \mathrm{End}_K(A))^G.$$

Proof. This immediately follows from [6, Proposition 1.6], by noting that the absolute Galois group of k acts on Γ through the quotient G. □

However, in the most general form, this description is not easy to use for determining when the right hand side of the equation is a division ring. On the other hand, generically the situation is much better.

Assumption 2.2. For the rest of this section, assume that $\mathrm{End}(A) = \mathrm{End}(A_K)$. Since we are interested in criteria for B to be simple, we will also assume from now on that A itself is simple, therefore so is A_K by the previous assumption.

Remark 2.3. This assumption is generically satisfied over number fields in the following sense: fix an abelian variety A over a number field k, and a Galois group G. A result of Ribet and Silverberg [10, 7] says that, given any subring $\mathcal{O} \subseteq \mathrm{End}_{\bar{k}}(A)$ there exists a unique minimal extension $L_{\mathcal{O}}/k$ such that $\mathcal{O} \subseteq \mathrm{End}_{L_{\mathcal{O}}}(A)$. So $\mathrm{End}_K(A) = \mathrm{End}(A)$ whenever $K \cap L_S = k$.

Notation 2.4. The following notation will be retained throughout the paper:

- K/k — a Galois extension of fields with Galois group G;
- A/k — a simple abelian variety;
- $S = \mathrm{End}(A)$;
- $R \leq S$ — a commutative subring;
- Γ — an R-free $R[G]$-module;
- $B = \Gamma \otimes_R A$ — the twist of A by Γ, which is an abelian variety over k;
- $D = S \otimes_{\mathbb{Z}} \mathbb{Q}$ — a division algebra;
- $F = R \otimes_{\mathbb{Z}} \mathbb{Q}$ — a field contained in D;

Under Assumption 2.2, Lemma 2.1 becomes

$$\mathrm{End}(B) \cong \mathrm{End}_{R[G]}(\Gamma) \otimes_R S. \tag{2.5}$$

In general, it is a subtle question with a rich literature when the tensor product of two division rings over a common subring is a division ring. But for a generic polarised abelian variety, $S = \mathbb{Z}$. More generally, if S is commutative, Schur's Lemma furnishes an elementary answer to the question of simplicity of B:

Proposition 2.6. *Assume, in addition to Assumption 2.2, that S is commutative, i.e. that D is a field. Then B is simple if and only if $\Gamma \otimes_R D$ is a simple $D[G]$-module.*

Proof. The twist B is simple if and only if $\mathrm{End}(B)$ is a division ring, if and only if

$$\mathrm{End}(B) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathrm{End}_{R[G]}(\Gamma) \otimes_R D$$

is a division algebra. It is an elementary computation that when S is commutative, $\mathrm{End}_{R[G]}(\Gamma) \otimes_R D$ is precisely the endomorphism ring of the $D[G]$-module $\Gamma \otimes_R D$, the isomorphism given by

$$\begin{array}{rcl} \mathrm{End}_{R[G]}(\Gamma) \otimes_R D & \rightarrow & \mathrm{End}_{D[G]}(\Gamma \otimes_R D), \\ \alpha \otimes f & \mapsto & (\gamma \otimes g \mapsto \alpha(\gamma) \otimes fg). \end{array}$$

We deduce that, by Schur's Lemma, B is simple if and only if $\Gamma \otimes_R D$ is a simple $D[G]$-module. □

There is slightly different way of phrasing this discussion, which is closer to Howe's original proof. Since A_K is assumed to be simple, S is a division ring, and $\mathrm{End}_K(A^n) \cong M_n(S)$, the n-by-n matrix ring over S. Since the base change of B to K is isomorphic to $(A_K)^n$, any endomorphism of B gives rise to an endomorphism of $(A_K)^n$, i.e. an element of $M_n(S)$. Conversely, it is easy to characterise the elements of $M_n(S)$ that descend to endomorphisms of B:

Proposition 2.7 ([4], Proposition 2.1)**.** *An element of $M_n(S)$ descends to an endomorphism of B if and only if it commutes with all elements of the image of G under the cocycle $a_\Gamma : G \rightarrow \mathrm{GL}_n(R) \leq \mathrm{GL}_n(S)$.*

Now, we merely need to observe that, as we remarked above, the cocycle a_Γ is in fact nothing but the group homomorphism $G \rightarrow \mathrm{Aut}(\Gamma)$ with respect to an R-basis on Γ. The commutant of its image in $M_n(S)$ is the intersection of $M_n(S)$ with the commutant of the image of a_Γ in $M_n(D)$, where $D = S \otimes \mathbb{Q}$ is, as in Proposition 2.6, assumed to be a field. Moreover, since for any $x \in M_n(D)$, some integer multiple of x lies in $M_n(S)$, the commutant of $a_\Gamma(G)$ in $M_n(S)$ is a division ring if and only if its commutant in $M_n(D)$ is a division algebra. By Schur's Lemma, the latter is the case if and only if $\Gamma \otimes_R D$ is simple.

Another example in which equation (2.5) can be completely analysed is when $D = S \otimes \mathbb{Q}$ is a quaternion algebra over $F = R \otimes \mathbb{Q}$. In that case, a theorem of Risman [8] asserts that if D' is any division algebra over F, then $D \otimes_F D'$ has zero-divisors if and only if D' contains a splitting field for D. So we immediately deduce:

Proposition 2.8. *Assume, in addition to Assumption 2.2, that D is a quaternion algebra over $F = R \otimes \mathbb{Q}$. Then B is simple if and only if $\mathrm{End}_{F[G]}(\Gamma \otimes F)$ contains no splitting field of D.*

A generalisation in a slightly different direction is the special case that $L = \mathrm{End}_{R[G]}(\Gamma) \otimes \mathbb{Q}$ is a field:

Proposition 2.9. *Assume, in addition to Assumption 2.2, that L is a field. Suppose also that R is contained in the centre of* $\mathrm{End}(A)$*. Then B is simple if and only if L intersects every splitting field of D in $F = R \otimes \mathbb{Q}$.*

Proof. This follows from the general theory of division algebras, see e.g. [1, §74A]. Indeed, let Z be the centre of D. If $L \cap Z \neq F$, then certainly $L \otimes_F D$ is not a division algebra, since $L \otimes_F Z$ is not a field. Suppose that $L \cap Z = F$, so that $L \otimes_F Z$ is a field. Then $L \otimes_F D$ is a simple algebra with centre $L \otimes_F Z$. The dimension of D over F is equal to the dimension of $L \otimes_F D$ over L, and their respective dimensions over their centres are therefore also equal. So L intersects a splitting field of D in a field that is bigger than F if and only if the index of $L \otimes_F D$ is smaller than that of D if and only if $L \otimes_F D$ has zero divisors. □

3. Consequences

We first explain how to deduce Theorem 1.1 from Propositions 2.6 and 2.8.

Let G be cyclic of odd prime order p. Recall that $I \leq \mathbb{Z}[G]$ is defined to be the augmentation ideal in $\mathbb{Z}[G]$, $I = \ker(\sum_{g \in G} n_g g \mapsto \sum_{g \in G} n_g)$. The complexification $I \otimes \mathbb{C}$ is isomorphic to the direct sum of all non-trivial simple $\mathbb{C}[G]$-modules, which are all Galois conjugate. It is therefore easy to see that $I \otimes_{\mathbb{Z}} \mathbb{Q}$ is a simple $\mathbb{Q}[G]$-module, and that moreover, given any number field D, $I \otimes_{\mathbb{Z}} D$ is reducible if and only if D intersects $\mathbb{Q}(\mu_p)$ non-trivially.

First, let A/k be an elliptic curve over a number field. Then $\mathrm{End}(A) \otimes \mathbb{Q}$ is a field, and the fact that $\mathrm{End}(A) = \mathrm{End}(A_K)$ for an odd degree extension K/k follows from classical CM theory, see e.g. [5, Chapter 3]. Thus, the dimension 1 case of Theorem 1.1 follows from Proposition 2.6.

The dimension 2 case is more subtle. Let A/k be an absolutely simple abelian surface over a number field. Then $\mathrm{End}(A_{\bar{k}}) \otimes \mathbb{Q}$ is one of the following:

1. $\mathbb{Q}$,
2. a real quadratic number field,
3. a CM field of degree 4,
4. an indefinite quaternion algebra over $\mathbb{Q}$.

We first claim that in all four cases, $\mathrm{End}(A) = \mathrm{End}(A_K)$ for an odd degree extension K/k. This is clear in case 1, and in case 3 this follows from classical CM theory, see e.g. [5, Chapter 3]. For case 2, observe that the absolute Galois group of k acts on $\mathrm{End}(A_{\bar{k}}) \otimes \mathbb{Q}$ by $\mathbb{Q}$-algebra automorphisms. If the endomorphism algebra is a quadratic field, then the action factors through a quotient of $\mathrm{Gal}(\bar{k}/k)$ of index at most 2, which proves the claim. Finally, case 4 is handled by [2, Theorem 1.3].

If $A/\bar{k}$ is isogenous to a product of elliptic curves, then there are more possibilities for the structure of $\mathrm{End}(A)$, which have been classified in [3, Theorem 4.3]. It follows from this classification that if $\mathrm{End}(A) \otimes \mathbb{Q}$ is a division algebra, then it is still either isomorphic to $\mathbb{Q}$ or a quadratic field or a quaternion algebra, and that moreover $\mathrm{End}(A) = \mathrm{End}(A_K)$ for any extension K/k of degree coprime to 6. So the dimension 2 case of Theorem 1.1 follows from Proposition 2.6 when $\mathrm{End}(A) \otimes \mathbb{Q}$ is a field, and from Proposition 2.8 when it is a quaternion algebra, which covers all possible cases.

To deduce Theorem 1.4 from Proposition 2.9, we use a result of Silverberg, which we will rephrase slightly for our purposes: for any fixed d, there exists a bound b depending only on d (specifically, $b = 4(9d)^{4d}$ is enough), such that for all abelian varieties over number fields A/k of dimension d, and all extensions K/k of prime degree greater than b, $\mathrm{End}(A) = \mathrm{End}(A_K)$. Theorem 1.4 is an immediate consequence of this result together with Proposition 2.9, because $\mathrm{End}_{\mathbb{Q}[G]}(\Gamma \otimes \mathbb{Q}) \cong \mathbb{Q}(\mu_p)$.

Proposition 2.6 has an application to questions of simplicity of Weil restrictions of scalars. If A/k is a simple abelian variety, and K/k is a finite Galois extension with Galois group G, then the Weil restriction of scalars $W_{K/k}(A_K)$ is never simple, since there is a surjective trace map $W_{K/k}(A_K) \to A$. Its kernel is, up to isogeny, precisely the twist $I \otimes_{\mathbb{Z}} A$, where I is the augmentation ideal in $\mathbb{Z}[G]$. The following is therefore an immediate consequence of Proposition 2.6:

Corollary 3.1. *Let A/k be an abelian variety with $\mathrm{End}(A_{\bar{k}}) = \mathbb{Z}$. Let K/k be a finite Galois extension with Galois group G. The kernel of the trace map $W_{K/k}(A_K) \to A$ is simple over k if and only if G has prime order.*

Proof. Cyclic groups of prime order are precisely the finite groups with only two rational irreducible representations, i.e. those for which $I \otimes_{\mathbb{Z}} \mathbb{Q}$ is a simple $\mathbb{Q}[G]$-module. □

If K/k is Galois with dihedral Galois group G of order D_{2p}, p an odd prime, then there is a unique intermediate quadratic extension $k' = k(\sqrt{d})/k$, and for any abelian variety A/k, $W_{K/k}(A_K) \sim A \times A_d \times X^2$, where A_d is the quadratic twist of A by k'/k. The remaining factor X (up to isogeny) is the twist of A by a lattice in the $(p-1)$-dimensional irreducible rational representation ρ of G, which is the sum of all the two-dimensional complex representations of G.

Corollary 3.2. *Let E/k be an elliptic curve over a number field, $K/k, X$ as above. Then X is simple.*

Proof. The values of each irreducible two-dimensional character of G generate the maximal real subfield $\mathbb{Q}(\mu_p)^+$ of the p-th cyclotomic field, and they are all Galois conjugate over $\mathbb{Q}$. They will therefore remain conjugate over any imaginary quadratic field, so the conclusion holds even when E has CM. □

We conclude with an amusing example of a "symplectic twist". Let E/k be an elliptic curve over a number field, let K/k be Galois with Galois group Q_8, the quaternion group. There are three intermediate quadratic fields, and correspondingly, the Weil restriction $W_{K/k}(E_K)$ has, up to isogeny, four factors E, E_1, E_2, E_3 that are quadratic twists of E. Write $W_{K/k}(E_K) \sim E \times E_1 \times E_2 \times E_3 \times H$.

Corollary 3.3. *Let K/k, E/k, H be defined as above. Then H is simple, unless E has CM by an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ with d equal to the sum of three squares, in which case H is isogenous to a product of two isomorphic simple factors.*

Proof. The factor H is (up to isogeny) the twist of E by two copies of the standard representation of Q_8. The endomorphism algebra of this representation is isomorphic to Hamilton's quaternions, which is split by precisely the imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ for which d is the sum of three squares. $\square$

References

[1] C. W. Curtis, I. Reiner, Methods of Representation Theory, with Applications to Finite Groups and Orders, Vol. 2, John Wiley and Sons, New York, 1987.

[2] L. V. Dieulefait, V. Rotger, The arithmetic of QM-abelian surfaces through their Galois representations, J. Algebra **281** (2004), 124–143.

[3] F. Fite, K. Kedlaya, V. Rotger, A. Sutherland, Sato–Tate distributions and Galois endomorphism modules in genus 2, Compos. Math. **148**, no. 5 (2012), 1390–1442.

[4] E. Howe, Isogeny classes of abelian varieties with no principal polarizations, in Moduli of abelian varieties (Texel Island, 1999), Progress in Math. **195**, Birkhäuser, Basel, 2001, 203–216.

[5] S. Lang, Complex Multiplication, Grundlehren der mathematischen Wissenschaften **255**, Springer Verlag, Berlin, 1983.

[6] B. Mazur, K. Rubin, A. Silverberg, Twisting commutative algebraic groups, J. Algebra **314** (2007), 419–438.

[7] K. A. Ribet, Endomorphisms of semi-stable abelian varieties over number fields, Annals Math. **101** (1975), 555–562.

[8] L. J. Risman, Zero divisors in tensor products of division algebras, Proc. Amer. Math. Soc. **51** (1975), 35–36.

[9] J.-P. Serre, Cohomologie Galoisienne (Cinquième édition, revisée et complétée), Lecture Notes in Math. **5**, Springer Verlag, Berlin, 1994.

[10] A. Silverberg, Fields of definition for homomorphisms of abelian varieties, J. Pure and Applied Algebra **77** (1992), 253–262.

Department of Mathematics, Warwick University, Coventry CV4 7AL, UK
E-mail address: a.bartel@warwick.ac.uk