Roots of unity and torsion points of abelian varieties

Davide Lombardo

Abstract We answer a question raised by Hindry and Ratazzi concerning the intersection between cyclotomic extensions of a number field K and extensions of K generated by torsion points of an abelian variety over K. We prove that the property called (μ) in [4] holds for any abelian variety, while the same is not true for the stronger version of the property introduced in [5].

Keywords Galois representations · Mumford-Tate conjecture · abelian varieties · algebraic cycles

Mathematics Subject Classification (2000) 11J95 · 11G10 · 14K15

1 Introduction

In this paper we consider the following problem: given a number field K, an abelian variety A/K (of dimension g), a prime ℓ, and a finite subgroup H of $A[\ell^\infty]$, how does the number field $K(H)$ intersect the ℓ-cyclotomic extension $K(\mu_{\ell^\infty})$? More precisely, is the intersection completely accounted for by the fact that $K(H)$ contains the image of the Weil pairing $H \times H \to \mu_{\ell^\infty}$? In order to study this question, Hindry and Ratazzi have introduced in [4] and [5] two variants of a property they call (μ), and which we now recall. We fix a polarization $\varphi : A \to A^\vee$ and, for every $n \geq 0$, we denote by e_{ℓ^n} the ℓ^n-Weil pairing $A[\ell^n] \times A[\ell^n] \to \mu_{\ell^n}$ given by composing the usual Weil pairing $A[\ell^n] \times A^\vee[\ell^n] \to \mu_{\ell^n}$ with the map $A[\ell^n] \to A^\vee[\ell^n]$ induced by φ. If H is a

D. Lombardo
Département de Mathématiques d'Orsay, 91405 Orsay (France)
Tel.: +33-633813380
E-mail: davide.lombardo@math.u-psud.fr

finite subgroup of $A[\ell^\infty]$ we now set

$$m_1(H) = \max \left\{ k \in \mathbb{N} \mid \begin{array}{c} \exists n \geq 0, \ \exists P, Q \in H \text{ of order } \ell^n \\ \text{such that } e_{\ell^n}(P, Q) \text{ generates } \mu_{\ell^k} \end{array} \right\}.$$

Following [5] we can then introduce the following definition:

Definition 1 We say that $(A/K, \varphi)$ satisfies property $(\mu)_s$ (where "s" stands for "strong") if there exists a constant $C > 0$, depending on A/K and φ, such that for all primes ℓ and all finite subgroups H of $A[\ell^\infty]$ the following inequalities hold:

$$\frac{1}{C}[K(\mu_{\ell^{m_1(H)}}) : K] \leq [K(H) \cap K(\mu_{\ell^\infty}) : K] \leq C[K(\mu_{\ell^{m_1(H)}}) : K].$$

Remark 1 It is easy to see that the choice of the polarization φ plays essentially no role, and $(A/K, \varphi)$ satisfies property $(\mu)_s$ for a given φ if and only $(A/K, \psi)$ satisfies property $(\mu)_s$ for every polarization ψ of A/K (possibly for different values of the constant C); for this reason we shall simply say that A/K satisfies property $(\mu)_s$ when it does for one (hence any) polarization. It is shown in [5] that if A/K satisfies the Mumford-Tate conjecture and has Mumford-Tate group isomorphic to $\mathrm{GSp}_{2 \dim A, \mathbb{Q}}$, then property $(\mu)_s$ holds for A.

We also consider the following variant of property $(\mu)_s$, which we call $(\mu)_w$ ("weak"), and which was first introduced in [4, Définition 6.3]:

Definition 2 We say that A satisfies property $(\mu)_w$ if the following is true: there exists a constant $C > 0$, depending on A/K, such that for all primes ℓ and all finite subgroups H of $A[\ell^\infty]$ there exists $n \in \mathbb{N}$ (in general depending on ℓ and H) such that

$$\frac{1}{C}[K(\mu_{\ell^n}) : K] \leq [K(H) \cap K(\mu_{\ell^\infty}) : K] \leq C[K(\mu_{\ell^n}) : K]. \qquad (1)$$

Clearly, property $(\mu)_s$ implies property $(\mu)_w$. In this paper we show the following two results:

Theorem 1 *Let K be a number field and A/K be an abelian variety. Property $(\mu)_w$ holds for A.*

Theorem 2 *There exists an abelian fourfold A, defined over a number field K, such that $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$ and for which property $(\mu)_s$ does not hold. More precisely, such an A can be taken to be any member of the family constructed by Mumford in [13].*

The most surprising feature of the counterexample given by theorem 2 is the condition $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$. Indeed, one is easily led to suspect that the possible failure of property $(\mu)_s$ is tied to the presence of additional endomorphisms, as the following two examples show; theorem 2, however, demonstrates that $(\mu)_s$ can fail even in the favorable situation when A has no extra endomorphisms. Notice however that an A as in theorem 2 has the property that

A^2 supports "exceptional" Tate classes, cf. [12], so the failure of property $(\mu)_s$ in this case can be understood in terms of the existence of certain algebraic cycles in the cohomology of A which do not correspond to endomorphisms.

Example 1 Property $(\mu)_s$ does not hold for abelian varieties of CM type. Indeed, let A/K be an abelian variety of dimension g admitting complex multiplication (over K) by an order R in the ring of integers of the CM field E. Let ℓ be a prime that splits completely in E and does not divide the index $[\mathcal{O}_E : R]$: we then have $R \otimes \mathbb{Z}_\ell \cong \mathcal{O}_E \otimes \mathbb{Z}_\ell \cong \mathbb{Z}_\ell^{2g}$, and by the theory of complex multiplication the action of $\mathrm{Gal}\left(\overline{K}/K\right)$ on $T_\ell(A)$ factors through $(R \otimes \mathbb{Z}_\ell)^\times$. It follows that in suitable coordinates the action of $\mathrm{Gal}\left(\overline{K}/K\right)$ on $A[\ell^n]$ is through diagonal matrices in $\mathrm{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z})$. Let now P be the ℓ^n-torsion point of A which, in these coordinates, is represented by the vector $(1, \ldots, 1)$. By our choice of coordinates, the Galois group of $K(A[\ell^n])$ over $K(P)$ is contained in

$$
\left\{ \sigma = \begin{pmatrix} \sigma_{1,1} & & & \\ & \sigma_{2,2} & & \\ & & \ddots & \\ & & & \sigma_{2g,2g} \end{pmatrix} \in \mathrm{GL}_{2g}\left(\mathbb{Z}/\ell^n\mathbb{Z}\right) \;\Big|\; \sigma \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \right\},
$$

a group which is clearly trivial: in other words, we have $K(P) = K(A[\ell^n])$. Let now H be the group generated by P. It is clear that $m_1(H) = 0$, because H is cyclic, but on the other hand $K(H) = K(P) = K(A[\ell^n])$ contains a primitive ℓ^n-th root of unity: since there are infinitely many primes ℓ satisfying our assumptions, this clearly contradicts property $(\mu)_s$ for A. In particular, this shows that in general property $(\mu)_s$ does not hold even if we restrict to the case of H being cyclic.

Example 2 Property $(\mu)_s$ does not hold for self-products (this example has been pointed out to the author by Antonella Perucca). Let B/K be any abelian variety and P, Q be points of $B[\ell^n]$ such that $e_{\ell^n}(P, Q)$ generates μ_{ℓ^n}. Consider now $A = B^2$ and $H = \langle (P, Q) \rangle$: clearly $m_1(H) = 0$ since H is cyclic, but $K(H) = K(P, Q)$ contains a root of unity of order ℓ^n, which contradicts property $(\mu)_s$ for A when n is large enough. In particular, choosing for B an abelian variety which satisfies property $(\mu)_s$ (for example an elliptic curve without CM, cf. [4]), this shows that $(\mu)_s$ needs not hold for a product when it holds for the single factors.

2 Property $(\mu)_w$

2.1 Preliminaries

We fix once and for all an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$, and consider the number field K as a subfield of $\overline{\mathbb{Q}} \subseteq \mathbb{C}$. The letter A denotes a fixed abelian variety over K; if ℓ is a prime number and n is a positive integer, we write G_{ℓ^n} for the Galois group of $K(A[\ell^n])/K$ and G_{ℓ^∞} for the Galois group of $K(A[\ell^\infty])/K$. Finally, we take the following definition for the Mumford-Tate group of A:

Definition 3 Let K be a number field and A/K be an abelian variety. Let V be the $\mathbb{Q}$-vector space $H_1(A(\mathbb{C}), \mathbb{Q})$, equipped with its natural Hodge structure of weight -1. Also let $V_\mathbb{Z} = H_1(A(\mathbb{C}), \mathbb{Z})$, write $\mathbb{S} := \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_{m,\mathbb{C}})$ for Deligne's torus, and let $h : \mathbb{S} \to \mathrm{GL}_{V \otimes \mathbb{R}}$ be the morphism giving V its Hodge structure. We define $\mathrm{MT}(A)$ to be the $\mathbb{Q}$-Zariski closure of the image of h in GL_V, and extend it to a scheme over $\mathbb{Z}$ by taking its $\mathbb{Z}$-closure in $\mathrm{GL}_{V_\mathbb{Z}}$.

Remark 2 Taking the $\mathbb{Z}$-Zariski closure in the previous definition allows us to consider points of $\mathrm{MT}(A)$ with values in arbitrary rings. It is clear that the Mumford-Tate group of A, even in this integral version, is insensitive to field extensions of K: indeed, it is defined purely in terms of data that can be read off $A_\mathbb{C}$, namely its Hodge structure and its integral homology. Notice that $\mathrm{MT}(A)_\mathbb{Q}$, being an algebraic group over a field of characteristic 0, is smooth by Cartier's theorem. It follows that $\mathrm{MT}(A)$ is smooth over an open subscheme of $\mathrm{Spec}\,\mathbb{Z}$.

The following theorem summarizes fundamental results, due variously to Serre [16], Wintenberger [22], Deligne [2, I, Proposition 6.2], Borovoǐ [1] and Pjateckiǐ-Šapiro [14], on the structure of Galois representations arising from abelian varieties over number fields; see also [6, §10] for a detailed proof of the last statement.

Theorem 3 *Let K be a number field and A/K be an abelian variety. There exists a finite extension L of K such that for all primes ℓ the image of the natural representation $\rho_{\ell^\infty} : \mathrm{Gal}(\overline{L}/L) \to \mathrm{Aut}\,T_\ell(A)$ lands into $\mathrm{MT}(A)(\mathbb{Z}_\ell)$, and likewise the image of $\rho_\ell : \mathrm{Gal}(\overline{L}/L) \to \mathrm{Aut}\,A[\ell]$ lands into $\mathrm{MT}(A)(\mathbb{F}_\ell)$.*

If furthermore the Mumford-Tate conjecture holds for A, then the index $[\mathrm{MT}(A)(\mathbb{Z}_\ell) : \mathrm{Im}\,\rho_{\ell^\infty}]$ is bounded by a constant independent of ℓ; the same is true for $[\mathrm{MT}(A)(\mathbb{F}_\ell) : \mathrm{Im}\,\rho_\ell]$.

2.2 Known results towards the Mumford-Tate conjecture

While theorem 3 will prove useful in establishing theorem 2, for the proof of theorem 1 we shall also need some results which are known to hold independently of the truth of the Mumford-Tate conjecture, and which we now recall. The crucial point is that, even though we do not know in general that the Zariski closure of G_{ℓ^∞} is "independent of ℓ" in the sense predicted by the Mumford-Tate conjecture, results of Serre and Wintenberger imply that G_{ℓ^∞} is not very far from being the group of $\mathbb{Z}_\ell$-points of an algebraic group. This is made more precise in the following theorem, for which we need to set some notation. Let A/K be an abelian variety over a number field, and for every prime ℓ let $\underline{H}_\ell$ be the identity component of the $\mathbb{Z}_\ell$-Zariski closure of G_{ℓ^∞}. The groups $\underline{H}_\ell$ turn out to be reductive, except for finitely many primes ℓ; when $\underline{H}_\ell$ is indeed reductive we write $\underline{S}_\ell$ for its derived subgroup and $\underline{C}_\ell$ for its center. Following the notation of [22], we shall write $H_\ell(\ell)$ (resp. $\underline{S}_\ell$, $\underline{C}_\ell$) for the special fiber of $\underline{H}_\ell$, and H_ℓ (resp. S_ℓ, C_ℓ) for its general fiber. We then have the following result:

Theorem 4 *(Serre [15], [16], [17], Wintenberger [22]) The following hold:*

1. *all the $\underline{H}_\ell$ but a finite number are smooth, reductive groups over $\mathbb{Z}_\ell$;*
2. *there is a finite extension K' of K such that for every prime ℓ the group $\rho_{\ell^\infty}\left(\mathrm{Gal}(\overline{K'}/K')\right)$ is contained in $\underline{H}_\ell(\mathbb{Z}_\ell)$;*
3. *the index $\left[\underline{H}_\ell(\mathbb{Z}_\ell) : \rho_{\ell^\infty}\left(\mathrm{Gal}(\overline{K'}/K')\right)\right]$ is bounded by a constant independent of ℓ;*
4. *for all primes ℓ but finitely many exceptions, the special fiber $H_\ell(\ell)$ of $\underline{H}_\ell$ acts semi-simply on $A[\ell]$, and the same is true for the special fiber $S_\ell(\ell)$ of $\underline{S}_\ell$;*
5. *there exist an integer N and a $\mathbb{Z}[1/N]$-subtorus $\underline{C}$ of $\mathrm{GL}_{2g,\mathbb{Z}[1/N]}$, containing the torus of homotheties, with the following property: for all primes ℓ not dividing N, the center $\underline{C}_\ell$ of $\underline{H}_\ell$ can be identified (up to conjugation) with $\underline{C} \times_{\mathbb{Z}[1/N]} \mathbb{Z}_\ell$.*

Proof Part (1) follows from [22, Theorem 1] upon applying results of Zarhin [23], as explained in [22, §2.1], while (2) is a theorem of Serre [15]. Part (3) follows from the main result of [22] (which describes the derived subgroup of $\underline{H}_\ell$) together with the arguments of [16] (a description of the center of $\underline{H}_\ell$), cf. [6, §10] for a detailed proof. Part (4) is a consequence of the fundamental results of Faltings [3], as it is again explained in [22, §2.1] (cf. also [17, §3.a]). Finally, (5) follows from Serre's theory of abelian representations: a detailed proof can be found in [19], see also [18] and [6, §10].

The next result we recall, again due to Serre, further implies that, even though we cannot show that the groups $\underline{H}_\ell$ are "all the same" (that is, that they all come from $\mathrm{MT}(A)$ by extension of scalars), their special fibers cannot vary too wildly:

Theorem 5 *(Serre [17, §1]) There exist a constant $c(g)$, depending only on $g = \dim A$, and finitely many $\mathbb{Z}$-algebraic subgroups $\underline{J}_1$, ..., $\underline{J}_k$ of $\mathrm{GL}_{2g,\mathbb{Z}}$ (again depending only on the dimension of A) with the following property: if ℓ is a prime larger than $c(g)$ and $H_\ell(\ell)$ acts semisimply on $A[\ell]$, then the $\overline{\mathbb{F}_\ell}$-algebraic group $\underline{S}_\ell \times_{\mathbb{Z}_\ell} \overline{\mathbb{F}_\ell}$ is $\mathrm{GL}_{2g,\overline{\mathbb{F}_\ell}}$-conjugate to one of the finitely many groups $\underline{J}_1 \times_{\mathbb{Z}} \overline{\mathbb{F}_\ell}$, ..., $\underline{J}_k \times_{\mathbb{Z}} \overline{\mathbb{F}_\ell}$.*

In view of the previous two theorems we introduce the following definition:

Definition 4 Let A be an abelian variety over a number field K and let N be as in part (5) of theorem 4. We shall say that a prime ℓ is *bad* (for A/K) if any of the following is true: $\underline{H}_\ell$ is not smooth reductive over $\mathbb{Z}_\ell$, $H_\ell(\ell)$ or $S_\ell(\ell)$ does not act semisimply on $A[\ell]$, ℓ divides N, $\ell \leq c(\dim A)$ (with c as in theorem 5), or ℓ is ramified in K. Theorem 4 ensures that for a given abelian variety there are only finitely many bad primes, and we call all the other primes *good*.

2.3 Proof of theorem 1: preliminary reductions

As the statement of theorem 1 is clearly invariant under extension of the base field, parts (2) and (3) of theorem 4 allow us to assume that $\rho_{\ell^\infty}\left(\mathrm{Gal}(\overline{K}/K)\right)$

is a subgroup of $\underline{H}_\ell(\mathbb{Z}_\ell)$ for all primes ℓ, and that furthermore the index $[\underline{H}_\ell(\mathbb{Z}_\ell) : \rho_{\ell^\infty}(\mathrm{Gal}(\overline{K}/K))]$ is bounded by a constant independent of ℓ. Since the statement of theorem 1 is also invariant under isogenies, making a further extension of the base field if necessary we can also assume without loss of generality that A is principally polarized, which implies that G_{ℓ^∞}, resp. G_ℓ, is a subgroup of $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$, resp. of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. The definition of $\underline{H}_\ell$ then shows that we have inclusions $\underline{H}_\ell \subseteq \mathrm{GSp}_{2g,\mathbb{Z}_\ell}$ and $H_\ell(\ell) \subseteq \mathrm{GSp}_{2g,\mathbb{F}_\ell}$.

The following lemma shows that the property of having index bounded by a constant is stable under passage to subgroups and quotients: knowing this will be useful to convert statements concerning the algebraic groups $\underline{H}_\ell$ into statements involving Galois groups, and vice versa.

Lemma 1 *Let C be a group and A, B be subgroups of C such that $[C : B]$ is finite. We have $[A : B \cap A] \leq [C : B]$. Moreover, if $\pi : C \to D$ is a quotient of C, then $[D : \pi(B)] \mid [C : B]$.*

Proof The map $A \hookrightarrow C \to C/B$ induces an injection (of sets) of $A/(A \cap B)$ into C/B. The second statement is obvious.

This easy fact allows us to work with "equalities up to a finite index", for which we now introduce some notations. If L_1, L_2 are number fields that depend on A/K and on some other set of parameters, we write $L_1 \doteq L_2$ to mean that there exists a constant C (depending on A/K only) such that the inequalities $[L_1 : L_1 \cap L_2] \leq C$ and $[L_2 : L_1 \cap L_2] \leq C$ hold for all values of the parameters; likewise, if G_1, G_2 are subgroups of a same group (and depend on some set of parameters), we write $G_1 \doteq G_2$ if both $[G_1 : G_1 \cap G_2]$ and $[G_2 : G_1 \cap G_2]$ are bounded by a constant depending only on A/K, uniformly in all other parameters. For two functions $f, g : I \to \mathbb{R}^+$, where I is any set, we write $f \doteq g$ if there is a constant $C' > 0$ such that $\frac{1}{C'} g(x) \leq f(x) \leq C' g(x)$ for all $x \in I$. Finally, to deal with arithmetic functions we introduce the following definition:

Definition 5 Let $\mathcal{P}$ denote the set of prime numbers, let I be any set and $h : I \times \mathcal{P} \to \mathbb{N}^+$ be any function. We say that $h(x, \ell)$ is a power of ℓ up to a bounded constant if there exists a $C'' > 0$ such that for all $x \in I$ and $\ell \in \mathcal{P}$ we have $\frac{h(x,\ell)}{\ell^{v_\ell(h(x,\ell))}} \leq C''$, or equivalently, if the prime-to-ℓ part of $h(x, \ell)$ is bounded independently of x and ℓ.

As a typical example of the use of this notation, notice that for an abelian variety A for which the Mumford-Tate conjecture is true the conclusion of theorem 3 can expressed by writing $\mathrm{Gal}(K(A[\ell^\infty])/K) \doteq \mathrm{MT}(A)(\mathbb{Z}_\ell)$ and $\mathrm{Gal}(K(A[\ell])/K) \doteq \mathrm{MT}(A)(\mathbb{F}_\ell)$, while theorem 4 implies that, for *any* abelian variety A over a number field K, possibly after replacing K with a finite extension we have $\mathrm{Gal}(K(A[\ell])/K) \doteq \underline{H}_\ell(\mathbb{F}_\ell)$.

We can then apply lemma 1 to $C = \underline{H}_\ell(\mathbb{F}_\ell)$, $B = \mathrm{Gal}(K(A[\ell])/K)$ and $A = \left\{ x \in \underline{H}_\ell(\mathbb{F}_\ell) \mid xh = h \quad \forall h \in H \right\}$ to get

$$\mathrm{Gal}(K(A[\ell])/K(H)) \doteq \left\{ x \in \underline{H}_\ell(\mathbb{F}_\ell) \mid xh = h \quad \forall h \in H \right\},$$

where the implied constant depends on A/K, but not on ℓ or H. Finally, notice that if A, B are groups (depending on some set of parameters) such that $[B : A] \le N$ for all values of the parameters, then taking $N' := N!$ we have $[B : A] \mid N'$, again for any choice of the parameters: if we so desire we can therefore replace boundedness conditions by divisibility conditions.

2.4 Smoothness

In the course of the proof of theorem 1 we shall need to know that certain algebraic groups are smooth; in this section we collect the relevant results in this direction. Let H be a finite subgroup of $A[\ell^\infty]$. Write H as $\prod_{i=1}^{2g} \mathbb{Z}/\ell^{m_i}\mathbb{Z}$ for certain integers $m_1 \ge \dots \ge m_{2g}$, let $e_1, \dots, e_{2g}$ be generators of the cyclic factors of H (so e_i is a torsion point of order ℓ^{m_i}), and let $\widehat{e}_1, \dots, \widehat{e}_{2g}$ be a basis of $T_\ell A$ lifting the e_i (that is, satisfying $\widehat{e}_i \equiv e_i \pmod{\ell^{m_i}}$ for $i = 1, \dots, 2g$). For a subset I of $\{1, \dots, 2g\}$ we let $\underline{\mathcal{G}}_I$ be the $\mathbb{Z}_\ell$-algebraic group given by

$$\underline{\mathcal{G}}_I = \left\{ M \in \underline{H}_\ell \mid M\widehat{e}_i = \widehat{e}_i \quad \forall i \in I \right\}.$$

We plan to show that $\underline{\mathcal{G}}_I$ and various other related groups are smooth (over $\mathbb{Z}_\ell$, or equivalently over $\mathbb{F}_\ell$, cf. lemma 3) whenever ℓ is sufficiently large with respect to A/K, independently of the choice of $\widehat{e}_1, \dots, \widehat{e}_{2g}$ and I (the result crucial to our applications is lemma 4). We shall make repeated use of the following fact:

Theorem 6 *Let ℓ be a prime number and k be a finite field of characteristic ℓ. Let $\mathcal{F}$ be an affine group scheme over k with coordinate ring R. The following are equivalent:*

1. *$\mathcal{F}$ is smooth;*
2. *$R \otimes_k \overline{k}$ is reduced;*
3. *the nilpotency index of $R \otimes_k \overline{k}$ is smaller than ℓ, that is, there exists an integer $e < \ell$ such that for all $a \in R \otimes_k \overline{k}$ and all positive integers n, the equality $a^n = 0$ implies $a^e = 0$;*
4. *the equality $\dim_k \operatorname{Lie} \mathcal{F} = \dim \mathcal{F}$ holds.*

Proof 1 and 2 are equivalent by [21, Theorem on p. 88]. 1 and 4 are equivalent by [21, Corollary on p. 94]. Clearly 2 implies 3, and 3 implies 2 by the same argument that proves Cartier's theorem (all algebraic groups over a field of characteristic zero are smooth), see for example [11, Proof of Theorem 10.1]. □

The following proposition, while certainly well-known to experts, does not seem to appear anywhere in the literature; we will use it as a substitute for Cartier's theorem on smoothness when working over a field of positive characteristic.

Proposition 1 *Let n, d, m be fixed positive integers. There exists a constant $c(n, d, m)$ with the following property: for every prime $\ell > c(n, d, m)$ and every finite field k of characteristic ℓ, every algebraic subgroup $\mathcal{F}$ of $\mathrm{GL}_{n,k}$ that is*

cut in $\dfrac{k[x_{ij}, y]}{(\det(x_{ij})y - 1)}$ by at most m equations of degree at most d is smooth over k.

Proof Let $I = (f_1, \ldots, f_t)$ be the ideal defining $\mathcal{F}$ in $\dfrac{k[x_{ij}, y]}{(\det(x_{ij})y - 1)}$, where $t \leq m$ and the total degree of every f_h is at most d. Let $R = \dfrac{k[x_{ij}, y]}{(\det(x_{ij})y - 1, I)}$ be the coordinate ring of $\mathcal{F}$. To test smoothness we can base-change to $\overline{k}$, and by theorem 6 we see that it suffices to prove that the nilpotency index of the ring $R \otimes_k \overline{k} \cong \dfrac{\overline{k}[x_{ij}, y]}{(\det(x_{ij})y - 1, f_1, \ldots, f_t)}$ is bounded by a function of n, d and m alone, uniformly in ℓ and k. Now just notice that the ideal $(\det(x_{ij})y - 1, f_1, \ldots, f_t)$ is generated by equations whose number and degree are bounded in terms of n, d, and m, so the result follows from [7, Theorem 1.3] (see also [8]). More precisely, since we have at most $m + 1$ equations of degree at most $\max\{d, n + 1\}$, [7, Theorem 1.3] shows that one can take $c(n, d, m) = \max\{d, n + 1\}^{m+1}$.

Lemma 2 *Let n be a positive integer, $\mathcal{F}$ be a group subscheme of $\mathrm{GL}_{n, \mathbb{Q}_\ell}$, and let $\underline{\mathcal{F}}$ be the Zariski closure of $\mathcal{F}$ in $\mathrm{GL}_{n, \mathbb{Z}_\ell}$. Then $\underline{\mathcal{F}}$ is flat over $\mathrm{Spec}\,\mathbb{Z}_\ell$.*

Proof An affine scheme $\mathrm{Spec}\,\underline{R}$ over $\mathbb{Z}_\ell$ is flat if and only if its coordinate ring $\underline{R}$ is a torsion-free $\mathbb{Z}_\ell$-module ([10, Corollary 2.14]). In our case, if I is the ideal of $\frac{\mathbb{Q}_\ell[x_{ij}, y]}{(\det(x_{ij})y - 1)}$ that defines $\mathcal{F}$, then $\underline{I} := I \cap \frac{\mathbb{Z}_\ell[x_{ij}, y]}{(\det(x_{ij})y - 1)}$ is the ideal defining $\underline{\mathcal{F}}$. In particular, the coordinate ring $\underline{R}$ of $\underline{\mathcal{F}}$ injects into the coordinate ring R of $\mathcal{F}$, which is torsion-free since it is a $\mathbb{Q}_\ell$-vector space.

Lemma 3 *Let n be a positive integer, $\mathcal{F}$ be a group subscheme of $\mathrm{GL}_{n, \mathbb{Q}_\ell}$, and let $\underline{\mathcal{F}}$ be the Zariski closure of $\mathcal{F}$ in $\mathrm{GL}_{n, \mathbb{Z}_\ell}$. Suppose furthermore that $\underline{\mathcal{F}}$ is smooth over $\mathbb{F}_\ell$: then $\underline{\mathcal{F}}$ is smooth over $\mathbb{Z}_\ell$.*

Proof In order for a scheme $\underline{\mathcal{F}} \big/ \mathrm{Spec}\,\mathbb{Z}_\ell$ to be smooth, it is necessary and sufficient that it is locally finitely presented and flat, with fibers that are smooth varieties all of the same dimension. Finite presentation is obvious in our context, and flatness follows from the previous lemma. The dimension of the fibers is locally constant by flatness, hence constant since the only open subset of $\mathrm{Spec}\,\mathbb{Z}_\ell$ containing the closed point is all of $\mathrm{Spec}\,\mathbb{Z}_\ell$. It remains to show smoothness of the fibers: the generic fiber is smooth by Cartier's theorem ([21, §11.4]), and the special fiber is smooth by assumption.

We finally come to the central result of this section:

Lemma 4 *For all primes ℓ larger than some bound depending only on A/K, for all $\mathbb{Z}_\ell$-bases $\widehat{e}_1, \ldots, \widehat{e}_{2g}$ of $T_\ell A$, and for all subsets I of $\{1, \ldots, 2g\}$, the stabilizer $\underline{\mathcal{G}}_I$ in $\underline{H}_\ell$ of the vectors $\widehat{e}_i$ (for $i \in I$) is smooth over $\mathbb{Z}_\ell$.*

Proof Notice first that $\underline{\mathcal{G}}_I$ can be obtained as the $\mathbb{Z}_\ell$-Zariski closure of the $\mathbb{Q}_\ell$-group scheme
$$\left\{ M \in H_\ell \mid M\widehat{e}_i = \widehat{e}_i \; \forall i \in I \right\}.$$
By lemma 3 it then suffices to prove smoothness over $\mathbb{F}_\ell$, and to do this we can base-change to $\overline{\mathbb{F}_\ell}$. We can also assume that ℓ is a good prime (cf. definition 4). By theorems 4 and 5 there are algebraic subgroups $\mathcal{S} := (\underline{J}_i)_{\overline{\mathbb{F}_\ell}}$ and $\mathcal{C} := (\underline{C})_{\overline{\mathbb{F}_\ell}}$ of $\mathrm{GL}_{2g,\overline{\mathbb{F}_\ell}}$ such that $(\underline{H}_\ell)_{\overline{\mathbb{F}_\ell}}$ is reductive, with center conjugated to $\mathcal{C}$ and derived subgroup conjugated to $\mathcal{S}$. In particular, we can find isomorphisms $\varphi_C : \mathcal{C} \to (\underline{C}_\ell)_{\overline{\mathbb{F}_\ell}}$ and $\varphi_S : \mathcal{S} \to (\underline{S}_\ell)_{\overline{\mathbb{F}_\ell}}$ that are given by conjugation by an element of $\mathrm{GL}_{2g}(\overline{\mathbb{F}_\ell})$, and consider the map
$$\begin{aligned} p : \mathcal{C} \times \mathcal{S} &\to \quad (\underline{H}_\ell)_{\overline{\mathbb{F}_\ell}} \\ (c, s) &\mapsto \varphi_C(c)\varphi_S(s). \end{aligned}$$
Notice that p is given by the composition of the morphism (φ_C, φ_S) with the multiplication map $m : \mathrm{GL}_{2g,\overline{\mathbb{F}_\ell}} \times \mathrm{GL}_{2g,\overline{\mathbb{F}_\ell}} \to \mathrm{GL}_{2g,\overline{\mathbb{F}_\ell}}$.

Observe furthermore that the polynomials defining m are clearly independent of ℓ, because m comes from base-change from the universal multiplication map $m : \mathrm{GL}_{2g,\mathbb{Z}} \times \mathrm{GL}_{2g,\mathbb{Z}} \to \mathrm{GL}_{2g,\mathbb{Z}}$. Moreover, since φ_C and φ_S are simply given by linear changes of basis, also the polynomials defining φ_C and φ_S have degree bounded independently of ℓ. It follows that the polynomials defining p have degree bounded independently of ℓ.

Consider now the pullback $\mathcal{F} := p^*\left((\underline{\mathcal{G}}_I)_{\overline{\mathbb{F}_\ell}}\right) \subseteq \mathcal{C} \times \mathcal{S}$: since $(\underline{\mathcal{G}}_I)_{\overline{\mathbb{F}_\ell}} \hookrightarrow (\underline{H}_\ell)_{\overline{\mathbb{F}_\ell}}$ is a closed embedding, $\mathcal{F} \hookrightarrow \mathcal{C} \times \mathcal{S}$ is again a closed embedding. We claim that $\mathcal{F}$, as a subgroup of $\mathrm{GL}_{2g,\overline{\mathbb{F}_\ell}} \times \mathrm{GL}_{2g,\overline{\mathbb{F}_\ell}} \subseteq \mathrm{GL}_{4g,\overline{\mathbb{F}_\ell}}$, is defined by equations whose number and degree are bounded independently of ℓ and of the vectors $\widehat{e}_i$. To see this, notice first that $\mathcal{C} \times \mathcal{S}$ is defined by equations bounded in number and degree – indeed, up to a linear change of coordinates (which does not alter neither the number nor the total degree of the involved polynomials), these are the same equations that define $\underline{C}$ and the group $\underline{J}_i$ over $\mathbb{Z}$, and there are only finitely many groups $\underline{J}_i$ to consider. Next remark that the conditions $M\widehat{e}_i = \widehat{e}_i$ that cut $\underline{\mathcal{G}}_I$ in $\underline{H}_\ell$ are given in coordinates by no more than $(2g)^2$ linear equations ($2g$ linear equations for each vector, and at most $2g$ vectors), each of which pulls back via p^* to a single equation in the coordinate ring of $\mathrm{GL}_{4g,\overline{\mathbb{F}_\ell}}$. Finally, the degree of these equations is bounded independently of ℓ, since it only depends on the degrees of the polynomials defining p, which as already proved are independent of ℓ. It follows from proposition 1 that for ℓ large enough $\mathcal{F}$ is smooth, hence its coordinate ring is reduced. Finally, notice that p induces an injection of the coordinate ring of $(\underline{\mathcal{G}}_I)_{\overline{\mathbb{F}_\ell}}$ in that of $\mathcal{F}$, so since the latter is reduced the same is true for the former: $(\underline{\mathcal{G}}_I)_{\overline{\mathbb{F}_\ell}}$ is then smooth by theorem 6.

An easy variant of the previous proof also yields:

Lemma 5 *Let* $\lambda : \mathrm{GSp}_{2n,\mathbb{Z}_\ell} \to \mathbb{G}_{m,\mathbb{Z}_\ell}$ *be the (algebraic) multiplier character. With the notation of the previous lemma, the* $\mathbb{Z}_\ell$-*algebraic group*
$$\underline{\mathcal{G}}_I^{(1)} = \left\{ M \in \underline{H}_\ell \mid Mh = h \quad \forall h \in H, \; \lambda(M) = 1 \right\}$$

is smooth over $\mathbb{Z}_\ell$ for all ℓ larger than some bound that only depends on A/K.

Proof Arguing as in the proof of lemma 4, it suffices to show that $p^* \left(\underline{\mathcal{G}}_I^{(1)} \right)_{\overline{\mathbb{F}_\ell}}$ is defined by equations whose number and degree are bounded independently of ℓ, of $\widehat{e}_i$, and of I. This follows easily from the same argument as in the previous proof, because the equations defining $p^* \left(\underline{\mathcal{G}}_I^{(1)} \right)_{\overline{\mathbb{F}_\ell}}$ are the same as those defining $p^* \left(\underline{\mathcal{G}}_I \right)_{\overline{\mathbb{F}_\ell}}$, together with the single equation $\lambda(M) - 1 = 0$, which is given by a polynomial whose degree is independent of ℓ: indeed, the morphism λ comes by base-change from a certain universal morphism $\lambda : \mathrm{GSp}_{2g,\mathbb{Z}} \to \mathbb{G}_{m,\mathbb{Z}}$, hence the polynomial that defines it does not depend on ℓ.

Definition 6 We shall say that the prime ℓ is *very good* for A/K if it is good and so large that all the groups $\underline{\mathcal{G}}_I$ and $\underline{\mathcal{G}}_I^{(1)}$ are smooth over $\mathbb{Z}_\ell$, for every $\mathbb{Z}_\ell$-basis of $T_\ell A$ and every subset I of $\{1, \ldots, 2g\}$.

2.5 Connected components

In this section we show that the groups we are interested in have a bounded number of connected components, and relate this number to certain cohomology groups. Recall from the previous section the notation $\underline{\mathcal{G}}_I$: given a $\mathbb{Z}_\ell$-basis $\widehat{e}_1, \ldots, \widehat{e}_{2g}$ of $T_\ell A$ and a subset I of $\{1, \ldots, 2g\}$, the $\mathbb{Z}_\ell$-algebraic group $\underline{\mathcal{G}}_I$ is the stabilizer in $\underline{H}_\ell$ of the vectors $\widehat{e}_i$ for $i \in I$.

Lemma 6 *There is a constant B, depending only on A/K, with the following property. For all primes ℓ that are good for A and for all subgroups H of $A[\ell]$, the number of connected components of*

$$\mathcal{T} = \left\{ M \in H_\ell(\ell) \mid Mh = h \quad \forall h \in H \right\} = (\underline{\mathcal{G}}_I)_{\mathbb{F}_\ell}$$

does not exceed B.

Proof Notice first that it is enough to bound the number of $\overline{\mathbb{F}_\ell}$-points of the group of components of $\mathcal{T}$, hence it is enough to consider the number of irreducible components of $\mathcal{T}_{\overline{\mathbb{F}_\ell}}$. As in the proof of lemma 4, we consider the pullback $p^* \mathcal{T}_{\overline{\mathbb{F}_\ell}} \subseteq \mathcal{C} \times \mathcal{S} \subseteq \mathrm{GL}_{4g, \overline{\mathbb{F}_\ell}}$, and remark that since $p^* \mathcal{T}_{\overline{\mathbb{F}_\ell}} \to \mathcal{T}_{\overline{\mathbb{F}_\ell}}$ is onto, it suffices to bound the number of irreducible components of $p^* \mathcal{T}_{\overline{\mathbb{F}_\ell}}$. Again as in the proof of lemma 4, we know that $p^* \mathcal{T}_{\overline{\mathbb{F}_\ell}}$ is defined by equations whose number and degree are bounded independently of ℓ and H (notice that it is enough to impose the condition $Mh = h$ for h ranging over a basis of H, and any such basis has cardinality at most $2g$).

By a variant of Bézout's theorem (see [20, Theorem 7.1] for a precise statement), this implies that the number of irreducible components of $p^* \mathcal{T}_{\overline{\mathbb{F}_\ell}}$ is bounded uniformly in ℓ and H, hence the same is true for the number of connected components of $\mathcal{T}_{\overline{\mathbb{F}_\ell}}$, whence a constant B such that $|\mathcal{T}/\mathcal{T}^0| \leq B$ for all good primes ℓ and all subgroups H of $A[\ell]$.

Similarly to what we did with lemmas 4 and 5, a simple variant of the same argument shows

Lemma 7 *There is a constant B_1, depending only on A/K, with the following property. For all primes ℓ that are good for A and for all subgroups H of $A[\ell]$, the number of connected components of*

$$\mathcal{T}_1 = \left\{ M \in H_\ell(\ell) \mid Mh = h \quad \forall h \in H, \ \lambda(M) = 1 \right\} = \left(\underline{\mathcal{G}}_I^{(1)} \right)_{\mathbb{F}_\ell}$$

does not exceed B_1.

Lemma 8 *Let $\mathcal{G}$ be a finite étale group scheme of order N over $\mathbb{F}_\ell$. The first cohomology group $H^1(\mathbb{F}_\ell, \mathcal{G})$ is finite, of order not exceeding N.*

Proof Recall ([21, §6.4]) that the association $\mathcal{G} \mapsto \mathcal{G}(\overline{\mathbb{F}_\ell})$ establishes an equivalence between the category of étale group schemes over $\mathbb{F}_\ell$ and that of finite groups with a continuous action of $\mathrm{Gal}\left(\overline{\mathbb{F}_\ell}/\mathbb{F}_\ell\right)$. To prove the lemma it is thus enough to consider the cohomology $H^1(\mathbb{F}_\ell, G)$ of a finite group G of order N equipped with a continuous action of $\hat{\mathbb{Z}} \cong \mathrm{Gal}\left(\overline{\mathbb{F}_\ell}/\mathbb{F}_\ell\right)$. An element of $H^1\left(\hat{\mathbb{Z}}, G\right)$ is represented by a continuous map $\hat{\mathbb{Z}} \to G$, which in turn is uniquely determined by the image of a topological generator of $\hat{\mathbb{Z}}$: it follows that there are no more than $|G| = N$ such maps, hence that the order of $H^1(\hat{\mathbb{Z}}, G)$ is bounded by N as claimed.

Lemma 9 *Let $\mathcal{G}$ be a linear algebraic group over $\mathbb{F}_\ell$. We have the inequality $|H^1(\mathbb{F}_\ell, \mathcal{G})| \leq |H^1(\mathbb{F}_\ell, \mathcal{G}/\mathcal{G}^0)|$, so in particular the order of $H^1(\mathbb{F}_\ell, \mathcal{G})$ does not exceed the order of the group of components of $\mathcal{G}$.*

Proof The long exact sequence in cohomology associated with the sequence

$$1 \to \mathcal{G}^0 \to \mathcal{G} \to \mathcal{G}/\mathcal{G}^0 \to 1$$

contains the segment $H^1(\mathbb{F}_\ell, \mathcal{G}^0) \to H^1(\mathbb{F}_\ell, \mathcal{G}) \to H^1(\mathbb{F}_\ell, \mathcal{G}/\mathcal{G}^0)$, where the first term is trivial by Lang's theorem (any connected algebraic group over a finite field has trivial H^1, [9, Theorem 2]). The first statement follows. The second is then a consequence of the previous lemma and of the fact that $\mathcal{G}/\mathcal{G}^0$ is étale by [21, §6.7].

2.6 Proof of theorem 1

We now come to the core of the proof of theorem 1. Let H be a finite subgroup of $A[\ell^\infty]$ of exponent ℓ^n. As shown in [5, Proposition 3.9], the degree $[K(H) \cap K(\mu_{\ell^\infty}) : K]$ is closely related to the multipliers of automorphisms in $\mathrm{Gal}\left(K(A[\ell^n])/K(H)\right)$, thought of as elements of $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z})$: through the next few lemmas we shall therefore investigate the image of the multiplier map when restricted to $\mathrm{Gal}\left(K(A[\ell^n])/K(H)\right)$.

Lemma 10 *Let A/K be an abelian variety over a number field. For all primes ℓ and for all finite subgroups H of $A[\ell]$ there exists $m \in \{0,1\}$ such that*

$$[K(\mu_{\ell^m}) : K] \stackrel{\circ}{=} [K(H) \cap K(\mu_\ell) : K],$$

that is to say, there exists $D > 0$ (depending on A/K) with the following property: for every ℓ and every subgroup H of $A[\ell]$ there exists $m \in \{0,1\}$ such that

$$D^{-1}[K(H) \cap K(\mu_\ell) : K] \le [K(\mu_{\ell^m}) : K] \le D[K(H) \cap K(\mu_\ell) : K]. \quad (2)$$

Proof Observe first that it suffices to prove that the conclusion of the lemma holds for all but finitely many primes: indeed, for a fixed prime ℓ the finite group $A[\ell]$ possesses only finitely many subgroups H, so we can choose D so large that (2) holds for any such H (with $m = 0$, say). We can therefore assume that ℓ is very good (cf. definition 6).

Recall that $H_\ell(\ell)$ is a subgroup of $\mathrm{GSp}_{2g,\mathbb{F}_\ell}$, so that there is a well-defined multiplier character $\lambda : H_\ell(\ell) \to \mathbb{G}_{m,\mathbb{F}_\ell}$. At the level of $\mathbb{F}_\ell$-points we have $G_\ell \subseteq \underline{H}_\ell(\mathbb{F}_\ell) \subseteq \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, and – since we assume A to be principally polarized – for all primes ℓ we have $\lambda \circ \rho_\ell = \chi_\ell$, the mod-$\ell$ cyclotomic character. Let now $e_1, \ldots, e_{2g}$ be an $\mathbb{F}_\ell$-basis of $A[\ell]$ such that $e_1, \ldots, e_r$ is an $\mathbb{F}_\ell$-basis of H. We consider the finite group $T = \{M \in G_\ell \mid M \cdot h = h \quad \forall h \in H\}$, that is, the stabilizer of H in G_ℓ, and the algebraic group

$$\mathcal{T} = \{M \in H_\ell(\ell) \mid M \cdot e_i = e_i, \ 1 \le i \le r\},$$

that is, the stabilizer of H in $H_\ell(\ell)$. It is clear by definition that $T = G_\ell \cap \mathcal{T}(\mathbb{F}_\ell)$; since $G_\ell \stackrel{\circ}{=} \underline{H}_\ell(\mathbb{F}_\ell)$, this shows in particular that $T \stackrel{\circ}{=} \mathcal{T}(\mathbb{F}_\ell)$. Notice that $\mathcal{T}$ is smooth over $\mathbb{F}_\ell$: indeed, the group $\mathcal{T}$ is the base-change to $\mathbb{F}_\ell$ of a corresponding group $\mathcal{G}_I$ over $\mathbb{Z}_\ell$ (notation as in section 2.4), and is therefore smooth over $\mathbb{F}_\ell$ by virtue of lemma 4 and the fact that ℓ is very good. Furthermore, by lemma 6, the group of components of $\mathcal{T}$ has order bounded by a constant B independent of ℓ and H. By lemma 7, the order of the group of connected components of the algebraic group

$$\mathcal{T}_1 = \{M \in H_\ell(\ell) \mid M \cdot h = h \quad \forall h \in H, \ \lambda(M) = 1\} = \ker(\lambda : \mathcal{T} \to \mathbb{G}_{m,\mathbb{F}_\ell})$$

is also bounded by a constant independent of ℓ and H, which we call B_1, and furthermore $\mathcal{T}_1$ is smooth since ℓ is very good. Finally, notice that the group $T_1 = \{M \in G_\ell \mid M \cdot h = h \quad \forall h \in H, \ \lambda(M) = 1\}$ satisfies $T_1 \stackrel{\circ}{=} \mathcal{T}_1(\mathbb{F}_\ell)$. Consider now the restriction of $\lambda : \mathrm{GSp}_{2g,\mathbb{F}_\ell} \to \mathbb{G}_{m,\mathbb{F}_\ell}$ to $\mathcal{T}^0$, the identity component of $\mathcal{T}$. As $\mathcal{T}^0$ is smooth, the image $\lambda(\mathcal{T}^0)$ is a connected reduced subgroup of $\mathbb{G}_{m,\mathbb{F}_\ell}$, hence it is either trivial or all of $\mathbb{G}_{m,\mathbb{F}_\ell}$. Let us consider the two cases separately.

$\lambda(\mathcal{T}^0)$ **is trivial.** As we have already remarked we have $T \subseteq \mathcal{T}(\mathbb{F}_\ell)$. It follows that the order of $\lambda(T)$ is at most the order of $\lambda(\mathcal{T}(\mathbb{F}_\ell))$, which in turn does not exceed $[\mathcal{T} : \mathcal{T}^0]$ since the restriction of λ to $\mathcal{T}^0$ is trivial. Hence we have $|\lambda(T)| \le [\mathcal{T} : \mathcal{T}^0] \le B$.

$\lambda : \mathcal{T}^0 \to \mathbb{G}_{m,\mathbb{F}_\ell}$ **is onto.** Consider the exact sequence

$$1 \to \mathcal{T}_1 \to \mathcal{T} \xrightarrow{\lambda} \mathbb{G}_{m,\mathbb{F}_\ell} \to 1$$

and take $\mathbb{F}_\ell$-rational points: the associated long exact sequence in cohomology shows that

$$\mathcal{T}(\mathbb{F}_\ell) \xrightarrow{\lambda} \mathbb{G}_{m,\mathbb{F}_\ell}(\mathbb{F}_\ell) = \mathbb{F}_\ell^\times \to H^1(\mathbb{F}_\ell, \mathcal{T}_1)$$

is exact, so $\left| \operatorname{coker}\left(\mathcal{T}(\mathbb{F}_\ell) \xrightarrow{\lambda} \mathbb{F}_\ell^\times \right) \right|$ is at most $\left| H^1(\mathbb{F}_\ell, \mathcal{T}_1) \right|$, which in turn (by lemma 9 and what we have already proved) does not exceed B_1. Since $T \overset{\circ}{=} \mathcal{T}(\mathbb{F}_\ell)$, it follows that $|\lambda(T)| \overset{\circ}{=} |\lambda(\mathcal{T}(\mathbb{F}_\ell))| \geq \frac{\ell - 1}{B_1}$, that is, there exists a constant B' (independent of ℓ, as long as it is very good) such that whenever $\lambda : \mathcal{T}^0 \to \mathbb{G}_{m,\mathbb{F}_\ell}$ is onto the inequality $|\lambda(T)| \geq \dfrac{\ell - 1}{B'}$ holds.

Let now B'' be a constant large enough that inequality (2) in the statement of the lemma holds, with $D = B''$, for all the (finitely many) primes ℓ that are not very good, and for the (finitely many) subgroups H of $A[\ell]$, for each of these primes. Finally set $D = \max \{B, B', B''\}$. We now show that inequality (2) is satisfied for all primes ℓ and all subgroups H of $A[\ell]$. It is clear by construction that this is true for the primes that are not very good, so we can suppose that ℓ is unramified in K and that $\mathcal{T}$ and $\mathcal{T}_1$ are smooth over $\mathbb{F}_\ell$.

Observe that the group T we considered above is by definition the Galois group of $K(A[\ell])/K(H)$, whereas the Galois group of $K(A[\ell])$ over $K(\mu_\ell)$ is $N := \ker\left(G_\ell \xrightarrow{\lambda} \mathbb{F}_\ell^\times \right)$. It follows that the Galois group of $K(A[\ell])$ over $K(H) \cap K(\mu_\ell)$ is the group generated by T and N, hence the degree of $K(H) \cap K(\mu_\ell)$ over K is the index of NT in G_ℓ. On the other hand we have $|G_\ell/NT| = \frac{|G_\ell/N|}{|NT/N|}$ (recall that N is normal in G_ℓ by construction), and G_ℓ/N is isomorphic to the image of $\lambda : G_\ell \to \mathbb{F}_\ell^\times$. As ℓ is unramified in K, the mod-ℓ cyclotomic character $\chi_\ell : \operatorname{Gal}(\overline{K}/K) \to \mathbb{F}_\ell^\times$ is surjective, hence we have $\lambda(G_\ell) = \chi_\ell(\operatorname{Gal}(\overline{K}/K)) = \mathbb{F}_\ell^\times$ and therefore

$$[K(H) \cap K(\mu_\ell) : K] = |G_\ell/NT| = \frac{|\lambda(G_\ell)|}{|\lambda(NT)|} = \frac{\ell - 1}{|\lambda(T)|}.$$

By our previous arguments we now see that

- either $\lambda(\mathcal{T}^0)$ is trivial, in which case $1 \leq |\lambda(T)| \leq B$ and (2) is satisfied by taking $m = 1$;

- or $\lambda : \mathcal{T}^0 \to \mathbb{G}_{m,\mathbb{F}_\ell}$ is onto, in which case we have $\dfrac{\ell - 1}{B'} \leq |\lambda(T)| \leq \ell - 1$ and (2) is satisfied by taking $m = 0$.

Remark 3 It is clear from the definitions that (if ℓ is large enough) the integer m of the previous lemma satisfies $m \geq m_1(H[\ell])$. For the group $\mathcal{H}$ considered below in the proof of theorem 2 we have $m_1(\mathcal{H}) = 0$ and $m = 1$, which shows that equality needs not hold.

To complete the proof of theorem 1 we need two more lemmas.

Lemma 11 *Let K be a number field and A/K be an abelian variety. For any finite subgroup H of $A[\ell^\infty]$ the degree $[K(H) : K(H[\ell])]$ is a power of ℓ (up to a bounded constant).*

Proof We use the notation from section 2.4: we write $H \cong \prod_{i=1}^{2g} \mathbb{Z}/\ell^{m_i}\mathbb{Z}$, and fix generators $e_1, \ldots, e_{2g}$ of H and a basis $\widehat{e}_1, \ldots, \widehat{e}_{2g}$ of $T_\ell A$ lifting the e_i. We suppose first that ℓ is a very good prime. Inspired by the approach of [5], given $\mathbb{Z}_\ell$-algebraic subgroups $\mathcal{G}_1 \subseteq \mathcal{G}_2 \subseteq \cdots \subseteq \mathcal{G}_t$ of a $\mathbb{Z}_\ell$-group $\mathcal{G}$, a strictly increasing sequence $n_1 < n_2 < \cdots < n_t$ of positive integers, and a positive integer n, we now denote by $\mathcal{G}(n; n_1, \ldots, n_t)$ the finite group

$$\left\{ M \in \mathcal{G}(\mathbb{Z}/\ell^n\mathbb{Z}) \mid M \in \mathcal{G}_i \bmod \ell^{\min(n, n_i)}, \quad i = 1, \ldots, t \right\}.$$

It is natural to also consider case of t being 0: if n_i is the empty sequence, we simply define $\mathcal{G}(n) = \mathcal{G}(\mathbb{Z}/\ell^n\mathbb{Z})$. To H we now attach a strictly decreasing sequence of positive integers $m^{(1)} > m^{(2)} > \cdots > m^{(t)} \geq 1$ (where $t \leq 2g$) by setting $m^{(1)} = \max\left\{ m_i \mid m_i \neq 0 \right\}$, and recursively

$$m^{(r+1)} = \max\left\{ m_i \mid 0 < m_i < m^{(r)} \right\},$$

and, for $1 \leq r \leq t$, we let $I_r = \left\{ i \in \{1, \ldots, 2g\} \mid m_i \geq m^{(r)} \right\}$. Finally, for $1 \leq r \leq t$, we set $\mathcal{G}_r := \underline{\mathcal{G}}_{I_{t+1-r}} = \left\{ M \in \underline{H}_\ell \mid M \cdot \widehat{e}_i = \widehat{e}_i \text{ for } i \in I_{t+1-r} \right\}$, and we consider the strictly *increasing* sequence $n_r = m^{(t+1-r)}$ (for $1 \leq r \leq t$).

By our assumptions on ℓ all the groups $\mathcal{G}_r$ are smooth over $\mathbb{Z}_\ell$, and, as in [5], we easily see that the $\mathcal{G}_r$ so defined form an increasing sequence of subgroups of $\mathcal{G} := \underline{H}_\ell$ such that $[K(H[\ell^m]) : K] \stackrel{\circ}{=} [\mathcal{G}(\mathbb{Z}/\ell^m\mathbb{Z}) : \mathcal{G}(m; n_1, \ldots, n_t)]$. We now show that (for any H and any $m \geq 1$) the number

$$\frac{[\mathcal{G}(\mathbb{Z}/\ell^m\mathbb{Z}) : \mathcal{G}(m; n_1, \ldots, n_t)]}{[\mathcal{G}(\mathbb{Z}/\ell\mathbb{Z}) : \mathcal{G}(1; n_1, \ldots, n_t)]} \tag{3}$$

is a power of ℓ. To prove this fact, we preliminarily show that for all $m \geq 2$ the reduction map $\mathcal{G}(\mathbb{Z}/\ell^m\mathbb{Z}) \xrightarrow{\pi_{m-1}} \mathcal{G}(\mathbb{Z}/\ell^{m-1}\mathbb{Z})$ maps $\mathcal{G}(m; n_1, \ldots, n_t)$ surjectively onto $\mathcal{G}(m-1; n_1, \ldots, n_t)$. We can proceed by induction on t, showing the stronger statement that this is true for any finite chain of groups $\mathcal{G}_1 \subseteq \mathcal{G}_2 \subseteq \cdots \subseteq \mathcal{G}_t \subseteq \mathcal{G}$ where each term is smooth over $\mathbb{Z}_\ell$. Indeed,

- for $t = 0$ the claim follows from the smoothness of $\mathcal{G}$ and Hensel's lemma;
- if $m \leq n_t$, then we have $\mathcal{G}(j; n_1, \ldots, n_t) = \mathcal{G}_t(j; n_1, \ldots, n_{t-1})$ both for $j = m$ and $j = m - 1$, so the claim follows from the induction hypothesis;
- if $m > n_t$, then on the one hand the map $\mathcal{G}(\mathbb{Z}/\ell^m\mathbb{Z}) \to \mathcal{G}(\mathbb{Z}/\ell^{m-1}\mathbb{Z})$ is surjective by smoothness of $\mathcal{G}$, and on the other hand, since by assumption $m - 1 \geq n_t > n_{t-1} > \ldots > n_1$, any lift to $\mathcal{G}(\mathbb{Z}/\ell^m\mathbb{Z})$ of a point in $\mathcal{G}(m-1; n_1, \ldots, n_t)$ belongs to $\mathcal{G}(m; n_1, \ldots, n_t)$. It follows that the induced map $\mathcal{G}(m; n_1, \ldots, n_t) \to \mathcal{G}(m-1; n_1, \ldots, n_t)$ is indeed surjective.

We now prove our claim that (3) is a power of ℓ by induction on m, the case $m = 1$ being trivial. Notice that, by Hensel's lemma and since $m \geq 2$, the kernel of π_{m-1} is an ℓ-group (of order $\ell^{\dim \mathcal{G}}$). It follows that π_{m-1} induces a surjective map $\mathcal{G}(m; n_1, \ldots, n_t) \to \mathcal{G}(m - 1; n_1, \ldots, n_t)$ whose kernel is an ℓ-group; in particular, the numbers $\frac{|\mathcal{G}(m; n_1, \ldots, n_t)|}{|\mathcal{G}(m-1; n_1, \ldots, n_t)|}$ and $\frac{|\mathcal{G}(\mathbb{Z}/\ell^m\mathbb{Z})|}{|\mathcal{G}(\mathbb{Z}/\ell^{m-1}\mathbb{Z})|}$ are both powers of ℓ, and an immediate induction shows that the same is true for (3).

Choosing m large enough that $H = H[\ell^m]$, it follows from our previous considerations that

$$[K(H) : K(H[\ell])] = \frac{[K(H[\ell^m]) : K]}{[K(H[\ell]) : K]} \stackrel{\circ}{=} \frac{[\mathcal{G}(\mathbb{Z}/\ell^m\mathbb{Z}) : \mathcal{G}(m; n_1, \ldots, n_t)]}{[\mathcal{G}(\mathbb{Z}/\ell\mathbb{Z}) : \mathcal{G}(1; n_1, \ldots, n_t)]}$$

is a power of ℓ (up to bounded constants), which finishes the proof of the lemma when all the stabilizers $\underline{\mathcal{G}}_I$ are smooth over $\mathbb{Z}_\ell$, and leaves us with only finitely many (not *very good*) primes to consider. To establish the lemma we thus need to show that, for ℓ ranging over these finitely many primes and H ranging over the finite subgroups of $A[\ell^\infty]$, the degree $[K(H) : K(H[\ell])]$ is within a constant factor of a power of ℓ. As we are only considering finitely many primes, there are only finitely many subgroups of $A[\ell]$, and therefore we have $[K(H[\ell]) : K] \stackrel{\circ}{=} 1$; hence we just need to show that $[K(H) : K]$ is a power of ℓ up to a constant factor. Let ℓ^m be the exponent of H. Since the prime-to-ℓ part of $[K(H) : K]$ divides the prime-to-ℓ part of $[K(A[\ell^m]) : K]$, it is enough to show that $|G_{\ell^m}| = |\operatorname{Gal}(K(A[\ell^m])/K)|$ is a power of ℓ up to a bounded constant. Let C be the least common multiple of the orders of the groups G_ℓ for ℓ ranging over the finitely many not *very good* primes. Consider the reduction map $\pi : G_{\ell^m} \to G_\ell$, and notice that its kernel is a subgroup of $\ker(\operatorname{GL}_{2g}(\mathbb{Z}/\ell^m\mathbb{Z}) \to \operatorname{GL}_{2g}(\mathbb{F}_\ell))$, hence in particular an ℓ-group; we can then write $\frac{|G_{\ell^m}|}{|\ker \pi|}$ as $|\pi(G_{\ell^m})|$, which by construction is an integer dividing C. Since $|\ker \pi|$ is a power of ℓ, we see that the prime-to-ℓ part of $|G_{\ell^m}|$ is bounded by C; this completes the proof in the non-smooth case as well.

Lemma 12 *Let K be a number field, A/K be an abelian variety, ℓ a prime number, and H a finite subgroup of $A[\ell^\infty]$. We have*

$$K(H) \cap K(\mu_\ell) \stackrel{\circ}{=} K(H[\ell]) \cap K(\mu_\ell),$$

and the degree of $K(H) \cap K(\mu_{\ell^\infty})$ over $K(H) \cap K(\mu_\ell)$ is a power of ℓ.

Proof Let m be such that $H \subseteq A[\ell^m]$. The Galois group of $K(A[\ell^m])$ over $K(H[\ell]) \cap K(\mu_\ell)$ is generated by the groups $U_1 := \operatorname{Gal}(K(A[\ell^m]/K(H[\ell]))$ and $N := \operatorname{Gal}(K(A[\ell^m])/K(\mu_\ell))$; notice that $N = \ker\left(G_{\ell^m} \xrightarrow{\lambda} \mathbb{F}_\ell^\times\right)$. Let now U_m be the Galois group of $K(A[\ell^m])$ over $K(H)$. By lemma 11 we see that $[U_1 : U_m]$ is a power of ℓ (up to a constant bounded independently of ℓ), hence $[NU_1 : NU_m] = \frac{|NU_1/N|}{|NU_m/N|} = \frac{|\lambda(U_1)|}{|\lambda(U_m)|}$ is again a power of ℓ (up to a constant independent of ℓ). On the other hand, $\lambda(U_1)$ is a subgroup of $\mathbb{F}_\ell^\times$, hence of order prime to ℓ: it follows that $\left|\frac{\lambda(U_1)}{\lambda(U_m)}\right| \stackrel{\circ}{=} 1$, and therefore $NU_1 \stackrel{\circ}{=} NU_m$. Now

NU_1 is the Galois group of $K(A[\ell^m])$ over $K(H[\ell]) \cap K(\mu_\ell)$, while NU_m is the Galois group of $K(A[\ell^m])$ over $K(H) \cap K(\mu_\ell)$: by Galois theory, this implies $K(H) \cap K(\mu_\ell) \stackrel{\circ}{=} K(H[\ell]) \cap K(\mu_\ell)$ as claimed. The second part is immediate by Galois theory.

Theorem 7 *(Theorem 1) Let K be a number field and A/K be an abelian variety. Property $(\mu)_w$ holds for A.*

Proof Fix a prime ℓ and a subgroup $H \subseteq A[\ell^\infty]$: we want to show that we can choose n so as to satisfy inequality (1) (for some constant C only depending on A/K). Let L be the intersection $K(H[\ell]) \cap K(\mu_\ell)$. By lemma 10, we can choose $m \in \{0,1\}$ so that

$$[L : K] \stackrel{\circ}{=} [K(\mu_{\ell^m}) : K], \tag{4}$$

and by lemma 12 there is an integer j such that $[K(H) \cap K(\mu_{\ell^\infty}) : L] \stackrel{\circ}{=} \ell^j$. Observe now that

$$[K(H) \cap K(\mu_{\ell^\infty}) : K] = [K(H) \cap K(\mu_{\ell^\infty}) : L]\,[L : K] \stackrel{\circ}{=} \ell^j [L : K],$$

hence by (4) we have $[K(H) \cap K(\mu_{\ell^\infty}) : K] \stackrel{\circ}{=} \ell^j \cdot [K(\mu_{\ell^m}) : K]$. Using the equalities (up to bounded constants) $[K(\mu_{\ell^{j+1}}) : K(\mu_\ell)] \stackrel{\circ}{=} [K(\mu_{\ell^j}) : K] \stackrel{\circ}{=} \ell^j$ we deduce

$$\begin{aligned}
[K(H) \cap K(\mu_{\ell^\infty}) : K] &\stackrel{\circ}{=} \ell^j \cdot [K(\mu_{\ell^m}) : K] \\
&\stackrel{\circ}{=} [K(\mu_{\ell^{j+m}}) : K(\mu_{\ell^m})] \cdot [K(\mu_{\ell^m}) : K] \\
&= [K(\mu_{\ell^{j+m}}) : K].
\end{aligned}$$

This shows that, if we take C to be the constant implied in the last formula, for all primes ℓ and all finite subgroups H of $A[\ell^\infty]$ inequality (1) can be satisfied by taking $n = m + j$, and therefore property $(\mu)_w$ holds for A as claimed.

3 Property $(\mu)_s$

Let F be any field. We start by considering the representation

$$\begin{aligned}
\rho : \mathrm{GL}_{2,F} \times \mathrm{GL}_{2,F} \times \mathrm{GL}_{2,F} &\to \ \mathrm{GSp}_{8,F} \\
(a, b, c) &\mapsto a \otimes b \otimes c,
\end{aligned} \tag{5}$$

where we identify F^8 with $F^2 \otimes F^2 \otimes F^2$. We equip F^8 with the symplectic form ψ given by $\psi_1 \otimes \psi_2 \otimes \psi_3$, where ψ_i is the standard symplectic form on the i-th factor F^2: the fact that the action of $\mathrm{GL}_{2,F}$ preserves ψ_i (up to a scalar) implies that the representation ρ does indeed land into $\mathrm{GSp}_{8,F}$.

Definition 7 We let M_F be the image of this representation: it is an algebraic group over F, and it contains the torus of homotheties.

Remark 4 Consider the $\mathbb{Z}_\ell$-Zariski closure of $M_{\mathbb{Q}_\ell}$ in $\mathrm{GSp}_{8,\mathbb{Z}_\ell}$, call it $\mathcal{M}_{\mathbb{Z}_\ell}$. By definition, $\mathcal{M}_{\mathbb{Z}_\ell}$ coincides with the $\mathbb{Z}_\ell$-Zariski closure of $M_{\mathbb{Q}} \times_{\mathbb{Q}} \mathbb{Q}_\ell$ in $\mathrm{GSp}_{8,\mathbb{Z}_\ell}$, which is smooth over $\mathbb{Z}_\ell$ for almost all ℓ because $M_{\mathbb{Q}}$ extends to a smooth scheme over an open subscheme of $\mathrm{Spec}\,\mathbb{Z}$. It follows that $\mathcal{M}_{\mathbb{Z}_\ell}$ is smooth over $\mathbb{Z}_\ell$ for almost all ℓ.

We think the algebraic group M_F as sitting inside $\mathbb{A}_F^{64}$ (the space of 8×8 matrices over F). It is not hard to find polynomials that belong to the ideal defining M_F: by construction ρ factors through $\mathrm{GL}_{2,F} \otimes \mathrm{GL}_{2,F} \otimes \mathrm{GL}_{2,F}$, so if we let $\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$ be any element in $M_F(\overline{F})$ (where every B_{ij} is a 4×4 matrix), the construction of the tensor product implies that the four matrices B_{ij} are pairwise linearly dependent (notice that this condition is purely algebraic, being given by the vanishing of sufficiently many determinants). Likewise, if we write $B_{ij} = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}$, where each C_{kl} is a 2×2 matrix, we must again have pairwise linear dependence of the C_{kl}, and this (being an algebraic condition) is again true for any point in $M_F(\overline{F})$. Let now e_1, e_2 be the standard basis of F^2 and write $e_{ijk} = e_i \otimes e_j \otimes e_k$ (with $i, j, k \in \{1, 2\}$) for the corresponding basis of F^8. We order these basis vectors as $e_{111}, e_{112}, e_{121}, e_{122}, e_{211}, e_{212}, e_{221}, e_{222}$. The form ψ on F^8 is then represented by the matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

and it is immediate to check that $e_{111}, e_{122}, e_{212}, e_{221}$ span a Lagrangian subspace.

Definition 8 Let F be any field. We let H be the subspace of $F^8 \cong \left(F^2\right)^{\otimes 3}$ generated by $e_{111}, e_{122}, e_{212}$, and e_{221}.

We now determine the stabilizer T of H in $M_F\left(\overline{F}\right)$. In matrix terms, an element t of T can be written as

$$t = \begin{pmatrix} 1 & \square & \square & 0 & \square & 0 & 0 & \square \\ 0 & \square & \square & 0 & \square & 0 & 0 & \square \\ 0 & \square & \square & 0 & \square & 0 & 0 & \square \\ 0 & \square & \square & 1 & \square & 0 & 0 & \square \\ 0 & \square & \square & 0 & \square & 0 & 0 & \square \\ 0 & \square & \square & 0 & \square & 1 & 0 & \square \\ 0 & \square & \square & 0 & \square & 0 & 1 & \square \\ 0 & \square & \square & 0 & \square & 0 & 0 & \square \end{pmatrix},$$

where each entry $\square$ is a priori any element of $\overline{F}$.

We now use the fact that $T \subseteq M_F(\overline{F})$ to show that T is in fact finite. Write as before B_{11} (resp. B_{12}, B_{21}, B_{22}) for the top-left (resp. top-right, bottom-left and bottom-right) block of t of size 4×4. Since B_{22} is nonzero, linear dependence of B_{22} and B_{12} can be expressed as $B_{12} = \alpha B_{22}$ for a certain $\alpha \in \overline{F}$; however, since B_{22} has some nonzero diagonal coefficients while the corresponding diagonal entries of B_{12} vanish, we must have $\alpha = 0$ and $B_{12} = 0$. The same argument, applied to B_{21} and B_{11}, shows that $B_{21} = 0$. On the other hand, the blocks B_{11} and B_{22} are both nonzero, so there exists a nonzero $\lambda \in \overline{F}^{\times}$ such that $B_{22} = \lambda B_{11}$: this leads immediately to

$$
t = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1/\lambda & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1/\lambda & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda
\end{pmatrix}.
$$

We now use the second part of our previous remark, namely the fact that the 2×2 blocks of B_{11} are linearly dependent as well. Comparing the top-left and bottom-right blocks of B_{11} gives the additional condition $\lambda^2 = 1$, that is, $\lambda = \pm 1$: thus the stabilizer in $M_F(\overline{F})$ of our Lagrangian subspace H consists of exactly two elements, namely the identity and the operator $\mathrm{diag}(1, -1, -1, 1, -1, 1, 1, -1)$ (at least if char $F \neq 2$: otherwise we have $-1 = 1$ and the two coincide). This stabilizer is also clearly finite as an algebraic group, since it has only finitely many points over $\overline{F}$.

Notice that this argument actually shows a little more. Let $\mathcal{M}_{\mathbb{Z}_\ell}$ be the $\mathbb{Z}_\ell$-Zariski closure of $M_{\mathbb{Q}_\ell}$ in $\mathrm{GSp}_{8,\mathbb{Z}_\ell}$. Let furthermore $\mathcal{H}$ be the Lagrangian subspace of $\mathbb{F}_\ell^8 \cong \mathbb{F}_\ell^2 \otimes \mathbb{F}_\ell^2 \otimes \mathbb{F}_\ell^2$ given in definition 8 (for the field $\mathbb{F}_\ell$): then the stabilizer of $\mathcal{H}$ in $\mathcal{M}_{\mathbb{Z}_\ell}(\overline{\mathbb{F}_\ell})$ has order at most 2. Indeed, all we have used in the above argument is the linear dependence of certain blocks in the matrix representation of the elements of the stabilizer and the fact that the equation $\lambda^2 = 1$ admits at most 2 solutions in $\overline{F}$: both properties are also true for the points of $\mathcal{M}_{\mathbb{Z}_\ell}$ with values in any integral $\mathbb{Z}_\ell$-algebra (in particular, $\overline{\mathbb{F}_\ell}$). We record this fact in the following

Proposition 2 *Let ℓ be a prime, $\mathcal{M}_{\mathbb{Z}_\ell}$ be the $\mathbb{Z}_\ell$-Zariski closure of $M_{\mathbb{Q}_\ell}$ in $\mathrm{GSp}_{8,\mathbb{Z}_\ell}$, and $\mathcal{H}$ be the subspace H of definition 8 for the field $\mathbb{F}_\ell$. The stabilizer of $\mathcal{H}$ in $\mathcal{M}_{\mathbb{Z}_\ell}(\overline{\mathbb{F}_\ell})$ consists of at most 2 elements.*

3.1 Mumford's examples, and the proof of theorem 2

We now recall the construction given by Mumford in [13]. Suppose we are given the data of a totally real cubic number field F and of a central simple division algebra D over F satisfying:

1. $\mathrm{Cor}_{F/\mathbb{Q}}(D) = M_8(\mathbb{Q})$;
2. $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H} \oplus \mathbb{H} \oplus M_2(\mathbb{R})$.

Being a division algebra, D is equipped with a natural involution $x \mapsto \overline{x}$; let G be the $\mathbb{Q}$-algebraic group whose $\mathbb{Q}$-points are given by $\{x \in D^* \mid x\overline{x} = 1\}$. Mumford constructed in [13] an abelian variety of dimension 4 with trivial endomorphism ring and Hodge group equal to G (in fact, he constructed a Shimura curve parametrizing abelian fourfolds whose Hodge group is contained in G, and showed that every sufficiently generic fiber has exactly G as its Hodge group). By specialization, there exists a principally polarized abelian fourfold A defined over a number field L and such that $\mathrm{Hg}(A) \cong G$; since $\mathrm{Hg}(A)$ is as small as it is possible for an abelian fourfold with no additional endomorphisms, the Mumford-Tate conjecture is known to hold for A (cf. [12]). By theorem 3 there is a finite extension K of L such that, if we let G_ℓ be the image of the mod-ℓ representation $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}\, A[\ell]$, then the inclusion $G_\ell \subseteq \mathrm{MT}(A)(\mathbb{F}_\ell)$ holds for all primes ℓ. On the other hand, the equality $\mathrm{Cor}_{F/\mathbb{Q}}(D) = M_8(\mathbb{Q})$ implies the existence of a ("norm") map $N : D^* \to \mathrm{GL}_8(\mathbb{Q})$, and Mumford's construction is such that the action of $G(\mathbb{Q}) = D^*$ on $V := H_1(A(\mathbb{C}), \mathbb{Q}) \cong \mathbb{Q}^8$ is given exactly by N. Furthermore, it is also known that N is a $\mathbb{Q}$-form of the $\mathbb{R}$-representation $G(\mathbb{R}) \cong \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SU}_2(\mathbb{R})^2 \to \mathrm{Sp}_8(\mathbb{R})$ coming from the tensor product of the standard representation of $\mathrm{SL}_2(\mathbb{R})$ by the unique 4-dimensional faithful orthogonal representation $\mathrm{SU}_2(\mathbb{R})^2 \to \mathrm{SO}_4(\mathbb{R})$. In particular, by extension of scalars to $\mathbb{C}$ we see that the action of $G(\mathbb{C}) \cong \mathrm{SL}_2(\mathbb{C})^3$ on $V_{\mathbb{C}}$ is given by the representation ρ of the previous paragraph (restricted to $\mathrm{SL}_2(\mathbb{C})^3$).

Lemma 13 *Let ℓ be a prime such that $G \times_{\mathbb{Q}} \mathbb{Q}_\ell$ is split. Then through the canonical identification $T_\ell(A) \otimes \mathbb{Q}_\ell \cong H_1(A(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{Q}_\ell$ we have the equality $\mathrm{MT}(A) \times_{\mathbb{Z}} \mathbb{Q}_\ell = M \times_{\mathbb{Q}} \mathbb{Q}_\ell$, where $M = M_{\mathbb{Q}}$ is the algebraic group of definition 7 for the field $\mathbb{Q}$.*

Proof The morphism $G \to \mathrm{Sp}_{8,\mathbb{Q}}$ is given by the norm map, and if $G \times_{\mathbb{Q}} \mathbb{Q}_\ell$ is split (hence isomorphic to $\mathrm{SL}_{2,\mathbb{Q}_\ell}^3$) the norm map is exactly

$$\rho : \mathrm{SL}_{2,\mathbb{Q}_\ell}^3 \to \mathrm{Sp}_{8,\mathbb{Q}_\ell}$$
$$(a, b, c) \mapsto a \otimes b \otimes c;$$

it follows that $M \times_{\mathbb{Q}} \mathbb{Q}_\ell$ contains $\mathrm{Hg}(A) \times_{\mathbb{Q}} \mathbb{Q}_\ell$ (as algebraic groups). On the other hand, $\mathrm{MT}(A)$ is the almost-direct product of $\mathrm{Hg}(A)$ by the homotheties torus $\mathbb{G}_m$, and we know that M also contains $\mathbb{G}_m$. This proves that we have $\mathrm{MT}(A) \times \mathbb{Q}_\ell \subseteq M \times \mathbb{Q}_\ell$, and since the two groups have the same dimension the inclusion must be an equality.

Extend now M and G to group schemes over $\mathbb{Z}$ by taking their $\mathbb{Z}$-Zariski closure in their respective ambient spaces; there is an open subscheme $\mathrm{Spec}\,\mathbb{Z}\left[\frac{1}{S}\right]$ of $\mathrm{Spec}\,\mathbb{Z}$ over which $M, \mathrm{MT}(A)$ and G are all smooth. Consider the family $\mathcal{F}$ of primes ℓ unramified in K, such that G splits over $\mathbb{Q}_\ell$, and which do not divide S. We claim that $\mathcal{F}$ is infinite. Indeed, for G to be split over $\mathbb{Q}_\ell$ it is

enough that the root datum of G be unramified at ℓ and that the Frobenius at ℓ act trivially on it, which – by Chebotarev's theorem – is the case for a positive-density set of primes (the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the root datum of G factors through a finite quotient): it is then clear that $\mathcal{F}$ is infinite, because only finitely many primes divide S or the discriminant of K. Pick now any ℓ in $\mathcal{F}$ and let $\mathcal{M} = M \times_{\mathbb{Z}} \mathbb{Z}_\ell$. The definition of $\mathcal{F}$ implies that $\mathcal{M}$ is a smooth $\mathbb{Z}_\ell$-model of $M \times_{\mathbb{Z}} \mathbb{Q}_\ell = M_{\mathbb{Q}_\ell}$, and by lemma 13 we have $\mathrm{MT}(A) \times_{\mathbb{Z}} \mathbb{Z}_\ell = \mathcal{M}$, because both groups can be obtained as the $\mathbb{Z}_\ell$-Zariski closure of the same generic fiber. In particular, we see that G_ℓ is contained in $\mathcal{M}(\mathbb{F}_\ell) = \mathrm{MT}(A)(\mathbb{F}_\ell)$. Take now $\mathcal{H} \subseteq A[\ell]$ to be the Lagrangian subspace of definition 8 (for the field $\mathbb{F}_\ell$). The field $K(\mathcal{H})$ is clearly contained in $K(A[\ell])$, so in order to describe $K(\mathcal{H})$ it suffices to describe $\mathrm{Gal}\left(K(A[\ell])/K(\mathcal{H})\right)$, that is, the stabilizer of $\mathcal{H}$ in G_ℓ; as G_ℓ is contained in $\mathcal{M}(\mathbb{F}_\ell)$, this stabilizer is certainly contained in the stabilizer of $\mathcal{H}$ in $\mathcal{M}(\mathbb{F}_\ell)$, which in turn consists of at most two elements by proposition 2. We have thus proved that the index $[K(A[\ell]) : K(\mathcal{H})]$ is at most 2, and since $K(\mu_\ell)$ is contained in $K(A[\ell])$ by the properties of the Weil pairing (recall that A is principally polarized) we have

$$[K(\mathcal{H}) \cap K(\mu_{\ell^\infty}) : K] \geq \frac{1}{2}\left[K(A[\ell]) \cap K(\mu_{\ell^\infty}) : K\right] \geq \frac{1}{2}\left[K(\mu_\ell) : K\right] = \frac{\ell - 1}{2},$$

where the last equality follows from the fact that ℓ is unramified in K. We then see that property $(\mu)_s$ does not hold for Mumford's example: indeed, $\mathcal{H}$ is Lagrangian, hence we have $m_1(\mathcal{H}) = 0$; but if property $(\mu)_s$ held for A/K, then (for some C) the inequality

$$\frac{\ell - 1}{2} \leq [K(\mathcal{H}) \cap K(\mu_{\ell^\infty}) : K] \leq C\left[K(\mu_{\ell^{m_1(\mathcal{H})}}) : K\right] = C$$

would be satisfied by all the primes in our infinite family $\mathcal{F}$, and this is clearly absurd. This establishes theorem 2.

References

1. Borovoĭ, M.V.: The action of the Galois group on the rational cohomology classes of type (p, p) of abelian varieties. Mat. Sb. (N.S.) **94(136)**, 649–652, 656 (1974)
2. Deligne, P., Milne, J.S., Ogus, A., Shih, K.: Hodge cycles, motives, and Shimura varieties, *Lecture Notes in Mathematics*, vol. 900. Springer-Verlag, Berlin-New York (1982)
3. Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. **73**(3), 349–366 (1983). DOI 10.1007/BF01388432. URL http://dx.doi.org/10.1007/BF01388432
4. Hindry, M., Ratazzi, N.: Torsion dans un produit de courbes elliptiques. J. Ramanujan Math. Soc. **25**(1), 81–111 (2010)

5. Hindry, M., Ratazzi, N.: Points de torsion sur les variétés abéliennes de type GSp. J. Inst. Math. Jussieu **11**(1), 27–65 (2012). DOI 10.1017/S147474801000023X. URL http://dx.doi.org/10.1017/S147474801000023X
6. Hindry, M., Ratazzi, N.: Torsion pour les variétés abéliennes de type I et II. ArXiv e-prints (2015)
7. Jelonek, Z.: On the effective Nullstellensatz. Invent. Math. **162**(1), 1–17 (2005). DOI 10.1007/s00222-004-0434-8. URL http://dx.doi.org/10.1007/s00222-004-0434-8
8. Kollár, J.: Sharp effective Nullstellensatz. J. Amer. Math. Soc. **1**(4), 963–975 (1988). DOI 10.2307/1990996. URL http://dx.doi.org/10.2307/1990996
9. Lang, S.: Algebraic groups over finite fields. Amer. J. Math. **78**, 555–563 (1956)
10. Liu, Q.: Algebraic geometry and arithmetic curves, *Oxford Graduate Texts in Mathematics*, vol. 6. Oxford University Press, Oxford (2002). Translated from the French by Reinie Erné, Oxford Science Publications
11. Milne, J.S.: Basic theory of affine group schemes (2012). Available at www.jmilne.org/math/
12. Moonen, B.J.J., Zarhin, Y.G.: Hodge and Tate classes on simple Abelian fourfolds. Duke Math. J **77**, 553–581 (1995)
13. Mumford, D.: A note of Shimura's paper "Discontinuous groups and abelian varieties". Math. Ann. **181**, 345–351 (1969)
14. Pjateckiĭ-Šapiro, I.I.: Interrelations between the Tate and Hodge hypotheses for abelian varieties. Mat. Sb. (N.S.) **85(127)**, 610–620 (1971)
15. Serre, J.P.: Letter to K. Ribet, January 29th, 1981. In: Œuvres. Collected papers. IV. Springer-Verlag, Berlin (2000)
16. Serre, J.P.: Letter to K. Ribet, March 7th, 1986. In: Œuvres. Collected papers. IV. Springer-Verlag, Berlin (2000)
17. Serre, J.P.: Letter to M-F. Vigneras, January 1st, 1983. In: Œuvres. Collected papers. IV. Springer-Verlag, Berlin (2000)
18. Ullmo, E., Yafaev, A.: Mumford-Tate and generalised Shafarevich conjectures. Annales mathématiques du Québec **37**(2), 255–284 (2013). DOI 10.1007/s40316-013-0009-4. URL http://dx.doi.org/10.1007/s40316-013-0009-4
19. Vasiu, A.: Some cases of the Mumford-Tate conjecture and Shimura varieties. Indiana Univ. Math. J. **57**(1), 1–75 (2008). DOI 10.1512/iumj.2008.57.3513. URL http://dx.doi.org/10.1512/iumj.2008.57.3513
20. Wallach, N.R.: On a theorem of Milnor and Thom. In: Topics in geometry, *Progr. Nonlinear Differential Equations Appl.*, vol. 20, pp. 331–348. Birkhäuser Boston, Boston, MA (1996)
21. Waterhouse, W.C.: Introduction to affine group schemes, *Graduate Texts in Mathematics*, vol. 66. Springer-Verlag, New York-Berlin (1979)
22. Wintenberger, J.P.: Démonstration d'une conjecture de Lang dans des cas particuliers. J. Reine Angew. Math. **553**, 1–16 (2002). DOI 10.1515/crll.2002.099. URL http://dx.doi.org/10.1515/crll.2002.099
23. Zarhin, Y.G.: Abelian varieties, ℓ-adic representations and Lie algebras. Rank independence on ℓ. Invent. Math. **55**(2), 165–176 (1979). DOI 10.1007/BF01390088. URL http://dx.doi.org/10.1007/BF01390088