# Kummer theory for abelian varieties

Flavio Perissinotto

**Abstract**

We outline a program to make Kummer theory effective in the setting of abelian varieties. We make progress on many aspects of this program and complete it for abelian varieties with complex multiplication. We also investigate analogues of Schinzel's theorem on abelian radical extensions in the context of abelian varieties.

## 1 Introduction

Let $A$ be an abelian variety of dimension $g$ defined over a number field $K$, for which we fix an algebraic closure $\overline{K}$. We denote by $A[N]$ the group of torsion points in $A(\overline{K})$ of order dividing $N$. If $P \in A(K)$, we denote by $K(\frac{1}{N}P)$ the smallest extension of $K$ containing all points $Q \in A(\overline{K})$ such that $NQ = P$. We fix a rational point $P \in A(K)$ and assume that the set $\mathbb{Z}P$ of multiples of $P$ is Zariski-dense in $A$.

Let $\kappa_N$ be the Kummer representation attached to $A$ and $P$. This is a representation of the absolute Galois group of $K(A[N])$ with values in $A[N] \cong (\mathbb{Z}/N\mathbb{Z})^{2g}$ whose image is isomorphic to the Galois group of the extension $K(\frac{1}{N}P)/K(A[N])$ (we refer to Section 1.2 for precise definitions). Our aim is to find an effective bound, independent of $N$, for the so-called Kummer failure of maximality, namely the ratio

$$f_N := \frac{N^{2g}}{\#(\mathrm{Im}(\kappa_N))}.$$

Remark that we will actually tackle the more general problem where $P$ is replaced by a finitely generated subgroup $G$ of $A(K)$.

The image of the Kummer representation for abelian varieties was first studied by Ribet [22], who proved the uniform boundedness of $f_N$ as $N = \ell$ ranges over the prime

numbers. He showed that the Kummer failure is trivial for all primes $\ell$ large enough, assuming a list of 'axioms' which were later proved by Faltings [4] and Serre [24]. The existence of a uniform bound for $f_N$ as $N$ ranges over all positive integers was proven by Bertrand [2]. Hindry [6] later gave a streamlined proof. The existence of a uniform bound on $f_N$ implies that, in the the $\ell$-adic (resp. adelic) case, the image of the Kummer representation is an open subgroup of $(\mathbb{Z}_\ell)^{2g}$ (resp. $(\hat{\mathbb{Z}})^{2g}$).

In the case of elliptic curves, effective bounds for the Kummer failure are known. The work of Javan Peykar [7] deals with CM elliptic curves, while the work of Tronto and Lombardo [14] handles the case of non-CM elliptic curves. In both cases, the effective bound is obtained by exploiting certain properties of the endomorphism ring. In his recent paper [26], Tronto refined these results, setting the foundations for possible similar results for other commutative connected algebraic groups. More precisely, he proves that, under certain conditions on the endomorphism ring and the geometric torsion of the algebraic group (which are satisfied for elliptic curves), the Kummer failure can be bounded in terms of three independent parameters.

In the case of abelian varieties, Tronto's result [26, Theorem 5.4] is as follows, where we denote by $\tau_\infty$ (resp. $\kappa_\infty$), the adelic torsion (resp. Kummer) representation:

**Theorem 1.1** (Tronto)**.** *Let $P \in A(K)$ be such that $\mathbb{Z}P$ is Zariski-dense in $A$, and let $\Gamma := \{Q \in A(\overline{K}) \mid \exists n \in \mathbb{Z}_{\geqslant 1} : nQ \in \langle P \rangle\}$. Assume that $A(\overline{K})_{\mathrm{tors}}$ is an injective $\mathrm{End}_K(A)$-module. Suppose that there exist positive integers $d, n, m$ such that:*

1. *$d(\Gamma \cap A(K)) \subseteq \langle P \rangle + A(K)_{\mathrm{tors}}$;*
2. *$n \cdot H^1(\mathrm{Im}(\tau_\infty), A(\overline{K})_{\mathrm{tors}}) = 0$;*
3. *the subring of $\mathrm{End}(A(\overline{K})_{\mathrm{tors}})$ generated by $\mathrm{Im}(\tau_\infty)$ contains $m \cdot \mathrm{End}(A(\overline{K})_{\mathrm{tors}})$.*

*Then $\mathrm{Im}(\kappa_\infty)$ contains $(dnm \cdot \hat{\mathbb{Z}})^{2g}$.*

Consequently, we have the following result (justified by Lemma 3.9):

**Corollary 1.2.** *For any positive integer $N$, the Kummer failure $f_N$ divides $(dnm)^{2g}$.*

In this paper we show that the three integers $d, n, m$ as in Theorem 1.1 exist for every abelian variety $A$ over a number field. Moreover, we prove that $d$ and $m$ can always be effectively bounded in terms of basic invariants of $A/K$, while $n$ can be effectively bounded in the case $A$ has CM over $\overline{K}$. We also show that the assumption on $A(\overline{K})_{\mathrm{tors}}$ is satisfied by an abelian variety $A'$ in the same isogeny class of $A$ and we study how

the minimal admissible values of $d, n, m$ change under isogeny. Since the degree of the isogeny $A \to A'$ can also be bounded effectively in terms of $A/K$, we ultimately obtain bounds that only depend on the abelian variety $A$, on the field $K$, and on the divisibility of the point $P$ (respectively, of the subgroup $G$ of $A(K)$) for which we consider the Kummer representation.

One of the results of this paper is therefore the following:

**Theorem 1.3.** *Consider an abelian variety $A$ of dimension $g$ defined over a number field $K$ and with complex multiplication over $\overline{K}$. Let $G$ be a finitely generated subgroup of $A(K)$. Suppose a set of generators of $G$ is linearly independent over $\mathrm{End}_K(A)$ and is given in terms of a $\mathbb{Z}$-basis for $A(K)/A(K)_{\mathrm{tors}}$. There exists an effective upper bound for $f_N$, uniform in $N$ and depending only on $K$, $A$ and $G$.*

Our bound in Theorem 1.3 depends exponentially on $[K(A[3]) : K]$, on $[K : \mathbb{Q}]$ and on $g$, and linearly on the Faltings height $h_F(A)$ and on the 'divisibility parameter' $d$ of the group $G$ (see Section 2.2). Notice that $[K(A[3]) : K]$ divides $\#\,\mathrm{GL}_{2g}(\mathbb{Z}/3\mathbb{Z})$ and can therefore be bounded by $3^{4g^2}$.

Further results in this paper arise from the study of possible analogues of Schinzel's theorem on radical extensions [23, Theorem 2] (see Theorem 8.1) in the setting of abelian varieties.

One result coming from the study of this problem is the following:

**Theorem 1.4.** *Let $A$ be an abelian variety over a number field $K$. The following are equivalent:*

*(i) The extension $K(A[n])/K$ is abelian for every positive integer $n$.*

*(ii) The variety $A$ is $K$-isogenous to a product of simple abelian varieties with CM over $K$.*

## 1.1 Structure of the paper

The paper is almost entirely dedicated to the proof of Theorem 1.3. In Section 2 we adapt Theorem 1.1 to the case when we consider a group $G$ instead of a single point $P$, and we provide methods to compute effectively the integer $d$. In Section 3 we prove a result (Theorem 3.1) which allows us to compare the cardinality of the images of torsion and Kummer representations for isogenous abelian varieties. In Section 4 we

take care of the assumption of Theorem 1.1 concerning the injectivity of the module of torsion points $A(\overline{K})_{\mathrm{tors}}$ by finding an abelian variety $A'$ isogenous to $A$ that satisfies this condition. Theorem 4.3 proves the existence of such an isogeny $A \to A'$ and gives an effective bound to its degree. Sections 5 and 6 are devoted, respectively, to finding effective bounds for the integer $n$ of Theorem 1.1 if $A$ has complex multiplication (see Corollary 5.2) and for the integer $m$ of the Theorem 1.1 for any abelian variety (see Theorem 6.3). Section 7 contains the proof of Theorem 1.3.

Finally, in Section 8, independently of the rest of the paper, we discuss analogues of Schinzel's theorem (see Theorem 8.1) in the case of abelian varieties, obtaining necessary and sufficient conditions for the extension $\mathrm{Gal}(K(\frac{1}{N}P)/K)$ to be abelian. In particular, we prove Theorem 1.4.

## 1.2 Preliminaries

Let $A$ be an abelian variety defined over a number field $K$ for which we fix an algebraic closure $\overline{K}$, and let $g$ be its dimension. Let $R := \mathrm{End}_K(A)$ be the ring of $K$-endomorphisms of $A$. We denote by $A(K)$ the Mordell-Weil group of $K$-rational points of $A$. If $N$ is any positive integer, we denote by $[N]$ the multiplication-by-$N$ endomorphism of $A$ and by $A[N]$ the subgroup of torsion points of $A(\overline{K})$ of order dividing $N$. We also write $K(A[N])$ for the $N$-th torsion field of $K$, obtained by adjoining to $K$ the coordinates of the points in $A[N]$. For any prime $\ell$ we write $T_\ell(A) := \varprojlim_n A[\ell^n]$ for the $\ell$-adic Tate module of $A$. Recall that $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. We write $V_\ell(A)$ for the base change of $T_\ell(A)$ to $\mathbb{Q}_\ell$ and $T(A) := \varprojlim_N A[N] = \prod_\ell T_\ell(A)$ for the adelic Tate module. For an element $e \in T_\ell(A)$, we write $e = (e^{(n)})_{n\in\mathbb{Z}_{\geqslant 1}}$ with $e^{(n)} \in A[\ell^n]$ and $\ell e^{(n)} = e^{(n-1)}$.

Let $\ell$ be a prime and let $z$ be an integer or an $\ell$-adic integer. We denote by $v_\ell(z)$ the $\ell$-adic valuation of $z$, with the convention $v_\ell(0) = +\infty$.

For any field $F$, after fixing an algebraic closure $\overline{F}$, we denote by $G_F$ the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$. For every positive integer $N$, fix a basis $\{T_1^{(N)}, T_2^{(N)}\}$ of $A[N]$ such that $NT_i^{(M)} = T_i^{(M/N)}$ whenever $N \mid M$.

We denote by $\tau_{A,N}$ the *$N$-torsion representation*

$$\tau_{A,N} : G_K \to \mathrm{Aut}(A[N])$$

given by the $\mathbb{Z}/N\mathbb{Z}$-linear action of $G_K$ on $A[N]$. The group $A[N]$ is abstractly isomorphic to $(\mathbb{Z}/N\mathbb{Z})^{2g}$, hence we also have $\mathrm{Aut}(A[N]) \cong \mathrm{GL}_{2g}(\mathbb{Z}/N\mathbb{Z})$. The Galois

group $\mathrm{Gal}(K(A[N])/K)$ can be identified with the image of $\tau_{A,N}$, and hence with a subgroup of $\mathrm{GL}_{2g}(\mathbb{Z}/N\mathbb{Z})$.

Given a point $P \in A(K)$, we denote by $K(\frac{1}{N}P)$ the smallest extension of $K$ over which all points $Q \in A(\overline{K})$ such that $NQ = P$ are defined. In particular, $K(\frac{1}{N}P) \supseteq K(A[N])$. We denote by $\kappa_{A,N}$ the *Kummer representation*

$$\begin{aligned} \kappa_{A,N} : G_{K(A[N])} &\to A[N] \\ \sigma &\mapsto \sigma(Q) - Q, \end{aligned}$$

where $Q \in A(\overline{K})$ is such that $NQ = P$. Since we only consider the action of $G_{K(A[N])}$, it is easy to see that the map $\kappa_{A,N}$ is independent of the choice of $Q$. The Galois group $\mathrm{Gal}(K(\frac{1}{N}P)/K(A[N]))$ can be identified with the image of $\kappa_{A,N}$, and hence with a subgroup of $(\mathbb{Z}/N\mathbb{Z})^{2g}$. We call *Kummer failure of maximality*, denoted by $f_N$, the integer $N^{2g}/\#\operatorname{Im}(\kappa_{A,N})$.

Fix a set of points $\{Q^{(N)}\}_{N\in\mathbb{Z}_{>0}} \subseteq A(\overline{K})$ such that $Q^{(1)} = P$ and $NQ^{(M)} = Q^{(M/N)}$ whenever $N \mid M$. An element $\sigma \in \mathrm{Gal}(K(\frac{1}{N}P)/K)$ can be expressed as a $(2g+1) \times (2g+1)$ matrix $M_\sigma$ with entries in $\mathbb{Z}/N\mathbb{Z}$ of the form

$$M_\sigma = \left(\begin{array}{c|c} B_\sigma & t_\sigma \\ \hline 0 & 1 \end{array}\right), \tag{1}$$

where $B_\sigma$ is the image of $\sigma$ under $\tau_{A,N}$, while $t_\sigma = \sigma(Q^N) - Q^N \in \operatorname{Im}(\kappa_{A,N})$. Given two elements $\sigma, \tau \in \mathrm{Gal}(K(\frac{1}{N}P)/K)$, we have that $M_{\sigma\tau} = M_\sigma M_\tau$.

Fix a prime $\ell$. By taking the inverse limit over $n$, the representations $\tau_{A,\ell^n}$ and $\kappa_{A,\ell^n}$ yield the *$\ell$-adic torsion representation* $\tau_{A,\ell^\infty} : G_K \to \mathrm{Aut}(T_\ell(A))$ and the *$\ell$-adic Kummer representation* $\kappa_{A,\ell^\infty} : G_{K(A[\ell^\infty])} \to T_\ell(A)$. Likewise, by taking the inverse limit over all positive integers $N$, we get the *adelic torsion representation* $\tau_{A,\infty} : G_K \to \mathrm{Aut}(T(A))$ and the *adelic Kummer representation* $\kappa_{A,\infty} : G_{K(A(\overline{K})_{\mathrm{tors}})} \to T(A)$. If the abelian variety $A$ is clear from the context, we drop the subscript $A$ from the notation.

We denote by $K_{\mathrm{tors}}$ the smallest extension of $K$ over which all points in $A(\overline{K})_{\mathrm{tors}}$ are defined. We let

$$\Gamma := \{Q \in A(\overline{K}) \mid \exists n \in \mathbb{Z}_{\geqslant 1} : nQ \in \langle P \rangle\}$$

and denote by $K_{\mathrm{kum}}$ the smallest extension of $K_{\mathrm{tors}}$ over which all points in $\Gamma$ are defined. We call $K_{\mathrm{tors}}$ and $K_{\mathrm{kum}}$ respectively the *torsion extension* and the *Kummer extension* of $K$ associated with $A$ and $P$.

By taking the limit, with our previous identifications, in the $\ell$-adic situation we have

$$\mathrm{Gal}(K(A[\ell^\infty])/K) \cong \mathrm{Im}(\tau_{\ell^\infty}) \subseteq \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$$

and

$$\mathrm{Gal}\left(K\left(\frac{1}{\ell^\infty}P\right)\Big/K(A[\ell^\infty])\right) \cong \mathrm{Im}(\kappa_{\ell^\infty}) \subseteq (\mathbb{Z}_\ell)^{2g}$$

and in the adelic case we have

$$\mathrm{Gal}(K_{\mathrm{tors}}/K) \cong \mathrm{Im}(\tau_\infty) \subseteq \mathrm{GL}_{2g}(\hat{\mathbb{Z}})$$

and

$$\mathrm{Gal}(K_{\mathrm{kum}}/K_{\mathrm{tors}}) \cong \mathrm{Im}(\kappa_\infty) \subseteq (\hat{\mathbb{Z}})^{2g}.$$

Moreover, an element $\sigma \in \mathrm{Gal}(K(\frac{1}{\ell^\infty}P)/K)$ (resp. $\sigma \in \mathrm{Gal}(K_{\mathrm{kum}}/K)$) can be identified with a matrix as in (1), where $B_\sigma$ is the image of $\sigma$ under $\tau_{\ell^\infty}$ (resp. $\tau_\infty$) and $t_\sigma$ is the inverse limit over $n$ of $\sigma(Q^{\ell^n})-Q^{\ell^n}$ (resp. the inverse limit over $N$ of $\sigma(Q^N)-Q^N$).

# 2 The divisibility parameter

Let $G$ be a subgroup of $A(K)$ generated by $r$ points that are linearly independent over $\mathrm{End}_K(A)$. For a positive integer $N$, let

$$\frac{1}{N}G := \{Q \in A(\overline{K}) \mid NQ \in G\} \quad \text{and} \quad \Gamma_G := \bigcup_N \frac{1}{N}G.$$

We consider the Kummer extension $K(\Gamma_G)/K_{\mathrm{tors}}$, which generalises the case considered in Theorem 1.1 (which corresponds to the case of rank 1). In this situation, the adelic Kummer representation we consider is

$$\kappa_N : G_{K(A[N])} \to \mathrm{Hom}\left(\frac{1}{N}G\Big/(G + A[N]), A[N]\right)$$
$$\sigma \mapsto (Q \mapsto \sigma(Q) - Q),$$

where the target space can be identified with $A[N]^r$. Indeed, if $P_1, \ldots, P_r$ are generators of $G$, an element in the codomain of $\kappa_N$ is uniquely determined by the images of points $Q_i$ such that $NQ_i = P_i$ (for each $i$ such image is independent of the choice of $Q_i$). The image of $\kappa_N$ is isomorphic to the Galois group of the Kummer extension

$K(\frac{1}{N}G)/K(A[N])$, and we define the Kummer failure of maximality in this situation as $f_N = N^{2gr}/\#\operatorname{Im}(\kappa_N)$. Similarly, the adelic representation is

$$\kappa_\infty : G_{K_{\mathrm{tors}}} \to \operatorname{Hom}\left(\Gamma_G \Big/ (G + A(\overline{K})_{\mathrm{tors}}), A(\overline{K})_{\mathrm{tors}}\right) \cong A(\overline{K})^r_{\mathrm{tors}}.$$

Remark that, if $r = 1$, the assumption that $P$ is linearly independent over $\operatorname{End}_K(A)$ is equivalent to requiring that $\mathbb{Z}P$ is Zariski-dense in $A$, and ensures that the index $[A(\overline{K})_{\mathrm{tors}} : \operatorname{Im}(\kappa_\infty)]$ is finite. Notice that Ribet in [22] uses the same assumption, which is needed to generalise [6, Proposition 1] to subgroups $G$ of $A(K)$.

Theorem 1.1 and Corollary 1.2 still hold with the expected adjustments, namely:

**Theorem 2.1.** *Let $G$ be a subgroup of $A(K)$ that is generated by $r$ elements that are linearly independent over $\operatorname{End}_K(A)$. Assume that $A(\overline{K})_{\mathrm{tors}}$ is an injective $R$-module. Suppose that there exist positive integers $d, n, m$ such that:*

1. *$d(\Gamma_G \cap A(K)) \subseteq G + A(K)_{\mathrm{tors}}$;*
2. *$n \cdot H^1(\operatorname{Im}(\tau_\infty), A(\overline{K})_{\mathrm{tors}}) = 0$;*
3. *the subring of $\operatorname{End}(A(\overline{K})_{\mathrm{tors}})$ generated by $\operatorname{Im}(\tau_\infty)$ contains $m \cdot \operatorname{End}(A(\overline{K})_{\mathrm{tors}})$.*

*Then $\operatorname{Im}(\kappa_\infty)$ contains $(dnm \cdot \hat{\mathbb{Z}})^{2gr}$. In particular, for any positive integer $N$, the Kummer failure $f_N$ divides $(dnm)^{2gr}$.*

The smallest positive integer $d$ that satisfies condition (1) in Theorem 1.1 (resp. Theorem 2.1) is called the *divisibility parameter* of $P$ (resp. of $G$).

**Lemma 2.2.** *The divisibility parameter $d$ exists. It is effectively computable if $P$ (resp. a set of generators of $G$) is known in terms of a $\mathbb{Z}$-basis for $A(K)/A(K)_{\mathrm{tors}}$.*

*Proof.* We can compute $d$ as shown in [27, Section 6.1]. Indeed, the method used for elliptic curves also applies to general abelian varieties. □

**Remark 2.3.** *In order to apply Lemma 2.2, we only need to know the non-zero coefficients of the point $P$ (resp. of the generators of the group $G$) with respect to some (potentially unknown) basis for $A(K)/A(K)_{\mathrm{tors}}$. Therefore, a priori, we do not need to know what the basis is, or even what the rank of the Mordell-Weil group is, to effectively compute $d$. Moreover, in the case a single point $P$ is considered, the parameter of divisibility $d$ is simply the $\gcd$ of its coefficients in any basis representation.*

We may still be able to bound the parameter $d$ effectively, through other methods. An example is the following result, which applies for example to Jacobians of curves of genus 2.

**Theorem 2.4.** *Let $A$ be an abelian variety over a number field $K$. Let $P \in A(K)$, and suppose that there exist:*

1. *an algorithm that, given a point in $A(K)$, computes its canonical height (up to arbitrary numerical precision);*
2. *an algorithm that, given a positive real number $\alpha$, enumerates the (finitely many) points in $A(K)$ whose canonical height is less than $\alpha$.*

*Then the divisibility parameter $d$ for $P$ can be effectively bounded.*

*Proof.* The parameter $d$ is the maximal integer for which there exist $Q \in A(K)$ and $T \in A(K)_{\mathrm{tors}}$ such that $P = dQ + T$. By standard properties of the canonical height $\hat{h}$, we know that $\hat{h}(P) = d^2\hat{h}(Q)$.

The canonical height $\hat{h}(P)$ can be computed through algorithm 1. Consider the finite set of points

$$S = \{Q' \in A(K) \;\big|\; \hat{h}(Q') \leqslant \hat{h}(P)\}$$

which is the output of algorithm 2 applied to the real number $\hat{h}(P)$, and let $S' = S \setminus A(K)_{\mathrm{tors}}$. Then we have:

$$d \leqslant \sqrt{\hat{h}(P)\left(\min_{Q' \in S'} \hat{h}(Q')\right)^{-1}}.$$

Note that, while there are more efficient algorithms to determine the set $A(K)_{\mathrm{tors}}$, the knowledge of the set $S$ is sufficient to determine it: indeed, $A(K)_{\mathrm{tors}}$ is contained in $S$, and we can test whether a point $T \in S$ is torsion by computing $iT$ for $i = 1, \ldots, \#S$ (indeed, the order of a torsion point is at most $\#A(K)_{\mathrm{tors}}$, which in turn is at most $\#S$) □

**Remark 2.5.** *Let $J$ be the Jacobian of an algebraic curve $C$ of genus 2 over a number field $K$ and let $P \in J(K)$. Suppose we know the equation of the curve $C$ and the Kummer coordinates of the point $P$ (see [19, §3]). Then there exist algorithms as in Theorem 2.4 (see for example [19]). The divisibility parameter $d$ for $P$ can therefore be effectively bounded in this case.*

**Example 2.6.** Consider the hyperelliptic curve $\mathcal{C}$ of genus 2 over $\mathbb{Q}$ given by the equation:

$$y^2 = x^6 - 6x^4 + 2x^3 + 5x^2 - 2x + 1$$

and let $J$ be the Jacobian of $\mathcal{C}$. Consider the rational points $p_1 = (-1, -1)$ and $p_2 = (2, 1)$ of $\mathcal{C}$. Let $P$ be the point of $J$ corresponding to the divisor class $[p_2 - p_1]$. One can compute that $\hat{h}(P) \sim 0.669$ and that the set

$$S' = \{P' \in J(\mathbb{Q}) \mid \hat{h}(P') \leqslant \hat{h}(P), P' \notin J(\mathbb{Q})_{\mathrm{tors}}\}$$

consists of 26 points, with $\min_{S'} \hat{h}(P') \sim 0.128$. The parameter $d$ is then bounded by $(\hat{h}(P)/\min_{S'} \hat{h}(P'))^{1/2} \sim 2.286$. Indeed, it can be checked in this case that $d = 1$.

# 3 Torsion and Kummer extensions for isogenous abelian varieties

Throughout this section, let $A$ and $A'$ be two isogenous abelian varieties of dimension $g$ defined over a number field $K$, and let $\varphi : A \to A'$ be a fixed $K$-isogeny between them. Let $D$ denote the degree of $\varphi$. We first define the tangent space $\mathcal{T}_\ell$ of the $\ell$-adic torsion representation of an abelian variety. We then compare the degrees of the torsion and Kummer extensions of $K$ associated with $A$ and $A'$. To do so, we compare the images of the relevant Galois representations. In particular, we will prove the following result, consequence of Lemmas 3.6 and 3.10 and Corollary 3.11:

**Theorem 3.1.** *Let $\varphi : A \to A'$ be an isogeny of abelian varieties of degree $D$ and consider a point $P \in A(K) \setminus A(K)_{\mathrm{tors}}$. For every prime $\ell$ and for every positive integer $n$ we have*

$$\#\operatorname{Im}(\tau_{A',\ell^n}) \leqslant (\#\mathcal{T}_\ell)^{v_\ell(D)} \cdot \#\operatorname{Im}(\tau_{A,\ell^n})$$
$$\frac{\ell^{2gn}}{\#\operatorname{Im}(\kappa_{A',\ell^n})} \Big| \ell^{v_\ell(D)} \cdot \# \frac{T_\ell(A)}{\operatorname{Im}(\kappa_{A,\ell^\infty})}$$

*and, for every positive integer $N$, we have*

$$\frac{N^{2g}}{\#\operatorname{Im}(\kappa_{A',N})} \Big| D \cdot \# \frac{T(A)}{\operatorname{Im}(\kappa_{A,\infty})}$$

*where the Kummer representations on $A$ and $A'$ are relative to the points $P$ and $\varphi(P)$ respectively, and where $\mathcal{T}_\ell$ is the tangent space of $\tau_{A,\ell^\infty}$.*

There exists a $K$-isogeny $\psi : A' \to A$ such that $\psi \circ \varphi = [D]$. If a prime $\ell$ does not divide $D$, then $[D]$ induces an isomorphism on $T_\ell(A)$, and therefore the map $T_\ell(A) \to T_\ell(A')$ induced by $\varphi$ is an isomorphism. It follows that the $\ell$-adic torsion representations on $A$ and $A'$ are isomorphic. If $\ell \mid D$, then $[D]$ is not an isomorphism on the Tate module, but it becomes an isomorphism on $V_\ell(A)$. The two torsion representations are again isomorphic when tensored by $\mathbb{Q}_\ell$, however, in general, $\mathrm{Im}(\tau_{A,\ell^\infty})$ and $\mathrm{Im}(\tau_{A',\ell^\infty})$ are not conjugate subgroups of $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$.

## 3.1 The tangent space of the image of the $\ell$-adic representation

Consider an abelian variety $A$ of dimension $g$ defined over a number field $K$. For a prime $\ell$ and a positive integer $n$, consider the group $\mathrm{Im}(\tau_{\ell^n})$ as a subgroup of $\mathrm{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z})$. Notice that we have

$$\frac{\#\,\mathrm{Im}(\tau_{\ell^{n+1}})}{\#\,\mathrm{Im}(\tau_{\ell^n})} = \#\ker\left(\mathrm{Im}(\tau_{\ell^{n+1}}) \xrightarrow{\bmod \ell^n} \mathrm{Im}(\tau_{\ell^n})\right).$$

The projection $\mathrm{Im}(\tau_{\ell^{n+1}}) \to \mathrm{Im}(\tau_{\ell^n})$ is surjective, and we can identify its kernel with a subgroup of

$$\ker\left(\mathrm{GL}_{2g}\left(\mathbb{Z}\big/\ell^{n+1}\mathbb{Z}\right) \xrightarrow{\bmod \ell^n} \mathrm{GL}_{2g}\left(\mathbb{Z}\big/\ell^{n}\mathbb{Z}\right)\right) = \mathrm{Id} + \ell^n \mathcal{M}_{2g\times 2g}(\mathbb{F}_\ell).$$

It is easy to check that the following map is a group homomorphism:

$$\begin{aligned}\ker\left(\mathrm{Im}(\tau_{\ell^{n+1}}) \to \mathrm{Im}(\tau_{\ell^n})\right) &\to \mathcal{M}_{2g\times 2g}(\mathbb{F}_\ell)\\ (\mathrm{Id} + \ell^n S) &\mapsto S.\end{aligned}$$

We call $\mathcal{T}_\ell^{(n)}$ its image: it is an $\mathbb{F}_\ell$-vector subspace of $\mathcal{M}_{2g\times 2g}(\mathbb{F}_\ell)$.

**Lemma 3.2** ( [13, Proof of Lemma 9]). *We have $\mathcal{T}_\ell^{(n)} \subseteq \mathcal{T}_\ell^{(n+1)}$ for all integers $n \geqslant 1$.*

Since $\mathcal{T}_\ell^{(n)}$ is a subspace of $\mathcal{M}_{2g\times 2g}(\mathbb{F}_\ell)$, which is a finite dimensional vector space over $\mathbb{F}_\ell$, Lemma 3.2 implies that $\dim(\mathcal{T}_\ell^{(n)})$ and hence also $\mathcal{T}_\ell^{(n)}$ stabilise for $n$ large enough. We denote such stabilised space by $\mathcal{T}_\ell$ and we call it the *tangent space* of the $\ell$-adic torsion representation $\tau_{\ell^\infty}$ (see [13, Definition 9]). In particular, for $n$ large enough, we have

$$\#\,\mathrm{Im}(\tau_{\ell^n}) = k \cdot \ell^{n\cdot\dim(\mathcal{T}_\ell)} \tag{2}$$

for some constant $k$ which does not depend on $n$.

**Example 3.3.** For an elliptic curve $E$, the tangent space $\mathcal{T}_\ell$ can be described as follows (see [12, Definitions 18 and 19]):

- if $E$ does not have CM, then $\mathcal{T}_\ell = \mathcal{M}_{2\times 2}(\mathbb{F}_\ell)$;
- if $E$ has CM and $\ell$ splits in $\mathrm{End}_{\overline{K}}(E)$, then, for a suitable choice of basis, $\mathcal{T}_\ell = \mathrm{Diag}_2(\mathbb{F}_\ell)$, the subspace of diagonal matrices;
- if $E$ has CM and $\ell > 2$ is inert in the quadratic ring $\mathrm{End}_{\overline{K}}(E)$, then, in a suitable basis,
$$\mathcal{T}_\ell = \left\{ \begin{pmatrix} x & dy \\ y & x \end{pmatrix} \mid x, y \in \mathbb{F}_\ell \right\},$$
where $d$ is a quadratic non-residue modulo $\ell$;
- more generally, if $\mathrm{End}_{\overline{K}}(E)$ is isomorphic to the quadratic ring $\mathbb{Z}[x]/(x^2 - cx - d)$, then in a suitable basis
$$\mathcal{T}_\ell = \left\{ \begin{pmatrix} x & dy \\ y & x + yc \end{pmatrix} \mid x, y \in \mathbb{F}_\ell \right\}.$$

## 3.2 Isogenies and Tate modules

Given a $K$-isogeny $\varphi$ between the abelian varieties $A$ and $A'$ and a prime $\ell$, there is an associated $\mathbb{Z}_\ell$-linear map on the Tate modules: if $e = (e^{(n)})_{n\in\mathbb{Z}_{\geqslant 1}}$ is a point of $T_\ell(A)$, we set $\varphi(e) = (\varphi(e^{(n)}))_{n\in\mathbb{Z}_{\geqslant 1}}$. Fix bases $v_1, \ldots, v_{2g}$ of $T_\ell(A)$ and $v'_1, \ldots, v'_{2g}$ of $T_\ell(A')$. Then $v_1 \otimes 1, \ldots, v_{2g} \otimes 1$ and $v'_1 \otimes 1, \ldots, v'_{2g} \otimes 1$ are bases for $V_\ell(A)$ and $V_\ell(A')$, respectively. We can describe $\varphi : T_\ell(A) \to T_\ell(A')$ as a matrix $M \in \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$ with $\ell$-integral entries (we write this matrix with respect to the chosen bases). Notice that the multiplication by an integer $N$ from $A$ to itself corresponds to the matrix $N\,\mathrm{Id}$, and the isogeny $\psi$ from $A'$ to $A$ such that $\psi \circ \varphi = [D]$ corresponds to the matrix $DA^{-1}$, which again has integer entries.

**Lemma 3.4.** *The matrix $M$ is such that $v_\ell(\det(M)) = v_\ell(D)$.*

*Proof.* One may easily check that the map
$$\begin{aligned} (T_\ell(A) \otimes \mathbb{Q}_\ell)/T_\ell(A) &\to A[\ell^\infty] \\ e \otimes \ell^{-n} &\mapsto e^{(n)} \end{aligned}$$

is an isomorphism of $\mathbb{Z}_\ell$-modules. Moreover, the kernel of the action of $M$ by multiplication on $(T_\ell(A) \otimes \mathbb{Q}_\ell)/T_\ell(A) \cong A[\ell^\infty]$ is the $\ell$-part of the kernel of the isogeny $\varphi$, whose cardinality equals $\ell^{v_\ell(D)}$.

As $\mathbb{Z}_\ell$ is a PID, we can write $M = P_1 S P_2$, where $S$ is the Smith normal form of $M$ and $P_1$ and $P_2$ are invertible matrices in $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$, so that $v_\ell(\det(M)) = v_\ell(\det(S))$. Since the matrices $P_1$ and $P_2$ are invertible, it suffices to compute the $\ell$-adic valuation of the cardinality of the kernel of the action of the diagonal matrix $S$.

Let the diagonal entries of $S$ be of the form $u_i \ell^{k_i}$ for $i = 1, \ldots, 2g$, where $u_i \in \mathbb{Z}_\ell^\times$ and the $k_i$ are non-negative integers. Let

$$h = \left( \sum_{n=1}^{t_i} w_{i,n} \ell^{-n} + \mathbb{Z}_\ell \right)_{i=1,\ldots,2g}$$

be an element in $(T_\ell(A) \otimes \mathbb{Q}_\ell)/T_\ell(A) \cong (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$, where the $t_i$ are non-negative integers and the $w_{i,n}$ are in $\{0, \cdots, \ell - 1\}$, with $w_{i,t_i} \neq 0$. Then for any element $h_0 \in \mathbb{Q}_\ell^{2g}$ whose class in $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$ is $h$, we have $S \cdot h_0 \in \mathbb{Z}_\ell^{2g}$ if and only if $k_i \geqslant t_i$ for all $i$, and hence the $\ell$-adic valuation of the cardinality of the kernel of $\varphi$ is $\sum_{i=1}^{2g} k_i = v_\ell(\det(S))$. □

The map $\varphi \otimes 1$ is an isomorphism between $V_\ell(A)$ and $V_\ell(A')$. A $K$-isogeny is compatible with the Galois action of $G_K$, hence for every $\sigma \in G_K$ and every $v \in V_\ell(A)$ we have:

$$\sigma \cdot v = (\varphi \otimes 1)^{-1}(\sigma \cdot (\varphi \otimes 1)(v)).$$

We conclude that

$$\mathrm{Im}(\tau_{A,\ell^\infty}) = M^{-1} \mathrm{Im}(\tau_{A',\ell^\infty}) M, \tag{3}$$

where $\mathrm{Im}(\tau_{A,\ell^\infty})$ is represented in the basis $v_i \otimes 1$ and $\mathrm{Im}(\tau_{A',\ell^\infty})$ is represented in the basis $v_i' \otimes 1$.

**Example 3.5.** Let $E$ be an elliptic curve over a number field $K$ and let $T \in E[\ell](K)$ be a point of prime order $\ell$. Consider the elliptic curve $E' = E/\langle T \rangle$ and let $\varphi$ be the canonical projection $\varphi : E \to E'$.

Let $e_1, e_2$ be a basis of $T_\ell(E)$, where $e_1^{(1)} = T$. We define a basis $e_1', e_2'$ of $T_\ell(E')$ as follows:

1. we set $e_2' = \varphi(e_2)$. Notice that $e_2^{(1)} \notin \langle T \rangle$ since $T$ and $e_2^{(1)}$ are linearly independent, and hence $e_2'^{(1)} \neq O$. This implies that $e_2'$ generates a saturated submodule of $T_\ell(E')$.

2. we choose $e'_1 = (e_1'^{(n)})_{n\in\mathbb{Z}_{\geqslant 1}} \in T_\ell(E')$ that completes $e'_2$ to a basis of $T_\ell(E')$ (the existence of such an $e'_1$ follows from the structure theory of finitely generated modules over a PID: any saturated submodule of a finitely generated, free module has a free complement).

Therefore we have $\varphi(e_2) = e'_2$ and $\varphi(e_1) = \alpha e'_1 + \beta e'_2$ with $\alpha, \beta \in \mathbb{Z}_\ell$. By definition of the isogeny $\varphi$, we know that $\varphi(e_1) \equiv 0 \mod \ell$, hence $\alpha \equiv \beta \equiv 0 \mod \ell$. Now, $\alpha \not\equiv 0 \bmod \ell^2$, for otherwise we would have

$$\varphi(e_1^{(2)}) = \beta e_2'^{(2)} = v(\ell\varphi(e_2^{(2)})) = v\varphi(e_2^{(1)})$$

where $\beta \equiv v\ell \mod \ell^2$, contradicting the fact that $\ker\varphi$ is generated by $T = e_1^{(1)}$. We then have

$$\langle \begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \begin{pmatrix}0\\ 1\end{pmatrix}\rangle = \langle \begin{pmatrix}\ell\\ 0\end{pmatrix}, \begin{pmatrix}0\\ 1\end{pmatrix}\rangle$$

as $\mathbb{Z}_\ell$-modules, hence we can choose $\alpha = \ell$ and $\beta = 0$. We conclude that, with this choice of basis, $\varphi$ acts on the Tate module as multiplication by the matrix $M = \left(\begin{smallmatrix}\ell & 0\\ 0 & 1\end{smallmatrix}\right)$. In particular, it is not a bijection on the Tate modules.

Consider now $\mathrm{Im}(\tau_{E,\ell^\infty})$. Since $T \in E[\ell](K)$ and $e_1^{(1)} = T$, we have

$$\mathrm{Im}(\tau_{E,\ell^\infty}) \subseteq \left\{ \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_\ell) \;\middle|\; a \equiv 1, c \equiv 0 \bmod \ell \right\}$$

as all elements of $G_K$ fix the point $T$. Applying (3) we get:

$$\mathrm{Im}(\tau_{E',\ell^\infty}) \subseteq \left\{ \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_\ell) \;\middle|\; a \equiv 1, b \equiv 0 \bmod \ell \right\}.$$

Automorphisms in $\mathrm{Im}(\tau_{E',\ell^\infty})$ do not necessarily fix a point of $E'[\ell]$, but fix the line corresponding to the second basis vector. In particular, $E'$ admits an $\ell$-isogeny over $K$: this is not surprising, as the isogeny having as kernel this fixed line is the dual of the map $E \to E'$ we started with.

## 3.3 Torsion extensions

Let $\varphi : A \to A'$ be a $K$-isogeny of degree $D$ and consider $\mathrm{Im}(\tau_{A,\ell^n})$ and $\mathrm{Im}(\tau_{A',\ell^n})$. Let $\mathcal{T}_\ell$ and $\mathcal{T}'_\ell$ be the tangent spaces relative to $A$ and $A'$, respectively.

**Lemma 3.6.** *For every $n \geqslant 1$ we have*

$$(\#\mathcal{T}'_\ell)^{-(2g-1)v_\ell(D)} \leqslant \frac{\#\operatorname{Im}(\tau_{A',\ell^n})}{\#\operatorname{Im}(\tau_{A,\ell^n})} \leqslant (\#\mathcal{T}_\ell)^{v_\ell(D)}.$$

*Proof.* Let $e := v_\ell(D)$ and $D = \ell^e D'$, where $D'$ is coprime to $\ell$. We claim that $A'[\ell^n] \subseteq \varphi(A[\ell^{n+e}])$. Indeed, let $P \in A'[\ell^n]$ and let $P = \varphi(Q)$ for some $Q \in A(\overline{K})$, which exists by surjectivity of $\varphi$ over $\overline{K}$. Consider an integer $E$ such that $ED' \equiv 1 \pmod{\ell^n}$, so that $P = ED'P$ and let $Q' = ED'Q$. We have

$$0 = \ell^n P = \ell^n \varphi(Q) = \varphi(\ell^n Q).$$

Since $\ell^n Q \in \ker(\varphi)$, we have $\ell^n Q \in A[D]$ and therefore $\ell^n Q' \in A[\ell^e]$. The claim follows as $P = \varphi(Q')$ and $Q' \in A[\ell^{n+e}]$. Since $\varphi$ commutes with the action of $G_K$, we have the inclusion

$$K(\varphi(A[\ell^{n+e}])) \subseteq K(A[\ell^{n+e}])$$

and hence $K(A'[\ell^n]) \subseteq K(A[\ell^{n+e}])$. The same reasoning, applied to the isogeny $\psi : A' \to A$ such that $\psi \circ \varphi = [D]$, implies that $K(A[\ell^n]) \subseteq K(A'[\ell^{n+(2g-1)e}])$ (recall that $\psi$ has degree $D^{2g-1}$). Since $\operatorname{Im}(\tau_{A,\ell^n})$ is isomorphic to the Galois group of the torsion extension $K(A[\ell^n])/K$, we have:

$$\frac{\#\operatorname{Im}(\tau_{A',\ell^n})}{\#\operatorname{Im}(\tau_{A,\ell^n})} \leqslant \frac{\#\operatorname{Gal}\left(K(A[\ell^{n+e}])/K\right)}{\#\operatorname{Gal}\left(K(A[\ell^n])/K\right)} \xrightarrow{n\to\infty} (\#\mathcal{T}_\ell)^e$$

and

$$\frac{\#\operatorname{Im}(\tau_{A',\ell^n})}{\#\operatorname{Im}(\tau_{A,\ell^n})} \geqslant \frac{\#\operatorname{Gal}\left(K(A'[\ell^n])/K\right)}{\#\operatorname{Gal}\left(K(A'[\ell^{n+(2g-1)e}])/K\right)} \xrightarrow{n\to\infty} \frac{1}{(\#\mathcal{T}'_\ell)^{(2g-1)e}}.$$

By Lemma 3.2, for any positive integer $t$ the sequence $(\#\operatorname{Gal}(K(A[\ell^{n+t}])/K(A[\ell^n])))_n$ is increasing (and eventually constant) and the same holds for $A'$, so this concludes the proof.

□

**Corollary 3.7.** *The tangent spaces $\mathcal{T}_\ell$ and $\mathcal{T}'_\ell$ have the same dimension.*

*Proof.* For $n$ large enough, let $\#\operatorname{Im}(\tau_{A,\ell^n}) = k_A \ell^{n\cdot\dim(T_\ell)}$ and $\#\operatorname{Im}(\tau_{A',\ell^n}) = k_{A'}\ell^{n\cdot\dim(\mathcal{T}'_\ell)}$ for some positive constants $k_A$ and $k_{A'}$ as in (2). By Lemma 3.6, $(k_A/k_{A'})\ell^{n(\dim(\mathcal{T}'_\ell)-\dim(\mathcal{T}_\ell))}$ is bounded, which implies that $\dim(\mathcal{T}'_\ell) = \dim(\mathcal{T}_\ell)$. □

**Remark 3.8.** *Corollary 3.7 can also be obtained by noticing that the $\mathbb{F}_\ell$-dimension of $\mathcal{T}_\ell$ (resp. $\mathcal{T}'_\ell$) is equal to the $\mathbb{Q}_\ell$-dimension of the identity component of the $\ell$-adic monodromy group attached to $A$ (resp. $A'$). Since an isogeny $A \to A'$ induces an isomorphism between the identity components of the respective $\ell$-adic monodromy groups, the claim follows.*

## 3.4 Kummer extensions

Let $\varphi : A \to A'$ be a $K$-isogeny of degree $D$. Let $M$ be the matrix associated with $\varphi$ introduced in Section 3.2. Let $P \in A(K) \setminus A(K)_{\mathrm{tors}}$ be a fixed non-torsion point. By equation (3) and the Galois-equivariance of $\varphi$, and using the notation (1), we have that

$$\begin{gathered}\mathrm{Gal}\left(K\left(\frac{1}{\ell^\infty}P\right)\Big/K\right) \xrightarrow{\sim} \mathrm{Gal}\left(K\left(\frac{1}{\ell^\infty}\varphi(P)\right)\Big/K\right)\\ \left(\begin{array}{c|c} B & t \\ \hline 0 & 1 \end{array}\right) \mapsto \left(\begin{array}{c|c} MBM^{-1} & Mt \\ \hline 0 & 1 \end{array}\right).\end{gathered}$$

Consider the $\ell$-adic Kummer representations $\kappa_{A,\ell^\infty}$ and $\kappa_{A',\ell^\infty}$, with respect to the points $P$ and $\varphi(P)$ respectively. The previous formula implies

$$\mathrm{Im}(\kappa_{A',\ell^\infty}) = \varphi(\mathrm{Im}(\kappa_{A,\ell^\infty})). \tag{4}$$

**Lemma 3.9.** *For any prime $\ell$ and any positive integers $n$ and $N$, we have*

$$\begin{aligned} f_{\ell^n} &\mid [T_\ell(A) : \mathrm{Im}(\kappa_{\ell^\infty})] \\ f_N &\mid [T(A) : \mathrm{Im}(\kappa_\infty)]. \end{aligned}$$

*Proof.* The considerations in [14, Remark 2.6] hold also in the case of abelian varieties. The statement follows. □

**Lemma 3.10.** *Let $\varphi : A \to A'$ be an isogeny of abelian varieties of degree $D$. Fix a point $P \in A(K) \setminus A(K)_{\mathrm{tors}}$ and suppose that the set $\mathbb{Z}P$ of multiples of $P$ is Zariski-dense in $A$. Consider the Kummer representations $\kappa_{A,\ell^\infty}$ and $\kappa_{A',\ell^\infty}$ relative to $(A, P)$ and $(A', \varphi(P))$ respectively. Then we have*

$$\#\frac{T_\ell(A')}{\mathrm{Im}(\kappa_{A',\ell^\infty})} = \ell^{v_\ell(D)} \cdot \#\frac{T_\ell(A)}{\mathrm{Im}(\kappa_{A,\ell^\infty})}$$

*and*

$$\#\frac{T_\ell(A')}{\kappa_{A',\ell^\infty}(\mathrm{Gal}(\overline{K}/K_{\mathrm{tors}}))} = \ell^{v_\ell(D)} \cdot \#\frac{T_\ell(A)}{\kappa_{A,\ell^\infty}(\mathrm{Gal}(\overline{K}/K_{\mathrm{tors}}))}.$$

*Proof.* As in Section 3.2, let $M$ be the matrix representing the injective linear morphism $\varphi : T_\ell(A) \to T_\ell(A')$ induced by $\varphi$ on the Tate modules. Recall from (4) that $\varphi(\mathrm{Im}(\kappa_{A,\ell^\infty})) = \mathrm{Im}(\kappa_{A',\ell^\infty})$. Let $\mu$ (resp. $\mu'$) be the Haar measure on $V_\ell(A)$ (resp. $V_\ell(A')$), normalised so that $\mu(T_\ell(A)) = 1$ (resp. $\mu'(T_\ell(A')) = 1$). Pulling back $\mu'$ along the invertible linear map $\varphi : V_\ell(A) \to V_\ell(A')$ we obtain a Haar measure on $V_\ell(A)$, which is therefore a multiple $c\,\mu$ of the Haar measure $\mu$. To determine $c$, we use the change of variables formula in $\ell$-adic integration:

$$c = c\int_{T_\ell(A)} d\mu = \int_{T_\ell(A)} \varphi^*(d\mu') = \int_{\varphi(T_\ell(A))} d\mu' = \mu'(\varphi(T_\ell(A))).$$

Since $T_\ell(A')$ is the disjoint union of $[T_\ell(A') : \varphi(T_\ell(A))]$ translates of $\varphi(T_\ell(A))$, we have

$$\mu'(\varphi(T_\ell(A))) = \frac{1}{[T_\ell(A') : \varphi(T_\ell(A))]} = \ell^{-v_\ell(\det(M))} = \ell^{-v_\ell(D)},$$

where the last two equalities follows from well-known facts in the theory of modules over a PID (Smith normal form) and Lemma 3.4. The Kummer image $\mathrm{Im}(\kappa_{A,\ell^\infty})$ is an open subgroup of $T_\ell(A)$: see for example [6, Proposition 1], which implies the openness of $\mathrm{Im}(\kappa_{A,\ell^\infty})$ by passing to the inverse limit (because $\mathbb{Z}P$ is Zariski-dense in $A$). We can then compute, using again the change of variables formula in $\ell$-adic integration:

$$\begin{aligned}\mu'(\mathrm{Im}(\kappa_{A',\ell^\infty})) &= \int_{\mathrm{Im}(\kappa_{A',\ell^\infty})} d\mu' = \int_{M(\mathrm{Im}(\kappa_{A,\ell^\infty}))} d\mu' \\ &= \int_{\mathrm{Im}(\kappa_{A,\ell^\infty})} M^*(d\mu') = c\int_{\mathrm{Im}(\kappa_{A,\ell^\infty})} d\mu = \ell^{-v_\ell(D)}\mu(\mathrm{Im}(\kappa_{A,\ell^\infty})).\end{aligned}$$

This concludes the proof of the first claimed equality, as

$$\#\frac{T_\ell A'}{\mathrm{Im}(\kappa_{A',\ell^\infty})} = \frac{1}{\mu'(\mathrm{Im}(\kappa_{A',\ell^\infty}))} \qquad \text{and} \qquad \#\frac{T_\ell A}{\mathrm{Im}(\kappa_{A,\ell^\infty})} = \frac{1}{\mu(\mathrm{Im}(\kappa_{A,\ell^\infty}))}.$$

The proof of the second equality in the statement follows, simply replacing $\mathrm{Im}\,\kappa_{A',\ell^\infty}$ with $\kappa_{A',\ell^\infty}(\mathrm{Gal}(\overline{K}/K_{\mathrm{tors}}))$ and $\mathrm{Im}\,\kappa_{A,\ell^\infty}$ with $\kappa_{A,\ell^\infty}(\mathrm{Gal}(\overline{K}/K_{\mathrm{tors}}))$. Note that the torsion fields of $A$ and $A'$ coincide. □

**Corollary 3.11.** *With notation and assumptions as in Lemma 3.10, let $N$ be any positive integer. We have*

$$\frac{N^{2g}}{\#\operatorname{Im}(\kappa_{A',N})} \mid D \cdot \#\frac{T(A)}{\operatorname{Im}(\kappa_{A,\infty})}.$$

*Proof.* By Lemma 3.9, the left-hand side divides $[T(A') : \operatorname{Im}(\kappa_{A',\infty})]$. We have

$$\frac{T(A')}{\operatorname{Im}(\kappa_{A',\infty})} \cong \frac{\prod_\ell T_\ell(A')}{\prod_\ell \kappa_{A',\ell^\infty}(\operatorname{Gal}(\overline{K}/K_{\mathrm{tors}}))} \cong \prod_\ell \frac{T_\ell(A')}{\kappa_{A',\ell^\infty}(\operatorname{Gal}(\overline{K}/K_{\mathrm{tors}}))}.$$

By the second part of Lemma 3.10 we then obtain that the order of $\frac{T(A')}{\operatorname{Im}(\kappa_{A',\infty})}$ is

$$\prod_\ell \#\frac{T_\ell(A')}{\kappa_{A',\ell^\infty}(\operatorname{Gal}(\overline{K}/K_{\mathrm{tors}}))} = \prod_\ell \ell^{v_\ell(D)} \frac{T_\ell(A)}{\kappa_{A,\ell^\infty}(\operatorname{Gal}(\overline{K}/K_{\mathrm{tors}}))} = D \cdot \#\frac{T(A)}{\operatorname{Im}\kappa_{A,\infty}}.$$

□

# 4 Injectivity of $A(\overline{K})_{\mathrm{tors}}$

Let $A$ be an abelian variety defined over a number field $K$. Consider the $\operatorname{End}_K(A)$-module $A(\overline{K})_{\mathrm{tors}}$. We aim to understand when this module is injective. By [26, Remark 5.2], if $\operatorname{End}_K(A)$ is a domain which is a maximal order inside $\operatorname{End}_K(A) \otimes \mathbb{Q}$, then $A(\overline{K})_{\mathrm{tors}}$ is an injective $\operatorname{End}_K(A)$-module. Up to isogeny, we can always assume that $\operatorname{End}_K(A)$ is a maximal order in $\operatorname{End}_K(A) \otimes \mathbb{Q}$ (see [11, Lemma A.3]). Our goal is then to drop the assumption that $\operatorname{End}_K(A)$ is a domain, or equivalently, that $A$ is a simple abelian variety over $K$.

Up to isogeny, we can write any abelian variety $A$ over $K$ as $A_1^{n_1} \times \ldots \times A_r^{n_r}$ for some non-negative integers $r, n_1, \ldots, n_r$, where each $A_i$ is $K$-simple and $A_i$ is not $K$-isogenous to $A_j$ for $i \neq j$. We will consider separately powers of simple abelian varieties and products of abelian varieties sharing no common factors.

**Lemma 4.1.** *If $A(\overline{K})_{\mathrm{tors}}$ is an injective $\operatorname{End}_K(A)$-module, then $A^n(\overline{K})_{\mathrm{tors}}$ is an injective $\operatorname{End}_K(A^n)$-module.*

*Proof.* We have $\operatorname{End}_K(A^n) = \mathcal{M}_{n\times n}(\operatorname{End}_K(A))$. Since any ring $R$ is Morita equivalent to $\mathcal{M}_{n\times n}(R)$ (see for example [8, Theorem 17.20]), we have an equivalence between the categories $\operatorname{End}_K(A)$-Mod and $\mathcal{M}_{n\times n}(\operatorname{End}_K(A))$-Mod. In particular, the

module $A(\overline{K})_{\mathrm{tors}}$ in the category of $\mathrm{End}_K(A)$-modules corresponds to $A^n(\overline{K})_{\mathrm{tors}} = (A(\overline{K})_{\mathrm{tors}})^{\oplus n}$ in the category of $\mathcal{M}_{n\times n}(\mathrm{End}_K(A))$ modules through this equivalence, from which the statement follows. □

**Lemma 4.2.** *Let $A$ and $B$ be abelian varieties defined over $K$ with no common factor and let $C = A \times B$. Then $C(\overline{K})_{\mathrm{tors}}$ is an injective $\mathrm{End}_K(C)$-module if and only if $A(\overline{K})_{\mathrm{tors}}$ and $B(\overline{K})_{\mathrm{tors}}$ are injective as modules over $\mathrm{End}_K(A)$ and $\mathrm{End}_K(B)$ respectively.*

*Proof.* We have $C(\overline{K})_{\mathrm{tors}} = A(\overline{K})_{\mathrm{tors}} \times B(\overline{K})_{\mathrm{tors}}$ and $\mathrm{End}_K(C) \cong \mathrm{End}_K(A) \times \mathrm{End}_K(B)$ as $A$ and $B$ have no common factor. We conclude because for two rings $R_1$ and $R_2$ the product category $R_1$-Mod $\times$ $R_2$-Mod and the category $(R_1 \times R_2)$-Mod are equivalent. □

**Theorem 4.3.** *Let $A$ be an abelian variety defined over the field $K = K(A[3])$. There exist an isogeny $\varphi : A \to A'$ and an isogeny $\psi : A' \to A$ such that $A'(\overline{K})_{\mathrm{tors}}$ is an injective $\mathrm{End}_K(A')$-module. There exists an effective bound $\Xi$, depending only on $A$ and on $K$, for the degree of both $\varphi$ and $\psi$.*

*Proof.* Since $K = K(A[3])$, we know that $\mathrm{End}_K(A) = \mathrm{End}_{\overline{K}}(A)$ (see for instance [3, Lemme 8]). By [21, Théorèmes 1.1 and 1.6] there exist $K$-isogenies $\varphi : A \to A' \cong A_1^{n_1} \times \ldots \times A_r^{n_r}$ and $\psi : A' \to A$, where the $A_i$ are geometrically simple abelian varieties defined over $K$ that are pairwise not isogenous over $\overline{K}$ and such that $\mathrm{End}_K(A_i)$ is a maximal order in $\mathrm{End}_K(A_i) \otimes \mathbb{Q} = \mathrm{End}_{\overline{K}}(A_i) \otimes \mathbb{Q}$ for each $i$. By [26, Remark 5.2], $A_i(\overline{K})_{\mathrm{tors}}$ is an injective $\mathrm{End}_K(A_i)$-module, so we can conclude by Lemmas 4.1 and 4.2. An effective bound $\Xi$ for the degree of $\varphi$ and $\psi$ is given in [5, Théorème 1.9(2)], see Remark 4.4 (notice that another non-effective but sharper bound is given in [5, Théorème 1.4]). □

**Remark 4.4.** *Let $A$ be an abelian variety of dimension $g$ defined over a field $K$. The explicit value of $\Xi$ given in [5] is:*

$$\Xi(A) = \Big((7g)^{8g^2}[K:\mathbb{Q}]\max(1, \log[K:\mathbb{Q}], h_F(A))\Big)^{2g^2}$$

*and it depends only on the dimension $g$ of $A$, on the degree $[K:\mathbb{Q}]$ and on the Faltings height $h_F(A)$.*

# 5 Torsion representations and homotheties for CM abelian varieties

In this section we consider the cohomology group $H^1(\mathrm{Im}(\tau_\infty), A(\overline{K})_{\mathrm{tors}})$ for an abelian variety $A$. We look for a positive integer $n$ that is a multiple of the exponent of this cohomology group. The best tool we have to find such an integer is Sah's Lemma (see for instance [1, Lemma A.2]), which states that, if an element $z$ is in the center of a group $G$, then $(z - \mathrm{Id})H^1(G, M) = 0$ for any $G$-module $M$, where we identify $z$ to the endomorphism of $H^1(G, M)$ induced by it. To use Sah's Lemma in our case, we consider homotheties inside $\mathrm{Im}(\tau_\infty)$.

Serre proved that for any abelian variety $A$ there exists an integer $c \geqslant 1$ such that the image of the torsion representation $\tau_\infty$ contains all the homotheties inside $(\hat{\mathbb{Z}}^\times)^c$ (see [28, Théorème 3]), but this integer $c$ is not effective.

The following result by Eckstein [3, Théorème 7] gives us an effective integer $c$ in the case of abelian varieties with complex multiplication, therefore allowing us to provide an effective integer $n$ to use in Theorem 1.1 (2) in this case.

**Theorem 5.1** (Eckstein)**.** *Let $A$ be an abelian variety over a number field $K$ and with complex multiplication over $\overline{K}$. Then $\mathrm{Im}(\tau_{\ell^\infty})$ contains $(\mathbb{Z}_\ell^\times)^c \subseteq \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$, where $c = [K(A[3]) : \mathbb{Q}]$ (which divides $\#\,\mathrm{Aut}(A[3]) \cdot [K : \mathbb{Q}]$).*

**Corollary 5.2.** *Let $A$ be an abelian variety over a number field $K$. There exists a positive integer $n$ such that*

$$n \cdot H^1(\mathrm{Im}(\tau_\infty), A(\overline{K})_{\mathrm{tors}}) = 0.$$

*If $A$ has complex multiplication over $\overline{K}$, then we can effectively bound the integer $n$ in terms of $g = \dim A$ and $[K : \mathbb{Q}]$.*

*Proof.* Let $c$ be a positive integer such that $\mathrm{Im}(\tau_\infty) \supseteq (\hat{\mathbb{Z}}^\times)^c$. In particular, by Theorem 5.1, we can choose $c = [K(A[3]) : \mathbb{Q}]$ if $A$ has complex multiplication over $\overline{K}$. We define the element $z = (z_\ell)_\ell \in \hat{\mathbb{Z}}$ as:

$$z_\ell = \begin{cases} 1 + 2^{v_2(c)+2} & \text{if } \ell = 2 \\ 2^c & \text{otherwise} \end{cases}$$

We have $z_\ell \in (\mathbb{Z}_\ell^\times)^c$ for each $\ell$, and therefore $z \in \hat{\mathbb{Z}}^{\times c} \subseteq \mathrm{Im}(\tau_\infty)$. Define

$$n := 2^{v_2(c)+2}(2^c - 1) \in \mathbb{Z}$$

and notice that $z - 1 = un$ for some unit $u \in \hat{\mathbb{Z}}^\times$. By Sah's Lemma, since $z$ is a homothety in $\mathrm{Im}(\tau_\infty)$ and hence in the centre of $\mathrm{Im}(\tau_\infty)$, we have that $z - 1$ kills $H^1(\mathrm{Im}(\tau_\infty), M)$ for any $\mathrm{Im}(\tau_\infty)$-module $M$, and hence the statement follows.

□

# 6 The algebra generated by the image of the torsion representation

In this section, we consider the subring of $\mathrm{End}(A(\overline{K})_{\mathrm{tors}})$ generated by $\mathrm{Im}(\tau_\infty)$. In order to apply Theorem 1.1, we wish to find an integer $m$ such that this subring contains $m \cdot \mathrm{End}(A(\overline{K})_{\mathrm{tors}})$. Notice that in the case of (non-CM) elliptic curves an effective value for such an integer $m$ was found by bounding the so-called parameter of maximal growth $\mu$ (see [27, §6.2]), that is, an integer such that the image of $\tau_\infty$ contains all the elements of the form $\mathrm{Id} + \mu B$ where $B \in \mathrm{End}(A(\overline{K})_{\mathrm{tors}}) \cong \mathcal{M}_{2g\times 2g}(\hat{\mathbb{Z}})$.

Let $R = \mathrm{End}_K(A)$. We first consider the $\ell$-adic case and look for integers $m_\ell$ such that the subring of $\mathrm{End}_R(T_\ell(A))$ generated by $\mathrm{Im}(\tau_{\ell^\infty})$ contains $m_\ell \cdot \mathrm{End}_R(T_\ell(A))$. We rely on the following result by Gaudron and Rémond (see [5, Théorème 1.5(2) and Théorème 1.9(5)]), which will also allow us to patch the various $\ell$-adic results to an adelic one.

**Theorem 6.1** (Gaudron-Rémond)**.** *There exist an integer $d$ and an explicit constant $\Xi$, depending on the abelian variety $A/K$ (see Remark 4.4), such that:*

$$\prod_\ell \mathrm{disc}(\mathbb{Z}_\ell[\mathrm{Im}(\tau_\ell)]) \mid d$$

*and*

$$\prod_\ell \mathrm{disc}(\mathbb{Z}_\ell[\mathrm{Im}(\tau_\ell)]) \leqslant \Xi^2.$$

**Lemma 6.2.** *Let $\ell$ be a prime and $R = \mathrm{End}_K(A)$. There exists a positive integer $m_\ell$ such that the subring of $\mathrm{End}_R(T_\ell A)$ generated by $\mathrm{Im}(\tau_{\ell^\infty})$ contains $m_\ell \cdot \mathrm{End}_R(T_\ell A)$. In particular one can take such an $m_\ell$ that satisfies $m_\ell^2 \mid \mathrm{disc}(\mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})])$.*

*Proof.* Let $V_\ell A = T_\ell A \otimes \mathbb{Q}_\ell$ and consider $\mathrm{End}_{\mathrm{Im}(\tau_{\ell^\infty})}(V_\ell A)$, the endomorphisms of $V_\ell A$ that commute with the elements of $\mathrm{Im}(\tau_{\ell^\infty})$. By Faltings's theorem (see [15, Chapter IV, Theorem 2.5]) we have that $\mathrm{End}_{\mathrm{Im}(\tau_{\ell^\infty})}(V_\ell A) = R \otimes \mathbb{Q}_\ell$. Therefore, the centraliser

$C_{\mathrm{End}(V_\ell A)}(\mathbb{Q}_\ell[\mathrm{Im}(\tau_{\ell^\infty})])$ of $\mathbb{Q}_\ell[\mathrm{Im}(\tau_{\ell^\infty})]$ inside $\mathrm{End}(V_\ell A)$ is $R\otimes\mathbb{Q}_\ell$. Trivially, the centraliser of $R\otimes\mathbb{Q}_\ell$ inside $\mathrm{End}(V_\ell A)$ is $\mathrm{End}_{R\otimes\mathbb{Q}_\ell}(V_\ell A)$, hence by the double centraliser theorem (see for example [17, Chapter IV, Theorem 1.14]) we obtain $\mathrm{End}_{R\otimes\mathbb{Q}_\ell}(V_\ell A) = \mathbb{Q}_\ell[\mathrm{Im}(\tau_{\ell^\infty})]$. This implies that $\mathrm{rk}_{\mathbb{Z}_\ell}(\mathrm{End}_R(T_\ell A)) = \mathrm{rk}_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})])$, and hence that the index $[(\mathrm{End}_R(T_\ell A)) : \mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})]]$ is finite. This proves the existence of $m_\ell$, which can be taken to be this index.

The second statement follows from the basic properties of discriminants, since we have

$$\mathrm{disc}(\mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})]) = [(\mathrm{End}_R(T_\ell A)) : \mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})]]^2 \cdot \mathrm{disc}(\mathrm{End}_R(T_\ell A)).$$

□

The next result can also be obtained directly from [5, Corollaire 13.8], but with a less sharp bound.

**Theorem 6.3.** *There exists a positive integer $m$ such that the subring of $\mathrm{End}(A(\overline{K})_{\mathrm{tors}})$ generated by $\mathrm{Im}(\tau_\infty)$ contains $m \cdot \mathrm{End}(A(\overline{K})_{\mathrm{tors}})$. We may take $m$ such that $m \leqslant \Xi$, where $\Xi$ is as in Remark 4.4.*

*Proof.* If we let $m_\ell$ be as in Lemma 6.2, by Theorem 6.1 we have $m_\ell = 1$ for almost all $\ell$. We can therefore define the integer $m = \prod_\ell m_\ell$, which is as requested because

$$\begin{aligned} m \cdot \mathrm{End}_R(TA) = m \cdot \prod_\ell \mathrm{End}_R(T_\ell A) &= \prod_\ell (m_\ell \cdot \mathrm{End}_R(T_\ell A)) \\ &\subseteq \prod_\ell \mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})] = \hat{\mathbb{Z}}[\mathrm{Im}(\tau_\infty)] \end{aligned}$$

by Lemma 6.2. To justify the last equality, note that for all $\hat{\mathbb{Z}}$-modules $M$ one has $M = \hat{\mathbb{Z}}M = (\prod_\ell \mathbb{Z}_\ell)\, M = \prod_\ell (\mathbb{Z}_\ell M)$, and it follows from the definitions that

$$\mathbb{Z}_\ell \left( \hat{\mathbb{Z}}[\mathrm{Im}(\tau_\infty)] \right) = \mathbb{Z}_\ell[\mathrm{Im}(\tau_{\ell^\infty})].$$

The last assertion follows from Theorem 6.1. □

# 7 An effective bound for the Kummer failure in the CM case

We are now ready to prove Theorem 1.3:

**Theorem 7.1.** *With the notation and the assumptions of Theorem 1.3, there is an abelian variety $A'$ over $K$ such that $A'(\overline{K})_{\mathrm{tors}}$ is an injective $\mathrm{End}_K(A')$-module and a $K$-isogeny $\varphi : A' \to A$ such that $\deg(\varphi)$ can be effectively bounded (the bound depending only on $A$ and $K$). Moreover, we have*

$$f_N \Big| \deg(\varphi) \cdot (dnm)^{2g} \tag{5}$$

*where $d$ is the divisibility parameter of $G \subseteq A(K)$ and $n > 0$ is the exponent of $H^1(\mathrm{Im}(\tau_{A',\infty}), A'(\overline{K})_{\mathrm{tors}})$ and $m$ is the smallest positive integer such that the subring of $\mathrm{End}(A'(\bar{K})_{\mathrm{tors}})$ generated by $\mathrm{Im}(\tau_{A',\infty})$ contains $m \cdot \mathrm{End}(A'(\bar{K})_{\mathrm{tors}})$. The integer $d$ can be effectively computed and the integers $n$ and $m$ exist and can be effectively bounded (where the bound depends only on $A$ and $K$).*

*Proof.* Since $[K(A[3], \frac{1}{N}G) : K(A[\mathrm{lcm}(3, N)])]$ divides $[K(\frac{1}{N}G) : K(A[N])]$, the Kummer failure for $A$ over $K$ divides the Kummer failure for $A$ over $K(A[3])$, and their ratio is at most $[K(A[3]) : K]$. We will then assume, without loss of generality, that $K = K(A[3])$. By Theorem 4.3 there exist $A'$ and $\varphi$ as in the statement. By Theorem 3.1 we have

$$f_N \Big| \deg(\varphi) \cdot \# \frac{T(A')}{\mathrm{Im}(\kappa_{A',\infty})}. \tag{6}$$

We can now apply Theorem 2.1 to the abelian variety $A'$. By Lemma 2.2, the divisibility parameter $d$ of $G \subseteq A$ is effectively computable, and it is easy to check that this is also the divisibility parameter of $\varphi^{-1}(G) \subseteq A'$. By Corollary 5.2, $n$ can be effectively bounded. By Theorem 6.3 $m$ exists and can be effectively bounded. By (6) and Theorem 2.1 we can conclude that (5) holds.

By Theorem 4.3, $\deg \varphi$ and $m$ are both bounded by the same constant $\Xi$, which only depends on $A$. Finally, the integer $n$ determined in Corollary 5.2 depends on the primes of $K$ for which $A'$ has bad reduction. By [25, Corollary 2], these are precisely the primes of bad reduction of $A$. □

**Corollary 7.2.** *We have*

$$f_N \leqslant \Xi(dn_0\Xi)^{2g} \quad \textit{and} \quad f_N \mid \Xi'(dn_0\Xi')^{2g}$$

*where $n_0$ is an effective constant such that $n_0 \cdot H^1(\mathrm{Im}(\tau_{A',\infty}), A'(\overline{K})_{\mathrm{tors}}) = 0$ and $\Xi$ is as in Remark 4.4 and $\Xi' = e^{\psi(\Xi)}$ where $\psi$ is the second Chebyshev function (namely, $\Xi'$ is the least common multiple of all integers less then or equal to $\Xi$).*

*Proof.* The integer $n_0$ exists by Corollary 5.2 and we may easily conclude. □

**Remark 7.3.** *In Theorem 7.1 we may remove the assumption that $A$ has complex multiplication over $K$, provided that we have an effective bound for $n$. Indeed, we have not assumed complex multiplication to effectively bound* $\deg \varphi$*, $d$ and $m$.*

# 8 Analogues of Schinzel's theorem on radical extensions for division fields

Schinzel's theorem on radical extensions [23, Theorem 2] (see also [10]) gives a characterization of the abelian radical extensions of a field. For number fields, it states:

**Theorem 8.1** (Schinzel)**.** *Let $K$ be a number field and let $n$ be a positive integer. For an element $a \in K$, the Galois group of the splitting field of $x^n - a$ over $K$ is abelian if and only if there exists an element $b \in K$ such that $a^w = b^n$, where $w$ is the largest divisor of $n$ such that $K$ contains the $w$-th roots of unity.*

Let $A$ be an abelian variety over a number field $K$. In this setting, the role of an element $a \in K$ in Schinzel's theorem is played by a point $P \in A(K)$, and similarly the Galois group of the splitting field of $x^n - a$ over $K$ corresponds to the Galois group of the extension $K(\frac{1}{n}P)/K$. Moreover, the group of torsion elements of order $n$ over $\overline{K}$ is cyclic group $\mu_n$ of roots of unity in the setting of Schinzel's theorem and the group $A[n] \cong (\mathbb{Z}/N\mathbb{Z})^{2g}$ in our setting.

A first obstacle to the generalization of Schinzel's theorem to abelian varieties comes from the fact that any cyclotomic extension $K(\zeta_n)/K$ is abelian, but the torsion extension $K(A[n])/K$ need not be, as its Galois group is a subgroup of $\mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z})$. Since $\mathrm{Gal}(K(A[n])/K)$ is a quotient of $\mathrm{Gal}(K(\frac{1}{n}P)/K)$, the latter group can be abelian only when the former is. This leads to the following question, which we answer in Section 8.1:

**Question 8.2.** *When is $K(A[n])/K$ abelian for all values of $n$?*

A second problem arises from the fact that the torsion subgroup $A[n]$ is not cyclic, as the cyclicity of $\mu_n$ plays a vital role in the proof of Schinzel's theorem. On top of this, if $A(K)_{\mathrm{tors}}$ is not cyclic, there is no clear integer $w'$ dividing $n$ which plays the same role as $w$ in the statement of Schinzel's theorem. Two candidates for $w'$ are the largest divisor of $n$ such that $A[w'] \subseteq A(K)$ and the integer $w' = \gcd(\exp(A(K)_{\mathrm{tors}}), n)$. We investigate the following question for both choices of $w'$, and we show in Section 8.2 that the answer is negative in both cases:

**Question 8.3.** *Fix a positive integer $n$ and assume $K(A[n])/K$ is abelian. Is it true that $K(\frac{1}{n}P)/K$ is abelian if and only if there exists $Q \in A(K)$ such that $w'P = nQ$?*

Finally, we consider the following question, to which we can only give a partial answer in Section 8.2:

**Question 8.4.** *Fix a positive integer $n$ and assume $K(\frac{1}{n}P)/K$ is abelian. Can we define a proper divisor $v$ of $n$ such that there exists $Q \in A(K)$ with $vP = nQ$?*

## 8.1 Abelian torsion extensions

The aim of this section is to answer Question 8.2 by proving Theorem 1.4. We show that an abelian variety $A$ is such that $K(A[n])$ is an abelian extension of $K$ for every $n$ if and only if $A$ is $K$-isogenous to a product of simple abelian varieties with CM over $K$. Notice that thea similar result over $\overline{K}$ was already proven in [9, Lemma 8.2].

*Proof of Theorem 1.4.* The abelian variety $A$ is $K$-isogenous to $A' := A_1 \times \cdots \times A_r$ where each $A_i$ is $K$-simple. We clearly have that $K(A'[n]) = K(A_1[n], \ldots, A_r[n])$. By the argument in the proof of Lemma 3.6, there exist integers $d, d' \geqslant 1$ such that $K(A'[n]) \subseteq K(A[nd])$ and $K(A[n]) \subseteq K(A'[nd'])$ for all $n \geqslant 1$. If $K(A[nd])/K$ is an abelian extension, we obtain that $K(A'[n])/K$ is abelian, and the same holds for $K(A_i[n])/K$ for all $i$. Similarly, if $K(A_i[nd'])$ is abelian for all $i$, then $K(A[n])/K$ is abelian. Thus, it suffices to prove the statement in the case $A$ is $K$-simple.

We first prove (i)⇒(ii). Let $g$ be the dimension of $A$ and fix a prime $\ell$. By taking the limit in $n$, since $K(A[\ell^n])/K$ is abelian, the image $G_{\ell^\infty}$ of $\tau_{A,\ell^\infty}$ is an abelian subgroup of $\mathrm{GL}(T_\ell(A)) \cong \mathrm{GL}_{2g}(\mathbb{Z}_\ell) \subset \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$. A well-known theorem of Faltings (see [15, Chapter IV, Theorem 2.5]) gives

$$\mathrm{End}_{G_{\ell^\infty}}(V_\ell(A)) \cong \mathrm{End}_{G_{\ell^\infty}}(\mathbb{Q}_\ell^{2g}) \cong \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell. \tag{7}$$

By assumption, $A$ is $K$-simple, so $\mathrm{End}_K(A)$ is an integral domain. By [18, Proposition 3.6], to prove that $A$ has CM over $K$ we aim to show that $\mathrm{End}_K(A) \otimes \mathbb{Q}$ contains a number field of degree $2g$ over $\mathbb{Q}$ (equivalently, it contains an étale $\mathbb{Q}$-algebra of degree $2g$ over $\mathbb{Q}$). By integrality of the free $\mathbb{Z}$-module $\mathrm{End}_K(A)$, it suffices to show that $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ contains a commutative semisimple $\mathbb{Q}$-subalgebra of rank $2g$.

Let $\mathcal{G}_{\ell^\infty}$ be the Zariski closure of $G_{\ell^\infty}$. Since $G_{\ell^\infty}$ is abelian, the identity component $\mathcal{G}^0_{\ell^\infty}$ is an abelian affine reductive (by Faltings' results [4]) algebraic group, hence a

torus. In particular, all of its irreducible representations over $\overline{\mathbb{Q}_\ell}$, which is algebraically closed of characteristic 0, are 1-dimensional. The same is true for $\mathcal{G}_{\ell^\infty}$ itself since this is a commutative group of multiplicative type [16, Theorem 12.30]. It follows that, as a representation of $G_{\ell^\infty}$, the $\overline{\mathbb{Q}_\ell}$-vector space $T_\ell \otimes \overline{\mathbb{Q}_\ell} \cong \overline{\mathbb{Q}_\ell}^{2g}$ decomposes as $\bigoplus W_i^{\oplus m_i}$, where each $W_i$ is 1-dimensional, $\sum_i m_i = 2g$, and $W_i, W_j$ are non-isomorphic for $i \neq j$.

Using (7) we obtain that $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \overline{\mathbb{Q}_\ell}$ is isomorphic to

$$\mathrm{End}_{G_{\ell^\infty}}(\overline{\mathbb{Q}_\ell}^{2g}) \cong \bigoplus_i \mathrm{End}_{G_{\ell^\infty}}\left(W_i^{\oplus m_i}\right) \cong \bigoplus_i \mathrm{Mat}_{m_i \times m_i}(\overline{\mathbb{Q}_\ell}), \tag{8}$$

where the last equality follows from Schur's lemma on irreducible representations.

Let $D = \mathrm{End}_K(A) \otimes \mathbb{Q}$ and let $F$ be its center. Since $A$ is $K$-simple, $D$ is a central simple algebra over $F$. Let $e = [F : \mathbb{Q}]$ and $m^2 = [D : F]$. As we are working in characteristic zero, we have $em^2 \mid 2g$ (see [20, §21, Theorem 2]). Moreover, the theory of central simple algebras shows that

$$D \otimes_{\mathbb{Q}} \overline{\mathbb{Q}_\ell} \cong \left(\mathrm{Mat}_{m \times m}(\overline{\mathbb{Q}_\ell})\right)^e.$$

Comparing this with (8), we obtain that $em = \sum_i m_i = 2g$ and hence, since $em^2 \mid 2g$, we must have $m = 1$. We conclude that $\mathrm{End}_K(A) \otimes \mathbb{Q}$ contains a field of degree $2g$ over $\mathbb{Q}$.

Now we prove (ii)⇒(i). It suffices to treat the case when $n$ is the power of a prime number $\ell$, and clearly it suffices to show that the extension $K(A[\ell^\infty])/K$ is abelian, or equivalently that $\mathrm{Im}(\tau_{\ell^\infty})$ is abelian. This is a well-known property of (simple) CM abelian varieties, see for example [25, Corollary 2 to Theorem 5]. □

## 8.2 Abelian Kummer extensions

Fix a positive integer $n$. Let $L_n = K(A[n])$ and suppose $\mathrm{Gal}(L_n/K)$ is abelian. Let $L'_n = K(\frac{1}{n}P)$ and $G_n = \mathrm{Gal}(L'_n/K)$. In general, as discussed in Section 1.2 and with the same notation, an element $\sigma \in G_n$ can be represented as a matrix:

$$M_\sigma = \left(\begin{array}{c|c} B_\sigma & t_\sigma \\ \hline 0 & 1 \end{array}\right) \in \mathcal{M}_{(2g+1)\times(2g+1)}(\mathbb{Z}/n\mathbb{Z}).$$

It is easy to check that, in general, two elements $\sigma, \tau$ in $G_n$ commute if and only if

$$(B_\sigma - \mathrm{Id})t_\tau = (B_\tau - \mathrm{Id})t_\sigma.$$

We begin by answering Question 8.3 choosing first $w'$ as the largest divisor of $n$ such that $A[w'] \subseteq A(K)$, and then $w' = \gcd(\exp(A(K)_{\mathrm{tors}}, n))$.

**Let $w'$ be the largest divisor of $n$ such that $A[w'] \subseteq A(K)$.** If there exists a point $Q \in A(K)$ such that $nQ = w'P$, then $G_n$ is abelian, since $K(\frac{1}{n}P)$ is the compositum of the two fields $K(A[n])$ and $K(\frac{1}{w'}Q)$, which are both abelian extensions of $K$. To see that the latter of these extensions is abelian, notice that, since $A[w'] \subseteq A(K)$, the extension $K(\frac{1}{w'}Q)$ is generated by the coordinates of any single point $R \in A(\overline{K})$ with $w'R = Q$.

However, the following example shows that the converse does not hold: if $G_n$ is abelian, there need not exist a point $Q \in A(K)$ such that $nQ = w'P$.

**Example 8.5.** Consider the elliptic curve $E : y^2 = x^3 + 1$ over the field $K = \mathbb{Q}(\sqrt{-3})$ whose torsion subgroup is $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. We have $w' = 2$. Let $P$ be a torsion point of order 6 and let $n = 3$. The extension $K(\frac{1}{3}P)/K$ is abelian, but there exists no point $Q \in E(K)$ such that $3Q = 2P$, as $Q$ would need to be a $K$-rational point of order 9.

**Let $w'$ be the greatest common divisor of $n$ and $\exp(A(K)_{\mathrm{tors}})$.** In this case neither of the two implications in Schinzel's theorem holds (see Examples 8.9 and 8.10), but we have the following result if $n = p$ is prime.

**Lemma 8.6.** *Let $p$ be a prime number and suppose that $K(A[p])/K$ is an abelian extension with group $H_p$. The exponent of $A(K)_{\mathrm{tors}}$ annihilates $H^1(H_p, A[p])$.*

*Proof.* Let $H_p'$ be the maximal subgroup of $H_p$ of order prime to $p$. Since $H_p$ is abelian, this is the direct product of the $q$-Sylow subgroups of $H_p$ for $q \neq p$. In particular, the order of $H_p/H_p'$ is a power of $p$. Consider the inflation-restriction sequence with respect to the normal subgroup $H_p'$ of $H_p$:

$$0 \to H^1(H_p/H_p', A[p]^{H_p'}) \to H^1(H_p, A[p]) \to H^1(H_p', A[p])^{H_p/H_p'}.$$

Since $(|H_p'|, |A[p]|) = 1$, the cohomology group $H^1(H_p', A[p])$ is trivial. We now distinguish two cases:

1. If $p \mid \#A(K)_{\mathrm{tors}}$, the exponent of $A(K)_{\mathrm{tors}}$ is a multiple of $p$, and therefore it annihilates $H^1(H_p, A[p])$, as it annihilates $A[p]$.

2. If $p \nmid \#A(K)_{\mathrm{tors}}$, then it suffices to prove that $H^1(H_p/H_p', A[p]^{H_p'})$ is trivial. More precisely, we show that $A[p]^{H_p'}$ is trivial. If not, $A[p]^{H_p'}$ would be a non-zero vector space over $\mathbb{F}_p$. It is well-known that a $p$-group acting on a non-trivial

vector space over $\mathbb{F}_p$ has non-zero fixed points. Applying this fact to the $p$-Sylow subgroup of $H_p/H_p'$ (which is the image in $H_p/H_p'$ of the $p$-Sylow subgroup of $H_p$) yields that $A[p]^{H_p} = A(K)[p]$ is nontrivial, contradiction.

□

**Corollary 8.7.** *Let $p$ be a prime. If $K(\frac{1}{p}P)/K$ is abelian and $A(K)[p] = \{0\}$, then we have $P = pQ$ for some $K$-rational point $Q$.*

*Proof.* Let $H_p$ be the Galois group of the extension $K(A[p])/K$ and let $G_p$ be the Galois group of $K(\frac{1}{p}P)/K$. Consider the following inflation-restriction sequence:

$$0 \to H^1(G_p/H_p, A[p]^{H_p}) \to H^1(G_p, A[p]) \to H^1(H_p, A[p])^{G_p/H_p}.$$

The cohomology group on the left is trivial, as $A[p]^{H_p} = A(K)[p] = \{0\}$, making the map on the right injective. The integer $\exp(A(K)_{\text{tors}})$ kills $H^1(H_p, A[p])^{G_p/H_p}$ by Lemma 8.6, hence $\exp(A(K)_{\text{tors}})$ also annihilates $H^1(G_p, A[p])$. Using the following injective map coming from the exact sequence in [14, Lemma 4.3] when $n = p$:

$$\frac{A(K) \cap pA(K(\frac{1}{p}P))}{pA(K)} \hookrightarrow H^1(G_p, A[p]),$$

we conclude that there exists a $K$-rational point $Q$ such that $P = pQ$. □

**Remark 8.8.** *An analogue of Lemma 8.6 does not hold for composite integers. Indeed, consider the subgroup $H$ of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ generated by the matrices*

$$\begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

*One easily checks that the invariants of $H$ acting on $(\mathbb{Z}/4\mathbb{Z})^2$ are given by $(\mathbb{Z}/2\mathbb{Z})^2$, while $H^1(H, (\mathbb{Z}/4\mathbb{Z})^2)$ has exponent $4$. With MAGMA, we found the following example, where $H$ is the Galois group of $K(E[4])/K$ for the elliptic curve $E$ over $K$, $K(\frac{1}{4}P)/K$ is abelian, but $w'P$ is not 4 times a $K$-rational point, where $w' = \gcd(4, \exp(E(K)_{tors})$.*

**Example 8.9.** Consider the elliptic curve $E : y^2 = x^3 + 2x^2 - 8x$ and $P = (4, 8)$ over the field $K = \mathbb{Q}(i)$. One can check that $E(K)_{\text{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2$ and that $K(\frac{1}{4}P, E[4])/K$ is abelian, with Galois group $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$. We have $w' := \gcd(4, \exp E(K)_{\text{tors}}) = 2$, but $w'P = 4Q$ does not have solutions in $E(K)$.

**Example 8.10.** Consider $n = 2$ and the abelian variety $A = E_1 \times E_2$ over $\mathbb{Q}$, where $E_1 : y^2 + y = x^3 - x$ has trivial torsion over $\mathbb{Q}$ and $E_2 : y^2 + xy = x^3 - x$ has torsion $\mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Q}$. Notice that $w' := \gcd(2, \exp A(\mathbb{Q})_{\mathrm{tors}}) = 2$. Clearly, $\mathbb{Q}(E[2])/\mathbb{Q}$ is not abelian as $\mathbb{Q}(E_1[2])/\mathbb{Q} \cong S_3$. For any point $P \in A(\mathbb{Q})$, we have that $w'P = nQ$ for $Q = P$, but $\mathbb{Q}(\frac{1}{2}P, A[2])/\mathbb{Q}$ is not abelian.

We now address Question 8.4. Let $G_n$ be abelian, and consider the injective homomorphism coming from the exact sequence in [14, Lemma 4.3]:

$$\begin{aligned} \alpha : \frac{A(K) \cap nA(L'_n)}{nA(K)} &\hookrightarrow H^1(G_n, A[n]) \\ P &\mapsto (\sigma \mapsto t_\sigma)\,. \end{aligned} \tag{9}$$

The group ring $\mathbb{Z}[G_n]$ acts on $A(L'_n)$ by extending the Galois action, and therefore it also acts on $H^1(G_n, A[n])$. We call $H$ the kernel of the action of $\mathbb{Z}[G_n]$ on $H^1(G_n, A[n])$, which – by Sah's lemma (see [1, Lemma A.2]) and since $G_n$ is abelian – contains the elements $(\sigma - 1)$ for $\sigma \in G_n$. If $a = \sum_g n_g g$ is an element of $\mathbb{Z}[G_n]$, we denote its trace by $||a|| = \sum_g n_g$. We define $v$ to be the positive integer such that the ideal $v\mathbb{Z}$ is generated by the integers $||h||$ for $h \in H$. Notice that $n \cdot 1 \in H$, therefore $v \mid n$. The following Proposition gives a partial answer to Question 8.4: even if $v$ divides $n$, we are not excluding that $v$ may be $n$ itself.

**Proposition 8.11.** *If $G_n$ is abelian and $v$ is as above, then there exists $Q \in A(K)$ such that $vP = nQ$.*

*Proof.* Since $G_n$ is abelian, the map $\alpha$ in (9) is $\mathbb{Z}[G_n]$-equivariant. Indeed, we have

$$\alpha(\sigma T)(\rho) = \rho(\sigma t) - \sigma t = \sigma(\rho t) - \sigma t = \sigma\left((\alpha T)(\rho)\right)$$

for all $\sigma, \rho \in G_n$ and for all $T \in (A(K) \cap nA(L'_n))/nA(K)$, with $t$ such that $nt = T$. Fix $h \in H$. We have

$$\alpha(hP) = h\alpha(P) = 0$$

by definition of $H$. Since $P$ belongs to $A(K)$, the Galois group $G_n$ acts trivially on it, and therefore $hP = ||h||P$. As $\alpha$ is injective, this implies that $||h||P \in nA(K)$, concluding the proof. □

## Acknowledgements

First of all, I would like to thank Davide Lombardo for his invaluable assistance throughout the preparation of this paper. He suggested several key ideas that led to Theorem 1.3 and consistently directed me to the best bibliography. Secondly, I am grateful to my supervisor, Antonella Perucca, for her steady support and her suggestion which resulted in Section 8. I also extend my thanks to Marco Streng for his asssistance on Theorem 1.4. Finally, I thank my other supervisor, Peter Stevenhagen, along with Hendrik Lenstra and Peter Bruin for helpful discussions. Supported by the Luxembourg National Research Fund PRIDE17/1224660/GPS. A CC BY or equivalent licence is applied to the AAM/VoR arising from this submission, in accordance with the grant's open access conditions.

## References

[1] Matthew H. Baker and Kenneth A. Ribet. Galois theory and torsion points on curves. volume 15, pages 11–32. 2003. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[2] D. Bertrand. Galois representations and transcendental numbers. In *New advances in transcendence theory (Durham, 1986)*, pages 37–55. Cambridge Univ. Press, Cambridge, 1988.

[3] Carola Eckstein. *Homothéties, à chercher dans l'action de Galois sur des points de torsion*, volume 2005/7 of *Prépublication de l'Institut de Recherche Mathématique Avancée [Prepublication of the Institute of Advanced Mathematical Research]*. Université Louis Pasteur. Institut de Recherche Mathématique Avancée (IRMA), Strasbourg, 2005.

[4] Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[5] Éric Gaudron and Gaël Rémond. Nouveaux théorèmes d'isogénie. *Mém. Soc. Math. Fr. (N.S.)*, (176):vi+129, 2023.

[6] Marc Hindry. Autour d'une conjecture de Serge Lang. *Invent. Math.*, 94(3):575–603, 1988.

[7] Abtien Javan Peykar. *Division points in arithmetic*. PhD thesis, Universiteit Leiden, 2021.

[8] Tsit Yuen Lam. *Lectures on modules and rings*, volume 189 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[9] Samuel Le Fourn, Davide Lombardo, and David Zywina. Torsion bounds for a fixed abelian variety and varying number field. Available at arXiv:2208.02345, 2023.

[10] Hendrik W. Lenstra. Commentary on H: Divisibility and congruences. *Andrzej Schinzel Selecta*, 2:901–902, 2007.

[11] Davide Lombardo. Explicit surjectivity of Galois representations for abelian surfaces and $\mathrm{GL}_2$-varieties. *J. Algebra*, 460:26–59, 2016.

[12] Davide Lombardo and Antonella Perucca. The 1-eigenspace for matrices in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. *New York J. Math.*, 23:897–925, 2017.

[13] Davide Lombardo and Antonella Perucca. Reductions of points on algebraic groups. *J. Inst. Math. Jussieu*, 20(5):1637–1669, 2021.

[14] Davide Lombardo and Sebastiano Tronto. Effective Kummer theory for elliptic curves. *Int. Math. Res. Not. IMRN*, (22):17662–17712, 2022.

[15] James S. Milne. Abelian varieties (v2.00). Course notes available at www.jmilne.org/math, 2008.

[16] James S. Milne. *Algebraic groups*, volume 170 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. The theory of group schemes of finite type over a field.

[17] James S. Milne. Class field theory (v4.03). Course notes available at www.jmilne.org/math, 2020.

[18] James S. Milne. Complex multiplication (v0.10). Course notes available at www.jmilne.org/math, 2020.

[19] Jan Steffen Müller and Michael Stoll. Canonical heights on genus-2 Jacobians. *Algebra Number Theory*, 10(10):2153–2234, 2016.

[20] David Mumford. *Abelian varieties*, volume 5 of *Tata Inst. Fundam. Res., Stud. Math.* London: Oxford University Press, 1970.

[21] Gaël Rémond. Variétés abéliennes et ordres maximaux. *Rev. Mat. Iberoam.*, 33(4):1173–1195, 2017.

[22] Kenneth A. Ribet. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.*, 46(4):745–761, 1979.

[23] Andrzej Schinzel. Abelian binomials, power residues and exponential congruences. *Acta Arithm.*, 32:245–274, 1977.

[24] Jean-Pierre Serre. Résumé des cours de 1985-86, 1986.

[25] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *The Annals of Mathematics, Second Series*, 88:492–517, 1968.

[26] Sebastiano Tronto. Division in modules and Kummer theory. Available at arXiv:2111.14363, 2023.

[27] Sebastiano Tronto. Radical entanglement for elliptic curves. Available at arXiv:2009.08298, 2023.

[28] Jean-Pierre Wintenberger. Démonstration d'une conjecture de Lang dans des cas particuliers. *J. Reine Angew. Math.*, 553:1–16, 2002.