SOME LOCAL-GLOBAL APPLICATIONS OF KUMMER THEORY

E. KOWALSKI

Abstract. We consider some problems in number theory which turn out to depend on various aspects of Kummer theory; among them are (1) does the assertion "b is in the subgroup generated by a" obey a local-global principle for points of an algebraic group over a number field; (2) if two abelian varieties have the same n-division fields for $n \geqslant 1$, what relation is there between them?

1. Introduction

This paper is concerned with some problems which may seem unrelated at first, but will be linked by their respective relations with various forms of Kummer theory.

The first question is, roughly speaking, whether the statement "a is in the subgroup generated by b" obeys a local-global principle, where a and b are rational points on some algebraic group over a number field.

More precisely, let G/k be an algebraic group over a number field k (thinking mostly of elliptic curves, or abelian varieties, or subgroups of $GL(n)$). Let a, b be elements in $G(k)$. One can define the reduction of a and b modulo almost all prime ideals $\mathfrak{p}$ of k. We denote this $a \,(\mathrm{mod}\, \mathfrak{p})$ or $a_{\mathfrak{p}}$ (see later for a more rigorous definition; this suffices for the informal statement that follows).

Our first problem is

Problem 1.1. *With notation as above, assume that for almost all $\mathfrak{p}$, $b \,(\mathrm{mod}\, \mathfrak{p})$ is in the subgroup generated by $a \,(\mathrm{mod}\, \mathfrak{p})$, i.e. there exists $n(\mathfrak{p}) \in \mathbf{Z}$ such that*

$$b \equiv a^{n(\mathfrak{p})} \,(\mathrm{mod}\, \mathfrak{p}). \tag{1}$$

Does it follow that b is in the subgroup generated by a in $G(k)$?

The second problem concerns abelian varieties. Let A be an abelian variety defined over a field k (without assumption for the moment). For any $d \geqslant 1$ let $k(A[d])$ be the Galois extension of k generated by "the coordinates of d-torsion points", i.e. the fixed field (in a given algebraic closure) of the subgroup of $\mathrm{Gal}(\bar{k}/k)$ consisting of elements acting trivially on $A[d]$. To what extent does the sequence of fields $k(A[d])$ characterize A?

Problem 1.2. *Let A and B be abelian varieties over k, where k is either a number field or a finite field. Say that A and B are isokummerian, denoted $A \simeq_{\kappa} B$, if there exists an integer $m \geqslant 1$ such that*

$$k(A[d]) = k(B[d]) \text{ if } (d, m) = 1. \tag{2}$$

What can one say about A and B?

We will show for instance that if A and B are elliptic curves, then this condition is equivalent with A and B being k-isogenous.

Finally, the following problem is a fairly direct generalization of a well-known elementary question, corresponding to $k = \mathbf{Q}$ (the history is briefly discussed in the introduction to [ZBC]):

1991 *Mathematics Subject Classification.* Primary 11G99; Secondary 11R99, 11G10.

Key words and phrases. Kummer Theory, Abelian Varieties, Division Fields.

Problem 1.3. *Let k be a number field, a and b be integers of k. Assume that*

$$\mathfrak{z}(a^n-1)=\mathfrak{z}(b^n-1) \text{ for } n\geqslant 1, \tag{3}$$

where $\mathfrak{z}(x)$ is the largest integer *$d\in\mathbf{Z}$, $d\geqslant 1$, such that $d\mid x$, with the additional convention $\mathfrak{z}(0)=+\infty$.*

What relation, if any, holds between a and b? What if $\mathfrak{z}(\cdot)$ is replaced by its square-free kernel, or equality by divisibility?

The arguments involved below will be fairly elementary, but even in the simpler cases they do involve some deep results of arithmetic and algebraic geometry. It would be interesting to find more elementary proofs of some of them.

2. Remarks on related results

Although the author, motivated mostly by the second problem above, came up with the arguments below on his own, there are quite a number of related papers and preprints.[1] We will list those we are currently aware of, and make some comments.

- Schinzel [Sc2] has solved Problem 1.1 for the multiplicative group.
- The "support problem" of Erdös asks what can be said of integers a and b such that

  $$p\mid a^n-1 \text{ implies } p\mid b^n-1.$$

  This is of course Problem 1.3 for $k=\mathbf{Q}$ and the squarefree kernel.
- For $k=\mathbf{Q}$, a related problem is to estimate the gcd of a^n-1 and b^n-1. Zannier, Bugeaud and Corvoja [ZBC] have recently proved that if a and b are multiplicatively independent, then for any $\varepsilon>0$ we have

$$(a^n-1,b^n-1)\ll_\varepsilon \exp(\varepsilon n) \text{ for } n\geqslant 2. \tag{4}$$

- The support problem is solved and generalized to elliptic curves by Corrales-Rodrigáñez and Schoof [CS] and is quite close to Problem 1.1, in particular their Theorem 2 implies our Theorem 3.3 for non-CM elliptic curves.
- Generalizations of the support problem are discussed in [BGK], [KP] and [Lar].
- Khare and Prasad [KP] solve the support problem for (some) abelian varieties and the authors prove a result generalizing the non-CM case of Theorem 3.3 to many abelian varieties. At the end of Section 6, we translate their proof in our context using their two main Lemmas.
- Larsen [Lar] gives a complete solution of the support problem for abelian varieties, but because of the generality, it turns out to not really give further results for us (see Remarks 6.2 and 9.2).
- The result most directly related to Problem 1.1 is proved by Weston [We]: this paper discusses the analogue for general subgroups of abelian varieties, instead of those generated by a single element. We also state a simple corollary of his main result at the end of Section 6.
- S. Wong [Wo] considers the following problem, for G an algebraic group over a number field k, S a finite subset of $G(k)$ and $n\geqslant 1$ an integer: assuming that for almost all $\mathfrak{p}$ in k there exists $x\in S$ (depending on $\mathfrak{p}$) such that $x\equiv ny_{\mathfrak{p}}$, for some $y_{\mathfrak{p}}\in G_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}})$, does it follow that S contains an n-th power of an element in $G(k)$? This is again clearly related to our work, and the results of [Wo] use many of the same techniques.
- This same divisibility problem is considered for $S=\{x\}$ and quite general commutative algebraic groups by Dvornicich and Zannier [DZ], using more cohomological methods.
- The paper [FJ] of Frey and Jarden deals with a problem similar to Problem 1.2 for elliptic curves over finitely generated fields. Their assumptions are much less stringent than ours and the methods quite different. Note that by the counter-example in Theorem 3.4, (6) due to Serre, their statements do not generalize to higher dimensional abelian varieties.

[1] Many of which appeared after the first version of this paper was ready.

All the papers dealing with the support problem have methods very similar to ours, based on Kummer theory. In fact, all those authors use them rather more subtly and more powerfully. However, the formalism introduced in the present paper is different and might be more generally useful, as explained briefly in the short Appendix, which for comparison discusses some notions of subsets in algebraic groups defined by local conditions. Also we have strived to give a uniform presentation, not requiring to distinguish between the multiplicative group and elliptic curves, with or without CM, for instance (compare e.g. [CS]).

See also Remarks 8.7, 6.12 for mention of other similar statements due to Rudnick–Ailon and others.

Notation. Since we will often speak of "the reduction modulo $\mathfrak{p}$" of points on an algebraic variety defined over a number field, we explain what is understood here by this. (For the groups of interest in the main results, this is hardly necessary, but we give some general definitions and facts in Section 3 and Section 4, so might as well assuage the fears of the more algebraically minded readers; number theorists can skip the next few paragraphs).

Let k be a number field, V/k an algebraic variety (in the old-fashioned sense, i.e. a reduced quasi-projective scheme of finite type over k). Let $\mathcal{O}$ be the ring of integers in k. By "chasing denominators" one sees that there exists "equations for V with integer coefficients" (i.e. a reduced scheme $\mathcal{V}/\mathcal{O}$ of finite type such that V is the generic fiber of $\mathcal{V}$). Such a $\mathcal{V}$ can be reduced modulo all primes of k, getting varieties over finite fields. If $a \in V(k)$ is a rational point, one can reduce a modulo $\mathfrak{p}$ for almost all $\mathfrak{p}$ (those not dividing the denominators of coordinates of a) and get corresponding reductions $a_{\mathfrak{p}} \in \mathcal{V}(\mathbf{F}_{\mathfrak{p}})$.

Such a $\mathcal{V}$ is not unique. However, with the assumption that $\mathcal{V}$ be of finite type, one has a sufficient uniqueness statement: if $\mathcal{V}_i$, $i = 1, 2$, are as above (finite type reduced schemes with generic fiber V), there exists a non-empty open subscheme U of the spectrum of $\mathcal{O}$ such that $\mathcal{V}_1$ is isomorphic to $\mathcal{V}_2$ over U (i.e. for almost all $\mathfrak{p}$, the reduction is really well-defined), and the reductions modulo almost all $\mathfrak{p}$ of a given $a \in V(k)$ correspond under this isomorphism. So one can speak of "the" reduction of a modulo almost all primes.

It is a deep problem to find the "best possible" $\mathcal{V}$, but this is irrelevant to what we do, as all the statements are based on assumptions valid for almost all $\mathfrak{p}$ only.

If in addition $V = G$ is an algebraic group, one can find a finite type *group* $\mathcal{G}/U$, where U is a non-empty open subscheme of $\operatorname{Spec}\mathcal{O}$, with generic fiber G. The sets of points of $\mathcal{G}$ modulo $\mathfrak{p} \in U$ are then finite groups, and the reductions of a are points in these finite groups.

We will usually denote $\mathcal{G}$ any such extension of G, We also use $G_{\mathfrak{p}}$ to denote the fiber above a prime ideal $\mathfrak{p}$, sometimes without explicit mention of a model $\mathcal{G}$, this being meaningful if $\mathfrak{p}$ ranges over an open set. We also speak of "having good reduction at $\mathfrak{p}$" for G, meaning a $\mathcal{G}/U$ has been chosen and $\mathfrak{p} \in U$, and for a set M of rational points, meaning that there exist a common open subset $V \subset U$ such that all $m \in M$ can be reduced for $\mathfrak{p} \in V$ (i.e. their denominators never contain a prime in V).

If a and $b \in V(k)$ are rational points, we write sometimes $a \equiv b \,(\operatorname{mod}\mathfrak{p})$ to mean that their reductions coincide; if not specified before, $\mathfrak{p}$ is meant to be any prime where both reductions make sense. We will often use the following trivial statement: if $a \equiv b \,(\operatorname{mod}\mathfrak{p})$ for infinitely many $\mathfrak{p}$, then $a = b$. (Think simply of coordinates).

For an abstract group G and $x \in G$, we denote by $\operatorname{ord}_G(x)$ the order of the element x, in $\mathbf{N} \cup \{+\infty\}$; if the finite group G is obtained by reduction modulo $\mathfrak{p}$ of some fixed algebraic group, we just write $\operatorname{ord}_{\mathfrak{p}}(a)$. Moreover, we let

$$\mathcal{Z}(x) = \{d \geqslant 1 \mid x \text{ is a } d \text{ th-power in } G\}. \tag{5}$$

The cardinality of a finite set X is denoted $|X|$.

Acknowledgements. I would like to thank to J. Ellenberg for some discussions and comments, Z. Rudnick for pointing out some related papers, and J-P. Serre for finding and explaining the (counter)-example of Theorem 3.4, 6. Also I thank the referee for other references and for remarks leading to improvements in the presentation.

3. Statement of results

To summarize briefly, we will satisfactorily settle Problem 1.1 when G is either the multiplicative group or an elliptic curve over a number field. Some partial results will also be stated for G isogenous to $A \times T$, with A/k an abelian variety and T a torus. We will give a complete answer to Problem 1.2 for elliptic curves, and solve it "up to finite obstruction" over finite fields. Finally, we also solve Problem 1.3 satisfactorily.

Now we turn to precise statements, starting with the situation of Problem 1.1. We make some definitions first.

Definition. Let G/k be a finite type group scheme over a number field k. Let $a \in G(k)$ be a rational point of G. The *subgroup locally generated by* a is the set of rational points $b \in G(k)$ such that there exists a non-empty open subscheme U in $\mathrm{Spec}(\mathcal{O})$ where a and b can be reduced, and for $\mathfrak{p} \in U$, there exists $n(\mathfrak{p}) \in \mathbf{Z}$ such that

$$a^{n(\mathfrak{p})} \equiv b \,(\mathrm{mod}\,\mathfrak{p}).$$

We denote this subgroup by $\ll a \gg \subset G(k)$.

It is obvious that $\ll a \gg$ is indeed a subgroup of $G(k)$ and that $<a> \subset \ll a \gg$, letting $<a>$ denote the usual subgroup generated by a.

Our Problem 1.1 can be generalized as follows:

Problem 3.1. *Let G/k be as above, and $a \in G(k)$. Compute $\ll a \gg \subset G(k)$.*

We begin with examples where $\ll a \gg \neq <a>$.

Proposition 3.2. *Let G/k be a group scheme over a number field.*

(1) *If there exists an embedding $\mathbf{G}_a \hookrightarrow G$, the answer to Problem 1.1 is "No", and in fact if $G = \mathbf{G}_a/k$, we have $\ll a \gg = \mathbf{Q}a \subset k$ for all $a \in k$.*

(2) *If $G = GL(n)$ and $a = a_s a_u \in G(k)$ is the Jordan-Hölder decomposition of an element such that $b = a_s \neq 1$, $a_u \neq 1$, then $b \in \ll a \gg$, $b \notin <a>$.*

Proof. (1) It is enough to treat the case $G = \mathbf{G}_a$. It is obvious that $\ll 0 \gg = 0$. Let $a \in k^\times$ and $b = ra$ with $r \in \mathbf{Q}$. For any prime ideal $\mathfrak{p}$ not dividing the denominator of b, we have $r \equiv n \,(\mathrm{mod}\,\mathfrak{p})$ for some $n \in \mathbf{Z}$, hence $b \in \ll a \gg$. So we have $\mathbf{Q}a \subset \ll a \gg$.

Conversely if $b \in \ll a \gg$, let $r = b/a \in k$. The assumption is that, modulo almost all $\mathfrak{p}$, r is in the prime field. This implies $r \in \mathbf{Q}$ (a theorem due to Kronecker, nicely discussed in [CL]; also it follows directly from Lemma 4.1 below since almost all primes will be split in $\mathbf{Q}(r)/\mathbf{Q}$).

(2) Recall that $a_s = b$ and $a_u \in G(k)$ (see e.g. [Bo, I-4]). For any prime $\mathfrak{p}$ at which we can reduce a and b we have (for m large enough)

$$a^{(N\mathfrak{p})^m} = a_s^{(N\mathfrak{p})^m} a_u^{(N\mathfrak{p})^m} \equiv a_s^{(N\mathfrak{p})^m} \equiv a_s = b \,(\mathrm{mod}\,\mathfrak{p}),$$

so $b \in \ll a \gg$, but obviously the assumptions imply that b is not in the subgroup of $G(k)$ generated by a. □

In particular, there is no straightforward local-global principle for "b belongs to $<a>$" when $G = GL(n)$, $n \geqslant 2$, for instance. It is probably true that this Proposition essentially exhausts all obstructions for linear groups, see Proposition 6.11. We will prove the following theorem in Section 6, together with partial results in other cases:

Theorem 3.3. *Let G be either an elliptic curve or the multiplicative group over a number field k. Then for any $a \in G(k)$ we have $\ll a \gg = <a>$.*

Turning to Problem 1.2, it is simple to show (see Lemma 8.2 below) that a given A is isokummerian with the product of its simple factors. It will be convenient to call A multiplicity-free if $A \simeq A_1 \times \cdots \times A_m$ with the A_i/k simple and pairwise non-isogeneous.

Theorem 3.4. (1) *For k a finite field, A/k and B/k abelian varieties over k. Let Φ_A be the multiplicative subgroup of $\mathbf{C}^\times$ generated by the conjugates of the Frobenius eigenvalues of A. Then $A \simeq_\kappa B$ if and only if $\Phi_A = \Phi_B$.*

(2) *Let k be a finite field of order p^f and A/k an abelian variety. The set B_A of k-isogeny classes of multiplicity-free abelian varieties which are isokummerian to A satisfies*

$$|\mathsf{B}_A| \leqslant c_{f,d}$$

for some integer $c_{f,d} \geqslant 1$ depending only on the degree $f = [k : \mathbf{Z}/p\mathbf{Z}]$ and on $d = \dim(A)$.[2]

(3) *Let k be a finite field, A/k an abelian variety. If k'/k is a finite extension k'/k and B'/k' satisfies $B \simeq_\kappa A \times_k k'$, then B' has a model B/k.*

(4) *Let k be a finite field or a number field, let E/k be an elliptic curve and B/k a multiplicity-free abelian variety. Then $E \simeq_\kappa B$ if and only if E and B are k-isogenous.*

(5) *Let k be a finite field and let A be a* product *of elliptic curves, B a multiplicity-free abelian variety. If $A \simeq_\kappa B$, there exists a finite extension k'/k such that the simple factors of $A \times k'$ coincide with those of $B \times k'$.*

(6) (Serre) *There exist simple abelian varieties A and B over a finite field k, such that $A \simeq_\kappa B$, and A and B are not isogenous over $\bar{k}$.*

Remark 3.5. Can one expect a stronger conclusion if one asks that the assumption be strengthened to $k(A[d]) = k(B[d])$ for *all* d? This is not clear. It follows for instance from an example of Whittmann [Wh, Appendix] that over a finite field, there can exist (ordinary) elliptic curves E_1 and E_2 such that $k(E_1[d]) = k(E_2[d])$ for all $d \geqslant 1$, without E_1 and E_2 being isomorphic, even without E_1 and E_2 having the same endomorphism ring. However, over number fields where the isogeny classes are in general quite small, it might be that a stronger statement is in fact true.

Finally, we can completely solve Problem 1.3.

Proposition 3.6. *Let $k/\mathbf{Q}$ be a Galois extension, a and $b \in \mathcal{O}_k$, non-zero. Then the following statements are equivalent:*

(1) *We have*

$$\mathfrak{z}(a^n - 1) \mid \mathfrak{z}(b^n - 1) \text{ for } n \geqslant 1, \tag{6}$$

(2) *The squarefree kernel of $\mathfrak{z}(a^n - 1)$ divides that of $\mathfrak{z}(b^n - 1)$ for all $n \geqslant 1$.*

(3) *We have $b \in <(a^\sigma)_\sigma>$, where σ runs over* $\mathrm{Gal}(k/\mathbf{Q})$, *i.e. b is in the subgroup of $k^\times$ generated by the conjugates of a.*

The next two sections deals with preliminary lemmas. The interrelation between the problems will become clear.

4. Preliminary lemmas

We start with some easy lemmas and well-known statements. The first is a classical result of algebraic number theory, which is (for instance) an immediate consequence of the Chebotarev Density Theorem.

Lemma 4.1. *Let L/k and K/k be finite Galois extensions of number fields. Then we have $L \subset K$ if and only if almost all prime ideals $\mathfrak{p}$ of k which are totally split in K are also in L.*

Next we show that $\ll a \gg$ for $a \in G(k)$ is well-defined independently of the reference field k or the ambient group G.

Lemma 4.2. *Let k be a number field, $G < H$ finite type (quasi-projective) group schemes over k, k'/k an arbitrary algebraic extension. For any $a \in G(k)$, we have*

$$\ll a \gg_{k,G} = \ll a \gg_{k',H} \subset H(k')$$

where on the left a is seen as an element of $G(k)$ and on the right as an element of $H(k')$.

[2] The proof will show how to get an effective estimate for $c_{f,d}$.

Proof. Let $x \in H(k')$ be in $\ll a \gg_{k',H}$. One reduces at once to k'/k finite. Embedding H in some projective space, then removing a hyperplane not containing x, then looking at the coordinates in the resulting affine space, we get $x \in H(k)$ by the theorem of Kronecker already mentioned in the proof of Proposition 3.2.

For almost all prime ideals $\mathfrak{p}$ in k, x modulo $\mathfrak{p}$ is in $\mathcal{G}_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}})$. Thus for any function f vanishing on G, we have $f(x) = 0$ since it reduces to 0 modulo infinitely many primes. Hence $x \in G(k)$. □

Remark 4.3. In particular, given $a \in G(k)$, to show that $<a> = \ll a \gg$ it suffices to do so after a finite extension of k. Notice also that $\ll a \gg$ is necessarily commutative since for any b, $c \in \ll a \gg$, the commutator $[b, c]$ satisfies $[b, c] \equiv 1 \pmod{\mathfrak{p}}$ for almost all $\mathfrak{p}$, hence $[b, c] = 1$.

Lemma 4.4. *Let G/k be a finite type connected commutative group scheme over a number field k. There exists an open set $U \subset \operatorname{Spec}(\mathcal{O}_k)$ and a model $\mathcal{G} \to U$ of G over U such that for $d \geqslant 1$ and any $\mathfrak{p} \in U$ with $(d, \mathfrak{p}) = 1$, the reduction map*

$$G[d](\bar{k}) \to \mathcal{G}[d](\bar{\mathbf{F}}_{\mathfrak{p}}) \tag{7}$$

is an isomorphism.

Proof. This follows from the case of linear groups and that of abelian varieties using Chevalley's exact sequence

$$0 \to L \to G \to A \to 0$$

where L/k is a commutative linear group and A/k is an abelian variety. The case of abelian varieties follows from [Mi-2, Pr. 20-7], and that of L reduces to the multiplicative group $\mathbf{G}_m$ since neither $\mathbf{G}_a/k$ nor $\mathbf{G}_a/\mathbf{F}_{\mathfrak{p}}$ has any d-torsion (since $(d, \mathfrak{p}) = 1$). □

The crucial step in the next section is based on an elementary property of certain finite abelian groups, which is a simple generalization of the classical Euler Criterion for quadratic residues: an element $a \in (\mathbf{Z}/p\mathbf{Z})^\times$, with p prime, is a square if and only if its order divides $(p-1)/2$. Recall that $\operatorname{ord}_G(x)$ is the order of an element $x \in G$ in a group and $\mathcal{Z}(x)$ is defined in (5).

Lemma 4.5. *Let $n \geqslant 1$, $R = \mathbf{Z}/n\mathbf{Z}$ and M a free R-module of finite rank. Let x, $y \in M$. If $\operatorname{ord}_M(x) \mid \operatorname{ord}_M(y)$, then $\mathcal{Z}(y) \subset \mathcal{Z}(x)$.*

More precisely, we have $\operatorname{ord}_M(x) = \operatorname{ord}_M(y)$ if and only if there exists $f \in \operatorname{Aut}(M)$ such that $f(y) = x$, and $\operatorname{ord}_M(x) \mid \operatorname{ord}_M(y)$ if and only if there exists $f \in \operatorname{End}(M)$ such that $f(y) = x$.

Proof. Since $x = f(y)$ immediately implies $\mathcal{Z}(y) \subset \mathcal{Z}(x)$, the second part is indeed more precise than the first one.

Writing $M = \prod_\ell M_\ell$ where M_ℓ is the ℓ-primary component of M, one reduces to $n = \ell^m$ for some $m \geqslant 1$. If $m = 1$, the result is trivial since $GL(V)$ acts transitively on $V - \{0\}$ for any finite dimensional vector space V over a field k.

Let ℓ^n, $n \leqslant m$, be the order of y in M. In a basis of M, this means that $y = (\ell^{m-n} y_i)_i$ with $y_i \in R$, and at least one of the y_i is not divisible by ℓ, hence invertible. The vector $y' = (y_i)$ is thus of (maximal) order ℓ^m, and hence is a component in a new basis of M. This way one can assume that $y = (\ell^{m-n}, 0, \ldots)$.

If $\operatorname{ord}(y) = \operatorname{ord}(x)$ we have similarly $x = (\ell^{m-n} x_i)$, and one of the x_i is invertible. Extend the column vector ${}^t(x_i)$ to an element f of $\operatorname{Aut}(M)$: then $f(y) = x$.

If $\operatorname{ord}(x) \mid \operatorname{ord}(y)$, the reasoning is similar, but one cannot ensure that $f \in \operatorname{Aut}(M)$.

(Alternatively, one can invoke Hensel's lemma and the ℓ-adic case). □

We now recall the setup of Kummer theory. For a commutative group scheme G/k over a field, with group law written additively,[3] we denote as usual by $G[n]$ the finite group scheme of points of order n on G. There is a natural action

$$\rho_n = \rho_{n,G} : \operatorname{Gal}(\bar{k}/k) \to \operatorname{Aut}(G[n])$$

[3] Except that for lack of a better word we say that an element is an n-th power, meaning $a = nb$ for some b.

of the Galois group of k on $G[n]$. Let $k(G[n]) = \bar{k}^{\ker \rho_n}$ denote the field generated by the coordinates of the n-torsion points. It is a finite Galois extension of k with Galois group isomorphic to $\mathrm{Im}(\rho_n)$.

In addition, let $M \subset G(k)$ be a subgroup of finite type of the rational points of G. Let $n^{-1}M$ be the group of its n-th roots:

$$n^{-1}M = \{x \in G(\bar{k}) \mid nx \in M\}.$$

This is again a $\mathrm{Gal}(\bar{k}/k)$-module of finite type. Note that $G[n](\bar{k}) \subset n^{-1}M$.

The absolute Galois group of k acts naturally on $n^{-1}M$. Let $k(n^{-1}M)$ denote the fixed field of the kernel of this action: this is the Kummer extension obtained by "adding the coordinates of the n-th roots of M to k". Note that $k(G[n]) \subset k(n^{-1}M)$.

Moreover we have the Kummer injection

$$\kappa \,:\, \mathrm{Gal}(k(n^{-1}M)/k(G[n])) \hookrightarrow \mathrm{Hom}(M, G[n]) \tag{8}$$

defined by $\kappa(\sigma)(x) = \sigma(y) - y$ for any y such that $ny = x$.

Lemma 4.6. *Let k be a number field, G/k a commutative group scheme over k, without additive factor $\mathbf{G}_a \hookrightarrow G$, $M \subset G(k)$ a finite type subgroup. For any prime ideal $\mathfrak{p}$ of k where G has good reduction, and any $n \geqslant 1$, the residue field extension of $k(G[n])/k$ at $\mathfrak{p}$ is*

$$\mathbf{F}_{\mathfrak{p}}(\mathcal{G}_{\mathfrak{p}}[n])/\mathbf{F}_{\mathfrak{p}},$$

and the residue field extension of $k(n^{-1}M)/k$ at $\mathfrak{p}$ is

$$\mathbf{F}_{\mathfrak{p}}(n^{-1}M_{\mathfrak{p}})/\mathbf{F}_{\mathfrak{p}},$$

if in addition M has good reduction at $\mathfrak{p}$.

Proof. This is because the restriction map $G[d](\bar{k}_{\mathfrak{p}}) \to \mathcal{G}_{\mathfrak{p}}(\bar{\mathbf{F}}_{\mathfrak{p}})$ is surjective (this is obvious by Lemma 4.4 if $\mathfrak{p} \nmid d$, which we can assume in our applications, and requires a little more thought in the general case). □

5. Enter Kummer

We can now outline our general strategy: the link between local assumptions (such as (1)) and a global statement will be provided by the fact that they straightforwardly imply inclusions of the Kummer extensions associated to n-division of the given points, for *all* $n \geqslant 1$. This is a powerful statement because of general theories that show that, in many cases, Kummer extensions are "as large as possible", unless the points being divided satisfy some relations. Those are usually weaker than we expect and some additional ad-hoc work has to be implemented afterwards.

Here is the very simple lemma we need:

Lemma 5.1. *Let G/k be as above, a and $b \in G(k)$ rational points. Assume that for almost all prime $\mathfrak{p}$ in k there exists a group homomorphism $f : \mathcal{G}(\mathbf{F}_{\mathfrak{p}}) \to \mathcal{G}(\mathbf{F}_{\mathfrak{p}})$ with $b_{\mathfrak{p}} = f(a_{\mathfrak{p}})$. Then for any $n \geqslant 1$ we have*

$$k(n^{-1}{<}b{>}) \subset k(n^{-1}{<}a{>}). \tag{9}$$

Proof. This is a tautology, given Lemma 4.1: if $\mathfrak{p}$ is a prime of good reduction for $\mathcal{G}$ (with respect to a and b), to say that $\mathfrak{p}$ is split in $k(n^{-1}{<}a{>})$ means, by Lemma 4.6, that $\mathfrak{p}$ is split in $k(G[n])$, and that a is an n-th power in $\mathcal{G}(\mathbf{F}_{\mathfrak{p}})$. But in this case $b = f(a)$ implies that b also is an n-th power, hence (going backwards) that $\mathfrak{p}$ is totally split in $k(n^{-1}{<}b{>})$. □

(See also the Appendix about the assumption in the lemma). Hence we obviously have

Corollary 5.2. *Let G be a commutative algebraic group over a number field k, $a \in G(k)$ and $b \in \ll a \gg$. For any $n \geqslant 1$ we have*

$$k(n^{-1}{<}b{>}) \subset k(n^{-1}{<}a{>}).$$

Problem 1.3 gives a similar conclusion.

Lemma 5.3. *Let k be a number field, a and b integers in k satisfying* (6)*. Let $G = \operatorname{Res}^k_{\mathbf{Q}} \mathbf{G}_m$ be the restriction of scalars of the multiplicative group from k to $\mathbf{Q}$.*

Then we have

$$\mathbf{Q}(n^{-1}{<}b{>}) \subset \mathbf{Q}(n^{-1}{<}a{>})$$

where a and b are seen as elements in $G(\mathbf{Q}) = k^\times$.

Proof. By Lemma 5.1 it is sufficient to prove that for almost all prime p there exists $f : \mathcal{G}(\mathbf{Z}/p\mathbf{Z}) \to \mathcal{G}(\mathbf{Z}/p\mathbf{Z})$ such that $b \equiv f(a) \,(\operatorname{mod} p)$. We can obviously assume that $k/\mathbf{Q}$ is a Galois extension.

By construction, we have $G(\mathbf{Q}) = k^\times$, and after reduction modulo p, for almost all p, we have group isomorphisms

$$\mathcal{G}(\mathbf{Z}/p\mathbf{Z}) \simeq (\mathcal{O}_k/p\mathcal{O}_k)^\times. \tag{10}$$

Let p be large enough. Let n be the order of a in $\mathcal{G}(\mathbf{Z}/p\mathbf{Z})$. Then

$$a^n \equiv 1 \,(\operatorname{mod} p) \text{ or equivalently } p \mid a^n - 1 \text{ in } \mathcal{O}_k.$$

By the assumption (6), we have $p \mid b^n - 1$ so $b^n \equiv 1 \,(\operatorname{mod} p)$ also, and in particular, the order of b modulo p divides that of a.

From (10) however, and since $k/\mathbf{Q}$ is Galois and the multiplicative group of a finite field is cyclic, it follows that $\mathcal{G}(\mathbf{Z}/p\mathbf{Z})$ is of the type

$$\mathcal{G}(\mathbf{Z}/p\mathbf{Z}) \simeq (\mathbf{Z}/s\mathbf{Z})^g$$

for some integers $s \geqslant 1$, $g \geqslant 1$. Hence we can apply Lemma 4.5 to conclude. □

Finally, we consider isokummerian abelian varieties over a finite field, and notice that this assumption can be translated to a property very close to (6) for their Frobenius endomorphisms.

Let k be a finite field of characteristic p, and A/k an abelian variety over k. We have the Frobenius morphism $\pi \in \operatorname{End}_k(A)$. The commutative $\mathbf{Q}$-algebra $\mathbf{Q}(\pi)$ is semi-simple (see e.g. [Mu, 19, Cor. 2]), thus isomorphic to a product of number fields, say

$$\mathbf{Q}(\pi) \simeq K_1^{n_1} \times \cdots \times K_m^{n_m}, \quad n_i \geqslant 1, \tag{11}$$

where $K_i \neq K_j$ for $i \neq j$. The conjugates in $\bar{\mathbf{Q}}$ of the components of π are the Frobenius eigenvalues λ_j, $1 \leqslant j \leqslant 2\dim(A)$. We will denote $K_A = \mathbf{Q}((\lambda_j)_j)$ the field generated by the Frobenius eigenvalues.

The Frobenius has the standard property that $A(k) = A(\bar{k})^\pi$, the group of elements in $A(\bar{k})$ fixed by π, and this allows us to easily compute $k(A[d])$ when $p \nmid d$.

Lemma 5.4. *Let k be a finite field of characteristic p and A/k an abelian variety over k. Let $d \geqslant 1$ be an integer not divisible by p. Then $k(A[d])$ is the extension field of k of degree*

$$[k(A[d]) : k] = \inf\{n \geqslant 1 \mid d \mid \pi^n - 1 \textit{ in } \operatorname{End}_k(A)\}. \tag{12}$$

Proof. By definition, $k(A[d])$ is the smallest field k_n such that $A[d](\bar{k}) \subset A(k_n)$. Let $\pi_n = \pi^n$ be the Frobenius of A over k_n. If $A[d](\bar{k}) \subset A(k_n)$ and $(d,p) = 1$, we have $\ker(d : A \to A) \subset \ker(\pi_n - 1)$ and since $(d,p) = 1$, $\pi_n - 1$ factorizes through d (because $A[d]$ is étale, see e.g. [Mi-2, Lemma 12.6]), i.e.

$$\pi^n - 1 = d\phi \text{ for some } \phi \in \operatorname{End}(A).$$

The converse is also true, proving the stated formula. □

Note that the divisibility in (12) takes place in a ring of characteristic 0. For a fixed integer $q \geqslant 1$ and an arbitrary ring R (of characteristic 0), we now denote by $\mathfrak{z}_q(x)$ the largest integer $d \geqslant 1$ such that $(d,q) = 1$ and $d \mid x$ in R, i.e. $x = dy$ for some $y \in R$; as $\mathbf{Z}$ is central in R, this is unambiguous.

Proposition 5.5. *Let k be a finite field. Let A/k and B/k be isokummerian abelian varieties over a finite field k, π_1 and π_2 their respective Frobenius morphisms, K_i the field generated by the eigenvalues of π_i and K the compositum $K = K_1K_2$. Then for all $n \geqslant 1$ we have*

$$K(n^{-1}{<}\pi_1, 1{>}) = K(n^{-1}{<}1, \pi_2{>})$$

where ${<}\cdot{>}$ refers to the algebraic torus $G = \mathrm{Res}_{\mathbf{Q}}^{K_1}(\mathbf{G}_m) \times \mathrm{Res}_{\mathbf{Q}}^{K_2}(\mathbf{G}_m)$.

Proof. First we show that $A \simeq_{\kappa} B$ if and only if there exists $m \geqslant 1$ such that

$$\mathfrak{z}_{pm}(\pi_1^n - 1) = \mathfrak{z}_{pm}(\pi_2^n - 1) \tag{13}$$

for all $n \geqslant 1$, where p is the characteristic of k.

Indeed, assume A and B are isokummerian and let m be such that $k(A[d]) = k(B[d])$ for all d coprime with m. As mentioned above, an integer d coprime with p divides $\pi_1^n - 1$ if and only if $A[d] \subset A(k_n)$, if and only if k_n is an extension of $k(A[d])$. So an integer d coprime with pm divides $\pi_1^n - 1$ if and only if $k(A[d]) = k(B[d]) \subset k_n$.

The assumption thus implies that $\pi_1^n - 1$ and $\pi_2^n - 1$ are divisible by the same integers coprime with pm, hence (13) follows. The converse is immediate from Lemma 5.4.

Now the remainder of the proof is similar to Lemma 5.3. Let $n \geqslant 1$ and let ℓ be a prime totally split in $K(n^{-1}{<}\pi_1, 1{>})$. Assume ℓ large enough so that $(\ell, pm) = 1$. Let r be the order of π_1 in $\mathcal{G}(\mathbf{Z}/\ell\mathbf{Z})$, namely the order of π_1 in $\mathcal{G}_1(\mathbf{Z}/\ell\mathbf{Z})$, where we let

$$G_i = \mathrm{Res}_{\mathbf{Q}}^{K_i}(\mathbf{G}_m).$$

As before this means that $\ell \mid \pi_1^r - 1$, so $\ell \mid \pi_2^r - 1$ by (13). Exchanging the roles of A and B we see that r is also the order of π_2 in $\mathcal{G}_2(\mathbf{Z}/\ell\mathbf{Z})$.

Since ℓ is totally split in K, hence in K_i, it follows from the definition of the restriction of scalars that

$$\mathcal{G}(\mathbf{Z}/\ell\mathbf{Z}) = (\mathcal{O}_{K_1}/\ell\mathcal{O}_{K_1})^\times \times (\mathcal{O}_{K_2}/\ell\mathcal{O}_{K_2})^\times$$

is of the form

$$\mathcal{G}(\mathbf{Z}/\ell\mathbf{Z}) \simeq (\mathbf{Z}/(\ell-1)\mathbf{Z})^{[K_1:\mathbf{Q}]+[K_2:\mathbf{Q}]}$$

(as an abelian group). Hence Lemma 4.5 applies and their exists a homomorphism f of $\mathcal{G}(\mathbf{Z}/\ell\mathbf{Z})$ such that $f(\pi_1, 1) = (1, \pi_2)$, so ℓ is also totally split in $K(n^{-1}\langle 1, \pi_2\rangle)$. By Lemma 4.1, we have therefore

$$K(n^{-1}\langle 1, \pi_2\rangle) \subset K(n^{-1}\langle \pi_1, 1\rangle),$$

and we get the converse inclusion in the same way. □

Remark 5.6. Here is a trivial variant that may also be interesting: let A/k and B/k be abelian varieties over a finite field k such that $k(A[d]) \subset k(B[d])$ for all $(d, m) = 1$, π_1 and π_2 their respective Frobenius. Then for all $n \geqslant 1$ we have

$$K(n^{-1}{<}1, \pi_2{>}) \subset K(n^{-1}{<}\pi_1, 1{>})$$

Having applied Lemma 5.1, we need to transform (9) into the desired conclusion. A number of tools are available: we will apply two, namely "usual" Kummer theory (see e.g. [La2, VIII-8]) and the Bashmakov-Ribet version of Kummer theory for abelian varieties and tori ([Ba], [Ri]), together with some tricks. The next section deals with Theorem 3.3, and is independent of the following two.

6. Proof of Theorem 3.3

We now prove Theorem 3.3, starting from Corollary 5.2. We present our argument maybe too abstractly, because we believe it might be possible to extend it further.

Definition. Let G/k be a commutative algebraic group over a number field which has no additive component $\mathbf{G}_a \hookrightarrow G$. Let $R = \mathrm{End}_k(G)$. One says that *G has large Kummer extensions* if for any finitely generated subgroup $M \subset G(k)$, such that there is a basis of M consisting of elements which are independent over R, the Kummer injection (8) is onto for almost all $n = \ell$ prime.

In particular, for such a group G, $G[\ell]$ is of order > 1 for any prime number ℓ. Ribet's extension [Ri, Th. 1.2] of Bashmakov's method [Ba] implies that if G/k is isogenous to a product $A \times T$, where A/k is an abelian variety and T is a torus, then G has large Kummer extensions. In fact, as explained by Hindry [Hi], Ribet's paper provides axioms under which a group has large Kummer extensions, which apply for tori. For general abelian varieties, the axioms are known as consequences of Faltings's Isogeny Theorem [Fa-1] and further results of Serre.

Proposition 6.1. *Let G/k be a commutative algebraic group over a number field which has large Kummer extensions. Let $a \in G(k)$ and $b \in \ll a \gg$. Then a and b are $\mathrm{End}_k(G)$-linearly dependent, i.e. there are elements f and $g \in \mathrm{End}_k(G)$, not both zero, such that*

$$f(a) = g(b). \tag{14}$$

Proof. By Corollary 5.2, we have for almost all primes ℓ

$$k(\ell^{-1}{<}a, b{>}) = k(\ell^{-1}{<}a{>}).$$

By the Kummer injection (8), $[k(\ell^{-1}{<}a{>}) : k(G[\ell])] \leqslant |G[\ell]|$, so

$$[k(\ell^{-1}{<}a, b{>}) : k(G[\ell])] \leqslant |G[\ell]| < |G[\ell]|^2,$$

and since G has large Kummer extensions, it follows that a and b are *not* independent over $\mathrm{End}_k(G)$. This is the result stated. □

Remark 6.2. This result also follows from Theorem 1 of [Lar], but the assumptions there are much weaker and the proof (consequently) not as simple as the one above.

We now wish to go from (14) to $b \in {<}a{>}$, but we do not know how to do it in general.

Definition. Let G/k be a commutative algebraic group over a number field. An element $a \in G(k)$ is said to be *well-spread* if for any finite set S of finite places of k, and for all but finitely many[4] $n \geqslant 1$ there exists $\mathfrak{p} \notin S$ such that $na \equiv 0 \,(\mathrm{mod}\, \mathfrak{p})$.

In fact, we will only use the following weaker consequences of this definition:

Lemma 6.3. *Let G/k be a commutative algebraic group over a number field, $a \in G(k)$ a well-spread point.*

(1) *The point a is of infinite order.*

(2) *For all prime numbers ℓ, all $k \geqslant 1$, there exists $\mathfrak{p}$ such that $\ell^k \mid \mathrm{ord}_{\mathfrak{p}}(a)$.*

(3) *We have*

$$\gcd(\mathrm{ord}_{\mathfrak{p}}(a)) = 1,$$

where $\mathfrak{p}$ ranges over any family containing almost all primes.

A point $a \in G(k)$ satisfying those three conditions might be called a *fairly well-spread point.*

Proof. (1) If a is of finite order d, then $\{na \mid n \geqslant 1\}$ is a finite set, hence so is $S = \{\mathfrak{p} \mid na \equiv 0 \,(\mathrm{mod}\, \mathfrak{p})$ for some $n \geqslant 1\}$. Clearly the condition in the definition does not hold for S.

(2) We need to prove that the ℓ-valuation of the orders of a modulo primes is not bounded. Let $k_0 \geqslant 1$ be an arbitrary integer, and consider the set

$$S_k = \{\mathfrak{p} \mid \ell^k a \equiv 0 \,(\mathrm{mod}\, p) \text{ for some } k < k_0\}.$$

This is a finite set of places hence, since a is well-spread, there exists $k \geqslant k_0$ and a prime $\mathfrak{p} \notin S_k$ such that $\ell^k a \equiv 0 \,(\mathrm{mod}\, \mathfrak{p})$. The order of a modulo $\mathfrak{p}$ is then a multiple of ℓ^{k_0} (otherwise $\mathfrak{p} \in S_k$).

(3) Let

$$S' = \{\mathfrak{p} \mid \ell a \equiv 0 \,(\mathrm{mod}\, \mathfrak{p}) \text{ for some prime number } \ell\}.$$

The set S' is infinite since a is well-spread. Given a set of primes containing almost all of them, take $\mathfrak{p}$ and $\mathfrak{q} \neq \mathfrak{p}$ in S', then we have

$$(\mathrm{ord}_{\mathfrak{p}}(a), \mathrm{ord}_{\mathfrak{q}}(a)) = 1.$$

[4] The exceptions depending possibly on S.

□

Lemma 6.4. *Let G/k be a commutative algebraic group over a number field, $a \in G(k)$ a well-spread element. Then*

$$\ll a \gg \cap\, G(k)_{tors} = \{0\}.$$

Proof. Let $b \in \ll a \gg$ be an element of finite order $n \geqslant 1$. Then for almost all $\mathfrak{p}$, $b \pmod{\mathfrak{p}}$ is of order n; since $b \in \ll a \gg$, we find that the order of a modulo $\mathfrak{p}$ is divisible by n for almost all $\mathfrak{p}$. Since a is well-spread, by (3) of Lemma 6.3, we have $n = 1$ and $b = 0$. □

The condition of being well-spread seems quite strong. In fact it is known in few cases only.

Proposition 6.5. *Let G/k be either the multiplicative group of a number field, or an elliptic curve over a number field. Then $a \in G(k)$ is well-spread if and only if a is of infinite order.*

Proof. If $G/k = E/k$ is an elliptic curve, this follows directly from the Siegel-Mahler Theorem (see e.g. [Si-1, Cor. 3.2.1]) on finiteness of S-integral points on elliptic curves, since in standard Weierstrass coordinates

$$y^2 = x^3 + a_4 x + a_6$$

a point $a = (x, y)$ is S-integral if and only if $a \not\equiv 0 \pmod{\mathfrak{p}}$ for $\mathfrak{p} \notin S$.

If $G/k = \mathbf{G}_m/k$, then it is a consequence of the finiteness theorem for S-unit equations $ax + by = 1$: indeed, let $a \in k^\times$ be an element which is not well-spread. This means there is a finite set S of places and infinitely many values of $n \geqslant 1$ such that $a^n - 1 = y$ is an S-unit. Let

$$T = S \cup \{\mathfrak{p} \mid v_{\mathfrak{p}}(a) \neq 0\}.$$

Then $a^n - y = 1$, a^n and y are both T-units, and there are infinitely many $n \geqslant 1$ for which this holds. However, Siegel (see e.g. [Si-1, Th. 4.1]) has shown that for any finite set of places T, there are only finitely many pairs (x, y) of T-units in k such that $x - y = 1$. Therefore the pairs (a^n, y) range over finitely many elements, and a is of finite order. □

Remark 6.6. In fact, in both cases, stronger results are known. In particular, the properties in Lemma 6.3 follow immediately from the fact that if $a \in G(k)$ is of infinite order, then for all but finitely many integers $n \geqslant 1$ there exists a prime $\mathfrak{p}$ with $\mathrm{ord}_{\mathfrak{p}}(a) = n$. This is proved by Schinzel [Sc1] for the multiplicative group, by Silverman [Si-2, Pr. 10] for elliptic curves over $\mathbf{Q}$ and by Cheon–Hahn [CH] for elliptic curves over arbitrary number fields.

The proof (for elliptic curves) uses a stronger version of Siegel's Theorem (see [Si-1, Ex. 3.3]) that says, roughly speaking, that as the height gets large, *both* the numerator and denominator of rational points on E get large.

How much can this be generalized? In particular (see below), is it true that any point of infinite order in a (simple) abelian variety A/k is well-spread, or at least satisfies the three conditions of Lemma 6.3? We will see below a more general case coming from [KP] .

The diophantine statement in the definition sounds plausible enough, but one should keep in mind Faltings's example [Fa-2]: on $A = E \times E$, take $a = (x, x)$ with $x \in E(k)$ an *integral point* of infinite order. Then none of the points $a_{n,m} = (nx, mx)$ with $(n, m) = 1$ ever satisfy $a_{n,m} \equiv 0 \pmod{\mathfrak{p}}$ for any $\mathfrak{p}$, since this would imply $x \equiv 0 \pmod{\mathfrak{p}}$, contradicting that x is integral.

Lemma 6.7. *Let G/k be a commutative algebraic group of finite type over a number field, $a \in G(k)$. Then a is of finite order if and only if the orders $\mathrm{ord}_{\mathfrak{p}}(a)$ of a modulo (almost all) primes are bounded.*

Proof. Only the "if" implication requires proof. Assume $M \geqslant 1$ is such that $\mathrm{ord}_{\mathfrak{p}}(a) \mid M$ for all $\mathfrak{p}$. Making a finite field extension, we can assume that $G[M](\bar{\mathbf{Q}}) \subset G(k)$.

The hypothesis means that $a_{\mathfrak{p}} \in \mathcal{G}_{\mathfrak{p}}[M]$ for almost all $\mathfrak{p}$, but also for almost all $\mathfrak{p}$ the reduction map

$$G[M](k) \to \mathcal{G}[M](\bar{\mathbf{F}}_{\mathfrak{p}})$$

is bijective (4.4) and $G[M](k)$ is finite, hence there exists an $a' \in G[M](k)$ such that $a \equiv a' \pmod{\mathfrak{p}}$ for infinitely many $\mathfrak{p}$. Then $a = a'$ is of finite order. □

The next two lemmas are a first step in making non-trivial use of the formalism satisfied by $\ll a \gg$.

Lemma 6.8. *Let A/k be a simple abelian variety over a number field, $a \in A(k)$ a well-spread element. If $f \in \mathrm{End}_k(A)$ is an isogeny satisfying $f(a) \in \ll a \gg$, then $f(a) \in \, <a>$.*

Proof. Let ℓ be a prime number. By (2) of Lemma 6.3, we can find infinitely many $\mathfrak{p}$ prime to ℓ such that ℓ divides the order of a modulo $\mathfrak{p}$. Take one such $\mathfrak{p}$ for which there exists $n \in \mathbf{Z}$ satisfying $f(a) \equiv na \,(\mathrm{mod}\, \mathfrak{p})$.

Since the group generated by $a \,(\mathrm{mod}\, \mathfrak{p})$ contains an element of order ℓ, there exists $y \in \mathcal{A}(\mathbf{F}_{\mathfrak{p}})[\ell]$ satisfying

$$f(y) = ny, \tag{15}$$

and because of Lemma 4.4 there exists $z \in A[\ell]$ such that $f(z) = nz$.

In other words, there is an eigenvector of f acting on $A[\ell]$ with eigenvalue a rational integer. Now consider f acting on the ℓ-adic Tate module of A, which is a finite dimensional $\mathbf{Q}_\ell$-vector space. Since A is simple, its minimal polynomial is irreducible and we know it is independent of ℓ. By Hensel's lemma, (15) implies that one eigenvalue of f (acting on the Tate module) is an integer modulo ℓ. By irreducibility, any eigenvalue θ is an integer modulo ℓ. Since ℓ ranges over almost all primes, and the characteristic polynomial doesn't depend on ℓ, it follows that θ and its conjugates are all integers (again Kronecker's Theorem), and finally that f is multiplication by n for some $n \in \mathbf{Z}$ (for the last step, say for instance that almost all primes are split in $\mathbf{Q}(\theta)$...) □

Proposition 6.9. *Let G/k be a commutative algebraic group scheme over a number field, $a \in G(k)$.*

(1) If $G = A$ is a simple abelian variety or $G = \mathbf{G}_m$, and a is well-spread then $\ll a \gg \, = \, <a>$.

(2) If a is of finite order, then $\ll a \gg \, = \, <a>$.

Proof. Let $b \in \ll a \gg$ for both parts.

We start with the second statement. Since a is of finite order, the orders $\mathrm{ord}_{\mathfrak{p}}(b)$ of b modulo primes are bounded, so Lemma 6.7 shows that b is a torsion point, say of order M. Then the injectivity of the reduction map on torsion (Lemma 4.4) $G(k)[M] \hookrightarrow G_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}})$ modulo some large prime $\mathfrak{p}$ shows that $b \in \ll a \gg$ implies $b \in \, <a>$.

We now come to part (1). In both cases, according to Proposition 6.1, there are endomorphisms f and $g \in \mathrm{End}_k(G)$, not both zero, with $f(a) = g(b)$.

Consider first the case of a simple abelian variety. Then f and g are both isogenies since a, being well-spread, is not a torsion point (Lemma 6.7 again). Similarly, b is of infinite order (otherwise, $f(da) = g(db) = 0$ for some d, hence a would be of finite order).

Composing with an isogeny $g' \in \mathrm{End}_k(B)$ such that $g' \circ g = d \in \mathbf{Z}$, we find that in fact there exists a non-zero isogeny $f \in \mathrm{End}_k(A)$ (not the same as before) and $m \geqslant 1$ such that $f(a) = mb$ In particular, we have also $f(a) \in \ll a \gg$.

By Lemma 6.8, we find that $f(a) = na$ for some $n \in \mathbf{Z}$, hence the equation we have is $na = f(a) = mb$ with $nm \neq 0$.

Now we can incorporate back the case $G = \mathbf{G}_m$: since $\mathrm{End}_k(\mathbf{G}_m) = \mathbf{Z}$, the equation $f(a) = g(b)$ is also of the form $na = mb$ (with $nm \neq 0$).

Reducing modulo $\mathfrak{p}$ and comparing with $b \equiv n(\mathfrak{p})a \,(\mathrm{mod}\, \mathfrak{p})$, we get

$$na \equiv n(\mathfrak{p})ma \,(\mathrm{mod}\, \mathfrak{p}).$$

This precisely means that $m \equiv 0 \,(\mathrm{mod}\, (n, \mathrm{ord}_{\mathfrak{p}}(a)))$. But since a is well-spread, taking suitable primes $\mathfrak{p}$ we find that $m \equiv 0 \,(\mathrm{mod}\, n)$ or $n \mid m$ (Lemma 6.3, (2)) Finally from $na = mb$, we get $b = (m/n)a + d$ with $d \in G[n]$ of finite order. However, this equation implies $d \in \ll a \gg$, hence $d = 0$ by Lemma 6.4.

Finally we have $b = (m/n)a \in \, <a>$. □

This proposition, in particular, proves Theorem 3.3. We conclude this section with some remarks about other cases.

First, in the recent preprint [KP], Khare and Prasad show (Corollary 2) what amounts to the following result: if A/k is an abelian variety over a number field of dimension $g \geqslant 1$ such that $\mathrm{End}(A) = \mathbf{Z}$ and $\mathrm{Gal}(k(A[\ell])/k) \simeq GSp_{2g}(\mathbf{F}_\ell)$ for all ℓ large enough, then $\ll a \gg = <a>$ for any $a \in A(k)$.

Note that by results of Serre [Se-6], the assumption on the Galois groups holds if $\mathrm{End}(A) = \mathbf{Z}$ for g odd or for $g \in \{2, 6\}$.

We can prove this as follows in our framework, using other results of [KP]: according to Proposition 6.9, we can assume that a is of infinite order. Then, as remarked earlier, it is enough to show that under the assumptions stated, the point a is fairly well-spread, i.e. satisfies the statements in Lemma 6.3. The first one is true, for the second we appeal to Lemma 3 of [KP], which states that for any $b \in A(k)$ and any prime ℓ, there are infinitely many prime ideals $\mathfrak{p}$ such that $\ell \mid \mathrm{ord}_{\mathfrak{p}}(b)$. (This does not require the assumptions on A).

Given a prime ℓ and $k \geqslant 1$, we apply this to $b = \ell^k a$. For any $\mathfrak{p}$ given by this, we have $\ell \mid \mathrm{ord}_{\mathfrak{p}}(\ell^k a)$, hence $\ell^{k+1} \mid \mathrm{ord}_{\mathfrak{p}}(a)$. Since k is arbitrary, this proves the second condition for a.

To show the last condition, we appeal to Lemma 5 of [KP], which does require the assumptions on A: for any a of infinite order and any prime ℓ, there exist infinitely many $\mathfrak{p}$ such that $\ell \nmid \mathrm{ord}_{\mathfrak{p}}(a)$. This clearly implies the required condition.

Weston [We] has proved a fairly general result about local-global relations for subgroups of Mordell-Weil groups of abelian varieties over number fields. A consequence of his main theorem is the following: if A/k is an abelian variety over a number field such that $\mathrm{End}_k(A)$ is commutative, and $a \in A(k)$ is a rational point, then $\ll a \gg \subset <a> + A(k)_{tors}$.

Note that if one could prove (3) of Lemma 6.4 for the abelian varieties of this theorem, the torsion indeterminacy could be removed (for infinite order points of course).

Although it is not clear whether a non-torsion point in a general torus is well-spread or not[5], we can show that $\ll a \gg = <a>$ is almost certainly always true. (Compare [DZ, Ex 5.1] where it is shown that a rational point of a torus can be divisible by a prime p at almost all places without being a p-th power).

Proposition 6.10. *Assume that for any number field k there exists an integer $w = w(k) \geqslant 1$ such that k contains infinitely many prime ideals $\mathfrak{p}$ with $N\mathfrak{p} = zq + 1$ with q prime and $z \mid w$.*

Then for any torus G/k over a number field and any $a \in G(k)$, we have $\ll a \gg = <a>$.

Proof. First by Corollary 4.2, we can assume that G/k is split, i.e. $G = \mathbf{G}_m^r$ for some $r \geqslant 1$.

If $r = 1$, Proposition 6.9 proves that $\ll a \gg = <a>$ for any a.

If $b = (b_i)$ is in $\ll a \gg = \ll (a_i) \gg$, we have $b_i \in \ll a_i \gg$, hence by the rank 1 case, there exists n_i such that

$$b_i = n_i a_i$$

(recall the group law is written additively). We wish to show that $n_i = n_j$ for all i and j. Clearly it suffices to show that $n_1 = n_2$ (i.e. to treat the case $r = 2$).

The assumption $b \in \ll a \gg$ means that for almost all $\mathfrak{p}$ we have

$$(b_1, b_2) = (n_1 a_1, n_2 a_2) \equiv n(\mathfrak{p})(a_1, a_2) \pmod{\mathfrak{p}}$$

for some $n(\mathfrak{p}) \in \mathbf{Z}$. Hence

$$n_1 \equiv n_2 \;(\mathrm{mod}\,(\mathrm{ord}_{\mathfrak{p}}(a_1), \mathrm{ord}_{\mathfrak{p}}(a_2))). \tag{16}$$

By hypothesis, there exist infinitely many prime ideals $\mathfrak{p}$ such that $N\mathfrak{p} - 1 = zq$ with q prime, $z \mid w$. The order of any element in $\mathbf{G}_m(k)$ modulo $\mathfrak{p}$ is a divisor of $N\mathfrak{p} - 1$, hence either a divisor of w, or a multiple of q.

[5] Or is merely fairly well-spread.

The set of those $\mathfrak{p}$ where $\mathrm{ord}_{\mathfrak{p}}(a_i) \mid w$ is finite, so we conclude that there are infinitely many such $\mathfrak{p}$ where

$$q \mid (\mathrm{ord}_{\mathfrak{p}}(a_1), \mathrm{ord}_{\mathfrak{p}}(a_2)). \tag{17}$$

Since $z \mid w$ is bounded, the number q gets arbitrarily large. Now (16) and (17) together imply $n_1 = n_2$ as desired. □

This allows the computation of $\ll a \gg$ for any point $a \in G(k)$ where G is a linear group.

Proposition 6.11. *Let k be a number field, $n \geqslant 1$ and $G \subset GL(n)$ a linear group over k. For any $a \in G(k)$, let $a = a_s a_u$ be its Jordan-Hölder decomposition. Then*

$$\ll a \gg = \ll a_s \gg a_u^{\mathbf{Q}}$$

where for $t \in k$, $a_u^t = \exp(t \log a_u)$ is in the 1-parameter subgroup generated by a_u. If the condition of Proposition 6.10 holds for k, then

$$\ll a \gg = <a> a_u^{\mathbf{Q}}.$$

Proof. We can assume $G = GL(n)$ by Lemma 4.2 (independence of $\ll \cdot \gg$ from the choice of ambient group).

Let $b = b_s b_u \in \ll a \gg$. Reducing modulo almost all $\mathfrak{p}$ and using the fact that a_s and a_u commute, there exists $n(\mathfrak{p}) \in \mathbf{Z}$ such that

$$b_s b_u \equiv a_s^{n(\mathfrak{p})} a_u^{n(\mathfrak{p})} \pmod{\mathfrak{p}},$$

and by unicity of the Jordan-Hölder decomposition, we deduce in particular $b_s \in \ll a_s \gg$ and $b_u \in \ll a_u \gg$.

Since we have an injection $\mathbf{G}_a \hookrightarrow G$ (over k) by $t \mapsto a_u^t = \exp(t \log a_u)$, Lemma 4.2 again implies that $\ll a_u \gg = a_u^{\mathbf{Q}}$. Hence we get $b \in \ll a_s \gg a_u^{\mathbf{Q}}$.

For the converse inclusion, note from Proposition 3.2, (2) that $a_s \in \ll a \gg$ so $\ll a_s \gg < \ll a \gg$. Then $a_u = a_s^{-1} a \in \ll a \gg$ (since a and a_s commute), hence $a_u^{\mathbf{Q}} = \ll a_u \gg < \ll a \gg$ also.

Now if the condition of Proposition 6.10 holds, we can also argue that since there exists a torus $T < GL(n)$ such that $a_s \in T(k)$, we have $\ll a_s \gg = <a_s>$ by the previous proposition together with Lemma 4.2 again. □

Remark 6.12. The assumption of Proposition 6.10 very probably holds, even with $w = 2$ (in which case $\mathfrak{p}$ is actually of degree 1). For $k = \mathbf{Q}$, primes of the type $p = 2q + 1$ are the famous Sophie Germain primes. Sieve methods, like in Chen's theorem, can be used to show that there are infinitely many primes p with $(p-1)/2$ having at most 2 prime factors, but it doesn't seem possible to use these to conclude.

Also related to the problem of computing $\ll a \gg$ for $\mathbf{G}_m \times \mathbf{G}_m$ is the preprint [RA] of Rudnick and Ailon. Their conjecture that if a and b are multiplicatively independent, then $(a^k - 1, b^k - 1) = 1$ infinitely often would imply that (a, b) is not well-spread for instance.

Remark 6.13. The same reasoning shows that if $G = G_1 \times G_2$ and $a = (a_1, a_2)$, then assuming that $\ll a_i \gg = <a_i>$, we will have $\ll a \gg = <a>$ if the greatest common divisors $(\mathrm{ord}_{\mathfrak{p}}(a_1), \mathrm{ord}_{\mathfrak{p}}(a_2))$ are not bounded, where $\mathfrak{p}$ ranges over any set containing almost all prime ideals.

Furthermore, a converse holds: if this gcd is bounded, say it is $= \delta$, then we have

$$(ma_1, na_2) \in \ll a \gg$$

if $m \equiv n \pmod{\delta}$.

For a product of two elliptic curves $E_1 \times E_2$, numerical experiments and simple-minded heuristics suggest that the gcd is unbounded. For instance, taking

$$E_1 : \ y^2 - y = x^3 - x, \text{ with } a_1 = (0, 0)$$

$$E_2 : \ y^2 = x^3 - x + 4, \text{ with } a_2 = (0, 2),$$

(both points are of infinite order) we find that

$$\begin{aligned}\operatorname{lcm}(\gcd(\operatorname{ord}_p(a_1),\operatorname{ord}_p(a_2))) &= 1249684129741371320018443292797088832789133225944 \\ &\quad 99546276465401457270823146965503396570875758811040 0\\ &= 2^6\cdot 3^5\cdot 5^2\cdot 7^2\cdot 11^2\cdot 13^2\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41\cdot 43\cdot 47\cdot 53\cdot 59\cdot 61\cdot 71\cdot 79\cdot 83\\ &\quad \cdot 89\cdot 97\cdot 101\cdot 109\cdot 127\cdot 137\cdot 149\cdot 173\cdot 311\cdot 397\cdot 419\cdot 547\cdot 599\cdot 643\cdot 653\cdot 677\\ &\quad \cdot 811\cdot 1103\cdot 1511\cdot 3557\cdot 4451\cdot 7411\cdot 16249\end{aligned}$$

where p runs over primes $\leqslant 100,000$. One argument has it that there are (experimentally and heuristically) many primes p where $|E_{i,p}(\mathbf{Z}/p\mathbf{Z})| = q|E_{i,tors}(k)|$ with q prime, among which there are only finitely many where $\operatorname{ord}_p(a_1) \mid |E_{1,tors}(k)|$ or $\operatorname{ord}_p(a_2) \mid |E_{2,tors}(k)|$. [6]

For the same reasons, it is unlikely that a similar argument could work for general abelian varieties, but it should apply to $\mathbf{G}_m \times E$, E/k an elliptic curve.

7. Proof of Proposition 3.6

We will first compute explicitly the kind of Kummer extensions involved in Lemma 5.3 and Proposition 5.5. From this, it will be a fairly simple matter of standard Kummer theory to deduce Proposition 3.6 and Theorem 3.4. (1).

Lemma 7.1. *Let k be a field of characteristic 0 and*

$$G = \prod_i \operatorname{Res}_k^{k_i}(\mathbf{G}_m)$$

a quasi-split torus over k, where k_i/k are finite Galois extensions of k. Let $K = \prod k_i$.

(1) *For $n \geqslant 2$, the n-torsion field $k(G[n])$ of G satisfies*

$$K(G[n]) = K(\boldsymbol{\mu}_n).$$

(2) *Let $a = (a_i) \in G(k)$. For $n \geqslant 2$, the Kummer extension of n-th roots of a satisfies*

$$K(n^{-1}{<}a{>}) = K(\boldsymbol{\mu}_n, (\sqrt[n]{a_i^\sigma})_{i,\sigma})$$

where σ runs over $\operatorname{Gal}(K/k)$, and we identify a_i with an element of $k_i^\times \subset K^\times$.

Proof. It suffices to deal with a single factor, i.e. $G = \operatorname{Res}_k^{k'}(\mathbf{G}_m)$ with $K = k'$. By the very definition of the restriction of scalars, there is a group isomorphism

$$G(\bar{k}) = \prod_\sigma \bar{k}^\times$$

where σ runs over the embeddings $k' \hookrightarrow \bar{k}$, the Galois action of $\operatorname{Gal}(\bar{k}/k')$ being componentwise, and the inclusion $(k')^\times = G(k) \hookrightarrow G(\bar{k})$ is given by

$$a \mapsto (\sigma(a))_\sigma. \tag{18}$$

(1) It follows that

$$G[n] = \{(\xi_\sigma)_\sigma \mid \xi_\sigma \in \boldsymbol{\mu}_n \text{ for all } \sigma\},$$

with a similar Galois action. So $\sigma \in \operatorname{Gal}(\bar{k}/k')$ acts trivially on $G[n]$ if and only if it does so on $\boldsymbol{\mu}_n$.

(2) For $a \in (k')^\times$ we have, using the description (18)

$$\{x \in G(\bar{k}) \mid x^n = a\} = \{(y_\sigma)_\sigma \mid y_\sigma^n = \sigma(a)\},$$

as $G[n]$-homogeneous space. The result thus follows immediately. □

The main tool will then be the following simple corollary of Kummer theory:

[6] The natural guess is that there are $\gg \sqrt{X}/(\log X)^2$ primes $p \leqslant X$ with the property stated.

Lemma 7.2. *Let k be a number field, $(a_0, \dots, a_m) \in (k^\times)^{m+1}$ elements of k. Then we have*

$$k(\boldsymbol{\mu}_n, \sqrt[n]{a_0}) \subset k(\boldsymbol{\mu}_n, \sqrt[n]{a_1}, \dots, \sqrt[n]{a_m}) \tag{19}$$

for all $n \geqslant 1$ if and only if $a_0 \in <a_1, \dots, a_m>$.

We need two simple lemmas.

Lemma 7.3. *Let k be a number field, let $G \subset k^\times$ be a finitely generated subgroup. For almost all prime numbers ℓ, the largest abelian subextension (over k) of the Kummer extension $k(\boldsymbol{\mu}_\ell, \ell^{-1}G)$ is $k' = k(\boldsymbol{\mu}_\ell, \ell^{-1}G_{tors})$.*

Proof. Let G^0 be the free part of G. Since $\mathbf{G}_m$ has large Kummer extensions, for ℓ large enough we have

$$\mathrm{Gal}(k(\boldsymbol{\mu}_\ell, \ell^{-1}G^0)/k(\boldsymbol{\mu}_\ell)) \simeq (\mathbf{Z}/\ell\mathbf{Z})^{\mathrm{rank}(G^0)},$$

and $\mathrm{Gal}(k(\boldsymbol{\mu}_\ell, \ell^{-1}G^0)/k) \simeq (\mathbf{Z}/\ell\mathbf{Z})^{\mathrm{rank}(G^0)} \ltimes (\mathbf{Z}/\ell\mathbf{Z})^\times$, hence the maximal abelian subextension is $k(\boldsymbol{\mu}_\ell)$. Adding the ℓ-th roots of G_{tors}, the result follows. □

The second one is a weak version of (consequences of) the S-unit theorem in infinite cyclotomic extensions.

Lemma 7.4. *Let k be a number field, $G \subset k^\times$ a finitely generated subgroup, $K = k(\boldsymbol{\mu}_\infty)$ the field obtained by adjoining all roots of unity to k. Then the group*

$$\tilde{G} = \{x \in K^\times \mid x^n \in G \textit{ for some } n \geqslant 1\}$$

is of the form $\tilde{G} \simeq \mu_\infty \times G_1$ for some subgroup G_1 such that $[G_1 : G] < +\infty$.

Proof. Let

$$K' = \bigcup_n k(\boldsymbol{\mu}_n, n^{-1}G)$$

be the Kummer extension associated to all n-th roots of G. By Kummer Theory the Galois group of K'/K is known to be a finite index subgroup of $\hat{\mathbf{Z}}^r$, where r is the rank of G (see e.g. [Hi, App.], [La1, IV-§4]).

If $y \in K^\times$ is not a root of unity and satisfies $x = y^n \in G$, we have $k(\boldsymbol{\mu}_n, x^{1/n}) \subset K$: it follows by Galois theory from the above that all such y belong to a finite subextension k_1/k inside K. Hence

$$\tilde{G} \subset \boldsymbol{\mu}_\infty \times \{x \in k_1^\times \mid x^n \in G \text{ for some } n \geqslant 1\}$$

and the second factor is finitely generated by the S-unit theorem. □

Proof of Lemma 7.2. The "if" part is obvious, so let's assume that (19) holds for $n \geqslant 1$. Let $G = <a_1, \dots, a_m>$ and $G' = <a_0, \dots, a_m>$ in $k^\times$.

By classical Kummer Theory (see e.g. [La2, VIII-8]), i.e. the classification of finite abelian extensions of $k(\boldsymbol{\mu}_n)$ of exponent dividing n by finite subgroups of $k(\boldsymbol{\mu}_n)^\times/(k(\boldsymbol{\mu}_n)^\times)^n$, the assumption is equivalent with $a_0 \in <a_1, \dots, a_m>(k(\boldsymbol{\mu}_n)^\times)^n$ for all $n \geqslant 1$. So for any $n \geqslant 1$ we can write

$$a_0 = \psi_n \beta_n^n, \text{ with } \psi_n \in G,\ \beta_n \in k(\boldsymbol{\mu}_n)^\times. \tag{20}$$

Let $\tilde{G}$, $\tilde{G}'$ be the groups defined in Lemma 7.4 for G and G'. By construction we have $\beta_n \in \tilde{G}'$, and because $\mathbf{G}_m/k$ has large Kummer extensions, it is clear that $a_0 \in \tilde{G}'$, i.e. $\tilde{G} = \tilde{G}'$.

By Lemma 7.4 we can therefore write $\beta_n = \xi_n \gamma_n$ with ξ_n a root of unity and $\gamma_n \in G_1' = G_1$. We know that $[G_1' : G] = [G_1 : G] < +\infty$. Take n a multiple of this index: then by definition $\gamma_n^n \in G$, hence (20) becomes

$$a_0 = \xi_n^n \psi_n \gamma_n^n \in \boldsymbol{\mu}_\infty(k^\times) \times G.$$

If we write $a_0 = \xi b$ with $\xi \in k^\times$ a root of unity of order $d \geqslant 1$ and $b \in G$, we see that for all prime numbers ℓ we have

$$k(\boldsymbol{\mu}_{\ell d}) \subset k(\boldsymbol{\mu}_\ell, \sqrt[\ell]{a_1}, \dots, \sqrt[\ell]{a_n}).$$

By Lemma 7.3, it follows that $\xi \in G$, hence the result. □

Proof of Proposition 3.6. It is clear that (1) implies (2). It suffices to show that (2) implies (3) implies (1).

The latter is easy: if $b \in <(a^\sigma)>$ is in the subgroup generated by the conjugates of a, say

$$b = \prod_\sigma \sigma(a)^{n(\sigma)},$$

then for any integers $n \geqslant 1$ and $d \geqslant 1$ such that $d \mid a^n - 1$, we have $d \mid (a^\sigma)^n - 1$ for all σ, hence

$$b^n \equiv \prod_\sigma \sigma(a)^{nn(\sigma)} \equiv 1 \,(\mathrm{mod}\, d),$$

so that (1) follows immediately.

Now assume that (2) holds. By Lemma 5.3 and Lemma 7.1, we have for any $n \geqslant 1$ the inclusion

$$k(\boldsymbol{\mu}_n, \sqrt[n]{b}) \subset k(\boldsymbol{\mu}_n, (\sqrt[n]{a^\sigma})_\sigma)$$

where σ ranges over $\mathrm{Gal}(k/\mathbf{Q})$. By Lemma 7.2, it follows that

$$b \in <(a^\sigma)> \subset k^\times,$$

as desired. □

8. End of the proof of Theorem 3.4

We come back to Problem 1.2. We mostly consider finite fields, for which Proposition 5.5 applies. The case of number fields can be reduced to that:

Lemma 8.1. *Let k be a number field, A and B abelian varieties over k. If $A \simeq_\kappa B$ then $\mathcal{A}_\mathfrak{p} \simeq_\kappa \mathcal{B}_\mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$, and conversely if there exists a fixed $m \geqslant 1$ such that*

$$\mathbf{F}_\mathfrak{p}(\mathcal{A}_\mathfrak{p}[d]) = \mathbf{F}_\mathfrak{p}(\mathcal{B}_\mathfrak{p}[d])$$

for all $\mathfrak{p}$ and all d coprime with $m\mathfrak{p}$, then $A \simeq_\kappa B$.

Proof. By Lemma 4.6, for almost all $\mathfrak{p}$ the residue field extension of $k(A[d])/k$ is $\mathbf{F}_\mathfrak{p}(\mathcal{A}[d])/\mathbf{F}_\mathfrak{p}$ and the first part follows.

The second is equally simple using Lemma 4.1; note that because the m in (2) is allowed to depend on A and B (hence here on $\mathfrak{p}$), one cannot simply ask that $\mathcal{A}_\mathfrak{p} \simeq_\kappa \mathcal{B}_\mathfrak{p}$ for all $\mathfrak{p}$. □

Also we make formal note of the following easy fact already mentioned:

Lemma 8.2. *Let k be a field, A and B isogenous abelian varieties over k. Then A and B are isokummerian.*

Proof. First, let $q = 1$ or p be the "characteristic exponent" of k. Let $f : A \to B$ be an isogeny. We have the exact sequence of Galois modules

$$0 \to \ker(f)(\bar{k}) \to A(\bar{k}) \to B(\bar{k}) \to 0.$$

Let $m = \deg(f)$, so that $\ker(f)(\bar{k}) \subset A[m](\bar{k})$. Then if $(d, mq) = 1$, looking at d-torsion points ($A[d]$ and $B[d]$ are étale in this case, so determined by their $\bar{k}$-points Galois module) in the above exact sequence we find that $A[d] \simeq B[d]$ as Galois modules, and in particular $k(A[d]) = k(B[d])$. □

We first derive the criterion of Theorem 3.4, (1), which we restate as a proposition; given Proposition 5.5, the argument is understandably very close to the proof of Proposition 3.6.

Recall that for A/k an abelian variety over a finite field, we let Φ_A denote the multiplicative subgroup of $\mathbf{C}^\times$ generated by the conjugates of the Frobenius eigenvalues of A. We call this for simplicity *the Frobenius group* of A.[7]

Proposition 8.3. *Let k be a finite field, A and B abelian varieties over k. Then $A \simeq_\kappa B$ if and only if $\Phi_A = \Phi_B$.*

[7] This is closely related to the notion (see [Se-5, p. 6]) of the *Frobenius torus* of an abelian variety over a finite field.

Proof. Let $\pi_1 \in \mathrm{End}_k(A)$, $\pi_2 \in \mathrm{End}_k(B)$ be the respective Frobenius endomorphisms of A and B, $\lambda_{i,j}$ the eigenvalues of π_i in $\bar{\mathbf{Q}}$, and $K_i = \mathbf{Q}((\lambda_{i,j})_j)$. If $A \simeq_\kappa B$, we have

$$K(n^{-1}{<}\pi_1, 1{>}) = K(n^{-1}{<}1, \pi_2{>})$$

(where $K = K_1K_2$), or equivalently

$$K(\boldsymbol{\mu}_n, (\sqrt[n]{\lambda_{1,j}})_j) = K(\boldsymbol{\mu}_n, (\sqrt[n]{\lambda_{2,j}})_j),$$

by Lemma 7.1. Applying Lemma 7.2, we get $\lambda_{1,j} \in {<}(\lambda_{2,i})_i{>} = \Phi_B$ for any j, hence $\Phi_A \subset \Phi_B$, and exchanging A and B, we get $\Phi_A = \Phi_B$.

Conversely, assuming that $\Phi_A = \Phi_B$, we deduce that A and B are isokummerian as in the proof of the easy part of Proposition 3.6, using (13). □

The other statements in Theorem 3.4 will be derived from this criterion. We recall the main statements of Honda-Tate theory ([Ta-1], [Ta-2]) which we'll use to analyze the Frobenius groups.

For any prime $\ell \neq p$, π acts semi-simply on the ℓ-adic Tate module of A, which is a $2\dim A$-dimensional free $\mathbf{Z}_\ell$-module, with "the same" eigenvalues λ_j. We have the Riemann Hypothesis, proved by Weil (see e.g. [Mu, 21, Th. 4]): for any eigenvalue λ of Frobenius, we have

$$|\lambda|^2 = |k| \tag{21}$$

for any embedding $\mathbf{Q}(\lambda) \hookrightarrow \bar{\mathbf{Q}} \hookrightarrow \mathbf{C}$. We recall that an algebraic integer λ, all conjugates of which are of the same modulus $\sqrt{q}$, is called a q-Weil number.

Now Honda-Tate theory gives:

(1) Two abelian varieties A and B over k are k-isogenous if and only if the characteristic polynomial of π_A is equal to that of π_B, if and only if the set of their Frobenius eigenvalues coincide.

(2) If $\lambda \in \bar{\mathbf{Q}}$ is a $|k|$-Weil number, there exists a simple abelian variety A/k for which the Frobenius eigenvalues are the conjugates of λ. This A is unique up to k-isogeny, and we will denote $M(\lambda)$ any simple abelian variety with this property.

Proof of (2) of Theorem 3.4. By Proposition 8.3, if B/k is multiplicity-free and isokummerian to A, any eigenvalue of Frobenius acting on B, say $\lambda = \lambda_{2,j}$, is an integer in $K_B = K_A$.

Let $M(\lambda)$ be the corresponding simple factor of B and $K_j \subset K_A$ the Galois closure of $\mathbf{Q}(\lambda)$. We denote $f = [k : \mathbf{Z}/p\mathbf{Z}]$, $d = \dim A$. Note that $[K_A : \mathbf{Q}] \leqslant (2d)!$

Claim. The dimension of $M(\lambda)$ is bounded by a function of d and f only, namely

$$\dim M(\lambda) \leqslant f(2d)!$$

Let us admit this. Then we have

$$N_{\mathbf{Q}}^{K_A}\lambda = (N_{\mathbf{Q}}^{K_j}\lambda)^{[K_A:K_j]} = |k|^{(\dim M(\lambda))[K_A:K_j]} = p^{f(\dim M(\lambda))[K_A:K_j]}$$

with an exponent of p, the characteristic of k, which is

$$\leqslant f[K_A : \mathbf{Q}] \dim M(\lambda) \leqslant (f(2d)!)^2.$$

Since λ is divisible only by primes above p, the number of which is at most $[K_A : \mathbf{Q}]$, and since this inequality bounds the valuation of any of those primes, the number N of possible values for λ is bounded by a function of d and f:

$$N \leqslant w(f(2d!))^{2(2d)!}$$

where w is the number of roots of unity in K_A, which obviously satisfies $w \ll (2d)!(\log d)$ (two Weil numbers in K_A differing by a unit differ by a root of unity in K_A.)

By part (2) of Honda-Tate theory, the number of elements in the set B_A is thus also bounded by a function of d and f. (The exact bound we can get is quite ridiculous as every $M(\lambda)$ described could be a distinct factor).

To prove the claim, we use the description of Honda-Tate [Ta-2, Th. 1 (ii)] of "the" simple abelian variety $M(\lambda)$.

Let $E = \mathrm{End}_k(M(\lambda)) \otimes \mathbf{Q}$, a central division algebra with center $\mathbf{Q}(\lambda)$. Then we have

$$2\dim M(\lambda) = [E : \mathbf{Q}(\lambda)]^{1/2}[\mathbf{Q}(\lambda) : \mathbf{Q}]. \tag{22}$$

The second factor is bounded by

$$[\mathbf{Q}(\lambda) : \mathbf{Q}] \leqslant [K_j : \mathbf{Q}] \leqslant [K_A : \mathbf{Q}] \leqslant (2d)!$$

For the first, the algebra E has invariant $\frac{1}{2}$ at a real place, is split at all finite places of $\mathbf{Q}(\lambda)$ outside p, and for a place $v \mid p$, its invariant at v is (loc.cit.)

$$\mathrm{inv}_v(E) = \frac{v(\lambda)}{v(|k|)}[\mathbf{Q}(\lambda)_v : \mathbf{Q}_p] = \frac{v(\lambda)f_v}{[k : \mathbf{Z}/p\mathbf{Z}]} = \frac{v(\lambda)f_v}{f} \in \mathbf{Q}/\mathbf{Z},$$

f_v being the absolute residual degree of v.

By the theory of division algebras over number fields, the dimension $[E : \mathbf{Q}(\lambda)]^{1/2}$ is the least common denominator of the local invariants (see e.g. [Se-1, XIII-Cor. 3]), hence it is $\leqslant 2f$ and we get

$$2\dim M(\lambda) \leqslant 2f(2d)!$$

which proves the claim. □

Proof of (3) of Theorem 3.4. The Frobenius eigenvalues of $A' = A \times_k k'$ are $\lambda_{1,j}^d$ where $d = [k' : k]$. Hence we have $\Phi_{A\times k'} \subset \Phi_A^d$, so if B'/k' is such that $B' \simeq_\kappa A \times k'$, its Frobenius eigenvalues are d-th powers in Φ_A, say $\lambda_{2,j} = \rho_j^d$ with $\rho_j \in \Phi_A$. It is clear that ρ_j is a $|k|$-Weil number. Let B/k be the abelian variety

$$B \simeq \prod_j M(\rho_j),$$

the product of the simple abelian varieties corresponding to ρ_j. Then $B \times k' \simeq B'$ by construction so B is a model of B' over k. □

Proof of (4) of Theorem 3.4. This is the case of elliptic curves. By Lemma 8.1 and Faltings's Isogeny Theorem [Fa-1], it is enough to treat the case of finite fields k. Let therefore E/k be an elliptic curve. We will show $\mathsf{B}_E = \{E\}$.

Let B be a multiplicity-free abelian variety, with $E \simeq_\kappa B$. Let λ be a Frobenius eigenvalue for B corresponding to a simple factor $M(\lambda)$.

First, assume E is supersingular. There are two cases: either $\pi_1 = \pm\sqrt{|k|} \in \mathbf{Q}$ (if $[k : \mathbf{Z}/p\mathbf{Z}]$ is even), and the conditions $\lambda \in \Phi_E \subset \mathbf{Q}$ and $|\lambda|^2 = |k|$ (21) imply $\lambda = \pi_1$; or $\pi_1 = i\sqrt{p}$ (up to conjugation, if $[k : \mathbf{Z}/p\mathbf{Z}]$ is odd) then $\lambda \in \Phi_E \subset \mathbf{R} \cup i\mathbf{R}$, and again the only $|k|$-Weil numbers in this set are $\pm\pi_1$. In either case $M(\lambda)$ is k-isogenous to E by Tate's Theorem.

Secondly, assume E is ordinary. Then $\mathbf{Q}(\pi_1)$ is an imaginary quadratic field, and π_1 and its conjugate $\bar\pi_1$ are coprime.

Indeed, since $N\pi_1 = |k|$, any prime ideal dividing both π_1 and $\bar\pi_1$ must be above p (the characteristic of k), and in $\mathbf{Q}$, so $p \mid a_E = \pi_1 + \bar\pi_1$, contradicting that E is ordinary. (If $k = \mathbf{Z}/p\mathbf{Z}$ is the prime field, π_1 and $\bar\pi_1$ are simply the primes above p in $\mathbf{Q}(\pi)$).

Coming back to the proof, since $\lambda \in <\pi_1, \bar\pi_1>$, write

$$\lambda = \pi_1^a \bar\pi_1^b \text{ with } a,\ b \in \mathbf{Z}.$$

Since λ is an integer and $(\pi_1, \bar\pi_1) = 1$, we have $a \geqslant 0$, $b \geqslant 0$. From the Riemann Hypothesis (21) we have $a + b = 1$, hence either $(a,b) = (1,0)$ and $\lambda = \pi_1$ or $(a,b) = (0,1)$ and $\lambda = \bar\pi_1$. Thus again $M(\lambda)$ is k-isogenous to E. □

Remark 8.4. Let A and B be isokummerian abelian varieties, multiplicity-free. We have shown this means that $\Phi_A = \Phi_B$. Here we relate this to geometric properties of A and B, hoping to ultimately show that (optimistically) A and B are $\bar k$-isogenous. Let λ be a Frobenius eigenvalue for A.

We have $\lambda \in \Phi_B$, i.e. there is a relation

$$\lambda = \prod_j \lambda_{2,j}^{m_j} \text{ with } m_j \in \mathbf{Z}. \tag{23}$$

Let

$$m = m^+ = \sum_{m_j \geqslant 0} m_j \geqslant 0, \text{ and } m^- = \sum_{m_j < 0} m_j.$$

Using the relation $\lambda\bar{\lambda} = |k| = q$ for any eigenvalue of Frobenius (i.e. the Riemann Hypothesis), we have first $m^+ - m^- = 2m - 1$, and then

$$q^m = \bar{\lambda} \prod_{m_j \geqslant 0} \lambda_{2,j}^{m_j} \prod_{m_j < 0} \bar{\lambda}_{2,j}^{-m_j}. \tag{24}$$

The product on the right *is* a Frobenius eigenvalue on (say) the ℓ-adic étale cohomology group

$$H^1_{et}(A, \mathbf{Q}_\ell) \otimes H^1_{et}(B, \mathbf{Q}_\ell)^{\otimes(2m-1)} \hookrightarrow H^{2m}_{et}(A \times B^{2m-1}, \mathbf{Q}_\ell),$$

and the identity shows that the corresponding eigenvector x has eigenvalue $= q^m$, which means

$$x \in H^{2m}_{et}(A \times B^{2m-1}, \mathbf{Q}_\ell(m))^{G_k}$$

after a Tate twist. The Tate Conjecture says that this $\mathbf{Q}_\ell$-vector space should be the space spanned by the image of the cycle map (see e.g. [Ta-3], [Mi-1, VI-9])

$$\gamma \,:\, CH^m(A \times B^{2m-1}) \otimes \mathbf{Q}_\ell \to H^{2m}_{et}(A \times B^{2m-1}, \mathbf{Q}_\ell(m))$$

from the space of cycles of codimension m to étale cohomology.

Assuming the Tate Conjecture, the existence of a relation (23) is therefore *equivalent* with the existence of some algebraic cycle Z in $A \times B^{2m-1}$, of codimension m, such that

$$\gamma(Z) \in H^1_{et}(A, \mathbf{Q}_\ell) \otimes H^1_{et}(B, \mathbf{Q}_\ell)^{\otimes(2m-1)}.$$

To conclude that the simple factor of A corresponding to λ is also one of B, it is sufficient (on the Tate Conjecture) that such a cycle doesn't exist otherwise. For $m = 1$, this is true, as this case of the conjecture was proved by Tate, and then the cycle γ gives the graph of a morphism $A \to B$ non-zero on $M(\lambda)$.

See also, for instance, [So, 3.2] or [LZ] for similar discussions, which are of the opposite flavor: "if there is no non-trivial relation between eigenvalues, then the Tate Conjecture holds".

Proof of (5) of Theorem 3.4. Let k be a finite field, $A = E_1 \times \cdots \times E_m$ and B an abelian variety such that $B \simeq_\kappa A$.

Let λ be a Frobenius eigenvalue for the simple factor $M(\lambda)$ of B. We have $\lambda \in \Phi_A$, hence a relation

$$q^m = \lambda\lambda_2 \cdots \lambda_{2m}$$

of the type (24) for some $m \geqslant 1$, where each λ_i is a Frobenius eigenvalue for one of the elliptic curves $E_i \hookrightarrow A$. Choose a relation of the form

$$\xi q^m = \lambda\lambda_2 \cdots \lambda_{2m} \tag{25}$$

with ξ a root of unity and m minimal. (With $\xi \neq 1$, such a relation might occur with m smaller than for $\xi = 1$).

Claim. We have $m = 1$, i.e. there exists i, $2 \leqslant i \leqslant 2m$ and a root of unity ξ such that $\lambda\lambda_i = \xi q$.

Assuming this, say $\xi^d = 1$, we have $\lambda^d = \lambda_i^d$, which means that over the extension k_d/k, the simple factor $M(\lambda)$ factors further as a product of d elliptic curves each k_d-isogenous to $E \times k_d$ where $E \simeq M(\lambda_i)$ is an elliptic factor of A.

This holds for all λ, and it follows that for some finite extension k'/k, $B \times k'$ is isogenous to a product of elliptic curves, each of the form $E_i \times k'$ for some i. Reversing now the role of A and B, over k', we see that the simple factors of A and B coincide (maybe over some further extension).

It remains to prove the claim. If λ is itself a Frobenius eigenvalue for an elliptic curve over k, this is simply a re-interpretation of [Sp, Prop.]. We will show that the proof of (loc. cit.) can be extended.

First, if all λ_i are supersingular, the result follows immediately. So, changing indices, we can assume λ_{2m} is ordinary. Let $K = \mathbf{Q}((\lambda_i)_{2\leqslant i\leqslant 2m})$; it is a composite of quadratic fields, hence Galois over $\mathbf{Q}$. Let

$$(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_s)^t \tag{26}$$

be the factorization of the principal ideal $(p) \subset \mathcal{O}_K$. Since p is decomposed in the various quadratic fields, the residual degree of each $\mathfrak{p}_i$ is $= 1$. Also, rearranging the prime ideals, we can assume that

$$(\lambda_{2m}) = (\mathfrak{p}_1 \cdots \mathfrak{p}_{s/2})^{rt}, \text{ where } r = [k : \mathbf{Z}/p\mathbf{Z}] \tag{27}$$

(since in $\mathbf{Q}(\lambda_{2m})$ we have $(\lambda_{2m}) = \mathfrak{q}^r$ with $(p) = \mathfrak{q}\bar{\mathfrak{q}}$, because for an ordinary elliptic curve, the Frobenius eigenvalues are coprime with p).

Let $\lambda_1 = \lambda$ and

$$\mathfrak{g}_i = \gcd((\lambda_{2m}), (\lambda_i)) \subset \mathcal{O}_K, \text{ for } 1 \leqslant i \leqslant 2m.$$

Using (26) and (27) in (25), by unicity of factorization we have

$$\prod_{1\leqslant i\leqslant 2m} \mathfrak{g}_i = (\lambda_{2m})^m.$$

By [Sp, Lemma 3], we have

$$N^K_{\mathbf{Q}} \mathfrak{g}_i \geqslant (N^K_{\mathbf{Q}} \lambda_{2m})^{1/2} = q^{[K:\mathbf{Q}]/4}$$

for $2 \leqslant i \leqslant 2m - 1$, *unless* $(\lambda_i\lambda_{2m}) = q\mathcal{O}_K$. But in this case $\lambda_i\lambda_{2m} = \xi q$ for some root of unity ξ, which is impossible as m was chosen to be minimal such that a relation (25) holds.

Therefore

$$\begin{aligned} q^{m[K:\mathbf{Q}]/2} = N^K_{\mathbf{Q}}(\lambda^m_{2m}) &= (N^K_{\mathbf{Q}} \mathfrak{g}_1) q^{[K:\mathbf{Q}]/2} \prod_{2\leqslant i\leqslant 2m-1} N^K_{\mathbf{Q}} \mathfrak{g}_i \\ &\geqslant (N^K_{\mathbf{Q}} \mathfrak{g}_1) q^{[K:\mathbf{Q}](1/2+(2m-2)/4)} = (N^K_{\mathbf{Q}} \mathfrak{g}_1) q^{m[K:\mathbf{Q}]/2}. \end{aligned}$$

It follows that $N^K_{\mathbf{Q}} \mathfrak{g}_1 = 1$, i.e. (λ) is coprime with (λ_{2m}). However from (27), the only q-Weil number with this property is

$$(\mathfrak{p}_{s/2+1} \cdots \mathfrak{p}_s)^{rt} = (\bar{\lambda}_{2m}).$$

Hence $(\lambda\lambda_{2m}) = q\mathcal{O}_K$; the claim is proved. □

Example 8.5. The following example shows that the extension k'/k in (3) of Theorem 3.4 can be non-trivial. Let k be a finite field of characteristic $\neq 2$, and let

$$\begin{aligned} A &= E_1 \times E_2 \times E_1^t \\ B &= E_1^t \times E_2^t \times E_2, \end{aligned}$$

where E_1 and E_2 are ordinary elliptic curves over k, non-isogenous over $\bar{k}$, and E_i^t is the quadratic twist of E_i. (The Frobenius eigenvalues of E_i^t are $-\pi_i$, $-\bar{\pi}_i$).

Claim.

(1) The k-simple factors of A and B do not coincide.

(2) A and B are isokummerian.

Proof. (1) This is obvious since E_i^t is not k-isogenous to E_i in odd characteristic.

(2) It suffices to show that $\Phi_A = \Phi_B$; with obvious notation we have

$$\begin{aligned} \Phi_A &= <\pi_1, \bar{\pi}_1, \pi_2, \bar{\pi}_2, -\pi_1, -\bar{\pi}_1> \\ \Phi_B &= <-\pi_1, -\bar{\pi}_1, -\pi_2, -\bar{\pi}_2, \pi_2, \bar{\pi}_2>. \end{aligned}$$

Writing the necessary relations as in (24), we have

$$q^2 = \pi_1 \cdot (-\bar{\pi}_1) \cdot \pi_2 \cdot (-\bar{\pi}_2)$$

so $\Phi_A \subset \Phi_B$, and

$$q^2 = (-\bar{\pi}_2) \cdot \pi_2 \cdot \pi_1 \cdot (-\bar{\pi}_1)$$

so $\Phi_B \subset \Phi_A$. □

Note that this example lifts to characteristic zero by Lemma 8.1, if we twist the elliptic curves E_1 and E_2 by the *same* quadratic character χ so that at a given $\mathfrak{p}$ the reduced varieties are either

$$\mathcal{A}_{\mathfrak{p}} = \mathcal{E}_{1,\mathfrak{p}} \times \mathcal{E}_{2,\mathfrak{p}} \times \mathcal{E}_{1,\mathfrak{p}} \text{ and } \mathcal{B}_{\mathfrak{p}} = \mathcal{E}_{1,\mathfrak{p}} \times \mathcal{E}_{2,\mathfrak{p}} \times \mathcal{E}_{1,\mathfrak{p}}$$

if $\chi(\mathfrak{p}) = 1$, or

$$\mathcal{A}_{\mathfrak{p}} = \mathcal{E}_{1,\mathfrak{p}} \times \mathcal{E}_{2,\mathfrak{p}} \times \mathcal{E}_{1,\mathfrak{p}}^t \text{ and } \mathcal{B}_{\mathfrak{p}} = \mathcal{E}_{1,\mathfrak{p}}^t \times \mathcal{E}_{2,\mathfrak{p}}^t \times \mathcal{E}_{2,\mathfrak{p}}$$

if $\chi(\mathfrak{p}) = -1$ (in this case, there is an easy additional verification to make if one of the curves has supersingular reduction).

If we twist E_1 and E_2 by different characters, on the other hand, there will be a positive density of primes $\mathfrak{p}$ at which

$$\mathcal{A}_{\mathfrak{p}} = \mathcal{E}_{1,\mathfrak{p}} \times \mathcal{E}_{2,\mathfrak{p}} \times \mathcal{E}_{1,\mathfrak{p}} \text{ and } \mathcal{B}_{\mathfrak{p}} = \mathcal{E}_{1,\mathfrak{p}} \times \mathcal{E}_{2,\mathfrak{p}}^t \times \mathcal{E}_{2,\mathfrak{p}}$$

which are not isokummerian when E_2 has ordinary reduction.

Proof of (6) of Theorem 3.4. We now present the example of Serre mentioned in Part 6. of Theorem 3.4. Let p be a prime number, $K_0/\mathbf{Q}$ a real quadratic field in which p decomposes, $a \in K_0$ an integer of K_0, coprime with p, with conjugate $\bar{a} \neq a$, such that

$$a^2 - 4p < 0,\ \bar{a}^2 - 4p < 0 \text{ and } (a^2 - 4p)(\bar{a}^2 - 4p) \text{ is not a square in } K_0.$$

Let further α, β (resp. $\tilde{\alpha}$, $\tilde{\beta}$) be the roots of the equation

$$X^2 - aX + p = 0 \text{ (resp. } X^2 - \bar{a}X + p = 0).$$

The algebraic integers $(\alpha, \beta, \tilde{\alpha}, \tilde{\beta})$ are Galois-conjugates over $\mathbf{Q}$ with Galois group the dihedral group D_4, and they are p-Weil numbers, so there exists an abelian variety $A_0/\mathbf{F}_p$ with Frobenius eigenvalues $(\alpha, \beta, \tilde{\alpha}, \tilde{\beta})$.

Let $\pi = \alpha^3\tilde{\alpha}^2$ and $\tau = \alpha^4\tilde{\alpha}$. Those are q-Weil numbers, with $q = p^5$. We claim they correspond to isokummerian abelian varieties which are non-isogenous over $\bar{\mathbf{F}}_q$. The second point is clear as $\pi/\tau = \tilde{\alpha}/\alpha$ is not a root of unity.

As to showing $M(\pi) \simeq_\kappa M(\tau)$, it suffices to show that $\tau \in \Phi_{M(\pi)}$ and conversely. However we have

$$\tau = \pi^2\varpi^{-1} \text{ with } \varpi = \alpha^2\tilde{\alpha}^3$$
$$\pi = \tau^6\vartheta_1\vartheta_2^{-4}\vartheta_3^{-3}$$

with

$$\begin{cases} \vartheta_1 = \beta^4\tilde{\alpha} \\ \vartheta_2 = \alpha^4\tilde{\beta} \\ \vartheta_3 = \tilde{\alpha}^4\alpha. \end{cases}$$

Since ϖ is a conjugate of π and ϑ_i, $i = 1, 2, 3$ are conjugates of τ, the result follows. More precisely, one shows that $\Phi_{A_0} \simeq \mathbf{Z}^3$ with generators α, $\tilde{\alpha}$ and p, and that $\Phi_{M(\pi)} = \Phi_{M(\tau)} \subset \Phi_{A_0}$ is then identified with the lattice

$$\{(i, j, k) \in \mathbf{Z}^3 \mid i + j + 2k \equiv 0 \pmod 5\}$$

of $\mathbf{Z}^3$.

The abelian varieties $M(\pi)$ and $M(\tau)$, by the results of Honda-Tate, are simple of dimension 20 and have endomorphism rings which are orders in a division algebra of dimension 25 over $K = \mathbf{Q}(\alpha, \beta, \tilde{\alpha}, \tilde{\beta})$ (as one sees by checking there is a place v in K above p for which $v(\alpha) = 1$, $v(\tilde{\alpha}) = 0$, so $v(\pi)/v(q) = 3/5$, $v(\tau)/v(q) = 4/5$).

As a completely concrete instance, for $p = 5$, one can take $K_0 = \mathbf{Q}(\sqrt{11})$, $a = 1 + \sqrt{11}$. □

This concludes the proof of Theorem 3.4. One can use Lemma 8.1 and the case of products of elliptic curves over finite fields to deduce some results over number fields, but the possibility of needing field extensions requires some care. For instance, it is easy to show that if k is a number field, A and B are both products of non-CM elliptic curves, then $A \simeq_{\kappa} B$ implies that over a finite extension k'/k, the simple factors of A and B coincide. We skip the fairly easy proof (one needs to show that for a set of density 1 of primes, the reductions of the factors of A and B remain pairwise non-isogenous, which follows e.g. from [Se-2, Lemme 7] and ℓ-adic arguments as in [Se-4, IV-15].)

Remark 8.6. For the case of elliptic curves over a number field, one can give a very quick alternative proof of (4) of Theorem 3.4, at least of the slightly weaker statement that the equality of division fields of elliptic curves implies isogeny over a finite extension of k: Serre [Se-2, Lemme 7] has shown that for any prime number ℓ, the image of Galois acting on $T_\ell E_1 \times T_\ell E_2$ is open in the subgroup

$$H_\ell = \{(g, h) \mid \det(g) = \det(h)\} \subset GL(4, \mathbf{Z}_\ell). \tag{28}$$

Fixing a prime ℓ, if E_1 and E_2 are not isogenous over $\bar{k}$ and without CM, then

$$[k((E_1 \times E_2)[\ell^m]) : k] > |GL(2, \mathbf{Z}/\ell^m\mathbf{Z})| \geqslant [k(E_i[\ell^m])/k],$$

so even the weaker assumption $k(E_1[\ell^m]) = k(E_2[\ell^m])$ for $m \geqslant 1$ implies that E_1 and E_2 are isogenous over $\bar{k}$. A very similar argument holds for CM curves, and presumably the properties of the Galois groups of division fields of abelian varieties should be such that the same reasoning applies in the general case (see the conjectures stated in [Se-3]). However such arguments do not apply to finite fields (if A/k is an abelian variety over a finite field of characteristic p, we see from Lemma 5.4 that $k(A[\ell^\infty]) = \bar{k}$ for any $\ell \neq p$).

On the other hand, our reasoning requires the consideration of more values of n and does not seem to extend to restricting to $n = \ell^m$. The same remark applies to our discussion of Proposition 3.6. See also [FJ] for stronger statements along those lines for elliptic curves.

Remark 8.7. Another related result of Serre is the local isogeny theorem discussed in [La1, p. 113]: if E_1 and E_2 are elliptic curves over a finite extension $k/\mathbf{Q}_p$, with non-integral j-invariants, and if

$$k(E_1[p^\infty]) = k(E_2[p^\infty]),$$

then E_1 and E_2 are isogenous. Lang's proof is also based on Kummer theory, for the multiplicative group, and the theory of the Tate curve.

9. Conclusion

Our work leaves open a number of paths for further investigation, with various questions arising, some of which are undoubtedly of interest. We list a few here:

- One can define the subgroup $\ll a_1, \ldots, a_n \gg$ locally generated by a *family* of elements $a_i \in G(k)$, instead of a single one. Its relation to $<a_1, \ldots, a_n>$ then must be determined. For the multiplicative group, Lemma 7.2 actually shows that $\ll a_1, \ldots, a_n \gg = <a_1, \ldots, a_n>$, and for an abelian variety A/k over a number field, one sees from Proposition 6.1 that at least if $\mathrm{End}_k(A) = \mathbf{Z}$, one has

$$\ll a_1, \ldots, a_n \gg \otimes \mathbf{Q} = <a_1, \ldots, a_n> \otimes \mathbf{Q}.$$

- Still concerning the local-global issues of Problem 1.1, we may interpret it slightly differently in terms of group actions: the additive group $\mathbf{Z}$ acts on $G(k)$ by $n \cdot a = a^n$. Taking a more general action of a group (abstract or algebraic) H on a variety X, the question becomes that of local-global principles for the statement "b is in the H-orbit of a", when this makes sense.

- Even when b is not in the subgroup generated by a, one may ask for the density, if it exists, of prime ideals $\mathfrak{p}$ such that $b_{\mathfrak{p}}$ *is* in the subgroup generated by $a_{\mathfrak{p}}$. For $\mathbf{G}_m/\mathbf{Q}$, this amounts to the two-variable Artin conjecture discussed by Moree and Stevenhagen [MS]. Gupta, Murty and others have worked on analogues of the Artin conjecture for elliptic curves.
- It seems natural to expect that further progress should come from the input of some aspects of transcendental number theory: compare [CL] and the bound (4) proved by transcendental methods.

Appendix: subgroups of algebraic groups defined by local conditions

Let G/k be an algebraic group of finite type over a number field. Given $a \in G(k)$ one can define a number of subsets in $G(k)$ based on local conditions on the reduction of a modulo (almost all) primes.

(1) The subset $O(a)$ is the set of all $b \in G(k)$ such that for almost all $\mathfrak{p}$, the order of $b_{\mathfrak{p}}$ in $G_{\mathfrak{p}}$ divides that of $a_{\mathfrak{p}}$.
(2) The subset $E(a)$ is the set of all $b \in G(k)$ such that for almost all $\mathfrak{p}$, there exists a group homomorphism $f_{\mathfrak{p}} : G_{\mathfrak{p}} \rightarrow G_{\mathfrak{p}}$ such that $b_{\mathfrak{p}} = f_{\mathfrak{p}}(a_{\mathfrak{p}})$.
(3) The subgroup $\ll a \gg$ is as defined in Section 3, the subgroup locally generated by a (Definition 3).
(4) The subgroup $<a>$ is the subgroup generated by a in $G(k)$.

The "support problem" of [CS] and [KP] can be stated as asking whether $O(a) = <a>$ for certain commutative groups, the multiplicative group and some abelian varieties, essentially. However, no formal definition of $O(a)$ is made. In the present paper, the subgroup $\ll a \gg$ is defined. The subset $E(a)$ is implicitly mentioned in both [KP] and in this paper (see Lemma 5.1). In [KP], the abstract morphism $\phi : A(k) \rightarrow A(k)$ that can be reduced for almost all $\mathfrak{p}$ is studied, in effect, through the fact that $\phi(a) \in E(a)$ for $a \in A(k)$.

In this appendix, we just make a few remarks on relations between those various locally defined subsets. First there are obvious inclusions

$$<a> \subset \ll a \gg \subset O(a) \text{ and } E(a) \subset O(a), \tag{29}$$

and if G is commutative, then $\ll a \gg \subset E(a)$.

For the multiplicative group, Gauss's result that "there are primitive roots", i.e. that the reduced groups $\mathbf{F}_{\mathfrak{p}}^{\times}$ are cyclic, shows that $\ll a \gg = E(a) = O(a)$, and one can show, as mentioned above, that $O(a) = <a>$, so all those sets coincide.

We have seen (mostly in Section 4) that the subgroup $\ll a \gg$ satisfies a number of simple formal properties.

(1) $\ll a \gg$ is an abelian group.
(2) $\ll a \gg$ doesn't depend on the choice of k, i.e. if K/k is a field extension then $\ll a \gg$ is the same whether one sees $a \in G(k)$ as defined over k or over K.
(3) $\ll a \gg$ doesn't depend on the choice of G, i.e. if $G \subset H$ is an injection then $\ll a \gg$ is the same whether one considers $a \in G(k)$ as point on G or on H.
(4) If $f : G \rightarrow H$ is a morphism, then f induces $f_a : \ll a \gg \rightarrow \ll f(a) \gg$ for any $a \in G(k)$ (i.e. if $b \in \ll a \gg$, then $f(b) \in \ll f(a) \gg$).
(5) In particular, if $(b_1, b_2) \in \ll (a_1, a_2) \gg \subset (G_1 \times G_2)(k)$, then $b_i \in \ll a_i \gg$.

All of these properties fail for $E(a)$ or $O(a)$ in general.

(1) If G is commutative, it is clear that $O(a)$ and $E(a)$ are subgroups of $G(k)$, but there is no reason for this to hold if G is not abelian. For instance consider $G = GL(3)$ and a, b, c the permutation matrices corresponding to the transpositions (1 2), (1 3) and (2 3) respectively. They reduce modulo $\mathfrak{p}$ to "the same" matrices, and there exist (inner) endomorphisms of $G_{\mathfrak{p}}$ bringing any of these to any other, so $b \in E(a)$, $c \in E(a)$ for instance. However bc corresponds to a 3-cycle, which has order 3, so $bc \notin O(a)$. Note however that $E(a)$ and $O(a)$ are always

pointed sets: $1 \in E(a)$, and $O(a)$ is symmetric ($b \in O(a)$ implies $b^{-1} \in O(a)$). It is not clear whether $E(a)$ is symmetric or not.

(2) To show that $E(a)$ or $O(a)$ can increase by field extensions, we compute them for the additive group.

Lemma 9.1. *Let $G = \mathbf{G}_a/k$ be the additive group. For any $a \in G(k)$ we have $E(a) = O(a) = ak$, i.e. $E(0) = O(0) = 0$ and $E(a) = O(a) = k$ if $a \neq 0$.*

By comparison, we have $\ll a \gg = \mathbf{Q} \cdot a$ for the additive group (cf. Proposition 3.2).

Proof. For $a = 0$ the answer is obvious, and it suffices to show that $E(a) = k$ for $a \neq 0$ for the second. But for any $\mathfrak{p}$ not dividing a, if p denotes the characteristic of the finite field $\mathbf{F}_{\mathfrak{p}}$, the reduction of a modulo $\mathfrak{p}$ is a non-zero element in the finite dimensional $\mathbf{F}_p$-vector space $\mathbf{F}_{\mathfrak{p}}$, hence there exists $g \in \mathrm{End}(\mathbf{F}_{\mathfrak{p}})$ bringing $a_{\mathfrak{p}}$ to any other element of $\mathbf{F}_{\mathfrak{p}}$. So for any $b \in k$, we have $b \in E(a)$. □

In particular, the answer does depend on the field k.

(3) To show that $E(a)$ can increase by changing the group, take $H = G \times G$ with the inclusion of G being $g \mapsto (g, 1)$. Then clearly $(1, a) \in E((a, 1)) = E(a)$ but $(1, a) \notin G(k)$ if $a \neq 1$.

(4) & (5) To show that $E(a)$ and $O(a)$ are not "functorial", take for f a projection map (i.e. the situation of Point (5))

$$f \,:\, G_1 \times G_2 \to G_1$$

then $(b_1, b_2) \in E(a)$ or $O(a)$ has no reason to imply $b_1 \in E(a_1)$ or $O(a_1)$. For instance, take $G_1 = G_2 = G$ and $(a, b) \in G \times G$ with $b \notin E(a)$ (resp. $O(a)$), then $(b, a) \in E((a, b))$ (resp. $(b, a) \in O((a, b))$), but $b = f((b, a)) \notin E(f(a, b)) = E(a)$.

All inclusions (29) can be strict, and one can have $\ll a \gg \not\subset E(a)$. We have shown examples already where $<a> \neq \ll a \gg$ and examples where $\ll a \gg \neq E(a)$.

A simple example where $E(a) \neq O(a)$ is obtained by taking $G = GL(4)$ and a a permutation matrix corresponding to $(1\ 2)(3\ 4)$. Then the permutation matrices corresponding to either transposition $(1\ 2)$ or $(3\ 4)$ are in $O(a)$, but not in $E(a)$. It is not so obvious to find examples in a commutative setting where $E(a) \neq O(a)$: this cannot occur for tori, for instance, or for elliptic curves, nor for abelian varieties which satisfy $O(a) = <a>$. However Larsen [Lar, Pr. 2] gives examples of abelian varieties and points a where $O(a) \neq <a>$, and they satisfy $E(a) \neq O(a)$ at least in some cases: let $A = E \times E$ where $E/\mathbf{Q}$ is an elliptic curve without CM, with rank $\geqslant 1$ and rational 2-torsion, and take

$$a = (x, x + s), \text{ and } b = (2x, 2x + t)$$

where $x \in E(\mathbf{Q})$ is of infinite order while s and t are distinct non-trivial 2-rational points. Larsen shows $b \in O(a)$ but b is not the image of a by an endomorphism of A. It is clear that $b \notin \ll a \gg$. Now assume for instance that $s = 2u$ where u is a rational point of order 4 and $x = 2y$ with $y \in E(\mathbf{Q})$. Then $b \notin E(a)$, since the latter would imply that $t \in 2E(\mathbf{Q})$ – this would be locally true, and then one can apply [Wo] or [DZ] – which is not possible. (Our conditions can be satisfied, e.g. take $E \,:\, y^2 + xy - 68y = x^3 - 68x^2$ with $t = (4, 32)$, $s = (68, 0) = 2(0, 0)$, $x = 2(-4, 48)$).

Remark 9.2. Because of this example, Larsen's Theorem 1 (if $b \in O(a)$, then $kb = f(a)$ for some $k \geqslant 1$ and $f \in \mathrm{End}(A)$) is the best possible solution for the support problem for general abelian varieties over number fields. The statement $<a> = \ll a \gg$, on the other hand, remains plausible.

Finally, a case where $\ll a \gg \not\subset E(a)$ is as follows: let $G = SL(2)$ and

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } b = a^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

then $b \in \ll a \gg$ of course, but using the description of group homomorphisms $SL(2, \mathbf{F}_p) \to SL(2, \mathbf{F}_p)$, one sees that b_p is not an image of a_p for $p \equiv 3 \,(\mathrm{mod}\, 4)$, as their eigenvalues are defined over different fields, which shows that $b \notin E(a)$.

Finally, it is clear that the definition of $\ll a \gg$ (like that of $<a>$) can be generalized to define the subgroup locally generated by an arbitrary family (a_i) of rational points $a_i \in G(k)$. Moreover, with obvious (and ugly!) notation, one then has $\ll \ll (a_i) \gg \gg = \ll (a_i) \gg$, so we have a kind of closure operator. Problems of local-global nature arise as before in this case. The only result known to the author is Weston's theorem [We] (a special case of which has been quoted above): if A/k is an abelian variety over a number field with $\mathrm{End}_k(A)$ commutative, and $\Sigma \subset A(k)$ is any set of rational points, then

$$\ll \Sigma \gg \subset <\Sigma> + A(k)_{tors}.$$

It is not so clear how to generalize the definition of $E(a)$ and especially $O(a)$ (for the former, one can ask that there exist a group homomorphism $f_{\mathfrak{p}} : (G_{\mathfrak{p}})^I \to G_{\mathfrak{p}}$ with $b_{\mathfrak{p}} = f_{\mathfrak{p}}(a_{i,\mathfrak{p}})$).

These various facts tend to indicate that $\ll a \gg$ might be the more useful notion in general (the others being more challenging...), especially in a non-commutative situation (see Proposition 6.11).

Remark 9.3. In addition, one may make similar definitions for slightly different situations where one has an arithmetic object over $\mathbf{Q}$ that admits "reduction maps" to local objects.[8] Examples are various cohomology groups with the restriction maps. Of course, one is then not very far from Selmer groups and the like...

References

[Ba] Bashmakov, M.: *The cohomology of abelian varieties over a number field*, Russian Math. Surveys 27 (1977), 25–70.

[BGK] Banaszak, G., Gajda, W. and Kraso, P.: *A support problem for the intermediate jacobians of ℓ-adic representations*, preprint 2002 (`http://www.math.uiuc.edu/Algebraic-Number-Theory/`).

[Bo] Borel, A.: *Linear Algebraic Groups*, Second edition, GTM 126, Springer-Verlag, 1991.

[CH] Cheon, J. and Hahn, S.: *The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve*, Acta Arith. 88 (1999) 219–222.

[CL] Chambert-Loir, A.: *Théorèmes d'algébricité en géométrie diophantienne*, Séminaire Bourbaki, exp. 886, 2001.

[CS] Corrales-Rodrigáñez, C. and Schoof, R.: *The support problem and its elliptic analogue*, J. Number Theory 64 (1997), no. 2, 276–290.

[DZ] Dvornicich, R. and Zannier, U.: *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. math. France 129 (2001), 317–338.

[Fa-1] Faltings, G.: *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[Fa-2] Faltings, G.: *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry, Perspect. Math. 15, Academic Press 1994, 175–182.

[FJ] Frey, G. and Jarden, M.: *Horizontal Isogeny Theorems*, Forum Math. 14 (2002), 931–952.

[Hi] Hindry, M.: *Autour d'une conjecture de Serge Lang*, Invent. math. 94 (1988), 575–603.

[KP] Khare, C. and Prasad, D.: *Reduction of abstract homomorphisms of lattices mod p and rigidity*, preprint 2002 (`http://www.math.uiuc.edu/Algebraic-Number-Theory/`).

[La1] Lang, S.: *Elliptic Curves Diophantine Analysis*, Grund. der math. Wiss. 231, Springer-Verlag 1978.

[La2] Lang, S.: *Algebra*, 2nd edition, Addison-Wesley, 1984.

[Lar] Larsen, M.: *The Support Problem for Abelian Varieties*, preprint, 2002 (`ArXiv:math.NT/0211118v1`).

[LZ] Lenstra, H. and Zarhin, Y.: *The Tate conjecture for almost ordinary abelian varieties over finite fields*, Advances in number theory (Kingston 1991), Oxford Univ. Press 1993, 179–194.

[Mi-1] Milne, J.: *Étale cohomology*, Princeton Univ. Press 1980.

[Mi-2] Milne, J.: *Abelian varieties*, in Arithmetic Geometry, 103–150, Cornell and Silverman, eds., Springer-Verlag 1986.

[MS] Moree, P. and Stevenhagen, P.: *A two-variable Artin conjecture*, J. Number Theory 85 (2000), 291–304.

[Mu] Mumford, D.: *Abelian varieties*, Tata Institute of Fundamental Research, Oxford Univ. Press 1970.

[Ri] Ribet, K.: *Kummer theory on extensions of abelian varieties by tori*, Duke Math. Journal 46 (1979), 745–761.

[8] Local may refer to reduction modulo p, or to points with p-adic coordinates instead.

[RA] Rudnick, Z. and Ailon, N.: *Torsion Points on Curves and Common Divisors of $a^k - 1$ and $b^k - 1$*, preprint, 2002 (`ArXiv:math.NT/0202102`).

[Sc1] Schinzel, A.: *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine angew. Math. 268/269 (1974), 27–33.

[Sc2] Schinzel A.: *On the congruence $a^x \equiv b(modp)$*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astron. Phys. 8 (1960), 307–309.

[Se-1] Serre, J-P.: *Corps locaux*, 3ème ed., Hermann 1968.

[Se-2] Serre, J-P.: *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259–331.

[Se-3] Serre, J-P.: *Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ-adiques*, in Motives (Seattle 1991), 377–400, Proc. Sympos. Pure Math. 55, Part 1, AMS 1994.

[Se-4] Serre, J-P.: *Abelian ℓ-adic representations and elliptic curves*, 1st Edition, Benjamin 1968; 3d Edition, Research Notes in Mathematics, 7. A K Peters, 1998.

[Se-5] Serre, J-P.: letter to K. Ribet, in Oeuvres, n. 133, vol. IV, 1–17, Springer-Verlag, 2000.

[Se-6] Serre, J-P.: Oeuvres, n. 133–138, vol. IV, Springer-Verlag, 2000.

[Si-1] Silverman, J.: *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, 1986.

[Si-2] Silverman, J.: *Wieferich's criterion and the abc-Conjecture*, J. of Number Theory 30 (1988), 226–237.

[So] Soulé, C.: *Groupes de Chow et K-théorie de variétés sur un corps fini*, Math. Ann. 268 (1984), 317–345.

[Sp] Spieß, M.: *Proof of the Tate Conjecture for products of elliptic curves over finite fields*, Math. Ann. 314 (1999), 285–290.

[Ta-1] Tate, J.: *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966) 134–144.

[Ta-2] Tate, J.: *Classes d'isogénies des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki, exp. 352, 1968.

[Ta-3] Tate, J.: *Conjectures for algebraic cycles in ℓ-adic cohomology*, in Motives (Seattle 1991), 75–83, Proc. Sympos. Pure Math. 55, Part 1, AMS 1994.

[We] Weston, T.: *Kummer theory and reductions of Mordell-Weil groups*, preprint 2002 (`ArXiv:math.NT/0208118v1`).

[Wh] Whittmann, C.: *Group structure of elliptic curves over finite fields*, J. of Number Theory 88 (2001), 335-344.

[Wo] Wong, S.: *Power residues on Abelian varieties*, Manuscripta Math. 102 (2000), 129–137.

[ZBC] Zannier, U., Bugeaud, Y. and Corvoja, P.: *An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$*, preprint (2001).

Université Bordeaux I - A2X, 351, cours de la Libération, 33405 Talence Cedex, France
E-mail address: `emmanuel.kowalski@math.u-bordeaux1.fr`