REDUCTIONS OF POINTS ON ALGEBRAIC GROUPS

DAVIDE LOMBARDO AND ANTONELLA PERUCCA

ABSTRACT. Let A be the product of an abelian variety and a torus defined over a number field K. Fix some prime number ℓ. If $\alpha \in A(K)$ is a point of infinite order, we consider the set of primes $\mathfrak{p}$ of K such that the reduction $(\alpha \bmod \mathfrak{p})$ is well-defined and has order coprime to ℓ. This set admits a natural density. By refining the method of R. Jones and J. Rouse (2010), we can express the density as an ℓ-adic integral without requiring any assumption. We also prove that the density is always a rational number whose denominator (up to powers of ℓ) is uniformly bounded in a very strong sense. For elliptic curves, we describe a strategy for computing the density which covers every possible case.

1. INTRODUCTION

1.1. **Reductions of a point having order coprime to ℓ.** Let A be a connected commutative algebraic group defined over a number field K, and fix some prime number ℓ. Let $\alpha \in A(K)$ be a point of infinite order and consider the primes $\mathfrak{p}$ of K for which the reduction of α modulo $\mathfrak{p}$ is well-defined and has order coprime to ℓ. The aim of this paper is understanding the natural density of this set (provided it exists):

$$\mathrm{Dens}_\ell(\alpha) := \mathrm{Dens}\{\, \mathfrak{p} \,:\, \ell \nmid \mathrm{ord}(\alpha \bmod \mathfrak{p})\}\,.$$

1.2. **History of the problem.** In the sixties, Hasse [11, 12] considered the case of A being the multiplicative group over the rationals and gave parametric formulas for $\mathrm{Dens}_\ell(\alpha)$. For a survey of related questions for the rational numbers, see [19] by Moree. The second author (partly joint with Debry) extended the method of Hasse to solve the case where A/K is a 1-dimensional torus over a number field [22, 6, 23]. In [25], Pink gave a motivic interpretation of the problem for abelian varieties: considering the tree of ℓ^∞ division points over α gives a Tate module $T_\ell(A, \alpha)$ which is an extension of the Tate module $T_\ell(A)$ by $\mathbb{Z}_\ell$ (and is a particular case of the Tate module of 1-motives first described by Deligne in [7]).

In [13], Jones and Rouse considered the Galois action on the tree of ℓ^∞ division points over α, which encodes the Kummer representation for α and the ℓ-adic representation attached to A. In [13, Theorem 3.8] they prove – for any connected commutative algebraic group – that if the image of the Kummer representation is as large as possible we have

$$\mathrm{Dens}_\ell(\alpha) = \int_{\mathcal{G}} \ell^{-v_\ell(\det(x-I))}\, d\mu_{\mathcal{G}}(x)$$

2010 *Mathematics Subject Classification.* Primary: 11F80; Secondary: 14L10; 11G05; 11G10.

Key words and phrases. reduction, Kummer theory, algebraic group, semiabelian variety, elliptic curve, Galois representations.

where $\mathcal{G}$ is the image of the ℓ-adic representation, identified with a subgroup of a suitable general linear group $\mathrm{GL}_b(\mathbb{Z}_\ell)$, and $d\mu_{\mathcal{G}}(x)$ is the normalized Haar measure on $\mathcal{G}$. They have also given criteria for their assumptions to be satisfied, and have determined the value of $\mathrm{Dens}_\ell(\alpha)$ for 1-dimensional tori and elliptic curves whenever the images of both the Kummer representation and the ℓ-adic representation are as large as possible (under a small assumption for CM curves [13, §5.2]). The case when A is an elliptic curve over the rationals and $\ell = 2$ has also been studied in detail, see [27, Remark 1.10].

1.3. **The general formula.** We suppose that the torsion/Kummer extensions $K(A[\ell^n], \ell^{-n}\alpha)$ grow maximally for every sufficiently large n (cf. Definition 8). For the product of an abelian variety and a torus we may assume this condition without loss of generality (cf. Remark 9).

In this situation, the natural density $\mathrm{Dens}_\ell(\alpha)$ exists by the argument of [13, Theorem 3.2] and the remark following it. By refining the method of Jones and Rouse we can generalize [13, Theorem 3.8] (which corresponds here to the case $\mathrm{c}_{\text{Kummer}} = 1$ and $\mathrm{w} \equiv 1$):

Theorem 1. *Let A/K be a connected commutative algebraic group defined over a number field, $\alpha \in A(K)$ a point of infinite order and ℓ a prime number as in Definition 8. If $\mathcal{G}$ is the image of the ℓ-adic representation, we have*

$$\mathrm{Dens}_\ell(\alpha) = \mathrm{c}_{\textit{Kummer}} \cdot \int_{\mathcal{G}} \ell^{-v_\ell(\det(x-I))} \cdot \mathrm{w}(x)\ d\mu_{\mathcal{G}}(x) \tag{1}$$

where the constant $\mathrm{c}_{\textit{Kummer}} := \mathrm{c}_{\textit{Kummer}}(A/K, \ell, \alpha)$ is as in Lemma 10 (it measures the failure of maximality for the Kummer extensions) and the function $\mathrm{w} := \mathrm{w}(A/K, \ell, \alpha)$ is as in Lemma 25 ($\mathrm{w}(x)$ is either zero or a power of ℓ with exponent in $\mathbb{Z}_{\leqslant 0}$; this function measures a particular relation between the torsion and the Kummer extensions).

1.4. **Rationality of the density.** For products of abelian varieties and tori, the density is always a rational number (this result is new even for elliptic curves):

Theorem 2. *If $(A/K, \ell, \alpha)$ are as in Definition 8, $\mathrm{Dens}_\ell(\alpha)$ is a rational number.*

In Section 7 we even prove (for all products of abelian varieties and tori) that the denominator of $\mathrm{Dens}_\ell(\alpha)$ can be universally bounded up to a power of ℓ:

Theorem 3. *Fix $g \geqslant 1$. There exists a polynomial $p_g(t) \in \mathbb{Z}[t]$ with the following property: whenever K is a number field and A/K is the product of an abelian variety and a torus with $\dim(A) = g$, then for all prime numbers ℓ and for all $\alpha \in A(K)$ we have*

$$\mathrm{Dens}_\ell(\alpha) \cdot p_g(\ell) \in \mathbb{Z}[1/\ell].$$

Remark 4. *The power of ℓ appearing in the denominator of $\mathrm{Dens}_\ell(\alpha)$ cannot be bounded uniformly even for fixed A, provided that $A(K)$ is infinite (see Remark 30).*

1.5. **The case of elliptic curves.** We have collected in a companion paper [16] general results on $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and all its Cartan subgroups (including the ramified ones): this leads to a very detailed classification of the elements in the image of the ℓ-adic representation attached to any elliptic curve according to the structure of their group of fixed points in $A[\ell^\infty]$. In this classification, a Cartan subgroup is called either *ramified* or *unramified*, and in the latter case it can be either *split* or *nonsplit*. Using these results, we prove in Section 6 the following results:

Theorem 5. *For elliptic curves* $\mathrm{Dens}_\ell(\alpha)$ *can be effectively computed. Furthermore, we have* $\mathrm{Dens}_\ell(\alpha) \cdot (\ell-1)(\ell^2-1)^2(\ell^t-1) \in \mathbb{Z}[1/\ell]$*, where* $t = 4$ *if the elliptic curve has complex multiplication over* $\overline{K}$ *and* $t = 6$ *otherwise.*

Theorem 6. *For elliptic curves, if* $\mathcal{G}$ *is open in* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ *or in the normalizer of an unramified Cartan subgroup, then the* ℓ*-adic valuation of the minimal denominator of* $\mathrm{Dens}_\ell(\alpha)$ *is at most* $(8+t)n_0 + 7$*, where* n_0 *is as in* (5) *and* t *is as in Theorem 5. In the remaining case, namely* $\mathcal{G}$ *open in the normalizer of a ramified Cartan with parameters* $(0, d)$*, there is a bound which depends only on* n_0 *and on* $v_\ell(d)$*.*

These two results, taken together, give a tight control on the height of the rational number $\mathrm{Dens}_\ell(\alpha)$ even over families of elliptic curves. Moreover (see Theorem 35) there are infinitely many non-isogenous curves and points on them which have the same value of $\mathrm{Dens}_\ell(\alpha)$.

1.6. **Further results.** In Section 3.2 we give a cohomological interpretation of the density, and more precisely of [13, Theorem 3.2]:

Theorem 7. *If* $(A/K, \ell, \alpha)$ *are as in Definition 8,* $\mathrm{Dens}_\ell(\alpha)$ *equals the Haar measure in* $\mathrm{Gal}(K(A[\ell^\infty], \ell^{-\infty}\alpha)/K)$ *of the set of automorphisms* σ *such that the Kummer cohomology class of* α *(defined in Section 3.1) is in the kernel of the restriction map*

$$\mathrm{Res}_\sigma : H^1\big(\mathrm{Gal}(K(A[\ell^\infty], \ell^{-\infty}\alpha)/K), T_\ell A\big) \to H^1(\langle\sigma\rangle, T_\ell A)\,,$$

where $\langle\sigma\rangle$ *denotes the procyclic subgroup generated by* σ*.*

The value of $\mathrm{Dens}_\ell(\alpha)$ is indeed only related to the field $K(A[\ell^\infty], \ell^{-\infty}\alpha)$, see Proposition 22. Finally, in Section 5 we show that (when A is the product of an abelian variety and a torus) $\mathrm{Dens}_\ell(\ell^n\alpha)$ converges to 1 as the power ℓ^n tends to infinity (both ℓ and n are allowed to vary), and this uniformly in the choice of $\alpha \in A(K)$.

1.7. **Notation and conventions.** If G is a compact Hausdorff topological group, we denote by μ_{G} (or simply by μ) its normalized Haar measure. By the *normalised counting measure* on a finite set A we mean the uniform probability measure μ_A for which $\mu_A(\{a\}) = \frac{1}{\#A}$ for all $a \in A$. We denote by ℓ a fixed prime number and call v_ℓ the ℓ-adic valuation on $\mathbb{Q}_\ell$ (we set $v_\ell(0) = +\infty$ and $\ell^{-v_\ell(0)} = 0$). We write $\mathrm{Mat}_b(\mathbb{Z}_\ell)$ for the ring of $b \times b$ matrices with coefficients in $\mathbb{Z}_\ell$, and define analogously $\mathrm{Mat}_b(\mathbb{Z}/\ell^n\mathbb{Z})$. We denote by I the identity matrix/endomorphism. The ℓ-adic valuation of a matrix is the minimum of the valuations of its entries. Because of its frequent use, we reserve the notation $\mathcal{G}$ for the image of the ℓ-adic representation. Finally, by a *CM elliptic curve* E over a number field K we shall mean an elliptic curve whose *geometric* endomorphism ring is an order in a quadratic imaginary field.

Acknowledgements. We thank R. Jones, J. Rouse, P. Jossen and A. Sutherland for helpful discussions.

2. Torsion fields and Kummer extensions

2.1. **The torsion, Kummer, and arboreal representations.** We recall from [13] the construction of the arboreal representation attached to A/K and to a point $\alpha \in A(K)$, which describes the natural Galois action on the tree of division points over α.

If A is a connected commutative algebraic group, we define its Tate module $T_\ell A$ as the projective limit of the torsion groups $A[\ell^n]$ (the transition homomorphism $A[\ell^{n+1}] \to A[\ell^n]$ is multiplication by ℓ). The Tate module is a $\mathbb{Z}_\ell$-module isomorphic to $\mathbb{Z}_\ell^b$, where b is the first Betti number of A (for elliptic curves $b = 2$).

The *torsion* (or *ℓ-adic*) *representation* of A is the representation of $\mathrm{Gal}(\overline{K}/K)$ with values in the automorphism group of $T_\ell A$ which is induced by the natural Galois action on the torsion points of A. Choosing a $\mathbb{Z}_\ell$-basis for $T_\ell A$ means fixing an isomorphism of $T_\ell A$ with $\mathbb{Z}_\ell^b$, so the choice of a basis allows us to identify the image of the ℓ-adic representation with a subgroup of $\mathrm{GL}_b(\mathbb{Z}_\ell)$. We also consider the *mod ℓ^n representation*, whose image is a subgroup of $\mathrm{GL}_b(\mathbb{Z}/\ell^n\mathbb{Z})$ and which describes the Galois action on the group $A[\ell^n]$.

The *Kummer representation* depends both on A/K and the point α. For every $n \geqslant 1$ we call $\ell^{-n}(\alpha)$ the set of points in $A(\overline{K})$ whose ℓ^n-th multiple equals α. The fields

$$K_n := K(A[\ell^n]) \qquad \text{and} \qquad K_{\alpha,n} := K_n(\ell^{-n}(\alpha))$$

are then finite Galois extensions of K. We denote the countable union of these fields by K_∞ and K_α respectively. We then define the Kummer map as

$$\begin{array}{ccc} \mathrm{Gal}(K_\alpha/K_\infty) & \to & T_\ell A \\ \sigma & \mapsto & (\sigma(\beta_n) - \beta_n)_{n\geqslant 1} \end{array} \tag{2}$$

where $\{\beta_n\}_{n\geqslant 1}$ is any sequence of points $\beta_n \in A(\overline{K})$ satisfying $\ell\beta_1 = \alpha$ and $\ell\beta_{n+1} = \beta_n$ for all $n \geqslant 1$. The definition does not depend on the choice of the sequence because σ is the identity on K_∞.

The *arboreal representation* encodes both the ℓ-adic representation and the Kummer representation, and is constructed in the following way. There is a natural map

$$\begin{array}{ccc} \mathrm{Gal}(\overline{K}/K) & \to & T_\ell A \rtimes \mathrm{Aut}(T_\ell A) \\ \sigma & \mapsto & (t_\sigma, M_\sigma), \end{array}$$

where M_σ is the image of σ under the ℓ-adic representation and where we define $t_\sigma := (\sigma(\beta_n) - \beta_n)_{n\geqslant 1}$ for some fixed choice of $\{\beta_n\}_{n\geqslant 1}$ as above. By definition, this map is trivial on $\mathrm{Gal}(\overline{K}/K_\alpha)$, hence it induces a well-defined homomorphism

$$\omega : \begin{array}{ccc} \mathrm{Gal}(K_\alpha/K) & \to & T_\ell A \rtimes \mathrm{Aut}(T_\ell A) \\ \sigma & \mapsto & (t_\sigma, M_\sigma) \end{array} \tag{3}$$

which we call the arboreal representation; ω is injective, and identifies $\mathrm{Gal}(K_\alpha/K)$ to a subgroup of $T_\ell A \rtimes \mathrm{Aut}(T_\ell A) \cong \mathbb{Z}_\ell^b \rtimes \mathrm{GL}_b(\mathbb{Z}_\ell)$. With this identification, we shall write

$$\sigma = (t_\sigma, M_\sigma). \tag{4}$$

We employ the same notation for $\sigma \in \mathrm{Gal}(K_{\alpha,n}/K)$, in which case we have $t_\sigma \in A[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^b$ and $M_\sigma \in \mathrm{Aut}\, A[\ell^n] \cong \mathrm{GL}_b(\mathbb{Z}/\ell^n\mathbb{Z})$.

2.2. **Growth conditions for torsion fields and Kummer extensions.** We denote by $\mathcal{G} \subseteq \mathrm{GL}_b(\mathbb{Z}_\ell)$ the image of the ℓ-adic representation and by $\mathcal{G}(n)$ the image of the mod ℓ^n representation, i.e. the image of $\mathcal{G}$ under the natural projection $\mathrm{GL}_b(\mathbb{Z}_\ell) \to \mathrm{GL}_b(\mathbb{Z}/\ell^n\mathbb{Z})$. We write $\dim \mathcal{G}$ for the dimension of the Zariski closure of $\mathcal{G}$ in $\mathrm{GL}_{b,\mathbb{Q}_\ell}$.

If A is an elliptic curve, by work of Serre [28] and by the classical theory of complex multiplication [31] we know the following: if $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$, then $\mathcal{G}$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ ($\dim \mathcal{G} = 4$), and otherwise $\mathcal{G}$ is open in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ ($\dim \mathcal{G} = 2$). See [16] for a classification of all Cartan subgroups and their normalizers.

Definition 8. *We say that $(A/K, \ell)$ satisfy the* eventual maximal growth of the torsion fields *if there exists a positive integer n_0 such that we have*

(C1) $$\#\,\mathcal{G}(n+1)/\#\,\mathcal{G}(n) = \ell^{\dim \mathcal{G}} \qquad \text{for every } n \geqslant n_0\,.$$

We say that $(A/K, \ell, \alpha)$ satisfy the eventual maximal growth of the Kummer extensions *if there exists a positive integer n_0 such that we have:*

(C2i) $$K_{n,\alpha} \text{ and } K_{n'} \text{ are linearly disjoint over } K_n \qquad \text{for every } n' \geqslant n \geqslant n_0$$

(C2ii) $$[K_{n'}(\ell^{-n'}\alpha) : K_{n'}(\ell^{-n}\alpha)] = \ell^{b(n'-n)} \qquad \text{for every } n' \geqslant n \geqslant n_0\,.$$

Equivalently, the conditions (C1), (C2i), and (C2ii) together mean that there exists a positive integer n_0 such that we have

(5) $$[K_{n'}(\ell^{-n'}\alpha) : K_n(\ell^{-n}\alpha)] = (\ell^{b+\dim \mathcal{G}})^{n'-n} \qquad \text{for every } n' \geqslant n \geqslant n_0\,.$$

2.3. **Results on the growth conditions.**

Remark 9. *If A/K is the product of an abelian variety and a torus, then we may always reduce to the situation of Definition 8. Indeed, A satisfies Condition* (C1) *for any prime ℓ; moreover, it also satisfies Conditions* (C2i) *and* (C2ii) *for any $\alpha \in A(K)$ such that $\mathbb{Z}\alpha$ is Zariski-dense in A. These facts follow from Lemma 12 below and [3, Theorem 2]. To reduce to the case where $\mathbb{Z}\alpha$ is Zariski-dense in A, consider the smallest algebraic subgroup A' of A containing α. By [22, Main Theorem], if the number n of connected components of A' is divisible by ℓ, then we have $\mathrm{Dens}_\ell(\alpha) = 0$. Otherwise we may replace α by $[n]\alpha$ and hence work with the connected component of the identity of A' in place of A: in this case we have $\mathrm{Dens}_\ell(\alpha) > 0$ by [22, Main Theorem].*

Lemma 10. *If* (C2i)-(C2ii) *hold, the following integer is independent of n for $n \geqslant n_0$:*

(6) $$\mathrm{c}_{\textit{Kummer}} := \ell^{bn}/\#\,\mathrm{Gal}(K_{\alpha,n}/K_n)\,.$$

Proof. $\#\,\mathrm{Gal}(K_{\alpha,n}/K_n) \cdot \ell^{-b(n-n_0)} = \#\,\mathrm{Gal}(K_n(\ell^{-n_0}\alpha)/K_n) = \#\,\mathrm{Gal}(K_{\alpha,n_0}/K_{n_0})\,.$ □

The following lemma is related to [29, Théorème 9] (but notice that we do not make any smoothness assumption on the reduction of G modulo ℓ):

Lemma 11. *Let* G *be an algebraic subgroup of* $\mathrm{GL}_{b,\mathbb{Q}_\ell}$. *Define* $\overline{\mathrm{G}} := \mathrm{G}(\mathbb{Q}_\ell) \cap \mathrm{GL}_b(\mathbb{Z}_\ell)$ *and write* $\overline{\mathrm{G}}(n)$ *for the reduction modulo ℓ^n of* $\overline{\mathrm{G}}$. *The sequence* $\#\,\overline{\mathrm{G}}(n+1)/\#\,\overline{\mathrm{G}}(n)$ *is non-decreasing for $n \geqslant 2$ and it is eventually equal to* $\ell^{\dim \mathrm{G}}$.

Proof. We have to study the order of $\mathrm{Ker}(n)$, the kernel of the reduction map $\overline{\mathrm{G}}(n+1) \to \overline{\mathrm{G}}(n)$. For every n, the map $M \mapsto \ell^{-n}(M-I)$ gives a group isomorphism between $\mathrm{Ker}(n)$ and some vector subspace $V_n \subseteq \mathrm{Mat}_b(\mathbb{Z}/\ell\mathbb{Z})$. The sequence $\#V_n$ is bounded from above by $\#\mathrm{Mat}_b(\mathbb{Z}/\ell\mathbb{Z})$, and it is non-decreasing: indeed, we now show that $V_n \subseteq V_{n+1}$. If $v \in V_n$, then $I + \ell^n v \in \mathrm{Ker}(n) \subseteq \overline{\mathrm{G}}(n+1)$, so there is some $\tilde{M} := I + \ell^n \tilde{v}$ in $\overline{\mathrm{G}}$ that is congruent to $1 + \ell^n v$ modulo ℓ^{n+1}. We have $v \in V_{n+1}$ because $\mathrm{Ker}(n+1)$ contains $I + \ell^{n+1} v$: indeed, this is the image in $\overline{\mathrm{G}}(n+2)$ of $\tilde{M}^\ell$ (this follows from $\ell^{n+2} \mid \ell^{2n}$). This proves that $\#V_n$ is eventually constant, and since the sequence $\#\overline{\mathrm{G}}(n)\ell^{-n\dim \mathrm{G}}$ converges to some positive number by [20, Theorem 2] we must have $\#V_n = \ell^{\dim \mathrm{G}}$ for all n sufficiently large. □

Lemma 12. *Semiabelian varieties satisfy* (C1) *for any prime ℓ.*

Proof. Let $\mathcal{G}_{\mathrm{Zar}}$ be the Zariski closure of $\mathcal{G}$ in $\mathrm{GL}_{b,\mathbb{Q}_\ell}$ and define $\overline{\mathcal{G}} := \mathcal{G}_{\mathrm{Zar}}(\mathbb{Q}_\ell) \cap \mathrm{GL}_b(\mathbb{Z}_\ell)$. By Proposition 18 we know that $\mathcal{G}$ is open in $\overline{\mathcal{G}}$, so there exists some positive integer n_0 such that for every $n \geqslant n_0$ the matrices of $\overline{\mathcal{G}}$ that reduce to the identity modulo ℓ^n are in $\mathcal{G}$. The statement then follows from Lemma 11, because for every sufficiently large n we have $\ker\left(\mathcal{G}(n+1) \to \mathcal{G}(n)\right) = \ker\left(\overline{\mathcal{G}}(n+1) \to \overline{\mathcal{G}}(n)\right)$. □

The proof of Lemma 11 implies that the following definition is well-posed:

Definition 13. *Let* G *be a subgroup of* $\mathrm{GL}_b(\mathbb{Z}_\ell)$ *that is open (for the ℓ-adic topology) in the $\mathbb{Z}_\ell$-points of its Zariski closure. The image of the map*

$$\begin{array}{ccc} \ker(\mathrm{G}(n+1) \to \mathrm{G}(n)) & \to & \mathrm{Mat}_b(\mathbb{Z}/\ell\mathbb{Z}) \\ M & \mapsto & \ell^{-n}(M-I) \end{array}$$

is independent of n for all sufficiently large n: it is a vector space of the same dimension as the Zariski closure of G*, and we call it the tangent space* $\mathbb{T}$ *of* G*.*

2.4. **Effectivity of Definition 8.** Consider the arboreal representation ω as in (3) and its reduction

$$\omega_n : \mathrm{Gal}(K_\alpha/K) \to A[\ell^n] \rtimes \mathrm{Aut}(A[\ell^n])\,.$$

Theorem 14. *Let $n \geqslant 1$ (resp. $n \geqslant 2$ if $\ell = 2$).*

(i) *If $[K_{n+1} : K_n] = \#\mathbb{T}$ holds, we have $[K_{m+1} : K_m] = \#\mathbb{T}$ for all $m \geqslant n$.*
(ii) *If $[K_{\alpha,n+1} : K_{\alpha,n}] = \#\mathbb{T}\ell^b$ holds, we have $[K_{\alpha,m+1} : K_{\alpha,m}] = \#\mathbb{T}\ell^b$ for all $m \geqslant n$ and the image of ω is the inverse image in $T_\ell A \rtimes \mathrm{Aut}(T_\ell(A))$ of the image of ω_n.*

Proof. (i) Define $H_m := \ker(\mathcal{G}(m+1) \to \mathcal{G}(m))$. We know $\#H_n = \#\mathbb{T}$ and by induction we prove $\#H_m = \#\mathbb{T}$ for $m \geqslant n$. Write the elements of H_m as $I + \ell^m x$, where x varies in a subset of $\mathrm{Mat}(\mathbb{Z}/\ell\mathbb{Z})$ of cardinality $\#\mathbb{T}$. To prove $\#H_{m+1} = \#\mathbb{T}$, we show that $I + \ell^{m+1}x$ is in $\mathcal{G}(m+2)$: this group contains $I + \ell^m x'$, where x' is some lift of x to $\mathrm{Mat}(\mathbb{Z}/\ell^2\mathbb{Z})$, and hence also $(I + \ell^m x')^\ell = I + \ell^{m+1}x$. Notice that here we use $m \geq 2$ if $\ell = 2$: indeed for $m = 1$ we have $(1 + 2x')^2 = 1 + 4x' + 4(x')^2$, which is not congruent to $1 + 4x'$ modulo 8 in general.

(ii) The kernel of the projection $\mathrm{Gal}(K_{\alpha,m+1}/K) \to \mathrm{Gal}(K_{\alpha,m}/K)$ is $\mathrm{Gal}(K_{\alpha,m+1}/K) \cap H'_m$, where we set $H'_m := A[\ell] \rtimes H_m$. From (i) we know that $\#H'_m = \#\mathbb{T}\ell^b$, so it suffices to

prove $H'_m \subseteq \mathrm{Gal}(K_{\alpha,m+1}/K)$. We know this assertion for $m = n$, so we suppose that it holds for some $m \geqslant n$ and prove it for $m+1$. Since H'_{m+1} is generated by $A[\ell] \times \{I\}$ and by $\{0\} \times H_{m+1}$, it suffices to prove that these are contained in $\mathrm{Gal}(K_{\alpha,m+2}/K)$. For $t \in A[\ell]$, we have $(t, I) \in H'_m \subseteq \mathrm{Gal}(K_{\alpha,m+1}/K)$, so there is $(u, M) \in \mathrm{Gal}(K_{\alpha,m+2}/K)$ satisfying $[\ell]u = t$ and $M \equiv I \pmod{\ell^{m+1}}$; we have $(u, M)^\ell = (t, I)$ because more generally $(u, M)^k = ([k]u, M^k)$ holds by induction for $k \geqslant 1$.
Writing again an element of H_{m+1} as $h = I + \ell^{m+1}x$, we know that $(0, I + \ell^m x)$ is in $\{0\} \times H_m \subseteq \mathrm{Gal}(K_{\alpha,m+1}/K)$ so we deduce as above that $\mathrm{Gal}(K_{\alpha,m+2})$ contains (t, h) for some $t \in A[\ell]$ and we conclude because $(0, h) = (-t, I)(t, h)$.

For every $m \geqslant n$ we have proven that $\mathrm{Im}(\omega_{m+1})$ is the inverse image of $\mathrm{Im}(\omega_m)$ in $A[\ell^{m+1}] \rtimes \mathrm{Aut}(A[\ell^{m+1}])$, so we conclude by taking the limit in m. □

Remark 15. *Let $(A/K, \ell, \alpha)$ be as in Definition 8. Provided that $\dim \mathcal{G}$ is known, by Theorem 14 we may take for n_0 the smallest integer $n \geqslant 1$ ($n \geqslant 2$ for $\ell = 2$) satisfying $[K_{n+1}(\ell^{-(n+1)}\alpha) : K_n(\ell^{-n}\alpha)] = \ell^{b+\dim \mathcal{G}}$. Recall that the problem of determining the Galois group of a number field can be effectively solved, and that the fields $K_m(\ell^{-m}\alpha)$ are generated over K by the roots of some explicit division polynomials, thus the above condition can be effectively tested. If A is an elliptic curve, $\dim \mathcal{G}$ is either 2 or 4 (see Section 2.2) and one can algorithmically decide which case applies* [1]*, so for elliptic curves the parameter n_0 is effectively computable.*

2.5. **Auxiliary results.**

Lemma 16 ([14, Lemma 4.4])**.** *Let A be a connected commutative algebraic group defined over a number field K. For any prime ℓ, the $\mathrm{Gal}(\overline{K}/K)$-representation afforded by $T_\ell(A)$ is unramified almost everywhere.*

Proposition 17. *If A/K is a connected commutative algebraic group defined over a number field, the torsion subgroup of $A(K_\mathfrak{p})$ is finite for every prime $\mathfrak{p}$ of K (where $K_\mathfrak{p}$ denotes the completion of K at $\mathfrak{p}$).*

Proof. Consider $A/K_\mathfrak{p}$ and its Chevalley decomposition $1 \to A_1 \to A \to A_2 \to 1$, where A_1 is a connected commutative linear algebraic group and A_2 is an abelian variety. Since $K_\mathfrak{p}$ is a p-adic field, the torsion subgroup of $A_2(K_\mathfrak{p})$ is finite by a classical theorem of Mattuck [18], so it suffices to show that the intersection between $\ker(A(K_\mathfrak{p}) \to A_2(K_\mathfrak{p}))$ and the torsion subgroup of $A(K_\mathfrak{p})$ is finite: we are thus reduced to proving that the torsion subgroup of $A_1(K_\mathfrak{p})$ is finite.

The solvable group A_1 has a normal unipotent subgroup such that the quotient is of multiplicative type (and connected, hence a torus): by the same argument as above, it suffices to treat the case of unipotent groups and of tori separately. By the Lie-Kolchin Theorem (and since we are in characteristic zero) the unipotent subgroup is torsion-free, while the assertion is clear for tori. □

Proposition 18. *For a semiabelian variety defined over a number field, the image of the ℓ-adic representation is open in its Zariski closure.*

Proof. We mimic the argument for abelian varieties [3, 4]. As explained in [3, Proof of Lemma 1], it suffices to show that the Lie algebra of the ℓ-adic representation ρ_ℓ is algebraic. By [3, Lemma 1 and Corollary to Lemma 2], it suffices to prove:

(1) ρ_ℓ is unramified outside a finite set of primes of K;
(2) ρ_ℓ is of Hodge-Tate type for all the primes of K lying over ℓ;
(3) elements that act semisimply on $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ are dense in the image of ρ_ℓ.

Property (1) is true by Lemma 16. The existence of the Hodge-Tate decomposition was proved by Faltings in [9] for smooth proper varieties, and it also holds for semiabelian varieties because of the existence of good compactifications for quasi-projective varieties, see [2] and [32, Remark 1.2]. The last property holds because the Frobenius automorphisms act semisimply on the rational Tate module: this follows easily from the analogous statement for abelian varieties and tori because the two sets of Frobenius eigenvalues are disjoint. Indeed, let T be a torus, A be an abelian variety, and F be a Frobenius element corresponding to a place with residue field $\mathbb{F}_q$. The eigenvalues of the action of F on $T_\ell(A)$ have modulus $\sqrt{q}$ by the Weil conjectures, while the eigenvalues of the action of F on $T_\ell(T)$ are of the form ωq, where ω is a root of unity (this last statement is obtained by recalling that the Galois representation on the Tate module of a torus is the tensor product of a permutation representation with the cyclotomic character). □

Finally, we will make use of the following result on profinite groups:

Lemma 19. [10, Lemma 18.1.1 and Proposition 18.2.2] *Let* G *be a profinite group and* H *a closed normal subgroup of* G*. If* π *denotes the natural projection* $\mathrm{G} \to \mathrm{G}\,/\,\mathrm{H}$*, then for any measurable subset* $S \subseteq \mathrm{G}\,/\,\mathrm{H}$ *the preimage* $\pi^{-1}(S)$ *is measurable in* G*, and its Haar measure is* $\mu_{\mathrm{G}\,/\,\mathrm{H}}(S)$*. If* $\mathrm{G}\,/\,\mathrm{H}$ *is finite (i.e. if* H *is open), this measure equals* $\#S/\#(\mathrm{G}\,/\,\mathrm{H})$*.*

3. Cohomological interpretation of the density

3.1. **The Kummer cohomology class.** Let A be a connected commutative algebraic group defined over a number field K and let ℓ be a prime number. If $\alpha \in A(K)$ and n is a positive integer, we denote by $\ell^{-n}(\alpha)$ the set of points $\alpha' \in A(\overline{K})$ satisfying $[\ell^n]\alpha' = \alpha$. We then call $\ell^{-\infty}(\alpha)$ the set consisting of all sequences $\beta := \{\beta_n\}_{n\geqslant 1}$ satisfying

$$[\ell]\beta_1 = \alpha \qquad \text{and} \qquad [\ell]\beta_{n+1} = \beta_n \quad \forall n \geqslant 1\,.$$

We have $\ell^{-n}(0) = A[\ell^n]$ and $\ell^{-\infty}(0) = T_\ell A$. If β, β' are in $\ell^{-\infty}(\alpha)$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we define $\sigma(\beta) := \{\sigma(\beta_n)\}_{n\geqslant 1}$ and $\beta' - \beta := \{\beta'_n - \beta_n\}_{n\geqslant 1}$. So for any $\beta \in \ell^{-\infty}(\alpha)$ we get a cocycle

$$\begin{array}{rccc} c_\beta : & \mathrm{Gal}(\overline{K}/K) & \to & T_\ell A \\ & \sigma & \mapsto & \sigma(\beta) - \beta. \end{array}$$

The induced map from $\mathrm{Gal}(K_\alpha/K)$ agrees with (2) on $\mathrm{Gal}(K_\alpha/K_\infty)$. A different choice of β alters c_β by a coboundary, so its class C_α in $H^1(\mathrm{Gal}(\overline{K}/K), T_\ell A)$ is well-defined: we call it the *Kummer class* of α. We equivalently consider C_α to be in $H^1(\mathrm{Gal}(K_\alpha/K), T_\ell A)$ and denote by $C_{\alpha,n}$ its image in $H^1(\mathrm{Gal}(K_\alpha/K), A[\ell^n])$, which is obtained by replacing a

sequence with its term of index n. Notice that $C_{\alpha,n}$ is trivial if and only if there is some point in $\ell^{-n}(\alpha)$ which is defined over K.

3.2. **Cohomological conditions.** For $\sigma \in \mathrm{Gal}(K_\alpha/K)$ the restriction map with respect to the profinite cyclic subgroup generated by σ is

$$\mathrm{Res}_\sigma : H^1(\mathrm{Gal}(K_\alpha/K), T_\ell A) \to H^1(\langle\sigma\rangle, T_\ell A)\,.$$

Likewise, for $\tau \in \mathrm{Gal}(K_{\alpha,n}/K)$ the restriction map with respect to the cyclic subgroup generated by τ is

$$\mathrm{Res}_\tau : H^1(\mathrm{Gal}(K_{\alpha,n}/K), A[\ell^n]) \to H^1(\langle\tau\rangle, A[\ell^n])\,.$$

Consider the following sets:

$$S_\alpha := \{\sigma \,:\, C_\alpha \in \ker(\mathrm{Res}_\sigma)\} = \{\sigma \,:\, \sigma\beta = \beta \text{ for some } \beta \in \ell^{-\infty}\alpha\} \subseteq \mathrm{Gal}(K_\alpha/K)$$

$$S_{\alpha,n} := \{\tau \,:\, C_{\alpha,n} \in \ker(\mathrm{Res}_\tau)\} = \{\tau \,:\, \tau\beta_n = \beta_n \text{ for some } \beta_n \in \ell^{-n}\alpha\} \subseteq \mathrm{Gal}(K_{\alpha,n}/K)\,.$$

Suppose that (C2i) and (C2ii) of Definition 8 hold and consider $n \geqslant n_0$: if $\tau \in S_{\alpha,n}$ fixes $\beta_n \in \ell^{-n}\alpha$, then there is $\tau' \in S_{\alpha,n+1}$ over τ that fixes some $\beta_{n+1} \in \ell^{-(n+1)}\alpha$ satisfying $[\ell]\beta_{n+1} = \beta_n$. We deduce that $S_{\alpha,n}$ is the image of $S_{\alpha,n+1}$ (by passage to the limit, also of S_α) in $\mathrm{Gal}(K_{\alpha,n}/K)$. Thus the Haar measure of S_α in $\mathrm{Gal}(K_\alpha/K)$ is well-defined and its value is

$$\mu(S_\alpha) = \lim_{n\to\infty} \frac{\#S_{\alpha,n}}{\#\,\mathrm{Gal}(K_{\alpha,n}/K)}$$

because we take the limit of a non-increasing sequence of positive numbers.

We may then rephrase Theorem 7 in the form

$$\mathrm{Dens}_\ell(\alpha) = \mu(S_\alpha)\,. \tag{7}$$

Proof of Theorem 7. Even though [13, Theorem 3.2] is stated only for products of abelian varieties and tori, the proof works equally well if one just assumes that the triple $(A/K, \ell, \alpha)$ satisfies the conditions of Definition 8. □

A similar result holds for the density of reductions such that the ℓ-adic valuation of the order of $(\alpha \bmod \mathfrak{p})$ is at most n: the cohomological condition becomes $C_\alpha \in \ker([\ell^n]\,\mathrm{Res}_\sigma)$.

3.3. **Basic properties of S_α.** We now give another characterization of the set S_α.

Remark 20 ([13, Proof of Theorem 3.8])**.** *Writing $\sigma = (t_\sigma, M_\sigma) \in \mathrm{Gal}(K_{\alpha,n}/K)$ as in* (4)*, we have*

$$\sigma \in S_{\alpha,n} \qquad \Leftrightarrow \qquad t_\sigma \in \mathrm{Im}(M_\sigma - I)\,.$$

Indeed, if $t_\sigma = (M_\sigma - I)\gamma$ for some $\gamma \in A[\ell^n]$ then we have $t_\sigma = \sigma(\beta_n) - \beta_n = \sigma(\gamma) - \gamma$ and hence $\beta_n - \gamma$ is a point in $\ell^{-n}(\alpha)$ fixed by σ. Conversely, if some $\beta'_n \in \ell^{-n}(\alpha)$ is fixed by σ then $\beta_n - \beta'_n$ is in $A[\ell^n]$ and its image under $M_\sigma - I$ is $\sigma(\beta_n) - \beta_n = t_\sigma$. The same remark holds for S_α, hence we have

$$S_\alpha = \{\sigma = (t, M) \in \mathrm{Gal}(K_\alpha/K) \,:\, M \in \mathcal{G} \text{ and } t \in \mathrm{Im}(M - I)\}\,. \tag{8}$$

Remark 21. *We may equivalently consider S_α as a subset of $\mathrm{Gal}(\overline{K}/K)$ or of $\mathrm{Gal}(K_\alpha/K)$: since $\bar\sigma \in \mathrm{Gal}(\overline{K}/K)$ acts on $\ell^{-\infty}(\alpha)$ through its image $\sigma \in \mathrm{Gal}(K_\alpha/K)$, the set*

$$\overline{S_\alpha} = \{\bar\sigma \in \mathrm{Gal}(\overline{K}/K) : \mathrm{Res}_{\bar\sigma}(C_\alpha) = 0\}$$

is the inverse image in $\mathrm{Gal}(\overline{K}/K)$ of S_α, and hence $\mu_{\mathrm{Gal}(\overline{K}/K)}(\overline{S_\alpha}) = \mu_{\mathrm{Gal}(K_\alpha/K)}(S_\alpha)$ by Lemma 19.

Proposition 22. *If L/K is any Galois extension which is linearly disjoint from K_α over K we have $\mathrm{Dens}_L(\alpha) = \mathrm{Dens}_K(\alpha)$.*

Proof. By Theorem 7 and Remark 21 we have to prove that, considering S_α as a subset of $\mathrm{Gal}(K_\alpha/K)$ or of $\mathrm{Gal}(L_\alpha/L)$, we have $\mu_{\mathrm{Gal}(K_\alpha/K)}(S_\alpha) = \mu_{\mathrm{Gal}(L_\alpha/L)}(S_\alpha)$. Since L and K_α are linearly disjoint over K, the restriction map $\mathrm{Gal}(L_\alpha/L) \to \mathrm{Gal}(K_\alpha/K)$ is an isomorphism of groups and of measured spaces. We may easily conclude because $\ell^{-\infty}(\alpha) \subset K_\alpha$, so that in particular the action of $\mathrm{Gal}(L_\alpha/L)$ on $\ell^{-\infty}\alpha$ factors through $\mathrm{Gal}(K_\alpha/K)$. □

4. The density as an ℓ-adic integral

4.1. **The 1-Eigenspace for elements in the image of the ℓ-adic representation.** Recall that we denote by $\mathcal{G}$ the image of the ℓ-adic Galois representation attached to A, and that $A[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^b$. For every $M \in \mathrm{Aut}(T_\ell(A))$, the kernel of $M - I : A[\ell^\infty] \to A[\ell^\infty]$ is a (possibly infinite) abelian ℓ-group. We restrict our attention to those M for which $\ker(M-I)$ is finite. If F is a finite abelian ℓ-group with at most b cyclic components, we define

$$\mathcal{M}_\mathrm{F} := \{M \in \mathcal{G} : \ker(M - I : A[\ell^\infty] \to A[\ell^\infty]) \cong \mathrm{F}\} \tag{9}$$

and also define

$$\mathcal{M} := \bigcup_\mathrm{F} \mathcal{M}_\mathrm{F}, \tag{10}$$

where the union is taken over all finite abelian ℓ-groups with at most b cyclic components, that is, such that $\dim_{\mathbb{F}_\ell} F/\ell F \le b$ (recall that b is the first Betti number of A, which is also the $\mathbb{Z}_\ell$-rank of $T_\ell(A)$). We write $\mathcal{M}_\mathrm{F}(n)$ for the image of $\mathcal{M}_\mathrm{F}$ under the reduction map $\mathcal{G} \to \mathcal{G}(n)$, and denote by $\exp \mathrm{F}$ the exponent of the finite group F.

Lemma 23. *The set $\mathcal{M}_\mathrm{F}$ of* (9) *is measurable in $\mathcal{G}$ and we have $\mu(\mathcal{M}_\mathrm{F}) = \mu(\mathcal{M}_\mathrm{F}(n))$ for every $n > v_\ell(\exp \mathrm{F})$. In particular we have $\mu(\mathcal{M}_\mathrm{F}) = 0$ if and only if $\mathcal{M}_\mathrm{F} = \emptyset$. The set $\mathcal{M}$ of* (10) *is measurable in $\mathcal{G}$ and, if A satisfies* (C1)*, we have $\mu(\mathcal{M}) = 1$.*

Proof. Call $\pi_n : \mathcal{G} \to \mathcal{G}(n)$ the reduction modulo ℓ^n. For $n > v_\ell(\exp \mathrm{F})$ the defining condition for $\mathcal{M}_\mathrm{F}$ can be checked modulo ℓ^n, so we have $\mathcal{M}_\mathrm{F} = \pi_n^{-1}(\mathcal{M}_\mathrm{F}(n))$ and the first assertion follows from Lemma 19. The set $\mathcal{M}$ is measurable because it is a countable union of measurable sets, and we are left to prove $\mu(\mathcal{G} \setminus \mathcal{M}) = 0$. Since $\mathcal{G} \setminus \mathcal{M} \subseteq \pi_n^{-1}(\pi_n(\mathcal{G} \setminus \mathcal{M}))$, by Lemma 19 it suffices to show that

$$\mu(\pi_n(\mathcal{G} \setminus \mathcal{M})) = \frac{\#\pi_n(\mathcal{G} \setminus \mathcal{M})}{\#\mathcal{G}(n)} \tag{11}$$

tends to 0 as n tends to infinity. By (C1), the cardinality of $\mathcal{G}(n)$ is asymptotically given by a constant (positive) multiple of $\ell^{n \dim \mathcal{G}}$. Let $\mathcal{G}_{\mathrm{Zar}}$ be the Zariski closure of $\mathcal{G}$ in $\mathrm{GL}_{b,\mathbb{Q}_\ell}$ and let V

be the closed ℓ-adic analytic subvariety of $\mathcal{G}_{\mathrm{Zar}}(\mathbb{Q}_\ell)$ defined by the equation $\det(M-I)=0$. Define $\mathrm{V}(\mathbb{Z}_\ell) := \mathrm{V}\cap \mathrm{GL}_b(\mathbb{Z}_\ell)$. If $M\in\mathcal{G}$ does not satisfy $\det(M-I)=0$ we must have $v_\ell \det(M-I)\leqslant n$ for some n, thus the kernel of $M-I$ is finite: this shows $\mathcal{G}\setminus\mathcal{M}\subseteq \mathrm{V}(\mathbb{Z}_\ell)$. The numerator of (11) is then at most $\#\pi_n(\mathrm{V}(\mathbb{Z}_\ell))$, which by [20, Theorem 4] is bounded from above by a constant times $\ell^{n\dim(\mathrm{V})}$. To conclude, we only need to prove $\dim(\mathrm{V})<\dim\mathcal{G}$.

Suppose instead $\dim(\mathrm{V})=\dim\mathcal{G}$. Then $\mathrm{V}(\mathbb{Z}_\ell)$ contains an open subset of $\mathcal{G}$ and hence the preimage of $\mathrm{V}(\mathbb{Z}_\ell)$ in $\mathrm{Gal}(\overline{K}/K)$ contains some open subset U. Since Frobenius elements are dense in $\mathrm{Gal}(\overline{K}/K)$, we can find infinitely many of them in U (and by definition any such automorphism acts on $T_\ell(A)$ with a fixed point). We now show that this is impossible.

By Lemma 16 we can find a prime $\mathfrak{p}$ of K such that a corresponding Frobenius element is in U, the characteristic of $\mathfrak{p}$ is different from ℓ, and the ℓ-adic Galois representation attached to A is unramified at $\mathfrak{p}$. Consider the completion $K_\mathfrak{p}$. The assumption that the representation is unramified implies that the image of $\mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$ in $\mathrm{Aut}(T_\ell(A))$ is topologically generated by a Frobenius element, and hence this Galois group acts on $T_\ell(A)$ with a fixed point. This contradicts the finiteness of the torsion subgroup of $A(K_\mathfrak{p})$, see Proposition 17. □

4.2. **The condition on the arboreal representation.** Recall from (7) that to compute the density $\mathrm{Dens}_\ell(\alpha)$ we just need to evaluate the Haar measure of the set S_α. By Remark (20), we know a condition describing the related sets $S_{\alpha,n}$. In this section, we count the elements of $S_{\alpha,n}$ by making use of that condition, and for this purpose we introduce sets $\mathcal{W}_n(M)$ and rational numbers $\mathrm{w}_n(M)$: roughly speaking, $\mathcal{W}_n(M)$ is given by the torsion points $t\in A[\ell^n]$ for which there is a Galois automorphism that sends β_n to β_n+t while acting as M on $A[\ell^n]$, and the number $\mathrm{w}_n(M)$ measures the intersection of $\mathcal{W}_n(M)$ with the image of $M-I$.

We keep the notation of Section 2.2 and suppose that $(A/K,\alpha,\ell)$ are as in Definition 8, fixing n_0 as appropriate. Recall that we identify $\mathcal{G}(n)$ and $\mathrm{Gal}\,(K_n/K)$ and that we see $\mathrm{Gal}\,(K_{\alpha,n}/K)$ as a subgroup of $A[\ell^n]\rtimes \mathrm{Gal}\,(K_n/K)$. Denoting by π_1,π_2 the two natural projections, for each $M\in\mathcal{G}(n)$ we define the set

$$\mathcal{W}_n(M) := \pi_1\circ\pi_2^{-1}(M) = \{t\in A[\ell^n] \mid (t,M)\in \mathrm{Gal}(K_n(\ell^{-n}\alpha)/K)\}\,. \tag{12}$$

Lemma 24. *The set $\mathcal{W}_n(M)$ is a translate of $\mathcal{W}_n(I)$.*

Proof. Fix $t_0\in\mathcal{W}_n(M)$. If $t\in\mathcal{W}_n(M)$, we have $(t,M)(t_0,M)^{-1}=(t-t_0,I)$ and hence $t-t_0\in\mathcal{W}_n(I)$. If $v\in\mathcal{W}_n(I)$, we have $(v,I)(t_0,M)=(v+t_0,M)$ and hence $v+t_0\in\mathcal{W}_n(M)$. □

We also define the rational number

$$\mathrm{w}_n(M) := \frac{\#\big(\mathrm{Im}(M-I)\cap\mathcal{W}_n(M)\big)}{\#\,\mathrm{Im}(M-I)}\,. \tag{13}$$

For $M\in\mathcal{G}$ we can define $\mathcal{W}_n(M):=\mathcal{W}_n(M_n)$ and $\mathrm{w}_n(M):=\mathrm{w}_n(M_n)$, where M_n is the reduction of M modulo ℓ^n.

Lemma 25. *If $M\in\mathcal{G}$, the value $\mathrm{w}_n(M_n)$ is independent of n for $n\geqslant n_0$, and we call it $\mathrm{w}(M)$: it is either zero or a power of ℓ with exponent $\leqslant 0$.*

Proof. In the course of this proof, given a subset W of a $\mathbb{Z}_\ell$-module B and a non-negative integer k, we denote by $\ell^{-k}W$ the set $\{b \in B : \ell^k b \in W\}$. We know $\mathrm{Im}(M_{n_0} - I) = \ell^{n-n_0}\,\mathrm{Im}(M_n - I)$ because the following diagram is commutative:

$$\begin{array}{ccc} A[\ell^n] & \xrightarrow{M_n} & A[\ell^n] \\ {\scriptstyle \ell^{n-n_0}}\downarrow & & \downarrow{\scriptstyle \ell^{n-n_0}} \\ A[\ell^{n_0}] & \xrightarrow{M_{n_0}} & A[\ell^{n_0}] \end{array}$$

We also have $\mathcal{W}_n(M_n) = \ell^{-(n-n_0)}\,\mathcal{W}_{n_0}(M_{n_0})$: an inclusion clearly holds, and the two sets have cardinality $\ell^{b(n-n_0)} \#\,\mathcal{W}_{n_0}(M_{n_0})$ by (C2ii) and because by definition we have

$$\mathcal{W}_{n_0}(M_{n_0}) = \{t \in A[\ell^{n_0}] \mid (t, M_{n_0}) \in \mathrm{Gal}(K_{n_0}(\ell^{-n_0}\alpha)/K)\}$$

where by (C2i) the condition on t can be rewritten as $(t, M_n) \in \mathrm{Gal}(K_n(\ell^{-n_0}\alpha)/K)$.

Denote by Z the kernel of the well-defined and surjective group homomorphism

$$\ell^{n-n_0} : \mathrm{Im}(M_n - I) \to \mathrm{Im}(M_{n_0} - I)\,. \tag{14}$$

To prove the first assertion it suffices to show that the induced (well-defined and surjective) group homomorphism

$$\ell^{n-n_0} : \mathrm{Im}(M_n - I) \cap \mathcal{W}_n(M_n) \to \mathrm{Im}(M_{n_0} - I) \cap \mathcal{W}_{n_0}(M_{n_0}) \tag{15}$$

is $\#Z$-to-1: this amounts to remarking that if $x \in \mathrm{Im}(M_n - I) \cap \mathcal{W}_n(M_n)$ then we have $x + Z \subseteq \mathcal{W}_n(M_n)$ because $\ell^{-(n-n_0)}(\ell^{n-n_0}x) \subseteq \ell^{-(n-n_0)}\,\mathcal{W}_{n_0}(M_{n_0}) = \mathcal{W}_n(M_n)$.

We now fix some $n \geqslant n_0$ and prove that $\mathrm{w}_n(M_n)$ is either zero or a power of ℓ (the condition on the exponent is clear from $\mathrm{w}_n(M_n) \leqslant 1$). Recall that $\mathrm{Im}(M_n - I)$ and $\mathcal{W}_n(I)$ are finite ℓ-groups. We may suppose that $\mathrm{Im}(M_n - I) \cap \mathcal{W}_n(M_n)$ is non-empty and fix some element t_0. By Lemma 24 we have

$$\mathcal{W}_n(M_n) \cap \mathrm{Im}(M_n - I) = \big(t_0 + \mathcal{W}_n(I)\big) \cap \big(t_0 + \mathrm{Im}(M_n - I)\big) = t_0 + \big(\mathcal{W}_n(I) \cap \mathrm{Im}(M_n - I)\big),$$

which implies our claim since $\mathcal{W}_n(I) \cap \mathrm{Im}(M_n - I)$ is an ℓ-group. □

Example 26. Even if $M \in \mathcal{M}$ we can have $\mathrm{w}(M) = 0$. Let $E/\mathbb{Q}$ be an elliptic curve such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$ and $\alpha \in E(\mathbb{Q})$ be a point of infinite order such that the arboreal representation attached to $(E/\mathbb{Q}, \alpha, \ell)$ is surjective (for an example, see Section 6.3), so that its image mod ℓ is $(\mathbb{Z}/\ell\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ (here we have fixed an isomorphism $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$). Consider the cyclic subgroup H of $E[\ell] \rtimes \mathrm{Aut}(E[\ell])$ generated by $\left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right)$, which has order ℓ. Writing K for the fixed field of H, the triple $(E/K, \ell, \alpha)$ clearly satisfies the conditions in Definition 8 with $n_0 = 1$. We can find $M \in \mathcal{M}$ such that $M_1 = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. By construction, the set $\mathcal{W}(M_1)$ contains only the element $\begin{pmatrix}0\\1\end{pmatrix}$, which is not in $\mathrm{Im}(M_1 - I)$. This shows $\mathrm{w}(M) = \mathrm{w}_1(M_1) = 0$.

4.3. **The general formula for the density.** By Lemma 23, the disjoint union $\mathcal{M} := \cup_{\mathrm{F}} \mathcal{M}_{\mathrm{F}}$ has full measure in $\mathcal{G}$, hence the domain of integration in (1) may be replaced by $\mathcal{M}$.

Proof of Theorem 1. Recalling (9), we consider the set

$$S_{\mathrm{F}} = \{\sigma = (t, M) \in \mathrm{Gal}(K_\alpha/K) \,:\, M \in \mathcal{M}_{\mathrm{F}} \text{ and } t \in \mathrm{Im}(M - I)\}\,. \tag{16}$$

To see that the Haar measure of S_{F} in $\mathrm{Gal}(K_\alpha/K)$ is well-defined and to compute it, we consider the reduction modulo ℓ^n of $\mathcal{M}_{\mathrm{F}}$ and the set

$$S_{\mathrm{F},n} = \{\sigma = (t, M) \in \mathrm{Gal}(K_{\alpha,n}/K) \,:\, M \in \mathcal{M}_{\mathrm{F}}(n) \text{ and } t \in \mathrm{Im}(M - I)\}\,. \tag{17}$$

We restrict to $n > \max\{n_0, v_\ell(\exp \mathrm{F})\}$, where n_0 is as in Definition 8. By (12) and (13) we have

$$\#S_{\mathrm{F},n} = \sum_{M \in \mathcal{M}_{\mathrm{F}}(n)} \#\big(\mathrm{Im}(M - I) \cap \mathcal{W}_n(M)\big) = \sum_{M \in \mathcal{M}_{\mathrm{F}}(n)} \ell^{bn - v_\ell \det(M-I)}\, \mathrm{w}_n(M)\,.$$

From (6) we deduce

$$\frac{\#S_{\mathrm{F},n}}{\#\,\mathrm{Gal}(K_{\alpha,n}/K)} = \frac{1}{\#\,\mathcal{G}(n)} \sum_{M \in \mathcal{M}_{\mathrm{F}}(n)} \mathrm{c}_{\text{Kummer}} \cdot \ell^{-v_\ell \det(M-I)} \cdot \mathrm{w}_n(M). \tag{18}$$

By (5) the left hand side of (18) is a non-increasing function of n, and therefore it admits a limit for $n \to \infty$, which is $\mu(S_{\mathrm{F}})$. We claim that $S_{\mathrm{F},n}$ is the image of S_{F} in $\mathrm{Gal}(K_{\alpha,n}/K)$.

The set $S_{\mathrm{F},n}$ clearly contains the reduction modulo ℓ^n of S_{F}, so we prove the other inclusion. Let $\sigma_n = (t_n, M_n) \in S_{\mathrm{F},n}$. The natural map $\mathrm{Gal}(K_\alpha/K) \to \mathrm{Gal}(K_{\alpha,n}/K)$ is surjective, so there is an element (t, M) in $\mathrm{Gal}(K_\alpha/K)$ that reduces to σ_n. Since $n > v_\ell(\exp \mathrm{F})$, we have $\ker(M - I) \simeq \ker(M_n - I)$ and hence $M \in \mathcal{M}_{\mathrm{F}}$. We now construct an element of S_{F} reducing to σ_n: take $a_n \in A[\ell^n]$ satisfying $(M_n - I)(a_n) = t_n$, and consider a lift a of a_n to $T_\ell(A)$; we may replace t by $(M - I)a$ because the difference is in $\ell^n T_\ell(A)$ and since $n > n_0$ we know that $\mathrm{Gal}(K_\alpha/K)$ contains $\ell^n T_\ell(A) \times \{I\}$.

The right-hand side of (18) is an integral over $\mathcal{M}_{\mathrm{F}}(n)$ with respect to the normalized counting measure of $\mathcal{G}(n)$ (see §1.7), and the matrices in $\mathcal{M}_{\mathrm{F}}$ are exactly the matrices in $\mathcal{G}$ whose reduction modulo ℓ^n lies in $\mathcal{M}_{\mathrm{F}}(n)$. By Lemma 25, taking the limit in n gives

$$\mu(S_{\mathrm{F}}) = \int_{\mathcal{M}_{\mathrm{F}}} \mathrm{c}_{\text{Kummer}} \cdot \ell^{-v_\ell \det(x-I)} \cdot \mathrm{w}(x)\; d\mu_{\mathcal{G}}(x)\,. \tag{19}$$

Consider the natural projection $\pi : \mathrm{Gal}(K_\alpha/K) \to \mathrm{Gal}(K_\infty/K)$. By Lemmas 19 and 23 the set S_α of (8) is the disjoint union of the sets $S_{\mathrm{F}} = S_\alpha \cap \pi^{-1}(\mathcal{M}_{\mathrm{F}})$ up to a set of measure 0, so we may conclude by Theorem 7 in the form of (7). □

4.4. **Equivalent formulations of** (1)**.** Recall that $\mathrm{Gal}(K_\alpha/K)$ is a subgroup of $T_\ell(A) \rtimes \mathcal{G}$ and consider the two projections: the integrand of (1) is then

$$M \;\mapsto\; \mu_{T_\ell(A)}\big(\mathrm{Im}(M - I) \cap \pi_1 \circ \pi_2^{-1}(M)\big),$$

where $\mu_{T_\ell(A)}$ is the normalized Haar measure on $T_\ell(A)$. Indeed, calling M_n the reduction of M modulo ℓ^n, we have by (12) and (13)

$$\ell^{-v_\ell \det(M_n - I)} \cdot \mathrm{w}_n(M_n) = \frac{\#\big(\operatorname{Im}(M_n - I) \cap \pi_1 \circ \pi_2^{-1}(M_n)\big)}{\#A[\ell^n]}$$

and $\mu_{T_\ell(A)}$ is the limit of the normalized counting measures (see §1.7) on $T_\ell(A)/\ell^n T_\ell(A) \simeq A[\ell^n]$.

Remark 27. *For every $M \in \mathcal{M}_{\mathrm{F}}$ we have $\ell^{v_\ell \det(M-I)} = \#\,\mathrm{F}$, so we can rewrite* (1) *as*

$$\mathrm{Dens}_\ell(\alpha) = \sum_{\mathrm{F}} \frac{\mathrm{c}_{\textit{Kummer}}}{\#\,\mathrm{F}} \cdot \delta(\mathrm{F}) \qquad \textit{where} \quad \delta(\mathrm{F}) := \int_{\mathcal{M}_{\mathrm{F}}} \mathrm{w}(x)\, d\mu_{\mathcal{G}}(x)\,. \tag{20}$$

Furthermore, we may restrict the sum in (20) to those groups F which contain a subgroup isomorphic to $A(K)[\ell^\infty]$ because for all but finitely many primes $\mathfrak{p}$ of K the group $A(K)[\ell^\infty]$ injects into the group of local points $A(\mathbb{F}_\mathfrak{p})$.

Example 28. Suppose that for all $n \geqslant 1$ the fields $K_{\alpha,n}$ and K_∞ are linearly disjoint over K_n, and that $[K_{\alpha,n} : K_n] = \ell^{b \max(n-d,0)}$ holds for some $d \geqslant 0$. We then have

$$\mathrm{Dens}_\ell(\alpha) = \sum_{\mathrm{F}} \frac{1}{\#\ell^d\,\mathrm{F}} \cdot \mu(\mathcal{M}_{\mathrm{F}})\,. \tag{21}$$

Indeed, let $M \in \mathcal{M}_{\mathrm{F}}(n)$ for some $n > \max(d, v_\ell(\exp \mathrm{F}))$. We know $\operatorname{Im}(M - I) = (\mathbb{Z}/\ell^n\mathbb{Z})^b/\,\mathrm{F}$ and $\mathcal{W}_n(M) = (\ell^d\mathbb{Z}/\ell^n\mathbb{Z})^b$, so by elementary group theory we have

$$\mathrm{w}_n(M) = \frac{\ell^{b(n-d)} \cdot (\#\ell^d\,\mathrm{F})^{-1}}{\ell^{bn} \cdot (\#\,\mathrm{F})^{-1}} = \frac{\#\,\mathrm{F}}{\ell^{bd} \cdot \#\ell^d\,\mathrm{F}}$$

independently of n and M, and we may easily conclude because $\mathrm{c}_{\mathrm{Kummer}} = \ell^{bd}$. The density in (21) equals the "probability" that the ℓ-part of $(\alpha \bmod \mathfrak{p})$ is trivial, if we assume this to be uniformly distributed. Indeed, $\mu(\mathcal{M}_{\mathrm{F}})$ is the "probability" that the ℓ-part of the group of local points $A_\mathfrak{p}(k_\mathfrak{p})$ is isomorphic to F (where F varies over all finite abelian ℓ-groups); in the group F the "probability" that an element (which is an ℓ^d-power) is coprime to ℓ is exactly $(\#\ell^d\,\mathrm{F})^{-1}$. The generic case corresponds to $d = 0$.

5. Asymptotic behaviour of the density

In this section we prove an uniform lower bound for the density under the assumption that A/K is the product of an abelian variety and a torus.

Theorem 29. *Let A/K be the product of an abelian variety and a torus defined over a number field. There exists a positive constant $c := c(A/K)$ such that the inequality*

$$\mathrm{Dens}_\ell(\ell^n\alpha) \geqslant 1 - \frac{c}{\ell^{n+1}}$$

holds for all primes ℓ, for all integers $n \geqslant 0$, and for all points $\alpha \in A(K)$. In particular, $\mathrm{Dens}_\ell(\ell^n\alpha)$ goes to 1 for $\ell^n \to \infty$ independently of α.

Remark 30. *An interesting consequence of this result is that the power of ℓ appearing in the denominator of $\mathrm{Dens}_\ell(\alpha)$ cannot be bounded uniformly in α even for a fixed A, provided that $A(K)$ is infinite. Indeed, the rational numbers $\mathrm{Dens}_\ell(\ell^n\alpha)$ in Theorem 29 must have unbounded height because they are strictly smaller than one: for any point β of infinite order on a semiabelian variety, $\mathrm{Dens}_\ell(\beta)$ is never equal to 1, see* [21, Corollary 14].

Lemma 31. *Let A be the product of an abelian variety A' and of a torus defined over a number field K. Call K' the splitting field of the torus (to be interpreted as K if the torus is trivial). For every prime number ℓ and for every integer $n \geqslant 1$ consider the subgroup $H_{\ell,n}$ of $\mathrm{Gal}(K_{\ell^n}/K)$ consisting of the elements that act on $A'[\ell^n]$ as multiplication by some scalar λ (if $A' \neq 0$) and that can be lifted to an automorphism of K'_{ℓ^n}/K' that acts as exponentiation by λ^2 on ζ_{ℓ^n}. There exists some positive constant $c' := c'(A/K)$ such that for every ℓ and n we have $\#H_{\ell,n} \geqslant c'\ell^n$.*

Proof. We claim that it is enough to prove the result under the additional assumption $K = K'$, that is, in the case of split tori. Indeed, let $H'_{\ell,n}$ denote the subgroup of $\mathrm{Gal}(K'_{\ell^n}/K')$ consisting of the elements that act on $A'[\ell^n]$ as multiplication by λ and on ζ_{ℓ^n} as exponentiation by λ^2. Then it is clear that there is an injective map $H'_{\ell,n} \to H_{\ell,n}$, and since $[\mathrm{Gal}(\overline{K}/K) : \mathrm{Gal}(\overline{K'}/K')] = [K' : K]$ we have $\#H_{\ell,n} \geq \frac{1}{[K':K]}\#H'_{\ell,n}$. Thus proving the result for K' is enough to establish it for K as well. If A' is trivial and hence $A = \mathbb{G}_m^r$, the ℓ^n-torsion field is $K(\zeta_{\ell^n})$, so $H_{\ell,n}$ is the group of squares in $\mathcal{G}(n) = \mathrm{Gal}(K(\mu_{\ell^n})/K)$. In this case we have $\#H_{\ell,n} \geq \frac{1}{2}[K(\mu_{\ell^n}) : K] \geq \frac{1}{[K:\mathbb{Q}]}\frac{\ell-1}{2} \cdot \ell^{n-1}$ and we can take $c' = \frac{1}{4[K:\mathbb{Q}]}$. If $A' \neq 0$, call $\hat{A}'$ the dual abelian variety of A' and let $S_{\ell,n}$ be the subgroup of $\mathcal{G}(n)$ consisting of those elements that act as a scalar on $(A' \times \hat{A}')[\ell^n]$. Notice that $A' \times \hat{A}'$ depends only on A.

By a theorem of Serre-Wintenberger ([36, Théorème 3]) there is a constant $d := d(A/K)$ such that for every ℓ and for every $k \in \mathbb{Z}^\times$ the matrix $k^d \cdot I$ is in the image of the ℓ-adic representation attached to $A' \times \hat{A}'$, so we have $\#S_{\ell,n} \geqslant \frac{\ell^n}{4d}$ (the index of the subgroup of d-th powers in $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$ is at most $2d$ and $\#(\mathbb{Z}/\ell^n\mathbb{Z})^\times \geqslant \frac{1}{2}\ell^n$). Considering the Weil pairing $A'[\ell^n] \times \hat{A}'[\ell^n] \to \langle\zeta_{\ell^n}\rangle$ we deduce that $S_{\ell,n}$ is contained in $H_{\ell,n}$ and we are done. □

Lemma 32. *Let A/K be the product of an abelian variety and a torus defined over a number field. For any integer $n \geqslant 1$ consider the set*

$$B_{\ell,n} := \{x \in \mathcal{G} \;\big|\; v_\ell \det(x - I) \geqslant n\}\,.$$

There exists a constant $c := c(A/K)$ such that $\mu(B_{\ell,n}) \leqslant c\ell^{-n}$ holds for all ℓ and n.

Proof. Set $B_{\ell,n}(n) := \{M \in \mathcal{G} : \det(M) \equiv 1 \pmod{\ell^n}\}$, and keep the notation of Lemma 31. Write $\mathcal{G}(n) = \coprod_{r\in\mathcal{R}} H_{\ell,n} \cdot r$, where $\mathcal{R}$ is a set of representatives for the cosets of $H_{\ell,n}$ in $\mathcal{G}(n)$. We identify an element of $H_{\ell,n}$ to its corresponding scalar λ. For a given r, the quantity $\det(\lambda r) = \lambda^b \det(r)$ is congruent to 1 modulo ℓ^n if and only if $\lambda^b \equiv \det(r)^{-1} \pmod{\ell^n}$. For any fixed r, at most $2b$ values of λ satisfy this congruence, and therefore every coset contains at most $2b$ matrices in $B_{\ell,n}(n)$. From Lemma 31 we deduce

$$\#B_{\ell,n}(n) \leqslant 2b \cdot \frac{\#\,\mathcal{G}(n)}{\#H_{\ell,n}} \leqslant \frac{2b}{c'}\ell^{-n} \cdot \#\,\mathcal{G}(n)\,.$$

Since $B_{\ell,n}$ is the inverse image in $\mathcal{G}$ of $B_{\ell,n}(n)$ we get $\mu(B_{\ell,n}) = \frac{\#B_{\ell,n}(n)}{\#\mathcal{G}(n)} \leqslant \frac{2b}{c'} \cdot \ell^{-n}$. □

Proof of Theorem 29. We want to compute the density of the set of primes $\mathfrak{p}$ for which the ℓ-adic valuation of the order of $(\alpha \bmod \mathfrak{p})$ is at most n. For the primes $\mathfrak{p}$ in the complement of this set, $\#A(\mathbb{F}_\mathfrak{p})$ is divisible by ℓ^{n+1}; in particular, the Frobenius at $\mathfrak{p}$ is an element of the set $B_{\ell,n+1}$ of Lemma 32. The result follows immediately. □

6. The density for elliptic curves

This section is devoted to elliptic curves, and it relies on the companion paper [16] for explicit results on the sets $\mathcal{M}_F$ from (9) and for a classification of all Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. In short, we describe a Cartan subgroup $C(c,d)$ with the help of two integer parameters c and d (see [16, Section 2]): essentially, $C(c,d)$ is the group of units of the ring $\mathbb{Z}_\ell[x]/(x^2 - cx - d)$. From these parameters one can easily read whether the Cartan subgroup is split, nonsplit or ramified (when $x^2 - cx - d$ is irreducible in $\mathbb{Z}[x]$, these terms roughly correspond to ℓ being respectively reducible, prime, or a divisor of the conductor in the ring $\mathbb{Z}[x]/(x^2 - cx - d)$; see [16, Definition 6] for a precise definition).

At the end of the section we test the value of the density $\mathrm{Dens}_\ell(\alpha)$ in some numerical examples: given an elliptic curve $E/\mathbb{Q}$, a point $\alpha \in E(\mathbb{Q})$, and a prime ℓ, we use SAGE [34] to count the number N_B of primes p up to some bound B (typically $B = 10^6$) for which $\ell \nmid \mathrm{ord}(\alpha \bmod p)$. We then compare the numerical value $N_B/\#\{p \text{ prime } : \ p \leq B\}$ with the value of $\mathrm{Dens}_\ell(\alpha)$ predicted by Theorem 5; in all cases, we find that the numerical experiments are in excellent agreement with our results.

6.1. Computability of the density.

We show that, in the special case of A/K being an elliptic curve, the value $\mathrm{Dens}_\ell(\alpha)$ can be effectively computed for all $\alpha \in A(K)$.

One can first determine whether the order of α is either coprime to ℓ, divisible by ℓ, or ∞. In the first two cases $\mathrm{Dens}_\ell(\alpha)$ is respectively 1 and 0, so we can assume without loss of generality that α is a point of infinite order. In this case, the set $\mathbb{Z}\alpha$ is Zariski-dense in A, so by Remark 9 we know that $\mathrm{Dens}_\ell(\alpha)$ is given by (20). We shall make use of the following definition:

Definition 33. *A subset of* $\mathbb{N}^2$ *is* admissible *if it is the product of two subsets of* $\mathbb{N}$ *which are either finite or consist of all integers greater than some given one. The family of finite unions of admissible sets is closed with respect to intersection, union and complement.*

As in Section 4.1 we study subsets of $\mathcal{G}$ of the form $\mathcal{M}_\mathrm{F}$, where F is a finite subgroup of $A[\ell^\infty]$. Since A is an elliptic curve we can write $\mathrm{F} = \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^{a+b}\mathbb{Z}$ for some integers $a, b \geqslant 0$. Setting $\mathcal{M}_{a,b} := \mathcal{M}_\mathrm{F}$ and

$$\delta(a,b) := \frac{1}{\mu(\mathcal{M}_{a,b})} \int_{\mathcal{M}_{a,b}} \mathrm{w}(x)\, d\mu_\mathcal{G}(x), \tag{22}$$

Equation (20) becomes

$$\mathrm{Dens}_\ell(\alpha) = \mathrm{c}_{\text{Kummer}} \cdot \sum_{(a,b)\in\mathbb{N}^2} \mu(\mathcal{M}_{a,b}) \cdot \ell^{-2a-b} \cdot \delta(a,b)\,. \tag{23}$$

Proposition 34. *The set $\mathbb{N}^2$ can be partitioned into finitely many, effectively computable admissible sets, such that on each one, δ is constant, and an effectively computable rational number.*

Proof. We first compute an integer n_0 as in Definition 8, see Remark 15. We may suppose $\mathcal{M}_{a,b} \neq \emptyset$ because by [16, Theorem 1] the pairs (a,b) satisfying $\mathcal{M}_{a,b} = \emptyset$ form an explicitly computable admissible set, and for them $\delta(a,b) = 0$. By definition, we know

$$\delta(a,b) = \lim_{n\to\infty} f_{a,b}(n) \qquad f_{a,b}(n) := \frac{1}{\#\mathcal{M}_{a,b}(n)} \sum_{M\in\mathcal{M}_{a,b}(n)} \mathrm{w}(M)\,. \tag{24}$$

Any single $\delta(a,b)$ can be computed effectively because $f_{a,b}(n)$ is independent of n for $n > \max\{n_0, a+b\}$. Indeed, we have $f_{a,b}(n+1) = f_{a,b}(n)$ because any lift of $M \in \mathcal{M}_{a,b}(n)$ to $\mathcal{G}(n+1)$ belongs to $\mathcal{M}_{a,b}(n+1)$ and hence all matrices in $\mathcal{M}_{a,b}(n)$ have the same number of lifts to $\mathcal{M}_{a,b}(n+1)$, namely $\#\mathbb{T}$. We also use the fact (Lemma 25) that $\mathrm{w}(M)$ only depends on M modulo ℓ^{n_0}. We shall repeatedly use the following fact: if we have

$$\#\{M \in \mathcal{M}_{a,b}(n) : M \equiv M_0 \pmod{\ell^{n_0}}\} = \frac{\#\mathcal{M}_{a,b}(n)}{\#\mathcal{M}_{a,b}(n_0)} \quad \forall M_0 \in \mathcal{M}_{a,b}(n_0) \tag{25}$$

for some $n > \max\{n_0, a+b\}$ then by Lemma 25 we also have

$$\delta(a,b) = f_{a,b}(n_0) = \frac{1}{\#\mathcal{M}_{a,b}(n_0)} \sum_{M_0\in\mathcal{M}_{a,b}(n_0)} \mathrm{w}(M_0)\,. \tag{26}$$

If $\mathcal{G}$ is open either in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or in the normalizer of a split/nonsplit Cartan: By [16, Theorem 27 (i)] we know that (25) holds and hence $\delta(a,b) = f_{a,b}(n_0)$. Since $\mathcal{M}_{a,b}(n_0) \neq \emptyset$, we get

$$\delta(a,b) = \begin{cases} 1 & \text{if } a \geqslant n_0 \\ \delta(a, n_0 - a) & \text{if } a+b \geqslant n_0 > a \end{cases} \tag{27}$$

because for $a \geqslant n_0$ the only matrix in $\mathcal{M}_{a,b}(n_0)$ is the identity and $\mathrm{w}(I) = 1$, while for $b \geqslant n_0 - a > 0$ the sets $\mathcal{M}_{a,b}(n_0)$ and $\mathcal{M}_{a,n_0-a}(n_0)$ coincide by [16, Proposition 32]. The assertion easily follows.

If $\mathcal{G}$ is open in the normalizer N of a Cartan subgroup C which is neither split nor nonsplit: We suppose $n_0 \geqslant 2$, and let $(0,d)$ be the parameters of C (this means that C is the group of units of the ring $\mathbb{Z}_\ell[x]/(x^2-d)$, see also [16, Section 2.3]). Recall that finitely many pairs (a,b) can be treated individually, so we restrict to $a+b > n_0$ and have $\delta(a,b) = f_{a,b}(a+b+1)$.

Write $C_{a,b} := \mathcal{M}_{a,b} \cap C$ and $C'_{a,b} := \mathcal{M}_{a,b} \cap (N \setminus C)$, and recall from [16, Proposition 26] that $C'_{a,b} = \emptyset$ for $a \geqslant 1$ if ℓ is odd and for $a \geqslant 2$ if $\ell = 2$. By [16, Theorems 27 and 28], a necessary condition for (25) not to hold is that both $C_{a,b}(n_0)$ and $C'_{a,b}(n_0)$ are non-empty, and hence $a = 0$ if ℓ is odd and $a \in \{0,1\}$ if $\ell = 2$.

The case when d is not a square in $\mathbb{Z}_\ell^\times$. By [16, Lemma 37] we know that for any fixed a the set $C_{a,b}$ is empty for b sufficiently large (and the result is effective). In particular (25) may fail only for finitely many and explicitly computable pairs (a,b), which we may individually consider. So we may suppose $\delta(a,b) = f_{a,b}(n_0)$.

Provided that $C_{a,b}$ is empty, $f_{a,b}(n_0)$ is independent of b for $b > n_0$: this follows from [16, Theorem 31 (ii)] because in this reference the set $\mathcal{N}_{a,b}(n_0)$ has this property. Moreover, if $a \geqslant n_0$ then $f_{a,b}(n_0) = 1$ because $\mathcal{M}_{a,b}(n_0) = \{I\}$. The assertion easily follows.

The case when d is a square in $\mathbb{Z}_\ell$. For $a \geqslant 2$ we have $C'_{a,b} = \emptyset$, thus (25) and hence (26) hold. By [16, Lemmas 37 (iii) and 38] we can deal with this case as above, so suppose $a \in \{0, 1\}$. The number of lifts to $\mathcal{M}_{a,b}(n+1)$ of a matrix M in $\mathcal{M}_{a,b}(n)$ depends at most on whether M belongs to the trivial/nontrivial coset of C in N (see [16, Theorem 28]), so we have:

$$\sum_{M \in \mathcal{M}_{a,b}(n)} \mathrm{w}(M) = \sum_{M_0 \in C_{a,b}(n_0)} \mathrm{w}(M_0) \, \frac{\#C_{a,b}(n)}{\#C_{a,b}(n_0)} + \sum_{M_0 \in C'_{a,b}(n_0)} \mathrm{w}(M_0) \, \frac{\#C'_{a,b}(n)}{\#C'_{a,b}(n_0)}. \tag{28}$$

For n sufficiently large ($n > \max\{n_0, a+b\}$ suffices) we have $\#C'_{a,b}(n)/\#\mathcal{M}_{a,b}(n) = \mu(C'_{a,b})/\mu(\mathcal{M}_{a,b})$ and by [16, Corollary 41] this equals some constant c_a for all sufficiently large b (the bound is effective). So by (28) the following holds for all sufficiently large b:

$$\delta(a,b) = \sum_{M_0 \in C_{a,b}(n_0)} \mathrm{w}(M_0) \, \frac{1 - c_a}{\#C_{a,b}(n_0)} + \sum_{M_0 \in C'_{a,b}(n_0)} \mathrm{w}(M_0) \, \frac{c_a}{\#C'_{a,b}(n_0)}.$$

For any fixed a, the sets $C_{a,b}(n_0)$ and $C'_{a,b}(n_0)$ are independent of b for b large enough (and the bound is effective), see [16, Lemma 39] and [16, Theorem 31 (ii)]. We deduce that $\delta(0,b)$ and $\delta(1,b)$ are constant for all sufficiently large b, with an effective bound. The assertion easily follows. □

Proof of Theorem 5. We show that the right-hand side of (23) is an effectively computable rational number whose (minimal) denominator satisfies the property given in the statement. By Lemma 10, the integer constant $\mathrm{c}_{\mathrm{Kummer}}$ is defined in terms of n_0 (effectively computable by Remark 15) and $\#\operatorname{Gal}(K_{\alpha,n_0}/K_{n_0})$. Since this Galois group is computable, the constant $\mathrm{c}_{\mathrm{Kummer}}$ is an explicitly computable power of ℓ and we are left to investigate the sum in (23).

By [16, Theorem 1] and Proposition 34 we can partition $\mathbb{N}^2$ into finitely many (explicitly computable) admissible sets S such that for each of them there is an (explicitly computable) rational constant $c_S \geqslant 0$ satisfying

$$\mu(\mathcal{M}_{a,b}) \cdot \delta(a,b) \cdot \ell^{-2a-b} = c_S \cdot \ell^{-ta-2b} \tag{29}$$

for every $(a,b) \in S$, where the constant t is as in the statement of the theorem. The sum in (23), restricted to the pairs $(a,b) \in S$, then becomes

$$c_S \cdot \sum_{a \in S_1} \ell^{-ta} \cdot \sum_{b \in S_2} \ell^{-2b} \tag{30}$$

where the sets S_1, S_2 are finite or have a finite complement in $\mathbb{N}$. We can explicitly evaluate the geometric series, and each sum is a rational number whose denominator divides a power of ℓ times $\ell^t - 1$ or $\ell^2 - 1$. We conclude by proving that, up to powers of ℓ, the minimal denominator of c_S divides $\#\,\mathcal{G}(n)$ for some $n \geqslant 1$ (this is enough to establish the proposition since $\#\,\mathcal{G}(n)$ divides $\#\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) = \ell(\ell^2-1)(\ell-1)$ up to a power of ℓ). Consider [16,

Lemma 25], formula (24) and the assertion following it: if $c_S \neq 0$ we can fix $(a,b) \in S$ and take n sufficiently large ($n > \max(n_0, a+b)$ suffices) so that we have

$$\mu(\mathcal{M}_{a,b}) \cdot \delta(a,b) = \mu(\mathcal{M}_{a,b}(n)) \cdot f_{a,b}(n) = \frac{\#\mathcal{M}_{a,b}(n)}{\#\,\mathcal{G}(n)} \cdot \frac{1}{\#\mathcal{M}_{a,b}(n)} \sum_{M \in \mathcal{M}_{a,b}(n)} \mathrm{w}(M)\,. \tag{31}$$

Since $\mathcal{M}_{a,b}(n)$ is a finite set and $\mathrm{w}(M)$ is a power of ℓ, we are done. □

Proof of Theorem 6. Consider the proof of Theorem 5, and in particular (30). Firstly, we need to bound the ℓ-adic valuation of the minimal denominator of c_S. If we choose $(a_0, b_0) \in S$ such that $a_0 + b_0$ is minimal and set $n_S := \max(n_0, a_0 + b_0) + 1$, then by (29), by (31) and by Lemma 25 we find that the ℓ-adic valuation of the minimal denominator of c_S is at most $v_\ell(\#\mathcal{G}(n_S)) + 2(n_S - 1)$.

Secondly, we have to bound the ℓ-adic valuation of the denominator of the geometric series in (30): this is at most $ta_S + 2b_S$, where $(a_S, b_S) \in S$ and if S_1, S_2 are finite we choose the largest element while if they are infinite we choose the smallest element.

Putting things together, to bound the ℓ-adic valuation of the minimal denominator of $\mathrm{Dens}_\ell(\alpha)$, we only have to bound (uniformly in S) the number

$$(6n_S - 5) + (ta_S + 2b_S)\,.$$

If $\mathcal{G}$ is open in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or in the normalizer of a split/nonsplit Cartan, then we choose the admissible sets $S = S_1 \times S_2$ according to the case distinction of [16, Proposition 33] and of (27): we take $\mathbb{Z}_{\geqslant n_0} \times \{0\}$, $\mathbb{Z}_{\geqslant n_0} \times \mathbb{Z}_{\geqslant 1}$, the sets $\{(a,b)\}$ with $a \leqslant n_0 - 1, b \leqslant n_0 - 1 - a$, the sets $\{a\} \times \mathbb{Z}_{\geqslant n_0 - a}$ with $a \leqslant (n_0 - 1)$. The value of n_S can be bounded by $n_0 + 2$. The value of $ta_S + 2b_S$ can be bounded by $(t+2)n_0$. We have thus found:

$$v_\ell(\mathrm{Dens}_\ell(\alpha)) \geqslant -((8+t)n_0 + 7)\,. \tag{32}$$

For $\mathcal{G}$ open in the normalizer of a ramified Cartan subgroup (whose parameters are then $(0,d)$ for some non-zero integer d), for simplicity we only show that the bound exists. We first of all work with the level $n_0 + v_\ell(d) + 1$ in place of n_0 (so that this level is also good for the other Cartan groups considered in [16, Lemmas 37,38], and such that it is at least 2, which is needed in this case for $\ell = 2$). The admissible sets used in Proposition 34 are defined in terms of n_0 and $v_\ell(d)$, and the same holds for those needed for classifying $\mu(\mathcal{M}_{a,b})$, see [16, Lemmas 37, 38 and Theorem 40]. Thus combining all these partitions the values of n_S and of (a_S, b_S) can be bounded in terms of n_0 and $v_\ell(d)$. □

6.2. **Surjective arboreal representations.** The following result generalizes [13, Theorems 5.5 and 5.10], which correspond to the special case $d = 0$. The expression $1 - \ell^{1-d}/(\ell^2 - 1)$ is the density for the multiplicative group, see [22, Theorem 1].

Theorem 35. *Let A/K be an elliptic curve, and let $\alpha \in A(K)$ be a point of infinite order. Fix a prime number ℓ. Suppose that for all $N > n \geqslant 1$ the fields $K_{\alpha,n}$ and K_N are linearly disjoint over K_n. Also suppose that there is some integer $d \geqslant 0$ satisfying $[K_{\alpha,n} : K_n] = \ell^{2\max(n-d,0)}$ for every $n \geqslant 1$.*

(1) *If the image of the ℓ-adic representation attached to A is $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we have:*

$$\mathrm{Dens}_\ell(\alpha) = 1 - \frac{\ell^{1-d} \cdot (\ell^3 - \ell - 1)}{(\ell^2 - 1) \cdot (\ell^3 - 1)}\,.$$

(2) *If the image of the ℓ-adic representation attached to A is either a split or a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we respectively have:*

$$\mathrm{Dens}_\ell(\alpha) = \Big(1 - \frac{\ell^{1-d}}{\ell^2 - 1}\Big)^2 \qquad \mathrm{Dens}_\ell(\alpha) = 1 - \frac{\ell^{2(1-d)}}{\ell^4 - 1}\,.$$

(3) *If the image of the ℓ-adic representation attached to A is the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ which is split or nonsplit, we have:*

$$\mathrm{Dens}_\ell(\alpha) = \frac{1}{2} \cdot \Big(1 - \frac{\ell^{1-d}}{\ell^2 - 1}\Big) + \frac{1}{2} \cdot \begin{cases} \Big(1 - \dfrac{\ell^{1-d}}{\ell^2 - 1}\Big)^2 & \textit{for a split Cartan} \\ \Big(1 - \dfrac{\ell^{2(1-d)}}{\ell^4 - 1}\Big) & \textit{for a nonsplit Cartan}\,. \end{cases}$$

Proof. Writing a closed formula for (21) amounts to evaluating some simple geometric series, because in [16, Section 1] we have explicit formulas for the measures $\mu(\mathcal{M}_{a,b})$. □

One can easily write analogous parametric formulas for the simultaneous reductions of many points: for $i = 1, \dots, n$ consider elliptic curves A_i/K and points $\alpha_i \in A(K)$ of infinite order. The density of primes $\mathfrak{p}$ such that the order of $(\alpha_i \bmod \mathfrak{p})$ is coprime to ℓ for every i is exactly the density $\mathrm{Dens}_\ell(\alpha)$ for the point $\alpha = (\alpha_1, \dots, \alpha_n)$ in the product $\prod_i A_i$.

6.3. **Examples for Theorem 35.** We tested the formulas of Theorem 35 in the examples below: the exact value of $\mathrm{Dens}_\ell(\alpha)$ was always in excellent agreement with a numerical approximation computed with SAGE (by restricting to primes up to 10^5).

For the elliptic curve $E : y^2 + y = x^3 - x$ over $\mathbb{Q}$ and the point $\gamma = (0, 0)$, the ℓ-arboreal representation is surjective onto $T_\ell(E) \rtimes \mathrm{GL}_2(\mathbb{Z}_\ell)$ for every ℓ [13, Example 5.4] (notice that E has trivial geometric endomorphism ring). We have:

ℓ	2			3			5		7	
α	γ	2γ	4γ	γ	3γ	9γ	γ	5γ	γ	7γ
$\mathrm{Dens}_\ell(\alpha)$	$\frac{11}{21}$	$\frac{16}{21}$	$\frac{37}{42}$	$\frac{139}{208}$	$\frac{185}{208}$	$\frac{601}{624}$	$\frac{2381}{2976}$	$\frac{2857}{2976}$	$\frac{14071}{16416}$	$\frac{16081}{16416}$

We now consider two examples with (potential) complex multiplication. For the elliptic curve $E : y^2 = x^3 + 3x$ over $\mathbb{Q}$, which has potential CM by the field $\mathbb{Q}(i)$, and for the point $\gamma = (1, -2)$, the 5-adic representation is surjective onto the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_5)$, and the Kummer extensions are as large as possible [13, Example 5.11]. We then have $\mathrm{Dens}_5(\gamma) = 817/1152$ and $\mathrm{Dens}_5(5\gamma) = 1081/1152$.

For the elliptic curve $E : y^2 = x^3 + 3$ over $\mathbb{Q}$ (which has potential CM by the field $\mathbb{Q}(\zeta_3)$) and the point $\gamma = (1, 2)$, the 2-adic representation is surjective onto the normalizer of a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$, and the Kummer extensions are as large as possible [13, Example 5.12]. So we have $\mathrm{Dens}_2(\gamma) = 8/15$, $\mathrm{Dens}_2(2\gamma) = 4/5$ and $\mathrm{Dens}_2(4\gamma) = 109/120$.

6.4. **Example (non-surjective mod 3 representation).** Consider the non-CM elliptic curve $E : y^2+y = x^3+6x+27$ over $\mathbb{Q}$ [33, label 153.b2] and the point of infinite order $\alpha = (5, 13)$. The image $\mathcal{G}$ of the 3-adic representation is open in $\mathrm{GL}_2(\mathbb{Z}_3)$ and we have

$$\mathcal{G}(1) = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \rangle$$

so that $\mathcal{G}(1)$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ of order 6. The 9-division polynomial of E has an irreducible factor of degree 27 whose splitting field has degree $2 \cdot 3^5$. Since the 9-division polynomial factors completely over $\mathbb{Q}(E[9])$, we deduce

$$2 \cdot 3^5 \mid [\mathbb{Q}(E[9]) : \mathbb{Q}] = [\mathbb{Q}(E[9]) : \mathbb{Q}(E[3])] \cdot [\mathbb{Q}(E[3]) : \mathbb{Q}] \mid 3^4 \cdot 6$$

and hence we have $[\mathbb{Q}(E[9]) : \mathbb{Q}(E[3])] = 3^4$. By Theorem 14, $\mathcal{G}$ is the inverse image of $\mathcal{G}(1)$ in $\mathrm{GL}_2(\mathbb{Z}_3)$. We then have $[\mathrm{GL}_2(\mathbb{Z}_3) : \mathcal{G}] = 8$, and one can check $\mu(\mathcal{M}_{0,0}(1)) = 0$. From [16, Proposition 32] we get $\mu(\mathcal{M}_{a,b}(1)) = 1/6$ for $a > 0$ and $\mu(\mathcal{M}_{0,b}(1)) = 5/6$ for $b > 0$. By [16, Proposition 33] we then obtain

$$\mu(\mathcal{M}_{a,b}) = \begin{cases} 0 & \text{if } a = b = 0 \\ 5 \cdot 3^{-b-1} & \text{if } a = 0, b > 0 \\ 8 \cdot 3^{-4a} & \text{if } a > 0, b = 0 \\ 32 \cdot 3^{-4a-b-1} & \text{if } a > 0, b > 0\,. \end{cases}$$

We show below that the image of the 3-arboreal representation of α is $T_3E \rtimes \mathcal{G}$; it follows that

$$\mathrm{Dens}_3(\alpha) = \sum_{a,b \geqslant 0} \mu(\mathcal{M}_{a,b}) 3^{-2a-b} = \frac{23}{104}$$

and we can similarly deal with the points 3α and 9α:

Point	α	3α	9α
Dens_3	$23/104$ $0.22115\ldots$	77/104 $0.74038\ldots$	95/104 $0.91346\ldots$
empirical density (primes up to 10^5)	0.22116	0.73806	0.91126

To prove that the image of the arboreal representation is $T_3E \rtimes \mathcal{G}$ we apply Theorem 14 with $n = 1$. We need to verify $[K_{\alpha,2} : K_{\alpha,1}] = 3^6$: one computes without difficulty $[K_{\alpha,1} : \mathbb{Q}] = 2 \cdot 3^3$, and we know $[K_2 : \mathbb{Q}] = 2 \cdot 3^5$, so we are left to check $[K_{2,\alpha} : K_2] = 3^4$. One divisibility is clear, so let us prove that 3^4 divides the degree of $K_{2,\alpha}$ over K_2.

Denote by L the field (of degree 3^4) generated over $\mathbb{Q}$ by a root of the 9-division polynomial of α. Since $K_{\alpha,2} \supseteq LK_2$, it suffices to show that L and K_2 are linearly disjoint over $\mathbb{Q}$. If not, exploiting the structure of the Galois group $\mathrm{Gal}(K_2/\mathbb{Q})$ we see there would be a subfield of $L \cap K_2$ of degree 3 over $\mathbb{Q}$. However, this field cannot exist because one can test with SAGE that the 9-division polynomial of α is irreducible over all subextensions of $\mathbb{Q}(E[9])$ of degree 3 over $\mathbb{Q}$.

6.5. **Example (index 3 in the normalizer of a split Cartan).** Consider the elliptic curve $y^2 + y = x^3 + 7140$ over $\mathbb{Q}$ [33, label 1521.b2], which has potential complex multiplication by $\mathbb{Z}[\zeta_3]$. Consider the point of infinite order $\alpha = (56, 427)$. The image $\mathcal{G}$ of the 13-adic Galois

representation is properly contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_{13})$: the image $\mathcal{G}(1)$ of the modulo-13 representation is generated by the matrices

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

thus it is a group of order 96 (and index 3) in the full normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/13\mathbb{Z})$, and one can check that $\mathcal{G}$ is the inverse image of $\mathcal{G}(1)$ in $\mathrm{GL}_2(\mathbb{Z}_{13})$. We use some notation from [16], see especially Theorem 4 in *loc. cit.*. A direct computation gives $\mu^C_{0,0}(1) = 41/48$, $\mu^C_{0,1}(1) = 1/8$ and hence $\mu_{a,b} > 0$ for every $a, b \geqslant 0$: we may then apply [16, Propositions 32-33]. A direct computation gives $\mu^*_{0,0}(1) = 11/12$, $\mu^*_{0,1}(1) = 1/12$, and we can apply [16, Theorem 40]. So we have

$$\mu^C_{a,b} = \begin{cases} \frac{41}{48} & \text{if} \quad a = b = 0 \\ \frac{3}{2} \cdot 13^{-b} & \text{if} \quad a = 0, b \geqslant 1 \\ 3 \cdot 13^{-2a} & \text{if} \quad a \geqslant 1, b = 0 \\ 6 \cdot 13^{-2a-b} & \text{if} \quad a \geqslant 1, b \geqslant 1 \end{cases} \quad \text{and} \quad \mu^*_{a,b} = \begin{cases} 11/12 & \text{if} \quad a = 0, b = 0 \\ 13^{-b} & \text{if} \quad a = 0, b \geqslant 1 \\ 0 & \text{if} \quad a > 0 \end{cases}$$

which by [16, Theorem 4] determines $\mu(\mathcal{M}_{a,b}) = \frac{1}{2}(\mu^C_{a,b} + \mu^*_{a,b})$. We claim that the image of the 13-arboreal representation of α is $T_{13}E \rtimes \mathcal{G}$, so we have

$$\mathrm{Dens}_{13}(\alpha) = \sum_{a,b \geqslant 0} \mu(\mathcal{M}_{a,b}) \cdot 13^{-2a-b} = 1 - \frac{36270}{(13^2-1)^2(13-1)}$$

and we can similarly deal with the point 13α:

Point	α	13α
Dens_{13}	$16801/18816$ $0.89291\ldots$	18649/18816 $0.99112\ldots$
empirical density	(primes up to 10^5) 0.89322	(primes up to 10^6) 0.99131

The claim can be proven by applying [13, Theorem 3.4] once we have checked its two assumptions. Firstly, $E[13]$ is an irreducible $\mathcal{G}(1)$-module and hence $E[13]^{\mathcal{G}(1)} = \{0\}$. We make use of [13, Lemmas 3.6 and 3.7]. We know $\alpha \notin 13E(\mathbb{Q})$ because α generates $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$. So we are left to prove that for $n \geqslant 1$ there is no nonzero homomorphism of $\mathcal{G}(1)$-modules between $J_n := \ker(\mathcal{G}(n+1) \to \mathcal{G}(n))$ (where the action is conjugation) and $E[13]$ (with the usual Galois action). Such a homomorphism would be surjective (the image is a non-trivial $\mathcal{G}(1)$-submodule of $E[13]$), and hence also injective because $\#J_n = 13^2$. This is not possible because $E[13]$ is irreducible and J_n has the 1-dimensional submodule $\langle (1 + 13^n)I \rangle$.

7. Universality of denominators

This Section is devoted to proving Theorem 3. For any given dimension there are only finitely many possible values for the first Betti number, so we prove instead:

Theorem 36. *Fix $b \geqslant 1$. There exists a polynomial $p_b(t)$ such that whenever K is a number field and A/K is the product of an abelian variety and a torus with first Betti number b, then for all prime numbers ℓ and for all $\alpha \in A(K)$ we have $\mathrm{Dens}_\ell(\alpha) \cdot p_b(\ell) \in \mathbb{Z}[1/\ell]$.*

7.1. **Preliminaries.** Fix an algebraic subgroup G of $\mathrm{GL}_{b,\mathbb{Q}_\ell}$. We set $\mathrm{G}(\mathbb{Z}_\ell) := \mathrm{G}(\mathbb{Q}_\ell) \cap \mathrm{GL}_b(\mathbb{Z}_\ell)$ and define $\mathrm{G}(n)$ as the reduction modulo ℓ^n of $\mathrm{G}(\mathbb{Z}_\ell)$. There is a rational constant $c(\mathrm{G})$ such that $\#\,\mathrm{G}(n) = c(\mathrm{G})\ell^{n\cdot\dim(\mathrm{G})}$ holds for all sufficiently large n. We also introduce the polynomial

$$gl_b(t) := \prod_{k=0}^{b-1}(t^b - t^k),$$

which satisfies $\#\,\mathrm{GL}_b(\mathbb{Z}/\ell\mathbb{Z}) = gl_b(\ell)$ for all primes ℓ.

Lemma 37. *We have $c(\mathrm{G})^{-1}\cdot gl_b(\ell) \in \mathbb{Z}[1/\ell]$ and $\#\,\mathrm{G}(n)^{-1}gl_b(\ell) \in \mathbb{Z}[1/\ell]$ for every $n \geqslant 1$.*

Proof. For every sufficiently large n we have $c(\mathrm{G})^{-1}\cdot gl_b(\ell) = \ell^{nd}\cdot \#\,\mathrm{G}(n)^{-1}\cdot gl_b(\ell)$ and we may conclude because $\#\,\mathrm{G}(n)$ divides $\#\,\mathrm{GL}_b(\mathbb{Z}/\ell^n\mathbb{Z}) = gl_b(\ell)\cdot\ell^{b^2(n-1)}$. □

7.2. **Generating sets of polynomials.** Let k be any field of characteristic 0 (we will only need the result for $\mathbb{Q}_\ell$). Recall that, given a linear algebraic group G defined over k, there exists a unique maximal solvable connected subgroup of G, called the *radical* $R\,\mathrm{G}$ of G. When G is reductive, its radical is an algebraic torus, which is also the identity component of the center of G.

Definition 38. *Let G be an algebraic subgroup of $\mathrm{GL}_{b,k}$ and denote by $\rho : \mathrm{G} \to \mathrm{GL}_{b,k}$ the tautological representation. We say that G is of class $\mathcal{C}$ if it is reductive, connected, and the following holds: one can choose an isomorphism $i : \mathbb{G}^r_{m,\overline{k}} \to R(\mathrm{G})_{\overline{k}}$ such that, for every direct factor $\mathbb{G}_{m,\overline{k}}$ of $\mathbb{G}^r_{m,\overline{k}}$, the weights of the representation $\mathbb{G}_{m,\overline{k}} \xrightarrow{i} R(\mathrm{G})_{\overline{k}} \xrightarrow{\rho} \mathrm{GL}_{b,\overline{k}}$ are in $\{0,1\}$ (that is, $\overline{k}^b$ is the direct sum of the subspace on which $\mathbb{G}_{m,\overline{k}}$ acts trivially and of the subspace on which $z \in \mathbb{G}_{m,\overline{k}}(\overline{k}) = \overline{k}^\times$ acts as z).*

Remark 39. *Notice that the property of being of class $\mathcal{C}$ is not a property of the abstract group G, but rather of the inclusion $\mathrm{G} \hookrightarrow \mathrm{GL}_{b,k}$; in other words, it depends both on the abstract group G and on the choice of a faithful representation $\mathrm{G} \to \mathrm{GL}_{b,k}$. Let $\mathrm{G} \subseteq \mathrm{GL}_{b,k}$ be a group of class $\mathcal{C}$. Then $\mathrm{G}_{\overline{k}}$ is of class $\mathcal{C}$ (the group G is geometrically connected because it is connected and has a rational point* [35, Tag 04KV]*). The radical of G is of class $\mathcal{C}$ (the condition on the weights follows from the fact that the formation of the radical commutes with base change). The derived subgroup of G is of class $\mathcal{C}$ (its radical is trivial, hence the weights of its action are zero).*

Lemma 40. *There exists an integer $D(b)$ such that any group $\mathrm{G}_{\bar{k}} \subseteq \mathrm{GL}_{b,\bar{k}}$ of class $\mathcal{C}$ can be defined in $\bar{k}[x_{ij}, y]/(\det(x_{ij})y - 1)$ by finitely many polynomials of degree at most $D(b)$.*

Proof. We know that $\mathrm{G}_{\overline{k}}$ is the almost-direct product of its derived group S (which is semisimple) and of its radical T. Notice that a change of basis in $\mathrm{GL}_{b,\bar{k}}$ changes neither the degree nor the number of the equations defining a subgroup, so we can work up to conjugation.

We first prove the statement for S. Clearly, it suffices to show that (up to conjugation) there are only finitely many semisimple subgroups of $\mathrm{GL}_{b,\bar{k}}$ (each of them will be described by a finite set of equations, and we can take the maximum over all such semisimple groups of the

degrees of the defining polynomials). This finiteness is well-known, and can be shown for example by the Lefschetz principle: this allows us to work over $\mathbb{C}$, at which point it suffices to remark that there are only finitely many conjugacy classes of semi-simple Lie subalgebras of $\mathrm{Lie}(\mathrm{GL}_{b,\mathbb{C}})$ [26, Section 12 (a)] and to invoke the correspondence between subgroups of $\mathrm{GL}_{b,\mathbb{C}}$ and subalgebras of $\mathrm{Lie}(\mathrm{GL}_{b,\mathbb{C}})$.

The statement is also true for T. Indeed by our assumption that G is of class $\mathcal{C}$ we can fix an isomorphism $i : \mathbb{G}_m^r \cong T$ in such a way that, up to conjugation, the action of $\mathbb{G}_m^r$ on $\overline{k}^b$ is given by

$$(z_1, \dots, z_r) \mapsto \mathrm{diag}(z_1^{a_{11}} \cdots z_r^{a_{1r}}, \dots, z_1^{a_{b1}} \cdots z_r^{a_{br}})$$

where the exponents a_{ij} are in $\{0, 1\}$. In these coordinates, the equations defining T inside $\mathrm{GL}_{b,\overline{k}}$ are then $x_{ij} = 0$ for $i \neq j$ and the finitely many equations of bounded degree $\prod_{i=1}^b x_{ii}^{v_i} = 1$, where the vector (v_i) ranges over a basis of $\ker(a_{ij})$ as a $\mathbb{Z}$-module.

To conclude, we make use of the theory of complexity developed in [5]: roughly speaking, one says that a variety has complexity bounded by M if it can be defined by at most M polynomials, of degree at most M, in an affine or projective space of dimension at most M; there is a similar notion of complexity for regular maps between varieties. We simply say that our varieties, or maps, have *bounded complexity* to mean that their complexity can be bounded above by a quantity depending only on b. In [5] the authors show that the notion of complexity enjoys various nice properties: what is essential for us is that if V is a variety of bounded complexity and ϕ is a regular map, also of bounded complexity, then one can give a bound on the complexity of $\phi(M)$. We can now finish the proof of the lemma: we have shown that S and T have bounded complexity and hence the same holds for $S \times T$ [5, Definition 3.1 and Remarks]. Since the product map $\mathrm{GL}_{b,\overline{k}} \times \mathrm{GL}_{b,\overline{k}} \to \mathrm{GL}_{b,\overline{k}}$ has bounded complexity [5, Definition 3.3], the same holds by [5, Lemma 3.4] for the restriction to $S \times T$ and for its image $\mathrm{G}_{\overline{k}}$, and this is what we needed to show. □

Theorem 41. *Let* $\mathrm{G} \subseteq \mathrm{GL}_{b,k}$ *be a group of class* $\mathcal{C}$*. There exist integers* $D(b), N(b)$ *(depending only on* b*) such that* G *can be defined in* $R := k[x_{ij}, y]/(\det(x_{ij})y - 1)$ *by at most* $N(b)$ *polynomials of degree at most* $D(b)$*.*

Proof. It suffices to show that there are defining polynomials of degree at most $D(b)$ because the polynomials in $k[x_{ij}, y]$ of a given degree form a finite dimensional vector space (whose dimension can be bounded purely in terms of the number of variables and of the degree, hence ultimately in terms of b). We let I be the ideal of G in R and $I_{\overline{k}} = I \otimes \overline{k}$ the ideal of $\mathrm{G}_{\overline{k}}$ in $R \otimes \overline{k}$. By Remark 39 and Lemma 40, the ideal $I_{\overline{k}}$ is defined by finitely many polynomials f_n of degree at most $D(b)$. Fix a finite, Galois extension L of k that contains all their coefficients, and let $\{t_m\}$ be a basis of L over k. The polynomials $\mathrm{tr}_{L/k}(t_m f_n)$ (the trace is taken coefficientwise) are in I and have degree bounded by $D(b)$; we claim that they generate I. To see this, fix an element $f \in I$ and notice that the polynomials f_n generate $I \otimes L$ in $R \otimes L$, which gives the existence of elements $a_n \in R \otimes L$ such that $f = \sum_{n=1}^r a_n f_n$. Moreover, $\mathrm{Gal}(L/k)$ acts trivially on the coefficients of f, so that we get

$$[L : k]f = \sum_{\sigma \in \mathrm{Gal}(L/k)} {}^{\sigma} f = \mathrm{tr}_{L/k}(f) = \sum_{n=1}^{r} \mathrm{tr}_{L/k}(a_n \cdot f_n).$$

Finally, writing $a_n = \sum_{m=1}^{[L:k]} t_m a_{m,n}$ with $a_{m,n} \in R$, we obtain

$$f = \frac{1}{[L:k]} \sum_{n=1}^{r} \sum_{m=1}^{[L:k]} \mathrm{tr}_{L/k}(t_m a_{m,n} \cdot f_n) = \frac{1}{[L:k]} \sum_{n=1}^{r} \sum_{m=1}^{[L:k]} a_{m,n} \, \mathrm{tr}_{L/k}(t_m \cdot f_n),$$

which shows that f is in the ideal generated by $\{\mathrm{tr}_{L/k}(t_m f_n)\}$. □

7.3. **The image of the ℓ-adic representation.** Let A be the product of an abelian variety and a torus defined over a number field. Let $\mathcal{G}_{\mathrm{Zar}}$ be the Zariski closure in $\mathrm{GL}_{b,\mathbb{Q}_\ell}$ of the image of the ℓ-adic Galois representation attached to A, where as above b is the first Betti number of A.

Proposition 42. *The identity component of $\mathcal{G}_{\mathrm{Zar}}$ is of class $\mathcal{C}$.*

Proof. The group $\mathcal{G}^0_{\mathrm{Zar}}$ is clearly connected, and it is the product of the identity components of the ℓ-adic monodromy groups associated with the torus and with the abelian variety. The claim is easy to show for the torus: passing to a finite extension we can assume that the torus is split (of rank r), so that the corresponding Galois representation is given by the cyclotomic character, acting diagonally on $\mathbb{Q}_\ell^r$; from this it is easy to deduce that the weight of the tautological representation is 1. We may then assume that A is an abelian variety, and hence $\mathcal{G}^0_{\mathrm{Zar}}$ is reductive by a celebrated theorem of Faltings. We are left to understand the tautological representation ρ of the reductive group $(\mathcal{G}^0_{\mathrm{Zar}})_{\overline{\mathbb{Q}_\ell}}$ on $\overline{\mathbb{Q}_\ell}^b$. Since ρ is the direct sum of irreducible representations, we may consider the weight of every irreducible factor ρ' separately. The weights of the action of the radical are in $\{0,1\}$ by the discussion following [24, Definition 4.1]: notice that by [24, Theorem 5.10] the pair given by $\mathcal{G}^0_{\mathrm{Zar}}$ together with its tautological representation is a weak Mumford-Tate pair in the sense of [24, Definition 4.1]. □

Proposition 43. *There is a non-zero integer $z(b)$, depending only on the Betti number b, such that the number of connected components of $\mathcal{G}_{\mathrm{Zar}}$ divides $z(b)$.*

Proof. For every prime number p let $\rho_p : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_b(\mathbb{Z}_p)$ be the p-adic representation attached to A, and call $\mathcal{G}_{\mathrm{Zar},p}$ the Zariski closure of its image. Let K^{conn} be the finite extension of K corresponding to $\rho_p^{-1}\left(\mathcal{G}^0_{\mathrm{Zar},p}(\mathbb{Q}_p) \cap \mathrm{GL}_b(\mathbb{Z}_p)\right)$. The degree $[K^{\mathrm{conn}} : K]$ is the number of connected components of $\mathcal{G}_{\mathrm{Zar},p}$. It is known by work of Serre [30] (cf. also [15, Introduction]) that K^{conn} is independent of p, so the degree $[K^{\mathrm{conn}} : K]$ divides the greatest common divisor of the supernatural numbers $\#\,\mathrm{GL}_b(\mathbb{Z}_p) = p^\infty \cdot \#\,\mathrm{GL}_b(\mathbb{F}_p)$, which is an integer depending only on b. □

7.4. **A theorem of Macintyre.** We apply a result of Macintyre [17] which – roughly speaking – is a uniformity statement for integrals over L_P-definable sets. L_P is a first-order language (in the sense of logic) that is similar to Denef's language used in [8]. It is obtained from the language of rings (i.e. a language with $0, 1, +, \cdot, -$) by adding 1-ary predicates P_n, for $n \geqslant 2$. Since L_P contains the language of rings, one can in particular write formulas in L_P that involve polynomials in the variables; we shall use the obvious notation x^n as a short-hand for multiplication iterated n times. We make $\mathbb{Q}_\ell$ an L_P-structure by interpreting P_n as the set of n-th powers in $\mathbb{Q}_\ell$ (i.e. $P_n(x)$ is true iff x is an n-th power in $\mathbb{Q}_\ell$). The advantage of this language for number-theoretical questions is that it makes it possible to express predicates

about *valuations*. For $x \in \mathbb{Q}_\ell$, we shall write as usual $v_\ell(x)$ for the ℓ-adic valuation of x, that is, the unique exponent $e \in \mathbb{Z}$ such that there exists a unit $u \in \mathbb{Z}_\ell^\times$ with $x = \ell^e u$. We start by showing that the valuation ring $\mathbb{Z}_\ell = \{x : v_\ell(x) \geqslant 0\}$ is L_P-definable:

Lemma 44. *There is a formula $\Phi(x)$ in L_P (independent of ℓ) such that, when $\mathbb{Q}_\ell$ is interpreted as an L_P-structure as above, we have $\Phi(x) \Leftrightarrow v_\ell(x) \geqslant 0$.*

Proof. Expanding the argument in [17, p.71], consider the formula $R(x, y)$ given by $P_2(1 + y^3x^4)$ and let $V := \{y : R(x, y)$ defines a valuation ring$\}$. The property $y \in V$ is expressible by a formula $\Omega(y)$ in L_P because the property of defining a valuation ring can be expressed in the language of rings. Indeed, $S \subseteq \mathbb{Q}_\ell$ is a valuation ring if and only if it is a subring that satisfies $(\forall x)(x \in S$ or $\exists x' : xx' = 1, x' \in S)$. When we interpret $\mathbb{Q}_\ell$ as an L_P-structure, $R(x, -\ell)$ defines precisely $\mathbb{Z}_\ell$. One can check that $v_\ell(x) \geqslant 0$ if and only if $(\forall y \in V)R(x, y)$: it follows that $v_\ell(x) \geqslant 0$ is equivalent to $(\forall y)(\Omega(y) \Rightarrow R(x, y))$. □

Corollary 45. *There is an L_P-formula $\Psi(x, y)$ such that, when $\mathbb{Q}_\ell$ is interpreted as an L_P-structure, we have $\Psi(x, y) \Leftrightarrow v_\ell(x) \geqslant v_\ell(y)$. Likewise, there are formulas that encode the statements $v_\ell(x) = 0$, $v_\ell(x) > v_\ell(y)$, and $v_\ell(x) = v_\ell(y) + 1$.*

Proof. Let Φ be the formula of Lemma 44. We can express $v_\ell(x) \geqslant v_\ell(y)$ by $\exists z : \Phi(z) \wedge (x = yz)$ and $v_\ell(x) = 0$ by $\exists y : \Phi(x) \wedge \Phi(y) \wedge (xy = 1)$. The property $v_\ell(z) > 0$ means $v_\ell(z) \geqslant 0 \wedge v_\ell(z) \neq 0$ while $v_\ell(x) > v_\ell(y)$ means $\exists z : v_\ell(z) > 0, x = yz$. Finally, $v_\ell(x) = v_\ell(y) + 1$ is equivalent to $v_\ell(x) > v_\ell(y)$ and $(\forall z)(v_\ell(z) > 0 \Rightarrow v_\ell(yz) \geqslant v_\ell(x))$. □

Let Ξ be a formula in L_P with $m + m'$ free variables (such a formula can be interpreted in $\mathbb{Q}_\ell$ for every prime ℓ). Define

(33)
$$\mathcal{A} := \{(X, \lambda) \in \mathbb{Q}_\ell^m \times \mathbb{Q}_\ell^{m'} : \Xi(X, \lambda)\} \qquad \text{and} \qquad \mathcal{A}(\lambda) := \{X : (X, \lambda) \in \mathcal{A}\} \subseteq \mathbb{Q}_\ell^m .$$

Such a set $\mathcal{A}$ is said to be L_P-definable. We also consider functions $\mathbb{Q}_\ell^n \to \mathbb{Z} \cup \{+\infty\}$. We deal only with L_P-*simple* functions of the form $v_\ell(f(x_1, \dots, x_n))$ where $f \in \mathbb{Z}[x_1, \dots, x_n]$ (see [17, Definition after Lemma 18], replacing L_{PD} by L_P).

Theorem 46. *(Macintyre* [17]*) Suppose $\mathcal{A}$ is an L_P-definable set, and α, α' are L_P-simple functions. We have*

$$\int_{\mathcal{A}(\lambda)} \ell^{-\alpha(X,\lambda)s - \alpha'(X,\lambda)}\, dX = \frac{\sum_{1 \leqslant i, i' \leqslant \varepsilon(\lambda)} \gamma_{i,i'}\, \ell^{-is - i'}}{c \prod_{1 \leqslant j < h} \left(1 - \ell^{-a_j s - a'_j}\right)}$$

whenever the integral is finite, where

1. *ε is L_P-simple with values in $\mathbb{N}$, and the $\gamma_{i,i'}$ are integers;*
2. *h is a constant independent of ℓ;*
3. *the a_j, a'_j are natural numbers, bounded by some constant τ independent of ℓ;*
4. *c divides $(\ell(\ell - 1))^m$, where m is the dimension of the integration space;*
5. *the numbers a_j, a'_j, τ, h and c, as well as the function ε, only depend on the formula defining $\mathcal{A}$ and on the polynomials defining α, α' (in particular, they are independent of λ and ℓ).*

Though not stated in this exact form, this theorem is fully proved in [17]: the main result is Corollary 2 on p.70, (2) is a direct consequence of Theorem 19 of op.cit., (3) is proved in §7.2.1, and (4) is proved in §7.2.2. The integrality of the constants a_j, a'_j provided by part (3) of the theorem will be crucial in establishing the rationality of ℓ-adic integrals in the next section: notice in particular that it implies that the denominator in the above fraction is a polynomial in ℓ^{-s} with rational coefficients.

7.5. **Rationality of ℓ-adic integrals.** Take $N := N(b), D := D(b)$ as in Theorem 41 and define the set

$$\mathcal{P} := \mathrm{Mat}_b(\mathbb{Z}_\ell) \times \left(\mathbb{Z}_\ell[x_{ij}]_{1\leqslant i,j\leqslant b,\deg\leqslant D}\right)^N \times \mathbb{Z}_\ell\,.$$

An element of $\mathcal{P}$ will be written as $\lambda := (T; f_1, \ldots, f_N; w_n)$ where $T \in \mathrm{Mat}_b(\mathbb{Z}_\ell)$, f_1 to f_N are polynomials in $\mathbb{Z}_\ell[x_{ij}]$ (for $1 \leqslant i, j \leqslant b$) of degree at most D, and w_n is an ℓ-adic integer which we only use through its valuation. For $z \in \mathbb{Z}_\ell$ we call reduction modulo z the identity map if $z = 0$ and the reduction modulo $\ell^{v_\ell(z)}$ otherwise. The set

(34)
$$\mathcal{A} = \left\{ (x, w; \lambda) \in \mathrm{Mat}_b(\mathbb{Z}_\ell) \times \mathbb{Z}_\ell \times \mathcal{P} \;\middle|\; \exists M \in \mathrm{Mat}_b(\mathbb{Z}_\ell) : \begin{array}{c} f_1(M) = \cdots = f_N(M) = 0 \\ v_\ell(\det(M)) = 0 \\ M \equiv x \pmod{w} \\ M \equiv I \pmod{w_n} \\ v_\ell(\det(TM - I)) + 1 = v_\ell(w) \end{array} \right\}$$

is L_P-definable: indeed, the vanishing of $f_i(M)$ is simply given by the vanishing of a suitable family of polynomials in the entries of M and of λ (this can be expressed in the language of rings), and the congruence conditions can be expressed in L_P by Lemma 44 and Corollary 45. We define $\mathcal{A}(\lambda)$ as in (33).

Proposition 47. *Fix $b \geqslant 1$. For every algebraic subgroup G of $\mathrm{GL}_{b,\mathbb{Q}_\ell}$ of class $\mathcal{C}$, for every integer $n \geqslant 0$, and for every $T \in \mathrm{GL}_b(\mathbb{Z}_\ell)$, there exists $\lambda \in \mathcal{P}$ such that $\mathcal{A}(\lambda)$ equals*

(35)
$$\mathcal{D}_n := \left\{ (x, w) \in \mathrm{Mat}_b(\mathbb{Z}_\ell) \times \mathbb{Z}_\ell \;\middle|\; \exists M \in \mathrm{G}(\mathbb{Z}_\ell) : \begin{array}{c} M \equiv x \pmod{w} \\ M \equiv I \pmod{\ell^n} \\ v_\ell \det(TM - I) + 1 = v_\ell(w) \end{array} \right\}.$$

Proof. By Theorem 41, there exist polynomials $f_1, \ldots, f_N$ of degree at most D which define G in $\mathrm{GL}_{b,\mathbb{Q}_\ell}$. The conditions $M \in \mathrm{Mat}_b(\mathbb{Z}_\ell)$, $v_\ell(\det(M)) = 0$ and $f_1(M) = \ldots = f_N(M) = 0$ give $M \in \mathrm{G}(\mathbb{Z}_\ell)$. The other conditions for $\mathcal{A}(\lambda)$ match those of $\mathcal{D}_n$ if we take $w_n = \ell^n$. □

Definition 48. *Let $\mathcal{D}_n$ be as in* (35)*. We set* $I_n(s) := \displaystyle\int_{\mathcal{D}_n} |w|^s \, dx \, dw\,.$

Lemma 49. *Fix $b \geqslant 1$. There exists a polynomial $r(t, u) \in \mathbb{Z}[t, u]$ such that for every ℓ, for every algebraic subgroup G of $\mathrm{GL}_{b,\mathbb{Q}_\ell}$ of class $\mathcal{C}$, for every $T \in \mathrm{GL}_b(\mathbb{Z}_\ell)$, for every integer $n \geqslant 0$ and for every real number $s > 0$ we have*

$$I_n(s) = \frac{\Psi_n(\ell^{-s})}{r(\ell^{-s}, \ell^{-1})}\,,$$

where $\Psi_n(t)$ is a polynomial in $\mathbb{Z}[1/\ell][t]$ which may depend on n, ℓ, G, T.

Proof. By Proposition 47 there exists λ such that $\mathcal{D}_n = \mathcal{A}(\lambda)$, and the integral $I_n(s)$ is finite because $|w|^s \leqslant 1$ and the integration space has finite measure. Theorem 46 (choosing $\mathcal{A}$ as in (34), $\alpha = v_\ell(w)$ and $\alpha' = 0$) then gives

$$I_n(s) = \frac{\Psi(\ell^{-s})}{c \prod_{1 \leqslant j < h} \left(1 - \ell^{-a_j s - a'_j}\right)},$$

where we have set $\Psi(t) := \sum_{1 \leqslant i, i' \leqslant \varepsilon(\lambda)} \gamma_{i,i'} \ell^{-i'} t^i \in \mathbb{Z}[1/\ell][t]$. Again by Theorem 46, the denominator divides $r(\ell^{-s}, \ell^{-1})$ up to a power of ℓ, where

$$r(t,u) := (1-u)^{b^2+1} \prod_{0 \leqslant a, a' \leqslant \tau} (1 - t^a u^{a'})^h .$$

Notice that we can reabsorb the power of ℓ in the numerator. To finish the proof, recall that τ and h only depend on the polynomial defining α (which is in particular independent of ℓ) and on the formula defining $\mathcal{A}$. Since by construction the latter depends only on b, this establishes our claim. □

7.6. **Uniform bound for the denominators.** Let G be an algebraic subgroup of $\mathrm{GL}_{b,\mathbb{Q}_\ell}$ of class $\mathcal{C}$. Fix some matrix T in $\mathrm{GL}_b(\mathbb{Z}_\ell)$. If $n, n' \geqslant 0$ and $m \geqslant 1$ are integers, we define

$$S_{n,n'}(m) := \left\{ M \bmod \ell^m \;\middle|\; \begin{array}{c} M \in \mathrm{G}(\mathbb{Z}_\ell) \\ M \equiv I \pmod{\ell^n} \\ v_\ell \det(TM - I) = n' \end{array} \right\} \tag{36}$$

and $N_{n,k} := \# S_{n,k-1}(k)$ (we also set $N_{n,0} = 0$). We consider the Poincaré series

$$P_n(t) := \sum_{k \geqslant 0} N_{n,k}\, t^k = \frac{\ell}{\ell - 1} \cdot \frac{\Psi_n(t\ell^{b^2+1})}{r(t\ell^{b^2+1}, \ell^{-1})} \tag{37}$$

where the second equality follows from Lemma 49 and the following computation:

$$\begin{aligned} I_n(s) &= \sum_{k=0}^{\infty} \ell^{-ks} \int_{\mathcal{D}_n \cap \{v_\ell(w) = k\}} dx\, dw \\ &= \sum_{k=0}^{\infty} \ell^{-ks} \left(\int_{x : (x, \ell^k) \in \mathcal{D}_n} dx \right) \left(\int_{w : v_\ell(w) = k} dw \right) \\ &= \sum_{k=0}^{\infty} \ell^{-ks} \cdot \frac{N_{n,k}}{\ell^{kb^2}} \cdot \left(\ell^{-k} - \ell^{-k-1} \right) \\ &= \frac{\ell - 1}{\ell} P_n(\ell^{-(s+1+b^2)}). \end{aligned}$$

Lemma 50. *Fix $b \geqslant 1$, and let $r(t,u)$ be as in Lemma 49. For every integer $n_0 \geqslant 0$ we have:*

$$(\ell - 1) \cdot r(\ell^{b^2-d}, \ell^{-1}) \cdot \sum_{k \geqslant n_0} \ell^{-dk-d-k} N_{n,k+1} \in \mathbb{Z}[1/\ell] .$$

Proof. We can write

$$\sum_{k\geqslant n_0} \ell^{-dk-d-k} N_{n,k+1} = \ell \cdot P_n(\ell^{-(d+1)}) - \ell \cdot \sum_{0\leqslant i\leqslant n_0} \ell^{-i(d+1)} N_{n,i}.$$

The finite sum is obviously in $\mathbb{Z}[1/\ell]$. We may conclude by applying (37):

$$\ell \cdot P_n(\ell^{-(d+1)}) \cdot (\ell-1) \cdot r(\ell^{b^2-d}, \ell^{-1}) = \ell^2 \cdot \Psi_n(\ell^{b^2-d}) \in \mathbb{Z}[1/\ell]\,.$$

□

Proposition 51. *Fix $b \geqslant 1$. There exists a polynomial $q_b(t) \in \mathbb{Z}[t]$ with the following property. If G is an algebraic subgroup of $\mathrm{GL}_{b,\mathbb{Q}_\ell}$ of class $\mathcal{C}$, $n \geqslant 0$ is an integer, and T is any matrix in $\mathrm{GL}_b(\mathbb{Z}_\ell)$, we have:*

$$q_b(\ell) \cdot \int_{\{M\in \mathrm{G}(\mathbb{Z}_\ell)\,\big|\, M\equiv I \,(\mathrm{mod}\ \ell^n)\}} \ell^{-v_\ell \det(TM-I)}\, d\mu_{\mathrm{G}(\mathbb{Z}_\ell)}(M) \ \in \mathbb{Z}[1/\ell].$$

Proof. Define $q_b(t) := gl_b(t)\cdot(t-1)\cdot r(t^{b^2-d}, t^{-1}) t^{\deg_u r(t,u)}$, where $r(t,u)$ is as in Lemma 49. Notice that if $m > \max(n, n')$ the set

$$S_{n,n'} := \left\{ M \;\middle|\; M \in \mathrm{G}(\mathbb{Z}_\ell), M \equiv I \,(\mathrm{mod}\ell^n), v_\ell \det(TM-I) = n' \right\}$$

is the inverse image in $\mathrm{G}(\mathbb{Z}_\ell)$ of the set $S_{n,n'}(m) \subseteq \mathrm{G}(m)$ from (36). In particular, if $n_0 > n$ is sufficiently large and $k \geqslant n_0$ we can write

$$\mu_{\mathrm{G}(\mathbb{Z}_\ell)}(S_{n,k}) = \frac{\#S_{n,k}(k+1)}{\#\,\mathrm{G}(k+1)} = \frac{N_{n,k+1}}{c(\mathrm{G})\ell^{d(k+1)}}.$$

For $k < n_0$ we may write instead $\mu_{\mathrm{G}(\mathbb{Z}_\ell)}\,(S_{n,k}) = \#S_{n,k}(n_0)/\#\,\mathrm{G}(n_0)$. We then have

$$\int_{\{M:M\equiv I\,(\mathrm{mod}\ \ell^n)\}} \ell^{-v_\ell \det(TM-I)}\, d\mu_{\mathrm{G}(\mathbb{Z}_\ell)}(M) = \sum_{k\geqslant n_0} \ell^{-k} \frac{N_{n,k+1}}{c(\mathrm{G})\ell^{d(k+1)}} + \sum_{k<n_0} \ell^{-k} \frac{\#S_{n,k}(n_0)}{\#\,\mathrm{G}(n_0)}\,.$$

The second sum, when multiplied by $q_b(\ell)$, gives an element of $\mathbb{Z}[1/\ell]$ by Lemma 37. For the first sum we may apply Lemmas 37 and 50. □

Proof of Theorem 36. We may assume without loss of generality that the order of α is infinite, because otherwise $\mathrm{Dens}_\ell(\alpha) \in \{0,1\}$. By Remark 9 and Theorem 1, $\mathrm{Dens}_\ell(\alpha)$ is an integral multiple of

$$\int_{\mathcal{G}} \mathrm{w}(x)\, \ell^{-v_\ell \det(x-I)}\, d\mu_{\mathcal{G}}(x)\,, \tag{38}$$

where $\mathcal{G} \subseteq \mathrm{GL}_b(\mathbb{Z}_\ell)$ is open in its Zariski closure $\mathcal{G}_{\mathrm{Zar}}$ by Proposition 18. If n is sufficiently large, we can write $\mathcal{G}$ as the disjoint union of finitely many cosets $T_i\,\mathrm{H}$, where

$$\mathrm{H} := \{x \in \mathcal{G}^0_{\mathrm{Zar}}(\mathbb{Z}_\ell) : x \equiv I \pmod{\ell^n}\}\,.$$

By Lemma 25, we may take n sufficiently large so that w is constant on $T_i\,\mathrm{H}$. We then rewrite (38) as the finite sum of terms of the form

$$\int_{T_i\,\mathrm{H}} \mathrm{w}(T_i)\, \ell^{-v_\ell \det(x-I)}\, d\mu_{\mathcal{G}}(x) = \frac{[\mathcal{G}_{\mathrm{Zar}}(\mathbb{Z}_\ell) : \mathcal{G}]}{[\mathcal{G}_{\mathrm{Zar}} : \mathcal{G}^0_{\mathrm{Zar}}]} \cdot \mathrm{w}(T_i) \cdot \int_{\mathrm{H}} \ell^{-v_\ell \det(T_i x - I)}\, d\mu_{\mathcal{G}^0_{\mathrm{Zar}}(\mathbb{Z}_\ell)}(x).$$

Since $\mathrm{w}(T_i) \in \mathbb{Z}[1/\ell]$ by Lemma 25, we may conclude by taking $p_b(t) = z(b)q_b(t)$, where $z(b)$ is as in Proposition 43 and $q_b(t) \in \mathbb{Z}[t]$ is as in Proposition 51. □

Proof of Theorem 2. Given a group $\mathcal{G}$ (the image of the ℓ-adic Galois representation attached to A) and its Zariski closure $\mathcal{G}_{\mathrm{Zar}}$, we can find integers N and D with the property that $\mathcal{G}_{\mathrm{Zar}}$ is defined by at most N polynomials of degree at most D. One can now repeat verbatim the proof of Theorem 36, replacing $N(b)$ and $D(b)$ with these N and D. □

REFERENCES

[1] J. D. Achter. Detecting complex multiplication. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 38–50. World Sci. Publ., Hackensack, NJ, 2005.

[2] A. Beilinson. p-adic periods and derived de Rham cohomology. *J. Amer. Math. Soc.*, 25(3):715–738, 2012.

[3] F. A. Bogomolov. Points of finite order on abelian varieties. *Izv. Akad. Nauk SSSR Ser. Mat.*, 44(4):782–804, 973, 1980.

[4] F. A. Bogomolov. Sur l'algébricité des représentations l-adiques. *C. R. Acad. Sci. Paris Sér. A-B*, 290(15):A701–A703, 1980.

[5] E. Breuillard, B. Green, and T. Tao. Approximate subgroups of linear groups. *Geom. Funct. Anal.*, 21(4):774–819, 2011.

[6] C. Debry and A. Perucca. Reductions of algebraic integers. *J. Number Theory*, 167:259–283, 2016.

[7] P. Deligne. Théorie de Hodge. III. *Inst. Hautes Études Sci. Publ. Math.*, 44:5–77, 1974.

[8] J. Denef. On the evaluation of certain p-adic integrals. In *Séminaire de théorie des nombres, Paris 1983–84*, volume 59 of *Progr. Math.*, pages 25–47. Birkhäuser Boston, Boston, MA, 1985.

[9] G. Faltings. p-adic Hodge theory. *J. Amer. Math. Soc.*, 1(1):255–299, 1988.

[10] M. D. Fried and M. Jarden. *Field Arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 11. Springer-Verlag Berlin Heidelberg, 3rd edition, 2008.

[11] H. Hasse. Uber die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteilbarer Ordnung mod p ist. *Math. Ann.*, 162:74–76, 1965/1966.

[12] H. Hasse. Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod. p ist. *Math. Ann.*, 166:19–23, 1966.

[13] R. Jones and J. Rouse. Galois theory of iterated endomorphisms. *Proc. Lond. Math. Soc. (3)*, 100(3):763–794, 2010. Appendix A by Jeffrey D. Achter.

[14] E. Kowalski. Some local-global applications of Kummer theory. *Manuscripta Math.*, 111(1):105–139, 2003.

[15] M. Larsen and R. Pink. A connectedness criterion for l-adic Galois representations. *Israel J. Math.*, 97:1–10, 1997.

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

[17] A. Macintyre. Rationality of p-adic Poincaré series: uniformity in p. *Ann. Pure Appl. Logic*, 49(1):31–74, 1990.

[18] A. Mattuck. Abelian varieties over p-adic ground fields. *Ann. of Math. (2)*, 62:92–119, 1955.

[19] P. Moree. Artin's primitive root conjecture—a survey. *Integers*, 12(6):1305–1416, 2012.

[20] J. Oesterlé. Réduction modulo p^n des sous-ensembles analytiques fermés de $\mathbf{Z}_p^N$. *Invent. Math.*, 66(2):325–341, 1982.

[21] A. Perucca. Prescribing valuations of the order of a point in the reductions of abelian varieties and tori. *J. Number Theory*, 129(2):469–476, 2009.

[22] A. Perucca. The order of the reductions of an algebraic integer. *J. Number Theory*, 148:121–136, 2015.

[23] A. Perucca. Reductions of 1-dimensional tori. *Int. J. Number Theory*, 13(6):1473–1489, 2017.

[24] R. Pink. l-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture. *J. Reine Angew. Math.*, 495:187–237, 1998.

[25] R. Pink. On the order of the reduction of a point on an abelian variety. *Math. Ann.*, 330(2):275–291, 2004.

[26] R. W. Richardson, Jr. A rigidity theorem for subalgebras of Lie and associative algebras. *Illinois J. Math.*, 11:92–110, 1967.
[27] J. Rouse and D. Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of galois. *Res. Number Theory*, 1:Art. 12, 34pp., 2015.
[28] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.
[29] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.
[30] J.-P. Serre. Résumé des cours de 1984-1985, Annuaire du Collge de France, 1985.
[31] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.
[32] T. Szamuely and G. Zábrádi. The p-adic Hodge decomposition according to Beilinson. *ArXiv e-prints*, June 2016. arXiv:1606.01921.
[33] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2016.
[34] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.5.1)*, 2017. `http://www.sagemath.org`.
[35] The Stacks Project Authors. *Stacks Project*. `http://stacks.math.columbia.edu`, 2017.
[36] J.-P. Wintenberger. Démonstration d'une conjecture de Lang dans des cas particuliers. *J. Reine Angew. Math.*, 553:1–16, 2002.

UNIVERSITY OF PISA, LARGO BRUNO PONTECORVO 5, 56127 PISA, ITALY

Email address: `davide.lombardo@unipi.it`

UNIVERSITY OF LUXEMBOURG. 6, AVENUE DE LA FONTE, 4364 ESCH-SUR-ALZETTE, LUXEMBOURG

Email address: `antonella.perucca@uni.lu`