ITERATED ENDOMORPHISMS OF ABELIAN ALGEBRAIC GROUPS

RAFE JONES AND JEREMY ROUSE

ABSTRACT. Given an abelian algebraic group A over a global field K, $\alpha \in A(K)$, and a prime ℓ, the set of all preimages of α under some iterate of $[\ell]$ has a natural tree structure. Using this data, we construct an "arboreal" Galois representation ω whose image combines that of the usual ℓ-adic representation and the Galois group of a certain Kummer-type extension. For several classes of A, we give a simple characterization of when ω is surjective. The image of ω also encodes information about the density of primes $\mathfrak{p}$ in K such that the order of the reduction mod $\mathfrak{p}$ of α is prime to ℓ. We compute this density in the general case for several A of interest. For example, if K is a number field, A/K is an elliptic curve with surjective 2-adic representation and $\alpha \in A(K)$, $\alpha \notin 2A(K)$, then the density of primes $\mathfrak{p}$ with α mod $\mathfrak{p}$ having odd order is 11/21.

1. INTRODUCTION

Let K be a global field, and denote by $\mathcal{O}$ the ring of integers of K if K is a number field and $K[C]$ if $K := K(C)$ is the function field of the curve C. For any quasiprojective variety V, finite morphism $\phi : V \to V$, and point α all defined over K, we construct an *arboreal Galois representation* $\omega : \mathrm{Gal}\,(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(T_\phi(\alpha))$, where $T_\phi(\alpha)$ is the tree of preimages of α under some iterate of ϕ. The image of ω gives density information about the behavior of the orbit of α under ϕ when one reduces modulo primes of $\mathcal{O}$. Our main results here concern the case where $V = A$ is an abelian algebraic group and ϕ is multiplication by a prime ℓ. In this case, finding the image of ω is closely related to doing ℓ-adic Kummer theory on A (see e.g [2, 25]; also [18] contains a nice overview of applications to versions of the support problem). Moreover, the density information regarding reduced orbits takes the form of divisibility properties of $|\alpha_p|$, the order of the reduction $\alpha_\mathfrak{p} \in A(\mathcal{O}/\mathfrak{p})$ for primes $\mathfrak{p}$ of $\mathcal{O}$ (see e.g. [24, 7]).

In this paper we consider certain classes of A of general interest, and address both the determination of the image of ω and the computation of the associated density. The image of ω consists of the image of the usual ℓ-adic representation, and in addition an ℓ-adic *Kummer part* that is isomorphic to a subgroup of the Tate module (see p. 3 for

2000 *Mathematics Subject Classification.* Primary 11F80; Secondary 14L10, 14K15.

details). When A is a one-dimensional torus, an elliptic curve, or a higher-dimensional irreducible abelian variety without complex multiplication, and the associated ℓ-adic representation is surjective, we give a simple characterization of when the Kummer part is the full Tate module (see Theorems 11, 20, 27, 35). In the latter three theorems, for all $\ell \neq 2$ the condition is simply $\alpha \notin \ell A(K)$. In the cases we consider, this makes explicit [3, Theorem 2, p.40], which states that if A is an abelian variety or the product of an abelian variety by a torus, then the Kummer part is the full Tate module for all but finitely many ℓ and has open image for all ℓ (see also [24, Theorem 2.8] and [7, Proposition 2.10] for the latter statement). This result stems essentially from work of Ribet [25, 11], where it is shown that for A belonging to a large class of commutative algebraic groups, the modulo-ℓ Kummer part is all of $A[\ell]$ for all but finitely many ℓ.

When the Kummer part is the full Tate module, we give a method for computing the associated density (Theorem 10), and carry out this computation when A is a one-dimensional torus or an elliptic curve. That the image of ω gives the density of ℓ-power divisibility properties of $|\alpha_p|$ has already been established for abelian varieties in [24] (see also [7, Proposition 2.11]), where it is also shown that all such properties of $|\alpha_{\mathfrak{p}}|$ occur for positive density sets of $\mathfrak{p}$, though no densities are computed. On the other hand, work originating with Hasse [8, 9] and including Moree [23] and others has led to the computation of all such densities in the case where A is a trivial one-dimensional torus.

As a sample corollary of our work, we obtain the following.

Theorem 1. *Let K be a number field and E an elliptic curve defined over K. Suppose that the 2-adic representation associated to E surjects onto $\mathrm{GL}_2(\mathbb{Z}_2)$ and $\alpha \in E(K)$ is any point with $\alpha \notin 2E(K)$. Then the density of primes $\mathfrak{p} \subset \mathcal{O}$ with $\alpha_{\mathfrak{p}}$ having odd order is 11/21.*

See Theorems 20 and 24 for results for all ℓ. Note also that the surjectivity of the 2-adic representation is easily verified in specific cases. For instance, in Example 23 we show the curve $E : y^2 + y = x^3 - x$ and point $\alpha = (0, 0)$ satisfy the hypotheses of Theorem 1. An immediate corollary is the following.

Corollary 2. *Let $E : y^2 + y = x^3 - x$, $\alpha = (0, 0)$, and suppose $a_1, a_2, \ldots$ is the corresponding elliptic divisibility sequence, i.e. that a_n is the appropriate square root of the denominator of $x([n]\alpha)$. Then the rank of apparition $r_p := \min\{n : p \mid a_n\}$ is odd for 11/21 of primes p.*

Remark. Compare Corollary 2 with the result of Lagarias [20], which is equivalent to the Fibonacci sequence having odd r_p for 1/3 of primes p. Note also that all our results on elliptic curves may be translated into results about corresponding elliptic divisibility sequences.

When E has complex multiplication, we show in Section 5.2 that the density mentioned in Theorem 1 is in general only $2/9$ when 2 splits in the CM ring of E, and in general $8/15$ when 2 is inert. We obtain similar results in the case of certain tori (Section 4). In the case of a higher-dimensional abelian variety without complex multiplication (Section 6), the computation of the associated densities appears difficult. Throughout, we give many examples to illustrate our large-image and density results.

A more detailed outline of the paper is as follows. In Section 2 we develop some general aspects of arboreal Galois representations. Let K^{sep} be a separable closure of K, and consider the set of nth preimages

$$U_n := \{\beta \in V(K^{\mathrm{sep}}) : \phi^n(\beta) = \alpha\}. \tag{1}$$

We define the *preimage tree* $T_\phi(\alpha)$ to be the disjoint union of the U_n; this set has a natural tree structure with root α. Since ϕ is defined over K, any $\sigma \in \mathrm{Gal}\,(K^{\mathrm{sep}}/K)$ preserves the connectedness of vertices, and thus acts on $T_\phi(\alpha)$ as a tree automorphism. This gives a homomorphism $\omega_{\phi,\alpha} : \mathrm{Gal}\,(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(T_\phi(\alpha))$ that we call the *arboreal representation* associated to ϕ, α, and often just denote by ω. In general one expects $\omega_{\phi,\alpha}$ to be surjective, though this is very difficult to prove for specific maps (see the discussion on p. 7). Denote by $G_\phi(\alpha)$ the image of $\omega_{\phi,\alpha}$. We define $\mathcal{F}(G_\phi(\alpha))$ to be the Haar measure of the set of $g \in G_\phi(\alpha)$ fixing at least one infinite limb of $T_\phi(\alpha)$. We show that $\mathcal{F}(G_\phi(\alpha))$ gives density information about the behavior of the reduced orbit $\{\overline{\phi}^n(\overline{\alpha}) : n = 1, 2, \ldots\}$, where the bars denote reduction modulo a prime $\mathfrak{p}$ in $\mathcal{O}$.

Beginning in Section 3 we specialize to the case where $V = A$ is an abelian algebraic group and ϕ is multiplication by a prime ℓ. In the cases of interest to us, $G_\phi(\alpha)$ is contained in $T_\ell(A) \rtimes \mathrm{Aut}(T_\ell(A))$, where $T_\ell(A)$ is the ℓ-adic Tate module of A. The image in the right side of this semi-direct product corresponds to the usual ℓ-adic representation of A, while the kernel of projection onto the right side corresponds to restriction of $\omega_{\phi,\alpha}$ to $\mathrm{Gal}\,(K^{\mathrm{sep}}/K(A[\ell^\infty]))$, where $K(A[\ell^\infty]) = \bigcup_n K(A[\ell^n])$. We call the subgroup of $T_\ell(A)$ obtained in this way the *Kummer part* of $G_{\phi,\alpha}$. We give general criteria for the Kummer part to be all of $T_\ell(A)$ (Theorem 9), and show that when this occurs we can determine $\mathcal{F}(G_\phi(\alpha))$ via a certain matrix computation (Theorem 10).

In the remainder of the paper, we examine classes of A that hold particular interest, and for convenience specialize to the case of K a number field (although similar arguments apply to the case of K a function field). We give simplified versions of Theorem 9 in each specific case (Theorems 11, 20, 27, 35). We also carry out the computation of $\mathcal{F}(G_\phi(\alpha))$ where possible, using Theorem 10. In Section 4 we discuss the case of algebraic tori. In the case $A = \mathbb{G}_m$, we reprove certain results of Hasse, Moree and others [23], and we treat the case where A is a twisted $\mathbb{G}_m$. We also discuss some examples of higher-dimensional tori. In Section 5 we deal with both

non-CM and CM elliptic curves. When $A = E$ is an elliptic curve with surjective ℓ-adic representation, we show that the Kummer part is the full Tate module if and only if $\alpha \notin \ell E(K)$ (Theorem 20). In this case, we compute in Theorem 24 that

$$\mathcal{F}(G_\phi(\alpha)) = \frac{\ell^5 - \ell^4 - \ell^3 + \ell + 1}{\ell^5 - \ell^3 - \ell^2 + 1}.$$

When E has CM, we obtain similar formulas (see Theorem 30).

In Section 6 we discuss the case of higher-dimensional abelian varieties. We show the Kummer part is the full Tate module when $\ell > 2$ and $\alpha \notin \ell A(K)$, and give an example where $\omega_\phi(\alpha)$ it is surjective for all ℓ. However, due to the complexity of $\mathrm{GSp}_{2d}(\mathbb{Z}_\ell)$ the computation described in Theorem 10 appears quite difficult to carry out. For small ℓ we approximate $\mathcal{F}(G_\phi(\alpha))$ using MAGMA, and show for instance that if $\dim A = 2$, $\ell = 2$, and A, α satisfy mild hypotheses, then $0.579 \leq \mathcal{F}(G_\phi(\alpha)) \leq 0.586$. Thus the density of the set of $\mathfrak{p} \subset \mathcal{O}$ such that the order of $\overline{\alpha} \in \overline{A}(k_\mathfrak{p})$ is odd moves farther from the naive value of $1/2$ in the dimension 2 case.

Question 3. *If we fix say $\ell = 2$ does the limit of $\mathcal{F}(G_\phi(\alpha))$ as the dimension of A grows exist? If so, what is it?*

The first part of Question 3 is answered in the affirmative by Jeff Achter in the first appendix to this article. One may also ask whether, if A and α are fixed and ℓ grows, the limit of $\mathcal{F}(G_\phi(\alpha))$ must always approach 1. Finally, we have included a brief appendix of data relating to each example in the paper.

2. General Arboreal Representations

In this section we develop the theory of general arboreal Galois representations. While this degree of generality will not be fully used in the sequel, it provides a framework for the computational component of the paper.

As in (1), we define U_n to be the set of nth preimages of α under the morphism $\phi : V \to V$. Note that $T_\phi(\alpha) := \bigsqcup_n U_n$ becomes a rooted tree with root α when we assign edges according to the action of ϕ, i.e. β_1 and β_2 are connected if and only if $\phi(\beta_1) = \beta_2$. Moreover, if $T_\phi(\alpha)$ is disjoint from the branch locus

$$B_\phi = \{\gamma \in V : \#\phi^{-1}(\gamma) < \deg \phi\},$$

then U_n has $(\deg \phi)^n$ elements and $T_\phi(\alpha)$ is the complete $(\deg \phi)$-ary rooted tree. This disjointness may be verified by checking that α is not in $\bigcup_n \phi^n(B_\phi)$.

Let K_n be the extension of K obtained by adjoining the coordinates of the elements of U_n, and let $K_\infty := \bigcup_n K_n$. Put $G_n = G_{n,\phi}(\alpha) := \mathrm{Gal}\,(K_n/K)$, and note that G_n is the quotient of $G_\phi(\alpha)$ obtained by restricting the action of $G_\phi(\alpha)$ on $T_\phi(\alpha)$ to the first n levels of $T_\phi(\alpha)$.

We now give a formal definition of $\mathcal{F}(G_\phi(\alpha))$. Note that $G_\phi(\alpha)$ is a profinite group and thus has a natural Haar measure μ, which we take normalized to have total mass 1. Define the *ends* of $T_\phi(\alpha)$ to be the profinite set $\varprojlim\{\phi^{-n}(\alpha)\}$ under the natural maps $\{\phi^{-n}(\alpha)\} \to \{\phi^{-m}(\alpha)\}$ for $n > m$ given by ϕ^{n-m}.

Definition. *Assuming the notation above, we let* $\mathcal{F}(G_\phi(\alpha)) := \mu(\{g \in G_\phi(\alpha) : g \text{ fixes at least one end of } T_\phi(\alpha)\})$.

Remark. A straightforward argument using the definitions yields

$$\mathcal{F}(G_\phi(\alpha)) = \lim_{n\to\infty} 1/\#G_n \cdot \#\{g \in G_n : g \text{ fixes at least one point in } U_n\}.$$

One may consider V as a scheme over $\operatorname{Spec}\mathcal{O}$, which we will also denote by V. For instance, one can embed V in $\mathbb{P}^m_K \subset \mathbb{P}^m_{\mathcal{O}}$, and then take as a model the Zariski closure of $V \subset \mathbb{P}^m_{\mathcal{O}}$. For each prime $\mathfrak{p} \subset \mathcal{O}$, denote the residue field corresponding to $\mathfrak{p}$ by $k_\mathfrak{p}$, the fiber of V over $\mathfrak{p}$ by $V_\mathfrak{p}$, and the $k_\mathfrak{p}$-points of $V_\mathfrak{p}$ by $V(k_\mathfrak{p})$. Note that for $\alpha \in V(K)$, for all but a finite number of primes $\mathfrak{p}$ there is a well-defined reduction $\overline{\alpha} \in V(k_\mathfrak{p})$. Moreover, the map $\phi : V \to V$ is given by polynomials in each projective coordinate, and these polynomials have a common root modulo only finitely many $\mathfrak{p}$. For any $\mathfrak{p}$ not among these finitely many, we then have a reduced morphism $\overline{\phi} : V_\mathfrak{p} \to V_\mathfrak{p}$ with $\deg\overline{\phi} = \deg\phi$. For a more detailed discussion of these matters, see [18, pp. 107-108].

In this section we show that $\mathcal{F}(G_\phi(\alpha))$ encodes certain dynamical information about $\overline{\alpha}$ under $\overline{\phi}$ as $\mathfrak{p}$ varies over the finite primes of K. By the density of a set S of primes of K, we mean the Dirichlet density

$$D(S) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}}, \tag{2}$$

where $N(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$. In the case where K is a number field, we may without loss of generality use the notion of natural density given by $d(S) = \lim_{n\to\infty} \#\{\mathfrak{p} \in S : N(\mathfrak{p}) \le n\}/\#\{\mathfrak{p} : N(\mathfrak{p}) \le n\}$.

Before stating the main result of this section, we give some terminology. If S is a set, $f : S \to S$ is a map, and f^n the nth iterate of f, we say that $s \in S$ is *periodic* under f if $f^n(s) = s$ for some $n \ge 1$. We say that s is *preperiodic* if s is not periodic but $f^n(s) = f^m(s)$ for some $n, m \ge 1$. Note that if S is finite then every point in S is either periodic or preperiodic.

Theorem 4. *Assuming the notation above, we have*

$$\mathcal{F}(G_\phi(\alpha)) \ge D(\{\mathfrak{p} \subset \mathcal{O} : \overline{\alpha} \in V(k_\mathfrak{p}) \text{ is periodic under } \overline{\phi}\}).$$

If in addition K_∞/K is finitely ramified, then we obtain equality.

Proof. Let $\operatorname{Per}(\phi, \alpha) = \{\mathfrak{p} \subset \mathcal{O} : \overline{\phi}^n(\overline{\alpha}) = \overline{\alpha} \text{ for some } n \ge 1\}$. We begin by showing that $\mathfrak{p} \in \operatorname{Per}(\phi, \alpha)$ if and only if for each n there is $\gamma \in V(k_\mathfrak{p})$ such that $\overline{\phi}^n(\gamma) = \overline{\alpha}$.

If $\overline{\phi}^m(\overline{\alpha}) = \overline{\alpha}$ for some m, then for any n we may write $n = mk + r$ with $0 \leq r < m$ and take $\gamma = \overline{\phi}^{m-r}(\overline{\alpha})$. To show the reverse inclusion, the finiteness of $V(k_{\mathfrak{p}})$ implies that there exist $n_2 > n_1$ and γ such that $\overline{\phi}^{n_1}(\gamma) = \overline{\phi}^{n_2}(\gamma) = \overline{\alpha}$. Then

$$\overline{\phi}^{n_2-n_1}(\overline{\alpha}) = \overline{\phi}^{n_2-n_1}(\overline{\phi}^{n_1}(\gamma)) = \overline{\phi}^{n_2}(\gamma) = \overline{\alpha}.$$

Now let

$$\Omega_N = \{\mathfrak{p} : \mathfrak{p} \text{ is unramified in } K_N \text{ and } \overline{\phi}^N(x) = \overline{\alpha} \text{ has no solution in } V(k_{\mathfrak{p}}) \}.$$

If $\mathfrak{p} \in \Omega_N$, then by the previous paragraph, clearly $\mathfrak{p} \notin \mathrm{Per}(\phi, \alpha)$. Since only finitely many primes ramify in K_N, we have

$$D(\mathrm{Per}(\phi, \alpha)) \leq 1 - D(\Omega_N). \tag{3}$$

Let G_K be Galois group of the separable closure of K, and let $\mathrm{Frob}_{\mathfrak{p}} \subset G_K$ be the Frobenius conjugacy class at $\mathfrak{p}$. By the Chebotarev density theorem, the density of $\mathfrak{p}$ with $\mathrm{Frob}_{\mathfrak{p}}$ having prescribed image $C \subseteq G_N$ is $\#C/\#G_N$.

Let $\mathfrak{p}$ be a prime of K not ramifying in K_N and such that $\deg \overline{\phi} = \deg \phi$; this excludes only a finite number. There exists $\gamma \in V(k_{\mathfrak{p}})$ such that $\overline{\phi}^N(\gamma) = \overline{\alpha}$ if and only if the action of $\mathrm{Frob}_{\mathfrak{p}}$ on U_N has a fixed point. By the Chebotarev density theorem the density of such $\mathfrak{p}$ is equal to

$$\#\{\sigma \in G_N : \sigma \text{ fixes at least one element of } U_N\}/\#G_N.$$

Let us denote this quantity by d_N, and note that $d_N = 1 - D(\Omega_N)$. By (3) we now have $D(\mathrm{Per}(\phi, \alpha)) \leq \lim_{N\to\infty} d_N$, and this last limit is just $\mathcal{F}(G)$, proving the first assertion of the theorem.

Suppose now that K_∞/K is finitely ramified. By the first paragraph of the proof, we then have that $\mathrm{Per}(\phi, \alpha)$ is the same as the complement of $\bigcup_{N\geq 1} \Omega_N$ except for a finite set of primes. Since the complements of the Ω_N are nested, this gives $D(\mathrm{Per}(\phi, \alpha)) = \lim_{N\to\infty} d_N$. □

We close this section with some general remarks about arboreal representations that will not be used in the sequel. A natural question to ask about $\omega_{\phi,\alpha}$ is how large one expects the image $G_\phi(\alpha)$ to be. In the case where V is a curve and ϕ is critically finite, i.e. the forward image of the branch locus B_ϕ is a finite set, one can show that $G_\phi(\alpha)$ is finitely generated as a profinite group (see e.g. [1, Theorem 1.1]). This immediately implies it cannot be all of $\mathrm{Aut}(T_\phi(\alpha))$. The main considerations of this paper fall into this category, as the multiplication by ℓ map on an abelian algebraic group is critically finite.

However, in the absence of this phenomenon, it is reasonable to expect the image of the arboreal representation to be large.

Question 5. *Let K be a global field, V be a curve, $\phi : V \to V$ be a finite morphism defined over K, and $\alpha \in V(K)$ be such that $T_\phi(\alpha)$ is the complete $(\deg \phi)$-ary rooted tree. Suppose ϕ is not critically finite. Must $G_\phi(\alpha)$ have finite index in $\mathrm{Aut}(T_\phi(\alpha))$?*

One may ask a similar question for higher-dimensional V, but in that case the definition of critically finite maps, and the ramification properties of extensions corresponding to them, are not well-studied. Question 5 is not even resolved in the case $K = \mathbb{Q}$, $V = \mathbb{P}^1$, $\phi = x^2 + c$ for $c \in \mathbb{Z}$. Indeed, it is known that $\omega_{\phi,\alpha}$ is surjective for certain values of c [31], but for instance when $c = 3$ surjectivity fails, and indeed it is not known if the image in this case has finite index in $\mathrm{Aut}(T_\phi(\alpha))$. However, the first author has answered Question 5 in the affirmative for two infinite families of quadratic polynomials $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ [12, Section 3]. For further discussion of these matters, see [4].

Finally, it can be shown that if $G_\phi(\alpha) \cong \mathrm{Aut}(T_\phi(\alpha)$ then $\mathcal{F}(G_\phi(\alpha)) = 0$, e.g via natural extensions of methods in [13, Section 5].

3. Arboreal representations associated to abelian algebraic groups

In this section, we specialize to the case of an abelian algebraic group $V = A$. We first give an interpretation of $\mathcal{F}(G_\phi(\alpha)$ in this case, then we describe the Galois groups $G_n := \mathrm{Gal}\,(K(U_n)/K)$ in terms of the groups $A[\phi^n] := \ker \phi^n$ and their automorphism groups. We show that the image $G_\phi(\alpha)$ of $\omega = \omega_{\phi,\alpha} : \mathrm{Gal}\,(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(T_\phi(\alpha))$ lands inside a particular semi-direct product, and fits into a short exact sequence with the Kummer part and the image of the ℓ-adic representation. Moreover, we give criteria for the Kummer part to be the full Tate module.

We fix $\alpha \in A(K)$ and $\phi \in \mathrm{End}(A)$, and we refer to $G_\phi(\alpha)$, $T_\phi(\alpha)$ and $\mathcal{F}(G_\phi(\alpha))$ as G, T, and $\mathcal{F}(G)$, respectively. Let K_∞ be the fixed field of $\ker \omega$. We denote the group operation on A additively. We assume that ϕ is a degree ℓ^d morphism with the property that neither 0, α, nor any of their preimages are branch points. This implies that the extensions K_n/K are Galois.

Proposition 6. *If A is a torus or an abelian variety and $\phi = [\ell]$, then $\mathcal{F}(G)$ is the density of $\mathfrak{p}$ such that the order of $\overline{\alpha} \in A(k_\mathfrak{p})$ is not divisible by ℓ.*

Proof. First note that K_∞/K is a finitely ramified extension. For the torus case this follows since after passing to a finite extension, the coordinates of elements of U_n consist of roots of unity multiplied by ℓ^nth roots of fixed algebraic numbers. The abelian variety case is handled by [10, p. 263]; indeed K_∞/K is unramified outside ℓ and the set of primes of bad reduction of A.

Thus by Theorem 4 we have $\mathcal{F}(G_\phi(\alpha)) = D(\{\mathfrak{p} \subset \mathcal{O} : \overline{\alpha} \in V(k_\mathfrak{p}) \text{ is periodic under } \ell\})$. Denote the order of $\overline{\alpha} \in A(k_\mathfrak{p})$ by m. We show that $\ell \mid m$ if and only if $\overline{\alpha}$ is periodic under ℓ. If $\ell \nmid m$ then $\ell \in (\mathbb{Z}/m\mathbb{Z})^\times$, whence $\ell^n \equiv 1 \bmod m$ for some n. Thus $[\ell^n]\overline{\alpha} = \overline{\alpha}$, whence $\overline{\alpha}$ is periodic under ℓ. Conversely, if $[\ell^n]\overline{\alpha} = \overline{\alpha}$ for some n, then $[\ell^n - 1]\overline{\alpha} = \overline{0}$, whence ℓ cannot divide the order of $\overline{\alpha}$. □

We now discuss the decomposition of ω into two parts in the case that A is an abelian algebraic group, and give notation and terminology that we use throughout the sequel. Let $A[\phi^n] = \{\gamma \in K^{\text{sep}} : \phi^n(\gamma) = 0\}$, and let $T_\phi(A) := \varprojlim A[\phi^n]$ be the Tate module of A. Note that in the notation of Section 2, $T_\phi(A)$ is the same as $T_\phi(O)$, where $O \in A$ is the identity.

Definition. *For each $n \geq 1$, let $\beta_n \in U_n$ be a chosen element so that $\phi(\beta_n) = \beta_{n-1}$, with $\beta_0 = \alpha$. Define*

$$\omega_n : \mathrm{Gal}\,(K_n/K) \to A[\phi^n] \rtimes \mathrm{Aut}(A[\phi^n])$$

by $\omega_n(\sigma) := (\sigma(\beta_n) - \beta_n, \sigma|_{A[\phi^n]})$. Passing to the inverse limit gives $\omega : \mathrm{Gal}\,(K_\infty/K) \to T_\phi(A) \rtimes \mathrm{Aut}(T_\phi(A))$.

Let also $K(A[\phi^\infty]) = \bigcup_n K(A[\phi^n])$ and $\rho : \mathrm{Gal}\,(K(A[\phi^\infty])/K \to \mathrm{Aut}(T_\phi(A))$ be the associated Galois representation. Denote by ρ_n the restriction of ρ to $\mathrm{Gal}\,(K(A[\phi^n])/K)$, and let $I_n = \mathrm{im}\,\rho_n$ and $\mathcal{I} := \varprojlim I_n = \mathrm{im}\,\rho$. Note that ω restricted to $\mathrm{Gal}\,(K(A[\phi^\infty])/K$ gives exactly ρ. Denote by κ the map $\mathrm{Gal}\,(K_\infty/K(A[\phi^\infty])) \to T_\phi(A)$. We refer to κ as the *Kummer map* and its image as the *Kummer part* of $\mathrm{Gal}\,(K_\infty/K)$. Note that κ is surjective if and only if $\mathrm{im}\,\omega \cong T_\phi(A) \rtimes \mathcal{I}$. The next proposition says that these two parts give us full information about the image of κ. It is closely related to [24, p. 5].

Proposition 7. *Assume the notation above. For $n \geq 1$, ω_n is an injective homomorphism.*

Proof. For $\sigma, \tau \in \mathrm{Gal}\,(K_n/K)$, we have

$$\begin{aligned}
\omega_n(\sigma\tau) &= (\sigma\tau(\beta_n) - \beta_n, \sigma\tau|_{A[\phi^n]}) \\
&= (\sigma(\tau(\beta_n)) - \sigma(\beta_n) + \sigma(\beta_n) - \beta_n, \sigma|_{A[\phi^n]}\tau|_{A[\phi^n]}) \\
&= ((\sigma(\beta_n) - \beta_n) + \sigma(\tau(\beta_n) - \beta_n), \sigma|_{A[\phi^n]}\tau|_{A[\phi^n]}) \\
&= (\sigma(\beta_n) - \beta_n, \sigma)(\tau(\beta_n) - \beta_n, \tau) \\
&= \omega_n(\sigma)\omega_n(\tau).
\end{aligned}$$

Thus, ω_n is a homomorphism. Suppose that $\sigma \in \ker \omega_n$. Then, $\sigma(\beta_n) - \beta_n = 0$ so $\sigma(\beta_n) = \beta_n$. Moreover, $\sigma|_{A[\phi^n]}$ is the identity. Thus, if $\beta \in U_n$ we have $\phi^n(\beta) = \alpha$ and so

$$\phi^n(\beta - \beta_n) = \phi^n(\beta) - \phi^n(\beta_n) = \alpha - \alpha = 0.$$

Thus, $\beta - \beta_n \in A[\phi^n]$. Hence, $\sigma(\beta - \beta_n) = \beta - \beta_n$. It follows that $\sigma(\beta) = \beta$. Thus σ fixes U_n and hence K_n, proving that $\sigma = 1$ and ω_n is injective. □

We summarize the preceding discussion and Proposition with the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}\,(K_\infty/K(A[\phi^\infty])) & \longrightarrow & \mathrm{Gal}\,(K_\infty/K) & \longrightarrow & \mathrm{Gal}\,(K(A[\phi^\infty])/K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \omega} & & \downarrow{\scriptstyle \rho} & & \\ 1 & \longrightarrow & T_{\phi(A)} & \longrightarrow & T_{\phi(A)} \rtimes \mathrm{Aut}(T_\phi(A)) & \longrightarrow & \mathrm{Aut}(T_\phi(A)) & \longrightarrow & 1 \end{array}$$

The rows are exact, the maps on the top row being the natural ones. The nontrivial maps on the bottom row are inclusion into the first factor, and projection onto the second factor, respectively. The vertical arrows are all injections. For each n one has a corresponding diagram modulo ℓ^n, with the vertical maps being κ_n, ω_n, and ρ_n. Finally, for the remainder of the article we regard ω as mapping into $T_{\phi(A)} \rtimes \mathrm{Aut}(T_\phi(A))$, rather than into the full automorphism group of the tree $T_\phi(\alpha)$. Thus we refer to ω as surjective when its image is all of $T_{\phi(A)} \rtimes \mathrm{Aut}(T_\phi(A))$.

We now work toward a theorem that will allow us to determine information about the image of ω. If G is any profinite group, we let $\Phi(G)$ denote its Frattini subgroup, namely the intersection of all maximal open subgroups of G. Properties of the Frattini subgroup of $\mathcal{I}$ will be important for determining the image of ω. At this point we assume that $A[\phi^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^d$, an assumption which will be in force throughout.

Theorem 8. *If there is a finite set S of primes of K such that $K(A[\phi^n])/K$ is unramified outside S for all $n \geq 1$, then the Frattini subgroup $\Phi(\mathcal{I})$ has finite index in $\mathcal{I}$.*

Proof. For $n > m$, denote by $\rho_{n,m}$ the natural restriction $I_n \to I_m$. Choosing consistent bases for $A[\phi^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^d$, we may consider elements of I_n as belonging to $\mathrm{GL}_d(\mathbb{Z}/\ell^n\mathbb{Z})$, with the reduction maps $\rho_{n,m}$ given by reducing mod ℓ^m.

We will first show that $\ker \rho_{n+1,n}$ is an elementary abelian ℓ-group. Note that $\ker \rho_{n+1,n} = \{M \in I_{n+1} : M \equiv 1 \pmod{\ell^n}\}$. If $M_1, M_2 \in \ker \rho_{n+1,n}$ and we write $M_1 = 1 + \ell^n A_1$ and $M_2 = 1 + \ell^n A_2$ then

$$M_1 M_2 = 1 + \ell^n(A_1 + A_2) + \ell^{2n} A_1 A_2 \equiv 1 + \ell^n(A_1 + A_2) \pmod{\ell^{n+1}}.$$

It follows that if we define $\tau : \ker \rho_{n+1,n} \to M_d(\mathbb{Z}/\ell\mathbb{Z})$ given by $\tau(M) = \frac{M-1}{\ell^n}$, then τ is a homomorphism. If $M \in \ker \tau$, then $M \equiv 1 \pmod{\ell^{n+1}}$ and so $M = 1$. It follows that τ is an injective homomorphism, and hence $\ker \rho_{n+1,n}$ is an elementary abelian ℓ-group.

Let $N = \ker \rho_1$. It follows that N is a pro-ℓ group. Also, it is clear that N has finite index in $\mathcal{I}$. Since every maximal subgroup of a finite ℓ-group has index ℓ,

every open maximal subgroup of N has index ℓ and hence $N/\Phi(N)$ may be viewed as an $\mathbb{F}_\ell$-vector space. Let L be the fixed field of N. If $L \subseteq M \subseteq K(A[\phi^\infty])$ is an extension with $[M : L] = \ell$ then M/L is unramified outside S. Hermite proved that there are only finitely many extensions of a given number field with bounded degree and unramified outside of a finite set of primes. It follows that $N/\Phi(N)$ is a finite-dimensional $\mathbb{F}_\ell$-vector space and hence $[N : \Phi(N)] < \infty$.

One may easily check that $\Phi(N)$ is fixed by all continuous automorphisms of N. Since conjugation by an element of $\mathcal{I}$ induces a continuous automorphism of N, it follows that $\Phi(N) \lhd \mathcal{I}$. Proposition 2.5.1(b) of [33], pg. 41 states that if $K \lhd G$, $H \leq G$ and $K \leq \Phi(H)$ then $K \leq \Phi(G)$. Applying this result with $K = \Phi(N)$, $H = N$ and $G = \mathcal{I}$ proves that $\Phi(N) \subseteq \Phi(\mathcal{I})$. Since $\Phi(N)$ has finite index in $\mathcal{I}$, the result follows. □

The following surjectivity criteria for κ will be used frequently in the rest of the paper.

Theorem 9. *Let notation be as above. Make the following assumptions.*

(1) *Assume that for all $n \geq 1$, $A[\phi^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^d$.*
(2) *Assume that I_n acts transitively on the elements of order ℓ^n in $A[\phi^n]$.*
(3) *Let k be large enough that $\ker \rho_k \subseteq \Phi(\mathcal{I})$. Assume that $K(\beta_1) \not\subseteq K(A[\phi^k])$.*

Then κ is surjective, i.e., $\operatorname{im} \omega_n \cong A[\phi^n] \rtimes I_n$ for all n.

Proof. Note that

$$\mathrm{Gal}\,(K_n/K(A[\phi^n])) \cong \{\sigma(\beta_n) - \beta_n : \sigma \in \mathrm{Gal}\,(K_n/K(A[\phi^n]))\} \subseteq A[\phi^n].$$

Case I: There is a $\sigma \in \mathrm{Gal}\,(K_n/K(A[\phi^n]))$ so that $\sigma(\beta_n) - \beta_n$ has order ℓ^n.

We denote elements of $A[\phi^n]$ by vectors $\vec{v}_i \in (\mathbb{Z}/\ell^n\mathbb{Z})^d$ and elements of $\mathrm{Aut}(A[\phi^n])$ by matrices $M \in \mathrm{GL}_d(\mathbb{Z}/\ell^n\mathbb{Z})$. Thus in the present case there is some $\vec{v}_1$ of order ℓ^n so that $(\vec{v}_1, 1) \in \operatorname{im} \omega_n$. Now, if $\vec{v}_2$ is another vector of order ℓ^n, then by assumption, $\mathrm{Gal}\,(K(A[\phi^n])/K)$ acts transitively on the elements of order ℓ^n in $A[\phi^n]$ and hence there is some $(\vec{v}_3, M) \in \operatorname{im} \omega_n$ so that $M^{-1}(\vec{v}_1) = \vec{v}_2$. Then, one checks that

$$(\vec{v}_3, M)^{-1}(\vec{v}_1, 1)(\vec{v}_3, M) = (\vec{v}_2, 1).$$

Thus, $(\vec{v}_2, 1) \in \operatorname{im} \omega_n$. It follows that $(\vec{v}, 1) \in \operatorname{im} \omega_n$ for all $\vec{v} \in A[\phi^n]$.

Now, if $M \in I_n \subseteq \mathrm{GL}_d(\mathbb{Z}/\ell^n\mathbb{Z})$, then there is some $\vec{v}$ so that $(\vec{v}, M) \in \omega_n$. Thus since $(-M^{-1}(\vec{v}), 1) \in \operatorname{im} \omega_n$, the product $(\vec{v}, M)(-M^{-1}(\vec{v}), 1) = (0, M)$ is in $\operatorname{im} \omega_n$ as well. Therefore $\operatorname{im} \omega_n \cong A[\phi^n] \rtimes I_n$, as desired.

Case II: For all $\sigma \in \mathrm{Gal}\,(K_n/K(A[\phi^n]))$, $\sigma(\beta_n) - \beta_n$ has order less than ℓ^n.

Since $\{\gamma \in A[\phi^n] : \gamma \notin A[\phi^{n-1}]\}$ is precisely the set of all elements of order ℓ^n in $A[\phi^n]$, it follows that $\sigma(\beta_n) - \beta_n \in A[\phi^{n-1}]$ for all $\sigma \in \mathrm{Gal}\,(K_n/K(A[\phi^n]))$. Thus,

$0 = \phi^{n-1}(\sigma(\beta_n)-\beta_n) = \sigma(\phi^{n-1}(\beta_n))-\phi^{n-1}(\beta_n) = \sigma(\beta_1)-\beta_1$. It follows that β_1 is fixed by $\mathrm{Gal}\,(K_n/K(A[\phi^n]))$ and hence $\beta_1 \in K(A[\phi^n])$. This shows that $K(\beta_1) \subseteq K(A[\phi^n])$.

If $\beta_1 \in K(A[\phi])$, then certainly $K(\beta_1) \subseteq K(A[\phi^k])$. Hence, assume that $\beta_1 \notin K(A[\phi])$. In this case, β_1 is not fixed by $\mathrm{Gal}\,(K_1/K(A[\phi]))$ and hence the Case I applies for $n = 1$. This shows that $\mathrm{Gal}\,(K_1/K) \cong A[\phi] \rtimes I_1$.

Next we will show that I_1 is a maximal subgroup of $A[\phi] \rtimes I_1$. If $M \subseteq A[\phi] \rtimes I_1$ with $I_1 < M$ then there is a $\sigma \in M$ so that $\sigma(\beta_1) - \beta_1 \neq 0$. Hence, $\sigma(\beta_1) - \beta_1$ has order ℓ and the same argument as in Case I shows that $M \cong A[\phi] \rtimes I_1$ and hence $M = A[\phi] \rtimes I_1$. Thus, I_1 is a maximal subgroup of $A[\phi] \rtimes I_1 \cong \mathrm{Gal}\,(K_1/K)$.

It follows that $K(\beta_1)$, the fixed field of I_1 is a minimal subfield of K_1 and hence a minimal subfield of K_∞. Hence, $\mathrm{Gal}\,(K_\infty/K(\beta_1))$ is a maximal subgroup of $\mathcal{I}$. Let L be the fixed field of $\Phi(\mathcal{I})$. If k is such that $\Phi(\mathcal{I}) \supseteq \ker \rho_k$ then $L \subseteq K(A[\phi^k])$. It follows that $K(\beta_1) \subseteq L \subseteq K(A[\phi^k])$, a contradiction. □

The following result gives a convenient method of computing $\mathcal{F}(G)$ in the case that κ is surjective, i.e. $\mathrm{im}\,\omega \cong \mathbb{Z}_\ell^d \rtimes \mathcal{I}$.

Theorem 10. *Suppose that $A[\phi^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^d$ for all n, κ is surjective, and $\mu(\{M \in \mathcal{I} : \det(M-I) = 0\}) = 0$. Then*

$$\mathcal{F}(G) = \int_{\mathcal{I}} \ell^{-\mathrm{ord}_\ell(\det(M-I))}\, d\mu. \tag{4}$$

Remark. One can show that if I_n acts transitively on the elements of order ℓ^n in $A[\phi^n]$ for all n, then $\mu(\{M \in \mathcal{I} : \det(M-I) = 0\}) = 0$.

Proof. We will frequently use the fact that if $X \in M_d(\mathbb{Z}_\ell)$ acts on $V = \mathbb{Z}_\ell^d$ with $\det(X) \neq 0$, then the image of $X : V \to V$ has index $\ell^{\mathrm{ord}_\ell(\det(X))}$. Note that if $\det(M-I) = 0$ then $\ell^{-\mathrm{ord}_\ell(\det(M-I))}$ is not defined, however by assumption this set has measure zero and so does not figure in the integral.

Suppose that $\sigma \in \mathrm{Gal}\,(K_n/K)$ and $\omega_n(\sigma) = (a, M) \in (\mathbb{Z}/\ell^n\mathbb{Z})^d \rtimes \mathrm{GL}_d(\mathbb{Z}/\ell^n\mathbb{Z})$. Then, if $\beta \in U_n$, then σ fixes β if and only if $\sigma(\beta) - \beta_n = \beta - \beta_n$. Write $\beta = \beta_n + \gamma$, where $\gamma \in A[\ell^n]$. Then, $\sigma(\beta) = \sigma(\beta_n) + \sigma(\gamma)$ and so

$$\sigma(\beta) - \beta_n = \sigma(\beta_n) - \beta_n + \sigma(\gamma).$$

The right hand side equals $\beta - \beta_n$ if and only if $\sigma(\beta_n) - \beta_n + \sigma(\gamma) = \gamma$. If $\omega_n(\sigma) = (a, M)$ then this means that $a + M(\gamma) = \gamma$, whence $(M-I)(-\gamma) = a$. This occurs if and only if a is in the image of $M - I$.

If $M \in I_n$ with $\det(M-I) \not\equiv 0 \pmod{\ell^n}$ and $\tilde{M}$ is any lift of M to H, then $\mathrm{ord}_\ell(\det(\tilde{M}-I)) = \mathrm{ord}_\ell(\det(M-I))$ and therefore the index of the image of $M-I$ (acting on $(\mathbb{Z}/\ell^n\mathbb{Z})^d$) and the index of the image of $(\tilde{M}-I)$ (acting on $\mathbb{Z}_\ell^d$) are the

same. It follows that the index of the image of $\det(M-I)$ is $\ell^{\mathrm{ord}_\ell(\det(M-I))}$. Hence, the number of fixed points divided by the size of $G_n = \mathrm{Gal}\,(K_n/K)$ is

$$\frac{\#F_n}{\#G_n} = \frac{\sum_{M\in I_n} \#\mathrm{im}\,(M-I)}{\#I_n\cdot \ell^{2n}} = \frac{\sum' \ell^{2n-\mathrm{ord}_\ell(\det(M-I))}}{\#I_n\cdot\ell^{2n}} + \frac{\sum'' \#\mathrm{im}\,(M-I)}{\#I_n\cdot\ell^{2n}},$$

where $\sum'$ and $\sum''$ are taken over all $M\in I_n$ with $\det(M-I)\not\equiv 0 \bmod \ell^n$ and $\det(M-I)\equiv 0 \bmod \ell^n$, respectively. We may rewrite the first sum as

$$\int_{\{M\in\mathcal{I}:\det(M-I)\not\equiv 0 \bmod \ell^n\}} \ell^{-\mathrm{ord}_\ell(\det(M-I))}\,d\mu.$$

From the assumption that $\mu\left(\{M\in\mathcal{I}:\det(M-I)=0\}\right)=0$ it follows that as $n\to\infty$, this integral tends to

$$\int_{\mathcal{I}} \ell^{-\mathrm{ord}_\ell(\det(M-I))}\,d\mu$$

and the second term tends to zero. This establishes (4). □

4. Tori

The multiplicative group scheme $\mathbb{G}_m = \mathrm{Spec}\ \mathbb{Z}[x,y]/(xy-1)$ is one of the simplest examples of an algebraic group. An algebraic torus A of dimension n is an algebraic group that is isomorphic to $\mathbb{G}_m^n$ over K^{sep}. If K is a number field, then there is a bijection between algebraic tori of dimension n up to K-isomorphism and

$$H^1(\mathrm{Gal}\,(\overline{K}/K), \mathrm{Aut}_{\overline{K}}(\mathbb{G}_m^n)) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}\,(\overline{K}/K), \mathrm{GL}_n(\mathbb{Z})).$$

In the special case $n=1$, $\mathrm{GL}_1(\mathbb{Z})\cong\mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}\,(\overline{K}/K),\mathbb{Z}/2\mathbb{Z})\cong K^\times/(K^\times)^2$. It follows every dimension 1 torus is isomorphic to one of the form

$$x^2 - dy^2 = 1$$

for some $d\in K^\times/(K^\times)^2$, where the group law is given by

$$(x_1,y_1)*(x_2,y_2) = (x_1x_2+dy_1y_2, x_1y_2+x_2y_1).$$

For such tori, we have the following surjectivity criteria for the Kummer map κ.

Theorem 11. *Let $A: x^2-dy^2=1$ be an abelian algebraic group over a number field K. Assume that the ℓ-adic representation on A is surjective. The Kummer map $\kappa:\mathrm{Gal}\,(\overline{K}/K(A[\ell^\infty]))\to\mathbb{Z}_\ell$ is surjective if and only if the following conditions are satisfied:*

1. *If ℓ is odd assume that $K(\beta_1)\not\subseteq K(A[\ell^2])$.*
2. *If $\ell=2$ assume that $K(\beta_1)\not\subseteq K(A[8])$.*

Proof. Necessity is clear. To show sufficiency, we use Theorem 9, whose conditions (1) and (2) are satisfied by our assumption that $\mathcal{I} \cong \mathbb{Z}_\ell^\times$. As for condition (3), note that $\mathbb{Z}_\ell^\times \cong \mathbb{Z}_\ell \times (\mathbb{Z}/(\ell-1)\mathbb{Z})$ if $\ell > 2$ or $\mathbb{Z}_\ell^\times \cong \mathbb{Z}_2 \times (\mathbb{Z}/2\mathbb{Z})$ if $\ell = 2$, and a simple computation of maximal subgroups shows that we may take $k = 2$ if $\ell > 2$ and $k = 3$ if $\ell = 2$. Thus the hypotheses of the present theorem satisfy (3) of Theorem 9 and the result follows. □

Remark. In the case $K = \mathbb{Q}$, one can show that for $\ell > 2$, if $\beta_1 \in \mathbb{Q}(A[\ell^2])$ then we have either that $\alpha \in \ell A(\mathbb{Q})$ or $\ell = 3$, $d = -3$ and $\alpha = 3\alpha_2 + \alpha_3$, where $\alpha_2 \in A(\mathbb{Q})$ and $\alpha_3 \in A(\mathbb{Q})[3]$.

The following proposition addresses conditions for surjectivity of the ℓ-adic representation.

Proposition 12. *Let ℓ be a prime. The ℓ-adic representation $\rho : \mathrm{Gal}\,(K(A[\ell^\infty])/K) \to \mathbb{Z}_\ell^\times$ is surjective if and only if the following conditions are satisfied:*

(1) *If ℓ is odd, then $[K(\zeta_{\ell^2}) : K] = \ell(\ell-1)$.*
(2) *If $\ell \equiv 3 \pmod 4$, then $-\ell d$ is not a square in K.*
(3) *If $\ell = 2$, then 2, $-d$, and $-2d$ are not squares in K.*

Proof. A straightforward but somewhat lengthy argument using the definitions. □

Corollary 13. *The arboreal representation $\omega : \mathrm{Gal}\,(K_\infty/K) \to \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ is surjective if and only if the conditions of Theorem 11 and Proposition 12 are satisfied.*

Proof. This follows from a simple diagram chase. □

Example 14. Suppose that $K = \mathbb{Q}$ and $d = 1$. In this case, $x^2 - y^2 = 1$ is isomorphic to $\mathbb{G}_m$ over $\mathbb{Q}$. If $\ell > 2$ and $\alpha \notin \ell A(\mathbb{Q})$, then Theorem 11 and the above remark demonstrate that $G = \mathrm{Gal}\,(K_\infty/K) \cong \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$. Moreover, one verifies directly that the same conclusion holds for $\ell = 2$ as long as the corresponding point $(\gamma, 1/\gamma)$ on $x'y' = 1$ satisfies condition (2) of Theorem 11, namely $\gamma \notin (\mathbb{Q}^\times)^2$ and $2\gamma \notin (\mathbb{Q}^\times)^2$.

Proposition 15. *Suppose that ℓ is prime, and $G \cong \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$. Then,*

$$\mathcal{F}(G) = \frac{\ell^2 - \ell - 1}{\ell^2 - 1}.$$

Proof. Clearly $\mu(\{x \in \mathbb{Z}_\ell^\times : x - 1 = 0\}) = 0$. Thus we may apply Theorem 10. Representing elements of $\mathbb{Z}_\ell^\times$ with their ℓ-adic expansions, we obtain

$$\mu(x \in \mathbb{Z}_\ell^\times : v_\ell(x-1) = n) = \begin{cases} (\ell-2)/(\ell-1) & \text{if } n = 0 \\ 1/\ell^n & \text{if } n \geq 1. \end{cases} \tag{5}$$

The integral in (4) is therefore

$$\frac{\ell-2}{\ell-1}+\sum_{k=1}^{\infty}\frac{1}{\ell^{2k}}=\frac{\ell-2}{\ell-1}+\frac{1}{\ell^2-1}=\frac{\ell^2-\ell+1}{\ell^2-1}.$$

□

Returning to Example 14, we see that in the case $A=\mathbb{G}_m$, $K=\mathbb{Q}$, we have $\mathcal{F}(G)=(\ell^2-\ell-1)/(\ell^2-1)$ for general $(\gamma,1/\gamma)\in\mathbb{G}_m(\mathbb{Q})$. More specifically, if $\gamma\in\mathbb{Q}$ is neither a square nor twice a square, the density of p such that the order of $\gamma\in(\mathbb{Z}/p\mathbb{Z})^\times$ is odd is $1/3$. Similar results were first proved by Hasse [8, 9]; see [23] for a complete accounting. For instance, Hasse showed that the density of primes p dividing 2^n+1 for some n is $\frac{17}{24}$. Note that $p\mid 2^n+1$ if and only if $2^n\equiv -1 \pmod p$, that is if and only if $(2,1/2)$ has even order in $\mathbb{G}_m(\mathbb{F}_p)$. Similarly, Lagarias' result [20] about primes dividing the nth Lucas number L_n corresponds to $\alpha=(1,1)$ on the disconnected abelian algebraic group $A: x^2-5y^2=\pm 4$. We have $[n]\alpha=(L_n,F_n)$, and one can easily show that α has even order mod p if and only if $p\mid L_n$ for some n. Finally, [14], contains a study of primes that divide iterates of polynomials of the form $(x+t)^2-(2+t)$. The nth such iterate is the x-coordinate of $[2^n](t,u)$ on $A: x^2-dy^2=4$, where d and u are chosen so that d is squarefree and $t^2-4=du^2$. A prime p divides the nth iterate if and only if $x([2^n](t,u))\equiv t \pmod p$. This occurs if and only if (t,u) has odd order mod p.

Example 16. Suppose that $K=\mathbb{Q}$, $d=-7$, $\ell=7$ and $\alpha=(3/4,1/4)$. In this case, one can show that K_n is the unique real subfield of $\mathbb{Q}\left(\zeta_{7^n},\left(\frac{3+\sqrt{-7}}{4}\right)^{1/7^n}\right)$ and $[K_n:K]=3\cdot 7^{2n-1}$. The density in this case is $\mathcal{F}(G)=\frac{17}{24}$, less than the density of $\frac{41}{48}$ that would be obtained if Proposition 12 applied.

The situation becomes more complex when we consider tori A with $A\cong\mathbb{G}_m\times\mathbb{G}_m$ over the algebraic closure of K. We will content ourselves with considering two examples.

Example 17. Suppose that $K=\mathbb{Q}$, $A\cong\mathbb{G}_m\times\mathbb{G}_m$ is given by $A: xyz=1$. Let ℓ, p and q be distinct primes and consider multiplication by ℓ with $\alpha=(p,q,\frac{1}{pq})$. In this case, $K_n=\mathbb{Q}(\zeta_{\ell^n},p^{1/\ell^n},q^{1/\ell^n})$ and $\mathrm{Gal}\,(K_n/\mathbb{Q})\cong(\mathbb{Z}/\ell^n\mathbb{Z})^2\rtimes(\mathbb{Z}/\ell^n\mathbb{Z})^\times$, so that ω is surjective. One can compute that $\mathcal{F}(G)=\frac{\ell^3-\ell^2-\ell-1}{\ell^3-1}$.

Example 18. Let $K=\mathbb{Q}$, and let A be defined by

$$1=x^3+2y^3+4z^3-6xyz=N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(x+y\sqrt[3]{2}+z\sqrt[3]{4}).$$

We take $\ell=2$ and $\alpha=(-1,1,0)$. In this example, $A\cong\mathbb{G}_m\times\mathbb{G}_m$ over $L=\mathbb{Q}(\sqrt[3]{2},\zeta_3)$. One can show that $K_n=\mathbb{Q}(\zeta_3,\zeta_{2^n},(\sqrt[3]{2}-1)^{1/2^n},(\zeta_3\sqrt[3]{2}-1)^{1/2^n})$. Then,

$$\mathrm{Gal}\,(K_n/\mathbb{Q})\cong(\mathbb{Z}/2^n\mathbb{Z})^2\rtimes(S_3\times(\mathbb{Z}/2^n\mathbb{Z})^\times),\ \text{and}\ \mathcal{F}(G)=67/168.$$

5. Elliptic Curves

5.1. **Elliptic curves without complex multiplication.** Suppose that A/K is an elliptic curve without complex multiplication, K is a number field, $\phi = [\ell]$, and $\alpha \in A(K)$.

To determine the image of ω, we need to determine both the image of the Kummer map $\kappa : \mathrm{Gal}\,(\overline{K}/K(A[\ell^\infty])) \to T_\ell(A) \cong \mathbb{Z}_\ell^2$ and the image of the associated ℓ-adic representation $\rho : \mathrm{Gal}\,(K(A[\ell^\infty])/K) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$.

We treat the Kummer part first, although before doing so we give a lemma that will be useful for determining surjectivity of both κ and ρ. It is a fairly simple surjectivity criteria for the 3-adic representation.

Lemma 19. *Let A/K be an elliptic curve and $\ell = 3$. Then, $\rho : \mathrm{Gal}\,(K(A[\ell^\infty])/K) \to \mathrm{GL}_2(\mathbb{Z}_3)$ is surjective if and only if*

1. *K is linearly disjoint from $\mathbb{Q}(\zeta_9)$,*
2. *$\mathrm{Gal}\,(K(A[3])/K) \cong \mathrm{GL}_2(\mathbb{F}_3)$, and*
3. *the 9-torsion polynomial (the polynomial in $K[x]$ whose roots are the numbers x so that $(x, y) \in A(\overline{K})$ has order 9) is irreducible over $K(\zeta_9)$.*

Moreover, if $\mathrm{Gal}\,(K(A[3])/K) \cong \mathrm{GL}_2(\mathbb{F}_3)$, but ρ is not surjective, then $[K(A[9]) : K] = 144$.

Proof. Suppose ρ is surjective. Then the first two conditions are clearly satisfied. Also, the mod 9 representation is clearly surjective. The restriction $\rho|_{K(\zeta_9)}$ then has image $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ in $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. It is easy to see that $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ acts transitively on the elements of order 9 in $(\mathbb{Z}/9\mathbb{Z})^\times$. Thus the 9-torsion points lie in a single Galois orbit over $K(\zeta_9)$, and hence the 9-torsion polynomial is irreducible. Therefore the third condition is also satisfied.

Conversely, suppose that the three conditions are satisfied. It is well-known that if the mod 9 representation is surjective, then the 3-adic representation is surjective. Considering the subgroups of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, the surjectivity of the mod 3 representation and the determinant map show that if the mod 9 representation is not surjective, then the image of $\rho : G_K \to \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ is a subgroup G with order 144. Then, the image of $\rho|_{K(\zeta_9)}$ is $G \cap \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$, which has order 24. It follows that the action of G on the 36 x-coordinates of the points of order 9 in $A[9]$ cannot be transitive, and hence the 9-torsion polynomial is reducible over $K(\zeta_9)$. □

Theorem 20. *Suppose that the ℓ-adic representation ρ associated to A is surjective. Then the Kummer map $\kappa : \mathrm{Gal}\,(\overline{K}/K(A[\ell^\infty])) \to \mathbb{Z}_\ell^2$ is surjective if and only if $\alpha \notin \ell A(K)$.*

Proof. First note that if $\alpha \in \ell A(K)$ then κ has trivial image.

Assume now that $\alpha \notin \ell A(K)$. We apply Theorem 9. Condition (1) of Theorem 9 is easily seen to be satisfied, and the assumption that ρ is surjective establishes condition (2). Thus it suffices to establish condition (3) of Theorem 9. To do this, we first show $\beta_1 \notin K(A[\ell])$ when $\ell > 2$. We first remark that the surjectivity of ρ and the assumption that $\alpha \notin \ell A(K)$ imply that if $\beta_1 \in K(A[\ell])$, then the Galois closure of $K(\beta_1)$ is $K(A[\ell])$. Indeed, β_1 cannot be in $A(K)$, and it follows that if $\beta_2 \neq \beta_1$ is a conjugate of β_1, then $\beta_2 - \beta_1 \in A[\ell]$ and is nonzero. The surjectivity of ρ then implies that $\mathrm{Gal}\,(K(A[\ell])/K)$ acts transitively and hence the Galois closure contains $A[\ell]$.

Suppose now to the contrary that $\beta_1 \in K(A[\ell])$. We showed that the Galois closure of $K(\beta_1)$ contains $K(A[\ell])$. This implies that if $H = \mathrm{Gal}\,(K(A[\ell])/K(\beta)) \subseteq L := \mathrm{Gal}\,(K(A[\ell])/K)$, then $\mathrm{core}_L(H) = 1$. Since $H \cap Z(L)$ is central in L, it follows that $H \cap Z(L) \lhd L$. However, since $\mathrm{core}_L(H) = 1$ it follows that $H \cap Z(L) = 1$. It follows then that

$$|L : H| = |L : HZ(L)||HZ(L) : H| = |L : HZ(L)|\frac{|HZ(L)|}{|H|} = |L : HZ(L)||Z(L)|.$$

Note that $Z(L) \cong (\mathbb{Z}/\ell\mathbb{Z})^\times$. Thus, $|Z(L)| = \ell - 1$. Now, $|L : H| = |K(\beta_1) : K|$ is the size of the Galois orbit of β_1. From above, it has size a multiple of $\ell - 1$. Applying the same argument to other preimages of α shows that all the Galois orbits have size a multiple of $\ell - 1$, and so it follows that $\ell - 1|\ell^{2d}$, the number of preimages of α. This implies that $\ell = 2$.

We now show that $\beta_1 \notin K(A[\ell])$ when $\ell = 2$. In this case $\mathrm{Gal}\,(K(A[2])/K) \cong S_3$ and this implies that $|L : H| = 3$. This implies that each Galois orbit has size three, which is a contradiction, since there are four preimages of α. Hence, $\beta_1 \notin K(A[\ell])$.

As the last step in establishing condition (3) of Theorem 9, we show that surjectivity criteria for the ℓ-adic representation are satisfied over $K(\beta_1)$ and use this to show that $K(\beta_1) \not\subseteq K(A[\ell^k])$, as desired. Since $\beta_1 \notin K(A[\ell])$, an argument analogous to that in the proof of Theorem 9 shows that $K(\beta_1)$ is a minimal subfield of $K(A[\ell^k])$ and that the Galois closure of $K(\beta_1)$ is $K_1 = K(\beta_1, A[\ell])$. Also, $\mathrm{Gal}\,(K_1/K) \cong (\mathbb{Z}/\ell\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Let $I_k = \mathrm{Gal}\,(K(A[\ell^k])/K)$, $M = \mathrm{Gal}\,(K(A[\ell^k])/K(\beta_1))$, and $N = \mathrm{Gal}\,(K(A[\ell^k])/K(A[\ell]))$. Since $K(\beta_1) \not\subseteq K(A[\ell])$ we have that $N \not\subseteq M$, and since M is maximal in I_k, it follows that $MN = I_k$.

Then, $\rho_1|_M : M \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ has kernel $M \cap N$. It follows that

$$\frac{M}{M \cap N} \cong \frac{MN}{N} \cong \frac{I_k}{N} \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Hence $\rho_1|_M$ is surjective.

If we think of A as an elliptic curve over $K(\beta_1)$, it follows that $\rho_1|_M : \mathrm{Gal}\,(\overline{K}/K(\beta_1)) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is surjective. Note that since $K(\beta_1)/K$ is a minimal subfield whose Galois closure has Galois group $(\mathbb{Z}/\ell\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we have $K(\beta_1) \cap K(\zeta_\ell^3) = K$. It follows that $K(\beta_1)$ is linearly disjoint from $K(\zeta_\ell^\infty)$.

If $\ell \geq 5$, Theorem 4.1 of [32] applies to A over $K(\beta_1)$. It follows that $\mathrm{Gal}\,(K_\infty/K(\beta_1)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$.

If $\ell = 2$, let Δ be the discriminant of the quadratic subfield of $K(A[2])/K$. Vasiu's Theorem 4.2.1 [32] gives surjectivity of the 2-adic representation over $K(\beta_1)$ provided $-\Delta$, 2Δ and -2Δ are not in squares in $K(\beta_1)$. If this is the case, then there is $\alpha \in K(\beta_1)$ so that $\alpha^2 = -\Delta$, $\alpha^2 = 2\Delta$ or $\alpha^2 = -2\Delta$. This implies that $K(\beta_1)$ contains a quadratic subfield, contradicting that $K(\beta_1)/K$ is a minimal subfield.

If $\ell = 3$, since the mod 3 representation is surjective over $K(\beta_1)$, either the 3-adic representation is surjective over $K(\beta_1)$, or $[K(\beta_1, A[9]) : K(\beta_1)] = 144$, by Lemma 19. This would imply that $[K(A[9]) : K] \leq [K(\beta_1, A[9]) : K] = 1296$. However, the given assumptions imply that $[K(A[9]) : K] = |\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})| = 3888$, a contradiction. Hence, $\rho|_M$ is surjective.

In any case, we see that $\mathrm{Gal}\,(K_\infty/K(\beta_1)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$. However, since $K(\beta_1) \subseteq K(A[\phi^k])$, the image must have index $[K(\beta_1) : K]$, a contradiction. □

We now turn to the surjectivity of ρ, on which there is a large literature. In particular, a result of Serre [28] implies that if ℓ is large enough, then ρ is surjective. Here we wish to give simple, explicit criteria for surjectivity of ρ for given ℓ. We use Theorem 4.1 of [32] for $\ell \geq 5$, and Theorem 4.2.1 of [32] for a surjectivity criteria for the 2-adic representation. The 3-adic representation has already been treated in Lemma 19.

Proposition 21. *Let ℓ be a prime. The ℓ-adic representation $\rho : \mathrm{Gal}\,(K(A[\ell^\infty])/K) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective if and only if the following conditions hold:*

1. *K is linearly disjoint from $\mathbb{Q}(\zeta_{\ell^n})$ for all n.*
2. *$\mathrm{Gal}\,(K(A[\ell])/K) \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*
3. *If $\ell = 2$, then $K(A[2])$ is linearly disjoint from $\mathbb{Q}(\sqrt{2}, i)$.*
4. *If $\ell = 3$, then the 9-torsion polynomial is irreducible over $K(\zeta_9)$.*

Proof. The necessity of the four conditions is trivial. Conditions (1) and (2) and [32, Theorem 4.1] imply that ρ is surjective provided $\ell \neq 2, 3$. If $\ell = 2$, [32, Theorem 4.2.1] gives this result assuming condition (3). When $\ell = 3$, condition (4) and Lemma 19 ensure the surjectivity of ρ. □

Corollary 22. *The arboreal representation $\omega : \mathrm{Gal}\,(K_\infty/K) \to (\mathbb{Z}_\ell)^2 \rtimes \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective if and only if the conditions of Theorem 20 and Proposition 21 are satisfied.*

Proof. The necessity is clear. Assume that κ is surjective, i.e. for all n $(\vec{v}, 1) \in \operatorname{im} \omega_n$ for all $v \in (\mathbb{Z}/\ell^n\mathbb{Z})^2$. The surjectivity of ρ_n implies that for any $M \in I_n$, there is some $\vec{v}$ with $(\vec{v}, M) \in \operatorname{im} \omega_n$. Since $(-M^{-1}(\vec{v}), 1) \in N$, we have $(\vec{v}, M)(-M^{-1}(\vec{v}), 1) = (0, M) \in \operatorname{im} \omega_n$. Therefore ω_n is surjective. □

Example 23. Let $A : y^2 + y = x^3 - x$. Then A is an elliptic curve of conductor 37. In [28] (pg. 310, 5.5.6), it is shown that $\operatorname{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all ℓ. It is also known that $\alpha = (0, 0)$ is a generator of $E(\mathbb{Q}) \cong \mathbb{Z}$. Moreover, one can check that the unique quadratic subfield of $\mathbb{Q}(A[2])/\mathbb{Q}$ is $\mathbb{Q}(\sqrt{37})$, and that the 9-torsion polynomial is irreducible over $\mathbb{Q}(\zeta_9)$. It follows that the ω representations are surjective for all ℓ.

Now we turn to the problem of computing the density $\mathcal{F}(G)$ in the situation that ω is surjective, i.e. $\operatorname{Gal}(K_\infty/K) \cong (\mathbb{Z}_\ell)^2 \rtimes \mathrm{GL}_2(\mathbb{Z}_\ell)$. To apply Theorem 10 in this case, we note that $I_n = \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ acts transitively on the elements of order ℓ^n in $A[\ell^n]$.

Theorem 24. *If $|\cdot|_\ell$ is the normalized absolute value on $\mathbb{Z}_\ell$, then we have*

$$\int_{\mathrm{GL}_2(\mathbb{Z}_\ell)} |\det(M - I)|_\ell^{-1} \, d\mu = \frac{\ell^5 - \ell^4 - \ell^3 + \ell + 1}{\ell^5 - \ell^3 - \ell^2 + 1}.$$

Proof. It is necessary to count the number c_n of matrices $M \in \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ with $\det(M - I) \equiv 0 \pmod{\ell^{n-1}}$ but $\det(M - I) \not\equiv 0 \pmod{\ell^n}$. Then the desired integral is

$$\sum_{n=1}^{\infty} \frac{c_n}{\#\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})}.$$

First, we compute c_1. This is the number of matrices $M \in \mathrm{GL}_2(\mathbb{F}_\ell)$ so that $M - I$ is invertible, that is, 1 is not an eignevalue of M. We will first count the number of matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$ that do have 1 as an eigenvalue. This implies that the other eigenvalue is in $\mathbb{F}_\ell$ and hence M has a Jordan form over $\mathbb{F}_\ell$. It follows that M is similar to one of

$$\begin{bmatrix} 1 & 0 \\ 0 & \lambda \end{bmatrix}, \lambda \neq 1, \text{ or } \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \text{ or } \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

The size of the conjugacy class is the index of the centralizer. We can easily compute that the centralizer of the first matrix is $\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \right\}$ which has size $(\ell - 1)^2$. The centralizer of the second matrix is $\left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \right\}$ which has size $\ell(\ell-1)$, and the centralizer of the third matrix is $\mathrm{GL}_2(\mathbb{F}_\ell)$, which has order $(\ell^2 - 1)(\ell^2 - \ell)$. It follows that

$$c_1 = \#\mathrm{GL}_2(\mathbb{F}_\ell) - \ell(\ell + 1)(\ell - 2) - (\ell - 1)(\ell + 1) - 1 = \ell^4 - 2\ell^3 - \ell^2 + 3\ell.$$

For $n \geq 2$, we pick a matrix $M \in \mathrm{GL}_2(\mathbb{F}_\ell)$ and count how many $\tilde{M} \in \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ there are with $\tilde{M} \equiv M$ and $\det(\tilde{M}-I) \equiv 0 \pmod{\ell^{n-1}}$ but $\det(\tilde{M}-I) \not\equiv 0 \pmod{\ell^n}$. The following simple lemma will be helpful for this purpose. We omit the proof.

Lemma 25. *Suppose that $a, b \in \mathbb{Z}/\ell\mathbb{Z}$, $c \in \mathbb{Z}/\ell^n\mathbb{Z}$, and $n \geq 2$. Then, the number of pairs $(\alpha, \beta) \in (\mathbb{Z}/\ell^n\mathbb{Z})$ with $\alpha\beta \equiv c \pmod{\ell^n}$ with $\alpha \equiv a \pmod{\ell}$ and $\beta \equiv b \pmod{\ell}$ is*

$$\begin{cases} 0 & ab \not\equiv c \pmod{\ell} \\ \ell^{n-1} & ab \equiv c \pmod{\ell} \text{ and one of } a \text{ or } b \text{ is nonzero.} \\ (\ell-1)(\mathrm{ord}_\ell(c)-1)\ell^{n-1} & a \equiv b \equiv c \equiv 0 \pmod{\ell}, c \not\equiv 0 \pmod{\ell^n} \\ (n\ell - n - \ell + 2)\ell^{n-1} & a \equiv b \equiv c \equiv 0 \pmod{\ell}, c \equiv 0 \pmod{\ell^n}. \end{cases}$$

If $M \not\equiv I \pmod{\ell}$ but M has one as an eigenvalue, a straightforward computation using Lemma 25 shows that there are $(\ell-1)\ell^{3n-3}$ matrices $\tilde{M} \in \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ with $\mathrm{ord}_\ell(\det(\tilde{M}-I)) = n-1$ for each $M \in \mathrm{GL}_2(\mathbb{F}_\ell)$. There are $\ell^3 - 2\ell - 1$ matrices that fall into this case.

If $M \equiv I \pmod{\ell}$, a more lengthy computation using Lemma 25 shows that there are

$$(\ell^2-1)\ell^{3n-3} - (\ell^2-1)\ell^{2n-1}$$

matrices $\tilde{M}$ in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ with $\mathrm{ord}_\ell(\det(\tilde{M}-I)) = n-1$. Hence, we have

$$c_n = (\ell-1)^2(\ell+1)\ell^{3n-2} - (\ell^2-1)\ell^{2n-1}.$$

Hence, we may split up

$$\sum_{n=1}^{\infty} \frac{c_n}{\#\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})}$$

as a sum of two geometric series, and we get

$$\mathcal{F}(G) = \frac{\ell^5 - \ell^4 - \ell^3 + \ell + 1}{\ell^5 - \ell^3 - \ell^2 + 1}.$$

□

5.2. **Complex Multiplication.** Suppose that A is an elliptic curve defined over a number field K, and that A has complex multiplication. Then $\mathrm{End}_{\overline{K}}(A) \cong R$, where R is an order in an imaginary quadratic field L. Suppose first that $L \subseteq K$, and put $R_\ell = R \otimes \mathbb{Z}_\ell$. Let $\mathcal{I} = \mathrm{Gal}\,(K(A[\ell^\infty])/K)$, so that $\mathcal{I}$ is the image of the ℓ-adic Galois representation associated to A. Then $\mathcal{I}$ is known to be isomorphic to a subgroup of $R_\ell^\times$ (see e.g. [29, p.502]). Indeed, we also have the analogue of Serre's open image theorem, namely that for any ℓ, $\mathcal{I}$ must have finite index in $R_\ell^\times$ and in fact $\mathcal{I} \cong R_\ell^\times$ for all but finitely many ℓ [28, p. 302].

A subgroup of $GL_2(\mathbb{Z}_\ell)$ that is isomorphic to $R_\ell^\times$ is called a *Cartan subgroup*, which we denote by C. In the case where $L \not\subseteq K$, we have that $\mathcal{I}$ is a subgroup of the normalizer N of some Cartan subgroup C. Indeed, $[\mathcal{I} : \mathcal{I} \cap C] = [K : L] = 2$, and thus $\mathcal{I}$ is the normalizer of its image in C.

Lemma 26. *Let R be the ring of integers in a quadratic imaginary field L, suppose ℓ is unramified in R, and put $R_\ell = R \otimes \mathbb{Z}_\ell$. If $\ell \geq 3$ then any subgroup $G \leq R_\ell^\times$ with full image in $(R_\ell/\ell^2 R_\ell)^\times$ is all of $R_\ell^\times$. For $\ell = 2$ a similar assertion holds with $(R_\ell/\ell^2 R_\ell)^\times$ replaced by $(R_\ell/\ell^3 R_\ell)^\times$.*

Proof. We proceed by describing the Frattini subgroup $\Phi(R_\ell^\times)$ of $R_\ell^\times$. First note that if S is the valuation ring in an unramified extension of $\mathbb{Q}_\ell$ of degree d, then the ℓ-adic logarithm gives an isomorphism $S^\times \cong \mathbb{F}_{\ell^d}^\times \times S$ if $\ell \geq 3$ and $S^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{F}_{\ell^d}^\times \times S$ if $\ell = 2$, where $\mathbb{F}_{\ell^d}$ is the finite field with ℓ^d elements [26, p. 257]. Since ℓS is the unique maximal subgroup of S, it follows that any maximal subgroup of $S^\times$ must contain ℓS, whence $\Phi(S^\times) \supseteq \ell S$. In the isomorphism given by the logarithm, ℓS maps to $\{x \in S^\times : x \equiv 1 \bmod \ell^2\}$ if $\ell \geq 3$ and $\{x \in S^\times : x \equiv 1 \bmod \ell^3\}$ if $\ell = 2$. Thus if $G \leq S^\times$ and G has full image in $S^\times/\ell^2 S^\times$ ($S^\times/\ell^3 S^\times$ if $\ell = 2$) then G surjects onto $S^\times/\Phi(S^\times)$ and hence $G = S^\times$.

If ℓ is inert in R, then R_ℓ is isomorphic to the valuation ring in an unramified quadratic extension of $\mathbb{Q}_\ell$, and the Lemma is proved. If ℓ splits in R, then $R_\ell^\times \cong \mathbb{Z}_\ell^\times \times \mathbb{Z}_\ell^\times$, and we have $\Phi(R_\ell^\times) \supseteq \ell\mathbb{Z} \times \ell\mathbb{Z}$. The proof then follows as in the previous paragraph. □

Theorem 27. *Let A be an elliptic curve defined over a number field K, suppose A has complex multiplication, and suppose that K does not contain the CM field of A. Let $H \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$ be the normalizer of the appropriate Cartan subgroup so that $\rho : \mathrm{Gal}\,(K(A[\ell^\infty])/K) \hookrightarrow H$, and suppose that in fact ρ is an isomophism. Finally, suppose $\ell \geq 3$. Then the Kummer map $\kappa : \mathrm{Gal}\,(\overline{K}/K(A[\ell^\infty])) \to \mathbb{Z}_\ell^2$ is surjective if and only if $\alpha \notin \ell A(K)$.*

Proof. The only if direction is trivial. Recall that K_n is defined to be the compositum of all $K(\beta)$ as β varies over all preimages of α under $[\ell]$. Let H_n be the reduction modulo ℓ^n of H.

Case I: Suppose that there is $\sigma \in \mathrm{Gal}\,(K_n/K(A[\ell^n]))$ with $\sigma(\beta_n) - \beta_n$ having order ℓ^n. When H is non-split, H_n acts transitively on the points of order ℓ^n in $(\mathbb{Z}/\ell^n\mathbb{Z})^2$, and we conclude that κ is surjective just as in the proof of Theorem 9. If H is split, we must do more. Note that

$$H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{Z}_\ell^\times \right\} \cup \left\{ \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix} : a, b \in \mathbb{Z}_\ell^\times \right\}.$$

Let $N = \mathrm{im}\,\kappa_n = \{\vec{v} : (\vec{v}, 1) \in \mathrm{im}\,\omega_n\}$, and note that we wish to show $N = (\mathbb{Z}/\ell^n\mathbb{Z})^2$. Since $\rho_n : \mathrm{Gal}\,(K(A[\ell^n])/K) \to H_n$ is surjective by hypothesis, for any $M \in H_n$ there

is some $(\vec{v}_3, M^{-1})$ in the image of ω_n. Then,

$$(\vec{v}_3, M^{-1})^{-1}(\vec{v}_1, 1)(\vec{v}_3, M^{-1}) = (M(\vec{v}_1), 1) \in \operatorname{im} \omega_n.$$

Hence if $\vec{v} \in N$ and $M \in H_n$, then $M\vec{v} \in N$. By assumption there is some $\vec{v}_1 \in N$ of order ℓ^n. Write $\vec{v}_1 = [a \quad b]^T$. Then, since $\vec{v}_1$ has order ℓ^n, one of a or b is coprime to ℓ. By applying $M = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, we see that there is some $\vec{v} \in N$ with a coprime to ℓ. Then,

$$\vec{v} + \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \vec{v} = \begin{bmatrix} 2a \\ 0 \end{bmatrix}.$$

Since $\ell > 2$, it follows that $2a$ is coprime to ℓ. Hence, there is an integer b so that $2ab \equiv 1 \pmod{\ell}$ and hence

$$b\left(\vec{v} + \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \vec{v}\right) = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \in N.$$

Applying $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ again we see that $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ is also in N. It follows that $N = (\mathbb{Z}/\ell^n\mathbb{Z})^2$.

Case II: Suppose that for all $\sigma \in \operatorname{Gal}(K_n/K(A[\ell^n]))$ we have $\sigma(\beta_n) - \beta_n$ of order less than ℓ^n.

As in the corresponding portion of the proof of Theorem 9, we deduce that $\beta_1 \in K(A[\ell^n])$ and H_1 is a maximal subgroup of $(\mathbb{Z}/\ell\mathbb{Z})^2 \rtimes H_1$. Note that $\alpha \notin \ell A(K)$ implies $\beta_1 \notin K$, whence the order of $\sigma(\beta_1) - \beta_1$ is greater than one. The assumption that $\operatorname{Gal}(K(A[\ell])/K) \cong H_1$ and the maximality of H_1 then imply $\operatorname{im} \omega_1 \cong (\mathbb{Z}/\ell\mathbb{Z})^2 \rtimes H_1$. Note also that $H_1 = \operatorname{Gal}(K_1/K(\beta_1))$, whence $K(\beta_1)$ is a minimal subfield of K_1.

It follows from the proof of Lemma 26 that the Frattini subgroup of H contains the kernel of reduction modulo ℓ^2. Hence, every minimal subfield of $K(A[\ell^n])$ is contained in $K(A[\ell^2])$. If $K(\beta_1) \subseteq K(A[\ell^2])$, then since the second is Galois over K, the Galois closure of the first is contained in the second. Hence $K_1 \subseteq K(A[\ell^2])$. Now, $|K_1 : K| = \ell^2 \cdot |H_1|$, and this equals $2\ell^2(\ell-1)^2$ in the split case and $2\ell^2(\ell^2-1)$ in the non-split case. Also, $|K(A[\ell^2]) : K| = |H_2|$, which has the same order as $\ell^2 \cdot |H_1|$ in both the split and non-split cases. Hence $K_1 = K(A[\ell^2])$. This implies that $H_2 \cong (\mathbb{Z}/\ell\mathbb{Z})^2 \rtimes H_1$.

We now obtain a contradiction by comparing the centers of these groups. Note that in both the split and non-split cases, $Z(H_2)$ contains aI for $a \in \mathbb{Z}/\ell^2\mathbb{Z}$ and hence has order a multiple of $\phi(\ell^2) = \ell(\ell-1)$.

However, if $(\vec{v}, M) \in Z((\mathbb{Z}/\ell\mathbb{Z})^2 \rtimes H_1)$, then

$$(\vec{v}, M)(0, M) = (\vec{v}, M^2)$$

but $(0, M)(\vec{v}, M) = (M\vec{v}, M^2)$. It follows that $M\vec{v} = \vec{v}$ for all $M \in H_1$. If $\ell \geq 3$, then $2I \in H_1$ and hence $\vec{v} = 0$. Therefore $Z((\mathbb{Z}/\ell^2\mathbb{Z})^2 \rtimes H_1) \subseteq Z(H_1)$, which has order $\ell - 1$. This is a contradiction. Hence, Case II does not occur, and ω_n is surjective. □

We now address the image of ρ, and using Lemma 26 we give a simple criteria for it to be as large as possible:

Proposition 28. *Let A, K, and H be as in Theorem 27, and again take $\ell \geq 3$. Then $\rho : \mathrm{Gal}\,(K(A[\ell^\infty])/K) \hookrightarrow H$ is an isomorphism if and only if $\mathrm{Gal}\,(K(A[\ell^2])/K) \cong H_2$.*

Proof. The only if direction is trivial. Suppose now that $\mathrm{Gal}\,(K(A[\ell^2])/K) \cong H_2$. Lemma 26 implies that $\mathrm{Gal}\,(K(A[\ell^\infty])/K)$ contains a subgroup C of H of index two, namely the Cartan subgroup. Since $\mathrm{Gal}\,(K(A[\ell^2])/K)$ already properly contains the reduction modulo ℓ^2 of C, the same is true of $\mathrm{Gal}\,(K(A[\ell^\infty])/K)$, and we conclude $\mathrm{Gal}\,(K(A[\ell^\infty])/K) \cong H$. □

Remark. When $\ell = 2$, we can obtain the conclusion of Theorem 27 under the stronger assumption that $[K(\beta_1, A[8]) : K(A[8])] = 4$. We can obtain the conclusion of Proposition 28 with the additional assumption that $\mathrm{Gal}\,(K(A[8])/K) \cong H_3$.

The following corollary has the same proof as Corollary 22.

Corollary 29. *Let H be as in Theorem 27, and let $\ell \geq 3$. The arboreal representation $\omega : \mathrm{Gal}\,(K_\infty/K) \to (\mathbb{Z}_\ell)^2 \rtimes H$ is surjective if and only if the conditions of Theorem 27 and Proposition 28 are satisfied. When $\ell = 2$ the conditions of the above remark are equivalent to the surjectivity of ω.*

Now we compute the densities $\mathcal{F}(G)$ in the CM case.

Theorem 30. *Let C be a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, and let $G = \mathbb{Z}_\ell^2 \rtimes C$ with the natural action. Let $h(x) = (x^2 - x - 1)/(x^2 - 1)$. Then $\mathcal{F}(G) = h(\ell)^2$ if C is split and $h(\ell^2)$ if C is inert. If $G = \mathbb{Z}_\ell^2 \rtimes N$, where N is the normalizer of a Cartan subgroup, then $\mathcal{F}(G) = (h(\ell)^2 + h(\ell))/2$ in the split case and $(h(\ell^2) + h(\ell))/2$ in the inert case.*

Proof. Letting μ be Haar measure, one easily sees that $\mu(\{M \in C : \det(M - I) = 0\}) = 0$, and similarly for N, whence Theorem 10 applies in all cases. Suppose first that C is non-split, whence $C \cong R_\ell^\times$, where R_ℓ may be taken to be the valuation ring in an unramified quadratic extension of $\mathbb{Q}_\ell$. By Theorem 10, to find $\mathcal{F}(G)$ it is enough to compute $t_n := \mu(\{x \in R_\ell^\times : v_\ell(x - 1) = n\})$ for each $n \geq 0$ and then evaluate the integral in (4). Since ℓ is a uniformizer for R_ℓ and the residue field has order ℓ^2, we have $t_0 = (\ell^2 - 2)/(\ell^2 - 1)$. When $n \geq 1$, for $x - 1$ to have valuation precisely n its ℓ-adic expansion must have constant term 1, order-i term 0 for $1 \leq i \leq n - 1$, and order-n term non-zero. Thus for $n \geq 1$, $t_n = 1/(\ell^{2n} - 1) \cdot 1/\ell^{2(n-1)} \cdot (\ell^2 - 1)/\ell^2 = 1/\ell^{2n}$.

The integral in (4) is therefore

$$\frac{\ell^2-2}{\ell^2-1}+\sum_{n=1}^{\infty}\frac{1}{\ell^{4n}}=\frac{\ell^4-\ell^2-1}{\ell^4-1},$$

and this last expression is just $h(\ell^2)$.

Now suppose that C is split, whence $C\cong\mathbb{Z}_\ell^\times\times\mathbb{Z}_\ell^\times$. In this case the Haar measure on C is just the product of the Haar measure μ on each copy of $\mathbb{Z}_\ell^\times$. The expression for $\mu(\{x\in\mathbb{Z}_\ell^\times\times\mathbb{Z}_\ell^\times : v_\ell(x-1)=n\})$ thus has $n+1$ terms, since the valuations of the two coordinates of $x-1$ must sum to n. From (5) it follows that for $n=0$ we get a measure of $(\ell-2)^2/(\ell-1)^2$, while for $n\geq 1$ a short computation shows the measure is

$$\frac{1}{\ell^n}\left(2\cdot\frac{\ell-2}{\ell-1}+n-1\right).$$

The integral in (4) thus becomes

$$\frac{(\ell-2)^2}{(\ell-1)^2}\ +\ \frac{2\ell-4}{\ell-1}\sum_{n=1}^{\infty}\frac{1}{\ell^{2n}}\ +\ \sum_{n=1}^{\infty}\frac{n-1}{\ell^{2n}},$$

and after evaluation of these sums one obtains $(\ell^4-2\ell^3-\ell^2+2\ell+1)/(\ell^2-1)^2$, which is equal to $h(\ell)^2$.

We now consider the case $G=\mathbb{Z}_\ell^2\rtimes N$, where N is the normalizer of a Cartan subgroup. We have $[N:G]=2$, and thus we need only determine the integral in (4) on the non-identity coset of C in N. When C is non-split, let $\gamma\in R_\ell$ be such that $R_\ell=\mathbb{Z}_\ell[\gamma]$ with x^2+cx+d the minimal polynomial of γ. Note that $\mathrm{ord}_\ell(c)=0$. We thus have in the split and non-split cases, respectively, that the non-identity coset of C in N consists of all

$$M=\begin{bmatrix}0&a\\b&0\end{bmatrix},\qquad M=\begin{bmatrix}a&bd-ac\\b&-a\end{bmatrix}.$$

In the former case we have $\det(M-I)=1-ab$ and in the latter $\det(M-I)=1-(a^2-abc+db^2)$. The maps $(a,b)\mapsto ab$ and $a+b\gamma\mapsto a^2-abc+db^2$ define homomorphisms ϕ_1 and ϕ_2 mapping $R_\ell^\times\to\mathbb{Z}_\ell^\times$ in the respective cases (ϕ_2 is the norm homomorphism). Both ϕ_1 and ϕ_2 are surjective for $\ell\geq 3$, as their images properly contain the squares in $\mathbb{Z}_\ell^\times$. For $\ell=2$ the surjectivity of ϕ_1 is clear, while for ϕ_2 it is useful to take $\gamma=\zeta_3$, so that $c=d=1$. Then $\operatorname{im}\phi_2$ contains the squares and is surjective on $(\mathbb{Z}/8\mathbb{Z})^\times$, and thus is surjective. The sets $\{x\in R_\ell : \mathrm{ord}_\ell(1-\phi_i(x))=n\}$ all have the form $\phi_i^{-1}(S)$, where S is defined via congruence conditions modulo ℓ^{n+1}. Since the ϕ_i-preimage of any congruence class modulo ℓ^{n+1} contains the same number of classes, it follows that $\mu(\phi_i^{-1}(S))=\mu(S)$, where the first measure is the Haar measure on $R_\ell^\times$ and the second is that on $\mathbb{Z}_\ell^\times$. Therefore finding the integral in (4) reduces to the same computation as in Theorem 15, which comes to $h(\ell)$. □

Example 31. Let $K = \mathbb{Q}$, $A : y^2 = x^3 + 3x$, $\alpha = (1, -2)$ and $\ell = 5$. The elliptic curve A has CM by the full ring of integers in $\mathbb{Z}[i]$, and 5 splits in $\mathbb{Z}[i]$. One can compute the Mordell-Weil group $A(\mathbb{Q})$ and check that α is a generator. Hence $\alpha \notin \ell A(\mathbb{Q})$. One can check using MAGMA that $\mathrm{Gal}\,(\mathbb{Q}(A[25])/\mathbb{Q}) \cong H_2$. Thus the hypotheses of Theorem 27 are satisfied, and we conclude by Theorem 30 and Proposition 6 that $\overline{\alpha}$ has order prime to 5 for $((19/24)^2 + 19/24)/2 = 817/1152 \approx 0.71$ of primes p. Compare this to the generic value of $2381/2976 \approx 0.80$ in the non-CM case.

Example 32. Let $K = \mathbb{Q}$, $A : y^2 = x^3 + 3$, $\alpha = (1, 2)$ and $\ell = 2$. The elliptic curve A has CM by $\mathbb{Z}[\zeta_3]$, α is a generator of the Mordell-Weil group of A, and 2 is inert in $\mathbb{Z}[i]$. A straightforward computation using MAGMA shows that $\mathrm{Gal}\,(\mathbb{Q}(A[8])/\mathbb{Q}) \cong H_3$ and ω_1 is surjective. The image of Frobenius at 71 acts on the Galois closure of $\mathbb{Q}(\beta_1)$ with order 4, while it acts on $\mathbb{Q}(A[8])$ with order 2. Hence $\beta_1 \notin \mathbb{Q}(A[8])$. Thus the conclusion of Theorem 27 holds, and by Theorem 30 and Proposition 6 we conclude that $\overline{\alpha}$ has odd order for $(11/15 + 1/3)/2 = 8/15 \approx 0.533$ of primes p.

Example 33. Let $K = \mathbb{Q}$, $A : y^2 = x^3 - 207515x + 44740234$, $\alpha = (253, 2904)$ and $\ell = 2$. The elliptic curve A has CM by the full ring of integers in $\mathbb{Q}(\sqrt{-7})$, and 2 splits in this ring. A computation using MAGMA shows that the conditions in the remark following Proposition 28 are satisfied and thus the conclusion of Theorem 27 holds. By Theorem 30 and Proposition 6 we have that $\overline{\alpha}$ has odd order for $(1/9 + (1/3))/2 = 2/9 \approx 0.222$ of primes p.

Example 34. Let $K = \mathbb{Q}$, $A : y^2 = x^3 + 3x$, $\alpha = (1, -2)$ and $\ell = 2$. The elliptic curve A has CM by $\mathbb{Z}[i]$ and in this case ℓ is ramified. A lengthy computation shows that the image of ω has index 4 in $\mathbb{Z}_2^2 \rtimes H$, where

$$H = \left\{ \begin{bmatrix} a & b \\ \mp b & \pm a \end{bmatrix} : a, b \in \mathbb{Z}_2, a^2 + b^2 \equiv 1 \pmod 2 \right\}$$

is the corresponding Cartan normalizer. The image of ω_2 is generated by

$$\left((1,1), \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right), \left((0,0), \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right), \left((1,1), \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix} \right).$$

One can compute that in this case $\mathcal{F}(G) = \frac{17}{32} \approx 0.531$.

6. Higher-Dimensional Abelian Varieties

If the abelian algebraic group A is projective, then A is an abelian variety. In this section we will describe the case when $\dim(A) > 1$. Assume that $\phi = [\ell]$, the multiplication by ℓ map and let $d = \dim(A)$.

To determine the image of ω it is crucial to know about the image of $\rho : \mathrm{Gal}\,(K(A[\ell^\infty])/K) \hookrightarrow \mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$.

The Weil e_m-pairing is a nondegenerate, skew-symmetric, Galois invariant pairing $e_m : A[m] \times \hat{A}[m] \to \mu_m$. If $\Phi : A \to \hat{A}$ is a polarization defined over K, then the pairing $e_{m,\Phi} : A[m] \times A[m] \to \mu_m$ given by $e_{m,\Phi}(a,b) = e_m(a, \Phi(b))$ is skew-symmetric and Galois invariant. Moreover, it is nondegenerate provided that m is coprime to $\#\ker(\Phi)$. The Galois invariance and non-degeneracy implies that $I_n \subseteq \mathrm{GSp}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$, the group of symplectic similitudes.

The following result gives criteria for when the map to the Kummer part is surjective.

Theorem 35. *Let ℓ be prime, $d \geq 2$ and assume that $\gcd(\ell, \#\ker(\Phi)) = 1$, and the ℓ-adic representation ρ is surjective. Then the Kummer map $\kappa : \mathrm{Gal}\left(\overline{K}/K(A[\ell^\infty])\right) \to \mathbb{Z}_\ell^{2d}$ is surjective if and only if the following conditions hold:*

1. *$\alpha \notin \ell A(K)$,*
2. *if $\ell = 2$, $\beta_1 \not\subseteq K(A[2])$.*

Proof. The proof follows that of Theorem 20 mutatis mutandis. The only differences are that Vasiu's Theorem 4.1 now applies to the $\ell = 3$ case, and that we assume $\beta_1 \notin K(A[\ell])$ when $\ell = 2$. □

Remark. When $\ell = 2$, $\mathrm{GSp}_{2d}(\mathbb{F}_2) = \mathrm{Sp}_{2d}(\mathbb{F}_2)$. This group has subgroups $\mathrm{SO}^+_{2d}(\mathbb{F}_2)$ and $\mathrm{SO}^-_{2d}(\mathbb{F}_2)$ stabilizing the two isomorphism classes of quadratic forms of dimension $2d$. The former has index $2^{2d-1} + 2^{d-1}$ and the latter has index $2^{2d-1} - 2^{d-1}$. These indices sum to 2^{2d}. For $d \geq 2$, it therefore seems possible that the preimages of α might fall into one Galois orbit of size $2^{2d-1} - 2^{d-1}$ and one Galois orbit of size $2^{2d-1} + 2^{d-1}$. It is an interesting question whether or not this occurs.

We have the following surjectivity criteria for ρ.

Proposition 36. *Let ℓ be a prime, $d \geq 2$ and assume that $\gcd(\ell, \#\ker(\Phi)) = 1$. Then, the ℓ-adic representation $\rho : \mathrm{Gal}\left(K(A[\ell^\infty])/K\right) \to \mathrm{GSp}_{2d}(\mathbb{Z}_\ell)$ is surjective if and only if the following conditions hold:*

1. *Assume that K is linearly disjoint from $\mathbb{Q}(\zeta_{\ell^n})$ for all n.*
2. *Assume that $\mathrm{Gal}\left(K(A[\ell])/K\right) \cong \mathrm{GSp}_{2d}(\mathbb{Z}/\ell\mathbb{Z})$.*
3. *If $\ell = d = 2$ assume also that $K(A[\ell])$ is linearly disjoint from $\mathbb{Q}(\sqrt{2}, i)$.*

Proof. This is a restatement of Vasiu's Theorems 4.1 and 4.2.1 from [32]. □

Remark. Suppose that d is odd, $d = 2$ or $d = 6$, and $\mathrm{End}(A) \cong \mathbb{Z}$. Théorème 3 of [27, Résumé des cours de 1985-1986] implies that the conditions of the above proposition are satisfied for ℓ sufficiently large.

Corollary 37. *The arboreal representation $\omega : \mathrm{Gal}\left(K_\infty/K\right) \to (\mathbb{Z}_\ell)^4 \rtimes \mathrm{GSp}_4(\mathbb{Z}_\ell)$ is surjective if and only if the conditions of Theorem 35 and Proposition 36 are satisfied.*

Proof. Similar to that of 22. □

Example 38. Let C be the hyperelliptic curve with affine model $y^2 = f(x)$, where $f(x) = 4x^6 - 8x^5 + 4x^4 + 4x^2 - 8x + 5$ and let $A = \mathrm{Jac}(C)$. In [5, p. 2] a non-singular model for C is given by

$$Y^2 = 5X_0^2 - 8X_0X_1 + 4X_1^2 + 4X_2^2 - 8X_2X_3 + 4X_3^2$$
$$X_0X_2 = X_1^2, \qquad X_0X_3 = X_1X_2, \qquad X_1X_3 = X_2^2.$$

The two points at infinity are at $(X_0 : X_1 : X_2 : X_3 : Y) = (0 : 0 : 0 : 1 : -2)$ and $(0 : 0 : 0 : 1 : 2)$. Denote the first by ∞^+. Let $P = (1 : 1 : 1 : 1 : 1)$ and let $\alpha = \infty^+ - P \in A(\mathbb{Q})$.

Proposition 39. *With A and α given above, we have*

$$\mathrm{Gal}\left(K_\infty/K\right) \cong (\mathbb{Z}_\ell)^4 \rtimes \mathrm{GSp}_4(\mathbb{Z}_\ell)$$

for all primes ℓ.

Proof. It suffices to verify the conditions of Theorem 35 and Proposition 36. Note that since $J = \mathrm{Jac}(C)$, J is endowed with a canonical principal polarization, so $\#\ker(\Phi) = 1$.

Next, we check condition (1) of Theorem 35. The Kummer surface K associated to A is $A/\langle[-1]\rangle$. It is a quartic curve in $\mathbb{P}^3$ with nodes at the images of $A[2]$, the fixed points of $[-1]$. Multiplication by $[m]$ descends to a morphism of K, and one may use the map $\phi : A \to K$ to define a height function $h : A \to \mathbb{R}$ on A. Let $\hat{h}$ denote the corresponding canonical height. One may use MAGMA to verify that for all $P \in A(\mathbb{Q})$, $|h(P) - \hat{h}(P)| \leq 3.10933$ and that $\hat{h}(\alpha) = 0.247060$. Suppose to the contrary that there is a prime ℓ and $\beta \in A(\mathbb{Q})$ with $\ell\beta = \alpha$. Then, $\hat{h}(\beta) = \frac{1}{\ell^2}\hat{h}(\alpha)$ and hence $|h(\beta)| \leq 3.10933 + 0.247060$. Computing all points $P \in J(\mathbb{Q})$ satisfying the above bound, we find that there are no such β.

Condition (1) of Proposition 36 is obvious.

Next, we check condition (2) of Proposition 36. In [6], Dieulefait indicates how one can check that the mod ℓ Galois representations associated to an abelian surface are surjective at all but finitely many primes, conditional on Serre's conjecture. Using the algorithm of Liu ([21]), we find that the conductor of A divides $2^4 \cdot 3^5 \cdot 13 \cdot 31$. We use Dieulefait's recipe and the explicit computation of the characteristic polynomials of the images of Frobenius in $\mathrm{Aut}(A[\ell])$ afforded by MAGMA. We find that at all primes $\ell > 7$ of good reduction, the mod ℓ representation is surjective conditional on Serre's conjecture. The two-torsion points of $A[2]$ are the Weierstrass points of C, and hence $\mathbb{Q}(A[2])$ is the splitting field of $f(x)$. One can check that the Galois group of the splitting field of $f(x)$ is isomorphic to $S_6 \cong \mathrm{GSp}_4(\mathbb{Z}/2\mathbb{Z})$. Further, explicit computations mod 3, 5, 7, 13 and 31 show that the mod ℓ representation is surjective

there as well. We remark that Serre's conjecture has been proven thanks to work of Khare and Wintenberger [15] and [16], and Kisin [17].

Next, we check condition (3) of Proposition 36. Since $\mathbb{Q}(A[2])/\mathbb{Q}$ has Galois group S_6, there is a unique quadratic subfield of $\mathbb{Q}(A[2])$, and computing the discriminant of $f(x)$, we find it to be $\mathbb{Q}(\sqrt{-3 \cdot 13 \cdot 31})$. Hence, $\mathbb{Q}(A[2])$ is linearly disjoint from $\mathbb{Q}(\sqrt{2}, i)$, as desired.

Finally, we check condition (2) of Theorem 35. In Appendix I to [5], Cassels and Flynn make explicit the morphism on the Kummer surface K induced by the multiplication by 2 map on A. One can check that the image $\phi(\alpha)$ of α on K is $(0:1:1:-4)$. Using this, one may compute the preimages on K of the point $\phi(\alpha)$, which corresponds to $\alpha \in A(\mathbb{Q})$. This gives rise to a system of four quartic equations in four unknowns. Using MAGMA's Gröbner basis routine to solve the corresponding system of algebraic equations, we find that the sixteen preimages are of the form $(1 : a_1 : a_2 : a_3)$. Here a_1, a_2 and a_3 generate $\mathbb{Q}(\beta)$ where β has minimal polynomial

$$g(x) = x^{16} - 12x^{14} - 36x^{13} + 316x^{12} - 912x^{11} + 1412x^{10} - 472x^9 - 1764x^8 + 3544x^7 - 4104x^6 + 3912x^5 - 3588x^4 - 5888x^3 + 8232x^2 - 4576x + 884.$$

It follows that the preimages of $(0:1:1:-4)$ lie in degree 16 extensions of $\mathbb{Q}$ and hence $[\mathbb{Q}(\beta_1) : \mathbb{Q}] = 16$. Hence, we cannot have $\beta_1 \in \mathbb{Q}(A[2])$ since $\mathrm{Gal}\left(\mathbb{Q}(A[2])/\mathbb{Q}\right) \cong S_6$ has no subgroups of index 16. Thus condition (6) holds. It follows that the splitting field of $g(x)$ is K_1 and so the Galois group of $g(x)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4 \rtimes \mathrm{GSp}_4(\mathbb{Z}/2\mathbb{Z})$. □

Unfortunately, we have been unable to exactly compute the corresponding densities for the groups $\mathbb{Z}_\ell^4 \rtimes \mathrm{GSp}_4(\mathbb{Z}_\ell)$. The nature of the explicit method employed in Theorem 24 seems unlikely to be fruitful. Here is a table of bounds computed from conjugacy class information for $\mathrm{GSp}_4(\mathbb{Z}/\ell^n\mathbb{Z})$.

ℓ	Lower bound	Upper bound	n used
2	$\frac{26701}{46080}$ (≈ 0.579)	$\frac{1201}{2048}$ (≈ 0.586)	4
3	$\frac{70769}{103680}$ (≈ 0.683)	$\frac{27203}{38880}$ (≈ 0.700)	2

In general, if ℓ is prime and $G_\phi(\alpha) = \mathbb{Z}_\ell^4 \rtimes \mathrm{GSp}_4(\mathbb{Z}_\ell)$, we have

$$\frac{\ell^7 - 2\ell^6 - \ell^5 + 4\ell^4 - 2\ell^3 + 2\ell^2 - 5}{(\ell^4 - 1)(\ell^2 - 1)(\ell - 1)} \leq \mathcal{F}(G) \leq \frac{\ell^7 - \ell^6 - \ell^5 + 3\ell^4 - 2\ell^3 + \ell^2 - 4}{\ell^7 - \ell^5 - \ell^3 + \ell}.$$

These follow from the computation of the number of $M \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ with $\det(M - I) \not\equiv 0 \pmod{\ell}$ in [19, p.61].

Appendix A. A result relating to Question 3

by Jeff Achter

Fix a prime ℓ. This appendix provides a proof of:

Proposition 40. *The limit* $\lim_{g\to\infty} \mathcal{F}(\mathbb{Z}_\ell^{2g} \rtimes \mathrm{GSp}_{2g}(\mathbb{Z}_\ell))$ *exists.*

The proof requires some notation concerning symplectic groups. Let ℓ be a fixed prime. For each natural number g, fix a free $\mathbb{Z}_\ell$-module V_g of rank $2g$, equipped with a symplectic pairing $\langle\cdot,\cdot\rangle$. For each natural number n, let $V_{g,n} = V_g \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell$. After a choice of basis of V, we have $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) \cong \mathrm{GSp}(V_{g,n}, \langle\cdot,\cdot\rangle)$. For natural numbers $n \geq m$, let $\rho_{g,n,m} : \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) \to \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^m\mathbb{Z}_\ell)$ and $\rho_{g,n} : \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) \to \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)$ be the usual reduction maps. For any ring Λ there is a group homomorphism $\mathrm{mult} : \mathrm{GSp}_{2g}(\Lambda) \to \Lambda^\times$, and $\mathrm{Sp}_{2g}(\Lambda) = \mathrm{mult}^{-1}(1)$. For $0 \leq r \leq g$ define

$$S(g,r,n) = \frac{\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)}{\#\mathrm{Sp}_{2r}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)\#\mathrm{Sp}_{2(g-r)}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \tag{6}$$

$$L(g,n) = \frac{\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)}{\#\,\mathrm{GL}_g(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)\cdot\#\,\mathrm{GL}_g(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)}, \tag{7}$$

with the convention that for $g = 0$, $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)$ and $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)$ are the trivial group. Then $S(g,r,n)$ is the number of decompositions $V_{g,n} = E \oplus W$ where $E \cong V_{r,n}$ and $W \cong V_{g-r,n}$, while $L(g,n)$ is the number of decompositions $V_{g,n} = E \oplus W$ where E and W are each isotropic. Recall that $\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell) = \prod_{j=1}^g \ell^{2j-1}(\ell^{2j}-1)$, $\#\,\mathrm{GL}_g(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell) = \prod_{j=1}^g \ell^{j-1}(\ell^j-1)$, and $\#\,\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) = \#((\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^\times)\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)$.

For $x \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)$, let

$$\epsilon(x) = \min\{\mathrm{ord}_\ell(\det(\widetilde{x} - \mathrm{id})) : \widetilde{x} \in \rho_{g,n}^{-1}(x)\}.$$

Set

$$F(g,n) = \frac{1}{\#\,\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \sum_{x \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \ell^{-\epsilon(x)}.$$

Lemma 41. *For each* g *and* n, $\left|\mathcal{F}(\mathbb{Z}_\ell^{2g} \rtimes \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)) - F(g,n)\right| < \ell^{-n}$.

Proof. Let $C_{g,n} = \{x \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) : \epsilon(x) < n\}$. If $x \in C_{g,n}$ and if $\widetilde{x} \in \rho_{g,n}^{-1}(x)$, then $\mathrm{ord}_\ell(\det(\widetilde{x} - \mathrm{id})) = \epsilon(x)$. Let $\widetilde{D}_{g,n} = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) - \rho_{g,n}^{-1}(C_{g,n})$. By Theorem 10,

we have

$$\begin{aligned}\left|F(g,n) - \mathcal{F}(\mathbb{Z}_\ell^{2g} \rtimes \mathrm{GSp}_{2g}(\mathbb{Z}_\ell))\right| &= \int_{\widetilde{D}_{g,n}} (\ell^{-n} - \ell^{-\mathrm{ord}_\ell(\widetilde{x})}) d\mu \\ &\leq \ell^{-n}\mu(\widetilde{D}_{g,n}) < \ell^{-n}.\end{aligned}$$

□

Define subsets of $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)$

$$\begin{aligned}\mathcal{U}_{g,n} &= \{x \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) : \text{each eigenvalue of } \rho_{g,n,1}(x) \text{ is 1 or } \mathrm{mult}(x) \bmod \ell\} \\ \mathcal{N}_{g,n} &= \{x \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) : \rho_{g,n,1}(x) - \mathrm{id} \text{ is invertible}\}\end{aligned}$$

and quantities

$$\begin{aligned}a_{g,n} &= \frac{\#\mathcal{U}_{g,n}}{\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)}, \qquad b_{g,n} = \frac{\#\mathcal{N}_{g,n}}{\#\,\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)}, \\ h(g,n) &= \frac{1}{\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \sum_{x \in \mathcal{U}_{g,n}} \ell^{-\epsilon(x)}.\end{aligned}$$

We adopt the convention that for $g = 0$, $\mathcal{U}_{0,n} = \mathcal{N}_{0,n} = \mathrm{GSp}_0(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)$. In particular, $a_{0,n} = b_{0,n} = 1$.

Lemma 42. *For each g and n, $a_{g,n} = a_{g,1}$ and $b_{g,n} = b_{g,1}$.*

Proof. Membership in $\mathcal{U}_{g,n}$ or in $\mathcal{N}_{g,n}$ is detectable modulo ℓ, and $\rho_{g,n,1}$ is a surjective homomorphism. □

Henceforth, let $a_g = a_{g,1}$ and $b_g = b_{g,1}$.

Lemma 43. *We have $a_1 = \frac{\ell^2-2}{(\ell^2-1)(\ell-1)}$. If $g \geq 2$, then $a_g < (\frac{\ell^3}{\ell^4-1})^{g-1} a_1$.*

Proof. The first claim follows from the calculation of c_1 in the proof of Theorem 24. For the second, suppose $g \geq 2$. Recall that if H is a finite group of Lie type over $\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell$, then the number of unipotent elements in H is $\ell^{\dim H - \mathrm{rank} H}$ [30]. Therefore, the number of unipotent elements in $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)$ is ℓ^{2g^2}, and the number of unipotent elements in $\mathrm{GL}_g(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)$ is ℓ^{g^2-g} . If $x \in \mathcal{U}_{g,1}$ is not unipotent, then there is a decomposition $V_{g,1} = E \oplus W$ where E and W are Lagrangian subspaces, $x|_E$ is unipotent, and $x|_W$ is uniquely determined by $\mathrm{mult}(x)$ and $x|_E$. The number of such decompositions of $V_{g,1}$ is $L(g,1)$, and the number of choices for $\mathrm{mult}(x)$ is $(\ell-2)$. By

(6) and (7),

$$\begin{aligned} a_g = \frac{\#\mathcal{U}_{g,1}}{\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)} &= \frac{\ell^{2g^2}}{\prod_{j=1}^{g}\ell^{2j-1}(\ell^{2j}-1)} + \frac{(\ell-2)\ell^{g^2-g}}{\prod_{j=1}^{g}\ell^{2(j-1)}(\ell^j-1)^2} \\ &= \prod_{j=1}^{g}\frac{\ell^{2j-1}}{\ell^{2j}-1} + \frac{\ell-2}{\prod_{j=1}^{g}(\ell^j-1)^2} \\ &< \left(\prod_{j=1}^{g-1}\frac{\ell^{2j-1}}{\ell^{2j}-1} + \frac{\ell-2}{\prod_{j=1}^{g-1}(\ell^j-1)^2}\right)\frac{\ell^{2g-1}}{\ell^{2g}-1} \\ &\leq a_{g-1}\frac{\ell^3}{\ell^4-1}. \end{aligned}$$

□

Define generating functions $A(T) = \sum_{g\geq 0} a_g T^g$ and $B(T) = \sum_{g\geq 0} b_g T^g$.

Lemma 44. *If $\ell \geq 3$, then there is a number $R > 1$ such that $A(T)$ is analytic and nonvanishing on the (complex) disk $|T| < R$.*

Proof. By Lemma 43, $\sum_{g\geq 1} a_g \leq a_1 \sum_{m\geq 0}(\ell^3/(\ell^4-1))^m$. Because $\ell \geq 3$, $\sum_{g\geq 1} a_g < 1 = a_0$. Therefore, $A(T)$ defines a nonvanishing analytic function on $|T| \leq 1$. □

Suppose $x \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) \cong \mathrm{GSp}(V_{g,n})$. Then x uniquely determines a decomposition

$$V_{g,n} = E_x \oplus W_x, \tag{8}$$

where $E_x \cong V_{r,n}$ for some r, $W_x \cong V_{g-r,n}$, $x|_{E_x} \in \mathcal{U}_{r,n}$, and $x|_{W_x} \in \mathcal{N}_{g-r,n}$. Therefore,

$$\begin{aligned} \#\,\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) &= \sum_{r=0}^{g} S(g,r,n)\#\mathcal{U}_{r,n}\#\mathcal{N}_{g-r,n} \\ &= \#\,\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)\sum_{r=0}^{g}\frac{\#\mathcal{U}_{r,n}}{\#\mathrm{Sp}_{2r}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)}\frac{\#\mathcal{N}_{g-r,n}}{\#\,\mathrm{GSp}_{2(g-r)}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)}, \end{aligned}$$

so that

$$\sum_{r=0}^{g} a_{r,n}b_{g-r,n} = 1. \tag{9}$$

Lemma 45. *The limit $\lim_{g\to\infty} b_g$ exists.*

Proof. Suppose $\ell \geq 3$. By (9), there is an equality of power series

$$A(T)\cdot B(T) = \sum_{g\geq 0} T^g = \frac{1}{1-T}.$$

By Lemma 44, there exists a number $R > 1$ such that the function $C(T) := 1/A(T)$ is analytic inside $|T| < R$. Let $C(T) = \sum c_g T^g$ be the series expansion of C centered at the origin. Since $B(T) = C(T)/(1-T)$, we have

$$b_g = \sum_{j=1}^{g} c_j.$$

Since $C(1)$ is well-defined, $\lim_{g\to\infty} b_g = C(1)$ exists.

If $\ell = 2$ then for each g, $\mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z}) = \mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z})$, and $x \in \mathcal{N}_g$ if and only if x is "eigenvalue-free" in the sense of [22]. The existence of $\lim_{g\to\infty} b_g$ follows immediately from [22, Thm. 5.3].

□

Proof of Proposition 40. By Lemma 41, it suffices to show that for each n, $\lim_{g\to\infty} F(g,n)$ exists. So, fix a natural number n; we will calculate $F(g,n)$ explicitly.

Suppose $x \in \mathrm{GSp}(V_{g,n}) \cong \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)$. Under the decomposition (8), $\epsilon(x) = \epsilon(x|_E)$. Since $S(g,r,n)/\#\,\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) = (\#\,\mathrm{GSp}_{2(g-r)}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)\cdot\#\mathrm{Sp}_{2r}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell))^{-1}$, we have

$$\begin{aligned} F(g,n) &= \frac{1}{\#\,\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \sum_{0\le r\le g} S(g,r,n)\cdot \#\mathcal{N}_{g-r,n} \cdot \sum_{x\in \mathrm{GSp}_{2r}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \ell^{-\epsilon(x)} \\ &= \sum_{0\le r\le g} \frac{\#\mathcal{N}_{g-r,n}}{\#\,\mathrm{GSp}_{2(g-r)}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \cdot \frac{1}{\#\mathrm{Sp}_{2r}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \sum_{x\in \mathrm{GSp}_{2r}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \ell^{-\epsilon(x)} \\ &= \sum_{0\le r\le g} b_{g-r,n} h(g,n) = \sum_{0\le r\le g} b_g h(g,n), \end{aligned}$$

by Lemma 42. Since $h(g,n) \le a_{g,n}/\ell = a_g/\ell$, it follows from Lemmas 43 and 45 that

$$\lim_{g\to\infty} F(g,n) = \lim_{g\to\infty} \sum_{0\le r\le g} b_g h(g,n)$$

exists. □

Appendix B. Numerical Data

In this appendix, we give numerical data related to the examples given in the paper. Each table below includes several choices of x, the number of primes $\le x$ where α (and/or A) has good reduction (total primes), and the number of such primes where the order of α is coprime to ℓ (good primes), and the ratio.

The following is data for Example 14, $A : x^2 - y^2 = 1$, with $\ell = 2$ and $\alpha = \left(\frac{5}{3}, \frac{4}{3}\right)$.

x	10^3	10^4	10^5	10^6	10^7	∞
Good primes	57	406	3197	26200	221805	
Total primes	167	1228	9591	78497	664578	
Ratio	.34132	.33062	.33333	.33377	.33375	.33333

The following is data for Example 16, $A : x^2 + 7y^2 = 1$, $\ell = 7$ and $\alpha = \left(\frac{3}{4}, \frac{1}{4}\right)$.

x	10^3	10^4	10^5	10^6	10^7	∞
Good primes	115	870	6805	55608	470765	
Total primes	167	1228	9591	78497	664578	
Ratio	.68862	.70847	.70952	.70841	.70837	.70833

The following is data for Example 18, $A : x^3 + 2y^3 + 4z^3 - 6xyz = 1$, with $\ell = 2$ and $\alpha = (-1, 1, 0)$.

x	10^3	10^4	10^5	10^6	10^7	∞
Good primes	62	492	3840	31353	265226	
Total primes	168	1229	9592	78498	664579	
Ratio	.36905	.40033	.40033	.39941	.39909	.39881

The following is data for Example 23, $A : y^2 + y = x^3 - x$, with $\ell = 2$ and $\alpha = (0, 0)$.

x	10^3	10^4	10^5	10^6	10^7	∞
Good primes	93	654	5029	41080	348035	
Total primes	167	1228	9591	78497	664578	
Ratio	.55689	.53257	.52434	.52333	.52369	.52381

The following is data for Example 32, $A : y^2 = x^3 + 3$, $\ell = 2$ and $\alpha = (1, 2)$.

x	10^3	10^4	10^5	10^6	10^7	∞
Good primes	90	670	5093	41868	354068	
Total primes	166	1227	9590	78496	664577	
Ratio	.54217	.54605	.53107	.53338	.53277	.53333

The following is data for Example 33, $A : y^2 = x^3 - 207515x + 44740234$, $\ell = 2$ and $\alpha = (253, 2904)$.

x	10^3	10^4	10^5	10^6	10^7	∞
Good primes	39	269	2113	17407	147714	
Total primes	165	1226	9589	78495	664576	
Ratio	.23636	.21941	.22036	.22176	.22227	.22222

The following is data for Example 34, $A : y^2 = x^3 + 3x$, $\ell = 2$ and $\alpha = (1, -2)$.

x	10^3	10^4	10^5	10^6	10^7	∞
Good primes	89	663	5082	41757	353023	
Total primes	166	1227	9590	78496	664577	
Ratio	.53614	.54034	.52993	.53196	.53120	.53125

The following is data for Example 38, $A = \mathrm{Jac}(C)$ where $C : y^2 = 4x^6 - 8x^5 + 4x^4 + 4x^2 - 8x + 5$, $\ell = 2$ and $\alpha = \infty^+ - P$.

x	10^3	10^4	10^5	10^6	10^7	∞
Good primes	101	725	5584	45832	388144	
Total primes	164	1225	9588	78494	664575	
Ratio	.61585	.59183	.58239	.58389	.58405	$0.57944 \leq \mathcal{F} \leq 0.58643$

ACKNOWLEDGEMENTS

We would like to thank Ken Ribet, Daniel Bertrand, Wojciech Gajda, Ken Ono, Ram Murty, Nigel Boston, and Jordan Ellenberg for helpful discussions and feedback.

References

[1] Wayne Aitken, Farshid Hajir, and Christian Maire. Finitely ramified iterated extensions. *Int. Math. Res. Not.*, (14):855–880, 2005.

[2] Marc Bachmakov. Un théorème de finitude sur la cohomologie des courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 270:A999–A1001, 1970.

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

[4] Nigel Boston and Rafe Jones. The image of an arboreal galois representation. preprint.

[5] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[6] L. V. Dieulefait. Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$. *Experiment. Math.*, 11(4):503–512 (2003), 2002.

[7] Wojciech Gajda and Krzysztof Gornisiewicz. Linear dependence in Mordell-Weil groups. *J. Reine Angew. Math.*, to appear.

[8] Helmut Hasse. Über 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.

[9] Helmut 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.

[10] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[11] Olivier Jacquinot and Kenneth A. Ribet. Deficient points on extensions of abelian varieties by $\mathbf{G}_m$. *J. Number Theory*, 25(2):133–151, 1987.

[12] Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. available at http://arxiv.org/abs/math/0612415.

[13] Rafe Jones. Iterated Galois towers, their associated martingales, and the p-adic Mandelbrot set. *Compositio Math.*, to appear.
[14] Richard Gottesman and Kwokfung Tang. Quadratic recurrences with a positive density of prime divisors. Preprint.
[15] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture (i). Preprint.
[16] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture (ii). Preprint.
[17] M. Kisin. Modularity of 2-adic Barsotti-Tate representations. Preprint.
[18] E. Kowalski. Some local-global applications of Kummer theory. *Manuscripta Math.*, 111(1):105–139, 2003.
[19] Doug Kuhlman. *On the orders of Jacobians of hyperelliptic curves*. PhD thesis, University of Illinois at Urbana-Champaign, 2000.
[20] J. C. Lagarias. The set of primes dividing the Lucas numbers has density 2/3. *Pacific J. Math.*, 118(2):449–461, 1985.
[21] Qing Liu. Conducteur et discriminant minimal de courbes de genre 2. *Compositio Math.*, 94(1):51–79, 1994.
[22] Peter M. Neumann and Cheryl E. Praeger. Derangements and eigenvalue-free elements in finite classical groups. *J. London Math. Soc. (2)*, **58**(3): 564-586, 1998.
[23] Pieter Moree. On primes p for which d divides $\mathrm{ord}_p(g)$. *Funct. Approx. Comment. Math.*, 33:85–95, 2005.
[24] Richard Pink. On the order of the reduction of a point on an abelian variety. *Math. Ann.*, 330(2):275–291, 2004.
[25] Kenneth A. Ribet. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.*, 46(4):745–761, 1979.
[26] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
[27] J.-P. Serre. *Œuvres. Collected papers. IV*. Springer-Verlag, Berlin, 2000. 1985–1998.
[28] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.
[29] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.
[30] T. A. Springer and R. Steinberg. Conjugacy classes. *Seminar on Algebraic Groups and Related Finite Groups* (The Institute for Advanced Study, Princeton, N.J., 1968/69), pp. 167–266. Lecture Notes in Mathematics, Vol. 131, Springer, Berlin, 1970.
[31] Michael Stoll. Galois groups over $\mathbf{Q}$ of some iterated polynomials. *Arch. Math. (Basel)*, 59(3):239–244, 1992.
[32] A. Vasiu. Surjectivity criteria for p-adic representations. II. *Manuscripta Math.*, 114(4):399–422, 2004.
[33] John S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1998.

Department of Mathematics, University of Wisconsin, Madison, WI 53706

E-mail address: jones@math.wisc.edu

E-mail address: rouse@math.wisc.edu