Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

Galois Theory of Iterated Endomorphisms

Rafe Jones and Jeremy Rouse

Abstract

Given an abelian algebraic group A over a global field F, $\alpha \in A(F)$, and a prime ℓ, the set of all preimages of α under some iterate of $[\ell]$ generates an extension of F that contains all ℓ-power torsion points as well as a Kummer-type extension. We analyze the Galois group of this extension, and for several classes of A we give a simple characterization of when the Galois group is as large as possible up to constraints imposed by the endomorphism ring or the Weil pairing. This Galois group encodes information about the density of primes $\mathfrak{p}$ in the ring of integers of F such that the order of $(\alpha \bmod \mathfrak{p})$ is prime to ℓ. We compute this density in the general case for several classes of A, including elliptic curves and one-dimensional tori. For example, if F is a number field, A/F is an elliptic curve with surjective 2-adic representation and $\alpha \in A(F)$ with $\alpha \notin 2A(F(A[4]))$, then the density of $\mathfrak{p}$ with $(\alpha \bmod \mathfrak{p})$ having odd order is $11/21$.

1. *Introduction*

Let F be a global field, A an abelian algebraic group defined over F, $\alpha \in A(F)$, and ℓ a prime. The tower of extensions $F([\ell^n]^{-1}(\alpha)), n \geq 1$ contains all ℓ-power torsion points for A, as well as a Kummer-type extension. The action of the absolute Galois group $\mathrm{Gal}\,(F^{\mathrm{sep}}/F)$ on this tower encodes density information about the orders of reductions $\alpha \bmod \mathfrak{p}$, as $\mathfrak{p}$ varies over primes of the ring of integers of F (or $F[C]$ if $F := F(C)$ is the function field of the affine curve C). (See Theorem 3.2.) In this paper we give criteria that ensure the Galois action on the tower $F([\ell^n]^{-1}(\alpha)), n \geq 1$ is as large as possible given natural constraints arising from the Weil pairing or endomorphisms not in $\mathbb{Z}$, and compute the associated density. We prove results such as:

Theorem 1.1. *Let F be a number field with ring of integers $\mathcal{O}_F$, E an elliptic curve defined over F, $\alpha \in E(F)$, and ℓ a prime. Suppose that $\alpha \notin \ell A(F)$ and the ℓ-adic Galois representation associated to E surjects onto $\mathrm{GL}_2(\mathbb{Z}_\ell)$. If $\ell = 2$, suppose in addition that $\alpha \notin 2A(F(A[4]))$. Then the density of primes $\mathfrak{p} \subset \mathcal{O}_F$ with $\alpha \bmod \mathfrak{p}$ having order prime to ℓ is*

$$\frac{\ell^5 - \ell^4 - \ell^3 + \ell + 1}{\ell^5 - \ell^3 - \ell^2 + 1}.$$

The hypotheses of Theorem 1.1 are easy to verify for specific E (see Proposition 5.1). The $\ell = 2$ case yields the following corollary.

Corollary 1.2. *The Somos-4 sequence is defined by $a_0 = a_1 = a_2 = a_3 = 1$ and for $n \geq 4$ by*

$$a_n = \frac{a_{n-1}a_{n-3} + a_{n-2}^2}{a_{n-4}}.$$

2000 *Mathematics Subject Classification* 11F80 (primary), 14L10, 14K15 (secondary).

The first author's research was partially supported by NSF grant DMS-0852826.

The density of primes $p \in \mathbb{Z}$ dividing at least one term of this sequence is 11/21.

Proof. Let E be defined by $y^2 + y = x^3 - x$, and let $\alpha = (0, 0)$. Assume for a moment that

$$[2n-3]\alpha = \left(\frac{a_n^2 - a_{n-1}a_{n+1}}{a_n^2}, \frac{a_{n-1}^2 a_{n+2} - 2a_{n-1}a_n a_{n+1}}{a_n^3} \right). \tag{1.1}$$

It follows that $p \mid a_n$ precisely when $[2n-3]\alpha \equiv O \bmod p$, which occurs if and only if α has odd order modulo p. In Example 5.4 we check the hypotheses of Theorem 1.1 for E and α, showing that the density of p such that α has odd order modulo p is 11/21.

To prove (1.1), one can use the group law on E to reduce (1.1) to the identity

$$F(a_{n-1}, a_n, a_{n+1}, a_{n+2}) = 0, \text{ where } F(a,b,c,d) = a^2d^2 - 4abcd + ac^3 + b^3d + b^2c^2.$$

It is easy to see that $F(a_{n-1}, a_n, a_{n+1}, a_{n+2}) = \frac{a_{n+2}}{a_{n-2}} F(a_{n-2}, a_{n-1}, a_n, a_{n+1})$. Equation (1.1) now follows by induction and the fact that $F(1,1,1,1) = 0$. □

We also examine the Galois action on the tower $F([\ell^n]^{-1}(\alpha)), n \geq 1$ in the context of abelian algebraic groups other than elliptic curves. Our analysis has two components: first, to give explicit conditions on A and α that guarantee the Galois action is as large as possible (subject to natural constraints such as commutativity with the Weil pairing or the action of endomorphism rings larger than $\mathbb{Z}$) and second, to compute the associated density in the case where the Galois action is as large as possible.

In pursuit of the first goal, we begin by setting K_∞ to be the union over $n \geq 1$ of the extensions $F([\ell^n]^{-1}(\alpha))$. The group $\mathrm{Gal}\,(K_\infty/F)$ acts naturally on the tree of preimages of α under repeated applications of ℓ, and thus we refer to the map

$$\omega : \mathrm{Gal}\,(F^{\mathrm{sep}}/F) \to \mathrm{Gal}\,(K_\infty/F)$$

as the *arboreal Galois representation* associated to A and α. The image of ω has as a quotient the usual ℓ-adic Galois representation attached to A, given by the action of Galois on the Tate module $T_\ell(\alpha)$ of A. The kernel of this quotient map is isomorphic to subgroup of $T_\ell(\alpha)$ (see p. 6 for details), and we refer to it as the *Kummer part* of the image of ω. The image of the ℓ-adic representation has been the subject of much study, and explicit conditions ensuring surjectivity (up to constraints imposed by the endomorphism ring or the Weil pairing) are generally known; here we collect them and give a few additions in the cases where ℓ is 2 or 3. Generally speaking, surjectivity modulo a low power of ℓ (usually 1) ensures ℓ-adic surjectivity. See Propositions 4.1 (for A a one-dimensional torus), 5.1 (for A and elliptic curve without complex multiplication), 5.7 (for A an elliptic curve with complex multiplication), and 6.1 (for A a higher-dimensional abelian variety). The study of the surjectivity of the Kummer part originated in [**1**], [**29**], and has continued recently thanks in part to applications to the support problem (see [**20**] for an overview). Our contribution is to give a simple characterization of when the Kummer part is the full Tate module for certain classes of A (see Theorems 4.2, 5.2, 5.8, 6.2). In the latter three theorems, for all $\ell \neq 2$ the condition is just $\alpha \notin \ell A(F)$. In the cases we consider, this makes explicit [**2**, 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 [**27**, Theorem 2.8] and [**8**, Proposition 2.10] for the latter statement). This result stems essentially from work of Ribet [**29**], [**14**], 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.

Our second goal is to compute, in the case where ω is surjective up to natural constraints, the density of $\mathfrak{p}$ such that $\alpha \bmod \mathfrak{p}$ has order prime to ℓ. In Theorem 3.8, we give a method for computing this density, and carry out this computation when A is a one-dimensional torus

(Proposition 4.5) or an elliptic curve (Theorem 5.5 in the non-CM case, and Theorem 5.10 in the CM case). For instance, when $A = E$ is an elliptic curve with complex multiplication, in general $\alpha \bmod \mathfrak{p}$ has odd order for a set of $\mathfrak{p}$ of density 2/9 when 2 splits in the CM ring of E, and 8/15 when 2 is inert in the CM ring of E. That the image of $\omega(\mathrm{Frob}_{\mathfrak{p}})$ encodes ℓ-power divisibility properties of $|\alpha \bmod \mathfrak{p}|$ has already been established for abelian varieties in [**27**] (see also [**8**, Proposition 2.11]), where it is shown that various phenomena occur for all primes in a set of positive Dirichlet density. However, no densities are computed for specific varieties. On the other hand, work originating with Hasse [**10**], [**11**] and including Moree [**25**] and others has led to the computation of all such densities in the case where A is a trivial one-dimensional torus.

In Section 2 we develop some general aspects of arboreal Galois representations for any quasi-projective variety V. In Section 3 we specialize to the case where $V = A$ is an abelian algebraic group. We discuss in detail the Kummer part of the image of ω, and its relation to the image of the usual ℓ-adic representation. We also give general criteria for the Kummer part to be the full Tate module (Theorem 3.4), and show that when this occurs we can determine $\mathcal{F}(G_\phi(\alpha))$ via a certain matrix computation (Theorem 3.8). 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 [**25**], 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. In Section 6 we treat the case of higher-dimensional abelian varieties. Although we are able to give explicit criteria ensuring that the Kummer part is the full Tate module (Theorem 6.2), the complexity of $\mathrm{GSp}_{2d}(\mathbb{Z}_\ell)$ makes the computation described in Theorem 3.8 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 $\mathfrak{p}$ such that $|\alpha \bmod \mathfrak{p}|$ is odd moves farther from the naive value of 1/2 in the dimension 2 case.

QUESTION 1.3. 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 1.3 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.

Acknowledgements. The authors are grateful to Antonella Perucca for her contributions to and close reading of the proof of Theorem 3.2, and for many useful comments. We extend a special thanks to the referee for a very close and helpful reading of the manuscript, and for an extensive set of detailed comments on ways to streamline the arguments in the paper. We would also like to thank Ken Ribet, Daniel Bertrand, Wojciech Gajda, Ken Ono, Ram Murty, Nigel Boston, and Jordan Ellenberg for helpful discussions and feedback. Finally, we have extensively used the computer package MAGMA [**3**] for computations.

2. *Preliminaries*

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.

Let V be a quasiprojective variety and $\phi : V \to V$ be a finite morphism, both defined over F. 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 adjacent 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 F obtained by adjoining the coordinates of the elements of U_n, and let $K_\infty := \bigcup_n K_n$. Put $\mathcal{G}_n = G_{n,\phi}(\alpha) := \mathrm{Gal}\,(K_n/F)$, and note that $\mathcal{G}_n$ 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 set

$$\mathcal{F}(G_\phi(\alpha)) := \mu(\{g \in G_\phi(\alpha) : g \text{ fixes at least one end of } T_\phi(\alpha)\}).$$

Remark. A straightforward argument using the definitions yields

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

This limit exists since the sequence is bounded and monotonically decreasing.

A primary consideration in this paper is reduction modulo $\mathfrak{p}$ of a quasiprojective variety and its self-morphisms. We sketch here what we mean by this; our discussion is an abbreviated form of that in [**20**, pp. 107-108]. There exists a reduced scheme $\mathcal{V}/\mathcal{O}$ of finite type such that V is the generic fiber of $\mathcal{V}$, as one can see by, loosely speaking, eliminating denominators in the defining equations of V. We denote by $V_\mathfrak{p}$ the fiber of $\mathcal{V}$ over $\mathfrak{p}$, and by $f_\mathfrak{p}$ the finite field $\mathcal{O}/\mathfrak{p}$. Given $\alpha \in V(F)$ and a finite morphism $\phi : V \to V$, for all but finitely many $\mathfrak{p}$ the following hold: $V_\mathfrak{p}$ is quasiprojective, there is a reduction $\alpha_\mathfrak{p} \in V_\mathfrak{p}(f_\mathfrak{p})$ of α that is independent of the choice of $\mathcal{V}$, and there is a reduced morphism $\overline{\phi} : V_\mathfrak{p} \to V_\mathfrak{p}$ with $\deg \overline{\phi} = \deg \phi$.

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 F. By the density of a set S of primes of F, we mean the Dirichlet density

$$D(S) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}}, \tag{2.1}$$

where $N(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$. Note that the limit above does not exist for all sets of primes, and so we define the upper density $D^+(S)$ to be the expression in (2.1) with lim replaced by lim sup. There is a stronger notion called natural density, given by

$$d(S) = \lim_{n\to\infty} \#\{\mathfrak{p} \in S : N(\mathfrak{p}) \le n\}/\#\{\mathfrak{p} : N(\mathfrak{p}) \le n\}.$$

In the case where F is a number field, the results of this paper hold with $D(S)$ replaced by $d(S)$, due to the Chebotarev density theorem (in the function field case, Chebotarev's theorem requires additional hypotheses to give results about natural density).

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.

PROPOSITION 2.1. *Assume the notation above, and let*

$$S = \{\mathfrak{p} \subset \mathcal{O} : \overline{\alpha} \in V(f_{\mathfrak{p}}) \text{ is periodic under } \overline{\phi}\}.$$

Then $\mathcal{F}(G_\phi(\alpha)) \geq D^+(S)$. *In particular, if* $D(S)$ *exists then* $\mathcal{F}(G_\phi(\alpha)) \geq D(S)$.

REMARK. In Theorem 3.2 we give conditions that imply $D(S)$ exists and that the inequality is an equality.

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

$$\Omega_n = \{\mathfrak{p} : \mathfrak{p} \text{ is unramified in } K_n \text{ and } \overline{\phi}^n(x) = \overline{\alpha} \text{ has no solution in } V(f_{\mathfrak{p}}) \}.$$

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

$$D^+(\mathrm{Per}(\phi, \alpha)) \leq 1 - D^+(\Omega_n). \tag{2.2}$$

Let G_F be Galois group of the separable closure of F, and let $\mathrm{Frob}_{\mathfrak{p}} \subset G_F$ 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 $C \subseteq \mathcal{G}_n$ exists and is $\#C/\#\mathcal{G}_n$.

Let $\mathfrak{p}$ be a prime of F not ramifying in K_n and such that $\deg \overline{\phi} = \deg \phi$; this excludes only a finite number. There exists $\gamma \in V(f_{\mathfrak{p}})$ 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 $\mathfrak{p}$ exists and equals

$$\#\{\sigma \in \mathcal{G}_n : \sigma \text{ fixes at least one element of } U_n\}/\#\mathcal{G}_n.$$

Let us denote this quantity by d_n, and note that $d_n = D(\Omega_n^c) = 1 - D(\Omega_n)$ (so in particular $D(\Omega_n)$ exists). By (2.2) we now have $D^+(\mathrm{Per}(\phi, \alpha)) \leq \lim_{n\to\infty} d_n$, and this last limit is just $\mathcal{F}(G)$. □

We close this section with some general remarks about arboreal representations. A natural question to ask is when $G_\phi(\alpha)$ must have finite index in $\mathrm{Aut}(T_\phi(\alpha))$, where the latter indicates the full group of tree automorphisms. Certainly this need not happen all the time, as the examples in the rest of this paper show: when V has a group structure, automorphisms of $T_\phi(\alpha)$ failing to commute with the group law cannot be Galois elements, preventing $G_\phi(\alpha)$ from being a large subgroup of $\mathrm{Aut}(T_\phi(\alpha))$. There are, however, situations where $G_\phi(\alpha) \cong \mathrm{Aut}(T_\phi(\alpha))$, such as when $F = \mathbb{Q}$, $V = \mathbb{P}^1$, $\phi = x^2 + 1$, and $\alpha = 0$ [**37**]. Indeed, a similar result holds for infinitely many ϕ in the family $x^2 + c$ [**37**], though even in this family open questions remain: for $c = 3$, $|\mathrm{Aut}(T_\phi(\alpha)) : G_\phi(\alpha)| \geq 2$, and the index is not known to be finite. Less is known about the more general question of whether $|\mathrm{Aut}(T_\phi(\alpha)) : G_\phi(\alpha)|$ must be finite in the case $F = \mathbb{Q}$ and $V = \mathbb{P}^1$. The first author has shown finite index for ϕ belonging to two infinite families of quadratic polynomials [**15**, Section 3], but otherwise the question remains open. For a related discussion, see [**4**]. We note that in the case where $|\mathrm{Aut}(T_\phi(\alpha)) : G_\phi(\alpha)|$ is finite, we have $\mathcal{F}(G) = 0$; this follows from natural generalizations of [**16**, Section 5].

3. *Arboreal representations associated to abelian algebraic groups*

In this section, we specialize to the case where $V = A$ is an abelian algebraic group and ϕ is multiplication by a prime ℓ. We first give an interpretation of $\mathcal{F}(G_\phi(\alpha))$ in this case, then we describe the Galois groups $\mathcal{G}_n := \mathrm{Gal}\,(F(U_n)/F)$ in terms of the groups $A[\ell^n] := \{x \in A : \ell^n x = 0\}$ and their automorphism groups. We show that the image $G_\phi(\alpha)$ of $\omega = \omega_{\phi,\alpha} : \mathrm{Gal}\,(F^{\mathrm{sep}}/F) \to \mathrm{Aut}(T_\phi(\alpha))$ 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 $\alpha \in A(F)$, and we refer to $G_\phi(\alpha)$, $T_\phi(\alpha)$ and $\mathcal{F}(G_\phi(\alpha))$ as G, T, and $\mathcal{F}(G)$, respectively. We denote the group operation on A additively. We assume that $\phi = [\ell]$ has degree ℓ^d and is finite and separable. This implies that ϕ has no branch points, and that the extensions K_n/F are Galois. It also implies that $A[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^d$ for all $n \geq 1$.

The map ω has a natural decomposition into two parts because A is an abelian algebraic group, and we now give some notation and terminology that we use throughout the sequel. Let $T_\ell(A) := \varprojlim A[\ell^n]$ be the Tate module of A. Note that in the notation of Section 2, $T_\ell(A)$ is the same as $T_\phi(O)$, where $O \in A$ is the identity. We make one change in notation: since $T_\ell(A)$ has a group structure, we use $\mathrm{Aut}(T_\ell(A))$ to denote the set of group automorphisms; before we used $\mathrm{Aut}(T_\phi(\alpha))$ to denote the set of tree automorphisms.

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

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

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

For the remainder of the paper, we will use the following notation.

Notation	Meaning
F	Base field
T_n	$F(A[\ell^n])$
F_n	$F(\beta_n)$
K_n	$T_n F_n$
T_∞	$\bigcup_{n=1}^{\infty} T_n$
K_∞	$\bigcup_{n=1}^{\infty} K_n$
$\mathcal{T}_n$	$\mathrm{Gal}\,(T_n/F)$, the torsion part
$\mathcal{K}_n$	$\mathrm{Gal}\,(K_n/T_n)$, the Kummer part
$\mathcal{G}_n$	$\mathrm{Gal}\,(K_n/F)$
ρ	$\mathrm{Gal}\,(T_\infty/F) \to \mathrm{Aut}(T_\ell(A))$, the torsion representation
$\mathcal{T}$	$\varprojlim \mathcal{T}_n$, the image of ρ
κ	$\mathrm{Gal}\,(K_\infty/T_\infty) \to T_\ell(A)$, the Kummer map
ω	$\mathrm{Gal}\,(K_\infty/F) \to T_\ell(A) \rtimes \mathrm{Aut}(T_\ell(A))$, the arboreal representation

The next proposition says that these two parts give us full information about the image of κ. It is closely related to [**27**, p. 5].

Proposition 3.1. *Assume the notation above. For $n \geq 1$, ω_n is an injective homomorphism.*

Proof. For $\sigma, \tau \in \mathrm{Gal}\,(K_n/F)$, 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, $\sigma|_{A[\ell^n]}$ is the identity. Thus, if $\beta \in U_n$ we have $\ell^n\beta = \alpha$ and so

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

Thus, $\beta - \beta_n \in A[\ell^n]$. 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:

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

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 $T_\ell(A) \rtimes \mathrm{Aut}(T_\ell(A))$, rather than into the full automorphism group of the tree $T_\ell(\alpha)$.

THEOREM 3.2. *Let $G = \mathrm{Gal}\,(K_\infty/F)$, and let $\mathcal{F}(G)$ be as defined on p. 4. Let A be the product of an abelian variety by a torus, $\phi = [\ell]$, and assume the orbit of $\alpha \in A(F)$ under $[\ell]$ is Zariski dense in A. Then the set*

$$\{\mathfrak{p} \subset \mathcal{O}_F : \textit{the order of } \overline{\alpha} \in A(f_\mathfrak{p}) \textit{ is not divisible by } \ell\}$$

has a Dirichlet density, and it is given by $\mathcal{F}(G)$.

REMARK (As pointed out to the authors by A. Perucca). If the orbit of α is not dense in A, the result still holds in many circumstances. In particular, if A_α is the smallest F-algebraic subgroup of A containing α, and the number of connected components of A_α is prime to ℓ, the result holds. One achieves this by replacing α with a multiple of itself to get that A_α is connected, then applying [**26**, Proposition 2.5] and proceeding with the proof below. In the case where the number of connected components of A_α is divisible by ℓ, it follows from [**26**, Main Theorem 1] that the set in Theorem 3.2 contains only finitely many primes.

Proof. We begin by noting that the hypothesis that the orbit of α is dense in A permits us to apply a theorem of Bertrand ([**2**, Theorem 2, p. 40]) showing that $\mathrm{im}\,\kappa$ has finite index in $T_\ell(A)$.

Let $\mathrm{Per}(\ell, \alpha) = \{\mathfrak{p} \subset \mathcal{O}_F : [\ell^n](\overline{\alpha}) = \overline{\alpha} \text{ for some } n \geq 1\}$. Denote the order of $\overline{\alpha} \in A(f_\mathfrak{p})$ by m. We show that $\ell \nmid m$ 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 $\overline{\alpha}$.

Next, let $\mathrm{Frob}_{\mathfrak{p}}$ denote the Frobenius conjugacy class at $\mathfrak{p}$ in $\mathrm{Gal}\,(F^{\mathrm{sep}}/F)$, and let $t_{\mathfrak{p},n}$ denote its image in $\mathcal{T}_n$. Define

$$NP_n := \{\mathfrak{p} \subset \mathcal{O} : \mathrm{Frob}_{\mathfrak{p}} \text{ has no fixed points in } U_n\}$$
$$P_n := \{\mathfrak{p} \subset \mathcal{O} : \mathrm{Frob}_{\mathfrak{p}} \text{ has a fixed point in } U_n \text{ and } \det(t_{\mathfrak{p},n} - \mathrm{id}) \neq 0\}.$$

By the Chebotarev density theorem, $D(P_n)$ and $D(NP_n)$ exist for all $n \geq 1$. We note that the extension K_∞/F is ramified over only finitely many primes, whence for all but finitely many $\mathfrak{p}$ there is a well-defined action of $\mathrm{Frob}_{\mathfrak{p}}$ on U_m for all $m \geq n$ (this will be used in the next paragraph). To prove finite ramification, it is enough to show that except for finitely many primes, the elements of U_n remain distinct under reduction modulo $\mathfrak{p}$. This follows from the fact that reduction modulo $\mathfrak{p}$ is injective on $A[\ell^n]$ for all n, except for finitely many $\mathfrak{p}$, a statement that holds for any connected abelian algebraic group (see [**20**, Lemma 4.4]).

Next, it follows from the proof of Proposition 2.1 that the complement of $\mathrm{Per}(\ell, \alpha)$ contains $\bigcup_{n\geq 1} NP_n$. We claim that $\bigcup_{n\geq 1} P_n \subseteq \mathrm{Per}(\ell, \alpha)$. Identify U_n with $A[\ell^n]$ via the map $\beta_n + \gamma \mapsto \gamma$, and note that under this identification $\mathrm{Frob}_{\mathfrak{p}}$ acts on U_n as $t_{\mathfrak{p},n} + \mathbf{v}$, where $t_{\mathfrak{p},n} \in \mathrm{GL}_m(\mathbb{Z}/\ell^n\mathbb{Z})$ and $\mathbf{v} = \sigma(\beta_n) - \beta_n \in A[\ell^n]$ (see Proposition 3.1). If $\mathfrak{p} \in P_n$ for some n, then this action has a fixed point, so $\mathbf{v} \in \mathrm{im}\,(t_{\mathfrak{p},n} - \mathrm{id})$. Since $\mathrm{ord}_\ell(\det(t_{\mathfrak{p},n} - \mathrm{id})) < n$, the $\mathbb{Z}/\ell^n\mathbb{Z}$-submodule $\mathrm{im}\,(t_{\mathfrak{p},n} - \mathrm{id})$ has index $\ell^{\mathrm{ord}_\ell(\det(t_{\mathfrak{p},n}))}$ in $A[\ell^n]$, and the same statement holds if n is replaced by any larger integer. Hence every lift of $\mathbf{v}$ to $A[\ell^m]$ for $m > n$ must be in $\mathrm{im}\,(t_{\mathfrak{p},m} - \mathrm{id})$, and it follows that Frob_p acts on U_k with a fixed point for all $k \geq 1$. By the first paragraph of the proof of Proposition 2.1, this implies $\mathfrak{p} \in \mathrm{Per}(\ell, \alpha)$.

Finally, for fixed n, the set of $\mathfrak{p}$ not belonging to P_n or NP_n is

$$E_n := \{\mathfrak{p} \in \mathcal{O} : \mathrm{Frob}_{\mathfrak{p}} \text{ has a fixed point in } U_n \text{ and } \det(t_{\mathfrak{p},n} - \mathrm{id}) = 0 \bmod \ell^n\}.$$

By the Chebotarev Density theorem, $D(E_n)$ is given by

$$\frac{1}{\#\mathcal{G}_n} \cdot \#\{g \in \mathcal{G}_n : g \text{ has a fixed point in } U_n \text{ and } \det(g|_{T_n} - \mathrm{id}) = 0 \bmod \ell^n\}.$$

If $\det(g|_{T_n} - \mathrm{id}) = 0 \bmod \ell^n$, then the index of $\mathrm{im}\,(g|_{T_n} - \mathrm{id})$ in $A[\ell^n]$ is at least ℓ^n. Hence

$$\#\{h \in \mathcal{G}_n : h|_{T_n} = g|_{T_n} \text{ and } h \text{ has a fixed point in } U_n\} \leq \frac{1}{\ell^n} \cdot \#A[\ell^n].$$

By [**2**, Theorem 2, p. 40], the subgroup of $h \in G$ with $h|_{T_\infty} = g|_{T_\infty}$ has finite index m in $T_\ell(\alpha)$. For n sufficiently large, this implies that $\#\{h \in \mathcal{G}_n : h|_{T_n} = g|_{T_n}\} = (1/m) \cdot \#A[\ell^n]$. We now have shown the proportion of $h \in \mathcal{G}_n$ with $h|_{T_n} = g|_{T_n}$ and that fix a point in $A[\ell^n]$ is at most m/ℓ^n. It follows that $D(E_n) \leq m/\ell^n$.

This gives $\lim_{n\to\infty} (D(P_n) + D(NP_n)) = 1$. Let L_s denote the lim sup of the expression in (2.1) for $S = \mathrm{Per}(\ell, \alpha)$, and L_i denote the corresponding lim inf. Since $\bigcup_{n\geq 1} P_n \subseteq \mathrm{Per}(\ell, \alpha)$, we have $L_i \geq \lim_{n\to\infty} D(P_n)$. Since the complement of $\mathrm{Per}(\ell, \alpha)$ contains $\bigcup_{n\geq 1} NP_n$, we have $L_s \leq 1 - \lim_{n\to\infty} D(NP_n)$. Hence $L_s = L_i = 1 - \lim_{n\to\infty} D(NP_n)$. This last expression is the same as $\mathcal{F}(G)$. □

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 $\mathcal{T}$ will be important for determining the image of ω.

THEOREM 3.3. *If $G \leq \mathrm{GL}_d(\mathbb{Z}_\ell)$ is a profinite group, then $[G : \Phi(G)]$ is finite.*

Proof. Let $N \leq G$ be the kernel of the map $G \to \mathrm{GL}_d(\mathbb{Z}/\ell\mathbb{Z})$. Since $\Phi(N) \leq \Phi(G)$ and N has finite index in G, it suffices to show that $[N : \Phi(N)]$ is finite. For $n \geq 1$, let $N^{(n)}$ be the kernel of the map $N \to \mathrm{GL}_d(\mathbb{Z}/\ell^n\mathbb{Z})$ and define $\delta_n : N^{(n)}/N^{(n+1)} \to M_d(\mathbb{Z}/\ell\mathbb{Z})$ by $\delta_n(g) = \frac{g-1}{\ell^n}$. It is easy to see that δ_n is an injective homomorphism. This implies that N is a pro-ℓ group, and hence $\Phi(N) = N'N^\ell$. We will show that $[N : N^\ell]$ is finite.

If $g = I + \ell^n M$, then

$$g^\ell = \sum_{k=0}^{\ell} \binom{\ell}{k} \ell^{nk} M^k \equiv I + \ell^{n+1} M \pmod{\ell^{2n}}.$$

If $\ell > 2$, then the above congruence holds modulo ℓ^{2n+1}. It follows that for $n \geq 2$ or $n = 1$ and $\ell > 2$, we have $g^\ell \in N^{(n+1)}$ and $\delta_{n+1}(g^\ell) = \delta_n(g)$. It follows that we have the increasing sequence

$$\delta_n(N^{(n)}/N^{(n+1)}) \subseteq \delta_{n+1}(N^{(n+1)}/N^{(n+2)}) \subseteq \cdots$$

where all the groups are contained in $M_d(\mathbb{Z}/\ell\mathbb{Z})$. Hence, there is some m so that the ℓth power map $N^{(n)}/N^{(n+1)} \to N^{(n+1)}/N^{(n+2)}$ is surjective for $n \geq m$. This implies that if $g \in N^{(m+1)}$, then g can be written as a product of ℓth powers in every quotient $N^{(m+1)}/N^{(m+k)}$. The fact that the $N^{(n)}$ form a base for the open neighborhoods of the identity then imply that $\Phi(N) \supseteq N^\ell \supseteq N^{(m+1)}$, and so $\Phi(N)$ has finite index in N, as desired. □

Our next goal is to develop criteria that will ensure that $\operatorname{im}\omega_n \cong A[\ell^n] \rtimes \mathcal{T}_n$.

THEOREM 3.4. *Let the notation be as above. Suppose that for some $m \geq 1$ the following hold.*

(i) *$A[\ell^m]/A[\ell^{m-1}]$ is irreducible as a $\mathcal{T}_m$-module.*
(ii) *$\alpha \notin A(F) \cap \ell A(T_n)$ for all $n \geq m$.*

Then $\operatorname{im}\omega_n \cong A[\ell^n] \rtimes \mathcal{T}_n$ for all $n \geq m$.

Proof. Recall $\mathcal{K}_n = \mathrm{Gal}\,(T_n(\beta_n)/T_n) = \operatorname{im}\omega_n \cap A[\ell^n]$. If $(a, X) \in A[\ell^n] \rtimes \mathcal{T}_n$, and $(b, 1) \in \operatorname{im}\omega_n \cap A[\ell^n]$, one can compute that

$$(a, X)(b, 1)(a, X)^{-1} = (Xb, 1),$$

and hence $\mathcal{K}_n$ has the structure of a $\mathcal{T}_n$-module. It suffices to show that $\mathcal{K}_n = A[\ell^n]$ for $n \geq m$, since in this case, if (a, X) is an arbitrary element of $A[\ell^n] \rtimes \mathcal{T}_n$ then there is some $(b, X) \in \operatorname{im}\omega_n$ and $(a - b, 1) \in \mathcal{K}_n$ and we have

$$(a - b, 1)(b, X) = (a, X) \in \operatorname{im}\omega_n,$$

and the desired result holds.

To show that $\mathcal{K}_n = A[\ell^n]$, we prove two things. First, if $M \leq A[\ell^n]$ is any $\mathcal{T}_n$-submodule, then either $M = A[\ell^n]$ or $M \leq A[\ell^{n-1}]$. Finally, we'll prove that $\mathcal{K}_n \leq A[\ell^{n-1}]$ does not occur.

We prove the first of the two statements above by induction on n. For the base case $n = m$, we have $A[\ell^m]/A[\ell^{m-1}]$ is irreducible as a $\mathcal{T}_m$-module, and so the homomorphism $M \to A[\ell^m]/A[\ell^{m-1}]$ is either trivial or surjective. In the first case, $M \leq A[\ell^{m-1}]$ and in the second, M contains a complete set of representatives of $A[\ell^m]/A[\ell^{m-1}]$. The latter fact, together with the observation that $\ell M \leq M$ implies that $M = A[\ell^m]$.

Suppose now that $n > m$ and M is a $\mathcal{T}_n$-submodule of $A[\ell^n]$. Then, ℓM is a $\mathcal{T}_{n-1}$-submodule of $A[\ell^{n-1}]$. Induction now implies that $\ell M \leq A[\ell^{n-2}]$ or $\ell M = A[\ell^{n-1}]$. In the first case, $M \leq A[\ell^{n-1}]$, while in the second the following commutative diagram with exact rows, together with the five-lemma, implies that $M = A[\ell^n]$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A[\ell] & \longrightarrow & M & \xrightarrow{\ell} & A[\ell^{n-1}] & \longrightarrow & 0 \\ \| & & \| & & \downarrow & & \| & & \| \\ 0 & \longrightarrow & A[\ell] & \longrightarrow & A[\ell^n] & \xrightarrow{\ell} & A[\ell^{n-1}] & \longrightarrow & 0 \end{array}$$

Finally, we will prove that $\mathcal{K}_n = A[\ell^n]$. We have the following diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A[\ell^n] & \longrightarrow & A & \xrightarrow{\ell} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \ell^{n-1}} & & \downarrow{\scriptstyle \ell^{n-1}} & & \| & & \\ 0 & \longrightarrow & A[\ell] & \longrightarrow & A & \xrightarrow{\ell} & A & \longrightarrow & 0 \end{array}$$

This gives rise to the following diagram with exact rows:

$$\begin{array}{ccccc} 0 & \longrightarrow & A(T_n)/\ell^n A(T_n) & \xrightarrow{\delta_n} & H^1(T_n, A[\ell^n]) \\ & & \downarrow & & \downarrow{\scriptstyle \ell^{n-1}} \\ 0 & \longrightarrow & A(T_n)/\ell A(T_n) & \xrightarrow{\delta_1} & H^1(T_n, A[\ell]) \end{array}$$

Here $\delta_n(\alpha)$ is the element of $H^1(T_n, A[\ell^n])$ represented by the 1-cocycle $\sigma \mapsto \sigma(\beta_n) - \beta_n$. Since $\mathcal{K}_n = \mathrm{Gal}\,(T_n(\beta_n)/T_n)$, it follows that if $\mathcal{K}_n \leq A[\ell^{n-1}]$, then $\delta_n(\alpha)$ lies in the kernel of $\ell^{n-1} : H^1(T_n, A[\ell^n]) \to H^1(T_n, A[\ell])$. This implies that $\delta_1(\alpha) = 0$, which by the diagram above implies that $\alpha \in A(F) \cap \ell A(T_n)$. This contradicts the second assumption of the theorem.

Thus, $\mathcal{K}_n = A[\ell^n]$ and $\mathrm{im}\,\omega_n \cong A[\ell^n] \rtimes \mathcal{T}_n$. □

We will see that in most cases, the conditions of Theorem 3.4 are satisfied with $m = 1$. The next three lemmas will deal with establishing condition 2 of Theorem 3.4 under suitable hypotheses.

LEMMA 3.5. *Suppose that $A[\ell]$ is irreducible as a $\mathcal{T}_1$-module, $\alpha \notin \ell A(T_1)$ and $\alpha \in \ell A(T_n)$ for some $n \geq 2$. Then $F(\beta_1) \subseteq T_n$ and $\mathrm{Gal}\,(T_n/F(\beta_1))$ is a maximal subgroup of $\mathrm{Gal}\,(T_n/F)$.*

Proof. The assumption that $\alpha \notin \ell A(T_1)$ implies that $\beta_1 \notin A(T_1)$ and so $\mathrm{Gal}\,(K_1/T_1) = A[\ell]$ and $\mathcal{G}_1 = \mathrm{Gal}\,(K_1/F) \cong A[\ell] \rtimes \mathcal{T}_1$. If $\mathcal{T}_1 \leq N \leq \mathcal{G}_1$ is any subgroup, then $N \cap A[\ell]$ is a $\mathcal{T}_1$-submodule, and hence $N = \mathcal{T}_1$ or $N = \mathcal{G}_1$. Thus, $\mathcal{T}_1$ (whose fixed field is $F(\beta_1)$) is a maximal subgroup of $\mathcal{G}_1$, as desired. This implies that there are no fields that lie between F and $F(\beta_1)$ and hence $\mathrm{Gal}\,(T_n/F(\beta_1))$ is a maximal subgroup of $\mathrm{Gal}\,(T_n/F)$ for any n with $F(\beta_1) \subseteq T_n$. □

Let $N^{(n)} = \mathrm{Gal}\,(T_\infty/T_n)$. Via the embedding of $\mathcal{T}_{n+1} \to \mathrm{GL}_d(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$, we have that $N^{(n)}/N^{(n+1)} \cong \{M \in \mathcal{T}_{n+1} : M \equiv 1 \pmod{\ell^n}\}$. The group $\mathcal{T}_1$ acts by conjugation on $N^{(n)}/N^{(n+1)}$ and hence $N^{(n)}/N^{(n+1)}$ has the structure of a $\mathcal{T}_1$-module.

LEMMA 3.6. *If $n \geq 1$ and $\mathrm{Hom}_{\mathcal{T}_1}(N^{(n)}/N^{(n+1)}, A[\ell]) = 0$, then $A(F) \cap \ell A(T_n) = A(F) \cap \ell A(T_{n+1})$.*

Proof. Suppose that $\alpha \in A(F) \cap \ell A(T_{n+1})$. This means that $\beta_1 \in A(T_{n+1})$, and $\delta_1(\alpha)(\sigma) = \sigma(\beta_1) - \beta_1$ gives rise to a cohomology class in $H^1(T_{n+1}/F, A[\ell])$. A refined form of the inflation-restriction sequence gives an exact sequence

$$0 \longrightarrow H^1(T_n/F, A[\ell]) \xrightarrow{\inf} H^1(T_{n+1}/F, A[\ell]) \xrightarrow{\mathrm{res}} H^1(T_{n+1}/T_n, A[\ell])^{\mathcal{T}_n}.$$

Now, $\mathrm{Gal}\,(T_{n+1}/T_n)$ acts trivially on $A[\ell]$ and so

$$H^1(T_{n+1}/T_n, A[\ell])^{\mathcal{T}_n} = \mathrm{Hom}_{\mathcal{T}_n}(N^{(n)}/N^{(n+1)}, A[\ell]) = \mathrm{Hom}_{\mathcal{T}_1}(N^{(n)}/N^{(n+1)}, A[\ell]) = 0.$$

Thus, the inflation map is a bijection between $H^1(T_{n+1}/F, A[\ell])$ and $H^1(T_n/F, A[\ell])$. This implies that the cocycle $\delta_1(\alpha)(\sigma)$ is trivial for $\sigma \in \mathrm{Gal}\,(T_{n+1}/T_n)$ and this implies that $\beta_1 \in A(T_n)$, as desired. □

LEMMA 3.7. *Suppose that there is a normal subgroup H of $\mathcal{T}_1$ with order coprime to ℓ and $A[\ell]^H = 0$. Then, $A(F) \cap \ell A(T_1) = \ell A(F)$.*

Proof. Suppose that $\alpha \in A(F)$ and $\beta_1 \in A(T_1)$. This gives rise to a cocycle $\delta_1(\alpha)(\sigma) = \sigma(\beta_1) - \beta_1$ that represents a cohomology class in $H^1(F, A[\ell])$. We have the inflation-restriction sequence

$$0 \longrightarrow H^1(\mathcal{T}_1/H, A[\ell]^H) \longrightarrow H^1(\mathcal{T}_1, A[\ell]) \longrightarrow H^1(H, A[\ell]).$$

Because $A[\ell]^H = 0$, the first term is zero, and because $A[\ell]$ has order a power of ℓ, which is coprime to $|H|$, the last term is also zero. Thus, $H^1(\mathcal{T}_1, A[\ell]) = 0$ by exactness.

We have another inflation-restriction sequence

$$0 \longrightarrow H^1(\mathcal{T}_1, A[\ell]) \longrightarrow H^1(F, A[\ell]) \xrightarrow{\text{res}} H^1(T_1, A[\ell])$$

and since $H^1(\mathcal{T}_1, A[\ell]) = 0$, it follows that the restriction map is injective. Since the restriction of δ_1 to $H^1(T_1, A[\ell])$ is zero, it follows that δ_1 is a coboundary and so $\beta_1 \in F$. □

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

THEOREM 3.8. *Suppose that κ is surjective. Then*

$$\mathcal{F}(G) = \int_{\mathcal{T}} \ell^{-\mathrm{ord}_\ell(\det(M-I))}\, d\mu. \tag{3.1}$$

Here, $d\mu$ denotes the Haar measure on $\mathcal{T}$, normalized so that $\mu(\mathcal{T}) = 1$, and we take $\mathrm{ord}_\ell(0) = \infty$.

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 by our convention that $\mathrm{ord}_\ell(0) = \infty$ we have $\ell^{-\mathrm{ord}_\ell(\det(M-I))} = 0$.

Suppose that $\sigma \in \mathcal{G}_n$ 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 $M \in \mathcal{T}_n$ with $\det(M - I) \not\equiv 0 \pmod{\ell^n}$ and $\tilde{M}$ is any lift of M to $\mathcal{T}$, 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 elements of $\mathcal{G}_n$ fixing some

point of U_n divided by the size of $\mathcal{G}_n = \mathrm{Gal}\,(K_n/F)$ is

$$\frac{\sum_{M\in\mathcal{T}_n} \#\mathrm{im}\,(M-I)}{\#\mathcal{T}_n\cdot\ell^{dn}} = \frac{\sum' \ell^{dn-\mathrm{ord}_\ell(\det(M-I))}}{\#\mathcal{T}_n\cdot\ell^{dn}} + \frac{\sum'' \#\mathrm{im}\,(M-I)}{\#\mathcal{T}_n\cdot\ell^{dn}},$$

where $\sum'$ and $\sum''$ are taken over all $M\in\mathcal{T}_n$ 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

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

As $n\to\infty$, this integral tends to

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

and the second term tends to zero. This establishes (3.1). □

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 F^{sep}. If F is a number field, then there is a bijection between algebraic tori of dimension n up to F-isomorphism and

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

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

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

for some $d\in F^\times/(F^\times)^2$, 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 ℓ-adic representation ρ.

PROPOSITION 4.1. *Let ℓ be a prime. The ℓ-adic representation $\rho:\mathcal{T}_\infty\to\mathbb{Z}_\ell^\times$ is surjective if and only if the following conditions are satisfied:*

(i) *We have $|F(\zeta_{\ell^3}+\zeta_{\ell^3}^{-1}):F| = \frac{\ell^2(\ell-1)}{2}$.*
(ii) *If $\ell\equiv 3 \pmod 4$, then $-\ell d$ is not a square in F.*
(iii) *If $\ell = 2$, then $-d$ and $-2d$ are not squares in F.*

Proof. Note that the coordinates of the ℓ^n torsion points on A are given by

$$\left(\frac{\zeta_{\ell^n}+\zeta_{\ell^n}^{-1}}{2}, \frac{\zeta_{\ell^n}-\zeta_{\ell^n}^{-1}}{2\sqrt{d}}\right).$$

Assume first that $\ell>2$. Since the square of $\frac{\zeta_{\ell^2}-\zeta_{\ell^2}^{-1}}{2\sqrt{d}}$ is in $F(\zeta_{\ell^2}+\zeta_{\ell^2}^{-1})$, and

$$|F(A[\ell^2]):F| = |F(A[\ell^2]):F(\zeta_{\ell^2}+\zeta_{\ell^2}^{-1})|\,|F(\zeta_{\ell^2}+\zeta_{\ell^2}^{-1}):F|,$$

condition (1) above is necessary. The maximal subgroups of $\mathbb{Z}_\ell^\times$ are those that contain the kernel of reduction mod ℓ, together with the unique subgroup of index ℓ in $\mathbb{Z}_\ell^\times$. The first condition above rules out the possibility of the image of ρ landing in this second subgroup, and so it suffices to determine when the mod ℓ Galois representation is surjective. Let $L = F(\zeta_\ell, \sqrt{d})$

and define $\phi : \mathrm{Gal}\,(L/F) \to \mathbb{F}_\ell^\times \times \mathbb{Z}/2\mathbb{Z}$ by $\phi(\sigma) = (\sigma|_{\mu_\ell}, \sigma(\sqrt{d})/\sqrt{d})$. If ϕ is surjective, then there is an element $\sigma \in \mathrm{Gal}\,(L/F)$ so that $\sigma(\zeta_\ell) = \zeta_\ell^{-1}$ and $\sigma(\sqrt{d}) = \sqrt{d}$. This element σ fixes $\zeta_\ell + \zeta_\ell^{-1}$, but it sends $\frac{\zeta_\ell - \zeta_\ell^{-1}}{2\sqrt{d}}$ to its negative. Thus, $\frac{\zeta_\ell - \zeta_\ell^{-1}}{2\sqrt{d}} \notin F(\zeta_\ell + \zeta_\ell^{-1})$ and so $|F(A[\ell]) : F(\zeta_\ell + \zeta_\ell^{-1})| = 2$ and we have that $|F(A[\ell]) : F| = \ell - 1$ and so ρ is surjective.

Suppose therefore that ϕ is not surjective. Condition (1) implies that $|F(\zeta_\ell + \zeta_\ell^{-1}) : F| = \frac{\ell-1}{2}$ and so the image of ϕ has index at most 2. There are three subgroups of $\mathbb{F}_\ell^\times \times (\mathbb{Z}/2\mathbb{Z})$ of index 2, and they are $\{(a, 1) : a \in \mathbb{F}_\ell^\times\}$, $\{(a^2, \pm 1) : a \in \mathbb{F}_\ell^\times\}$ and $\{(a, \left(\frac{a}{\ell}\right)) : a \in \mathbb{F}_\ell^\times\}$.

In the first case, $\sqrt{d}$ is fixed by $\mathrm{Gal}\,(L/F)$ and so $\sqrt{d} \in K$. In this case, $F(A[\ell]) = F(\zeta_\ell)$, and since $|F(\zeta_\ell) : F| = \ell - 1$, ρ is surjective.

In the second case, $|F(\zeta_\ell) : F| = (\ell - 1)/2$. Here we have $F(A[\ell]) = F(\zeta_\ell, \sqrt{d})$ and this has degree $\ell - 1$ over F and so ρ is surjective.

In the third case, $\sqrt{d} \in F(\zeta_\ell)$ and $|F(\zeta_\ell) : F| = \ell - 1$. If $\sqrt{d} \in F(\zeta_\ell + \zeta_\ell^{-1})$, then $F(A[\ell]) = F(\zeta_\ell)$ and ρ is surjective. If not, then $\ell \equiv 3 \pmod 4$, $-\ell d = \alpha^2$ for some $\alpha \in F$, and we have that

$$\frac{\zeta_\ell - \zeta_\ell^{-1}}{2\sqrt{d}} = \frac{\zeta_\ell - \zeta_\ell^{-1}}{2\alpha\sqrt{-1/\ell}}$$

lies in $F(\zeta_\ell + \zeta_\ell^{-1})$. In this case, $|F(A[\ell]) : F| = \frac{\ell-1}{2}$ and ρ is not surjective.

For $\ell = 2$, one computes that $F(A[8]) = F(\sqrt{2}, \sqrt{-d})$. It follows then that ρ is surjective if and only if $|F(A[8]) : F| = 4$. This occurs if and only if 2, $-d$ and $-2d$ are not squares in F. Since $F(\zeta_8 + \zeta_8^{-1}) = F(\sqrt{2})$, condition (1) guarantees that 2 is not a square in F. □

Next, we have the following surjectivity criteria for the Kummer map κ.

THEOREM 4.2. *Let $A : x^2 - dy^2 = 1$ be a one-dimensional torus over F and let $\alpha \in A(F)$. Assume that the ℓ-adic representation on A is surjective. The Kummer map $\kappa : \mathrm{Gal}\,(\overline{F}/T_\infty) \to \mathbb{Z}_\ell$ is surjective if and only if the following conditions are satisfied:*

(i) $\alpha \notin \ell A(F)$.
(ii) *If $\ell = 2$, assume that $F(\beta_1) \not\subseteq F(A[8])$.*

Proof. The necessity is clear since either of the above two conditions will force the image of κ to have index a multiple of ℓ.

First assume $\ell > 2$. The hypotheses of Lemma 3.7 are satisfied with $H = \mathcal{T}_1 \cong (\mathbb{Z}/\ell\mathbb{Z})^\times$. Moreover, $N^{(n)}/N^{(n+1)}$ is one-dimensional with the trivial action, while $A[\ell]$ has the non-trivial action. Thus, the hypotheses of Lemma 3.6 are satisfied. Theorem 3.4 now implies that κ is surjective.

If $\ell = 2$ and $\beta_1 \in 2A(T_n)$ for some n, then Lemma 3.5 implies that $F(\beta_1) \subseteq F(A[8])$. This contradicts the hypothesis. Hence, $\beta_1 \notin 2A(T_n)$ for any n, and Theorem 3.4 implies that κ is surjective. □

As a consequence we obtain conditions for the surjectivity of ω.

COROLLARY 4.3. *The arboreal representation $\omega : \mathrm{Gal}\,(K_\infty/F) \to \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ is surjective if and only if the conditions of Theorem 4.2 and Proposition 4.1 are satisfied.*

Proof. It is clear that ω is surjective if and only if κ and ρ are surjective. □

EXAMPLE 4.4. Suppose that $F = \mathbb{Q}$ and $d = 1$. In this case, $x^2 - y^2 = 1$ is isomorphic to $\mathbb{G}_m$ over $\mathbb{Q}$. If $\ell > 2$ and $\alpha = (x_0, y_0) \notin \ell A(\mathbb{Q})$, then Theorem 4.2 and the above remark demonstrate that $G = \mathrm{Gal}\,(K_n/F) \cong \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$. Moreover, one verifies directly that the same conclusion holds for $\ell = 2$ as long as the corresponding point $(\gamma, 1/\gamma) = \left(\frac{x_0+y_0}{2}, \frac{x_0-y_0}{2}\right)$ on $x'y' = 1$ satisfies condition (2) of Theorem 4.2. In this case, $\mathbb{Q}(A[8]) = \mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(\beta_1) = \mathbb{Q}(\sqrt{\gamma})$. Since the quadratic subfields of $\mathbb{Q}(\zeta_8)$ are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, and $\mathbb{Q}(\sqrt{-2})$, this is equivalent to none of $\pm\gamma$ or $\pm 2\gamma$ being squares in $\mathbb{Q}$.

PROPOSITION 4.5. *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. We will apply Theorem 3.8. Representing elements of $\mathbb{Z}_\ell^\times$ with their ℓ-adic expansions, we obtain

$$\mu(\{x \in \mathbb{Z}_\ell^\times : v_\ell(x-1) = n\}) = \begin{cases} (\ell-2)/(\ell-1) & \text{if } n = 0 \\ 1/\ell^n & \text{if } n \geq 1. \end{cases} \tag{4.1}$$

The integral in (3.1) 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 4.4, we see that in the case $A = \mathbb{G}_m$, $F = \mathbb{Q}$, 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 plus or minus 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 [**10**], [**11**]; see [**25**] 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 $p \mid 2^n + 1$ for some n 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 [**22**] about primes dividing the nth Lucas number L_n follows from our results above since it is easy to see that p divides some L_n if and only if the point $(3/2, 1/2)$ on $A : x^2 - 5y^2 = 1$ has even order in $A(\mathbb{F}_p)$. Finally, [**9**], contains a study of primes that divide sequences of the shape $a_1 = t^2 - t - 2$, $a_n = (a_{n-1} + t)^2 - (2 + t)$. The nth term a_n comes from $\alpha = (t, u)$ on $A : x^2 - dy^2 = 4$, where d and u are chosen so that d is squarefree and $t^2 - 4 = du^2$. In particular,

$$a_n = x([2^n](t, u)) - t.$$

A prime p divides a_n 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 4.6. Suppose that $F = \mathbb{Q}$, $d = -7$, $\ell = 7$ 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 $[F_n : F] = 3 \cdot 7^{2n-1}$. 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 4.5 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 F. We will content ourselves with considering two examples.

EXAMPLE 4.7. Suppose that $F = \mathbb{Q}$, $A \cong \mathbb{G}_m \times \mathbb{G}_m$ 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, $F_n = \mathbb{Q}(\zeta_{\ell^n}, p^{1/\ell^n}, q^{1/\ell^n})$ and $\mathcal{G}_n \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes (\mathbb{Z}/\ell^n\mathbb{Z})^\times$, so that ω is surjective. One can compute that $\mathcal{F}(G) = \frac{\ell^3-\ell^2-\ell-1}{\ell^3-1}$.

EXAMPLE 4.8. Let $F = \mathbb{Q}$, 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 $F_n = \mathbb{Q}(\zeta_3, \zeta_{2^n}, (\sqrt[3]{2} - 1)^{1/2^n}, (\zeta_3\sqrt[3]{2} - 1)^{1/2^n})$. Then,

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

5. *Elliptic Curves*

5.1. *Elliptic curves without complex multiplication*

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

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

We treat the torsion part first by giving criteria for $\rho : \mathcal{T} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ to be surjective. This problem has been well-studied. In particular, in [**32**] it is shown that ρ is surjective provided ℓ is large enough.

Recall that the n-torsion polynomial of an elliptic curve $E : y^2 = x^3 + Ax + B$ is the polynomial whose roots are the x-coordinates of the points of order n in $E(\overline{F})$.

PROPOSITION 5.1. *Let ℓ be a prime. The ℓ-adic representation $\rho : \mathrm{Gal}\,(T_\infty/F) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective if and only if the following conditions hold:*

(i) *The base field F is linearly disjoint from $\mathbb{Q}(\zeta_{\ell^n})$ for all n.*
(ii) *$\mathcal{T}_1 \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*
(iii) *If $\ell = 2$ and D is the discriminant of the 2-torsion polynomial, then $-D$, $2D$ and $-2D$ are not squares in F, and the 4-torsion polynomial is irreducible and its Galois group has order 48 over F.*
(iv) *If $\ell = 3$, then the 9-torsion polynomial is irreducible over $F(\zeta_9)$.*

Proof. Serre [**33**] [IV, 3.4, Lemma 3] shows that if $\ell \geq 5$, then no proper closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ surjects onto $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. From the formula

$$\det \rho(\mathrm{Frob}_p) = \chi_\ell(p),$$

where χ_ℓ is the ℓ-adic cyclotomic character, we see that $\rho|_{\mathrm{Gal}\,(F_{\zeta_{\ell^\infty}}/F)}$ surjects onto $\mathrm{SL}_2(\mathbb{Z}_\ell)$ if and only if the map $\rho|_{F(\zeta_\ell)}$ surjects onto $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. The linear disjointness of F with $\mathbb{Q}(\zeta_{\ell^n})$ implies that $\det \rho : \mathrm{Gal}\,(T_\infty/F) \to \mathbb{Z}_\ell^\times$ is surjective. This demonstrates that conditions (1) and (2) are necessary for any ℓ and sufficient for $\ell \geq 5$.

For $\ell = 3$, the proof of Theorem 3.3 shows that $\Phi(\mathrm{GL}_2(\mathbb{Z}_3)) \supseteq N^{(2)}$, where $N^{(k)} = \ker(\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z}))$. A computation then shows that there are five maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ with indices 2, 3, 3, 4, and 27, respectively. The maximal subgroups

of index 2, 4, and one of those with index 3 correspond to the maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \cong S_4$. The other maximal subgroup of index 3 is

$$\{M \in \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) : \det(M) \equiv \pm 1 \pmod 9\}.$$

To ensure the image of ρ does not lie in the maximal subgroup of index 3 described above, it is necessary and sufficient to assume that F is linearly disjoint from $\mathbb{Q}(\zeta_9)$. The maximal subgroup of index 27 is generated by

$$\begin{bmatrix} 0 & 7 \\ 5 & 8 \end{bmatrix}, \begin{bmatrix} 2 & 5 \\ 5 & 6 \end{bmatrix}.$$

Its intersection with $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ has order 24. The 9-torsion polynomial is irreducible over $F(\zeta_9)$ if and only if $(\operatorname{im}\rho_2) \cap \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ acts transitively on the x-coordinates of the 9-torsion points. If the image of ρ lies in the maximal subgroup of index 27, then it cannot act transitively on the 36 x-coordinates, since the order of the group is only 24. On the other hand, if ρ_2 is surjective, then since $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ acts transitively on elements of order 9 in $(\mathbb{Z}/9\mathbb{Z})^2$, it follows that $\mathrm{Gal}\,(F(A[9])/F)$ acts transitively on the elements of order 9 in $A[9]$, and hence on roots of the 9-torsion polynomial. Thus, a necessary and sufficient condition for ρ to be surjective is that the 9-torsion polynomial is irreducible over $F(\zeta_9)$.

For $\ell = 2$, the proof of Theorem 3.3 shows that $\Phi(GL_2(\mathbb{Z}_2)) \supseteq N^{(3)}$. A computation then shows that there are 9 maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$. Seven of these have index 2, one has index 3, and one has index 4.

To guarantee that the image of ρ does not lie in one of the subgroups of index 2, it is necessary and sufficient that $F(\sqrt{2})$, $F(i)$, and the quadratic subfield of $F(A[2])$ are three independent quadratic extensions of F. This is guaranteed by the condition (1) and the first part of condition (3), since $F(\zeta_8) \subseteq F(A[8])$. To guarantee that the image of ρ does not lie in one of the subgroups of index 3, it is necessary and sufficient that $3|[F(A[2]) : F]$, which is guaranteed by condition (2).

The maximal subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ of index 4 is generated by

$$\begin{bmatrix} 0 & 3 \\ 3 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 3 \\ 0 & 1 \end{bmatrix}.$$

Note that if A is written in the form $A : y^2 = x^3 + ax + b$ then the action of $[-1]$ on (x, y) is $(x, y) \mapsto (x, -y)$. Hence, the Galois extension obtained by adjoining the x-coordinates is the image of ρ_2 in $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})/\langle \pm I \rangle$. In the case that ρ_2 is surjective, it has order 48, while in the case where the image of ρ_2 is contained in the maximal subgroup of index 4 (and all the other conditions of the theorem are met) it has order 12. □

Remark. There are modular curves of genus zero that parametrize the elliptic curves $E/\mathbb{Q}$ for which the mod ℓ representations are surjective, but the mod ℓ^2 representations are not. In [**7**], Elkies computes this parametrization for $\ell = 3$ and gives the first examples of curves $E/\mathbb{Q}$ for which the mod 3 representation is surjective but the mod 9 representation is not. The CM elliptic curve $y^2 + y = x^3$ is the smallest conductor curve for which the mod 2 representation is surjective, but the mod 4 representation is not.

Theorem 5.2. *Suppose that the ℓ-adic representation $\rho : \mathrm{Gal}\,(T_\infty/F) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective. Then the Kummer map $\kappa : \mathrm{Gal}\,(K_\infty/T_\infty) \to \mathbb{Z}_\ell^2$ is surjective if and only if the following conditions hold:*

(i) *The point $\alpha \notin \ell A(F)$.*
(ii) *If $\ell = 2$, $F(\beta_1) \not\subseteq F(A[4])$.*

Proof. It is clear that if either of the stated conditions fails to hold, then κ fails to be surjective.

Assume that $\ell > 2$ and $\alpha \notin \ell A(F)$. Then, $H = Z(\mathcal{T}_1) \cong (\mathbb{Z}/\ell\mathbb{Z})^\times$ is a normal subgroup of $\mathcal{T}_1$ with order coprime to ℓ and with $A[\ell]^H = 0$. Thus, Lemma 3.7 implies that $A(F) \cap \ell A(T_1) = \ell A(F)$. Next, $N^{(n)}/N^{(n+1)}$ is isomorphic to $M_2(\mathbb{F}_\ell)$ as a $\mathcal{T}_1$-module with the conjugation action. This decomposes as a direct sum of a three-dimensional and a one-dimensional $\mathcal{T}_1$-module, and hence $\mathrm{Hom}_{\mathcal{T}_1}(N^{(n)}/N^{(n+1)}, A[\ell]) = 0$. Thus, Lemma 3.6 implies that $A(F) \cap \ell A(T_n) = A(F) \cap \ell A(T_{n+1})$ for all $n \geq 1$. It follows that for any $n \geq 1$, $A(F) \cap \ell A(T_n) = \ell A(F)$. Finally, the surjectivity of ρ implies that $A[\ell]$ is irreducible as a $\mathcal{T}_1$-module. Thus, Theorem 3.4 implies that $\operatorname{im} \omega_n \cong A[\ell^n] \rtimes \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ for all $n \geq 1$.

When $\ell = 2$, again we have that $A[\ell]$ is irreducible as a $\mathcal{T}_1$-module. Thus, Lemma 3.5 implies that if $F(\beta_1) \subseteq T_n$, then $\mathrm{Gal}\,(T_n/F(\beta_1))$ is a maximal subgroup of $\mathcal{T}_n$. The condition that $F(\beta_1) \not\subseteq F(A[2])$ implies that $\mathrm{Gal}\,(K_1/F) \cong (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and that $|F(\beta_1) : F| = 4$. Since the only maximal subgroup of index 4 of $\mathrm{GL}_2(\mathbb{Z}_2)$ contains $N^{(2)} = \ker \rho_2$, it follows that if $F(\beta_1) \subseteq T_n$ for some n, then $F(\beta_1) \subseteq T_2$. This contradicts the hypotheses of the theorem. Thus, $F(\beta_1) \not\subseteq T_n$ for any n and Theorem 3.4 gives $\operatorname{im} \omega_n \cong A[\ell^n] \rtimes \mathcal{T}_n$ for all $n \geq 1$. □

REMARK. The condition that $F(\beta_1) \not\subseteq F(A[4])$ is necessary. In particular, if $A : y^2 + y = x^3 - 3x + 4$ and $\alpha = (4, 7)$, then ρ is surjective, but $F(\beta_1) \subseteq F(A[4])$.

COROLLARY 5.3. *The arboreal representation $\omega : \mathrm{Gal}\,(K_\infty/F) \to (\mathbb{Z}_\ell)^2 \rtimes \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective if and only if the conditions of Theorem 5.2 and Proposition 5.1 are satisfied.*

Proof. The necessity is clear. The sufficiency follows from the basic fact that if $N \lhd G$ and $M \subseteq G$ is a subgroup with $M \cap N = N$ and $M/N = G/N$, then $M = G$. □

EXAMPLE 5.4. Let $A : y^2 + y = x^3 - x$. Then A is an elliptic curve of conductor 37. In [**32**] (pg. 310, 5.5.6), it is shown that $\mathrm{Gal}\,(\mathbb{Q}(A[\ell])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all ℓ. It is also known that $\alpha = (0, 0)$ is a generator of $E(\mathbb{Q}) \cong \mathbb{Z}$. One can check that the 9-torsion polynomial is irreducible over $\mathbb{Q}(\zeta_9)$, and this implies that the ω representation is surjective for $\ell > 2$. For $\ell = 2$, one can check that the 4-torsion polynomial has Galois group of order 48, and that the discriminant of the two-torsion polynomial is 592. Further, Frobenius at 19 acts on K_1 with order 4, while it acts on $\mathbb{Q}(A[4])$ with order 2. It follows that $K_1 \not\subseteq \mathbb{Q}(A[4])$, and hence the ω representation is 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. $\mathrm{Gal}\,(K_\infty/F) \cong (\mathbb{Z}_\ell)^2 \rtimes \mathrm{GL}_2(\mathbb{Z}_\ell)$.

THEOREM 5.5. *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

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

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 eigenvalue 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 $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_\ell)$ 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 $\det(\tilde{M} - I) \not\equiv 0 \pmod{\ell^n}$. Write

$$\tilde{M} - I = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}.$$

The condition that $\det(\tilde{M} - I) \equiv 0 \pmod{\ell^{n-1}}$ but $\det(\tilde{M} - I) \not\equiv 0 \pmod{\ell^n}$ is equivalent to the existence of $i \in (\mathbb{Z}/\ell^n\mathbb{Z})$ and $\epsilon \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ so that

$$\begin{aligned} \alpha\delta &\equiv i + \epsilon\ell^{n-1} \pmod{\ell^n} \\ \beta\gamma &\equiv i \pmod{\ell^n}. \end{aligned}$$

Hence, the number of such M is

$$\sum_{\epsilon=1}^{\ell-1} \sum_{i=0}^{\ell^n-1} \#\{(\alpha,\delta) : \alpha\delta \equiv i + \epsilon\ell^{n-1} \pmod{\ell^n}, \alpha \equiv a-1 \pmod{\ell}, \delta \equiv d-1 \pmod{\ell}\}$$
$$\cdot \#\{(\beta,\gamma) : \beta\gamma \equiv i \pmod{\ell^n}, \beta \equiv b \pmod{\ell}, \gamma \equiv c \pmod{\ell}\}.$$

We use the following simple lemma to compute the quantities that appear in the above expression. We omit the proof of the lemma.

LEMMA 5.6. *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 5.6 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 5.6 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

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

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 F, and that A has complex multiplication. Then $\mathrm{End}_{\overline{F}}(A) \cong R$, where R is an order in an imaginary quadratic field L. Suppose first that $L \subseteq F$, and put $R_\ell = R \otimes \mathbb{Z}_\ell$. Let $\mathcal{T} = \mathrm{Gal}\,(T_\infty/F)$, so that the action of $\mathcal{T}$ on $A[\ell^\infty]$ gives the ℓ-adic Galois representation associated to A. Then $\mathcal{T}$ is known to be isomorphic to a subgroup of $R_\ell^\times$, provided that ℓ does not ramify in L or divide the index of R in the maximal order of L (see e.g. [**34**, p. 502]). We also have the analogue of Serre's open image theorem, namely that for any ℓ, $\mathcal{T}$ must have finite index in $R_\ell^\times$ and in fact $\mathcal{T} \cong R_\ell^\times$ for all but finitely many ℓ [**32**, 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 $L \not\subseteq F$, we have that $\mathcal{T}$ is a subgroup of the normalizer N of some Cartan subgroup C, which contains C as a subgroup of index two. Indeed, $[\mathcal{T} : \mathcal{T} \cap C] = [L : F \cap L] = 2$, and thus $\mathcal{T}$ is the normalizer of its image in C.

We begin by addressing the image of ρ.

PROPOSITION 5.7. *Let A be an elliptic curve defined over a number field F, and suppose that the image of $\rho : \mathcal{T} \to GL_2(\mathbb{Z}_\ell)$ is contained in the normalizer N of a Cartan subgroup but not in a Cartan subgroup. Denote by N_m the image of N in $GL_2(\mathbb{Z}/\ell^m\mathbb{Z})$. If $\ell \geq 3$, then ρ maps onto N if and only if $\mathcal{T}_2 \cong N_2$. For $\ell = 2$, the same conclusion holds if and only if $\mathcal{T}_3 \cong N_3$*

REMARK. Proposition 5.7 also holds in the case where the image of ρ is contained in a Cartan subgroup C, with analogous conditions ensuring that ρ maps onto C.

Proof. The only if direction is trivial. Let C be the Cartan subgroup of N, and suppose that $\mathcal{T}_2 \cong N_2$ ($\mathcal{T}_3 \cong N_3$ for $\ell = 2$). Denote by C_m the image of C in $GL_2(\mathbb{Z}/\ell^m\mathbb{Z})$, and recall $C \cong (R \otimes \mathbb{Z}_\ell)^\times$, where R is an order in an imaginary quadratic number field. Thus $\mathcal{T} \cap C$ surjects onto C_2 (C_3 if $\ell = 2$). We will show that this implies $\mathcal{T} \cap C$ surjects onto $C/\Phi(C)$, where $\Phi(C)$ is the Frattini subgroup of C. It follows that $\mathcal{T} \cap C = C$, and since $\mathcal{T}$ is not contained in C this shows $\mathcal{T} = N$.

To determine $\Phi(C)$, 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 [**30**, p. 257]. Since ℓS is the Frattini subgroup of S, it follows that the log of any maximal subgroup of $S^\times$ must contain ℓS, whence $\log \Phi(S^\times) \supseteq \ell S$. Under the log isomorphism, ℓS corresponds 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 $(S/\ell^2 S)^\times$ ($(S/\ell^3 S)^\times$ 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 result is proved by the previous paragraph. If ℓ splits in R, then $R_\ell^\times \cong \mathbb{Z}_\ell^\times \times \mathbb{Z}_\ell^\times$, and we have $\log \Phi(R_\ell^\times) \supseteq \ell\mathbb{Z} \times \ell\mathbb{Z}$. The proof then follows as in the previous paragraph. □

THEOREM 5.8. *Let A be an elliptic curve defined over a number field F, and suppose that the image of $\rho : \mathcal{T} \to GL_2(\mathbb{Z}_\ell)$ is the full normalizer N of a Cartan subgroup. Suppose further that we are not in the case where $\ell = 2$ and the underlying Cartan subgroup is split. Then the Kummer map $\kappa : \mathrm{Gal}\,(K_\infty/T_\infty) \to \mathbb{Z}_\ell^2$ is surjective if and only if $\alpha \notin \ell A(F)$.*

Proof. The only if direction is trivial. For the other direction, assume first that N is the normalizer of a Cartan subgroup C, excluding the case where C is split and $\ell = 2$. We apply Theorem 3.4 with $m = 1$. The first hypothesis of Theorem 3.4 is satisfied since a computation shows that $\mathcal{T}_1$ acts irreducibly on $A[\ell]$ (indeed, transitively when C is non-split).

To verify the second hypothesis of Theorem 3.4 with $m = 1$, we first apply Lemma 3.7 with $H = C_1$, the reduction modulo ℓ of C. This works since C_1 has order $\ell^2 - 1$ in the non-split case and $(\ell - 1)^2$ with $\ell > 2$ in the split case, and clearly $A[\ell]^{C_1} = 0$. We may also apply Lemma 3.6 for all $n \geq 1$, since the two-dimensional $\mathcal{T}_1$-module $N^{(n)}/N^{(n+1)}$ has a one-dimensional submodule (namely that generated by the multiplicative identity matrix), while the two-dimensional $\mathcal{T}_1$-module $A[\ell]$ is irreducible. Theorem 3.4 now applies to prove the theorem. □

REMARK. In the setup of Theorem 5.8, when $\ell = 2$ and the underlying Cartan subgroup is split, $\mathcal{T}_m$ does not act irreducibly on $A[\ell^m]/A[\ell^{m-1}]$ for any m, meaning we cannot apply Theorem 3.4. However, we can obtain the conclusion of Theorem 5.8 under the stronger assumption that $[T_3(\beta_1) : T_3] = 4$. Indeed, a computation of the Frattini subgroup of $\mathbb{Z}_2^2$ shows that if κ is not surjective then $[T_n(\beta_1) : T_n] \leq 2$ for some n. This implies that $T_1(\beta_1) \cap T_n$ contains a degree-two (and therefore minimal) subextension of T_∞/T_1. It follows from the proof of Proposition 5.7 that such an extension lies in T_3, and one deduces $[T_3(\beta_1) : T_3] \leq 2$.

The following corollary has the same proof as Corollary 5.3.

COROLLARY 5.9. *Let N be as in Theorem 5.8, and let $\ell \geq 3$. The arboreal representation $\omega : \mathrm{Gal}\,(K_\infty/K) \to (\mathbb{Z}_\ell)^2 \rtimes N$ is surjective if and only if the conditions of Theorem 5.8 and Proposition 5.7 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 5.10. *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. Let μ be the Haar measure, and suppose first that C is not-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 3.8, 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 (3.1). 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 $n \geq 1$, $t_n = 1/(\ell^2-1) \cdot 1/\ell^{2(n-1)} \cdot (\ell^2-1)/\ell^2 = 1/\ell^{2n}$. The integral in (3.1) 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 (4.1) 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 (3.1) 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 (3.1) 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 $\mathrm{im}\,\phi_2$ 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 (3.1) reduces to the same computation as in Theorem 4.5, which comes to $h(\ell)$. □

Example 5.11. Let $F = \mathbb{Q}$, $A : y^2 = x^3+3x$, $\alpha = (1,-2)$ and $\ell = 5$. The elliptic curve A has CM by the full ring of integers $\mathbb{Z}[i]$ in $L = \mathbb{Q}(i)$, 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 $\alpha \notin \ell A(\mathbb{Q})$. Next, we will show that $\mathrm{Gal}\,(\mathbb{Q}(A[25])/\mathbb{Q}) \cong N_2$, which has order 800. If λ is a prime ideal above 5, one can explicitly construct a point $P \in A[\lambda]$ that lies in a degree 4 extension of L. This shows that the natural homomorphism $\mathrm{Gal}\,(L(A[\lambda])/L) \to (\mathbb{Z}[i]/\lambda)^\times$ is an isomorphism, and therefore $\mathrm{Gal}\,(L(A[\lambda])/L)$ is cyclic of order 4. Moreover, the quadratic subfield of $L(A[\lambda])/L$ is ramified at λ.

Explicit class field theory (see Theorem 2.5.6 of [**35**]) shows that the extension obtained by adjoining the squares of the x-coordinates of $A[\lambda^2]$ to L has degree 5. Let M_1 be the compositum of the extension obtained by adjoining the squares of the x-coordinates of $A[\lambda^2]$ and all coordinates of the points in $A[\lambda]$. From above, we have $|M_1 : L| = 20$, and that every subextension of M_1 is ramified at λ. Let $\overline{\lambda}$ be the other prime above 5, and let M_2 be the extension obtained by adjoing all coordinates of points in $A[\overline{\lambda}]$, and the squares of the x-coordinates of points in $A[\overline{\lambda}^2]$. Similarly, $|M_2 : L| = 20$ and every subextension of M_2 is ramified at $\overline{\lambda}$.

Since $\mathbb{Z}[i]$ has class number one, L has no unramified abelian extensions and hence $M_1 \cap M_2 = L$ and $|M_1 M_2 : L| = 400$. Now, $M_1, M_2 \subseteq L(A[25])$, and the natural map $\mathrm{Gal}\,(L(A[25])/L) \to (\mathbb{Z}[i]/25\mathbb{Z}[i])^\times$ is injective. Since $|(\mathbb{Z}[i]/25\mathbb{Z}[i])^\times| = 400$, it follows that the above map is surjective, and $M_1 M_2 = L(A[25])$. Finally, since $\mathbb{Q}(A[25])$ is generalized dihedral over $\mathbb{Q}$, it contains L and hence $|\mathbb{Q}(A[25]) : \mathbb{Q}| = 800$, as desired.

Thus the hypotheses of Theorem 5.8 are satisfied, and we conclude by Theorem 5.10 and Theorem 3.2 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 5.12. 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 $\mathbb{Z}[\zeta_3]$. We will show that $\mathrm{Gal}\,(\mathbb{Q}(A[8])/\mathbb{Q}) \cong N_3$, which has order 96. It is easy to see that $\mathbb{Q}(A[2]) = \mathbb{Q}(\zeta_3, (-3)^{1/3})$. Thus, 3 divides $|\mathbb{Q}(A[8]) : \mathbb{Q}|$ and $L \subseteq \mathbb{Q}(A[8])$, where $L = \mathbb{Q}(\zeta_3)$. Explicit class field theory predicts that the extension M of L obtained by adjoining the cubes of the x-coordinates of points in $A[8]$ has degree 8. Further, this extension is only ramified at 2, and hence every subextension of M is ramified at 2 since L has no unramified abelian extensions.

In addition, the 4-torsion polynomial is $x^6 + 60x^3 - 72$. Therefore if α is the cube of the x-coordinate of a 4-torsion point, then $\alpha^2 + 60\alpha - 72 = 0$. Therefore, the y-coordinate β of a 4-torsion point satisfies $\beta^2 = \alpha + 3$ and so

$$(\beta^2 - 3)^2 + 60(\beta^2 - 3) - 72 = \beta^4 + 54\beta^2 - 243 = 0.$$

The discriminant of the polynomial $x^4 + 54x^2 - 243$ is $-2^{12} \cdot 3^{15}$, which is a a square in L. It follows that $L(\beta)/L$ is a Klein-4 extension, and is given by $L(\beta) = L(i, \sqrt{-1 + \zeta_3})$. The extension $L(\sqrt{-1 + \zeta_3})/L$ is ramified at the prime ideal above 3 in O_L and hence is not contained in M. It follows that 16 divides $[L(A[8]) : L]$ and hence 32 divides $[\mathbb{Q}(A[8]) : \mathbb{Q}] = 2[L(A[8]) : L]$. Thus, $[\mathbb{Q}(A[8]) : \mathbb{Q}] = 96$, as desired.

Since $\alpha \notin 2A(\mathbb{Q})$, ω is surjective. By Theorem 5.10 and Theorem 3.2 we conclude that $\overline{\alpha}$ has odd order for $(11/15 + 1/3)/2 = 8/15 \approx 0.533$ of primes p.

Example 5.13. 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 Theorem 5.7 are satisfied and thus the conclusion of Theorem 5.8 holds. By Theorem 5.10 and Theorem 3.2 we have that $\overline{\alpha}$ has odd order for $(1/9 + (1/3))/2 = 2/9 \approx 0.222$ of primes p.

Example 5.14. 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 $\rho:\mathrm{Gal}\,(T_\infty/F)\hookrightarrow \mathrm{GL}_{2d}(\mathbb{Z}_\ell)$.

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 $\mathcal{T}_n\subseteq \mathrm{GSp}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$, the group of symplectic similitudes. For more background about abelian varieties, see [**12**], section A.7.

We have the following surjectivity criteria for ρ.

PROPOSITION 6.1. *Let ℓ be a prime, $d\geq 2$ and assume that $\gcd(\ell,\#\ker(\Phi))=1$. Then, the ℓ-adic representation $\rho:\mathrm{Gal}\,(T_\infty/F)\to\mathrm{GSp}_{2d}(\mathbb{Z}_\ell)$ is surjective if and only if the following conditions hold:*

(i) *F is linearly disjoint from $\mathbb{Q}(\zeta_{\ell^n})$ for all n.*
(ii) $\mathrm{Gal}\,(T_1/F)\cong\mathrm{GSp}_{2d}(\mathbb{Z}/\ell\mathbb{Z})$.
(iii) *If $\ell=d=2$, then T_1 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 [**38**]. □

REMARK. Suppose that d is odd, $d=2$ or $d=6$, and $\mathrm{End}(A)\cong\mathbb{Z}$. Théorème 3 of [**31**, Résumé des cours de 1985-1986] implies that the conditions of the above proposition are satisfied for ℓ sufficiently large.

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

THEOREM 6.2. *Let ℓ be prime, $d\geq 2$ and assume that $\gcd(\ell,\#\ker(\Phi))=1$, and the ℓ-adic representation $\rho:\mathrm{Gal}\,(T_\infty/F)\to\mathrm{GSp}_{2d}(\mathbb{Z}_\ell)$ is surjective. Then the Kummer map $\kappa:\mathrm{Gal}\,(K_\infty/T_\infty)\to\mathbb{Z}_\ell^{2d}$ is surjective if and only if the following conditions hold:*

(i) *$\alpha\notin\ell A(F)$,*
(ii) *if $\ell=2$, $\beta_1\notin A(T_1)$.*

Proof. When $\ell>2$, the only modification necessary in the proof of Theorem 5.2 is in showing that $\mathrm{Hom}_{\mathcal{T}_1}(N^{(n)}/N^{(n+1)},A[\ell])=0$. To justify such a statement, one can use the computation of Liebeck and Seitz (see Proposition 1.10 of [**23**]) of the composition factors of this module over $\overline{\mathbb{F}}_\ell$, combined with the Restriction Theorem (see the theorem in Section 2.11 of Humphreys' book [**13**]) to conclude that these composition factors are still irreducible over

$\mathbb{F}_\ell$. We find that $N^{(n)}/N^{(n+1)}$ is a one-dimensional extension of an irreducible $\mathcal{T}_1$-module of dimension $2g^2+g$, so again $\mathrm{Hom}_{\mathcal{T}_1}(N^{(n)}/N^{(n+1)}, A[\ell]) = 0$.

When $\ell = 2$, we assume that $\beta_1 \notin A(T_1)$. We seek to apply Lemma 3.6. In this case, $V = N^{(n)}/N^{(n+1)}$ has a natural submodule of dimension $V_1 = 2g^2 - g$. In order to conclude that $\mathrm{Hom}_{\mathcal{T}_1}(N^{(n)}/N^{(n+1)}, A[2]) = 0$, one shows that any submodule M of V with $V/M \cong A[\ell]$ must contain V_1. This implies that V_1 has codimension one in M, and it can be checked that no such submodule M exists. Thus, the hypotheses of Lemma 3.6 are satisfied, and we can conclude that $\alpha \notin A(F) \cap \ell A(T_n)$ for any n. Then Theorem 3.4 implies that ω_n is surjective. □

Remark. When $\ell = 2$, $\mathrm{GSp}_{2d}(\mathbb{F}_2) = \mathrm{Sp}_{2d}(\mathbb{F}_2)$ is simple (provided $d \geq 3$) and so Lemma 3.7 does not apply. Indeed, suppose that $\alpha \in 2A(T_1)$, but $\alpha \notin 2A(F)$. This means that $\delta_1(\alpha)$ lies in the kernel of the restriction map $H^1(F, A[2]) \to H^1(T_1, A[2])$. However, the exactness of

$$0 \longrightarrow H^1(\mathrm{Gal}\,(T_1/K), A[2]) \longrightarrow H^1(F, A[2]) \longrightarrow H^1(T_1, A[2])$$

implies that the kernel is $H^1(\mathrm{Gal}\,(T_1/K), A[2])$, which is shown to be isomorphic to $\mathbb{Z}/2\mathbb{Z}$ by Pollatsek in [**28**]. It follows from the explicit construction of the non-trivial cocycles that $\alpha \in 2A(T_1)$ if and only if the preimages of α are a union of two Galois orbits of size $2^{2d-1} + 2^{d-1}$ and $2^{2d-1} - 2^{d-1}$, respectively, corresponding to the subgroups $\mathrm{SO}^+_{2d}(\mathbb{F}_2)$ and $\mathrm{SO}^-_{2d}(\mathbb{F}_2)$ stabilizing the two isomorphism classes of quadratic forms of dimension $2d$. It is interesting to ask whether there are abelian varieties $A/\mathbb{Q}$ and $\alpha \in A(\mathbb{Q}) - 2A(\mathbb{Q})$ for which this occurs.

Corollary 6.3. *The arboreal representation $\omega : \mathrm{Gal}\,(K_\infty/F) \to (\mathbb{Z}_\ell)^{2d} \rtimes \mathrm{GSp}_{2d}(\mathbb{Z}_\ell)$ is surjective if and only if the conditions of Theorem 6.2 and Proposition 6.1 are satisfied.*

Example 6.4. 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 6.5. *With A and α given above, we have*

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

for all primes ℓ.

Proof. It suffices to verify the conditions of Theorem 6.2 and Proposition 6.1. 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 6.2. 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 6.1 is obvious.

Next, we check condition (3) of Proposition 6.1. 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.

Next, we check condition (2) of Proposition 6.1. In [**6**], Dieulefait indicates how one can check that the mod ℓ Galois representations associated to an abelian surface A with $\mathrm{End}(A) \cong \mathbb{Z}$ are surjective at all but finitely many primes, conditional on Serre's conjecture. To show that $\mathrm{End}(A) \cong \mathbb{Z}$, one can compute that the two-torsion points of $A[2]$ are the Weierstrass points, and so $\mathbb{Q}(A[2])$ is the splitting field of $f(x)$. This has Galois group isomorphic to $S_6 \cong \mathrm{GSp}_4(\mathbb{F}_2)$. Hence, Proposition 6.1 implies that the 2-adic Galois representation is surjective. The injectivity of the map

$$\mathrm{End}(A) \otimes \mathbb{Z}_\ell \to \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A)) \cong \mathbb{Z}_\ell$$

implies that $\mathrm{End}(A)$ has rank 1 and so $\mathrm{End}(A) \cong \mathbb{Z}$. Using the algorithm of Liu ([**24**]), 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. 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 [**17**] and [**18**], and Kisin [**19**].

Finally, we check condition (2) of Theorem 6.2. 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

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

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 $\mathrm{Gal}\,(\mathbb{Q}(A[2])/\mathbb{Q}) \cong S_6$ 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 $(\mathbb{Z}/2\mathbb{Z})^4 \rtimes \mathrm{GSp}_4(\mathbb{Z}/2\mathbb{Z})$. □

Remark. As far as the authors are aware, the curve C given above is the first example of a hyperelliptic curve of genus 2 for which all of the ℓ-adic Galois representations associated to $\mathrm{Jac}(C)$ are surjective.

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 5.5 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 [**21**, p. 61].

Appendix A. *A result relating to Question 1.3*

by Jeffrey D. Achter[†]

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

PROPOSITION A.1. *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_g, 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 $\mathrm{Sp}_{2g}(\Lambda) = \mathrm{mult}^{-1}(1)$. If $m \in \Lambda^\times$ and $S \subseteq \mathrm{GSp}_{2g}(\Lambda)$, let $S^{(m)} = S \cap \mathrm{mult}^{-1}(m)$.

Since a matrix over $\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell$ is invertible if and only if its reduction modulo ℓ is,

$$\begin{aligned} \#\,\mathrm{GL}_g(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) &= \ell^{(n-1)g^2} \#\,\mathrm{GL}_g(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell) \\ &= \ell^{(n-1)g^2} \prod_{j=1}^{g} \ell^{j-1}(\ell^j - 1). \end{aligned}$$

If $n \geq 2$, a direct calculation shows that $\ker \rho_{g,n,n-1}$ is isomorphic to the Lie algebra $\mathfrak{sp}_{2g,\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell}$, so that for $n \geq 1$ we have

$$\begin{aligned} \#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) &= \ell^{(n-1)(2g^2+g)} \#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell) \\ &= \ell^{(n-1)(2g^2+g)} \prod_{j=1}^{g} \ell^{2j-1}(\ell^{2j} - 1). \end{aligned}$$

Since mult is surjective, $\#\,\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) = \#((\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^\times)\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)$.

[†]Partially supported by NSA grant H98230-08-1-0051.

For $0 \le r \le g$ define

$$S(g,r,n) = \frac{\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)}{\#\mathrm{Sp}_{2r}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)\#\mathrm{Sp}_{2(g-r)}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \tag{A.1}$$

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

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 Lagrangian.

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 A.2. *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 3.8, we have

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

□

If $x \in \mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)$, then its characteristic polynomial $f_x(T)$ is self-reciprocal. More generally, if $x \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)$ has multiplier $\mathrm{mult}(x) = m$, then the roots (over the algebraic closure of $\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell$) of $f_x(T)$ may be arranged in g pairs $\{\alpha, m/\alpha\}$.

If $x \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)$, let $\overline{\mathrm{mult}(x)} \in (\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)^\times$ be the reduction of its multiplier modulo ℓ. Define subsets of $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)$

$$\begin{aligned}\mathcal{U}_{g,n} &= \{x \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) : \text{each eigenvalue of } \rho_{g,n,1}(x) \text{ is 1 or } \overline{\mathrm{mult}(x)}\} \\ &= \{x \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) : f_x(T) \equiv (T-1)^g(T - \mathrm{mult}(x))^g \bmod \ell\} \\ \mathcal{N}_{g,n} &= \{x \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) : \rho_{g,n,1}(x) - \mathrm{id} \text{ is invertible}\} \\ &= \{x \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) : f_x(1) \not\equiv 0 \bmod \ell\}\end{aligned}$$

and quantities

$$a_{g,n}^{(m)} = \frac{\#\mathcal{U}_{g,n}^{(m)}}{\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \quad b_{g,n}^{(m)} = \frac{\#\mathcal{N}_{g,n}^{(m)}}{\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \quad d_{g,n}^{(m)} = \frac{1}{\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)} \sum_{x \in \mathcal{U}_{g,n}^{(m)}} \ell^{-\epsilon(x)}$$

for each $m \in (\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^\times$. 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, $a_{0,n}^{(m)} = b_{0,n}^{(m)} = 1$.

While this notation is convenient, in fact the quantities $a_{g,n}^{(m)}$ and $b_{g,n}^{(m)}$ are independent of n, in the following sense.

LEMMA A.3. *Suppose g and n are natural numbers with $n \geq 2$, and that $m \in (\mathbb{Z}/\ell^n)^\times$. Let $\overline{m}$ be the class of m modulo ℓ. Then $a_{g,n}^{(m)} = a_{g,1}^{(\overline{m})}$ and $b_{g,n}^{(m)} = b_{g,1}^{(\overline{m})}$.*

Proof. It suffices to prove that if $\overline{x} \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)$ with multiplier $\mathrm{mult}(\overline{x}) = \overline{m}$, and if m is any lift of $\overline{m}$ to $(\mathbb{Z}_\ell/\ell^n\mathbb{Z})^\times$, then $\#\rho_{g,n,1}^{-1}(\overline{x})^{(m)}/\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) = 1/\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)$. Since $\rho_{g,n,1}$ is surjective, $\#\rho_{g,,n,1}^{-1}(\overline{x}) = \ell^{(2g^2+g+1)(n-1)}$. Suppose m' is a second lift of $\overline{m}$. Choose $y \in \rho_{g,n,1}^{-1}(\mathrm{id})$ with $\mathrm{mult}(y) = m'm^{-1}$; then multiplication by y shows that $\#\rho_{g,n,1}^{-1}(\overline{x})^{(m)} = \#\rho_{g,n,1}^{-1}(\overline{x})^{(m')}$. There are ℓ^{n-1} different lifts m, and thus $\#\rho_{g,n,1}^{-1}(\overline{x})^{(m)}/\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell) = \ell^{-(n-1)}\ell^{(2g^2+g+1)(n-1)}/\ell^{(2g^2+g)(n-1)}\#\mathrm{Sp}_{2g}(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)$, as desired. □

Define generating functions

$$A_n^{(m)}(T) = \sum_{g\geq 0} a_{g,n}^{(m)} T^g$$
$$B_n^{(m)}(T) = \sum_{g\geq 0} b_{g,n}^{(m)} T^g.$$

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

$$V_{g,n} = E_x \oplus W_x, \tag{A.3}$$

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 $x|_{W_x} \in \mathcal{N}_{g-r,n}$. We may thus index elements of $\mathrm{GSp}(V_{g,n})$ by decompositions (A.3) and suitable choices for $x|_{E_x}$ and $x|_{W_x}$, so that

$$\#\,\mathrm{GSp}_{2g}(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^{(m)} = \sum_{r=0}^{g} S(g,r,n)\#\mathcal{U}_{r,n}^{(m)}\#\mathcal{N}_{g-r,n}^{(m)}. \tag{A.4}$$

LEMMA A.4. *For each $n \in \mathbb{N}$ and $m \in (\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^\times$, $A_n^{(m)}(T)$ is a convergent nonvanishing function on a (complex) disk of radius $R > 1$.*

Proof. By Lemma A.3, it suffices to prove the result for $n = 1$. 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 $\ell^{\dim H - \mathrm{rank} H}$ [**36**]. 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}.

In particular, $a_{g,1}^{(1)} = \ell^{g^2}/\prod_{j=1}^{g}(\ell^{2j}-1)$; an appeal to the ratio test shows that $A_1^{(1)}(T)$ converges on any disk of radius smaller than ℓ. Moreover, since $a_{0,1}^{(1)} = 1$ and $\ell \geq 3$, $a_{0,1}^{(1)} > \sum_{g\geq 1} a_{g,1}^{(1)}$ and thus $A_1^{(1)}(T)$ is nonvanishing on some disk of radius greater than one.

Now suppose $m \in (\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)^\times$ is not one. If $x \in \mathcal{U}_{g,1}^{(m)}$, then there is a decomposition $V_{g,1} = E \oplus W$ where E and W are Lagrangian subspaces stable under x, $x|_E$ is unipotent, and $x|_W$ is uniquely determined by $\mathrm{mult}(x)$ and $x|_E$. The number of decompositions of $V_{g,1}$ as a sum of Lagrangian subspaces is $L(g,1)$, and the number of choices for $x|_E$ is ℓ^{g^2-g}. Therefore, $a_{g,1}^{(m)} = 1/\prod_{j=1}^{g}(\ell^j-1)^2$, and the argument proceeds as before. □

LEMMA A.5. *Suppose $n \in \mathbb{N}$ and $m \in (\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^\times$. Then $\lim_{g\to\infty} b_{g,n}^{(m)}$ exists.*

Proof. Using (A.1), the decomposition (A.4) shows that for each g, $\sum_{r=0}^{g} a_{r,n}^{(m)} b_{g-r,n}^{(m)} = 1$. Therefore, there is an equality of generating functions

$$A_n^{(m)}(T) \cdot B_n^{(m)}(T) = \sum_{g \geq 0} T^g = \frac{1}{1-T}.$$

By Lemma A.4, there exists a number $R > 1$ such that the function $C_n^{(m)}(T) := 1/A_n^{(m)}(T)$ is analytic inside $|T| < R$. Let $C_n^{(m)}(T) = \sum c_{g,n}^{(m)} T^g$ be the series expansion of C centered at the origin. Since $B_n^{(m)}(T) = C_n^{(m)}(T)/(1-T)$, we have

$$b_{g,n}^{(m)} = \sum_{j=1}^{g} c_{g,j}^{(m)}.$$

Since $C_n^{(m)}(1)$ is well-defined, $\lim_{g\to\infty} b_{g,n}^{(m)} = C_n^{(m)}(1)$ exists. □

Proof Proof of Proposition A.1. By Lemma A.2, it suffices to show that for each n, $\lim_{g\to\infty} F(g,n)$ exists. Suppose $x \in \mathrm{GSp}(V_{g,n})$; write $V_{g,n} = E_x \oplus W_x$ as in (A.3). Then $\epsilon(x) = \epsilon(x|_{E_x})$. Therefore, we may compute $F(g,n)$ as

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

Since for fixed n there are finitely many choices for m, it suffices to show that $\lim_{g\to\infty} \sum_{r=0}^{g} b_{g-r,n}^{(m)} d_{r,n}^{(m)}$ exists. This follows from the existence (Lemma A.5) of $\lim_{g\to\infty} b_{g,n}^{(m)}$, and the fact that each term of $\sum_{g\geq 0} d_{g,n}^{(m)}$ is smaller than the corresponding term in the convergent (Lemma A.4) series $\sum_{g\geq 0} a_{g,n}^{(m)}$. □

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 $\leq x$ 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 4.4, $A : x^2 - y^2 = 1$, 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 4.6, $A : x^2 + 7y^2 = 1$, $\ell = 7$ 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 4.8, $A : x^3 + 2y^3 + 4z^3 - 6xyz = 1$, 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 5.4, $A : y^2 + y = x^3 - x$, 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 5.12, $A : y^2 = x^3 + 3$, $\ell = 2$ 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 5.13, $A : y^2 = x^3 - 207515x + 44740234$, $\ell = 2$ 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 5.14, $A : y^2 = x^3 + 3x$, $\ell = 2$ 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 6.4, $A = \mathrm{Jac}(C)$ 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	$0.57944 \leq \mathcal{F} \leq 0.58643$

References

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

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

3. W. Bosma, J. J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3):235–266, 1997.

4. Nigel Boston and Rafe Jones. The image of an arboreal Galois representation. *Pure and Applied Mathematics Quarterly* 5(1):213-225 (Special Issue: in honor of Jean-Pierre Serre, Part 2 of 2), 2009.

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. Noam D. Elkies. Elliptic curves with 3-adic Galois representations surjective mod 3 but not mod 9. available at http://arxiv.org/abs/math/0612734

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

9. Richard Gottesman and Kwokfung Tang. Quadratic recurrences with a positive density of prime divisors. Preprint.

10. 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.

11. 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.

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

13. James E. Humphreys. *Modular representations of finite groups of Lie type*, volume 326 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2006.

14. 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.

15. Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *J. Lond. Math. Soc. (2)*, 78(2):523–544, 2008.

16. Rafe Jones. Iterated Galois towers, their associated martingales, and the p-adic Mandelbrot set. *Compos. Math.*, 143(5):1108–1126, 2007.

17. C. Khare and J.-P. Wintenberger. Serre's modularity conjecture (i). Preprint.

18. C. Khare and J.-P. Wintenberger. Serre's modularity conjecture (ii). Preprint.

19. M. Kisin. Modularity of 2-adic Barsotti-Tate representations. Preprint.

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

21. Doug Kuhlman. *On the orders of Jacobians of hyperelliptic curves*. PhD thesis, University of Illinois at Urbana-Champaign, 2000.

22. J. C. Lagarias. The set of primes dividing the Lucas numbers has density 2/3. *Pacific J. Math.*, 118(2):449–461, 1985.

23. Martin W. Liebeck and Gary M. Seitz. On the subgroup structure of exceptional groups of Lie type. *Trans. Amer. Math. Soc.*, 350(9):3409–3482, 1998.

24. Qing Liu. Conducteur et discriminant minimal de courbes de genre 2. *Compositio Math.*, 94(1):51–79, 1994.

25. Pieter Moree. On primes p for which d divides $\mathrm{ord}_p(g)$. *Funct. Approx. Comment. Math.*, 33:85–95, 2005.

26. Antonella Perucca Prescribing valuations of the order of a point in the reductions of abelian varieties and tori. *J. Number Theory* 129(2):469-476, 2009.

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

28. Harriet Pollatsek. First cohomology groups of some linear groups over fields of characteristic two. *Illinois J. Math.*, 15:393–417, 1971.

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

30. Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

31. Jean-Pierre Serre. *Œuvres. Collected papers. IV*. Springer-Verlag, Berlin, 2000. 1985–1998.

32. Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

33. Jean-Pierre Serre. Abelian l-adic representations and elliptic curves. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam 1968.

34. Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

35. Joseph H. Silverman. Advanced Topics in the Arithmetic of Elliptic Curves, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

36. 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.

37. Michael Stoll. Galois groups over $\mathbf{Q}$ of some iterated polynomials. *Arch. Math. (Basel)*, 59(3):239–244, 1992.

38. A. Vasiu. Surjectivity criteria for p-adic representations. II. *Manuscripta Math.*, 114(4):399–422, 2004.

Rafe Jones
Department of Mathematics and CS
College of the Holy Cross
Worcester, MA 01607
USA

rjones@holycross.edu

Jeremy Rouse
Department of Mathematics
University of Illinois
Urbana, IL 61801
USA

jarouse@math.uiuc.edu