# SELMER STABILITY FOR ELLIPTIC CURVES IN GALOIS $\ell$-EXTENSIONS

SIDDHI PATHAK AND ANWESH RAY

Abstract. We study the behavior of Selmer groups of an elliptic curve $E/\mathbb{Q}$ in finite Galois extensions with prescribed Galois group. Fix a prime $\ell \geq 5$, a finite group $G$ with $\#G = \ell^n$, and an elliptic curve $E/\mathbb{Q}$ with $\mathrm{Sel}_\ell(E/\mathbb{Q}) = 0$ and surjective mod-$\ell$ Galois representation. We show that there exist infinitely many Galois extensions $F/\mathbb{Q}$ with Galois group $\mathrm{Gal}(F/\mathbb{Q}) \simeq G$ for which the $\ell$-Selmer group $\mathrm{Sel}_\ell(E/F)$ also vanishes. We obtain an asymptotic lower bound for the number $\mathcal{M}(G, E; X)$ of such fields $F$ with absolute discriminant $|\Delta_F| \leq X$, proving that there is an explicit constant $\delta > 0$ such that

$$\mathcal{M}(G, E; X) \gg X^{\frac{1}{\ell^{n-1}(\ell-1)}} (\log X)^{\delta-1}.$$

The asymptotic for $\mathcal{M}(G, E; X)$ matches the conjectural count for all $G$-extensions $F/\mathbb{Q}$ for which $|\Delta_F| \leq X$, up to a power of $\log X$. This demonstrates that Selmer stability is not a rare phenomenon.

## 1. Introduction

1.1. **Background and motivation.** Let $E$ be an elliptic curve defined over a number field $K$. The group $E(K)$ of $K$-rational points, known as the Mordell–Weil group, is finitely generated, and its rank is a fundamental arithmetic invariant. One fruitful approach to studying the structure of $E(K)$ is through Galois cohomology. For a fixed integer $n \geq 1$, the $n$-torsion subgroup $E[n] \subset E(\overline{K})$ carries a natural action of the absolute Galois group $\mathrm{G}_K := \mathrm{Gal}(\overline{K}/K)$. The Selmer group $\mathrm{Sel}_n(E/K) \subset H^1(K, E[n])$, defined by imposing local conditions at all primes of $K$, sits in a natural short exact sequence,

$$0 \to E(K)/nE(K) \to \mathrm{Sel}_n(E/K) \to Ш(E/K)[n] \to 0$$

encoding information about both the Mordell–Weil group and the Tate–Shafarevich group $Ш(E/K)$.

A central question in arithmetic geometry is to understand how the Mordell–Weil rank of a fixed elliptic curve varies in field extensions. For instance, given an elliptic curve $E/\mathbb{Q}$, it is natural to ask how often its rank remains the same in a finite extension $L/\mathbb{Q}$. More specifically, one studies how frequently $\mathrm{rank}\, E(L) = \mathrm{rank}\, E(\mathbb{Q})$ as $L$ ranges over number fields of fixed degree, ordered by discriminant.

In particular, these diophantine stability questions are studied for cyclic extensions of $\mathbb{Q}$ with prime degree. Mazur and Rubin [MR10] studied the distribution of 2-Selmer ranks in families of quadratic twists of a fixed elliptic curve. Their techniques yield results on the stability of rank across large sets of quadratic twists, and under certain conditions, also demonstrate that arbitrarily large ranks can arise after base change by quadratic extensions. For any prime $\ell$, Klagsbrun–Mazur–Rubin [KMR14], Mazur–Rubin [MRL18] have studied the behavior of $\ell$-Selmer groups in $\mathbb{Z}/\ell\mathbb{Z}$-extensions, establishing patterns of stability and growth. Smith has recently obtained similar results using arithmetic statistics and the geometry of numbers [Smi26, Smi22].

The broader phenomenon of rank growth and stability in families of number field extensions has attracted significant recent attention. For example, see the work of Lemke-Oliver and

Research of the first author was partially supported by an INSPIRE faculty fellowship.

**Data availability statement:** Data sharing not applicable – no new data generated, or the article describes entirely theoretical research.

**Conflict of interest statement:** The authors do not have any conflict of interest to declare.

Thorne [LOT21], Shnidman and Weiss [SW23], Beneish–Kundu–Ray [BKR24], Berg–Ryan–Young [BRY24], Keliher [Kel24], Pathak–Ray [PR25] and Keliher–Park [KP25].

Understanding Galois extensions of a fixed number field with a prescribed Galois group is a fundamental problem in number theory. Conjectures predicting the asymptotic number of such extensions, ordered by their absolute discriminant, were proposed by Malle [Mal02, Mal04]. These conjectures may be viewed as statistical refinements of the classical inverse Galois problem. Substantial progress towards this has been made in special cases. For example, the conjecture is known for abelian groups, due to the work of Mäki [Mäk85] and Wright [Wri89], and more recently for certain nilpotent groups by Koymans and Pagano [KP23]. Although the inverse Galois problem for finite solvable groups over number fields was resolved by Shafarevich [Š54], Malle's conjecture remains open for general solvable groups.

1.2. **Main results.** In this article, we apply Galois-theoretic methods to study the behavior of the Mordell–Weil rank and Selmer group of an elliptic curve $E/\mathbb{Q}$ in certain families of Galois extensions $L/\mathbb{Q}$ with a prescribed Galois group. Fix a prime $\ell \geq 5$, a finite $\ell$-group $G$, and an elliptic curve $E/\mathbb{Q}$. Assume that $\mathrm{Sel}_\ell(E/\mathbb{Q}) = 0$, or equivalently, $E(\mathbb{Q})[\ell] = 0$, $\operatorname{rank} E(\mathbb{Q}) = 0$ and $Ш(E/\mathbb{Q})[\ell] = 0$. Further, suppose that the Galois representation

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

associated to $E[\ell]$ is surjective. Under these assumptions, we show that there exist infinitely many Galois extensions $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$ such that $\mathrm{Sel}_\ell(E/L) = 0$. Moreover, we obtain an asymptotic lower bound for the number of such extensions ordered by their absolute discriminant.

For each real number $X > 0$, let $\mathcal{N}(G; X)$ denote the number of Galois extensions $L/\mathbb{Q}$ with Galois group $G$ and discriminant satisfying $|\Delta_L| \leq X$. The Hermite–Minkowski theorem ensures that $\mathcal{N}(G; X)$ is finite for every $X$, and hence is well-defined.

Let $\mathcal{G}$ be a finite group and $\pi_{\mathcal{G}} : \mathcal{G} \hookrightarrow S_{\#\mathcal{G}}$ denote the regular representation of $\mathcal{G}$. For $g \in \mathcal{G}$, define the index of $g$, denoted $\mathrm{ind}(g)$, as

$$\mathrm{ind}(g) := \#\mathcal{G} - \#\text{ orbits of } \pi_{\mathcal{G}}(g).$$

We set $a(\mathcal{G}) := \big(\min_{g \neq 1} \mathrm{ind}(g)\big)^{-1}$ and note that when $\mathcal{G}$ is an $\ell$-group with $\ell^n$ elements, $a(\mathcal{G}) = \big(\ell^{n-1}(\ell-1)\big)^{-1}$. The weak form of Malle's conjecture (cf. [Mal02, p.316]) predicts that for any $\epsilon > 0$, there exist constants $c_1(\mathcal{G}), c_2(\mathcal{G}; \epsilon) > 0$ such that

$$c_1(\mathcal{G})\, X^{a(\mathcal{G})} \leq \mathcal{N}(\mathcal{G}; X) \leq c_2(\mathcal{G}; \epsilon)\, X^{a(\mathcal{G})+\epsilon}$$

for all sufficiently large $X$. This has been established for all finite nilpotent groups by Klüners and Malle [KM04]. For finite nilpotent groups satisfying additional hypotheses, Koymans and Pagano [KP23] have proven a stronger version of Malle's conjecture, obtaining the exact asymptotic.

On the other hand, let $\mathcal{M}(\mathcal{G}, E; X)$ denote the number of Galois extensions $F/\mathbb{Q}$ with $\mathrm{Gal}(F/\mathbb{Q}) \simeq \mathcal{G}$, $|\Delta_F| \leq X$, and $\mathrm{Sel}_\ell(E/F) = 0$. Note that for such fields $F/\mathbb{Q}$, $\operatorname{rank} E(F) = 0$ and $Ш(E/F)[\ell] = 0$. Thus, the Mordell–Weil rank and the $\ell$-part of the Tate-Sharevich group of $E$ remain stable in $F/\mathbb{Q}$. For a group $G$ with $\#G = \ell^n$, our main result establishes asymptotic lower bounds for $\mathcal{M}(G, E; X)$ as $x \to \infty$, showing that it grows comparably to $\mathcal{N}(G; X)$. This demonstrates that the vanishing of the $\ell$-Selmer group over such $G$-extensions is not a rare phenomenon.

**Theorem 1.1.** *Let $\ell \geq 5$ be a prime number, and let $E/\mathbb{Q}$ be an elliptic curve with $\mathrm{Sel}_\ell(E/\mathbb{Q}) = 0$. Assume further that the representation $\rho_{E,\ell}$ is surjective. Then*

$$\mathcal{M}(G, E; X) \gg X^{\frac{1}{\ell^{n-1}(\ell-1)}} (\log X)^{\delta-1} = X^{a(G)} (\log X)^{\delta-1},$$

*where $\delta := \frac{\ell^2-\ell-1}{\ell^{n-1}(\ell^2-1)}$.*

It follows that the asymptotic growth of $\mathcal{M}(G,E;X)$ matches that of $\mathcal{N}(G;X)$ up to a power of $\log X$. In particular,

$$\lim_{X\to\infty}\frac{\log \mathcal{M}(G,E;X)}{\log \mathcal{N}(G;X)}=1.$$

For $\ell=5$, it is proven by Bhargava and Shankar [BS13] that there is a positive density of elliptic curves (ordered by height) $E_{/\mathbb{Q}}$ for which $\mathrm{Sel}_\ell(E/\mathbb{Q})=0$. On the other hand, a result of Duke [Duk97] shows that $\rho_{E,\ell}$ is surjective for almost all elliptic curves $E_{/\mathbb{Q}}$. Thus for $\ell=5$, the conditions of Theorem 1.1 hold for a positive density of elliptic curves over $\mathbb{Q}$.

It is conceivable that the results of this article can be generalized to elliptic curves defined over arbitrary number fields. However, for ease of exposition, we restrict ourselves in this paper to the case of elliptic curves defined over $\mathbb{Q}$.

1.3. **Methodology.** Let $L/K$ be an $\ell$-cyclic extension of number fields, and let $E$ be an elliptic curve defined over $\mathbb{Q}$, satisfying the hypotheses of Theorem 1.1. Suppose in addition that the $\ell$-Selmer group of $E$ over $K$ vanishes. Analyzing local to global control arguments for Selmer groups, we show that under certain ramification and splitting conditions for the extension $L/K$, the implication

$$\mathrm{Sel}_\ell(E/K)=0\Rightarrow \mathrm{Sel}_\ell(E/L)=0$$

holds. The argument then follows via induction on the length of $G$. The inverse Galois problem for finite $\ell$-groups is known from the work of Reichardt [Rei37] and Scholz [Sch37]. The Galois cohomological strategy allows us to inductively construct towers of number fields

$$\mathbb{Q}=L_0\subset L_1\subset\cdots\subset L_{n-1}\subset L_n=F,$$

where $\mathrm{Gal}(F/\mathbb{Q})\simeq G$ and $L_i/L_{i-1}$ is an $\ell$-cyclic extension. Furthermore, extending the methods of Klüners and Malle, we are able to construct many such extensions, for which at each stage, the implication

$$\mathrm{Sel}_\ell(E/L_{i-1})=0\Rightarrow \mathrm{Sel}_\ell(E/L_i)=0$$

is satisfied. A synthesis of methods from Galois cohomology, arithmetic statistics and analytic number theory give us an asymptotic lower bound, in terms of $X$, for the number of such extensions $F/\mathbb{Q}$ with $|\Delta_F|\leq X$.

1.4. **Organization.** Including the introduction, the article is organized into four sections. Section 2 revisits the classical strategy of Reichardt [Rei37] and Scholz [Sch37] for resolving the inverse Galois problem for finite $\ell$-groups over $\mathbb{Q}$. Our emphasis is on making explicit which primes split or ramify in such extensions. This information is essential for analyzing the behavior of Selmer groups in Galois towers. In Section 3, we establish sufficient conditions on an $\ell$-cyclic extension $L/K$ under which the vanishing of $\mathrm{Sel}_\ell(E/K)$ implies the vanishing of $\mathrm{Sel}_\ell(E/L)$. These build upon previous constructions in [PR25, Section 2]. We conclude this section by proving the existence of infinitely many $G$-extensions $L/\mathbb{Q}$ such that $\mathrm{Sel}_\ell(E/L)=0$. Finally, Section 4 is devoted to the proof of Theorem 1.1. We recall key results of Klüners and Malle concerning the enumeration of $G$-extensions of $\mathbb{Q}$ ordered by absolute discriminant. The problem is reduced to counting global Galois cohomology classes subject to prescribed local conditions. To estimate the size of these cohomology groups, we invoke a formula of Wiles which yields precise asymptotics, allowing us to deduce the desired lower bounds.

## 2. The inverse Galois problem for finite $\ell$-groups

Shafarevich proved that given any number field $K$ and a finite solvable group $G$, there exists a Galois extension $L/K$ with $\mathrm{Gal}(L/K)\simeq G$ (see [Saf54] and [NSW08, Chapter IX, Section 6]). Let $\ell$ be an odd prime number. Given a natural number $k$, let $\mu_k$ denote the set of $k$-th roots of unity. Fix throughout this article a finite group $G$ with $\#G=\ell^n$. In this special case, the

inverse Galois problem over $\mathbb{Q}$ for the group $G$ is due to Reichardt [Rei37] and Scholz [Sch37]. An exposition of their method can be found in [Mas06]. In this section, we review this construction with a view towards its application in establishing diophantine stability results, for which we need an understanding of the ramification of primes. More precisely, we shall see that these sets of primes are prescribed by *Chebotarev conditions*.

2.1. **The embedding problem.** We show that there is a Galois extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$. We note that $G$ has a nontrivial center. Thus by induction on $n = \mathrm{length}(G)$, there is a filtration of $G$ by normal subgroups $G_i$:

$$\{1\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G \tag{2.1}$$

such that for all $i$,

- $G_{i-1}/G_i \simeq \mathbb{Z}/\ell\mathbb{Z}$,
- $1 \to \mathbb{Z}/\ell\mathbb{Z} \to G/G_i \to G/G_{i-1} \to 1$ is a central extension of $G/G_{i-1}$.

We construct Galois extensions

$$K = L_0 \subset L_1 \subset L_2 \subset \ldots L_{n-1} \subset L_n = L$$

such that $\mathrm{Gal}(L_i/K) \simeq G/G_i$. We assume that $n \geq 1$ and reduce the solution to that of an *embedding problem*.

Let $G$ be a finite $\ell$-group and let $\widetilde{G}$ be a central extension of $G$

$$1 \to \mathbb{Z}/\ell\mathbb{Z} \xrightarrow{\iota} \widetilde{G} \xrightarrow{\pi} G \to 1. \tag{2.2}$$

Let $\mathrm{G}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and assume that there exists a Galois extension $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$. This gives rise to a surjection $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ such that $\overline{\mathbb{Q}}^{\ker\varphi} = L$. The embedding problem asks whether $L$ can be embedded into a larger Galois extension $\widetilde{L}/\mathbb{Q}$ along with an isomorphism $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}) \simeq \widetilde{G}$, such that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{Gal}(\widetilde{L}/L) & \to & \mathrm{Gal}(\widetilde{L}/\mathbb{Q}) & \to & \mathrm{Gal}(L/\mathbb{Q}) & \to 0 \\ & & \downarrow & & \downarrow & & \downarrow & \\ 0 & \to & \mathbb{Z}/\ell\mathbb{Z} & \to & \widetilde{G} & \to & G & \to 0. \end{array}$$

In the above diagram, the downward arrows are isomorphisms. Equivalently, the embedding problem is solvable if $\varphi$ can be lifted to a surjective homomorphism $\widetilde{\varphi} : \mathrm{G}_{\mathbb{Q}} \twoheadrightarrow \widetilde{G}$. Indeed, setting $\widetilde{L} := \overline{\mathbb{Q}}^{\ker\widetilde{\varphi}}$ we find that $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}) \simeq \widetilde{G}$. Note that if the extension (2.2) is non-split then any lift $\widetilde{\varphi}$ is surjective. In order to inductively construct the extensions $L_i$, it suffices to solve the embedding problem for

$$1 \to \mathbb{Z}/\ell\mathbb{Z} \to G/G_{i+1} \to G/G_i \to 1$$

for each $i$ in the range $0 \leq i < n$.

2.2. **Cohomological parametrization of extension classes.** We recall how to parametrize group extensions by cohomology classes. Let $A$ be a given abelian group and $G$ be an arbitrary finite group, and consider a central extension of $G$ by $A$:

$$1 \to A \to \widetilde{G} \xrightarrow{\pi} G \to 1.$$

Then $A$ has an induced $G$-module structure which we describe. Let $\eta : G \to \widetilde{G}$ be a set theoretic section of the map $\pi : \widetilde{G} \to G$. Since $\pi$ is surjective, such a map exists. We define the action of $G$ on $A$ as follows: for $a \in A$ and $\sigma \in G$,

$$\sigma \cdot a := \eta(\sigma)\, a\, \eta(\sigma)^{-1}.$$

There are a few things to take note of here. First, since $A$ is a normal subgroup of $G$, the element $\eta(\sigma)\, a\, \eta(\sigma)^{-1}$ is in $A$. Next, since $A$ is abelian, $\sigma \cdot a$ is independent of the choice of set theoretic section $\eta$. From here on, when referring to $A$ as a $G$-module, it will be with respect to this chosen action, and $H^i(G, A)$ will be the associated cohomology groups. Two extensions $\widetilde{G}_1$ and $\widetilde{G}_2$ are said to be equivalent if there is an isomorphism $f : \widetilde{G}_1 \xrightarrow{\sim} \widetilde{G}_2$ such that the following diagram commutes:

$$\begin{array}{ccccc} A & \longrightarrow & \widetilde{G}_1 & \longrightarrow & G \\ \| & & \downarrow f & & \| \\ A & \longrightarrow & \widetilde{G}_2 & \longrightarrow & G. \end{array}$$

**Proposition 2.1.** *Let $G$ be a finite group and $A$ be an abelian group which is also a $G$-module. There is a bijection between*

- *equivalence classes of $A$-extensions of $G$:*

$$1 \mapsto A \xrightarrow{\iota} \widetilde{G} \xrightarrow{\pi} G \to 1$$

  *such that for any set theoretic section $\eta : G \to \widetilde{G}$ of $\pi$, we have that $\sigma \cdot a = \eta(\sigma)\, a\, \eta(\sigma)^{-1}$*
- *elements of $H^2(G, A)$.*

*The class associated to $\widetilde{G}$ is denoted by $\theta_{\widetilde{G}} \in H^2(G, A)$. Moreover, the association has the property that the* trivial *class $\widetilde{G} := G \ltimes A$ corresponds to the trivial element in $H^2(G, A)$.*

*Proof.* This is a standard result, cf. [Wei94, Theorem 6.6.3]. □

## 2.3. **The method of Reichardt and Scholz.**

**Definition 2.2.** *Let $G$ be an $\ell$-group with $\#G = \ell^n$. Let $L/\mathbb{Q}$ be a Galois extension with* $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$ *and choose $N \geq n$. The extension $L/\mathbb{Q}$ satisfies the* Scholz property *for $N$, denoted $(\mathfrak{S}_N)$, if:*

- *every rational prime $p$ ramified in $L$ satisfies $p \equiv 1 \pmod{\ell^N}$,*
- *for each prime $v|p$ of $L$, we have that $L_v/\mathbb{Q}_p$ is totally ramified.*

Assuming that there exists a Galois extension $L/\mathbb{Q}$ satisfying $(\mathfrak{S}_N)$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$, we embed $L$ into a larger Galois extension $\widetilde{L}$ with $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}) \simeq \widetilde{G}$, also satisfying $(\mathfrak{S}_N)$.

**Theorem 2.3.** *Let $\ell$ be an odd prime number, $G$ be a finite group with $\#G = \ell^n$, and fix $N \geq n$. Suppose that there exists a Galois extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$ which satisfies $(\mathfrak{S}_N)$. Let $\{p_1, \ldots, p_m\}$ denote the primes that ramify in $L$. Then the embedding problem for $L$ and $\widetilde{G}$ is solvable. Moreover, the solution $\widetilde{L}$ can be chosen to satisfy $(\mathfrak{S}_N)$ with at most one additional prime outside $\{p_1, \ldots, p_m\}$ being ramified in $\widetilde{L}$.*

The proof of Theorem 2.3 is important for us to outline since the construction will be extended in subsequent sections in which our diophantine stability results are proven. More specifically, the additional ramified prime in $\widetilde{L}$ will be chosen to belong to an infinite set of primes defined by Chebotarev conditions. These conditions will be shown to be compatible with the Chebotarev conditions on primes that ensure Diophantine stability for a given elliptic curve.

2.3.1. *Proof of Theorem 2.3 in the split case.* First, we consider the case when (2.2) is split. Let $p_1, \ldots, p_m$ be the rational primes which are ramified in $L$ and $q$ be a prime number. It is easy to see that $q$ splits completely in the field $L\left(\mu_{\ell^N}, \sqrt[\ell]{p_1}, \ldots, \sqrt[\ell]{p_m}\right)$ if and only if the following conditions are satisfied:

(i) $q \equiv 1 \pmod{\ell^N}$,
(ii) $q$ splits completely in $L$,
(iii) $q \notin \{p_1, \ldots, p_m\}$ and $p_i$ is an $\ell$-th power in $\mathbb{F}_q^\times$ for $i = 1, \ldots, m$.

By the Chebotarev density theorem, there exists a positive density set of primes $\mathcal{P}_L$ that satisfy the above conditions. More specifically, this density is given by

$$\delta(\mathcal{P}_L) := \frac{1}{\left[L\left(\mu_{\ell^N}, \sqrt[\ell]{p_1}, \ldots, \sqrt[\ell]{p_m}\right) : \mathbb{Q}\right]}.$$

Let $q \in \mathcal{P}_L$ and $M_q \subset \mathbb{Q}(\mu_q)$ be the field such that $\mathrm{Gal}(M_q/\mathbb{Q}) \simeq \mathbb{Z}/\ell\mathbb{Z}$. Set $\widetilde{L} := L \cdot M_q$. Since $q$ is totally ramified in $M_q$ and split in $L$, it follows that $L \cap M_q = \mathbb{Q}$, therefore, $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}) \simeq G \times \mathbb{Z}/\ell\mathbb{Z} = \widetilde{G}$. It is easy to see that $\widetilde{L}$ satisfies $(\mathfrak{S}_N)$. In greater detail, each of the primes $p_i$ are of the form $p_i \equiv 1 \bmod \ell^N$ as $L$ satisfies $(\mathfrak{S}_N)$. The prime $q$ is assumed to satisfy $q \equiv 1 \bmod \ell^N$. Thus, all primes that ramify in $\widetilde{L}$ are $\equiv 1 \bmod \ell^N$. Given a prime $p_i$ for $i = 1, \cdots, m$, let $\widetilde{v}$ be a prime of $\widetilde{L}$ that lies above $p_i$. Let $v$ (resp. $v'$) be a prime of $L$ (resp. $M_q$) such that $\widetilde{v}|v$ (resp. $\widetilde{v}|v'$), as depicted below:


Since $L$ satisfies $(\mathfrak{S}_N)$, we have that $f(v \mid p_i) = 1$. By condition (iii) in the choice of $\mathcal{P}_L$, $p_i$ splits completely in $M_q$. Therefore, we deduce that $f(\widetilde{v} \mid p_i) = 1$, i.e., $\widetilde{L}_{\widetilde{v}}/\mathbb{Q}_{p_i}$ is totally ramified. Since $q$ splits completely in $L$ and is totally ramified in $M_q$, $f(\widetilde{w} \mid q) = 1$ for any prime $\widetilde{w}$ of $\widetilde{L}$ that lies above $q$. Thus, $\widetilde{L}$ as defined above is a solution the embedding problem and satisfies $(\mathfrak{S}_N)$. The set of primes ramified in $\widetilde{L}$ is precisely $\{p_1, \cdots, p_m, q\}$ and therefore, $\widetilde{L}$ is ramified at exactly one additional prime.

2.3.2. *Proof of Theorem 2.3 in the non-split case.* Next we focus our attention on the case when (2.2) is non-split, or equivalently, $\theta_{\widetilde{G}} \in H^2(G, \mathbb{Z}/\ell\mathbb{Z})$ is nontrivial. In this case, the extension $\widetilde{L}/L/\mathbb{Q}$ is constructed in three steps.

**Step 1:** We construct an extension $\widetilde{L}$ that solves the embedding problem for the desired group extension $\widetilde{G}$.

**Step 2:** We modify $\widetilde{L}$ so that the set of primes that ramify in $\widetilde{L}$ matches the set of ramified primes of $L$.

**Step 3:** We adjust $\widetilde{L}$ further to satisfy $(\mathfrak{S}_N)$, allowing at most one additional ramified prime $q$.

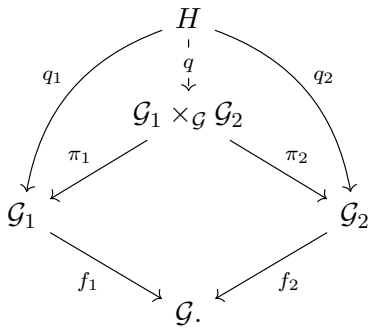
We note that step 1 corresponds to Proposition 2.9, step 2 corresponds to Proposition 2.13, and step 3 corresponds to Proposition 2.15. Recall that $L$ induces a surjective homomorphism $\varphi : \mathrm{G}_{\mathbb{Q}} \twoheadrightarrow G$ and that there is a bijection between the central extensions $\widetilde{G}$ of $G$ by $\mathbb{Z}/\ell\mathbb{Z}$ and the elements of $H^2\left(G, \mathbb{Z}/\ell\mathbb{Z}\right)$. Let $\theta = \theta_{\widetilde{G}} \in H^2\left(G, \mathbb{Z}/\ell\mathbb{Z}\right)$ be the element corresponding to the extension $\widetilde{G}$. The map $\varphi$ induces a homomorphism

$$\varphi^* : H^2\left(G, \mathbb{Z}/\ell\mathbb{Z}\right) \longrightarrow H^2\left(\mathrm{G}_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z}\right). \tag{2.3}$$

**Definition 2.4.** *Let $\mathcal{G}$, $\mathcal{G}_1$ and $\mathcal{G}_2$ be groups, and let $f_1 : \mathcal{G}_1 \to \mathcal{G}$ and $f_2 : \mathcal{G}_2 \to \mathcal{G}$ be surjective homomorphisms. The fibre product $\mathcal{G}_1 \times_{\mathcal{G}} \mathcal{G}_2$ is the group*

$$\mathcal{G}_1 \times_{\mathcal{G}} \mathcal{G}_2 = \{(g_1, g_2) \in \mathcal{G}_1 \times \mathcal{G}_2 \mid f_1(g_1) = f_2(g_2)\}$$

*with projections $\pi_1 : \mathcal{G}_1 \times_{\mathcal{G}} \mathcal{G}_2 \to \mathcal{G}_1$ and $\pi_2 : \mathcal{G}_1 \times_{\mathcal{G}} \mathcal{G}_2 \to \mathcal{G}_2$. It satisfies the universal property: for any group $H$ with homomorphisms $q_1 : H \to \mathcal{G}_1$ and $q_2 : H \to \mathcal{G}_2$ such that $f_1 \circ q_1 = f_2 \circ q_2$, there exists a unique homomorphism $q : H \to \mathcal{G}_1 \times_{\mathcal{G}} \mathcal{G}_2$ making the diagram below commute:*




**Proposition 2.5.** *The embedding problem for (2.2) is solvable if and only if $\varphi^*(\theta) = 0$, where $\varphi^*$ is given by (2.3).*

*Proof.* This is a well known result, we give a sketch of the argument. Setting $\mathfrak{G} := \widetilde{G} \times_G \mathrm{G}_{\mathbb{Q}}$, consider the fiber product diagram:

$$\begin{array}{ccccccccc} 1 & \to & \mathbb{Z}/\ell\mathbb{Z} & \to & \mathfrak{G} & \to & \mathrm{G}_{\mathbb{Q}} & \to 1 \\ & & \| & & \downarrow & & \downarrow \varphi & \\ 1 & \to & \mathbb{Z}/\ell\mathbb{Z} & \to & \widetilde{G} & \to & G & \to 1. \end{array}$$

Denote by $\pi_1 : \mathfrak{G} \to \widetilde{G}$ and $\pi_2 : \mathfrak{G} \to \mathrm{G}_{\mathbb{Q}}$ the projection maps to the first and second factors. It is easy to see that the top row is a central extension corresponding to $\varphi^*(\theta)$. This sequence splits if and only if $\varphi^*(\theta) = 0$. If the extension splits, there exists a section $j : \mathrm{G}_{\mathbb{Q}} \hookrightarrow \mathfrak{G}$ to the projection map $\pi_2 : \mathfrak{G} \twoheadrightarrow \mathrm{G}_{\mathbb{Q}}$. Then $\widetilde{\varphi} := \pi_1 \circ j$ is a lift of $\varphi$. Since it is assumed that (2.2) is nonsplit, $\widetilde{\varphi}$ is surjective. The proof of the converse follows along similar lines, and is omitted. □

In what follows, for ease of notation, set $H^i(F, \cdot) := H^i(\mathrm{G}_F, \cdot)$, where $F$ is a field of characteristic 0. Given a prime number $p$, denote by

$$\mathrm{res}_p^i : H^i(\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z}) \longrightarrow H^i(\mathbb{Q}_p, \mathbb{Z}/\ell\mathbb{Z})$$

the natural restriction map. This induces a map

$$\alpha : H^2(\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z}) \xrightarrow{\oplus_p \mathrm{res}_p^2} \bigoplus_p H^2(\mathbb{Q}_p, \mathbb{Z}/\ell\mathbb{Z}).$$

**Proposition 2.6.** *The map $\alpha$ is an injection.*

*Proof.* Let $F$ be a field of characteristic zero that contains the $\ell$-th roots of unity, and let $\mathrm{Br}(F)$ denote its Brauer group. By the standard identification $\mathrm{Br}(F) \cong H^2(F, \overline{F}^{\times})$. Letting $\mathrm{Br}(F)[\ell]$ be the $\ell$-torsion in the Brauer group, there is a natural isomorphism:

$$H^2(F, \mathbb{Z}/\ell\mathbb{Z}) \cong \mathrm{Br}(F)[\ell].$$

Now, let $K = \mathbb{Q}(\mu_\ell)$ be the cyclotomic field generated by the $\ell$-th roots of unity, and let $M_K$ denote the set of places of $K$. By the Brauer–Hasse–Noether theorem, the natural localization map

$$\alpha_K : H^2(K, \mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \bigoplus_{v \in M_K} H^2(K_v, \mathbb{Z}/\ell\mathbb{Z})$$

is injective, meaning that an element of $H^2(K, \mathbb{Z}/\ell\mathbb{Z})$ is determined by its local invariants.

Since $K/\mathbb{Q}$ is a Galois extension with degree prime to $\ell$, the inflation–restriction sequence for group cohomology shows that the restriction map

$$H^2(\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z}) \longrightarrow H^2(K, \mathbb{Z}/\ell\mathbb{Z})$$

is also injective.

These maps fit naturally into the following commutative diagram:

$$\begin{array}{ccc} H^2(\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z}) & \xrightarrow{\text{res}} & H^2(K, \mathbb{Z}/\ell\mathbb{Z}) \\ \alpha \downarrow & & \downarrow \alpha_K \\ \bigoplus_{v \in M_{\mathbb{Q}}} H^2(\mathbb{Q}_p, \mathbb{Z}/\ell\mathbb{Z}) & \xrightarrow{\text{res}} & \bigoplus_{v \in M_K} H^2(K_v, \mathbb{Z}/\ell\mathbb{Z}). \end{array}$$

We deduce from injectivity of the horizontal restriction maps and the injectivity of $\alpha_K$ that $\alpha$ is injective. □

Given a prime $p$, let $G_p := \text{Gal}(L_v/\mathbb{Q}_p) \subset G$, where $v$ is a prime of $L$ lying over $p$. A different choice of $v$ gives rise to the same subgroup of $G$ up to conjugation by an element of $G$. Set $\theta_p$ to denote the image of $\theta$ with respect to the natural restriction map:

$$\text{res}_p : H^2(G, \mathbb{Z}/\ell\mathbb{Z}) \to H^2(G_p, \mathbb{Z}/\ell\mathbb{Z}).$$

Consider the associated central extension

$$0 \to \mathbb{Z}/\ell\mathbb{Z} \to \widetilde{G}_p \to G_p \to 1 \tag{2.4}$$

and let $\varphi_p : \text{G}_{\mathbb{Q}_p} \twoheadrightarrow G_p$ be the natural quotient map. The *local embedding problem* then asks whether $\varphi_p$ admits a lift to a homomorphism $\widetilde{\varphi}_p : \text{G}_{\mathbb{Q}_p} \to \widetilde{G}_p$. Here we do not insist that $\widetilde{\varphi}_p$ is surjective. By arguments similar to those in the proof of Proposition 2.5, we find that the local embedding problem at $p$ has a solution if and only if $\varphi_p^*(\theta_p) = 0$.

**Proposition 2.7.** *With the notation as above, a surjective lift $\widetilde{\varphi} : \text{G}_{\mathbb{Q}} \twoheadrightarrow \widetilde{G}$ exists if and only if the local embedding problem is solvable for all primes $p$.*

*Proof.* By Proposition 2.5, a surjective lift $\widetilde{\varphi}$ exists if and only if $\varphi^*(\theta) = 0$. The map $\alpha : H^2(\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z}) \to \bigoplus_{p \in M_{\mathbb{Q}}} H^2(\mathbb{Q}_p, \mathbb{Z}/\ell\mathbb{Z})$ maps $\varphi^*(\theta)$ to the tuple $\alpha(\varphi^*(\theta)) = \left(\varphi_p^*(\theta_p)\right)_p$. Proposition 2.6 shows that the map $\alpha$ is injective, so it suffices to verify that $\varphi_p^*(\theta_p) = 0$ for all primes $p$. This is equivalent to the existence of a local lift $\widetilde{\varphi}_p : \text{G}_{\mathbb{Q}_p} \to \widetilde{G}_p$ at each prime $p$, which establishes the claim. □

We now show that the local embedding problem is solvable. We then deduce from Proposition 2.7 that a surjective lift $\widetilde{\varphi} : \text{G}_{\mathbb{Q}} \twoheadrightarrow \widetilde{G}$ of $\varphi : \text{G}_{\mathbb{Q}} \to G$ does exist. Given a finite group $\mathcal{G}$, recall that the Frattini subgroup $\Phi(\mathcal{G})$ is the intersection of all proper maximal subgroups of $\mathcal{G}$. If $\mathcal{G}$ is an $\ell$-group, then $\Phi(\mathcal{G}) = \mathcal{G}^p[\mathcal{G}, \mathcal{G}]$, and $\mathcal{G}/\Phi(\mathcal{G}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^d$ for some $d \geq 0$. It is well known that if $\mathcal{G}$ is a finite $\ell$-group, then $\mathcal{G}$ is cyclic if and only if the Frattini quotient $\mathcal{G}/\Phi(\mathcal{G}) \simeq \mathbb{Z}/\ell\mathbb{Z}$.

**Proposition 2.8.** *Suppose $L/\mathbb{Q}$ is a Galois extension with $\text{Gal}(L/\mathbb{Q}) \simeq G$ and canonical surjection $\varphi : \text{G}_{\mathbb{Q}} \twoheadrightarrow G$ as before. Then, for every prime $p$, the local embedding problem (2.4) is solvable.*

*Proof.* If the sequence (2.4) splits, then $\theta_p = 0$. Note that the local embedding problem is solvable if and only if $\varphi_p^*(\theta_p) = 0$. Thus we assume without loss of generality that (2.4) is non-split.

First suppose that $p$ is unramified in $L$. In this case, $G_p$ is cyclic, generated by the Frobenius element. Let $\mathbb{Q}_p^{\text{nr}}$ be the maximal unramified extension of $\mathbb{Q}_p$ and note that $\text{Gal}(\mathbb{Q}_p^{\text{nr}}/\mathbb{Q}_p)$ is isomorphic to $\widehat{\mathbb{Z}}$. We seek a lift $\widetilde{\varphi}_p : \widehat{\mathbb{Z}} \to \widetilde{G}_p$ of $\varphi_p$. In order to show that $\widetilde{\varphi}_p$ exists, it suffices to prove that $\widetilde{G}_p$ is cyclic. Indeed, $G_p$ is cyclic, in particular, abelian. Hence $\mathbb{Z}/\ell\mathbb{Z}$ contains

$[\widetilde{G}_p, \widetilde{G}_p]$. If $\mathbb{Z}/\ell\mathbb{Z} = [\widetilde{G}_p, \widetilde{G}_p]$, then, $\mathbb{Z}/\ell\mathbb{Z}$ is contained in $\Phi(\widetilde{G}_p) = [\widetilde{G}_p, \widetilde{G}_p]\widetilde{G}_p^{\ell}$. Therefore, there is a surjection $\widetilde{G}_p/\left(\mathbb{Z}/\ell\mathbb{Z}\right) \twoheadrightarrow \widetilde{G}_p/\Phi(\widetilde{G}_p)$. In particular, we find that $\widetilde{G}_p/\Phi(\widetilde{G}_p)$ must be cyclic. It follows that $\widetilde{G}_p$ must be cyclic as well. This contradicts the assumption that $[\widetilde{G}_p, \widetilde{G}_p] = \mathbb{Z}/\ell\mathbb{Z}$. Thus, $\widetilde{G}_p$ is abelian. Since $G_p$ is cyclic and the sequence (2.4) is non-split, this forces $\widetilde{G}_p$ to be cyclic. Therefore, $\varphi_p : \widehat{\mathbb{Z}} \to G_p$ lifts to a map $\widetilde{\varphi}_p : \widehat{\mathbb{Z}} \to \widetilde{G}_p$.

Next, we consider the case in which $p$ is ramified. Note that $p \equiv 1 \pmod{\ell^N}$ by the property $(\mathfrak{S}_N)$ and thus $p \neq \ell$ and the ramification of $p$ in $L$ is tame. Choose a prime $v$ of $L$ which lies above $p$. We have that $(\mathcal{O}_{L_v}/v)^{\times} = (\mathbb{Z}/p\mathbb{Z})^{\times}$. Choose a uniformizer $\pi$ of $L_v$ and consider the homomorphism $\lambda : G_p \to (\mathbb{Z}/p\mathbb{Z})^{\times}$ defined by $\sigma \mapsto \overline{\left(\frac{\sigma\pi}{\pi}\right)}$. Since $\mathbb{Z}/p\mathbb{Z}$ is the residue field of $L_v$, it is easy to check that $\lambda$ is a homomorphism. The kernel of $\lambda$ is the wild inertia subgroup of $G_p$, which is trivial. Thus, $G_p$ injects into $(\mathbb{Z}/p\mathbb{Z})^{\times}$. It follows therefore that $\varphi_p$ factors through a map $\mathrm{Gal}(F/\mathbb{Q}_p) \to \mathrm{G}_p$, where $F$ is the maximal abelian tamely ramified extension of $\mathbb{Q}_p$ with exponent dividing $\ell^N$. More explicitly, $F = F_1 \cdot F_2$, where $F_1$ is the unramified extension of $\mathbb{Q}_p$ of degree $\ell^N$ and $F_2 := \mathbb{Q}_p(p^{1/\ell^N})$. Because $G_p$ is abelian, it follows (from the same argument as in the unramified case) that $\widetilde{G}_p$ is abelian. Note that $\mathrm{Gal}(F/\mathbb{Q}_p) \simeq (\mathbb{Z}/\ell^N\mathbb{Z}) \oplus (\mathbb{Z}/\ell^N\mathbb{Z})$. As $G_p$ is a quotient of $\mathrm{Gal}(F/\mathbb{Q}_p)$, we find that $G_p \simeq \mathbb{Z}/\ell^k\mathbb{Z}$, or $G_p \simeq \mathbb{Z}/\ell^{k_1}\mathbb{Z} \oplus \mathbb{Z}/\ell^{k_2}\mathbb{Z}$ for some $k_1, k_2 \geq 1$. Since $\widetilde{G}_p$ is abelian and fits into a non-split sequence (2.4), we find that $\widetilde{G}_p \simeq \mathbb{Z}/\ell^{k+1}\mathbb{Z}$ or $\widetilde{G}_p \simeq \mathbb{Z}/\ell^{k_1+1}\mathbb{Z} \oplus \mathbb{Z}/\ell^{k_2}\mathbb{Z}$ respectively. In both cases it is clear that $\varphi_p : \mathrm{Gal}(F/\mathbb{Q}_p) \to G_p$ lifts to a homomorphism $\widetilde{\varphi}_p : \mathrm{Gal}(F/\mathbb{Q}_p) \to \widetilde{G}_p$. This completes the proof. □

**Proposition 2.9.** *There is a surjective lift $\widetilde{\varphi} : \mathrm{G}_{\mathbb{Q}} \twoheadrightarrow G$ of $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$.*

*Proof.* Proposition 2.8 implies that for each prime $p$, the local embedding problem is solvable, i.e., there is a lift $\widetilde{\varphi}_p$ of $\varphi_p$. Thus it follows from Proposition 2.7 that a lift $\widetilde{\varphi} : \mathrm{G}_{\mathbb{Q}} \to \widetilde{G}$ of $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ exists. Since the extension

$$1 \to \mathbb{Z}/\ell\mathbb{Z} \to \widetilde{G} \to G \to 1$$

is non-split, $\widetilde{\varphi}$ is surjective. □

This completes Step 1. We now move on to Step 2 which involves modifying $\widetilde{L}$ so that the set of primes that ramify in $\widetilde{L}$ matches the set of ramified primes in $L$.

The action of $\mathrm{G}_{\mathbb{Q}}$ on $\mathbb{Z}/\ell\mathbb{Z}$ is trivial, allowing us to identify $H^1(\mathrm{G}_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$ with $\mathrm{Hom}(\mathrm{G}_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$. Let $\widetilde{L}$ and $\widetilde{L}'$ be extensions of $L$ that solve the embedding problem, and let $\widetilde{\varphi}, \widetilde{\psi} : \mathrm{G}_{\mathbb{Q}} \to \widetilde{G}$ be the corresponding lifts of $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ respectively. Then for $\sigma \in \mathrm{G}_{\mathbb{Q}}$, we have that

$$\widetilde{\psi}(\sigma)\widetilde{\varphi}(\sigma)^{-1} \in \mathbb{Z}/\ell\mathbb{Z} = \ker(\widetilde{G} \to G).$$

The map $f := \widetilde{\psi}\widetilde{\varphi}^{-1} : \mathrm{G}_{\mathbb{Q}} \to \mathbb{Z}/\ell\mathbb{Z}$ is a homomorphism. In greater detail,

$$\begin{aligned} f(\sigma_1\sigma_2) =& \widetilde{\psi}(\sigma_1\sigma_2)\widetilde{\varphi}(\sigma_1\sigma_2)^{-1} \\ =& \widetilde{\psi}(\sigma_1)\widetilde{\psi}(\sigma_2)\widetilde{\varphi}(\sigma_2)^{-1}\widetilde{\varphi}(\sigma_1)^{-1} \\ =& \widetilde{\psi}(\sigma_1)\widetilde{\varphi}(\sigma_1)^{-1}\widetilde{\psi}(\sigma_2)\widetilde{\varphi}(\sigma_2)^{-1} = f(\sigma_1)f(\sigma_2) \end{aligned}$$

wherein the second last equality follows since $\widetilde{\psi}(\sigma_2)\widetilde{\varphi}(\sigma_2)^{-1}$ belongs to the center of $G$. It is clear that $f(1) = 1$ and $f(\sigma^{-1}) = f(\sigma)^{-1}$. Conversely, suppose that $f \in H^1(\mathrm{G}_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$ and $\widetilde{L}/L/\mathbb{Q}$ solves the embedding problem, with $\widetilde{\varphi} : \mathrm{G}_{\mathbb{Q}} \to \widetilde{G}$ the corresponding homomorphism. Then, $\widetilde{\psi} := \widetilde{\varphi}f : \mathrm{G}_{\mathbb{Q}} \to \widetilde{G}$ is a well defined surjective homomorphism that lifts $\varphi$. This also gives rise to a solution $\widetilde{L}'/L/K$ of the embedding problem.

**Definition 2.10.** *With respect to above notation, we refer to $\widetilde{L}'$ as the* twist *of $\widetilde{L}$ by $f$, and denote it by $\widetilde{L}^f$.*

By Proposition 2.9 a solution $\widetilde{L}/L/\mathbb{Q}$ of the embedding problem always exists. Hence there is a bijection:

$$\left\{\widetilde{L}^f/L/\mathbb{Q} : \widetilde{L}^f \text{ solves the embedding problem}\right\} \leftrightarrow H^1(\mathrm{G}_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z}).$$

Let $C$ be a finite dimensional vector space over $\mathbb{Z}/\ell\mathbb{Z}$ equipped with an action of $\mathrm{G}_{\mathbb{Q}}$. Set $C^* := \mathrm{Hom}\,(C, \mu_\ell)$ with the induced Galois module structure. Given a vector space $V$ over $\mathbb{Z}/\ell\mathbb{Z}$, denote by $V^\vee := \mathrm{Hom}(V, \mathbb{Z}/\ell\mathbb{Z})$. A prime $p$ is said to be ramified in $C$ if the inertia group $\mathrm{I}_p \subset \mathrm{G}_{\mathbb{Q}_p}$ acts non-trivially on $C$. The field $\mathbb{Q}(C)$ is the Galois extension of $\mathbb{Q}$ *cut out by* $C$. In greater detail, $\mathbb{Q}(C) := \overline{\mathbb{Q}}^{\ker \rho_C}$ where $\rho_C : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}(C)$ is the representation of $\mathrm{G}_{\mathbb{Q}}$ on $C$. Note that a prime $p$ is ramified in $C$ if and only if it ramifies in $\mathbb{Q}(C)$. Let $\Sigma_C$ be the set of primes $p$ such that either $p \neq \ell$ and $p$ is ramified in $C$, or $p = \ell$. Fix a finite set of primes $S$ containing $\Sigma_C$ and let $\mathbb{Q}_S$ be the maximal algebraic extension of $\mathbb{Q}$ in which all primes $p \notin S$ are unramified. Given a number field $F \subset \mathbb{Q}_S$, we set $H^i(\mathbb{Q}_S/F, \cdot) := H^i(\mathrm{Gal}(\mathbb{Q}_S/F), \cdot)$ where $i = 1, 2$. Moreover, we set $H^i(\mathbb{Q}_p, \cdot) := H^i(\mathrm{G}_{\mathbb{Q}_p}, \cdot)$. We define:

$$Ш^i_S(C) := \ker\left(H^i(\mathbb{Q}_S/\mathbb{Q}, C) \longrightarrow \bigoplus_{p\in S} H^i(\mathbb{Q}_p, C)\right).$$

Global duality for Ш-groups [NSW08, Theorem 8.6.7] states that there is a natural isomorphism:

$$Ш^2_S(C) \simeq Ш^1_S(C^*)^\vee. \tag{2.5}$$

For each prime $p \in S$ let $\mathcal{L}_p$ be a subspace of $H^1(\mathbb{Q}_p, C)$ and let $\mathcal{L}_p^\perp$ be the orthogonal complement of $\mathcal{L}_p$ with respect to the nondegenerate Tate local duality pairing:

$$\langle\cdot,\cdot\rangle_p : H^1(\mathbb{Q}_p, C) \times H^1(\mathbb{Q}_p, C^*) \xrightarrow{\cup} H^1(\mathbb{Q}_p, \mu_\ell) \xrightarrow{\sim} \mathbb{Z}/\ell\mathbb{Z}.$$

In other words,

$$\mathcal{L}_p^\perp := \{v \in H^1(\mathbb{Q}_p, C^*) \mid \langle w, v\rangle_p = 0 \text{ for all } w \in \mathcal{L}_p\}.$$

**Definition 2.11.** *With respect to notation above, the Selmer and dual Selmer groups, denoted $H^1_{\mathcal{L}}(\mathbb{Q}_S/\mathbb{Q}, C)$ and $H^1_{\mathcal{L}^\perp}(\mathbb{Q}_S/\mathbb{Q}, C^*)$ are defined as follows:*

$$H^1_{\mathcal{L}}(\mathbb{Q}_S/\mathbb{Q}, C) := \ker\left\{H^1(\mathbb{Q}_S/\mathbb{Q}, C) \longrightarrow \bigoplus_{p\in S} \frac{H^1(\mathbb{Q}_p, C)}{\mathcal{L}_p}\right\},$$

$$H^1_{\mathcal{L}^\perp}(\mathbb{Q}_S/\mathbb{Q}, C^*) := \ker\left\{H^1(\mathbb{Q}_S/\mathbb{Q}, C^*) \longrightarrow \bigoplus_{p\in S} \frac{H^1(\mathbb{Q}_p, C^*)}{\mathcal{L}_p^\perp}\right\}.$$

A well known formula due to Wiles implies that

$$\begin{aligned}\dim H^1_{\mathcal{L}}(\mathbb{Q}_S/\mathbb{Q}, C) - \dim H^1_{\mathcal{L}^\perp}(\mathbb{Q}_S/\mathbb{Q}, C^*) &= \dim H^0(\mathbb{Q}, C) - \dim H^0(\mathbb{Q}, C^*) \\ &+ \sum_{p\in S\cup\{\infty\}} \Big(\dim \mathcal{L}_p - \dim H^0(\mathbb{Q}_p, C)\Big),\end{aligned} \tag{2.6}$$

where it is understood that $\mathcal{L}_\infty = 0$. A variation of the Poitou–Tate sequence gives the following:

$$\begin{aligned} 0 \to H^1_{\mathcal{L}}(\mathbb{Q}_S/\mathbb{Q}, C) \to H^1(\mathbb{Q}_S/\mathbb{Q}, C) \to \bigoplus_{p\in S} \left( \frac{H^1(\mathbb{Q}_p, C)}{\mathcal{L}_p} \right) \\ \to H^1_{\mathcal{L}^\perp}(\mathbb{Q}_S/\mathbb{Q}, C^*)^\vee \to H^2(\mathbb{Q}_S/\mathbb{Q}, M) \to \bigoplus_{p\in S} H^2(\mathbb{Q}_p, C), \end{aligned} \tag{2.7}$$

see for instance, [Tay03, p. 555, l.7]. We set $I_p$ to be the inertia subgroup of $\mathrm{G}_{\mathbb{Q}_p}$ and given a $\mathrm{G}_{\mathbb{Q}_p}$-module $M$, set:

$$H^1_{\mathrm{nr}}(\mathbb{Q}_p, M) := \mathrm{image}\{H^1(\mathrm{G}_{\mathbb{Q}_p} / \mathrm{I}_p, M^{\mathrm{I}_p}) \xrightarrow{\mathrm{inf}} H^1(\mathbb{Q}_p, M)\}.$$

Consider the Selmer condition $\mathcal{L}^{\mathrm{nr}}$ where $\mathcal{L}^{\mathrm{nr}}_p := H^1_{\mathrm{nr}}(\mathbb{Q}_p, C)$ for all $p \in S$. We note that

$$\dim \mathcal{L}^{\mathrm{nr}}_p = \dim H^1(\widehat{\mathbb{Z}}, C^{\mathrm{I}_p}) = \dim H^0(\widehat{\mathbb{Z}}, C^{\mathrm{I}_p}) = \dim H^0(\mathbb{Q}_p, C), \tag{2.8}$$

where we identify $\mathrm{G}_{\mathbb{Q}_p} / \mathrm{I}_p$ with $\widehat{\mathbb{Z}}$ (see also [Ram02, Lemma 3]).

**Lemma 2.12.** *With respect to notation above, suppose that the action of $\mathrm{G}_{\mathbb{Q}}$ on $C$ is trivial. Then the following assertions hold:*

*(1)* $\dim H^1_{\mathcal{L}^{\mathrm{nr}}}(\mathbb{Q}_S/\mathbb{Q}, C) = \dim H^1_{\mathcal{L}^{\mathrm{nr}\perp}}(\mathbb{Q}_S/\mathbb{Q}, C^*) = 0.$

*(2) The map*

$$H^1(\mathbb{Q}_S/\mathbb{Q}, C) \longrightarrow \bigoplus_{p\in S} \frac{H^1(\mathbb{Q}_p, C)}{H^1_{\mathrm{nr}}(\mathbb{Q}_p, C)} \tag{2.9}$$

*is an isomorphism.*

*Proof.* Since the Galois action on $C$ is trivial, $H^1(\mathbb{Q}_S/\mathbb{Q}, C)$ consists of homomorphisms $f : \mathrm{G}_{\mathbb{Q}} \to C$ which are unramified away from $S$, and $H^1_{\mathcal{L}^{\mathrm{nr}}}(\mathbb{Q}_S/\mathbb{Q}, C)$ is the subset of homomorphisms which are unramified at all primes. Such unramified homomorphisms cut out unramified abelian extensions of $\mathbb{Q}$. Since there are no proper abelian unramified extensions of $\mathbb{Q}$, it follows that $H^1_{\mathcal{L}^{\mathrm{nr}}}(\mathbb{Q}_S/\mathbb{Q}, C) = 0$. Thus, $\dim H^1_{\mathcal{L}^{\mathrm{nr}}}(\mathbb{Q}_S/\mathbb{Q}, C) = 0$. Recall from (2.8) that for $p \in S$,

$$\dim \mathcal{L}^{\mathrm{nr}}_p - \dim H^0(\mathbb{Q}_p, C) = 0.$$

We have that

$$\dim \mathcal{L}^{\mathrm{nr}}_\infty - \dim H^0(\mathbb{Q}_\infty, C) = -\dim C.$$

Note that since the action on $C$ is the trivial one,

$$\dim H^0(\mathbb{Q}, C) = \dim C \text{ and } \dim H^0(\mathbb{Q}, C^*) = 0.$$

Thus, from (2.6),

$$\dim H^1_{\mathcal{L}^{\mathrm{nr}}}(\mathbb{Q}_S/\mathbb{Q}, C) - \dim H^1_{\mathcal{L}^{\mathrm{nr},\perp}}(\mathbb{Q}_S/\mathbb{Q}, C^*) = \dim C - 0 + \sum_{p\in S} 0 - \dim C = 0.$$

Thus, we deduce that

$$\dim H^1_{\mathcal{L}^{\mathrm{nr}\perp}}(\mathbb{Q}_S/\mathbb{Q}, C^*) = \dim H^1_{\mathcal{L}^{\mathrm{nr}}}(\mathbb{Q}_S/\mathbb{Q}, C) = 0.$$

This completes the proof of (1). Part (2) then follows from (1) and the exact sequence (2.7). □

**Proposition 2.13.** *With respect to notation above, there exists $\widetilde{L}/L/\mathbb{Q}$ solving the embedding problem such that $\widetilde{L}$ is ramified at the same set of primes as $L$.*

*Proof.* It follows from Proposition 2.9 that there exists $\widetilde{L}/L/\mathbb{Q}$ solving the embedding problem. Let $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ and $\widetilde{\varphi} : \mathrm{G}_{\mathbb{Q}} \to \widetilde{G}$ be the homomorphisms corresponding to $L$ and $\widetilde{L}$ respectively. Let $\Sigma$ (resp. $S$) be the set of primes which ramify in $L$ (resp. $\widetilde{L}$). We modify $\widetilde{\varphi}$ by a class $f \in H^1(\mathrm{G}_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$ such that $\widetilde{\psi} := \widetilde{\varphi} f$ is unramified at all primes $p \notin \Sigma$. For each prime $p \in S$ we can choose a lift $\widetilde{\psi}_p : \mathrm{G}_{\mathbb{Q}_p} \to \widetilde{G}_p$ of $\varphi_p$ such that for $p \in S \setminus \Sigma$, $\widetilde{\psi}_p$ is unramified. Such a lift can be constructed as in the proof of Proposition 2.8. For $p \in S \setminus \Sigma$, let $f_p \in H^1(\mathbb{Q}_p, \mathbb{Z}/\ell\mathbb{Z})$ be such that $\widetilde{\psi}_p = \widetilde{\varphi}_p f_p$. On the other hand, for $p \in \Sigma$, set $f_p := 0$. Consider the tuple of elements

$$(f_p)_{p \in S} \in \left( \bigoplus_{p \in S} \frac{H^1(\mathbb{Q}_p, \mathbb{Z}/\ell\mathbb{Z})}{H^1_{\mathrm{nr}}(\mathbb{Q}_p, \mathbb{Z}/\ell\mathbb{Z})} \right).$$

By part 2 of Lemma 2.12, there exists $f \in H^1(\mathbb{Q}_S/\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z})$ which restricts to $(f_p)_{p \in S}$. Note that by construction, $f_{|\,\mathrm{I}_p} = f_{p|\,\mathrm{I}_p}$ for all $p \in S$. It follows that $\widetilde{\psi} := \widetilde{\varphi} f$ is unramified at all primes $p \in S \setminus \Sigma$. Let $\widetilde{L}'$ be the extension corresponding to $\widetilde{\psi}$, then $\widetilde{L}'/L/\mathbb{Q}$ is a solution to the embedding problem which is unramified away from $\Sigma$. □

Let $F$ be the $\mathbb{Z}/\ell^{N-1}\mathbb{Z}$-extension of $\mathbb{Q}$ which is contained in $\mathbb{Q}(\mu_{\ell^N})$. Note that $\mathbb{Q}(\mu_{\ell^N}) = F \cdot \mathbb{Q}(\mu_\ell)$.

**Lemma 2.14.** *The following assertions hold:*

*(i) The fields $F$ and $L$ are linearly disjoint,*
*(ii) $FL$ and $\mathbb{Q}(\mu_\ell, \sqrt[\ell]{p_1}, \ldots, \sqrt[\ell]{p_m})$ are linearly disjoint.*

*Proof.* The prime $\ell$ is unramified in $L$ and is totally ramified in $F$. Therefore, $F$ and $L$ are linearly disjoint. The Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_\ell, \sqrt[\ell]{p_1}, \ldots, \sqrt[\ell]{p_m})/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^m \rtimes (\mathbb{Z}/\ell\mathbb{Z})^\times$, where multiplication is given by $(x, y) \cdot (x', y') = (x + yx', yy')$. It is easy to see that this group has no quotient of order $\ell$. On the other hand, $FL$ is an $\ell$-group. Hence we find that $FL \cap \mathbb{Q}(\mu_\ell, \sqrt[\ell]{p_1}, \ldots, \sqrt[\ell]{p_m}) = \mathbb{Q}$. □

**Proposition 2.15.** *There exists $\widetilde{L}/L/\mathbb{Q}$ solving the embedding problem such that:*

*(1) $\widetilde{L}$ satisfies $(\mathfrak{S}_N)$,*
*(2) $\widetilde{L}$ is ramified at the primes in $\Sigma$ and one additional prime $q$. The prime $q$ can be chosen from a certain set of primes which has positive density.*

*Proof.* From Proposition 2.13, we obtain a solution $\widetilde{L}$ to the embedding problem for $\widetilde{G}$, which is ramified at precisely the same set of primes $\Sigma = \{p_1, \ldots, p_m\}$ as $L$. Each prime $p_i$ satisfies $p_i \equiv 1 \pmod{\ell^N}$, and the decomposition group $G_{p_i}$ coincides with the inertia group $\mathrm{I}_{p_i}$ at $p_i$. Since $p_i$ is tamely ramified in $L$, the inertia group $\mathrm{I}_{p_i}$ is cyclic, and consequently, $G_{p_i}$ is also cyclic for each $i = 1, \ldots, m$.

Now, fix $p = p_i$ and let $I'_p$ (resp. $G'_p$) is the inertia (resp. decomposition) group of $p$ in $\widetilde{L}$. On the other hand, we set $\widetilde{I}_p$ (resp. $\widetilde{G}_p$) to be the inverse image of $I_p$ (resp. $G_p$) with respect to the map $\pi : \widetilde{G} \to G$. Since $I_p = G_p$, it follows that $\widetilde{I}_p = \widetilde{G}_p$. Since the ramification of $p$ is tame, the inertia groups $I_p$ and $I'_p$ are cyclic. Suppose that $I_p \simeq \mathbb{Z}/\ell^\alpha\mathbb{Z}$. From the proof of Proposition 2.8, $\widetilde{G}_p$ is abelian, hence so is $\widetilde{I}_p$. Therefore, there are two possibilities for $\widetilde{I}_p$.

**Case 1.** $\widetilde{I}_p \simeq \mathbb{Z}/\ell^\alpha\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$**:** Since $I'_p$ is cyclic and the quotient map from $I'_p$ to $I_p$ is surjective, it follows that $I'_p \simeq I_p$. On the other hand, $G'_p \subseteq \widetilde{G}_p = \widetilde{I}_p$ and thus $G'_p/I'_p$ is either 1 or $\mathbb{Z}/\ell\mathbb{Z}$. There is an inclusion

$$G'_p/I'_p \hookrightarrow \widetilde{G}_p/I'_p \xrightarrow{\sim} \mathbb{Z}/\ell\mathbb{Z}$$

with respect to which the Frobenius element $\sigma_p$ maps to some $c_p \in \mathbb{Z}/\ell\mathbb{Z}$. If $c_p = 1$, then $G'_p = I'_p$ and the condition $(\mathfrak{S}_N)$ is satisfied at $p$.

**Case 2.** $\widetilde{I}_p \simeq \mathbb{Z}/\ell^{\alpha+1}\mathbb{Z}$**:** Since the map $I'_p \to I_p$ is surjective, it follows that $I'_p = \widetilde{I}_p = \widetilde{G}_p$. This forces $I'_p = G'_p$. In this case, we simply set $c_p := 1$.

If $c_p = 1$ for all the primes $p$ in Case 1 above, then $\widetilde{L}$ satisfies property $(\mathfrak{S}_N)$. Otherwise, we must modify $\widetilde{L}$. Define $X$ as the set of all primes ramified in $L$ such that $\widetilde{I}_p \simeq I_p \times \mathbb{Z}/\ell\mathbb{Z}$.

Given a prime $q \equiv 1 \pmod{\ell^N}$, there exists a unique surjective Galois character

$$\chi^{(q)} : \mathrm{Gal}(\mathbb{Q}(\mu_q)/\mathbb{Q}) \to \mathbb{Z}/\ell\mathbb{Z}.$$

Identifying $\mathrm{Gal}(\mathbb{Q}(\mu_q)/\mathbb{Q})$ with $(\mathbb{Z}/q\mathbb{Z})^\times$, and the $\ell$-torsion in $(\mathbb{Z}/q\mathbb{Z})^\times$ with $\mathbb{Z}/\ell\mathbb{Z}$, $\chi^{(q)}$ is given by $\chi^{(q)}(a) := a^{(q-1)/\ell}$. Set $\mathbb{L} := L\left(\mu_{\ell^N} \cup \{\sqrt[\ell]{p} | p \in X\}\right)$ and let $\Delta := \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. There exists $\sigma \in \Delta$ such that, for any prime $q$ unramified in $\mathbb{L}$ with $\sigma_q = \sigma$, the following conditions hold:

(1) $q \equiv 1 \pmod{\ell^N}$,
(2) $q$ splits completely in $L/\mathbb{Q}$,
(3) $\chi^{(q)}(p) = c_p$ for all $p \in X$.

More precisely, $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ is the element defined by:

- $\sigma_{|FL} = 1$,
- $\sigma(\zeta_\ell) = \zeta_\ell$,
- $\sigma(\sqrt[\ell]{p}) = c_p\sqrt[\ell]{p}$ for all primes $p \in X$.

Such an element exists since $FL \cap \mathbb{Q}\left(\mu_{\ell^N} \cup \{\sqrt[\ell]{p} | p \in X\}\right) = \mathbb{Q}$ by Lemma 2.14. Let $\widetilde{\varphi} : \mathrm{G}_\mathbb{Q} \to \widetilde{G}$ correspond to $\widetilde{L}$, and define $\widetilde{\psi} := \widetilde{\varphi}(\chi^{(q)})^{-1}$, with the corresponding extension denoted $\widetilde{L}'/L/\mathbb{Q}$. This modified extension solves the embedding problem for $\widetilde{G}$ while ensuring that property $(\mathfrak{S}_N)$ is satisfied.

□

**Theorem 2.16.** *Let $G$ be an $\ell$-group. Then there exist infinitely many Galois extensions $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$.*

*Proof.* Set $N$ to be such that $\#G = \ell^N$. Recall the filtration on $G$ by subgroups $G_i$ as in (2.1). By induction on $i$, we construct Galois extensions

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \ldots L_{n-1} \subset L_n = L$$

such that $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq G/G_i$ and $L_i/\mathbb{Q}$ satisfies the condition $(\mathfrak{S}_N)$. Assume that $L_i/\mathbb{Q}$ can be constructed so that $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq G/G_i$ and $(\mathfrak{S}_N)$ is satisfied. If the exact sequence

$$1 \to \mathbb{Z}/\ell\mathbb{Z} \to G/G_{i+1} \to G/G_i \to 1$$

is split, then the construction of $L_{i+1}/L_i/\mathbb{Q}$ follows from the argument in section 2.3.1. On the other hand, if the above exact sequence is non-split, then, the construction of $L_{i+1}/L_i/\mathbb{Q}$ can be obtained by Proposition 2.15 in section 2.3.2. The construction involves an application of the Chebotarev density theorem in choosing the prime $q$. In particular, there are infinitely many choices of $q$, and hence, infinitely many choices of $L_{i+1}$. This completes the proof. □

## 3. Selmer and diophantine stability results

3.1. **Selmer groups and diophantine stability in cyclic $\ell$-extensions.** We summarize and recall the results in [PR25, section 2]. Throughout this section, $\ell$ is a fixed odd rational prime number and $L/K$ a Galois extension of number fields with $\mathrm{Gal}(L/K) = G \simeq \mathbb{Z}/\ell\mathbb{Z}$. Let $M$ be a finite dimensional $\mathbb{F}_\ell$ vector space equipped with the structure of a $G$-module. Define $M^G := \{m \in M \mid gm = m \text{ for all } g \in G\}$ and $M_G := M/\langle (g-1)m \mid g \in G, m \in M\rangle$. The following lemma is useful.

**Lemma 3.1.** *If $M^G = 0$ or $M_G = 0$, then $M = 0$.*

*Proof.* See [NSW08, Proposition 1.6.12]. □

Let $E$ be a fixed elliptic curve defined over $K$. Given a finite extension $F/K$, denote by $E(F)$ (resp. $Ш(E/F)$) the *Mordell–Weil group* (resp. *Tate–Shafarevich group*) of $E$ over $F$. Fix an algebraic closure $\overline{L}$ of $L$ and let $\mathrm{G}_L = \mathrm{Gal}(\overline{L}/L)$ denote the absolute Galois group of $L$. Let $\Omega_L$ be the set of all non-archimedean places of $L$, and for each $v \in \Omega_L$, let $L_v$ denote the completion of $L$ at $v$. Choose an algebraic closure $\overline{L}_v$ of $L_v$ and fix an embedding $\iota_v : \overline{L} \hookrightarrow \overline{L}_v$. This choice induces an embedding of Galois groups $\iota_v^* : \mathrm{G}_{L_v} \hookrightarrow \mathrm{G}_L$, where we set $\mathrm{G}_{L_v} := \mathrm{Gal}(\overline{L}_v/L_v)$. For notational convenience, we write

$$H^i(L, \cdot) := H^i(\mathrm{G}_L, \cdot), \quad H^i(L_v, \cdot) := H^i(\mathrm{G}_{L_v}, \cdot)$$

for all $i \geq 0$ and $v \in \Omega_L$. Given a global cohomology class $f$, we denote its restriction to $\mathrm{G}_{L_v}$ by $\mathrm{res}_v(f)$.

Given a prime $v$ of $L$ and a natural number $n$, let

$$\kappa_{E,v}^{(n)} : \frac{E(L_v)}{\ell^n E(L_v)} \hookrightarrow H^1(L_v, E[\ell^n])$$

denote the *Kummer map*. Passing to the direct limit, we get the map:

$$\kappa_{E,v} : E(L_v) \otimes \left(\mathbb{Q}_\ell/\mathbb{Z}_\ell\right) \hookrightarrow H^1(L_v, E[\ell^\infty]).$$

For $n \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$, the Selmer group associated with the pair $(E, L)$ and the prime power $\ell^n$ is defined as

$$\mathrm{Sel}_{\ell^n}(E/L) := \ker\left(H^1(L, E[\ell^n]) \to \prod_{v \in \Omega_L} H^1(L_v, E)[\ell^n]\right).$$

Equivalently, $\mathrm{Sel}_{\ell^n}(E/L)$ consists of cohomology classes $f \in H^1(L, E[\ell^n])$ whose restrictions to every completion $L_v$, for $v \in \Omega_L$, lie in the image of the local Kummer map $\kappa_{E,v}^{(n)}$. There is a natural short exact sequence relating the Mordell–Weil, Selmer and Tate–Shafarevich groups:

$$0 \to E(L) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \to \mathrm{Sel}_{\ell^\infty}(E/L) \to Ш(E/L)[\ell^\infty] \to 0.$$

**Definition 3.2.** *Let $S$ be the finite set of primes $v$ of $K$ such that at least one of the following conditions is satisfied:*

- *$v$ is ramified in $L$,*
- *$E$ has bad reduction at $v$,*
- *$v$ divides $\ell$.*

We denote by $S(L)$ the set of primes of $L$ lying above those in $S$. Let $L_S$ be the maximal subextension of $\overline{L}/L$ in which all non-archimedean primes $v \notin S$ remain unramified. In fact, the $\ell$-Selmer group of $E$ over $L$ is then given by

$$\mathrm{Sel}_\ell(E/L) := \ker\left(H^1(L_S/L, E[\ell]) \xrightarrow{\Phi_{S,L}} \bigoplus_{w \in S(L)} H^1(L_w, E)[\ell]\right),$$

where $\Phi_{S,L}$ is the direct sum of restriction maps at primes $w \in S(L)$. Given a vector space $V$ over $\mathbb{F}_\ell$, set $V^\vee$ to denote its dual. The Cassels–Poitou–Tate sequence then gives the following:

$$0 \to \mathrm{Sel}_\ell(E/K) \to H^1(K_S/K, E[\ell]) \xrightarrow{\Phi_{S,K}} \bigoplus_{v \in S} H^1(K_v, E)[\ell] \to \mathrm{Sel}_\ell(E/K)^\vee \to H^2(K_S/K, E[\ell]) \to \ldots,$$

cf. [CS10, p.8]. For a prime $v$ of $K$, define the restriction map

$$\gamma_v : H^1(K_v, E)[\ell] \to \bigoplus_{w|v} H^1(L_w, E)[\ell],$$

where $w$ runs over primes of $L$ above $v$. Assume that $\mathrm{Sel}_\ell(E/K) = 0$, and note that in this case the map $\Phi_{S,K}$ is surjective. Note that there is a short exact sequence

$$0 \to E(K) \otimes \mathbb{Z}/\ell\mathbb{Z} \to \mathrm{Sel}_\ell(E/K) \to Ш(E/K)[\ell] \to 0.$$

As $\mathrm{Sel}_\ell(E/K) = 0$, we have that $E(K) \otimes \mathbb{Z}/\ell\mathbb{Z} = 0$, implying $E(K)[\ell] = 0$ and $\operatorname{rank} E(K) = 0$. Thus we have a commutative diagram:

$$\begin{array}{ccccccc} 0 = \mathrm{Sel}_\ell(E/K) & \longrightarrow & H^1(K_S/K, E[\ell]) & \xrightarrow{\Phi_{S,K}} & \bigoplus_{v\in S} H^1(K_v, E)[\ell] & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 \longrightarrow \mathrm{Sel}_\ell(E/L)^G & \longrightarrow & H^1(K_S/L, E[\ell])^G & \to & \left(\bigoplus_{w\in S(L)} H^1(L_w, E)[\ell]\right)^G, & & \end{array} \tag{3.1}$$

where $\gamma = \bigoplus_{v\in S} \gamma_v$.

**Proposition 3.3.** *Suppose* $\mathrm{Sel}_\ell(E/K) = 0$. *Let* $S$ *be as in Definition 3.2. Then:*

*(i)* $\dim_{\mathbb{F}_\ell}(\mathrm{Sel}_\ell(E/L)^G) = \sum_{v\in S} \dim_{\mathbb{F}_\ell}(\ker \gamma_v)$.

*(ii)* $\mathrm{Sel}_\ell(E/L) = 0$ *if and only if* $\gamma_v$ *is injective for all* $v \in S$.

*Proof.* Consider the commutative diagram (3.1). The inflation-restriction sequence gives

$$\ker \beta \simeq H^1(L/K, E(L)[\ell]), \quad \operatorname{coker}\beta \subseteq H^2(L/K, E(L)[\ell]).$$

As $L/K$ is a $p$-extension and $E(L)[\ell]^G = E(K)[\ell] = 0$, Lemma 3.1 yields $E(L)[\ell] = 0$, so $\ker\beta = \operatorname{coker}\beta = 0$. Thus, $\mathrm{Sel}_\ell(E/L)^G \simeq \ker\gamma$, proving (i). The claim in (ii) follows from Lemma 3.1. □

Given a prime $v$ of $K$, let $k_v$ be the residue field of $K$ at $v$ and let $\widetilde{E}(k_v)$ be the group of $k_v$ points of the reduction of $E$ at $v$.

**Proposition 3.4.** *With respect to the above notation, assume that the following conditions hold:*

*(i)* $\mathrm{Sel}_\ell(E/K) = 0$,

*(ii) all primes of* $K$ *that lie above* $\ell$ *and the primes of bad reduction for* $E$ *are completely split in* $L$,

*(iii) all primes* $v$ *of* $K$ *that ramify in* $L$ *satisfy* $\widetilde{E}(k_v)[\ell] = 0$.

*Then,* $\mathrm{Sel}_\ell(E/L) = 0$.

*Proof.* It follows from the assumptions above that $\gamma_\ell$ is injective for every prime $\ell \in S$ and thus by Proposition 3.3, $\mathrm{Sel}_\ell(E/L) = 0$. For further details, we refer to the proof of [PR25, Proposition 2.9]. □

Let $\rho_{E,\ell} : \mathrm{G}_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ be the Galois representation on $E[\ell]$, and let $\mathbb{Q}(E[\ell])$ be the field fixed by $\ker\rho_{E,\ell}$, so that $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \simeq \operatorname{im}\rho_{E,\ell}$. For a prime $p$ of good reduction for $E$, let $\mathrm{G}_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ with inertia subgroup $\mathrm{I}_p$, and choose a lift $\sigma_p \in \mathrm{G}_{\mathbb{Q}_p}$ of the Frobenius. The trace and determinant of $\rho_{E,\ell}(\sigma_p)$ satisfy

$$\operatorname{trace}\rho_{E,\ell}(\sigma_p) \equiv a_p(E) \bmod \ell, \quad \det\rho_{E,\ell}(\sigma_p) \equiv p \bmod \ell.$$

Setting $K(E[\ell]) = K \cdot \mathbb{Q}(E[\ell])$, we introduce a key set of primes central to our results.

**Definition 3.5.** *Define* $\mathfrak{T}_{E,K}$ *as the set of rational primes* $p$ *satisfying: (a)* $p \neq \ell$, *(b)* $p$ *is a prime of good reduction for* $E$, *(c)* $p$ *is completely split in* $K(\mu_\ell)$, *and (d)* $\operatorname{trace}(\rho_{E,\ell}(\sigma_p)) \neq 2$.

**Remark 3.6.** *For $p \in \mathfrak{T}_{E,K}$, $\widetilde{E}(k_v)[\ell] = 0$ for any of the primes of $K$ such that $v|\ell$ (cf.* [PR25, Lemma 2.11]*).*

**Lemma 3.7.** *If $\rho_{E,\ell}$ is surjective and $K(\mu_\ell) \cap \mathbb{Q}(E[\ell]) = \mathbb{Q}(\mu_\ell)$, then $\mathfrak{T}_{E,K}$ has natural density*

$$\mathfrak{d}(\mathfrak{T}_{E,K}) = \frac{\ell^2 - \ell - 1}{[K(\mu_\ell) : \mathbb{Q}(\mu_\ell)]\,(\ell^2 - 1)(\ell - 1)}.$$

*In particular, $\mathfrak{T}_{E,K}$ is infinite.*

*Proof.* See the proof of [PR25, Lemma 2.12]. □

3.2. **Main results.** Let $\ell \geq 5$ be a prime number and $E$ be an elliptic curve over $\mathbb{Q}$. We note the following recurring observation.

**Lemma 3.8.** *Assume that $\rho_{E,\ell}$ is surjective and let $F/\mathbb{Q}(\mu_\ell)$ be a Galois extension for which $\mathrm{Gal}(F/\mathbb{Q}(\mu_\ell))$ is an $\ell$-group. Then,*

$$F \cap \mathbb{Q}(E[\ell]) = \mathbb{Q}(\mu_\ell).$$

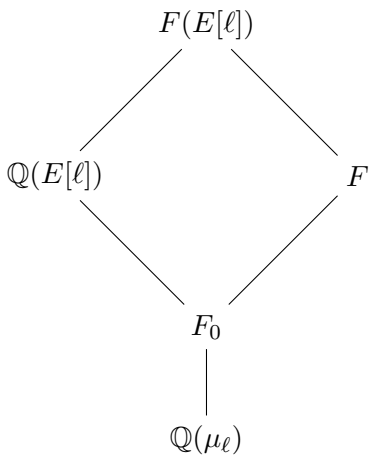
*Proof.* Since $\rho_{E,\ell}$ is surjective, it induces an isomorphism

$$\varrho : \mathrm{Gal}\left(\mathbb{Q}(E[\ell])/\mathbb{Q}(\mu_\ell)\right) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{F}_\ell).$$

Set $F_0 := F \cap \mathbb{Q}(E[\ell])$ and

$$N := \varrho\left(\mathrm{Gal}(\mathbb{Q}(E[\ell])/F_0)\right) \subseteq \mathrm{SL}_2(\mathbb{F}_\ell).$$

Consider the field diagram:




Since $F_0$ is a Galois $\ell$-extension of $\mathbb{Q}(\mu_\ell)$, $N$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$ and we have that

$$[\mathrm{SL}_2(\mathbb{F}_\ell) : N] = [F_0 : \mathbb{Q}(\mu_\ell)] = \ell^k,$$

for some $1 \leq \ell^k \leq [F : \mathbb{Q}(\mu_\ell)]$. For primes $\ell \geq 5$, Galois [Gal46, p. 412] showed that $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is simple. Therefore, $\mathrm{SL}_2(\mathbb{F}_\ell)$ does not contain a proper normal subgroup $N$ with odd index $[\mathrm{SL}_2(\mathbb{F}_\ell) : N]$. It thus follows that $\ell^k = 1$ and $F_0 = \mathbb{Q}(\mu_\ell)$. □

For the discussion below, assume the following:

- $\rho_{E,\ell}$ is surjective, and
- $\mathrm{Sel}_\ell(E/\mathbb{Q}) = 0$.

For ease of notation, we set $\mathfrak{T}_E := \mathfrak{T}_{E,\mathbb{Q}}$. Let $\Sigma$ be a finite set of primes containing $\ell$ and the primes at which $E$ has bad reduction. The result below is used in conjunction with Proposition 3.4 to prove Theorem 3.10, which is the main result of this section.

**Proposition 3.9.** *Let $G$ be an $\ell$-group with $\#G = \ell^n$ and let $N \geq n$. There are infinitely many Galois extensions $L/\mathbb{Q}$ such that:*

*(i)* $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$,
*(ii) if $p_1, \ldots, p_m$ are all the primes that are ramified in $L$, then $m \leq n$, $p_1, \ldots, p_m \in \mathfrak{T}_E \setminus \Sigma$, $p_i \equiv 1 \pmod{\ell^N}$ and the inertial degree of $p_i$ in $L$ is 1 for $i = 1, \ldots, m$,*
*(iii) all primes $q \in \Sigma$ are completely split in $L$.*

*Proof.* We prove the result by induction on $n$. First we consider the case when $n = 1$, i.e., when $G \simeq \mathbb{Z}/\ell\mathbb{Z}$. Given a prime $p \equiv 1 \pmod{\ell}$, let $L^p$ be the unique $\mathbb{Z}/\ell\mathbb{Z}$-extension of $\mathbb{Q}$ which is contained in $\mathbb{Q}(\mu_p)$. We show that there is a positive density of primes $p$ for which:

(1) $p \in \mathfrak{T}_E \setminus \Sigma$
(2) $p \equiv 1 \pmod{\ell^N}$
(3) all primes $q \in \Sigma$ split completely in $L^p$.

For such a $p$, $p$ is totally ramified in $L^p$ and thus the inertial degree of $p$ in $L^p$ is 1. Therefore, $L^p$ satisfies the conditions (i), (ii), (iii). We show that $p$ as above is determined by certain non-empty Chebotarev conditions. In other words, there exists a Galois extension $\mathcal{F}/\mathbb{Q}$ and a conjugation invariant non-empty subset $\mathcal{S} \subseteq \mathrm{Gal}(\mathcal{F}/\mathbb{Q})$, such that a prime $p$ which is unramified in $\mathcal{F}$ satisfies (1), (2), (3) if and only if the Frobenius element $\sigma_p \in \mathcal{S}$. The condition that $p \equiv 1 \pmod{\ell^N}$ is equivalent to the requirement that $p$ splits completely in $\mathbb{Q}(\mu_{\ell^N})$, i.e., $\sigma_p = 1$. The primes $q \in \Sigma$ are required to split in $L^p$. In other words, $q$ is an $\ell$-th power modulo $p$. Thus, $p$ is required to split completely in $\mathcal{F}' := \mathbb{Q}(\mu_{\ell^N} \cup \{\sqrt[\ell]{q} \mid q \in \Sigma\})$. On the other hand, by Lemma 3.8, $\mathcal{F}' \cap \mathbb{Q}(E[\ell]) = \mathbb{Q}(\mu_\ell)$. Setting $\mathcal{F} := \mathcal{F}' \cdot \mathbb{Q}(E[\ell]) = \mathbb{Q}(E[\ell] \cup \mu_{\ell^N} \cup \{\sqrt[\ell]{q} \mid q \in \Sigma\})$, one finds that

$$\mathrm{Gal}\left(\mathcal{F}/\mathbb{Q}(\mu_\ell)\right) \simeq \mathrm{Gal}\left(\mathcal{F}'/\mathbb{Q}(\mu_\ell)\right) \times \mathrm{Gal}\left(\mathbb{Q}(E[\ell])/\mathbb{Q}(\mu_\ell)\right).$$

Let $\mathcal{S} := \mathcal{S}_1 \times \mathcal{S}_2$ where $\mathcal{S}_1 = \{1\} \subset \mathrm{Gal}(\mathcal{F}'/\mathbb{Q}(\mu_\ell))$ and $\mathcal{S}_2 \subset \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}(\mu_\ell))$ consisting of $\sigma$ such that $\operatorname{trace} \rho_{E,\ell}(\sigma) \not\equiv 2 \pmod{\ell}$. It is clear that if $p \notin \Sigma$ is a prime which is unramified in $\mathcal{F}$ and $\sigma_p \in \mathcal{S}$, then the conditions (1)–(3) are satisfied. By the Chebotarev density theorem, this set of primes $p$ has positive density.

For $n \geq 2$ by induction hypothesis, suppose that we are given a central extension

$$1 \to \mathbb{Z}/\ell\mathbb{Z} \to G \to \overline{G} \to 1$$

and that there exists a Galois extension $L/\mathbb{Q}$ of degree $\ell^{n-1}$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq \overline{G}$ such that (i)–(iii) are satisfied. Let $\{p_1, \ldots, p_m\}$ (with $m \leq n-1$) be the primes that ramify in $L$. Then we show that there exists $\widetilde{L}/L/\mathbb{Q}$ such that $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}) \simeq G$ satisfying (i)–(iii), and $\widetilde{L}$ is ramified at $\{p_1, \ldots, p_m, p_{m+1}\}$ where $p_{m+1}$ is a prime which belongs to a set defined by non-empty Chebotarev conditions, thus completing the inductive step.

By Proposition 2.13, there exists $\widetilde{L}_0/L/\mathbb{Q}$ such that $\mathrm{Gal}(\widetilde{L}_0/\mathbb{Q}) \simeq G$ and the only primes which ramify in $\widetilde{L}_0$ are $p_1, \ldots, p_m$. We shall modify $\widetilde{L}_0$ (as in Definition 2.10) to get $\widetilde{L}/L/\mathbb{Q}$ as above. Since $L$ satisfies condition (ii), each of the primes $p_i$ has inertial degree 1 in $L$. Let $c_{p_i} \in \mathbb{Z}/\ell\mathbb{Z}$ be as defined in the proof of Proposition 2.15. Since $L$ satisfies condition (iii), for each prime $w \in \Sigma$, there is an element $c_w \in \mathbb{Z}/\ell\mathbb{Z}$ such that the Frobenius at $w$ maps to $c_w$. Now let $p$ be a prime such that:

(a) $p \in \mathfrak{T}_E \setminus (\Sigma \cup \{p_1, \ldots, p_m\})$,
(b) $p$ splits in $L(\mu_{\ell^N})$,
(c) for each prime $v \in \Sigma \cup \{p_1, \ldots, p_m\}$, $\sigma_v$ maps to $c_v$ in $\mathbb{Z}/\ell\mathbb{Z}$ (via the natural map $\mathrm{G}_{\mathbb{Q}_v} \to G$).

These conditions are determined by non-empty Chebotarev sets. Condition (a) is determined in the field extension $\mathbb{Q}(E[\ell])/\mathbb{Q}(\mu_\ell)$, and (b),(c) are determined in $\mathcal{F}' := L(\mu_{\ell^N}, \sqrt[\ell]{v} \mid v \in \Sigma \cup \{p_1, \ldots, p_m\})$. Let $\mathcal{S}_1 \subset \mathrm{Gal}(\mathcal{F}'/\mathbb{Q}(\mu_\ell))$ be the Chebotarev set which corresponds to conditions (b) and (c), and $\mathcal{S}_2 \subset \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}(\mu_\ell))$ corresponds to condition (a). Note that $\mathcal{F}'$ is an

$\ell$-extension of $\mathbb{Q}(\mu_\ell)$. Lemma 3.8 thus implies that $\mathcal{F}' \cap \mathbb{Q}(E[\ell]) = \mathbb{Q}(\mu_\ell)$. Therefore,

$$\mathrm{Gal}\left(\mathcal{F}/\mathbb{Q}(\mu_\ell)\right) = \mathrm{Gal}\left(\mathcal{F}'/\mathbb{Q}(\mu_\ell)\right) \times \mathrm{Gal}\left(\mathbb{Q}(E[\ell])/\mathbb{Q}(\mu_\ell)\right)$$

and let $\mathcal{S} := \mathcal{S}_1 \times \mathcal{S}_2$. By construction, $\mathcal{S} \subset \mathrm{Gal}(\mathcal{F}/\mathbb{Q})$ is the non-empty Chebotarev set which determines conditions (a)–(c). Thus, by the Chebotarev density theorem, the set of primes satisfying (a)–(c) has positive density. We choose one such prime $p$ and take $p_{m+1} := p$. Let $\chi^{(p)} : \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \to \mathbb{Z}/\ell\mathbb{Z}$ be the associated character and take $\widetilde{L}$ be the twist of $\widetilde{L}_0$ by $(\chi^{(p)})^{-1}$ as in Definition 2.10. This modification satisfies all the required conditions and completes the inductive argument. □

**Theorem 3.10.** *Let $\ell \geq 5$ be a prime and $E$ be an elliptic curve over $\mathbb{Q}$. Assume that $\rho_{E,\ell} : \mathrm{G}_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective and that $\mathrm{Sel}_\ell(E/\mathbb{Q}) = 0$. Let $G$ be an $\ell$-group. Then there are infinitely many $G$-extensions $L/\mathbb{Q}$ for which $\mathrm{Sel}_\ell(E/L) = 0$.*

*Proof.* According to Proposition 3.9, there exist infinitely many Galois extensions $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$ such that:

- if $p_1, \ldots, p_m$ denote the primes that ramify in $L$, then $m \leq n$, each $p_i \in \mathfrak{T}_E \setminus \Sigma$, $p_i \equiv 1 \bmod \ell^N$, and the inertial degree of $p_i$ in $L$ is equal to 1 for all $i = 1, \ldots, m$;
- every prime $q \in \Sigma$ is completely split in $L$.

We fix such an extension $L/\mathbb{Q}$ and filter it by a tower of intermediate fields

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_{n-1} \subset L_n = L,$$

with $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq G/G_i$ and $G_i$ are as in (2.1). By assumption, $\mathrm{Sel}_\ell(E/L_0) = 0$. We prove by induction on $i$ that $\mathrm{Sel}_\ell(E/L_i) = 0$, assuming the vanishing of $\mathrm{Sel}_\ell(E/L_{i-1})$. To do so, it suffices to verify that the extension $L_i/L_{i-1}$ satisfies conditions (i)–(iii) of Proposition 3.4.

Since $\mathrm{Sel}_\ell(E/L_{i-1}) = 0$ by the inductive hypothesis, condition (i) is satisfied. Moreover, because all rational primes in $\Sigma$ split completely in $L$, in particular every prime of $L_{i-1}$ lying above $\Sigma$ splits completely in $L_i$, verifying condition (ii). To verify condition (iii), let $v$ be a prime of $L_{i-1}$ that ramifies in $L_i$. Then $v \mid p_i$ for some $i$, and since the inertial degree of $p_i$ in $L$ is 1, it follows that the residue field $k_v \simeq \mathbb{F}_{p_i}$. For each $p_i \in \mathfrak{T}_E$, we have $\widetilde{E}(\mathbb{F}_{p_i})[\ell] = 0$ by Remark 3.6, so condition (iii) is satisfied. This completes the proof. □

## 4. Density results and connections with Malle's conjecture

In this section, we fix a prime $\ell \geq 5$ and an elliptic curve $E/\mathbb{Q}$ satisfying:

- $\mathrm{Sel}_\ell(E/\mathbb{Q}) = 0$,
- the mod $\ell$ Galois representation $\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective.

Let $G$ be a finite $\ell$-group with $\#G = \ell^n$. We recall that Theorem 3.10 establishes the existence of infinitely many Galois extensions $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$ and $\mathrm{Sel}_\ell(E/L) = 0$. In this section, we go further and obtain asymptotic lower bounds for the number of such extensions $L/\mathbb{Q}$, counted by their absolute discriminant. We then compare these lower bounds with the expected asymptotics for the total number of $G$-extensions of $\mathbb{Q}$, as predicted by the weak form of Malle's conjecture.

4.1. **Counting $\ell$-extensions by discriminant.** Let $G$ be a finite $\ell$-group and $\overline{G}$ be a quotient of $G$ such that there is a central extension:

$$1 \to \mathbb{Z}/\ell\mathbb{Z} \to G \to \overline{G} \to 1. \tag{4.1}$$

Let $L/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) \simeq \overline{G}$ and $\widetilde{L}/L/\mathbb{Q}$ a solution to the above embedding problem. Let $\zeta$ be a primitive $\ell$-th root of unity and let $\sigma$ be a generator of $\mathrm{Gal}(\widetilde{L}(\mu_\ell)/\widetilde{L})$ with $\sigma(\zeta) = \zeta^q$.

**Proposition 4.1.** *With respect to notation above, the following assertions hold.*

*(i) There exists* $\alpha \in L(\mu_\ell)^\times$ *such that* $\widetilde{L}(\mu_\ell) = L(\mu_\ell, \sqrt[\ell]{\alpha})$ *and* $\sigma(\alpha)/\alpha^q \in \big(L(\mu_\ell)^\times\big)^q$.

*(ii) Any other solution* $\widetilde{L}'/L/\mathbb{Q}$ *to the embedding problem is given by* $\widetilde{L}' = \widetilde{L}_b$, *where* $\widetilde{L}_b$ *is the index* $(\ell-1)$ *subfield of* $L(\mu_\ell, \sqrt[\ell]{b\alpha})$ *where* $b \in \mathbb{Q}(\mu_\ell)^\times$ *and satisfies* $\sigma(b)/b^q \in (\mathbb{Q}(\mu_\ell)^\times)^\ell$.

*Proof.* The assertions (i) and (ii) follow from Proposition 3.3 and 3.4 of [KM04] respectively. □

Let $\mathbb{Q}_1$ be the unique $\mathbb{Z}/\ell\mathbb{Z}$-extension of $\mathbb{Q}$ which is contained in $\mathbb{Q}(\mu_{\ell^2})$. Let $b \in \mathbb{Q}(\mu_\ell)^\times$ be such that $\sigma(b)/b^q \in (\mathbb{Q}(\mu_\ell)^\times)^\ell$. Setting $L := \mathbb{Q}$ and $\overline{G} = 1$, we choose $\widetilde{L} := \mathbb{Q}_1$. Then, any other cyclic $\ell$-extension of $\mathbb{Q}$ is obtained by twisting $\mathbb{Q}_1$ by an element $b$. One denotes this twist by $\mathbb{Q}_b$ and thus we have an indexing of all cyclic $\ell$-extensions of $\mathbb{Q}$.

**Proposition 4.2.** *With respect to the notation above, the following assertions hold.*

*(i) The association* $\mathbb{Q}_b \mapsto \widetilde{L}_b$ *between cyclic* $\ell$*-extensions of* $\mathbb{Q}$ *and solutions to the embedding problem for* $L/\mathbb{Q}$ *has finite fibers with cardinality bounded only in terms of* $\overline{G}$ *and* $\ell$.

*(ii) There is a constant* $C > 0$ *such that*

$$C|\Delta_{\widetilde{L}_b}| \leq |\Delta_{\mathbb{Q}_b}|^{\ell^{n-1}}.$$

*Proof.* The result follows from [KM04, Proposition 3.5]. □

Recall from Definition 2.10 that $\widetilde{L}' = \widetilde{L}^f$ where $f \in H^1(\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z})$. Identify $H^1(\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z})$ with $\mathrm{Hom}(\mathrm{G}_\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z})$. By Kummer theory, there's an isomorphism

$$\mathrm{Hom}(\mathrm{G}_\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z}) \simeq \{b \in \mathbb{Q}(\mu_\ell)^\times/(\mathbb{Q}(\mu_\ell)^\times)^\ell : \sigma(b)/b^q \in (\mathbb{Q}(\mu_\ell)^\times)^\ell\}.$$

Let $f_b$ be the homomorphism corresponding to $b$. We have that $\widetilde{L}^{f_b} = \widetilde{L}_b$.

4.2. **An application of Wiles' formula.** Recall that $E_{/\mathbb{Q}}$ is an elliptic curve such that $\mathrm{Sel}_\ell(E/\mathbb{Q}) = 0$ and $\rho_{E,\ell}$ is surjective. It follows from Proposition 3.9 that there exists $\widetilde{L}/L/\mathbb{Q}$ solving the embedding problem (4.1) such that

(i) if $p_1, \ldots, p_m$ are all the primes that are ramified in $\widetilde{L}$, then $m \leq n$, $p_1, \ldots, p_m \in \mathfrak{T}_E \setminus \Sigma$, $p_i \equiv 1 \pmod{\ell^N}$ and the inertial degree of $p_i$ in $L$ is 1 for $i = 1, \ldots, m$,

(ii) all primes $q \in \Sigma$ are completely split in $\widetilde{L}$.

Let $S$ be a finite set of primes in $\mathfrak{T}_{E,L}$ disjoint from $\Sigma \cup \{p_1, \ldots, p_m\}$. Let $V_S$ be the space of cohomology classes $f \in H^1(\mathbb{Q}_S/\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z})$ such that $\mathrm{res}_q(f) = 0$ for all primes $q \in \Sigma \cup \{p_1, \ldots, p_m\}$. Setting $\widetilde{S} := S \cup \Sigma \cup \{p_1, \ldots, p_m\}$, the space $V_S = H^1_\mathcal{L}(\mathbb{Q}_{\widetilde{S}}/\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z})$ is determined by Selmer conditions $\{\mathcal{L}_q\}_{q \in \widetilde{S}}$ defined as follows:

$$\mathcal{L}_q := \begin{cases} H^1(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z}) & \text{if } q \in S \\ 0 & \text{if } q \in \Sigma \cup \{p_1, \ldots, p_m\}. \end{cases}$$

Let $\overline{\chi}$ be the mod $\ell$ cyclotomic character. The dual Selmer group $V_S^\perp := H^1_{\mathcal{L}^\perp}(\mathbb{Q}_{\widetilde{S}}/\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z}(\overline{\chi}))$ is given by:

$$V_S^\perp = \ker\{H^1(\mathbb{Q}_{\widetilde{S}}/\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z}(\overline{\chi})) \longrightarrow \bigoplus_{q \in S} H^1(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z}(\overline{\chi}))\}.$$

Given a prime $q \equiv 1 \mod \ell$, it follows from local class field theory that

$$\dim H^1(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z}) = 2.$$

Wiles' formula (2.6) yields

$$\begin{aligned}\dim V_S \geq & 1+\sum_{q\in S}\Big(\dim H^1(\mathbb{Q}_q,\mathbb{Z}/\ell\mathbb{Z})-\dim H^0(\mathbb{Q}_q,\mathbb{Z}/\ell\mathbb{Z})\Big)\\ & -\sum_{q\in\Sigma\cup\{p_1,\ldots,p_m\}\cup\{\infty\}}\dim H^0(\mathbb{Q}_q,\mathbb{Z}/\ell\mathbb{Z})\\ =&\#S-\#\Sigma-m.\end{aligned}$$

**Lemma 4.3.** *Let $S$ be a finite set of primes in $\mathfrak{T}_{E,L}$ disjoint from $\Sigma\cup\{p_1,\ldots,p_m\}$ and $f\in V_S$. Then, the following assertions hold:*

*(i)* $\mathrm{Sel}_\ell(E/\widetilde{L}^f)=0$,

*(ii)* $|\Delta_{\widetilde{L}^f}|\leq c_2\left(\prod_{q\in S}q\right)^{\ell^{n-1}(\ell-1)}$, *for an absolute constant* $c_2>0$.

*Proof.* Let $q_1,\ldots,q_r$ be the rational primes which are ramified in $\widetilde{L}^f$. Then by construction, $q_1,\ldots,q_r$ are primes in $S\cup\{p_1,\ldots,p_m\}$. Since $\mathrm{res}_q(f)=0$ at all primes of $q\in\Sigma$, it follows that all primes of $\Sigma$ are completely split in $\widetilde{L}^f$. On the other hand, let $v$ be a prime of $L$ which ramifies in $\widetilde{L}^f$ and $q$ be the rational prime such that $v|q$. If $q=p_i$, then $k_v=\mathbb{F}_{p_i}$. If $q\in S$, then $q$ splits in $L$ and we have that $k_v=\mathbb{F}_q$. Thus, $\widetilde{E}(k_v)[\ell]=\widetilde{E}(\mathbb{F}_q)[\ell]=0$. It then follows from Proposition 3.4 that

$$\mathrm{Sel}_\ell(E/L)=0\Rightarrow\mathrm{Sel}_\ell(E/\widetilde{L}^f)=0.$$

This proves part (i).

Let $\mathbb{Q}_f$ be the cyclic $\ell$-extension of $\mathbb{Q}$ which is cut out by $f$ and set $\Delta_f:=\Delta_{\mathbb{Q}_f}$. We have that $|\Delta_f|\leq(\prod_{q\in S}q)^{\ell-1}$ and part (ii) follows from Proposition 4.2. □

**Lemma 4.4.** *There is a finite set of primes $S_0$ contained in $\mathfrak{T}_{E,L}$ such that $V_{S_0}^{\perp}=0$.*

*Proof.* Let $\psi_1,\ldots,\psi_r$ be the non-zero elements in $H^1(\mathbb{Q}_{\Sigma\cup\{p_1,\ldots,p_m\}}/\mathbb{Q},\mathbb{Z}/\ell\mathbb{Z}(\overline{\chi}))$. Let $\psi\in\{\psi_1,\ldots,\psi_r\}$ and $\Omega:=\mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$. Note that the inflation–restriction sequence gives:

$$0\to H^1\left(\Omega,\mathbb{Z}/\ell\mathbb{Z}(\overline{\chi})\right)\to H^1(\mathbb{Q}_{\Sigma\cup\{p_1,\ldots,p_m\}}/\mathbb{Q},\mathbb{Z}/\ell\mathbb{Z}(\overline{\chi}))\xrightarrow{\mathrm{res}}\mathrm{Hom}(\mathbb{Q}_{\Sigma\cup\{p_1,\ldots,p_m\}}/\mathbb{Q}(\mu_\ell),\mathbb{Z}/\ell\mathbb{Z}(\overline{\chi}))^{\Omega}.$$

Since $\#\Omega$ is coprime to $\ell$, $H^1\left(\Omega,\mathbb{Z}/\ell\mathbb{Z}(\overline{\chi})\right)=0$ and thus the restriction map is an injection. Thus the homomorphism $\mathrm{res}(\psi)$ is non-zero. It gives rise to a $\mathbb{Z}/\ell\mathbb{Z}$ extension $L_\psi$ over $\mathbb{Q}(\mu_\ell)$, which is a Galois extension of $\mathbb{Q}$ with

$$\mathrm{Gal}(L_\psi/\mathbb{Q})\simeq\Omega\ltimes\mathrm{Gal}(L_\psi/\mathbb{Q}(\mu_\ell)).\tag{4.2}$$

Here, the action of $\Omega$ on $\mathrm{Gal}(L_\psi/\mathbb{Q}(\mu_\ell))\simeq\mathbb{Z}/\ell\mathbb{Z}$ is via the character $\overline{\chi}$.

There are two possibilities for the intersection $L_\psi\cap L(\mu_\ell)$, namely either $L_\psi\cap L(\mu_\ell)=L_\psi$ or $L_\psi\cap L(\mu_\ell)=\mathbb{Q}(\mu_\ell)$. Recall that $\Omega$ acts non-trivially on $\mathrm{Gal}(L_\psi/\mathbb{Q}(\mu_\ell))$. On the other hand, $\mathrm{Gal}(L(\mu_\ell)/\mathbb{Q})\simeq\Omega\times\mathrm{Gal}(L/\mathbb{Q})$. Therefore, if $L_\psi\subset L(\mu_\ell)$, then the action of $\Omega$ on $\mathrm{Gal}(L_\psi/\mathbb{Q}(\mu_\ell))$ would be trivial, which contradicts (4.2). Thus we have that $L_\psi\cap L(\mu_\ell)=\mathbb{Q}(\mu_\ell)$. Lemma 3.8 implies that $L_\psi\cap\mathbb{Q}(E[\ell])=\mathbb{Q}(\mu_\ell)$. The Chebotarev conditions determining $\mathfrak{T}_{E,L}$ are thus independent of the extension $L_\psi/\mathbb{Q}(\mu_\ell)$. There is thus a nonempty Chebotarev set contained in $\mathrm{Gal}(L_\psi\cdot L(E[\ell])/\mathbb{Q})$ determining a positive density set of primes $q\in\mathfrak{T}_{E,L}$ which are non-split in the extension $L_\psi/\mathbb{Q}(\mu_\ell)$. Pick one such prime $q_i$ for each $\psi_i$ for $i=1,\ldots,r$. Then setting $S_0:=\{q_1,\ldots,q_r\}$, we have that:

$$V_{S_0}^{\perp}=\ker\{H^1(\mathbb{Q}_{S_0\cup\Sigma\cup\{p_1,\ldots,p_m\}}/\mathbb{Q},\mathbb{Z}/\ell\mathbb{Z}(\overline{\chi}))\longrightarrow\bigoplus_{q\in S_0}H^1(\mathbb{Q}_q,\mathbb{Z}/\ell\mathbb{Z}(\overline{\chi}))\}.$$

For each $\psi_i$, $\mathrm{res}_{q_i}(\psi_i)\neq0$ and hence $\psi_i\notin V_{S_0}^{\perp}$. This implies that $V_{S_0}^{\perp}=0$, thus proving the result. □

**Definition 4.5.** *For the rest of this article, we fix a choice of $S_0$ as in Lemma 4.4 and set $Z := S_0 \cup \Sigma \cup \{p_1, \dots, p_m\}$.*

Let $T \subset \mathfrak{T}_{E,L} \setminus Z$ be a finite set of primes. Let $W_T$ be the subset of $V_{S_0 \cup T}$ consisting of $f$ which are ramified at each of the primes in $T$. We have a natural exact sequence:

$$0 \to V_{S_0} \xrightarrow{\iota} V_{S_0 \cup T} \xrightarrow{\pi} \bigoplus_{q \in T} \frac{H^1(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z})}{H^1_{\mathrm{nr}}(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z})}. \tag{4.3}$$

**Lemma 4.6.** *The following assertions hold:*

*(i) The sequence (4.3) above is a short exact sequence, i.e., $\pi$ is surjective;*
*(ii) $\#W_T = (\ell-1)^{\#T} \# V_{S_0}$.*

*Proof.* For the proof of part (i) it suffices to show that

$$\dim V_{S_0 \cup T} = \dim V_{S_0} + \sum_{q \in T} \dim \left( \frac{H^1(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z})}{H^1_{\mathrm{nr}}(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z})} \right).$$

There is a unique unramified $\mathbb{Z}/\ell\mathbb{Z}$-extension of $\mathbb{Q}_q$, and thus, $\dim H^1_{\mathrm{nr}}(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z}) = 1$. Since $q \equiv 1 \pmod{\ell}$ for all primes $q \in \mathfrak{T}_{E,L}$, a simple application of local class field theory shows that $\dim H^1(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z}) = 2$. It thus follows that

$$\dim \left( \frac{H^1(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z})}{H^1_{\mathrm{nr}}(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z})} \right) = 1.$$

By the choice of $S_0$ in Lemma 4.4 one has that $V_{S_0}^{\perp} = 0$ and consequently, $V_{S_0 \cup T}^{\perp} = 0$ as well. Thus by Wiles' formula,

$$\dim V_{S_0 \cup T} = \dim V_{S_0} + \sum_{q \in T} (\dim H^1(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z}) - \dim H^0(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z})) = \dim V_{S_0} + \#T$$

and part (i) follows.

Part (ii) can be derived from part (i) by noting that $W_T = \pi^{-1}(\mathcal{W})$, where

$$\mathcal{W} \subset \bigoplus_{q \in T} \frac{H^1(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z})}{H^1_{\mathrm{nr}}(\mathbb{Q}_q, \mathbb{Z}/\ell\mathbb{Z})}$$

consists of elements $(h_q)_{q \in T}$ such that $h_q \neq 0$ for all $q \in T$. We find that

$$\#W_T = \#V_{S_0} \times \#\mathcal{W} = \#V_{S_0} (\ell-1)^{\#T}.$$

□

As $T$ ranges over finite subsets of $\mathfrak{T}_{E,L} \setminus Z$, the sets $W_T$ are mutually disjoint. To see this in detail, let $T$ and $T'$ be distinct finite subsets of $\mathfrak{T}_{E,L} \setminus Z$. Without loss of generality, suppose that $T \not\subset T'$. Then there exists a prime $q \in T \setminus T'$. By construction, every element of $W_T$ is ramified at $q$, whereas every element of $W_{T'}$ is unramified at $q$. It follows that $W_T \cap W_{T'} = \emptyset$. Let $W$ denote the disjoint union $W = \bigsqcup_T W_T$ as $T$ ranges over finite subsets of $\mathfrak{T}_{E,L} \setminus Z$.

*Proof of Theorem 1.1.* Let $\widetilde{L}/L/\mathbb{Q}$ be defined as in the start of Section 4.2 and $Z$ be the finite set of primes defined above (see Definition 4.5). Set

$$g(s) := \sum_T (\ell-1)^{\#T} \left( \prod_{q \in T} q \right)^{-s} = \prod_{q \in \mathfrak{T}_{E,L} \setminus Z} \left( 1 + (\ell-1) q^{-s} \right),$$

where $T$ ranges over finite subsets of $\mathfrak{T}_{E,L} \setminus Z$. Write $g(s) = \sum_{n \geq 1} a_n n^{-s}$ where $a_n := (\ell-1)^r$ if $n$ is a product of $r$ distinct primes in $\mathfrak{T}_{E,L} \setminus Z$, and $a_n := 0$ otherwise.

Arguing as in [Ser75, Theorem 2.4, p.5], we find that

$$\log g(s) = (\ell-1)\sum_{q\in\mathfrak{T}_{E,L}} \frac{1}{q^{-s}} + \theta_1(s)$$

where $\theta_1$ is holomorphic on $\operatorname{Re} s \geq 1$. Moreover,

$$\log g(s) = (\ell-1)\alpha \log\left(\frac{1}{s-1}\right) + \theta_2(s),$$

where $\alpha := \mathfrak{d}(\mathfrak{T}_{E,L})$. It follows from Lemma 3.7 that

$$(\ell-1)\alpha = \delta = \frac{\ell^2-\ell-1}{\ell^{n-1}(\ell^2-1)}.$$

Thus, we find that

$$g(s) = (s-1)^{-\delta}\, h(s),$$

where $h(s)$ is a non-zero holomorphic function in $\operatorname{Re}(s) \geq 1$. By Delange's Tauberian theorem (cf. [Ten15, Theorem 7.28]),

$$\sum_{n\leq X} a_n \gg X(\log X)^{\delta-1}. \tag{4.4}$$

By Lemma 4.3, $\operatorname{Sel}_\ell(E/\widetilde{L}^f) = 0$ for all $f \in W$ and thus,

$$\mathcal{M}(G,E,X) \geq \#\{f \in W \mid |\Delta_{\widetilde{L}^f}| \leq X\}. \tag{4.5}$$

According to Lemma 4.3, we have that $|\Delta_{\widetilde{L}^f}| \leq c_2 \left(\prod_{q\in S_0\cup T} q\right)^{\ell^{n-1}(\ell-1)}$, for an absolute constant $c_2 > 0$. Thus, from (4.5), we deduce that

$$\mathcal{M}(G,E,X) \geq \#\left\{ f \in W : \prod_{q\in T} q \leq c_3 X^{\frac{1}{\ell^{n-1}(\ell-1)}} \right\}, \tag{4.6}$$

where $c_3 > 0$ is an explicit constant given by

$$c_3 := \left( c_2^{\frac{1}{\ell^{n-1}(\ell-1)}} \prod_{q\in S_0} q \right)^{-1}.$$

Note that

$$\#\left\{ f \in W : \prod_{q\in T} q \leq c_3 X^{\frac{1}{\ell^{n-1}(\ell-1)}} \right\} = \sum_{n\leq c_3 X^{\frac{1}{\ell^{n-1}(\ell-1)}}} a_n \tag{4.7}$$

and thus from (4.4) and (4.6), we deduce that

$$\mathcal{M}(G,E,X) \gg X^{\frac{1}{(\ell-1)\ell^{n-1}}} (\log X)^{\delta-1}.$$

□

## References


[BKR24] Lea Beneish, Debanjana Kundu, and Anwesh Ray. Rank jumps and growth of Shafarevich-Tate groups for elliptic curves in $\mathbb{Z}/p\mathbb{Z}$-extensions. *J. Aust. Math. Soc.*, 116(1):1–38, 2024.

[BRY24] Jennifer Berg, Nathan C. Ryan, and Matthew P. Young. Vanishing of quartic and sextic twists of $L$-functions. *Res. Number Theory*, 10(1):Paper No. 20, 25, 2024.

[BS13] Manjul Bhargava and Arul Shankar. The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1. *arXiv preprint arXiv:1312.7859*, 2013.

[CS10] J. Coates and R. Sujatha. *Galois cohomology of elliptic curves*. Published by Narosa Publishing House, New Delhi; for the Tata Institute of Fundamental Research, Mumbai, second edition, 2010.

[Duk97] William Duke. Elliptic curves with no exceptional primes. *C. R. Acad. Sci. Paris Sér. I Math.*, 325(8):813–818, 1997.

[Gal46] Évariste Galois. OEmathematic works. *Journal of Pure and Applied Mathematics*, 11:381–444, 1846.

[Kel24] Daniel Keliher. Rank growth of elliptic curves in $S_4$- and $A_4$-quartic extensions of the rationals. *Pacific J. Math.*, 331(2):331–352, 2024.

[KM04] Jürgen Klüners and Gunter Malle. Counting nilpotent Galois extensions. *J. Reine Angew. Math.*, 572:1–26, 2004.

[KMR14] Zev Klagsbrun, Barry Mazur, and Karl Rubin. A Markov model for Selmer ranks in families of twists. *Compos. Math.*, 150(7):1077–1106, 2014.

[KP23] Peter Koymans and Carlo Pagano. On malle's conjecture for nilpotent groups. *Transactions of the American Mathematical Society, Series B*, 10(11):310–354, 2023.

[KP25] Daniel Keliher and Sun Woo Park. Rank growth of elliptic curves over s3 extensions with fixed quadratic resolvents. *arXiv preprint arXiv:2502.05705*, 2025.

[LOT21] Robert J. Lemke Oliver and Frank Thorne. Rank growth of elliptic curves in non-abelian extensions. *Int. Math. Res. Not. IMRN*, 2021(24):18411–18441, 2021.

[Mäk85] Sirpa Mäki. *On the density of abelian number fields*, volume 54. Suomalainen tiedeakatemia, 1985.

[Mal02] Gunter Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002.

[Mal04] Gunter Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004.

[Mas06] Adam Massey. The inverse Galois problem for nilpotent groups of odd order. *course notes available at http://www. math. ucla. edu/ amassey3102/Thesis*, 2, 2006.

[MR10] B. Mazur and K. Rubin. Ranks of twists of elliptic curves and Hilbert's tenth problem. *Invent. Math.*, 181(3):541–575, 2010.

[MRL18] Barry Mazur, Karl Rubin, and Michael Larsen. Diophantine stability. *American Journal of Mathematics*, 140(3):571–616, 2018.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren Math. Wiss.* Berlin: Springer, 2nd ed. edition, 2008.

[PR25] Siddhi Pathak and Anwesh Ray. Rank stability of elliptic curves in certain non-abelian extensions. *Mathematische Nachrichten*, 298(2):730–753, 2025.

[Ram02] Ravi Ramakrishna. Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur. *Ann. Math. (2)*, 156(1):115–154, 2002.

[Rei37] Hans Reichardt. Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung. *J. Reine Angew. Math.*, 177:1–5, 1937.

[Saf54] I. R. Safarevic. Construction of fields of algebraic numbers with given solvable Galois group. *Izv. Akad. Nauk SSSR Ser. Mat.*, 18:525–578, 1954.

[Sch37] Arnold Scholz. Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung. I. *Math. Z.*, 42:161–188, 1937.

[Ser75] Jean-Pierre Serre. Divisibilité de certaines fonctions arithmétiques. In *Séminaire Delange-Pisot-Poitou (16e année: 1974/75), Théorie des nombres, Fasc. 1*, pages Exp. No. 20, 28. Secrétariat Math., Paris, 1975.

[Smi22] Alexander D. Smith. The distribution of $\ell^\infty$-Selmer groups in degree $\ell$ twist families II. Preprint, arXiv:2207.05143 (2022), 2022.

[Smi26] Alexander Smith. The distribution of $\ell^\infty$-Selmer groups in degree $\ell$ twist families I. *J. Amer. Math. Soc.*, 39(1):1–72, 2026.

[SW23] Ari Shnidman and Ariel Weiss. Rank growth of elliptic curves over $n$-th root extensions. *Trans. Amer. Math. Soc. Ser. B*, 10:482–506, 2023.

[Tay03] Richard Taylor. On icosahedral Artin representations. II. *Amer. J. Math.*, 125(3):549–566, 2003.

[Ten15] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion.

[Š54] I. R. Šafarevič. Construction of fields of algebraic numbers with given solvable Galois group. *Izv. Akad. Nauk SSSR Ser. Mat.*, 18:525–578, 1954.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Camb. Stud. Adv. Math.* Cambridge: Cambridge University Press, 1994.

[Wri89] David J Wright. Distribution of discriminants of abelian extensions. *Proceedings of the London Mathematical Society*, 3(1):17–50, 1989.

(Pathak) Chennai Mathematical Institute, H1, SIPCOT IT Park, Kelambakkam, Siruseri, Tamil Nadu 603103, India
*Email address*: siddhi@cmi.ac.in

(Ray) Chennai Mathematical Institute, H1, SIPCOT IT Park, Kelambakkam, Siruseri, Tamil Nadu 603103, India
*Email address*: anwesh@cmi.ac.in