TAMELY RAMIFIED COVERS OF THE PROJECTIVE LINE WITH ALTERNATING AND SYMMETRIC MONODROMY

RENEE BELL, JEREMY BOOHER, WILLIAM Y. CHEN, AND YUAN LIU

Abstract. Let k be an algebraically closed field of characteristic p and X the projective line over k with three points removed. We investigate which finite groups G can arise as the monodromy group of finite étale covers of X that are tamely ramified over the three removed points. This provides new information about the tame fundamental group of the projective line. In particular, we show that for each prime $p \geq 5$, there are families of tamely ramified covers with monodromy the symmetric group S_n or alternating group A_n for infinitely many n. These covers come from the moduli spaces of elliptic curves with $\mathrm{PSL}_2(\mathbb{F}_\ell)$-structure, and the analysis uses work of Bourgain, Gamburd, and Sarnak, and adapts work of Meiri and Puder about Markoff triples modulo ℓ.

Contents

1. Introduction

1.1. **Three-Point Covers.** Let k be an algebraically closed field and X an algebraic curve over k. If $k = \mathbb{C}$, it follows from the Riemann existence theorem that the étale fundamental group of X, which we denote as $\pi_1(X)$, is the profinite completion of the topological fundamental group of the corresponding Riemann surface. In this case, the étale fundamental group is closely linked to topology. This connection is weaker in characteristic p, even for simple examples like $X = \mathbb{A}^1_{\overline{\mathbb{F}}_p}$; Artin–Schreier theory implies that $\pi_1(\mathbb{A}^1_{\overline{\mathbb{F}}_p})$ is topologically infinitely generated, whereas the topological fundamental group of $(\mathbb{A}^1_{\mathbb{C}})^{\mathrm{an}}$ is trivial. These Artin–Schreier covers of the affine line have no analog in characteristic zero, and in general covers of degree divisible by p are responsible for much of the additional complexity that arises in characteristic p.

More precisely, suppose X is a smooth affine curve over an algebraically closed field k of characteristic p obtained from a smooth projective connected curve $\overline{X}$ of genus g by removing r points. If $\widetilde{X}$ is a smooth lift of X to an algebraically closed field of characteristic 0, then by the theory of specialization of the fundamental group, the maximal prime-to-p quotients of the étale fundamental groups are isomorphic, i.e. $\pi_1(X)^{(p')} \cong \pi_1(\widetilde{X})^{(p')}$ [Gro71, X, Cor 3.9]. This philosophy is extended in a conjecture of Abhyankar (now a theorem of Harbater and Raynaud) which states that a finite

Date: December 1, 2022.

group G is a quotient of $\pi_1(X)$ if and only if its maximal prime-to-p quotient is a quotient of $\pi_1(\widetilde{X})$ [Abh57, Har94, Ray94]. Since the fundamental group of the Riemann surface $\widetilde{X}(\mathbb{C})$ is free of rank $2g+r-1$, it follows that a finite group G arises as the Galois group of a connected étale cover of X if and only if the maximal prime-to-p quotient of G is generated by $2g+r-1$ elements.

While Abhyankar's conjecture specifies the finite quotients of $\pi_1(X)$, this is not enough to determine $\pi_1(X)$ as it is not topologically finitely generated. Furthermore, these results say nothing about the structure of the inertia groups of the covers under consideration. By Grothendieck's theory of specialization [Gro71, XIII, Cor 2.12], if $f : Y \to X$ is a G-Galois cover where G is a quotient of $\pi_1(X)$ but not a quotient of $\pi_1(\widetilde{X})$, then f is necessarily wildly ramified when extended to a branched cover of $\overline{X}$. Hence it is natural to study the difference between $\pi_1(\widetilde{X})$ and the tame fundamental group $\pi_1^t(X)$ which classifies étale covers of X that are tamely ramified when extended to a branched cover of $\overline{X}$. So we are led to the following question:

Question. Which finite quotients of $\pi_1(\widetilde{X})$ are quotients of $\pi_1^t(X)$? Equivalently, which finite groups generated by $2g+r-1$ elements arise as Galois groups of connected tamely ramified covers of X?

For examples of groups G which are a finite quotient of $\pi_1(\widetilde{X})$ but not of $\pi_1^t(X)$, see [Kan86, p. 204] and [Ste98, Proposition 4.3]. Since $\pi_1^t(X)$ is topologically finitely generated, a complete answer to this question would in some sense determine $\pi_1^t(X)$ (see [RZ10, Theorem 3.2.9]). We are not aware of even a conjectural general answer, so we are interested in techniques for producing tamely ramified covers.

In this paper we will introduce a new technique for producing tamely ramified covers of $\mathbb{P}^1_{\overline{\mathbb{F}}_p} - \{0,1,\infty\}$ using moduli spaces of elliptic curves with G-structures. More precisely, by a three-point cover (in characteristic p) we mean a finite flat map of smooth curves $Y \to \mathbb{P}^1_{\overline{\mathbb{F}}_p}$ which is unramified away from $\{0,1,\infty\}$. A three-point cover is *tame* if the ramification indices above $0,1,\infty$ are prime to p. One consequence of our methods is the following.

Theorem A (see Theorem B below). *For any prime $p \geq 5$, there are infinitely many n for which there exists a tame three-point cover defined over $\mathbb{F}_p$ which is Galois with Galois group isomorphic to S_n. The same is true for A_n, except we only show that the cover is defined over $\mathbb{F}_{p^2}$.*

This is a consequence of Theorem B below, which together with Theorem C gives more precise information about which n occur. Note that by Abhyankar's conjecture, every symmetric and alternating group is the Galois group of a three-point cover. The main point of our result is that our covers are *tame*, even though in all but finitely many cases p *divides* the order of the Galois group.

To date, the main tool for understanding good reduction of three-point covers is the following criterion of Obus–Raynaud, which comes from a detailed analysis of the stable reduction of three-point covers in characteristic 0:

Theorem (Obus, Raynaud [Obu17, Ray99]). *Let G be a finite group with cyclic p-Sylow subgroup. Let $K_0 := Frac(W(k))$, where k is an algebraically closed field of characteristic p. Let K/K_0 be a finite extension of degree $e(K)$, where $e(K)$ is less than the number of conjugacy classes of order p in G. If $f : Y \to \mathbb{P}^1_K$ is a three-point G-Galois cover defined over K (as a G-Galois cover), then f has potentially good reduction, realized over a tame extension L/K of degree dividing the exponent of the center $Z(G)$ of G. In particular, if $Z(G)$ is trivial, then f has good reduction.*

In particular, one may attempt to use group theory to construct a three-point cover in characteristic zero with Galois group G and with ramification indices coprime to p, reduce the cover modulo p, and then apply the theorem to deduce the reduction modulo p is the desired cover. For an example with $G = \mathrm{GL}_m(\mathbb{F}_q)$ for appropriately chosen m and q, see [Obu17, §6]. Note that the theorem does not apply to almost all the groups in Theorem A. For example, it does not apply to the symmetric group $G = S_n$ if $n \geq 2p$, since in that case the p-Sylow subgroup of S_n is not cyclic.

Our technique takes the opposite perspective to that of Obus–Raynaud. Instead of constructing covers in characteristic 0 and showing that they have good reduction, we consider covers which arise as maps between moduli spaces defined integrally which are automatically smooth and tamely ramified by virtue of the moduli problem we consider. Then working over the generic fiber, we study the monodromy for these maps of moduli spaces to determine exactly which groups we've managed to realize as quotients of $\pi_1^t(\mathbb{P}^1_{\overline{\mathbb{F}}_p} - \{0, 1, \infty\})$. For this latter part, which in general is a difficult combinatorial problem[1], we crucially rely on input from the work of Meiri–Puder [MP18] and Bourgain–Gamburd–Sarnak [BGS16a, BGS16b].

More precisely, for a prime $\ell \geq 5$, let $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$ denote the moduli stack of elliptic curves equipped with a $\mathrm{PSL}_2(\mathbb{F}_\ell)$-Galois cover defined étale locally on the base (to be made more precise in §2). Let $\mathcal{M}(1)$ denote the moduli stack of elliptic curves. Its coarse moduli scheme $M(1)$ is isomorphic to the affine line $\operatorname{Spec} \mathbb{Z}[j]$ with parameter given by the j-invariant. The forgetful map $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}} \to \mathcal{M}(1)$ is finite étale over $\mathbb{Z}[1/|\,\mathrm{PSL}_2(\mathbb{F}_\ell)|]$ and induces a map of coarse moduli schemes $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}} \to M(1)$. For $p \nmid |\,\mathrm{PSL}_2(\mathbb{F}_\ell)|$, its base change to $\overline{\mathbb{F}}_p$ gives a smooth cover of $\mathbb{P}^1_{\overline{\mathbb{F}}_p}$, *tamely ramified* above $j = 0, 1728, \infty$.

The scheme $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{\overline{\mathbb{Q}}}$ is never geometrically connected, but experimentally[2] every connected component we've computed has alternating or symmetric monodromy over $M(1)$. We cannot prove this in general, but by adapting the work of [MP18], we are able to establish this for a particular component. Specifically, we consider the open and closed substack

$$\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2} \subset \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$$

corresponding to $\mathrm{PSL}_2(\mathbb{F}_\ell)$-covers with "trace invariant -2" (see §2.5). The degree of the induced map on coarse schemes is

$$n_\ell := \begin{cases} \frac{\ell(\ell+3)}{4} & \ell \equiv 1 \mod 4 \\ \frac{\ell(\ell-3)}{4} & \ell \equiv 3 \mod 4. \end{cases}$$

In §3 we explain how any geometric fiber $\overline{F(\ell)}_{-2}$ of $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ over $\mathcal{M}(1)$ can be identified with the set $Y^*(\ell)$ of equivalence classes of non-zero $\mathbb{F}_\ell$-points of the affine surface $\mathbb{X}$ defined by the Markoff equation

$$x^2 + y^2 + z^2 - xyz = 0;$$

two points are equivalent if one is obtained by negating two of the coordinates of the other. (The $\mathbb{F}_\ell$ points of $\mathbb{X}$ also have a moduli interpretation as a fiber of $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$.) Under this identification, the monodromy action of $\pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}})$ on the fiber $\overline{F(\ell)}_{-2}$ translates into the action of a certain group of automorphisms of $\mathbb{X}$. This action was studied by Bourgain–Gamburd–Sarnak, who showed that for primes ℓ not in a density 0 "exceptional" set $\mathcal{E}$, this action is transitive [BGS16a, BGS16b]. In particular, for any $\epsilon > 0$, the number of primes $\ell \leq T$ with $\ell \in \mathcal{E}$ is at most T^ϵ for T large

[1] This is related to the question of Nielsen equivalence generating pairs in combinatorial group theory [Pak01, §2].

[2] We've checked by computer that every component of $M(\mathrm{PSL}_2(\mathbb{F}_q))^{\mathrm{abs}}_{\overline{\mathbb{Q}}}$ has alternating or symmetric monodromy over $M(1)_{\overline{\mathbb{Q}}}$ for every prime power $q \leq 43$.

enough. They furthermore conjecture that this transitivity holds for all ℓ. By Galois theory, this transitivity is the same as the connectedness of $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$.

We can understand the geometric monodromy of the map of coarse spaces $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2} \to M(1)$ using work of Meiri and Puder [MP18]. Let

$$\mathbf{P}(\ell) := \begin{array}{c}\text{The property that either } \ell \equiv 1 \mod 4, \text{ or} \\ \text{the order of } \frac{3+\sqrt{5}}{2} \in \mathbb{F}_{\ell^2} \text{ is at least } 32\sqrt{\ell+1}.\end{array} \tag{1-1-1}$$

In the Appendix to [MP18], it is proven that $\mathbf{P}(\ell)$ holds for a density 1 set of primes ℓ. For a prime $\ell \notin \mathcal{E}$ for which $\mathbf{P}(\ell)$ holds, the work of Meiri and Puder shows that the geometric monodromy group will contain the alternating group on the fiber.

We use these results to obtain the following asymptotic statement:

Theorem B (see Theorem 3.5.1)**.** *For primes $\ell \geq 5$ outside of the exceptional set $\mathcal{E}$, $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ is smooth and geometrically connected. If furthermore $\boldsymbol{P}(\ell)$ holds, the geometric monodromy group over $M(1)$ satisfies*

$$\mathrm{Mon}(M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}/M(1)) \cong \begin{cases} S_{n_\ell} & \ell \equiv 5,7,9,11 \mod 16 \\ A_{n_\ell} & \ell \equiv 1,3,13,15 \mod 16. \end{cases}$$

When $\ell \equiv 5,7,9,11 \mod 16$, the fiber at any prime $p \nmid |\mathrm{PSL}_2(\mathbb{F}_\ell)| = \frac{\ell(\ell^2-1)}{2}$ is a tamely ramified three-point cover with monodromy group S_{n_ℓ} defined over $\mathbb{F}_p$. When $\ell \equiv 1,3,13,15 \mod 16$, the fiber at any prime $p \nmid |\mathrm{PSL}_2(\mathbb{F}_\ell)|$ is a tamely ramified three-point cover with monodromy group A_{n_ℓ} defined over $\mathbb{F}_{p^2}$.

For a fixed prime $p \geq 5$, the set of ℓ for which the Theorem yields tame three-point covers in characteristic p is the set of primes ℓ such that $\frac{\ell(\ell^2-1)}{2} \not\equiv 0 \mod p$ (density > 0), $\ell \notin \mathcal{E}$ (density 1), and $\mathbf{P}(\ell)$ holds (density 1). Thus, there is a positive density set of primes ℓ for which Theorem B yields the desired tame three-point cover mod p, from which we deduce Theorem A.

We also prove a less precise result for sufficiently large ℓ which removes the restriction that $\ell \notin \mathcal{E}$. Specifically, let $M(\ell)$ denote the modular curve classifying elliptic curves with "full level ℓ structure of determinant 1" (see §3.4 below). Let $\Gamma(1)'$ be the commutator subgroup of $\mathrm{SL}_2(\mathbb{Z})$. It can be checked that it is a torsion-free congruence subgroup of level 6 and index 12, and that the corresponding stack $\mathcal{M}'$ over $\mathcal{M}(1)$ is the complement of the zero section of an elliptic curve over $\mathbb{Z}[1/6]$. The pullback

$$\pi_\ell : M(\ell)' := M(\ell) \times_{\mathcal{M}(1)} \mathcal{M}' \longrightarrow \mathcal{M}' \tag{1-1-2}$$

is thus a $\mathrm{SL}_2(\mathbb{F}_\ell)$-cover of a punctured elliptic curve and has good reduction at all $p \nmid 6\ell$. Taking the quotient by the center, we obtain a $\mathrm{PSL}_2(\mathbb{F}_\ell)$-cover

$$\overline{\pi_\ell} : M(\ell)'/\{\pm I\} \longrightarrow \mathcal{M}' \tag{1-1-3}$$

with good reduction at all $p \nmid 6\ell$. This cover defines a $\mathbb{Q}$-point of $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$, and we let $\mathcal{M}(\overline{\pi_\ell})$ denote the connected component containing $\overline{\pi_\ell}$. Let $M(\overline{\pi_\ell})$ be its coarse moduli space. One can compute that the covering $\overline{\pi_\ell}$ also has trace invariant -2, and hence $\mathcal{M}(\overline{\pi_\ell})$ is a component of $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$. The conjecture of Bourgain, Gamburd, and Sarnak (see Conjecture 3.1.2) would imply that $\mathcal{M}(\overline{\pi_\ell}) = \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ (see Proposition 3.2.5).

Let $d_\ell := \deg(M(\overline{\pi_\ell})/M(1))$. The work of Bourgain, Gamburd, and Sarnak shows there is an integer $N_{1/2}$ such that $n_\ell - d_\ell \leq \ell^{1/2}$ when $\ell \geq N_{1/2}$.

Theorem C. *Fix a prime ℓ for which $\boldsymbol{P}(\ell)$ holds. If $\ell \equiv 1 \mod 4$ assume that $\ell \geq \max(N_{1/2}, 13)$ while if $\ell \equiv 3 \mod 4$ assume that $\ell \geq \max(N_{1/2}, 23)$. Then $M(\overline{\pi_\ell})$ is geometrically connected, smooth over $\mathbb{Z}[1/|\operatorname{PSL}_2(\mathbb{F}_\ell)|]$, and finite étale over $M(1)-\{j=0,1728\}$. The geometric monodromy group $\operatorname{Mon}(M(\overline{\pi_\ell})/M(1))$ is isomorphic to either A_{d_ℓ} or S_{d_ℓ}. In either case, there is an at-most-quadratic extension K_ℓ of $\mathbb{Q}$ with ring of integers $\mathcal{O}_{K_\ell}$ such that the monodromy is defined over $\mathcal{O}_{K_\ell}$. Let k_ℓ be the residue field of a prime of $\mathcal{O}_{K_\ell}$ lying above p for $p \nmid |\operatorname{PSL}_2(\mathbb{F}_\ell)|$. Then the fiber over k_ℓ is a smooth, geometrically connected, $\operatorname{Mon}(M(\overline{\pi_\ell})/M(1))$-cover of $\mathbb{P}^1_{k_\ell}$ tamely ramified only over three points. Moreover, if $\operatorname{Mon}(M(\overline{\pi_\ell})/M(1)) \cong S_{d_\ell}$, then we may take $K_\ell = \mathbb{Q}$ and hence $k_\ell = \mathbb{F}_p$.*

Remark 1.1.1. The particular form of the monodromy groups of $M(\operatorname{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}} \to M(1)$ - in particular the fact that $|S_{n_\ell}|, |A_{n_\ell}|$ are divisible by many primes which don't divide $|\operatorname{PSL}_2(\mathbb{F}_\ell)|$ - is crucial to ensure that our result is interesting; specifically, that we obtain many primes of good reduction that *divide* the order of the monodromy group. It is a consequence of Belyi's theorem (see Theorem 2.2.3) or [DDH89] that every three-point cover can be realized as a map between moduli spaces. Thus, given an abstract three-point cover, one could try to find a moduli-interpretation of it, with the hopes of using that moduli-interpretation to deduce good reduction at "interesting primes p". A general procedure for finding a moduli-interpretation in terms of G-structures amounts to an effective version of Asada's theorem (see Theorem 2.2.2(7) below), which exists by the work of Bux–Ershov–Rapinchuk [BER11] and a subsequent improvement by Ben-Ezra and Lubotzky [BEL18, Theorems 2.7, 2.9]. However, their methods *never* yield automatic good reduction at primes dividing the order of the monodromy group.

Remark 1.1.2. Let F_2 be a free group of rank 2. The connectedness of $M(\operatorname{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ is a consequence of the transitivity of the action of $\operatorname{Aut}^+(F_2)$ (the index two subgroup of $\operatorname{Aut}(F_2)$ consisting of automorphisms which induce automorphisms of determinant 1 on $F_2/[F_2, F_2] \cong \mathbb{Z}^2$) on the set of equivalence classes $X := \{(a,b) \mid a, b \text{ generate } \operatorname{SL}_2(\mathbb{F}_\ell) \text{ and } \operatorname{tr}[a,b] = -2 \in \mathbb{F}_\ell\}/\sim$, where two pairs are equivalent if they are conjugate by an element of $\operatorname{SL}_2(\overline{\mathbb{F}_\ell})$ (see §3). On its face, this transitivity is a difficult problem in combinatorial group theory [LP01, §2]. However, because $\operatorname{SL}_2(\mathbb{F}_\ell)$ is the $\mathbb{F}_\ell$-points of an *algebraic group*, the set X inherits an algebraic structure: it is the set of $\mathbb{F}_\ell$ points of a certain *character variety* on which $\operatorname{Aut}^+(F_2)$ acts via automorphisms of the variety. In the case of $\operatorname{SL}_2(\mathbb{F}_\ell)$, this variety turns out to be an (affine) *ruled surface*. The analysis of [BGS16a,BGS16b] and [MP18] make crucial use of this structure, especially the fact that $\operatorname{Aut}^+(F_2)$ is generated by the conjugates of an automorphism which correspond to "rotations" along the ruling. In general, if G is a finite group of Lie type, this suggests that a deeper understanding of the stacks $\mathcal{M}(G)$ may be obtained from the study of the associated character variety.

Remark 1.1.3. We work with the moduli of elliptic curves with G-structures when $G = \operatorname{SL}_2(\mathbb{F}_\ell)$ and $G = \operatorname{PSL}_2(\mathbb{F}_\ell)$. While the results of [Che18] are applicable for any finite group G, our choice of G allows us to leverage the work of [BGS16b] and [MP18] to understand the connected components of $M(G)^{\mathrm{abs}}$ and the monodromy. Empirically, for other choices of G there is more variability in the monodromy group. For example, taking $G = A_7$ we compute that of the 17 components of $M(A_7)^{\mathrm{abs}}$, two have symmetric monodromy, twelve have alternating monodromy, and three have smaller monodromy. While this diversity would complicate any analysis, it also provides opportunities to realize additional groups as quotients of $\pi_1^t(\mathbb{P}^1_{\overline{\mathbb{F}}_p} - \{0, 1, \infty\})$.

Remark 1.1.4. Our results address a function field analog of a question articulated in [RV15] about the existence of number fields with little ramification and large Galois groups. For a number field K of degree d over $\mathbb{Q}$, say that K is full if the associated Galois group is either S_d or A_d.

The question is whether given a set of places $\mathcal{P}$ of $\mathbb{Q}$, are there infinitely many full number fields unramified outside $\mathcal{P}$?

Roberts and Venkatesh construct examples by specializing maps between appropriately chosen Hurwitz spaces, but are unable to guarantee there are infinitely many specializations which produce non-isomorphic examples in order to prove [RV15, Conjecture 8.1].

Analogously, our results show that for any set of $\mathbb{F}_p$-rational places $\mathcal{P}$ of $\mathbb{F}_p(t)$ with $\#\mathcal{P} \geq 3$, there exist infinitely many non-isomorphic full extensions unramified outside of $\mathcal{P}$.

1.2. **Organization of the paper.** In §2, we review the moduli of elliptic curves and the theory of G-structures, and explain how to use them to produce covers of the projective line. We begin with the analytic theory in §2.1, which gives a concrete relation between the Galois theory for coverings of the moduli stack of elliptic curves and the Galois theory for coverings of its coarse moduli space (see Proposition 2.1.2 and Corollary 2.1.3). While these results could have also been obtained algebraically, we find that the analytic perspective leads to a less technical exposition and naturally takes us through the necessary background to make clear the connection between our moduli stacks and the classical construction of modular curves as quotients of the upper half plane. Next, in §2.2, we recall the arithmetic theory of the moduli of elliptic curves with G-structures (see [Che18]), whose moduli stacks $\mathcal{M}(G)$ are finite étale over the moduli stack of elliptic curves. In §2.3, making crucial use of the algebraic theory, we explain how to use their coarse moduli schemes to obtain tame covers of the projective line in characteristic p. We then introduce the notion of absolute G-structures in §2.4, and study their Higman and trace invariants in §2.5.

In §3, we prove Theorem B. We review the work of Bourgain–Gamburd–Sarnak and Meiri–Puder on Markoff triples modulo ℓ in §3.1. In §3.2, we relate the geometric fibers of $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ and $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ with Markoff triples modulo ℓ and relate the monodromy action on the fibers with the action of a group of automorphisms of the Markoff surface. In §3.3 we analyze the ramification of the coarse schemes of these stacks as covers of the j-line and produce a $\mathbb{Q}$-rational point above $j = 0$. In §3.4 we give a conceptual explanation of a rational point over $j = 0$. We give the proof of Theorem B in §3.5.

Finally, in §4, we address the case that ℓ lies in the exceptional set $\mathcal{E}$ of primes not covered by the arguments of [BGS16b]. By adapting the arguments of [MP18] to apply to the largest orbit in $Y^*(\ell)$, we prove Theorem C and obtain additional tamely ramified covers with symmetric or alternating Galois groups at the cost of only being able to bound the degree.

1.3. **Notation and Conventions.** Throughout, $\overline{\mathbb{Q}}$ will denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

Throughout this paper we will try to reserve the letter p to refer to the characteristic of a field over which we are working, and ℓ will generally refer to a prime distinct from p.

Often script letters "$\mathcal{M}$" will be used to denote a stack, in which case the corresponding Roman letter "M" will be used to denote its coarse space/scheme.

For groups F and G, $\mathrm{Epi}^{\mathrm{ext}}(F, G)$ is the set of equivalence classes of surjections $F \twoheadrightarrow G$ considered up to conjugation on G (or equivalently in F).

When there is no risk of confusion, we will denote both the étale fundamental group of a scheme and the topological fundamental group of an analytic space by π_1. When there is risk of confusion, we use $\pi_1^{\text{ét}}$ and π_1^{top}.

1.4. **Acknowledgements.** Bell was supported by European Research Council grant #715747 (to François Charles). Booher was partially supported by the Marsden Fund Council administered by the Royal Society of New Zealand. Chen was partially supported by the National Science

Foundation under Award No. DMS-1803357. We thank Piotr Achinger, Jordan Ellenberg, David Harbater, Julia Hartmann, Andrew Obus, and Rachel Pries for helpful conversations, and the American Mathematical Society and the organizers of the math research community "Explicit Methods in Arithmetic Geometry in Characteristic p" which was the genesis of this project. We also thank the anonymous referee for comments on an earlier draft.

2. Moduli of elliptic curves with G-structure

Here we review the moduli stack of elliptic curves with G-structure and explain how to use their connected components to construct tamely ramified three-point covers in characteristic p.

2.1. **Analytic Moduli of Elliptic Curves.**

In this section we review the analytic theory of the moduli of elliptic curves. The main purpose is to explain the relationship between the geometric fiber of a finite étale cover of the moduli stack with the geometric fiber of the corresponding map on coarse spaces (see Proposition 2.1.2 and Corollary 2.1.3). By standard GAGA arguments, the same results will hold over algebraically over $\overline{\mathbb{Q}}$ or $\mathbb{C}$.

For an analytic elliptic curve E, a *framing* on E is a choice of basis $\mathfrak{f} = (\mathfrak{f}_1, \mathfrak{f}_2)$ of $H_1(E, \mathbb{Z})$ such that the intersection product $\mathfrak{f}_1 \cdot \mathfrak{f}_2 = 1$. Given a holomorphic family of elliptic curves over a complex analytic manifold, by Ehresmann's fibration theorem the family is topologically locally constant, and a framing on the family is defined to be a locally constant family of framings on the fibers. Let $\mathcal{T}$ denote the moduli stack of framed elliptic curves, then $\mathcal{T}$ is a complex manifold isomorphic to the upper half plane (see [Hai11, Proposition 2.4] and [FM12, Proposition 10.1]). A point of $\mathcal{T}$ is thus an isomorphism class of framed elliptic curves.

Explicitly, this isomorphism can be defined as follows. Let $\mathcal{H} := \{z \in \mathbb{C} : \Im(z) > 0\}$ be the upper half plane. The action of $\mathbb{Z}^2$ on $\mathcal{H} \times \mathbb{C}$ given by

$$(\tau, z) \cdot (n, m) = (\tau, z + n\tau + m) \qquad (\tau, z) \in \mathcal{H} \times \mathbb{C},\ (n, m) \in \mathbb{Z}^2$$

is free. Let $\mathbb{E} := (\mathcal{H} \times \mathbb{C})/\mathbb{Z}^2$, then together with the zero section $\mathcal{H} \times \{0\}$, $\mathbb{E}$ is a family of elliptic curves over $\mathcal{H}$. We give $\mathbb{E}$ the structure of a framed family by specifying the ordered basis $(\mathfrak{f}_1, \mathfrak{f}_2)$ of $H_1(\mathbb{E}_\tau, \mathbb{Z})$ to be given by the straight-line paths $0 \rightsquigarrow 1$ and $0 \rightsquigarrow \tau$ respectively in $\mathbb{C}$. This defines a framing $\mathfrak{f}_{\mathbb{E}}$ on $\mathbb{E}$ and determines the isomorphism $\mathcal{H} \xrightarrow{\sim} \mathcal{T}$.

Fix a framed elliptic curve $(E_0, \mathfrak{f}_0)$ and let Γ_{E_0} denote its (orientation-preserving) mapping class group (see [FM12, §2.1]). Then Γ_{E_0} acts on $\mathcal{T}$ as follows. Given a framed elliptic curve $(E, \mathfrak{f})$, up to homotopy there is a unique homeomorphism of elliptic curves $\phi_{\mathfrak{f}_0, \mathfrak{f}} : E_0 \to E$ which respects the framings. Then Γ_{E_0} acts on $\mathcal{T}$ by the rule

$$\gamma \cdot (E, \mathfrak{f}) = (E, (\phi_{\mathfrak{f}_0,\mathfrak{f}} \circ f_\gamma \circ \phi_{\mathfrak{f}_0,\mathfrak{f}}^{-1})(\mathfrak{f})) \tag{2-1-1}$$

where f_γ is a self-homeomorphism of E_0 representing γ. This gives a *right* action of Γ_{E_0} on $\mathcal{T}$. Since (2-1-1) defines a free and transitive action of Γ_{E_0} on the set of framings of E, the stack quotient $[\mathcal{T}/\Gamma_{E_0}]$ is naturally the complex analytic moduli stack of elliptic curves, denoted $\mathcal{M}(1)^{\mathrm{an}}$. Since $\mathcal{T}$ is simply connected, relative to the base point $(E_0, \mathfrak{f}_0) \in \mathcal{T}$, the group Γ_{E_0} acts (on the left) on the fiber functor associated to the Galois category of $\mathcal{M}(1)^{\mathrm{an}}$ [Noo05, §18]. This action induces an isomorphism

$$\pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E_0) \xrightarrow{\sim} \Gamma_{E_0}. \tag{2-1-2}$$

The action of Γ_{E_0} on $H_1(E_0, \mathbb{Z})$ also induces a canonical isomorphism [FM12, Theorem 2.5]

$$\Gamma_{E_0} \xrightarrow{\sim} \mathrm{SL}(H_1(E_0, \mathbb{Z})). \tag{2-1-3}$$

We can relate the action of Γ_{E_0} on $\mathcal{T}$ to the usual action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ as follows. Let $\mathrm{SL}_2(\mathbb{Z})$ act on the set of framings of E_0 by

$$\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \cdot \mathfrak{f} := \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \left[\begin{smallmatrix} \mathfrak{f}_1 \\ \mathfrak{f}_2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} c\mathfrak{f}_2 + d\mathfrak{f}_1 \\ a\mathfrak{f}_2 + b\mathfrak{f}_1 \end{smallmatrix}\right] \qquad \text{for } \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z}),$$

then this action is free and transitive and defines an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{T}$.[3] Via the isomorphism $(\mathbb{E}, \mathfrak{f}_{\mathbb{E}}) : \mathcal{H} \xrightarrow{\sim} \mathcal{T}$, one can check that this $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathcal{T}$ is transported to the usual $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathcal{H}$ given by fractional linear transformations: $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \cdot \tau = \frac{a\tau+b}{c\tau+d}$. In particular, we see that the framed family $\mathbb{E}$ induces an explicit universal cover $\mathcal{H} \to \mathcal{M}(1)^{\mathrm{an}}$, which induces an isomorphism $[\mathcal{H}/\,\mathrm{SL}_2(\mathbb{Z})] \xrightarrow{\sim} \mathcal{M}(1)^{\mathrm{an}}$.

Similarly, the topological quotient $\mathcal{T}/\Gamma_{E_0} \cong \mathcal{H}/\,\mathrm{SL}_2(\mathbb{Z})$ is the *coarse (analytic) moduli space* of elliptic curves, which we denote $M(1)^{\mathrm{an}}$. On $\mathcal{H}$, the j-invariant is a holomorphic function which is invariant under $\mathrm{SL}_2(\mathbb{Z})$, and descends to an isomorphism $\mathcal{H}/\,\mathrm{SL}_2(\mathbb{Z}) \cong \mathbb{C}$. Given an elliptic curve E, $E \cong \mathbb{E}_\tau$ for some $\tau \in \mathcal{H}$, and the j-invariant of E is just $j(E) := j(\tau)$. We will often use the j function to identify $\mathcal{H}/\,\mathrm{SL}_2(\mathbb{Z})$ with $\mathbb{C}$.

Remark 2.1.1. If we choose an isomorphism $\mathcal{M}(1)^{\mathrm{an}} \cong [\mathcal{H}/\,\mathrm{SL}_2(\mathbb{Z})]$ as above, then Galois theory gives a correspondence between finite index subgroups $\Gamma \le \mathrm{SL}_2(\mathbb{Z})$ and connected finite covers of $\mathcal{M}(1)^{\mathrm{an}} \cong [\mathcal{H}/\,\mathrm{SL}_2(\mathbb{Z})]$. Explicitly, the cover corresponding to Γ is simply the projection map $[\mathcal{H}/\Gamma] \to [\mathcal{H}/\,\mathrm{SL}_2(\mathbb{Z})]$, and its coarse space is the topological quotient $\mathcal{H}/\Gamma$ (a "modular curve"). From this perspective, all finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ are treated equally. As discussed in [Che18] and reviewed below, this allows us to describe a generalization of the notion of "level structure" for elliptic curves whose moduli spaces incorporate both congruence and noncongruence modular curves.

For an analytic space B and a family of elliptic curves $E_B \to B$, letting E_{b_0} be the fiber of E_B above $b_0 \in B$, there is a monodromy representation

$$\rho_{b_0} : \pi_1^{\mathrm{top}}(B, b_0) \longrightarrow \mathrm{SL}(H_1(E_{b_0}, \mathbb{Z})).$$

We may extend this construction to obtain a monodromy representation for the universal family over $\mathcal{M}(1)^{\mathrm{an}}$

$$\rho_E : \pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E) \longrightarrow \mathrm{SL}(H_1(E, \mathbb{Z}))$$

which is precisely the composition of the isomorphisms (2-1-2) and (2-1-3). If we view E_B as a map $B \to \mathcal{M}(1)^{\mathrm{an}}$, then $\rho_{b_0}, \rho_{E_{b_0}}$ fit into a commutative diagram

(2-1-4)
$$\begin{tikzcd}
\pi_1^{\mathrm{top}}(B, b_0) \arrow[r, "(E_B)_*"] \arrow[dr, "\rho_{b_0}"'] & \pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E_{b_0}) \arrow[d, "\rho_{E_{b_0}}"] \\
 & \mathrm{SL}(H_1(E_{b_0}, \mathbb{Z}))
\end{tikzcd}$$

Coarse monodromy via stacky monodromy. Now suppose $\mathcal{M} \to \mathcal{M}(1)^{\mathrm{an}}$ is any finite (étale) cover, and let M be the coarse moduli space of $\mathcal{M}$; the universal property of coarse moduli spaces yields

[3] We note that this action is *not* the same as the one coming from the isomorphism $\mathbb{Z}^2 \xrightarrow{\sim} H_1(E_0, \mathbb{Z})$ sending (e_1, e_2) to $(\mathfrak{f}_{0,1}, \mathfrak{f}_{0,2})$. This isomorphism would induce an isomorphism $\mathrm{SL}_2(\mathbb{Z}) \cong \mathrm{SL}(H_1(E_0, \mathbb{Z})) \cong \Gamma_{E_0}$ which would yield the action $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \cdot \tau = \frac{b+d\tau}{a+c\tau}$ for $\tau \in \mathcal{H}$.

a commutative (but not cartesian!) diagram

$$\begin{tikzcd}
\mathcal{M} \arrow[r] \arrow[d] & M \arrow[d] \\
\mathcal{M}(1)^{\mathrm{an}} \arrow[r] & M(1)^{\mathrm{an}}
\end{tikzcd}$$

Let $\mathcal{M}(1)^\circ \subset \mathcal{M}(1)^{\mathrm{an}}$ denote the open substack parametrizing elliptic curves without fibers of j-invariant 0 or 1728. Its coarse space is just $M(1)^\circ := M(1)^{\mathrm{an}} - \{j = 0, 1728\}$. Then the restricted cover $\mathcal{M}^\circ \subset \mathcal{M}$ is still a cover of $\mathcal{M}(1)^\circ$, but moreover its coarse space M° is now also a finite cover of $M(1)^\circ$, corresponding to the fact that the $\mathrm{SL}_2(\mathbb{Z})$ action on $\mathcal{H}$ descends to an action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathcal{H}$ which is *free* on the complement of the orbits of $e^{2\pi i/6}$ and i (where $j = 0, 1728$). We wish to understand the monodromy of $M^\circ/M(1)^\circ$ via the monodromy of $\mathcal{M}/\mathcal{M}(1)^{\mathrm{an}}$.

Let $B := M(1)^\circ$ and let E be an elliptic curve over B with "j-invariant j". That is, it has no fibers of j-invariants $0, 1728$ and the induced map $M(1)^\circ \xrightarrow{E} \mathcal{M}(1)^\circ \to M(1)^\circ$ is the identity. For example, we may take E to be given by

$$y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}. \tag{2-1-5}$$

Let $b_0 \in B$ be a base point, then the induced map $B \to \mathcal{M}(1)^{\mathrm{an}}$ sends b_0 to the elliptic curve E_{b_0}, and the fiber $\mathcal{M}_{E_{b_0}}$ is by definition the underlying set of the fiber product $\{b_0\} \times_{\mathcal{M}(1)^{\mathrm{an}}} \mathcal{M}$. This fiber admits a natural action of $\mathrm{Aut}(E_{b_0}) = \{[\pm 1]\}$, as well as a natural monodromy action of $\pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E_{b_0})$. There is a natural map[4]

$$\mathrm{Aut}(E_{b_0}) \hookrightarrow \pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E_{b_0})$$

which is an isomorphism onto the center of $\pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E_{b_0})$, and the actions of $\mathrm{Aut}(E_{b_0})$ and $\pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E_{b_0})$ on $\mathcal{M}_{E_{b_0}}$ are compatible with respect to this map. The map to the coarse space $\mathcal{M} \to M$ induces a map $\mathcal{M}_{E_{b_0}} \to M_{b_0}$ which is surjective and since $j(E_{b_0}) \neq 0, 1728$, it induces a bijection of sets

$$\alpha : \mathcal{M}_{E_{b_0}}/\{[\pm 1]\} \xrightarrow{\sim} M_{b_0}.$$

We have a commutative diagram

$$\begin{tikzcd}
\mathcal{M}^\circ_B \arrow[r] \arrow[d] & \mathcal{M}^\circ \arrow[r] \arrow[d] & M^\circ \arrow[d] \\
B \arrow[r, "E"] & \mathcal{M}(1)^\circ \arrow[r] & M(1)^\circ
\end{tikzcd}$$

where the left square is cartesian and the right square is induced by the universal property of coarse spaces. Remembering that $B = M(1)^\circ$, the composition of the bottom row is the identity, and so the composition of the top row is a map of covers of $M(1)^\circ$ which induces the map $(\mathcal{M}^\circ_B)_{b_0} = \mathcal{M}_{E_{b_0}} \to M_{b_0}$. In particular, this map must be equivariant for the monodromy action of $\pi_1^{\mathrm{top}}(M(1)^\circ, b_0)$, and hence α is equivariant for $\pi_1^{\mathrm{top}}(M(1)^\circ, b_0)$ acting on $\mathcal{M}_{E_{b_0}}$ via

$$\pi_1^{\mathrm{top}}(M(1)^\circ, b_0) \xrightarrow{E_*} \pi_1^{\mathrm{top}}(\mathcal{M}(1)^\circ, E_{b_0}) \longrightarrow \pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E_{b_0}).$$

Proposition 2.1.2. *Let $\mathcal{M} \to \mathcal{M}(1)^{\mathrm{an}}$ be a finite cover and let $M \to M(1)^{\mathrm{an}}$ be the induced map on coarse spaces. Let $M^\circ \to M(1)^\circ$ be the restriction to the preimage over the complement of $j = 0, 1728$. Let E be any elliptic curve over $M(1)^\circ$ with "j-invariant j".*

[4] If x is the point of $\mathcal{M}(1)$ corresponding to E_{b_0}, then in the language of [Noo04] and [Noo05], this map is the canonical map from the "inertial fundamental group" or "hidden fundamental group" to the full fundamental group, and is denoted "ω_x".

(1) Let $b_0 \in M(1)^\circ$, and let $\mathcal{M}_{E_{b_0}}$ be the fiber of $\mathcal{M}/\mathcal{M}(1)^{\mathrm{an}}$ over E_{b_0}. Then the natural map $\mathcal{M} \to M$ induces a bijection

$$\alpha : \mathcal{M}_{E_{b_0}}/\{[\pm 1]\} \xrightarrow{\sim} M_{b_0}.$$

(2) If the monodromy of $\mathcal{M}/\mathcal{M}(1)^{\mathrm{an}}$ is given by $\pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E_{b_0}) \to \mathrm{Aut}(\mathcal{M}_{E_{b_0}})$, and Z is the center of $\pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E_{b_0})$, then the monodromy action of $\pi_1^{\mathrm{top}}(M(1)^\circ, b_0)$ on M_{b_0} associated to the cover $M^\circ/M(1)^\circ$ is given by either path in the commutative diagram

$$\begin{tikzcd}
\pi_1^{\mathrm{top}}(M(1)^\circ, b_0) \arrow[r, "E_*"] & \pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E_{b_0}) \arrow[r] \arrow[d] & \pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E_{b_0})/Z \arrow[d] & \\
& \mathrm{Aut}(\mathcal{M}_{E_{b_0}}) \arrow[r] & \mathrm{Aut}(\mathcal{M}_{E_{b_0}}/\{[\pm 1]\}) \arrow[r, "\alpha_*"] & \mathrm{Aut}(M_{b_0})
\end{tikzcd}$$

Proof. The first statement was established in the discussion before the Proposition. To check the second, it remains to prove that the composition $\pi_1^{\mathrm{top}}(M(1)^\circ, b_0) \to \mathrm{Aut}(M_{b_0})$ is independent of the choice of E. This follows as the composition is simply the monodromy of $M^\circ/M(1)^\circ$, which makes no mention of E. It also follows from §7 and §8 of [Kod63] that the map E_* is surjective, though we will not need this. □

For any elliptic curve $E/M(1)^\circ$ with "j-invariant j", the local monodromy on homology around $j = 0, 1728$ or ∞ relative to some framing of a nearby fiber is conjugate to $\pm \left[\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right]$, $\pm \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ or $\pm \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ respectively. (See [Kod63, §7-8], or we can also check this for our choice of E as in (2-1-5) using Tate's algorithm.) By the commutativity of (2-1-4), the proposition also implies:

Corollary 2.1.3. *Let $\mathcal{M} \to \mathcal{M}(1)^{\mathrm{an}}$ be any finite cover, let $M \to M(1)^{\mathrm{an}}$ be the corresponding map of coarse spaces, and let $\overline{M} \to \overline{M(1)^{\mathrm{an}}}$ denote the map of their smooth compactifications. Fix an isomorphism $\mathbb{Z}^2 \cong H_1(E_{b_0}, \mathbb{Z})$ corresponding to some framing, and let $\psi : \pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, E_{b_0}) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z})$ be the isomorphism induced by the framing via* (2-1-2) *and* (2-1-3). *Then letting $\mathrm{SL}_2(\mathbb{Z})$ act on $\mathcal{M}_{E_{b_0}}$ via ψ, the fibers of $\overline{M} \to \overline{M(1)^{\mathrm{an}}}$ above $j = 0, 1728, \infty$ are in bijection with the orbit spaces*

$$(\mathcal{M}_{E_{b_0}}/\{[\pm 1]\})/\langle\left[\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right]\rangle, (\mathcal{M}_{E_{b_0}}/\{[\pm 1]\})/\langle\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]\rangle, (\mathcal{M}_{E_{b_0}}/\{[\pm 1]\})/\langle\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]\rangle$$

respectively. In each case, ramification indices correspond to orbit sizes of the corresponding monodromy matrix. In particular, all ramification indices of points above $j = 0$ must divide 3, all ramification indices above $j = 1728$ must divide 2, and all ramification indices above $j = \infty$ must divide the order of $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ acting on $\mathrm{Aut}(\mathcal{M}_{E_{b_0}}/\{[\pm 1]\})$.

Proof. The only thing to note is that all the indeterminacies due to the various "up to conjugations" that appear do not affect the final result. □

2.2. **Arithmetic moduli of elliptic curves with G-structures.** Let G be a finite group. In this section we will define the moduli stacks $\mathcal{M}(G)$ which will later be used to obtain the desired three-point covers. Throughout this section we will work over the base $\mathbb{Z}[1/|G|]$; we do not discuss what happens at primes dividing $|G|$.

A G-torsor over a scheme X is a finite étale morphism $f : Y \to X$ equipped with an X-linear action of G on Y which acts freely and transitively on geometric fibers. A morphism of G-torsors over X is an X-linear, G-equivariant morphism. Such morphisms, if they exist, are necessarily isomorphisms. If Y is connected then we will say that f is a Galois cover (or a G-Galois cover or a G-cover if we wish to emphasize the Galois group).

Let $\mathcal{M}(1)$ denote the moduli stack of elliptic curves. An object of $\mathcal{M}(1)$ over a scheme S is an elliptic curve E/S (equipped with a zero section $O : S \to E$), and a morphism $E/S \to E'/S'$ is given by a cartesian diagram

$$\begin{tikzcd} E \arrow[r] \arrow[d] & E' \arrow[d] \\ S \arrow[r] & S' \end{tikzcd}$$

which respects the corresponding zero sections. Let $M(1)$ denote its coarse moduli scheme. It is well known that $M(1)$ is the j-line $\mathrm{Spec}(\mathbb{Z}[1/|G|][j])$.

Let $\mathcal{T}_G^{\mathrm{pre}} : \mathcal{M}(1) \to \mathbf{Sets}$ be the presheaf which associates to any object E/S of $\mathcal{M}(1)$ the set of isomorphism classes of G-torsors over the punctured elliptic curve $E^\circ := E - O$ with geometrically connected fibers over S. Let $\mathcal{T}_G$ denote the sheafification of $\mathcal{T}_G^{\mathrm{pre}}$ relative to the étale topology[5]; a G-structure on E/S is by definition an element of $\mathcal{T}_G(E/S)$. In other words, a G-structure on E/S is given by a collection of G-torsors defined étale locally on S whose common restrictions are isomorphic. A more concrete combinatorial characterization of G-structures will be given in Theorem 2.2.2(3).

Let $\mathcal{M}(G)$ denote the category whose objects are pairs $(E/S, \alpha)$, where $\alpha \in \mathcal{T}_G(E/S)$ is a G-structure, and morphisms are morphisms in $\mathcal{M}(1)$ which respect the G-structure. There is a natural forgetful functor $\pi : \mathcal{M}(G) \to \mathcal{M}(1)$.

Remark 2.2.1. Here we record some technical remarks.

(1) Note that while the construction of $\mathcal{M}(G)$ here differs from that given in [Che18], the resulting objects are isomorphic. To see this, one checks that by Galois theory, one obtains a natural map from the presheaf $\mathcal{T}_G^{pre}$ to the presheaf of [Che18, Definition 2.2.3] which is locally an isomorphism. Thus, their sheafifications are isomorphic.

(2) If $S = \mathrm{Spec}\, k$ where k is a separably closed field, then there are no nontrivial étale coverings of $\mathrm{Spec}\, k$, so in this case a G-structure on any elliptic curve E over k is the same as a connected G-torsor on E°.

(3) In the description of G-structures given above, note that there is no "cocycle condition" requiring that the isomorphisms are compatible. If G has trivial center, then geometrically connected G-torsors over E°/S have no nontrivial automorphisms (and hence the isomorphisms are automatically compatible), so by descent the set of G-structures on E/S is precisely the set of isomorphism classes of geometrically connected G-torsors over E°/S. However, if G has nontrivial center, there can exist G-structures on E/S which do not come from a G-torsor on E°/S; this is reflected in the fact that $\mathcal{T}_G$ is defined as a sheafification. The benefit of setting things up this way is that the forgetful functor $\mathcal{M}(G) \to \mathcal{M}(1)$ is *representable*, and in fact finite étale. If we had instead defined $\mathcal{T}_G^{\mathrm{pre}}$ as a presheaf of *groupoids* of G-torsors (which would implicitly include a cocycle condition), then $\mathcal{T}_G^{\mathrm{pre}}$ would already be a sheaf (of groupoids), and this would lead to a Hurwitz stack in the style of [BR11] or [ACV03]. Such stacks have a more natural "moduli interpretation", but the tradeoff is that its forgetful map to $\mathcal{M}(1)$ is typically not representable, hence not finite.

(4) (Analysis to arithmetic) As seen in §2.1, the analytic theory of the moduli of elliptic curves yields very concrete descriptions of finite covers of the moduli stack of elliptic curves. Because of this concreteness, and to avoid introducing additional notation to deal with profinite

[5] Here, the étale topology on $\mathcal{M}(1)$ is the inherited topology from the big étale site $(\mathbf{Sch}/\mathbb{Z}[1/|G|])_{\text{ét}}$. That is to say, a family of maps in $\mathcal{M}(1)$ with fixed target E/S is a covering family if their images in $\mathbf{Sch}/\mathbb{Z}[1/|G|]$ is an étale covering.

groups, when discussing Galois theory we will sometimes prefer to state the analytic version of the corresponding algebraic statement over $\mathbb{C}$. By the Riemann existence theorem for stacks (see [Noo05] Theorem 20.1), nothing is lost in this translation. Finally, to pass from algebraic stacks over $\mathbb{C}$ to stacks over $\overline{\mathbb{Q}}$, one should keep in mind the philosophy that "a base change between algebraically closed fields of characteristic 0 does not change the fundamental group". For schemes, this follows from the Künneth formula for fundamental groups (see [Gro71, Exposé XIII Proposition 4.6]) . For $\mathcal{M}(1)$, one may use the fact that one may find a geometrically connected finite étale Galois cover $U \to \mathcal{M}(1)$ with U a scheme. One then writes $\pi_1(\mathcal{M}(1))$ as an extension of the Galois group by $\pi_1(U)$. The Galois group is not changed by algebraically closed base extension and by the Kunneth formula neither is $\pi_1(U)$. The "short five lemma" then yields the invariance of $\pi_1(\mathcal{M}(1))$ under change of algebraically closed fields. In what follows we will use this result freely.

Next we record some of the salient properties of $\mathcal{M}(G)$.

Theorem 2.2.2. *Let G be a finite group, and let $\pi : \mathcal{M}(G) \to \mathcal{M}(1)$ be the forgetful map. We will work universally over* $\operatorname{Spec}\mathbb{Z}[1/|G|]$ *unless otherwise stated.*

(1) (Étaleness) The category $\mathcal{M}(G)$ is a Deligne-Mumford stack and the forgetful functor $\pi : \mathcal{M}(G) \to \mathcal{M}(1)$ is finite étale.

(2) (Coarse moduli and ramification) $\mathcal{M}(G)$ admits a coarse moduli scheme $M(G)$ which is a normal affine scheme finite over $M(1) \cong \operatorname{Spec}\mathbb{Z}[1/|G|][j]$, and smooth of relative dimension 1 over $\mathbb{Z}[1/|G|]$. Moreover, $M(G)$ is étale over the complement of the sections $j = 0$ and $j = 1728$ in $M(1)$. If either $6 \mid |G|$ or S is a regular Noetherian $\mathbb{Z}[1/|G|]$-scheme, then $M(G) \times_{\mathbb{Z}[1/|G|]} S$ is the coarse moduli scheme of $\mathcal{M}(G) \times_{\mathbb{Z}[1/|G|]} S$, and is normal.

(3) (Combinatorial description of G-structures) Let $\mathbb{L}$ be the set of prime divisors of $|G|$. For any profinite group π, let $\pi^{\mathbb{L}}$ denote the maximal pro-$\mathbb{L}$-quotient of π. Let E be an elliptic curve over a scheme S. Let $x \in E^\circ$ be a geometric point, and let s be its image in S. The sequence $E_s^\circ \hookrightarrow E \to S$ induces an outer representation

$$\rho_{E,x} : \pi_1^{\text{ét}}(S, s) \to \operatorname{Out}(\pi_1^{\mathbb{L}}(E_s^\circ, x))$$

which, by precomposition, gives a natural right action of $\pi_1(S, s)$ on the set

$$\operatorname{Epi}^{\text{ext}}(\pi_1^{\mathbb{L}}(E_s^\circ, x), G) := \operatorname{Epi}(\pi_1^{\mathbb{L}}(E_s^\circ, x), G)/\operatorname{Inn}(G)$$

of surjective morphisms $\pi_1^{\mathbb{L}}(E_s^\circ, x) \to G$ up to conjugation in G. By the Galois correspondence, this action corresponds to a finite étale morphism $F \to S$. There is a cartesian diagram:

$$\begin{tikzcd} F \arrow[r] \arrow[d] & \mathcal{M}(G) \arrow[d, "\pi"] \\ S \arrow[r, "E/S"] & \mathcal{M}(1). \end{tikzcd}$$

In particular, since the primes dividing $|G|$ are in $\mathbb{L}$, this diagram defines a bijection

$$\mathcal{T}_G(E/S) \xrightarrow{\sim} \{\varphi \in \operatorname{Epi}^{\text{ext}}(\pi_1(E_s^\circ, x), G) \mid \varphi \circ \rho_{E,x}(\sigma) = \varphi \quad \text{for all } \sigma \in \pi_1(S, s)\},$$

where we recall that $\mathcal{T}_G(E/S)$ is by definition the set of G-structures on E/S.

(4) (Fibers) Let E be an elliptic curve over an algebraically closed field k of characteristic not dividing $|G|$, and let $x_0 \in E^\circ(k)$. Let $x_E : \operatorname{Spec} k \to \mathcal{M}(1)$ be the geometric point given by E and let $\pi : \mathcal{M}(G) \to \mathcal{M}(1)$ be the forgetful map. Then the geometric fiber $\pi^{-1}(x_E)$ is

in bijection with the set of isomorphism classes of connected G-torsors over E°. By Galois theory, taking monodromy representations gives a bijection

$$\pi^{-1}(x_E) \xrightarrow{\sim} \mathrm{Epi}^{\mathrm{ext}}(\pi_1^{\text{ét}}(E^\circ, x_0), G) := \mathrm{Epi}(\pi_1^{\text{ét}}(E^\circ, x_0), G)/\operatorname{Inn}(G), \tag{2-2-1}$$

If E is an elliptic curve over $\mathbb{C}$ and $x_0 \in E^\circ(\mathbb{C})$, by Galois theory taking monodromy representations gives a bijection

$$\pi^{-1}(x_E) \xrightarrow{\sim} \mathrm{Epi}^{\mathrm{ext}}(\pi_1^{\mathrm{top}}(E^\circ(\mathbb{C}), x_0), G).$$

In particular, if G is not generated by two elements, then $\mathcal{M}(G)$ is the empty stack.

(5) *(Monodromy) Let E be an elliptic curve over $\mathbb{C}$, $x_0 \in E^\circ(\mathbb{C})$, $\Pi := \pi_1^{top}(E^\circ(\mathbb{C}), x_0)$, and let $x_E : \operatorname{Spec}\mathbb{C} \to \mathcal{M}(1)$ be the geometric point corresponding to E. Then Π is a free group of rank 2, and the canonical map $\Pi \to H_1(E,\mathbb{Z})$ induces an isomorphism $\Pi/[\Pi,\Pi] \cong H_1(E,\mathbb{Z})$. Let Γ_E denote the orientation-preserving mapping class group of $E^\circ(\mathbb{C})$, and let $\mathrm{Out}^+(\Pi)$ be the preimage of $\mathrm{SL}(H_1(E,\mathbb{Z}))$ under the canonical map*

$$\alpha : \mathrm{Out}(\Pi) \to \mathrm{GL}(H_1(E,\mathbb{Z})).$$

The outer action of Γ_E on Π is faithful and identifies Γ_E with $\mathrm{Out}^+(\Pi)$. As α is an isomorphism, it induces isomorphisms $\Gamma_E \xrightarrow{\sim} \mathrm{Out}^+(\Pi) \xrightarrow{\sim} \mathrm{SL}(H_1(E,\mathbb{Z}))$. The analytic theory identifies Γ_E with the topological fundamental group of the analytic moduli stack of elliptic curves (with base point E), from which we obtain a canonical isomorphism $\Gamma_E^\wedge \xrightarrow{\sim} \pi_1^{\text{ét}}(\mathcal{M}(1)_{\overline{\mathbb{Q}}}, x_E)$ (where $^\wedge$ denotes profinite completion). In particular, there is a canonical injective map $\Gamma_E \hookrightarrow \pi_1^{\text{ét}}(\mathcal{M}(1)_{\overline{\mathbb{Q}}}, x_E)$ with dense image. With respect to this map, the bijection

$$\pi^{-1}(x_E) \xrightarrow{\sim} \mathrm{Epi}^{\mathrm{ext}}(\Pi, G)$$

of (4) is Γ_E-equivariant. To summarize, we have canonical isomorphisms

$$\pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, x_E) \cong \Gamma_E \cong \mathrm{Out}^+(\Pi) \cong \mathrm{SL}(H_1(E,\mathbb{Z}))$$

and

$$\pi_1^{\text{ét}}(\mathcal{M}(1)_{\overline{\mathbb{Q}}}, x_E) \cong \pi_1^{\mathrm{top}}(\mathcal{M}(1)^{\mathrm{an}}, x_E)^\wedge.$$

(6) *(Functoriality) Let $\mathcal{C}$ denote the category whose objects are finite groups generated by two elements, and whose morphisms are surjective homomorphisms. If $f : G_1 \twoheadrightarrow G_2$ is a morphism in $\mathcal{C}$, then we obtain a map $\mathcal{T}_f^{\mathrm{pre}} : \mathcal{T}_{G_1}^{\mathrm{pre}} \to \mathcal{T}_{G_2}^{\mathrm{pre}}$ defined by sending the G_1-torsor $X^\circ \to E^\circ$ to the G_2-torsor $X^\circ/\ker(f) \to E^\circ$ where the G_2-action is given by the canonical isomorphism $G_2 \cong G_1/\ker(f)$. This induces a map $\mathcal{T}_f : \mathcal{T}_{G_1} \to \mathcal{T}_{G_2}$, whence a map*

$$\mathcal{M}(f) : \mathcal{M}(G_1) \to \mathcal{M}(G_2).$$

The maps $\mathcal{M}(f)$ make the rule sending $G \in \mathcal{C}$ to the map $\mathcal{M}(G) \to \mathcal{M}(1)$ into an epimorphism-preserving functor from $\mathcal{C}$ to the category[6] *of stacks finite étale over $\mathcal{M}(1)$. Let E, Π, Γ_E be as in (4); then in terms of the Galois correspondence for covers of $\mathcal{M}(1)$, given a surjection $f : G_1 \to G_2$, the induced map $\mathcal{M}(G_1) \to \mathcal{M}(G_2)$ (of $\mathbb{Z}[1/|G|]$-stacks) is given by the Γ_E-equivariant map of fibers*

$$f_* : \mathrm{Epi}^{\mathrm{ext}}(\Pi, G_1) \to \mathrm{Epi}^{\mathrm{ext}}(\Pi, G_2)$$

obtained by post-composing every surjection with f.

(7) *(Cofinality — Asada's theorem) For any stack $\mathcal{M}$ finite étale over $\mathcal{M}(1)_{\overline{\mathbb{Q}}}$, there is a finite group G such that $\mathcal{M}$ is dominated by some connected component of $\mathcal{M}(G)_{\overline{\mathbb{Q}}}$.*

[6] Here we mean the (1-)category associated to the (2,1)-category, see [Noo04, §4].

Proof. Part (1) is [Che18, Proposition 3.1.4] . Everything in (2) except for normality and étaleness is [Che18, Proposition 3.3.4]. The normality of $M(G)$ follows from the fact that $M(G)$ is the quotient of a smooth representable moduli problem by a finite group (see [Che18, §3.3.3]). Let $U \subset M(1)$ be the complement of $j = 0, 1728$; to see $M(G)$ is étale over the complement of U, consider a finite étale surjection $\mathcal{M} \to \mathcal{M}(G)$ with $\mathcal{M}$ representable (we may for example take $\mathcal{M}$ to be the fiber product over $\mathcal{M}(1)$ of $\mathcal{M}(G)$ with the moduli stack of elliptic curves with full level p^2 structure for some $p \mid |G|$). By [KM85, Corollary 8.4.5], the map $\mathcal{M}_U \to U$ is étale. Since $\mathcal{M}, M(G)$ and $M(1)$ are regular, by purity of the branch locus we are reduced to checking étaleness of extensions of complete discrete valuation rings. Since ramification indices of such extensions are multiplicative, étaleness of the composite $\mathcal{M}_U \to \mathcal{M}(G)_U \to U$ implies étaleness of $\mathcal{M}(G)_U \to U$. Part (3) is [Che18, Proposition 2.2.6(1,2)]. Part (4) follows from part (3), setting $S = \operatorname{Spec} k$. For (5), a theorem of Nielsen gives that α is an isomorphism [OZ81, Theorem 3.1], and the isomorphism $\Gamma_E^\wedge \cong \pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}}, E)$ follows from the Riemann existence theorem for stacks [Noo05, Theorem 20.4]. The rest of (5) is simply an unfolding of definitions, part (6) is [Che18, Proposition 3.2.8], and part (7) is Asada's theorem (see [Che18, Theorem 3.4.2], [BER11], [Asa01, §7]). □

Using Belyi's theorem together with the fact that $\mathcal{M}(1)$ admits a finite étale cover by $\mathbb{P}^1 - \{0, 1, \infty\}$, it follows from Theorem 2.2.2(7) that every algebraic curve over $\overline{\mathbb{Q}}$ is the quotient of a component of $M(G)_{\overline{\mathbb{Q}}}$. In fact, we may say even more:

Theorem 2.2.3. *In the category of finite étale covers of $\mathcal{M}(1)_{\overline{\mathbb{Q}}}$, let $\mathcal{C}$ denote the full subcategory generated by the connected components of $\mathcal{M}(G)_{\overline{\mathbb{Q}}}$. Let C denote the set of isomorphism classes in $\mathcal{C}$. Since $\mathcal{M}(G)$ is defined over $\mathbb{Q}$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\pi_0(\mathcal{M}(G)_{\overline{\mathbb{Q}}})$, and hence on C. This action is* faithful*.*

Moreover, let X be a smooth projective curve over $\overline{\mathbb{Q}}$. Then there is a finite group G and a component $\mathcal{M} \subset \mathcal{M}(G)_{\overline{\mathbb{Q}}}$ such that:

1. *There is a unique minimal subfield $K \subset \overline{\mathbb{Q}}$ such that $\mathcal{M}$ is the base change of a geometrically connected component $\mathcal{M}_K$ of $\mathcal{M}(G)_K$.*
2. *Let M_K be the coarse scheme of $\mathcal{M}_K$, and let $\overline{M_K}$ be its smooth compactification. Then there is a finite group $H \subset \mathrm{Aut}_K(\overline{M_K})$ such that $\overline{M_K}/H \otimes_K \overline{\mathbb{Q}} \cong X$.*

In short, every curve over $\overline{\mathbb{Q}}$ admits a model as a quotient of a component of $M(G)$ *over the field of definition of that component.*

Proof. The faithfulness of the action follows from the rest: if the action had a non-trivial kernel $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$, then every component of $\pi_0(\mathcal{M}(G)_{\overline{\mathbb{Q}}})$ would arise from base change of a component over L. But taking X to be an elliptic curve over $\overline{\mathbb{Q}}$ with j-invariant outside L, X cannot admit a model as quotient of a component $M(G)$ over the field of definition of that component.

To prove (1) and (2), the idea is to combine Belyi's theorem with an explicit version of Asada's theorem due to Ellenberg–Mcreynolds [EM12]. Let X be a smooth projective curve over $\overline{\mathbb{Q}}$. Fix an elliptic curve E over $\mathbb{C}$ and a basis for $\Pi := \pi_1(E^\circ(\mathbb{C}))$, which we use to identify $H_1(E(\mathbb{C}), \mathbb{Z}) \cong \mathbb{Z}^2$ and $\pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}}, E) \cong \widehat{\mathrm{SL}_2(\mathbb{Z})}$. Let $\Gamma(2)' \leq \mathrm{SL}_2(\mathbb{Z})$ be the subgroup generated by $\langle \left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right] \rangle$. Then $\Gamma(2)'$ is a free group which has index 2 inside $\Gamma(2) := \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}))$, and we have $\Gamma(2) = \langle \Gamma(2)', -I \rangle$ where $-I := \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$. Let V be the finite étale covering of $\mathcal{M}(1)_{\overline{\mathbb{Q}}}$ corresponding to (the closure in $\widehat{\mathrm{SL}_2(\mathbb{Z})}$ of) $\Gamma(2)'$. Since $\Gamma(2)'$ is torsion-free, V is a scheme [Che18, Theorem 3.5.3], and by Riemann–Hurwitz applied to the ramification description given in Corollary 2.1.3,

$V \cong \mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0,1,\infty\}$. By Belyi's theorem, there is an open $U \subset X$ together with a finite étale map $U \to V$. Thus, U is finite étale over $\mathcal{M}(1)_{\overline{\mathbb{Q}}}$, and hence corresponds to a finite index subgroup $\Gamma_U \leq \Gamma(2)'$. Let $\Gamma'_U := \langle \Gamma_U, -I\rangle$. Let $\mathcal{U}'$ denote the cover of $\mathcal{M}(1)_{\overline{\mathbb{Q}}}$ corresponding to (the closure of) Γ'_U. Then by Proposition 2.1.2(1) the natural map $U \to \mathcal{U}'$ induces an isomorphism on coarse schemes. By [EM12, Theorem 1.2], Γ'_U is the *Veech group of an origami.* From the description of origami Veech groups given in [Sch04] (specifically Corollary 2.7 and Lemma 2.8(2)), this means that there is an integer d and a permutation group $G \leq S_d$ such that Γ'_U is the stabilizer inside $\mathrm{SL}_2(\mathbb{Z}) \cong \mathrm{Out}^+(\Pi)$ of an element of

$$\mathrm{Epi}^{\mathrm{ext}}(\Pi, G)/N_{S_d}(G)$$

where the normalizer $N_{S_d}(G)$ of G in S_d acts on G by conjugation inside S_d. This implies that $\mathcal{U}'$ is the quotient of a component $\mathcal{M} \subset \mathcal{M}(G)_{\overline{\mathbb{Q}}}$ by the action of $H := N_{S_d}(G)/C_{S_d}(G)$, where $C_{S_d}(G)$ is the centralizer of G in S_d.

Now we address (1). First we define the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action on C. Fix a base point $x : \mathrm{Spec}\,\overline{\mathbb{Q}} \to \mathcal{M}(1)_{\overline{\mathbb{Q}}}$, there is a homotopy exact sequence

$$1 \to \pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}}, x) \to \pi_1(\mathcal{M}(1)_{\mathbb{Q}}, x) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to 1. \tag{2-2-2}$$

Thus the action of $\pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}})$ on the geometric fiber $\pi^{-1}(x)$ of $\pi : \mathcal{M}(G) \to \mathcal{M}(1)$ can be viewed as the restriction of the action of $\pi_1(\mathcal{M}(1)_{\mathbb{Q}})$. Galois theory gives a bijection between $\pi_0(\mathcal{M}(G)_{\overline{\mathbb{Q}}})$ and the set of orbits of the former action, and via the exact sequence (2-2-2), we obtain an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the orbits and hence on $\pi_0(\mathcal{M}(G)_{\overline{\mathbb{Q}}})$. For any other base point x', any isomorphism of the fiber functors associated to x and x' differ by conjugation in $\pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}}, x)$, so this action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\pi_0(\mathcal{M}(G)_{\overline{\mathbb{Q}}})$ is independent of the choice of base point.

We say that a subfield $L \subset \overline{\mathbb{Q}}$ is a field of definition of $\mathcal{M}/\mathcal{M}(1)_{\overline{\mathbb{Q}}}$ if $\mathcal{M} \to \mathcal{M}(1)_{\overline{\mathbb{Q}}}$ is the base change of a cover $\mathcal{M}_L \to \mathcal{M}(1)_L$. We claim that L is a field of definition of $\mathcal{M}/\mathcal{M}(1)_{\overline{\mathbb{Q}}}$ if and only if $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ fixes $\mathcal{M} \in \pi_0(\mathcal{M}(G)_{\overline{\mathbb{Q}}})$. Indeed, let $O \subset \pi^{-1}(x)$ be the $\pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}})$-orbit corresponding to $\mathcal{M}$. If L is a field of definition, then comparing the exact sequence (2-2-2) with the analogous sequence for $\mathcal{M}(1)_L$, we find that the action of $\pi_1(\mathcal{M}(1)_{\mathbb{Q}})$ on $\pi^{-1}(x)$ restricts to a $\pi_1(\mathcal{M}(1)_L)$-action which preserves O. In other words $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ fixes $\mathcal{M}$. Conversely, if $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ fixes $\mathcal{M}$, then we obtain an action of $\pi_1(\mathcal{M}(1)_L)$ on O which by Galois theory corresponds to a finite étale cover of $\mathcal{M}(1)_L$ whose base change to $\mathcal{M}(1)_{\overline{\mathbb{Q}}}$ is $\mathcal{M}$, so L is a field of definition. This establishes our claim, and also shows that the intersection K of all fields of definition (which is also the fixed field of the stabilizer of $\mathcal{M}$ under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) is the unique minimal field of definition. This proves (1).

For (2), the action of H is defined on $\mathcal{M}(G)_{\mathbb{Q}}$, and hence we may form the quotient $\mathcal{M}_K/H$. It follows from Proposition 2.1.2(1) that the coarse scheme of $\mathcal{M}_K/H$ is precisely M_K/H, where M_K is the coarse scheme of $\mathcal{M}_K$. Taking compactifications, we find that $\overline{M_K}/H$ is a K-model of X. □

2.3. **Obtaining tamely ramified 3-point covers.**

Given any connected component $\mathcal{M}$ of $\mathcal{M}(G)_{\overline{\mathbb{Q}}}$, by Theorem 2.2.2(2), we find that the map from its coarse moduli scheme M to the j-line

$$\pi : M \to M(1)_{\overline{\mathbb{Q}}} \cong \mathrm{Spec}\,\overline{\mathbb{Q}}[j]$$

describes a three-point cover with good reduction at all $p \nmid |G|$. The purpose of this section is to show that reduction of this cover to any $p \nmid |G|$ is tamely ramified, i.e. that all ramification indices of π are coprime to $6|G|$. It is an often overlooked consequence of Abhyankar's lemma that when the branch divisor has normal crossings and is mixed characteristic, tameness of the restriction to special fibers is automatic, without having to know anything about the ramification indices of the generic fiber. Nonetheless, after explaining tameness, we also describe the ramification indices in Proposition 2.3.4.

To obtain tameness, we will need the following well-known lemma for which we do not know a reference. (A slightly more general version is stated without proof in the paragraph before [ACV03, §4.2.3].)

Lemma 2.3.1. *Let S be a regular Noetherian scheme. Let $f : X \to S$ be smooth proper morphism. For a normal crossings divisor $D \subset X$ that is smooth over S, let $U := X - D$. Let $\pi : V \to U$ be finite étale, and let Y be the normalization*[7] *of X inside V. Suppose for every maximal point*[8] *$\eta \in D$, the integral closure of $\mathcal{O}_{X,\eta}$ inside the function field of V is tamely ramified over* $\operatorname{Spec} \mathcal{O}_{X,\eta}$.

(1) The natural diagram

$$\begin{tikzcd} V \arrow[r, hook] \arrow[d, "\pi"] & Y \arrow[d, "\overline{\pi}"] \\ U \arrow[r, hook] & X \end{tikzcd}$$

is cartesian, $\overline{\pi}$ is finite flat, Y is smooth over S, and for every $s \in S$ the restriction $\overline{\pi}_{X_s}$ is tamely ramified over D_s.

(2) Let $\tilde{D} \subset Y$ be the reduced closed subscheme corresponding to $\overline{\pi}^{-1}(D)$, then $\tilde{D}$ is finite étale over D. For any irreducible component $Z \subset \tilde{D}$ and any $z, z' \in Z$, the ramification indices of $\overline{\pi}|_{Y_{f(\overline{\pi}(z))}}$ and $\overline{\pi}|_{Y_{f(\overline{\pi}(z'))}}$ at z, z' are the same.

(3) The function $n_{Y/S} : S \to \mathbb{Z}$ counting the number of irreducible components in the geometric fibers of Y/S is locally constant on S.

Note that if S has generic characteristic 0, then the tameness condition (and hence also the consequent tameness in the special fiber) is automatic!

Proof. Since $U \subset X$ is the complement of a normal crossings divisor, $V \to X$ is affine [Sta18, 07ZU], and hence the diagram is cartesian by Zariski's Main Theorem [Sta18, 03GT(1)] . Finiteness of $\overline{\pi}$ follows from [AM69, Proposition 5.17]. Next, for a geometric point $\overline{x}$ lying over a point $x \in D$, let $A := \mathcal{O}^{\mathrm{sh}}_{X,x}$ be the strict henselization of the local ring at x, and let $X_1 := \operatorname{Spec} A$. On X_1, D is cut out by some $g \in A$. By Abhyankar's lemma (see [Sta18, 0EYG] and also [GM71, Corollary 2.3.4]), the restriction $Y_{X_1} \to X_1$ is the disjoint union of covers of the form

$$Y' := \operatorname{Spec} A[T]/(T^e - g) \to X_1 = \operatorname{Spec} A$$

where e is invertible on X_1. This immediately yields the flatness of Y/X, étaleness of $\tilde{D}/D$, the local constancy of ramification indices on D, and the tameness of the restrictions of $\overline{\pi}$ to fibers. This proves all of (1) and (2) except the smoothness of Y over S.

Let $s := f(x)$, and let k be a finite extension of the residue field $k(s)$ of s. Since X/S is smooth, $A \otimes_S k$ is also a regular local ring. Let $\mathfrak{m}$ be its maximal ideal, and let $\overline{g}$ be the image of g in $A \otimes_S k$. Since D is S-smooth, the quotient $(A \otimes_S k)/(\overline{g})$ is also regular, so $\overline{g}$ is a member of a regular sequence of parameters for $A \otimes_S k$ [Sta18, 00NR]. It follows that the rings $(A \otimes_S k)[T]/(T^e - \overline{g})$ are regular where the regular parameter $\overline{g}$ is replaced by T [GM71, Lemma 1.8.6]. Since k was arbitrary, this shows that the normalization Y has geometrically regular fibers. Since $Y \to S$ is flat and finitely presented, we find that Y/S is also smooth [Sta18, 01V8].

[7] This is equivalent to the normalization of X inside the function field of V, which is a finite extension of that of X. See [Sta18, 0BAK] for the definition of relative normalization.

[8] a maximal point is a generic point of an irreducible component

Finally, the local constancy of $n_{Y/S}$ follows from Stein factorization [Sta18, 0E0N], noting that Y/S is smooth, so every connected component is irreducible. □

Using the lemma, we obtain the following procedure for producing tamely ramified 3-point covers using connected components of $\mathcal{M}(G)_{\overline{\mathbb{Q}}_p}$. Given a finite étale morphism $\pi : Y \to X$, we may form the Galois closure: this is a finite étale morphism $\pi' : Y' \to X$ which is Galois [Sta18, 03SF], factors through π, and which is universal with respect to this property. This generalizes the familiar operation of taking the Galois closure of a separable extension of fields.

Proposition 2.3.2. *Let $n \geq 1$ be an integer divisible by 6. Let $\mathcal{M}'$ be a stack finite étale over $\mathcal{M}(1)_{\mathbb{Z}[1/n]}$.*

(1) For each connected component $\mathcal{M}$ of $\mathcal{M}'_{\overline{\mathbb{Q}}}$, there is a connected finite étale $\mathbb{Z}[1/n]$-algebra A such that $\mathcal{M}'_A$ admits an A-section containing the image of $\mathcal{M}$. For any such A, $\mathcal{M}$ extends to a connected component $\mathcal{M}_A$ of $\mathcal{M}'_A$ with geometrically connected fibers.

(2) Let M_A be the coarse moduli scheme of $\mathcal{M}_A$, then M_A comes with a map $\pi : M_A \to M(1)_A \cong \operatorname{Spec} A[j]$, unramified away from $j = 0, 1728$, such that the restrictions of π to the special fibers of $M(1)_A$ are tamely ramified.

(3) Let $K := \operatorname{Frac}(A)$, let $M(1)^\circ_A := M(1)_A - \{j = 0, 1728\}$, and let $M^\circ_A = \pi^{-1}(M(1)^\circ_A)$. For some finite extension L/K the Galois closure N_L of $M^\circ_L \to M(1)^\circ_L$ is geometrically connected. Let B be the integral closure of A in L, and let N_B be the normalization of M°_B inside N_L. Then $N_B \to M(1)^\circ_B$ is the Galois closure of $M^\circ_B \to M(1)^\circ_B$ and has geometrically connected fibers. In particular, the Galois groups of the special fibers of N_B are isomorphic to the Galois group of $N_L \to M(1)^\circ_L$.

(4) Let H be the Galois group of $N_L \to M(1)^\circ_L$ and let $d := \deg(\pi)$. If $H \cong S_d$, then we may take $L = K$ and $B = A$. If $H \cong A_d$, then we may take L to be an at most quadratic extension of K.

Proof. Let D be a $\mathbb{Z}[1/n]$-section of $\mathcal{M}(1)_{\mathbb{Z}[1/n]}$. Since the map $\mathcal{M}'_{\mathbb{Z}[1/n]} \to \mathcal{M}(1)_{\mathbb{Z}[1/n]}$ is finite étale, there is a connected finite étale $\mathbb{Z}[1/n]$-algebra A such that $\mathcal{M}'_A \times_{\mathcal{M}(1)_A} D_A$ is totally split over A. Let $\mathcal{M}_A$ be the connected component of $\mathcal{M}'_A$ containing the image of $\mathcal{M}$; then $\mathcal{M}_A$ is connected and being étale over $\mathcal{M}(1)_A$, its generic fiber is also connected. Since it admits an A-section, its generic fiber is geometrically connected. To see that the closed fibers are geometrically connected, by Theorem 2.2.2(2), it suffices to show this for coarse schemes. Let $\overline{M(1)}_A := \mathbb{P}^1_A$ be the compactification of $M(1)_A$. Because $6 \mid n$, $M(1)^\circ_A \subset \overline{M(1)}_A$ is the complement of a smooth divisor, and hence applying Lemma 2.3.1 to the map $M^\circ_A \to M(1)^\circ_A \subset \overline{M(1)}_A$ we find that the closed fibers are geometrically connected and tamely ramified over the corresponding closed fibers of $\overline{M(1)}_A$. This establishes (1) and (2).

Let N_B be the normalization of $M(1)^\circ_B$ inside N_L. Let $k(N_L)$ be the function field of N_L and P be the Galois closure of $M^\circ_B/M(1)^\circ_B$. Since N_L is a Galois closure of the generic fiber, $k(P)$ is a finite extension of $k(N_L)$. Thus, since every codimension-1 point $x \in M(1)^\circ_B$ is unramified in $k(P)$, it is also unramified in $k(N_L)$. By purity, N_B is étale over M°_B, which shows that N_B is a Galois closure of $M^\circ_B \to M(1)^\circ_B$, so $N_B \cong P$. We are again in the situation of Lemma 2.3.1, from which we find that the special fiber of N_B is geometrically connected (and tamely ramified). This establishes (3).

Finally, we address (4). Let $x : \operatorname{Spec} K \to M(1)^\circ_K$ be a K-point, and let $\overline{x}$ be the corresponding geometric point with values in an algebraic closure $\overline{K}$ of K. Let $\Pi := \pi_1(M(1)^\circ_K, \overline{x})$ and $\overline{\Pi} :=$

$\pi_1(M(1)^\circ_{\overline{K}}, \overline{x})$. The maps $M(1)^\circ_{\overline{K}} \to M(1)^\circ_K \to \operatorname{Spec} K$ induce an exact sequence (see [Sza09, Proposition 5.6.1])

$$1 \to \overline{\Pi} \to \Pi \to \operatorname{Gal}(\overline{K}/K) \to 1$$

which is split by x. Via this splitting, we obtain an isomorphism

$$\Pi \cong \overline{\Pi} \rtimes \operatorname{Gal}(\overline{K}/K). \tag{2-3-1}$$

Let $M^\circ_{\overline{x}}$ denote the geometric fiber of M°_K over $\overline{x}$, which has cardinality $\deg(\pi)$. Galois theory identifies the isomorphism class of the covering $M^\circ_K \to M(1)^\circ_K$ with the equivalence class of the homomorphism

$$\rho : \Pi \to \operatorname{Sym}(M^\circ_{\overline{x}})$$

up to inner automorphisms of $\operatorname{Sym}(M^\circ_{\overline{x}})$. (Here $\operatorname{Sym}(M^\circ_{\overline{x}})$ is the symmetric group on the fiber $M^\circ_{\overline{x}}$.) The image of $\overline{\rho} := \rho|_{\overline{\Pi}}$ is the geometric monodromy group of π, and is isomorphic to H. The kernel of ρ corresponds to the Galois closure of M°_K. If $\overline{\rho}$ surjects onto $\operatorname{Sym}(M^\circ_{\overline{x}})$, then $[\Pi : \ker(\rho)] = [\overline{\Pi} : \ker(\overline{\rho})]$, and hence the Galois closure of M°_K is already geometrically connected, so we may take $L = K$. If the image of $\overline{\rho}$ is the alternating group, then using the decomposition (2-3-1) , we may take L to be the at-most-quadratic extension corresponding to the (at-most-index-2) subgroup

$$\rho^{-1}(\operatorname{Alt}(M^\circ_{\overline{x}})) \cap \operatorname{Gal}(\overline{K}/K) \subset \operatorname{Gal}(\overline{K}/K). \qquad \square$$

Remark 2.3.3. When $H \cong A_d$, the proof of the Proposition 2.3.2(4) gives a necessary and sufficient condition on when we may take $L = K$ in terms of the $\operatorname{Gal}(\overline{K}/K)$-action on the fiber $M^\circ_{\overline{x}}$: we must have $\rho^{-1}(\operatorname{Alt}(M^\circ_{\overline{x}})) \cap \operatorname{Gal}(\overline{K}/K) = \operatorname{Gal}(\overline{K}/K)$. Thus when K is a finite field, we may take $L = K$ when the action of the Frobenius on the fiber is even, while we must use a quadratic extension when the action of the Frobenius on the fiber is odd.

For a general finite étale map of stacks $\mathcal{M} \to \mathcal{M}(1)_{\overline{\mathbb{Q}}}$, the ramification of the map on coarse schemes is described by Corollary 2.1.3. Here we spell out what it means combinatorially when $\mathcal{M} = \mathcal{M}(G)_{\overline{\mathbb{Q}}}$ for a finite group G.

Let E be an elliptic curve over $\mathbb{C}$ with j-invariant not 0 or 1728. Fix an embedding $i : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Using i, we will view E as a geometric point of both $\mathcal{M}(1)_{\overline{\mathbb{Q}}}$ and $M(1)_{\overline{\mathbb{Q}}}$. Let $x_0 \in E^\circ(\mathbb{C})$ and $\Pi := \pi_1^{\mathrm{top}}(E^\circ(\mathbb{C}), x_0)$. Let x, y be a basis for Π with intersection number $+1$. Consider the four automorphisms of Π:

$$\gamma_0 : (x,y) \mapsto (xy^{-1}, x) \quad \gamma_{1728} : (x,y) \mapsto (y^{-1}, x), \quad \gamma_\infty : (x,y) \mapsto (x, xy) \quad \gamma_{-I} : (x,y) \mapsto (x^{-1}, y^{-1}).$$

Since γ_{-I} is central in $\operatorname{Out}(\Pi) \cong \mathrm{GL}_2(\mathbb{Z})$, the natural action of $\operatorname{Aut}(\Pi)$ on $\operatorname{Epi}(\Pi, G)$ descends to an action of $\operatorname{Aut}(\Pi)$ on the set

$$\tilde{F}(G) := \operatorname{Epi}^{\mathrm{ext}}(\Pi, G)/\langle \gamma_{-I} \rangle$$

which visibly factors through $\operatorname{Out}(\Pi)/\langle \gamma_{-I} \rangle \cong \mathrm{PGL}_2(\mathbb{Z})$. Let $\overline{M(G)}_{\overline{\mathbb{Q}}}$ and $\overline{M(1)}_{\overline{\mathbb{Q}}}$ be the smooth compactifications of $M(G)_{\overline{\mathbb{Q}}}$ and $M(1)_{\overline{\mathbb{Q}}}$ respectively. Using the bijection of Theorem 2.2.2(4) and taking coarse schemes, we may identify the fiber of $\overline{M(G)}_{\overline{\mathbb{Q}}} \to \overline{M(1)}_{\overline{\mathbb{Q}}}$ above E with $\tilde{F}(G)$, and the fibers above $j = 0, 1728, \infty$ with the quotient sets

$$\tilde{F}(G)/\langle \gamma_0 \rangle, \quad \tilde{F}(G)/\langle \gamma_{1728} \rangle, \quad \tilde{F}(G)/\langle \gamma_\infty \rangle$$

respectively, such that the ramification indices at each point correspond to the size of the its orbit under γ_0, γ_{1728}, or γ_∞ respectively in $\tilde{F}(G)$. Let $e(G)$ denote the least positive integer n satisfying $g^n = 1$ for all $g \in G$.

Proposition 2.3.4. *With the notation of the preceding paragraphs, the ramification indices of* $\overline{M(G)}_{\overline{\mathbb{Q}}} \to \overline{M(1)}_{\overline{\mathbb{Q}}}$ *all divide* $6 \cdot e(G)$*. Specifically, the ramification indices above* $j = 0$ *all divide 3, and the ramification indices above* $j = 1728$ *all divide 2, and the ramification indices of* π *above* $j = \infty$ *all divide* $e(G)$*.*

Proof. First note that relative to the isomorphism $\mathrm{Out}(\Pi) \cong \mathrm{GL}_2(\mathbb{Z})$ induced by the basis x, y, the automorphisms $\gamma_0, \gamma_{1728}, \gamma_\infty, \gamma_{-I}$ viewed inside $\mathrm{Out}(\Pi)$ correspond to the matrices

$$\left[\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right].$$

Also note that the action of γ_{-I} (resp. $\left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$) on Π (resp. $H_1(E(\mathbb{C}), \mathbb{Z})$) is induced by the automorphism $[-1]$ of E. If every instance of $\overline{\mathbb{Q}}$ in the statement is replaced by $\mathbb{C}$, then using standard GAGA arguments (see [Noo05, Theorem 20.4]), the descriptions of the fibers follow from Theorem 2.2.2(4) together with Proposition 2.1.2 and Corollary 2.1.3. Since γ_0 (resp. γ_{1728}) has order 3 (resp. 2) in $\mathrm{Out}(\Pi)/\langle\gamma_{-I}\rangle$, the ramification indices above $j = 0$ (resp. $j = 1728$) must divide 3 (resp. 2). Finally, note that γ_∞ must act on $\tilde{F}(G)$ with order dividing $e(G)$.

To pass from $\mathbb{C}$ to $\overline{\mathbb{Q}}$ we use Remark 2.2.1(4) plus "coarse base change" in characteristic 0 [Che18, Proposition 3.3.4]. □

2.4. **Absolute G-structures.** There is a natural action of $\mathrm{Aut}(G)$ on $\mathcal{M}(G)$ which factors through a free action of $\mathrm{Out}(G)$. Thus the quotient $\mathcal{M}(G)/\mathrm{Out}(G)$ is also finite étale over $\mathcal{M}(1)$ and we will denote it by[9]

$$\mathcal{M}(G)^{\mathrm{abs}} := \mathcal{M}(G)/\mathrm{Out}(G).$$

For an elliptic curve E over a $\mathbb{Z}[1/|G|]$-scheme S corresponding to a map $E : S \to \mathcal{M}(1)$, a section of the finite étale S-scheme $S \times_{\mathcal{M}(1)} \mathcal{M}(G)^{\mathrm{abs}}$ is called an *absolute G-structure* on E; $\mathcal{M}(G)^{\mathrm{abs}}$ is then the moduli stack of elliptic curves with absolute G-structures. In the notation of Theorem 2.2.2(3), the set of absolute G-structures is in bijection with the set:

$$\{\varphi \in \mathrm{Epi}^{\mathrm{ext}}(\pi_1^{\mathbb{L}}(E_s^\circ, x), G)/\mathrm{Out}(G) \mid \varphi \circ \rho_{E,x}(\sigma) = \varphi \quad \text{for all } \sigma \in \pi_1(S, s)\}$$

As before, φ is an equivalence class of surjections to G (in this case, an $\mathrm{Aut}(G)$-orbit), and an absolute G-structure is given by an equivalence class which is stabilized by the action of $\pi_1(S, s)$.

We may also give a geometric description of absolute G-structures. Given a scheme S and an elliptic curve E/S with zero section O, let $E^\circ := E - O$. A *mere G-cover*[10] of E° is a finite étale map $\pi : X \to E^\circ$ whose geometric fibers over S are connected, and such that $\mathrm{Aut}(\pi)$ is isomorphic to G. A morphism of mere G-covers of E° is a morphism in the category $\mathbf{Sch}/E^\circ$. In particular we do not specify a G-action on X and hence we do not require that morphisms be G-equivariant. Let $\mathcal{T}_G^{\mathrm{abs,pre}} : \mathcal{M}(1) \to \mathbf{Sets}$ be the presheaf which associates to an elliptic curve E/S the set of isomorphism classes of mere G-covers of E°. Then $\mathcal{M}(G)^{\mathrm{abs}}$ is isomorphic to the stack obtained from the sheafification of $\mathcal{T}_G^{\mathrm{abs,pre}}$ in the étale topology. Thus, informally speaking an absolute G-structure on E/S is given by the data of mere G-covers defined étale locally on S whose common restrictions are isomorphic, but with no requirement that the isomorphisms satisfy the cocycle condition.

Remark 2.4.1. Note that if $\pi : X \to E^\circ$ is finite étale, geometrically connected over S, and such that there is a surjective étale map $S' \to S$ such that the pullback $X_{S'} \to E^\circ_{S'}$ is Galois, then π

[9] Here, the superscript abs is short for "absolute", and the distinction between $\mathcal{M}(G)$ and $\mathcal{M}(G)^{\mathrm{abs}}$ is analogous to Fried's distinction between "inner" and "absolute" Hurwitz stacks (see [Ber13] Remark 4.56).

[10] We use the word "mere" in a similar way as [DD97].

defines an absolute G-structure on E/S even though π itself may not have enough automorphisms to be Galois.

We now make this concrete in the case that $G = \mathrm{SL}_2(\mathbb{F}_\ell)$ and $G = \mathrm{PSL}_2(\mathbb{F}_\ell) := \mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm I\}$. The main point is that as equivalence classes of $\mathrm{SL}_2(\mathbb{F}_\ell)$ or $\mathrm{PSL}_2(\mathbb{F}_\ell)$-structures, the equivalence relation is given by conjugation in $\mathrm{SL}_2(\overline{\mathbb{F}}_\ell)$ or $\mathrm{PSL}_2(\overline{\mathbb{F}}_\ell)$, and hence it will make sense to speak of the trace of the monodromy given by a generator of inertia in the fundamental group of a punctured elliptic curve (see §2.5 below).

Fix a prime ℓ, let $N_{\mathrm{SL}_2(\overline{\mathbb{F}}_\ell)}(\mathrm{SL}_2(\mathbb{F}_\ell))$ be the normalizer of $\mathrm{SL}_2(\mathbb{F}_\ell)$ in $\mathrm{SL}_2(\overline{\mathbb{F}}_\ell)$ and define

$$D(\ell) := N_{\mathrm{SL}_2(\overline{\mathbb{F}}_\ell)}(\mathrm{SL}_2(\mathbb{F}_\ell))/\,\mathrm{SL}_2(\mathbb{F}_\ell). \tag{2-4-1}$$

It can be shown that for $\ell = 2$, $D(\ell)$ is trivial, and for odd ℓ, $D(\ell)$ is a cyclic group of order two, generated by any matrix of the form $\left[\begin{smallmatrix} u & 0 \\ 0 & u^{-1}\end{smallmatrix}\right]$ where $u \in \overline{\mathbb{F}}_\ell - \mathbb{F}_\ell$ with $u^2 \in \mathbb{F}_\ell$. Let F_2 denote the free group of rank 2. Thus $D(\ell)$ acts on $\mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{SL}_2(\mathbb{F}_\ell))$ by conjugation, and its action commutes with the action of $\mathrm{Out}(F_2)$, so $\mathrm{Out}(F_2)$ also acts on

$$F(\ell) := \mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{SL}_2(\mathbb{F}_\ell))/D(\ell). \tag{2-4-2}$$

Since $\{\pm I\}$ is the center of $\mathrm{SL}_2(\mathbb{F}_\ell)$, $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is a characteristic quotient and hence $D(\ell)$ acts on $\mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{PSL}_2(\mathbb{F}_\ell))$, and again its action commutes with the action of $\mathrm{Out}(F_2)$. Thus as before $\mathrm{Out}(F_2)$ also acts on

$$\overline{F(\ell)} := \mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{PSL}_2(\mathbb{F}_\ell))/D(\ell). \tag{2-4-3}$$

It follows from [Ste16, Theorem 30] (noting that there are no field and graph automorphisms for $\mathrm{SL}_2(\mathbb{F}_\ell)$) that $\mathrm{Out}(\mathrm{SL}_2(\mathbb{F}_\ell))$ has order 2 for odd ℓ and is trivial otherwise. Thus, $D(\ell)$ induces the full outer automorphism group of $\mathrm{SL}_2(\mathbb{F}_\ell)$. Indeed, if $\ell = 2$, $D(2) = \mathrm{Out}(\mathrm{SL}_2(\mathbb{F}_2)) = 1$; if ℓ is odd, then if A represents the nontrivial element of $D(\ell)$, then conjugation by A cannot be an inner automorphism, for otherwise $AB = \pm I$ for some $B \in \mathrm{SL}_2(\mathbb{F}_\ell)$, which is absurd. Similarly, $\mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_\ell))$ also has order 2 for ℓ odd, so we find that $D(\ell)$ also induces the full outer automorphism group of $\mathrm{PSL}_2(\mathbb{F}_\ell)$. Translating this into our geometric setting gives:

Proposition 2.4.2. *We have that* $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))/D(\ell) = \mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$ *and* $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))/D(\ell) = \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$. *The characteristic quotient* $\mathrm{SL}_2(\mathbb{F}_\ell) \to \mathrm{PSL}_2(\mathbb{F}_\ell)$ *induces a commutative diagram of* $\mathrm{Out}(F_2)$*-equivariant maps*

$$\begin{tikzcd} \mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{SL}_2(\mathbb{F}_\ell)) \arrow[r] \arrow[d] & \mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{PSL}_2(\mathbb{F}_\ell)) \arrow[d] \\ F(\ell) \arrow[r] & \overline{F(\ell)} \end{tikzcd} \tag{2-4-4}$$

For any elliptic curve E over $\mathbb{C}$, $x_0 \in E$, fix an isomorphism $\pi_1^{top}(E^\circ(\mathbb{C}), x_0) \cong F_2$, yielding isomorphisms $\pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}}, E) \cong \widehat{\mathrm{Out}^+(F_2)} \simeq \widehat{\mathrm{SL}_2(\mathbb{Z})}$ as in Theorem 2.2.2(5). Relative to these isomorphisms, the monodromy action of $\pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}})$ on the geometric fiber of $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$ (resp. $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$) over E corresponds to the $\mathrm{Out}^+(F_2)$-action on $F(\ell)$ (resp. $\overline{F(\ell)}$).

In particular, the diagram (2-4-4) induces the following diagram of in the category of finite étale stacks over $\mathcal{M}(1)_{\mathbb{Z}[1/|\operatorname{SL}_2(\mathbb{F}_\ell)|]}$.

$$\begin{tikzcd}
\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell)) \arrow[r] \arrow[d] & \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell)) \arrow[d] \\
\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}} \arrow[r] & \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}
\end{tikzcd}$$

Proof. This follows from the above discussion and Theorem 2.2.2. □

2.5. **The Higman and trace invariants.**

In this section we will define the trace invariant of an absolute $\mathrm{SL}_2(\mathbb{F}_\ell)$ (resp. $\mathrm{PSL}_2(\mathbb{F}_\ell)$)-structure on an elliptic curve, which is derived from the finer Higman invariant. The Higman invariant can be defined for general G-structures, and in the case of a covering of an elliptic curve branched only over the origin, it is equivalent to the "Hurwitz datum" associated to a branched Galois covering of curves (see [BR11, §2.2]).

The Higman invariant geometrically. Let G be a finite group. The stacks $\mathcal{M}(G)_{\mathbb{C}}$ are generally not connected. One can often distinguish connected components of $\mathcal{M}(G)_{\mathbb{C}}$ using the *Higman invariant*. Analytically, given a G-torsor over a complex-analytic elliptic curve E, the monodromy around a small positively oriented loop on E winding once around the puncture determines a conjugacy class of G, which we call the Higman invariant of the torsor. Note that such a loop represents the commutator of a positively oriented basis of $\pi_1(E^\circ)$. Since the mapping class group of the torus must preserve the homotopy class of this loop, the Higman invariant is locally constant on $\mathcal{M}(G)_{\mathbb{C}}$.

Algebraically, let E be an elliptic curve over an algebraically closed field k of characteristic prime to $|G|$. Let $f^\circ : X^\circ \to E^\circ$ be a G-torsor, and let $f : X \to E$ be the extension of f to a finite map of smooth proper curves. Then the action of G extends to X and acts transitively on the fibers of f, in particular on the fiber X_O above the puncture $O \in E$. For any point $x \in X_O$, the inertia group $G_x := \mathrm{Stab}_G(x)$ is cyclic of order equal to the ramification index at x. Let T_x be the Zariski tangent space at x. Since G_x acts freely on $\mathcal{O}_{X,x}$, we obtain an injective local monodromy representation

$$\rho_x : G_x \hookrightarrow \mathrm{GL}(T_x).$$

Since T_x is a 1-dimensional k-vector space, $\mathrm{GL}(T_x) \cong k^\times$ canonically and hence ρ_x identifies G_x with the group of e-th roots of unity in k. If we make a choice of a primitive e-th root of unity $\zeta \in k$, then we may define the Higman invariant[11] of f (relative to ζ) to be the set

$$\{\rho_x^{-1}(\zeta) \bigm| x \in X_O\}.$$

Since G acts transitively on X_O, this set is a conjugacy class of G. In some situations it is useful to speak of the Higman invariant relative to a primitive nth root of unity ζ_n where $e \mid n$. In that case the Higman invariant of a torsor with ramification index e relative to ζ_n is by definition the Higman invariant relative to $\zeta_n^{n/e}$.

The Higman invariant is locally constant. This is shown for example in [BR11, Proposition 3.2.5] for Hurwitz data, but for completeness we give an argument here.

Proposition 2.5.1. *Let $n := |G|$, and let ζ_n be any primitive nth root of unity in $\mathbb{C}$. Then the Higman invariant relative to ζ_n is locally constant on $\mathcal{M}(G)_{\mathbb{Z}[1/n,\zeta_n]}$.*

[11] By the Chevalley-Weil formula, this Higman invariant also determines the Hurwitz representations associated to the cover, and conversely by [BR11, §3.2] the Hurwitz representations also determine the Higman invariant.

Proof. For any geometric point $x : \operatorname{Spec} k \to \mathcal{M}(G)_{\mathbb{Z}[1/n,\zeta_n]}$, let $U \to \mathcal{M}(G)_{\mathbb{Z}[1/n,\zeta_n]}$ be a connected étale neighborhood of x, corresponding to an elliptic curve E/U with G-structure. Possibly passing to a further étale localization, we may assume that the G-structure is given by a G-torsor $f^\circ : X^\circ \to E^\circ$. Since U is regular, applying Lemma 2.3.1, we may extend f° to a branched G-cover $f : X \to E$ of smooth proper curves, branched only above the zero section of E, such that the reduced ramification divisor is étale over the zero section of E. Étale localizing even more, we may assume the reduced ramification divisor is a disjoint union of copies of U. Let $D \subset X$ be a component of the reduced ramification divisor, with ideal sheaf $\mathcal{I}$. Then the conormal sheaf $\mathcal{I}/\mathcal{I}^2$ is invertible on D, and viewing G as a constant group scheme over U, the action of $G_D := \operatorname{Stab}_G(D) \subset G$ on D gives a homomorphism of constant U-group schemes

$$\rho : G_D \to \underline{\operatorname{Aut}}_D((\mathcal{I}/\mathcal{I}^2)^\vee) \cong \underline{\operatorname{Aut}}_U((\mathcal{I}_U/\mathcal{I}_U^2)^\vee) \cong \underline{\operatorname{Aut}}_U(\mathcal{O}_U) \cong \mathcal{O}_U^\times$$

where the isomorphisms are canonical. Thus the image of ρ is necessarily contained in the subgroup scheme $(\mu_n)_U$. For geometric points $s \in U$, the restrictions $\rho|_{(G_D)_s}$ (taken up to conjugacy in G_s) give precisely the Hurwitz data of the restrictions $f_s : X_s \to E_s$, and the preimages $\rho_s^{-1}(\zeta_n)$ give precisely the Higman invariants of f_s. Since ρ was a homomorphism of constant group schemes, this establishes the local constancy of the Higman invariant. □

Higman invariants on $\mathcal{M}(G)$. For a conjugacy class $C \subset G$, we wish to speak of the open and closed substacks of $\mathcal{M}(G)$ having "Higman invariant C". For this to make sense, we must understand the "ring of definition" of a conjugacy class.

In this section let k be any field of characteristic prime to $|G|$, not necessarily algebraically closed. Let $x : \operatorname{Spec} k \to \mathcal{M}(G)$ be a point corresponding to a G-structure on an elliptic curve E/k. If $\iota : k \hookrightarrow \overline{k}$ is an algebraic closure, and $\zeta_e \in \overline{k}$ is a primitive eth root of unity, then the point

$$\overline{x} : \operatorname{Spec} \overline{k} \xrightarrow{\operatorname{Spec} \iota} \operatorname{Spec} k \xrightarrow{x} \mathcal{M}(G)$$

corresponds to an actual G-torsor over an elliptic curve branched only over the origin. Thus, it makes sense to consider the Higman invariant of $\overline{x}$ relative to ζ_e^i for i coprime to e. If the Higman invariant of $\overline{x}$ relative to ζ_e is C (a conjugacy class of G), then the Higman invariant of $\overline{x}$ relative to ζ_e^i is C^i.

Suppose $S \subset G$ is a conjugation-stable subset consisting of elements of the same order e (a union of conjugacy classes of order e). Let $\mathbb{F}$ be the prime subfield of k, and let $\mathbb{F}(e)$ denote the minimal extension of $\mathbb{F}$ containing a primitive eth root of unity. Let $\chi_e : \operatorname{Gal}(\mathbb{F}(e)/\mathbb{F}) \to (\mathbb{Z}/e\mathbb{Z})^\times$ be the cyclotomic character. For any integer i, let $S^i := \{s^i : s \in S\}$ and let $R(S) := \{S^i : i \text{ is coprime to } e\}$. Note $R(S)$ is a set of conjugation-stable subsets of G, and that for any i, $S^i \cap S$ is either empty or a union of conjugacy classes. The group $(\mathbb{Z}/e\mathbb{Z})^\times$ naturally acts on primitive eth roots of unity, and we similarly define an action on $R(S)$ by

$$\begin{array}{rrcl} \text{(2-5-1)} \qquad & \rho_S : (\mathbb{Z}/e\mathbb{Z})^\times & \longrightarrow & \operatorname{Sym}(R(S)) \\ & i & \longmapsto & \left(S \mapsto S^i\right). \end{array}$$

Define $\rho_{\mathbb{F},S} : \operatorname{Gal}(\mathbb{F}(e)/\mathbb{F}) \to \operatorname{Sym}(R(S))$ by $\rho_{\mathbb{F},S} := \rho_S \circ \chi_e$, and (for any prime field $\mathbb{F}$) let $\mathbb{F}(S) \subset \mathbb{F}(e)$ be the fixed field of $\ker(\rho_{\mathbb{F},S})$. Suppose we are given an embedding $\mathbb{F}(S) \hookrightarrow k$; for example this will be the case if x is a point of $\mathcal{M}(G)_{\mathbb{F}(S)}$.

Definition 2.5.2. Keeping the notation as above, let $\mu_e/\mathbb{F}(S)$ denote the group scheme which is the kernel of the eth power map on $\mathbb{G}_{m,\mathbb{F}(S)}$. Its automorphism group is canonically isomorphic to $(\mathbb{Z}/e\mathbb{Z})^\times$. Let $\mu_{e,S,\mathbb{F}}$ denote the set of $\ker(\rho_S)$-orbits of closed points of order e in the group scheme μ_e over $\mathbb{F}(S)$. We will think of $\mu_{e,S,\mathbb{F}}$ as a collection of closed subschemes of the group scheme $\mu_e/\mathbb{F}(S)$.

Remark 2.5.3. Explicitly, a choice of $\omega \in \mu_{e,S,\mathbb{F}}$ amounts to a $\ker(\rho_S)$-orbit of primitive e-th roots of unity in $\mathbb{F}(e)$. There are two extreme cases. If ρ_S is faithful (the sets S^i are all distinct for $i \in (\mathbb{Z}/e\mathbb{Z})^\times$), then $\mathbb{F}(S) = \mathbb{F}(\zeta_e)$ and the closed points of μ_e are $\mathbb{F}(S)$-points, and in this case choosing ω is equivalent to choosing a primitive e-th root of unity. In the other extreme, if ρ_S is trivial ($S^i = S$ for every i coprime to e), then $\mathbb{F}(S) = \mathbb{F}$, $\ker(\rho_S) = \mathrm{Aut}(\mu_e) = (\mathbb{Z}/e\mathbb{Z})^\times$, and there is only one choice of ω, namely the closed subscheme corresponding to the collection of all primitive eth roots of unity. We think of $\mathbb{F}(S)$ as the "field of definition" of S.

Lemma 2.5.4. *Suppose $S \subset G$ is a conjugacy-stable set consisting of elements of the same order e. Let $\omega \in \mu_{e,S,\mathbb{F}}$ be an orbit, and let $x : \operatorname{Spec} k \to \mathcal{M}(G)$ be a point. Suppose we are given an embedding $\mathbb{F}(S) \hookrightarrow k$. The following are equivalent:*

(a) For some algebraic closure $\iota : k \hookrightarrow \overline{k}$ and some morphism

$$z : \operatorname{Spec} \overline{k} \to \omega$$

of $\operatorname{Spec} \mathbb{F}(S)$-schemes with corresponding primitive eth root of unity $\zeta_e \in \overline{k}$, the Higman invariant of $\overline{x} := x \circ \operatorname{Spec}(\iota)$ relative to ζ_e is contained in S.

(b) For any *algebraic closure $\iota : k \hookrightarrow \overline{k}$ and any morphism*

$$z : \operatorname{Spec} \overline{k} \to \omega$$

of $\operatorname{Spec} \mathbb{F}(S)$-schemes with corresponding primitive eth root of unity $\zeta_e \in \overline{k}$, the Higman invariant of $\overline{x} := x \circ \operatorname{Spec}(\iota)$ relative to ζ_e is contained in S.

Proof. The key point is that if z' is another $\overline{k}$-point of ω, corresponding to a root of unity $\zeta'_e \in \overline{k}$, then because z, z' are morphisms of $\operatorname{Spec} \mathbb{F}(S)$-schemes, they differ by some $\sigma \in \mathrm{Gal}(\overline{k}/\mathbb{F}(S))$, so $\zeta'_e = \zeta_e^i$ for some $i \in \ker(\rho_S)$ by definition of $\mathbb{F}(S)$. If $C \subset S$ is the Higman invariant of $\overline{x}$ relative to ζ_e, then $C^i \subset S^i$ is the Higman invariant relative to ζ'_e, but as $i \in \ker(\rho_S)$, $S^i = S$, and hence the Higman invariant lies in S. A similar argument also implies independence of the choice of algebraic closure. □

When any of the equivalent conditions in Lemma 2.5.4 are satisfied for a conjugation-stable set of elements of the same order e, we say that *x has Higman invariant in S relative to ω.*

Now let $\mathcal{O}_{\mathbb{Q}(S)}$ be the ring of integers of $\mathbb{Q}(S)$; for any prime $\mathfrak{p} \subset \mathcal{O}_{\mathbb{Q}(S)}[1/|G|]$ lying above $(p) \subset \mathbb{Z}$, the residue field $k(\mathfrak{p})$ is equal to $\mathbb{F}_p(S)$. Moreover, for any $\omega \in \mu_{e,S,\mathbb{Q}}$, ω uniquely extends to a closed subscheme of the group scheme μ_e over $\mathcal{O}_{\mathbb{Q}(S)}[1/|G|]$, and its fiber over a prime $\mathfrak{p} \subset \mathcal{O}_{\mathbb{Q}(S)}[1/|G|]$ is an element of $\mu_{E,S,k(\mathfrak{p})}$, which we will call the *reduction of ω mod $\mathfrak{p}$*. By the above discussion together with local constancy, the following definition makes sense:

Definition 2.5.5. Let $S \subset G$ be a union of conjugacy classes of order e. Let $\omega \in \mu_{e,S,\mathbb{Q}}$. Given a point $x : \operatorname{Spec} k \to \mathcal{M}(G)_{\mathcal{O}_{\mathbb{Q}(S)}[1/|G|]}$ lying over a prime $\mathfrak{p} \subset \mathcal{O}_{\mathbb{Q}(S)}[1/|G|]$, we say that x has Higman invariant in S relative to ω if it has Higman invariant in S relative to the reduction of ω mod $\mathfrak{p}$. Given a connected scheme B and a map $f : B \to \mathcal{M}(G)_{\mathcal{O}_{\mathbb{Q}(S)}[1/|G|]}$, we will say that it has Higman invariant in S relative to ω if for some (equivalently any) point $b \in B$, the map $b \hookrightarrow B \xrightarrow{f} \mathcal{M}(G)_{\mathcal{O}_{\mathbb{Q}(S)}[1/|G|]}$ has Higman invariant in S relative to ω. If we do not specify ω, then it will be understood that we take ω to be the orbit of $\exp(2\pi i/e)$ relative to our fixed embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$.

In particular, $\mathbb{Q}(S) \subset \mathbb{Q}(\zeta_e)$ is an abelian number field, and the substack of $\mathcal{M}(G)_{\mathcal{O}_{\mathbb{Q}(S)}[1/|G|]}$ consisting of objects with Higman invariant in S relative to ω is open and closed.

Remark 2.5.6. If $k = \mathbb{C}$, since the local picture at a ramified point is given by $z \mapsto z^e$, we may check that in this case the Higman invariant defined analytically for $E(\mathbb{C})$ agrees with the Higman invariant defined for E relative to $\exp(2\pi i/e)$.[12]

The Higman invariant algebraically. By Theorem 2.2.2(4), for any elliptic curve E over $\overline{\mathbb{Q}}$ with mapping class group $\Gamma_E := \Gamma_{E(\mathbb{C})}$ and base point $x_0 \in E^\circ(\mathbb{C})$, the connected components of $\mathcal{M}(G)_{\overline{\mathbb{Q}}}$ are in bijection with the Γ_E-orbits on the set

$$\mathrm{Epi}^{\mathrm{ext}}(\pi_1^{top}(E^\circ(\mathbb{C}), x_0), G).$$

Fixing a basis for the fundamental group with intersection number $+1$ (a "positively oriented basis"), we may identify $\pi_1^{top}(E^\circ(\mathbb{C}), x_0)$ with the free group F_2 on two generators a, b, and Γ_E with $\mathrm{Out}^+(F_2)$ (see Theorem 2.2.2(5)). Under this identification, a positively oriented generator of inertia around O is given by the commutator $[a, b]$. Thus, the Higman invariant of the G-torsor corresponding to (the conjugacy class of) a homomorphism $\varphi : F_2 \to G$ is the conjugacy class of the commutator $[\varphi(a), \varphi(b)]$. This class is an invariant of the $\mathrm{Out}^+(F_2)$ action on the set

$$\mathrm{Epi}^{\mathrm{ext}}(F_2, G)$$

and correspondingly it does not depend on the choice of positively oriented basis a, b. Abstractly, if F_2 is the free group on a, b, then we define the Higman invariant of an element of $\mathrm{Epi}^{\mathrm{ext}}(F_2, G)$ to be the conjugacy class of $\varphi([a, b]) = [\varphi(a), \varphi(b)]$.

The trace invariant. We now specialize to the cases of $G = \mathrm{SL}_2(\mathbb{F}_\ell)$ and $G = \mathrm{PSL}_2(\mathbb{F}_\ell)$ for ℓ prime.

Definition 2.5.7. Let F_2 be the free group on generators a, b. Given a homomorphism $\varphi : F_2 \to \mathrm{SL}_2(\mathbb{F}_\ell)$, the *trace invariant* of φ is $\mathrm{tr}([\varphi(a), \varphi(b)])$. For a homomorphism $\varphi : F_2 \to \mathrm{PSL}_2(\mathbb{F}_\ell)$, its trace invariant is defined to be $\mathrm{tr}([A, B])$ where $A, B \in \mathrm{SL}_2(\mathbb{F}_\ell)$ are any lifts of $\varphi(a)$ and $\varphi(b)$.

Remark 2.5.8. Since the kernel of $\mathrm{SL}_2(\mathbb{F}_\ell) \to \mathrm{PSL}_2(\mathbb{F}_\ell)$ is central, the trace invariant for $\varphi : F_2 \to \mathrm{PSL}_2(\mathbb{F}_\ell)$ is well-defined on $\mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{PSL}_2(\mathbb{F}_\ell))$ and is independent of the choice of lifts. Moreover, the trace invariant is invariant under the actions of $\mathrm{Out}^+(F_2)$ and $D(\ell)$ on $\mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{SL}_2(\mathbb{F}_\ell))$, and likewise for $\mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{PSL}_2(\mathbb{F}_\ell))$.

Geometrically, we will define:

Definition 2.5.9. Given a point $x : \mathrm{Spec}\,\overline{\mathbb{Q}} \to \mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))_{\overline{\mathbb{Q}}}$, its *trace invariant* is the trace of its Higman invariant. For a point $y \in \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))_{\overline{\mathbb{Q}}}$, its trace invariant is the trace of the Higman invariant of any lift of y to a point of $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))_{\overline{\mathbb{Q}}}$. Such lifts are guaranteed to exist by Theorem 2.2.2(6), and the resulting trace is well-defined by Remark 2.5.8.

For $t \in \mathbb{F}_\ell$, let

$$S(t) := \{A \in \mathrm{SL}_2(\mathbb{F}_\ell) \mid \mathrm{tr}(A) = t, A \neq \pm I\} \tag{2-5-2}$$

By [MW13, Proposition 5.1], $S(t)$ is a union of conjugacy classes of the same order e. Let $n_\ell := |\mathrm{SL}_2(\mathbb{F}_\ell)|$. We will say that an object of $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))_{\mathcal{O}_{\mathbb{Q}(S(t))}[1/n_\ell]}$ has trace invariant t if it has Higman invariant in $S(t)$. Given an object $B \to \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))_{\mathcal{O}_{\mathbb{Q}(S(t))}[1/n_\ell]}$, we say that it has trace invariant t if for some geometric point $b \in B$, there is a lift of b to $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))_{\mathcal{O}_{\mathbb{Q}(S(t))}[1/n_\ell]}$ which

[12] In the analytic setting, the choice of root of unity was implicitly defined by an orientation, which can be thought of as a choice of generator of the fundamental group of a punctured neighborhood of $O \in E(\mathbb{C})$. Varying the group G, this orientation implicitly makes the choices of roots of unity $\zeta_e := \exp(2\pi i/e)$ which are compatible in the sense that $\zeta_e^r = \zeta_{e/r}$ for any $r \mid e$. If $k = \overline{\mathbb{Q}}$, such a system can be thought of as an "étale orientation" on $E/\overline{\mathbb{Q}}$.

has trace invariant t. For the same reasons as above such lifts exist and the resulting trace is well-defined.

The local constancy of the Higman invariant implies the local constancy of the trace invariant. Thus, for any $\mathcal{O}_{\mathbb{Q}(S(t))}[1/n_\ell]$-algebra A, we obtain open and closed substacks

$$\begin{aligned}\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))_{t,A} &\subset \mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))_A\\ \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))_{t,A} &\subset \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))_A\end{aligned}$$

consisting of objects of trace invariant t. As with the Higman invariant, one may check that the algebraic version of the trace invariant agrees with the geometric version in characteristic 0 if one fixes an isomorphism $F_2 \cong \pi_1^{\mathrm{top}}(E^\circ(\mathbb{C}), x_0)$ sending a, b to a positively oriented basis.

Remark 2.5.10. Note that since $\mathrm{SL}_2(\mathbb{F}_\ell)$ is never abelian and the Higman invariant is the commutator of a generating pair, it cannot be contained in any proper normal subgroup. Thus in Definition 2.5.9, nothing is lost by excluding $\pm I$ from $S(t)$.

3. Markoff triples as level structures on elliptic curves

The *Markoff surface* is the surface $\mathbb{X}$ (over $\mathbb{Z}$) given by the equation

$$x^2 + y^2 + z^2 - xyz = 0. \tag{3-0-1}$$

A Markoff triple is a solution to this equation.

For any prime ℓ, let $X(\ell) := \mathbb{X}(\mathbb{F}_\ell)$ and $X^*(\ell) := X(\ell) - \{(0,0,0)\}$.

In this section we will explain how for $\ell \geq 3$, the set $X^*(\ell)$ is in bijection with the set of absolute $\mathrm{SL}_2(\mathbb{F}_\ell)$-structures on an elliptic curve with trace invariant -2. Under this correspondence (Proposition 3.2.3), the natural monodromy action of $\pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}})$ translates into an action on $X^*(\ell)$ given by automorphisms of the Markoff surface. This correspondence allows us to translate the work of Bourgain–Gamburd–Sarnak [BGS16a, BGS16b] and Meiri–Puder [MP18] into statements about the connectedness of the substack $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2} \subset \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$, and the explicit "coordinatization" it provides results in a remarkably simple calculation of the ramification behavior of $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ over $j = 0, 1728$ in $M(1)$. The ramification calculation has the pleasant consequences of establishing the existence of a $\mathbb{Q}$-rational point of $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$ (hence proving the $\mathbb{Q}$-rationality of the substack), and determining the monodromy group of $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ over $M(1)$ assuming it is connected. While not necessary for our argument, in §3.4 we show how this rational point arises from a natural covering of classical congruence modular curves. Finally, in §3.5 we conclude by putting everything together and proving Theorem B.

3.1. The work of Bourgain–Gamburd–Sarnak and Meiri–Puder.

Let τ_{12} (resp. τ_{23}) be the automorphism of $\mathbb{A}^3$ by exchanging the first and second coordinates (resp. second and third coordinates), and R_3 be the "Vieta involution" given by $R_3 : (x, y, z) \mapsto (x, y, xy - z)$. Let Γ be the group of automorphisms of $\mathbb{A}^3$ generated by R_3, τ_{12}, and τ_{23}. The group Γ clearly preserves $\mathbb{X}$, and hence induces a group of permutations Γ on $X^*(\ell)$.

Markoff showed that Γ acts transitively on the set of positive integer Markoff triples [Mar79, Mar80]. The analogous question about the action of Γ on $X^*(\ell)$ was studied by Bourgain–Gamburd–Sarnak in [BGS16b, BGS16a] because of its connection with strong approximation. There, they show that the action is transitive for a density 1 set of primes ℓ.

Theorem 3.1.1 (Bourgain, Gamburd, Sarnak [BGS16a])**.** *Let $\mathcal{E}$ be the set of primes ℓ for which Γ does not act transitively on $X^*(\ell)$. For any $\varepsilon > 0$, the number of primes $\ell \leq T$ with $\ell \in \mathcal{E}$ is at* *most T^ε, for T large enough. Moreover, for any $\varepsilon > 0$, the largest Γ-orbit in $X^*(\ell)$ is of size at least $|X^*(\ell)| - \ell^\varepsilon$, for ℓ large enough (whereas $|X^*(\ell)| \sim \ell^2$).*

Moreover, they conjecture that transitivity holds for all ℓ:

Conjecture 3.1.2 (Bourgain, Gamburd, Sarnak)**.** *Let ℓ be a prime. The action of Γ on $X^*(\ell)$ is transitive.*

Definition 3.1.3. Let $\mathcal{V}$ denote the group of automorphisms of $\mathbb{A}^3$ negating two of the coordinates. It preserves $\mathbb{X}$. Given $(x,y,z) \in X^*(\ell)$, its $\mathcal{V}$-orbit is denoted $[x,y,z]$ and is called a *block*. Let $Y^*(\ell) := X^*(\ell)/\mathcal{V}$ denote the set of blocks of $X^*(\ell)$. Explicitly we have

$$[x,y,z] := \{(x,y,z),(x,-y,-z),(-x,y,-z),(-x,-y,z)\}.$$

Let Q_ℓ be the permutation group induced by the action of Γ_ℓ on $Y^*(\ell)$. This is the image of Γ_ℓ under the natural map $X^*(\ell) \to Y^*(\ell)$.

Using the fact that $\mathbb{X}$ is a ruled surface, the cardinality of $Y^*(\ell)$ can be computed as follows (see [MP18, Lemmas 2.2, 2.3] and [BGS16a, Lemmas 3-5])

$$n_\ell := |Y^*(\ell)| = \begin{cases} \frac{\ell(\ell+3)}{4} & \text{if } \ell \equiv 1 \mod 4 \\ \frac{\ell(\ell-3)}{4} & \text{if } \ell \equiv 3 \mod 4. \end{cases} \tag{3-1-1}$$

Assuming the transitivity of Q_ℓ (equivalently Γ_ℓ), Meiri and Puder are able to describe Q_ℓ in most cases:

Theorem 3.1.4 (Meiri, Puder [MP18, Theorem 1.3, 1.4])**.** *Let $\ell \geq 5$ be a prime.*

(1) If $\ell \equiv 1 \mod 4$ and Q_ℓ is transitive, then Q_ℓ is the full alternating or symmetric group on $Y^*(\ell)$.

(2) If $\ell \equiv 3 \mod 4$, Q_ℓ is transitive, and the property $\boldsymbol{P}(\ell)$ holds, then Q_ℓ is the full alternating or symmetric group on $Y^*(\ell)$.

In the latter case, the condition in $\mathbf{P}(\ell)$ is satisfied for a density one set of primes. Moreover, Meiri and Puder conjecture that Q_ℓ is always the full alternating or symmetric group:

Conjecture 3.1.5 ([MP18, Conjecture 1.2])**.** *For $\ell \geq 5$, Q_ℓ is the full alternating or symmetric group on $Y^*(\ell)$.*

Remark 3.1.6. When Q_ℓ is the full alternating or symmetric group on $Y^*(\ell)$, it follows from [CGMP16, Theorem 1.2] that Q_ℓ is the alternating group when $\ell \equiv 3 \mod 16$ and the symmetric group otherwise.

3.2. **Markoff triples as absolute G-structures.** Since the trace invariant for both $\mathrm{SL}_2(\mathbb{F}_\ell)$ and $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is invariant under $D(\ell)$ (see §2.4), it is well-defined on $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))/D(\ell)$. Since the Higman invariant is locally constant, so is the trace invariant. Thus, using the notation of Definition 2.5.9, for any $t \in \mathbb{F}_\ell$ and any $\mathcal{O}_{\mathbb{Q}(S(t))}[1/n_\ell]$-algebra A, we may consider the open and closed substacks

$$\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{t,A} := \mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))_{t,A}/D(\ell) \subset \mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))_A/D(\ell) = \mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_A$$
$$\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{t,A} := \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))_{t,A}/D(\ell) \subset \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))_A/D(\ell) = \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_A.$$

consisting of absolute $\mathrm{SL}_2(\mathbb{F}_\ell)$ or $\mathrm{PSL}_2(\mathbb{F}_\ell)$-structures on elliptic curves with trace invariant t. Likewise we may consider $F(\ell)_t \subset F(\ell)$ and $\overline{F(\ell)}_t \subset \overline{F(\ell)}$ which are the geometric fibers with trace invariant t. By definition there are decompositions

$$\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_A = \bigsqcup_{t\in\mathbb{F}_\ell} \mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{t,A} \qquad \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_A = \bigsqcup_{t\in\mathbb{F}_\ell} \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{t,A} \tag{3-2-1}$$

The traces for which the corresponding substack is nonempty is completely described in [MW13] (in particular, for $\ell \geq 13$, every trace except 2 appears). We conjecture (see 3.2.8 below) that the decompositions of (3-2-1) are decompositions into *connected components*.

Definition 3.2.1. We define

$$\begin{aligned} \mathrm{Tr} : \mathrm{Hom}(F_2, \mathrm{SL}_2(\mathbb{F}_\ell)) &\longrightarrow \mathbb{F}_\ell^3 \\ \varphi &\mapsto (\mathrm{tr}(\varphi(a)), \mathrm{tr}(\varphi(b)), \mathrm{tr}(\varphi(ab))). \end{aligned}$$

The group $\mathcal{V}$ acts on $\mathbb{F}_\ell^3 = \mathbb{A}^3(\mathbb{F}_\ell)$ by negating two of the coordinates. We may similarly define

$$\begin{aligned} \overline{\mathrm{Tr}} : \mathrm{Hom}(F_2, \mathrm{PSL}_2(\mathbb{F}_\ell)) &\longrightarrow \mathbb{F}_\ell^3/\mathcal{V} \\ \varphi &\mapsto [(\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB))] \end{aligned}$$

where $A, B \in \mathrm{SL}_2(\mathbb{F}_\ell)$ are any lifts of $\varphi(a)$ and $\varphi(b)$.

It is again straightforward to verify that $\overline{\mathrm{Tr}}$ is well-defined. Since traces are conjugation invariant, $\mathrm{Tr}, \overline{\mathrm{Tr}}$ descend to maps on $F(\ell), \overline{F(\ell)}$ (defined in (2-4-2) and (2-4-3)), giving a commutative diagram

$$\begin{tikzcd} F(\ell) \arrow[r, "\mathrm{Tr}"] \arrow[d] & \mathbb{F}_\ell^3 \arrow[d] \\ \overline{F(\ell)} \arrow[r, "\overline{\mathrm{Tr}}"] & \mathbb{F}_\ell^3/\mathcal{V}. \end{tikzcd} \tag{3-2-2}$$

By the work of Macbeath, for any prime ℓ, the horizontal maps in (3-2-2) are *injective* [Mac69, Theorem 3]. (This injectivity holds even if ℓ is replaced by a prime power.)

Remark 3.2.2. This injectivity morally comes from the fact that $\mathbb{A}^3$ is the *character variety* for SL_2-representations of F_2. Over $\mathbb{C}$, this is just the classical Fricke-Vogt theorem giving an isomorphism

$$\mathrm{Hom}(F_2, \mathrm{SL}_2(\mathbb{C})) /\!\!/ \mathrm{SL}_2(\mathbb{C}) \cong \mathbb{A}^3_{\mathbb{C}}$$

(see [Gol03, §2] , [Gol04]). Over $\mathbb{Z}$, more precise statements can be found in [BH95].

If $(x, y, z) = (\mathrm{tr}(\varphi(a)), \mathrm{tr}(\varphi(b)), \mathrm{tr}(\varphi(ab))) \in \mathbb{F}_\ell^3$ is the image of $\varphi \in F(\ell)$, then the trace invariant of φ can be expressed in terms of (x, y, z) as follows (see [Gol04, §1.3 (8)])

$$\mathrm{tr}(\varphi([a, b])) = x^2 + y^2 + z^2 - xyz - 2.$$

Thus $X(\ell) \cap \mathrm{Tr}(F(\ell)) \subset \mathbb{F}_\ell^3$ are exactly the images of elements of $F(\ell)$ of trace invariant -2. Furthermore:

Proposition 3.2.3. *For $\ell \geq 3$, restricting to objects of trace invariant -2, the maps* Tr *and* $\overline{\mathrm{Tr}}$ *of* (3-2-2) *restrict to give a commutative diagram*

$$\begin{tikzcd} F(\ell)_{-2} \arrow[r, "\mathrm{Tr}"] \arrow[d] & X^*(\ell) \arrow[d] \\ \overline{F(\ell)}_{-2} \arrow[r, "\overline{\mathrm{Tr}}"] & Y^*(\ell). \end{tikzcd} \tag{3-2-3}$$

(1) The horizontal maps are bijections, and all fibers of the vertical maps have cardinality 4.

(2) Under these bijections, the action of $\mathrm{Out}(F_2)$ *on* $F(\ell)_{-2}$ *(resp.* $\overline{F(\ell)}_{-2}$*) translates into the action of* Γ *on* $X^*(\ell)$ *(resp.* $Y^*(\ell)$*) from Definition 3.1.3. Specifically, letting* a, b *be a basis for* F_2*, then* $\mathrm{Out}(F_2)$ *is generated by the images of the automorphisms* $r, s, t \in \mathrm{Aut}(F_2)$ *described below. We record the corresponding automorphisms they induce on* $X^*(\ell)$ *via* Tr*:*

$$\begin{array}{rcl} r:(a,b) & \mapsto & (a^{-1},b) \\ s:(a,b) & \mapsto & (b,a) \\ t:(a,b) & \mapsto & (a^{-1},ab) \end{array} \quad \textit{corresponds to (under } \mathrm{Tr}\textit{)} \quad \begin{array}{rcl} R_3:(x,y,z) & \mapsto & (x,y,xy-z) \\ \tau_{12}:(x,y,z) & \mapsto & (y,x,z) \\ \tau_{23}:(x,y,z) & \mapsto & (x,z,y) \end{array}$$

(3) For $\ell = 3$*, the sets appearing in (3-2-3) are all empty. For* $\ell \geq 5$*, these sets are all nonempty. For* $\ell = 2$*,* $F(\ell)_{-2}, \overline{F(\ell)}_{-2}$ *are both empty but* $X^*(\ell), Y^*(\ell)$ *are not.*

Remark 3.2.4. We note that whereas $\mathrm{Aut}(F_2)$ acts on the right on $F(\ell)_{-2}$ (resp. $\overline{F(\ell)}_{-2}$), the automorphisms $R_3, \tau_{12}, \tau_{23}$ act on the left on $X^*(\ell)$ (resp. $Y^*(\ell)$). Accordingly, Tr induces an *anti-homomorphism* $\mathrm{Tr}_* : \mathrm{Aut}(F_2) \to \mathrm{Aut}(\mathbb{A}^3)$. In particular, $\mathrm{Tr}_*(r \circ s) = \mathrm{Tr}_*(s) \circ \mathrm{Tr}_*(r)$.

Proof. The bijectivity for (1) is explained in [MP18, §6] , but we will give a short argument here. The top row is injective by [Mac69, Theorem 3]. It is surjective by the analysis of [MW13, §11]. Since $\ell \neq 2$, $\mathcal{V}$ acts freely on $X^*(\ell)$ and hence all fibers of $X^*(\ell) \to Y^*(\ell)$ have cardinality 4. On the other hand, given a generating pair A, B of $\mathrm{PSL}_2(\mathbb{F}_\ell)$, with lifts $\tilde{A}, \tilde{B}$ to $\mathrm{SL}_2(\mathbb{F}_\ell)$, the four lifts $\{(\pm\tilde{A}, \pm\tilde{B})\}$ of (A, B) have distinct images in $X^*(\ell)$, so all fibers of $F(\ell)_{-2} \to \overline{F(\ell)}_{-2}$ also have cardinality 4. Thus, $\overline{\mathrm{Tr}}$ is bijective as well.

For (2), the automorphisms r, s, t are generators of $\mathrm{Aut}(F_2)$ (see [MW13] §2), thus their images in $\mathrm{Out}(F_2) \cong \mathrm{GL}_2(\mathbb{Z})$ are also generators. Finally, it is also easy to check that s (resp. t) corresponds to τ_{12} (resp. τ_{23}). To see that r corresponds to R_3, we use the Fricke identity

$$\mathrm{tr}(AB) + \mathrm{tr}(A^{-1}B) = \mathrm{tr}(A)\,\mathrm{tr}(B)$$

valid for $A, B \in \mathrm{SL}_2(R)$ for any ring R. (It follows from the Cayley Hamilton theorem, which implies $A + A^{-1} = \mathrm{tr}(A)I$, upon multiplying by B and taking traces.)

For (3), the nonemptiness of the sets when $\ell \geq 5$ follows from the Trace Theorem of [MW13]. The statements for $\ell = 2, 3$ are checkable by hand. □

Proposition 3.2.5. *Let* $Q_\ell^+ \leq Q_\ell$ *be the permutation image of* $\mathrm{Out}^+(F_2)$ *acting on* $Y^*(\ell)$ *via* $\overline{\mathrm{Tr}}$*. Then* Q_ℓ^+ *is transitive if and only if* Q_ℓ *is transitive. In particular, Conjecture 3.1.2 is equivalent to the connectedness of* $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\overline{\mathbb{Q}}}$*, which in turn implies the connectedness of* $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\overline{\mathbb{Q}}}$*.*

Proof. Certainly transitivity of $\mathrm{Out}^+(F_2)$ implies the transitivity of $\mathrm{Out}(F_2)$. Now suppose $\mathrm{Out}(F_2)$ acts transitively. If $\mathrm{Out}^+(F_2)$ does not act transitively, then since $\mathrm{Out}^+(F_2)$ is normal of index 2 inside $\mathrm{Out}(F_2)$, any representative for its nontrivial coset must act on $F(\ell)_{-2}$ without fixed points, exchanging the two $\mathrm{Out}^+(F_2)$-orbits. However, this is false, since

$$s : (a, b) \mapsto (a^{-1}, ab)$$

corresponds to the permutation $\tau_{12} \in \Gamma$ having the fixed point $(3, 3, 3) \in X^*(\ell)$. Making the appropriate translations using Propositions 2.4.2 and 3.2.3, Galois theory then yields the equivalence of Conjecture 3.1.2 with the connectedness of $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$. Finally, note that the transitivity of the action of $\mathrm{Out}^+(F_2)$ on $F(\ell)_{-2}$ implies the transitivity of $\mathrm{Out}^+(F_2)$ on $\overline{F(\ell)}_{-2}$, which again by Galois theory implies the connectedness of $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\overline{\mathbb{Q}}}$. □

Finally, we end this subsection by showing that "trace invariant -2" is defined over $\mathbb{Q}$:

Proposition 3.2.6. *Let $m_\ell := |\,\mathrm{SL}_2(\mathbb{F}_\ell)|$. Then in the notation of (2-5-2), $\mathbb{Q}(S(-2)) = \mathbb{Q}$. In other words, the property "has trace invariant -2" is well-defined on $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{\mathbb{Z}[1/m_\ell]}$ and $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{\mathbb{Z}[1/m_\ell]}$.*

The corresponding open and closed substacks are denoted by

$$\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\mathbb{Z}[1/m_\ell]} \quad \text{and} \quad \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\mathbb{Z}[1/m_\ell]}. \tag{3-2-4}$$

Proof. We begin by considering $\mathrm{SL}_2(\mathbb{F}_\ell)$. In the notation of Definition 2.5.9, we wish to show that $\mathbb{Q}(S(-2)) = \mathbb{Q}$. This would follow from the stronger statement that for any $s \in S(-2)$, $s^i \in S(-2)$ for any i coprime to $|s|$. Indeed, by [MW13, Proposition 5.1], every element of $S(-2)$ is conjugate to one of

$$T := \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}, \text{ or } T' := \begin{bmatrix} -1 & a \\ 0 & -1 \end{bmatrix}$$

where $a \in \mathbb{F}_\ell^\times - (\mathbb{F}_\ell^\times)^2$ if ℓ is odd (for $\ell = 2$, T' is not needed). If ℓ is odd, T and T' have order 2ℓ and if $\ell = 2$, then T has order 2. In either case, every other generator of the cyclic group $\langle T\rangle$ (resp. $\langle T'\rangle$) is an odd power of T (resp. T'), and hence also lies in $S(-2)$.

The case of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is similar, where we note that the commutator trace of a generating pair of $\mathrm{SL}_2(\mathbb{F}_\ell)$ cannot have trace 2. Indeed, two elements with commutator trace 2 must generate an affine subgroup (see [MW13, §3]). □

Remark 3.2.7. By Proposition 3.2.5, the Conjecture 3.1.2 of Bourgain, Gamburd and Sarnak is equivalent to the connectedness of $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$. This connectedness would also follow from a special case of the "Classification Conjecture" of McCullough-Wanderley [MW13], which amounts to asserting that the union of the Higman invariant with its inverse completely characterizes the $\mathrm{Out}(F_2)$ orbits[13] on $\mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{SL}_2(\mathbb{F}_q))$. From our perspective, it is natural to ask if the Higman invariant is a complete invariant for the $\mathrm{Out}^+(F_2)$ orbits on $\mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{SL}_2(\mathbb{F}_q))$. We have computationally verified this for all $q \le 73$, except for $q = 9$, where it is false. Nonetheless, we will tentatively conjecture:

Conjecture 3.2.8. *For every prime power $q \neq 9$, the Higman invariant is a complete invariant for the orbits of $\mathrm{Out}^+(F_2)$ on $\mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{SL}_2(\mathbb{F}_q))$.*

Note that for any conjugacy class C of $\mathrm{SL}_2(\mathbb{F}_q)$, the field $\mathbb{Q}(C)$ is an abelian extension of $\mathbb{Q}$ as $\rho_{\mathbb{Q},C}$ factors through an abelian group (see (2-5-1)). Thus conjecture 3.2.8 would imply that the components of $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_q))_{\overline{\mathbb{Q}}}$ are all defined over abelian number fields. Note that the conjecture cannot be true with $\mathrm{SL}_2(\mathbb{F}_q)$ replaced by a general finite group G. Indeed, by Theorem 2.2.3, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the set of components $\bigcup_G \pi_0(\mathcal{M}(G)_{\overline{\mathbb{Q}}})$, and hence the connected components cannot all be defined over abelian number fields.

[13] The action of $\mathrm{Out}(F_2)$ does not preserve the Higman invariant. The "orientation reversing" automorphism $(x, y) \mapsto (y, x)$ replaces the Higman invariant with its inverse

3.3. **Explicit ramification behavior.** We now use the identifications given in Proposition 2.4.2 to analyze the ramification of $M(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\overline{\mathbb{Q}}}$ and $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\overline{\mathbb{Q}}}$ over $M(1)$. Let a, b be a basis for F_2, and define the following automorphisms of F_2

$$\gamma_0 : (a,b) \mapsto (ab^{-1}, a) \quad \gamma_{1728} : (a,b) \mapsto (b^{-1}, a) \quad \gamma_\infty : (a,b) \mapsto (a, ab), \quad \gamma_{-I} : (a,b) \mapsto (a^{-1}, b^{-1}).$$

Using the isomorphism $\mathrm{Out}^+(F_2) \cong \mathrm{SL}_2(\mathbb{Z})$, it is easy to check that $\mathrm{Out}^+(F_2)$ is generated by the images of γ_0 and γ_{1728}. Since γ_{-I} acts trivially on $X^*(\ell)$ and $Y^*(\ell)$, by Proposition 2.3.4 the fibers of $M(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ (resp. $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$) above $j = 0, 1728, \infty$ are precisely the quotients of $X^*(\ell)$ (resp. $Y^*(\ell)$) by the actions of the groups generated by $\gamma_0, \gamma_{1728}, \gamma_\infty$ respectively, with ramification indices corresponding to orbit sizes.

Remark 3.3.1. The work in [BGS16a] studies the action of γ_∞ on $X^*(\ell)$ in great detail. Moreover their "rotations" are all induced by a conjugate of γ_∞ or γ_∞^{-1}. The geometric situation above the cusp $j = \infty$ is more delicate, and we do not treat it here.

Above $j = 0, 1728$, we have the following:

Proposition 3.3.2. *Let M be either $M(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\overline{\mathbb{Q}}}$ or $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\overline{\mathbb{Q}}}$. The ramification indices of the map $M \to M(1)_{\overline{\mathbb{Q}}}$ above $j = 0$ are all 3, except for a single unramified point which is $\mathbb{Q}$-rational. For $M(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\overline{\mathbb{Q}}}$, all ramification points above $j = 1728$ have index 2, and there are precisely two unramified points if $\ell \equiv 1, 7 \mod 8$, and no unramified points otherwise. In $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\overline{\mathbb{Q}}}$, again all ramified points above $j = 1728$ have index 2, and there is a unique unramified point if $\ell \equiv 1, 7 \mod 8$ and no unramified points otherwise.*

Proof. We need to analyze the action of γ_0, γ_{1728} on $X^*(\ell)$ and $Y^*(\ell)$. This is an explicit calculation which we have relegated to the Appendix (see Lemma A.1.1). To see that the unique unramified points are rational, note that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the fibers of $M \to M(1)_{\overline{\mathbb{Q}}}$ above $j = 0, 1728$, preserving ramification indices. If there is a unique unramified point, then it must be stabilized by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, hence it must be $\mathbb{Q}$-rational. □

Recall that $Q_\ell^+ \leq Q_\ell$ is the subgroup corresponding to the action of $\mathrm{Out}^+(F_2)$ on $Y^*(\ell)$ via $\overline{\mathrm{Tr}}$ (see Propositions 3.2.3, 3.2.5), and recall from (3-1-1) that

$$n_\ell = |Y^*(\ell)| = \begin{cases} \frac{\ell(\ell+3)}{4} & \ell \equiv 1 \mod 4 \\ \frac{\ell(\ell-3)}{4} & \ell \equiv 3 \mod 4. \end{cases} \tag{3-3-1}$$

Since $\mathrm{Out}^+(F_2)$ is generated by the images of γ_0, γ_{1728}, the above ramification description would allow us describe exactly when Q_ℓ^+ is contained in the alternating group on $Y^*(\ell)$.

Proposition 3.3.3. *For $\ell \geq 3$, on $Y^*(\ell)$, γ_0 always acts as an even permutation, and γ_{1728} acts as an even permutation if and only if $\ell \equiv 1, 3, 13, 15 \mod 16$, and it is odd when $\ell \equiv 5, 7, 9, 11 \mod 16$.*

Proof. From the ramification description given in Proposition 3.3.2 (or Lemma A.1.1), we see that the parity of γ_{1728} acting on $Y^*(\ell)$ is precisely the parity of the number of ramified points above

$j = 1728$ in $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$. This number is

$$\big(\#\text{ ramified points above } j = 1728\big) = \begin{cases} \frac{\ell(\ell+3)-4}{8} & \text{if } \ell \equiv 1 \mod 8 \\ \frac{\ell(\ell-3)}{8} & \text{if } \ell \equiv 3 \mod 8 \\ \frac{\ell(\ell+3)}{8} & \text{if } \ell \equiv 5 \mod 8 \\ \frac{\ell(\ell-3)-4}{8} & \text{if } \ell \equiv 7 \mod 8. \end{cases}$$

Computing the parity of this number forces us to consider $\ell \mod 16$, which gives us the desired result. We leave the details to the reader. □

Corollary 3.3.4. *If $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\overline{\mathbb{Q}}}$ is connected and its monodromy group over $M(1)_{\overline{\mathbb{Q}}}$ contains A_{n_ℓ}, then the monodromy group is A_{n_ℓ} if $\ell \equiv 1, 3, 13, 15 \mod 16$, and is S_{n_ℓ} if $\ell \equiv 5, 7, 9, 11 \mod 16$.*

3.4. Geometric construction of the $\mathbb{Q}$-rational unique unramified point of $M(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\overline{\mathbb{Q}}}$.

Here we explain how the $\mathbb{Q}$-rational unique unramified point of $M(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ over $j = 0$ from Proposition 3.3.2 can be obtained from a covering of congruence modular curves. The resulting point, relative to a certain isomorphism $F_2 \cong \pi_1^{\mathrm{top}}(E^\circ(\mathbb{C}), x_0)$ as in Proposition 2.4.2, will correspond to the point $(3, 3, 6) \in X^*(\ell)$. However, the connected component of $M(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ containing that point is independent of the choice of isomorphism.

Let $\Gamma(1) := \mathrm{SL}_2(\mathbb{Z})$, then it can be checked (for example, in GAP) that its commutator subgroup $\Gamma(1)'$ is a torsion-free congruence subgroup of level 6 and index 12, with $\mathrm{SL}_2(\mathbb{Z})/\Gamma(1)' \cong \mathbb{Z}/12\mathbb{Z}$. In fact it can be verified in GAP that $\Gamma(1)'$ is free on the generators

$$\left[\begin{smallmatrix} 2 & -1 \\ -1 & 1 \end{smallmatrix}\right], \quad \left[\begin{smallmatrix} 1 & -1 \\ -1 & 2 \end{smallmatrix}\right]. \tag{3-4-1}$$

Let E be an elliptic curve over $\mathbb{Q}$. In this subsection we will fix an isomorphism $\pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}}, E_{\overline{\mathbb{Q}}}) \cong \widehat{\mathrm{SL}_2(\mathbb{Z})}$ as in Theorem 2.2.2, and using this isomorphism we will silently identify the two groups.

In particular, $\widehat{\mathrm{SL}_2(\mathbb{Z})}$ is endowed with an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ from the split exact sequence

$$1 \to \widehat{\mathrm{SL}_2(\mathbb{Z})} \to \pi_1(\mathcal{M}(1)_{\mathbb{Q}}, E_{\overline{\mathbb{Q}}}) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to 1$$

with splitting given by the section $E_* : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \pi_1(\mathcal{M}(1)_{\mathbb{Q}}, E_{\overline{\mathbb{Q}}})$.

The closure $\overline{\Gamma(1)'}$ of $\Gamma(1)'$ inside $\widehat{\mathrm{SL}_2(\mathbb{Z})}$ corresponds to a degree 12 finite étale cover $\mathcal{M}' \to \mathcal{M}(1)_{\overline{\mathbb{Q}}}$ with $\pi_1(\mathcal{M}'_{\overline{\mathbb{Q}}}) \cong \overline{\Gamma(1)'}$. Since $\Gamma(1)'$ is torsion free, $\mathcal{M}'$ is a scheme.

The structure of $\mathcal{M}'$ can be understood as follows. The map $\mathcal{M}' \to M(1)_{\overline{\mathbb{Q}}}$ is a branched covering of curves of degree 6. By Corollary 2.1.3, it is étale over the complement of $j = 0, 1728, \infty$, with a unique totally ramified cusp (preimage of ∞), and 2 (resp. 3) points above $j = 0$ (resp. $j = 1728$) with ramification indices 3 (resp. 2).

By Riemann–Hurwitz, one finds that $\mathcal{M}'$ is a once-punctured elliptic curve. By functoriality of coarse schemes, $\mathrm{Gal}(\mathcal{M}'/\mathcal{M}(1)_{\overline{\mathbb{Q}}}) \cong \mathbb{Z}/12\mathbb{Z}$ acts on the map $\mathcal{M}' \to M(1)_{\overline{\mathbb{Q}}}$. By Proposition 2.1.2, one finds that this action yields a surjection of Galois groups

$$\mathrm{Gal}(\mathcal{M}'/\mathcal{M}(1)_{\overline{\mathbb{Q}}}) \twoheadrightarrow \mathrm{Gal}(\mathcal{M}'/M(1)_{\overline{\mathbb{Q}}})$$

with kernel of order 2. Thus, $\mathrm{Gal}(\mathcal{M}'/M(1)_{\overline{\mathbb{Q}}}) \cong \mathbb{Z}/6\mathbb{Z}$, and it preserves the cusp, so it acts (faithfully) as automorphisms of the punctured elliptic curve $\mathcal{M}'$. Thus, we have

$$j(\mathcal{M}') = 0.$$

Since $\overline{\Gamma(1)'}$ is characteristic inside $\widehat{\mathrm{SL}_2(\mathbb{Z})}$, it is preserved by the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action, and hence the map $\mathcal{M}' \to \mathcal{M}(1)_{\overline{\mathbb{Q}}}$ has a $\mathbb{Q}$-model $\mathcal{M}'_{\mathbb{Q}} \to \mathcal{M}(1)_{\mathbb{Q}}$.

Remark 3.4.1. The stack $\mathcal{M}'$ has a natural moduli interpretation over $\mathbb{Z}[1/6]$. Given an elliptic curve $f : E \to S$ the sheaf $f_*\Omega^1_{E/S}$ is an invertible $\mathcal{O}_S$-module. If it is free and $\omega \in H^0(S, f_*\Omega^1_{E/S})$ is a basis, and if moreover 6 is invertible on S, then the basis ω determines a Weierstrass equation for E inside $\mathbb{P}^2_S$ (see [KM85, §2.2]) relative to which ω can be written as $\omega = \frac{-dx}{2y}$. Let $\Delta(E,\omega)$ be the discriminant of E relative to the Weierstrass equation defined by ω. By standard calculations ([Sil09, Table 3.1]), we have

$$\Delta(E, u\omega) = u^{-12}\Delta(E,\omega).$$

The moduli stack classifying pairs (E,ω) is naturally a $\mathbb{G}_m$-torsor over $\mathcal{M}(1)_{\mathbb{Z}}$, and hence the moduli stack "$\mathcal{M}(\Delta = 1)$" classifying pairs (E,ω) with $\Delta(E,\omega) = 1$ is a μ_{12}-torsor over $\mathcal{M}(1)_{\mathbb{Z}[1/6]}$. In particular it is finite étale. Since the abelianization of $\widehat{\mathrm{SL}_2(\mathbb{Z})} = \pi_1(\mathcal{M}(1)_{\overline{\mathbb{Q}}})$ is $\mathbb{Z}/12\mathbb{Z}$, $\mathcal{M}(\Delta = 1)$ is a moduli-theoretic model of $\mathcal{M}'$ over $\mathbb{Z}[1/6]$.

We will obtain a $\mathbb{Q}$-rational point of $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$ by pulling back the modular curve corresponding to the principal congruence subgroup $\Gamma(\ell) := \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}))$ to $\mathcal{M}'_{\mathbb{Q}}$. This modular curve is a geometric component of the classical moduli problem classifying elliptic curves with full level ℓ structure. This moduli problem is defined over $\mathbb{Q}$, but over $\mathbb{Q}$ it is not geometrically connected. Its geometrically connected components (ie, modular curves) classify elliptic curves E equipped with a basis for $E[n]$ with a fixed Weil pairing; these components are defined over cyclotomic field $\mathbb{Q}(\zeta_\ell)$. However, we may obtain a $\mathbb{Q}$-model of the modular curve by twisting the definition of a full level ℓ structure as in Deligne-Rapoport [DR75, §V4.1-2] . We briefly recall the definition here.

For an integer $n \geq 1$ and an elliptic curve E over a $\mathbb{Z}[1/n]$-scheme S, the Weil pairing on $E[n]$ is a map of finite étale S-schemes

$$e_n(*,*) : E[n] \times E[n] \longrightarrow \mu_n$$

which on geometric fibers is alternating and nondegenerate. Let

$$\omega(*,*) : (\mu_n \times \mathbb{Z}/n\mathbb{Z}) \times (\mu_n \times \mathbb{Z}/n\mathbb{Z}) \longrightarrow \mu_n$$

be defined on geometric fibers as the unique alternating pairing satisfying

$$\omega((\zeta, 0), (1, k)) = \zeta^k \qquad \text{for } \zeta \in \mu_n, k \in \mathbb{Z}/n\mathbb{Z}.$$

Then ω is also nondegenerate. With E as above, a *full level n structure of determinant* 1 on E is an isomorphism of finite étale group schemes $\alpha : \mu_n \times \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} E[n]$ compatible with the pairings e_n and ω. Equivalently, we require that the following diagram commutes:

$$\begin{tikzcd}
(\mu_n \times \mathbb{Z}/n\mathbb{Z}) \times (\mu_n \times \mathbb{Z}/n\mathbb{Z}) \arrow[r, "\alpha\times\alpha"] \arrow[dr, "\omega"'] & E[n] \times E[n] \arrow[d, "e_n"] \\
 & \mu_n.
\end{tikzcd}$$

Let $\mathcal{M}(\ell)_{\mathbb{Q}}$ be the moduli stack classifying elliptic curves with full level ℓ-structure of determinant 1 in the sense described above. Over $\mathbb{Q}(\zeta_\ell)$, if we choose a primitive ℓth root of unity $\zeta \in \mathbb{Q}(\zeta_\ell)$, then to any "full level n structure of determinant 1" $\alpha : \mu_\ell \times \mathbb{Z}/\ell\mathbb{Z} \to E[\ell]$ as given above, we may associate the "classical" full level ℓ structure given by $(\alpha(\zeta, 0), \alpha(1, 1))$. Compatibility with ω, e_ℓ implies that over $\mathbb{Q}(\zeta_\ell)$, the set of full level ℓ structures of determinant 1 is in bijection with the set of full level ℓ structures with Weil pairing ζ, so $\mathcal{M}(\ell)$ is a $\mathbb{Q}$-model of the classical modular curve $Y(\ell)$.

The finite étale cover $\mathcal{M}(\ell)_{\mathbb{Q}} \to \mathcal{M}(1)_{\mathbb{Q}}$ is not Galois, but its base change to $\mathbb{Q}(\zeta_\ell)$ is Galois with Galois group isomorphic to $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ (using an isomorphism $(\mathbb{Z}/\ell\mathbb{Z})^2 \cong \mu_\ell \times \mathbb{Z}/\ell\mathbb{Z}$ over $\mathbb{Q}(\zeta_\ell)$). Let $\mathcal{M}(\ell)'_{\mathbb{Q}} := (\mathcal{M}(\ell) \times_{\mathcal{M}(1)} \mathcal{M}')_{\mathbb{Q}}$, then we obtain the map

$$\pi_\ell : \mathcal{M}(\ell)'_{\mathbb{Q}} \longrightarrow \mathcal{M}'_{\mathbb{Q}}$$

appearing in (1-1-2). This map is finite étale, and becomes $\mathrm{SL}_2(\mathbb{F}_\ell)$-Galois over $\mathbb{Q}(\zeta_\ell)$ and thus it determines a $\mathbb{Q}$-rational point of $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$ using Remark 2.4.1.

To see that it has trace invariant -2, it suffices to work analytically. Note that the cover $\mathcal{M}(\ell)^{\mathrm{an}} \to \mathcal{M}(1)^{\mathrm{an}}$ corresponds to the congruence subgroup $\Gamma(\ell)$. With suitable choices of base points, the monodromy of $\mathcal{M}(\ell)^{\mathrm{an}} \to \mathcal{M}(1)^{\mathrm{an}}$ is given by the map

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z})/\Gamma(\ell) \cong \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

and the monodromy of the pullback $\mathcal{M}(\ell)' \to \mathcal{M}'$ is just the composition

$$\varphi : \Gamma(1)' \hookrightarrow \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z})/\Gamma(\ell) \cong \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Now one can compute, using the generators of $\Gamma(1)'$ given in (3-4-1), that the trace invariant of φ is precisely

$$\mathrm{tr}\left(\left[\left[\begin{smallmatrix} 2 & -1 \\ -1 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & -1 \\ -1 & 2 \end{smallmatrix}\right]\right]\right) = \mathrm{tr}\left(\left[\begin{smallmatrix} 5 & 6 \\ -6 & -7 \end{smallmatrix}\right]\right) = -2.$$

Thus, π_ℓ determines a $\mathbb{Q}$-rational point of $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$, and hence its image in $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ yields a $\mathbb{Q}$-point of $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ as desired. Moduli theoretically, this point is given by the cover

$$\overline{\pi}_\ell : \mathcal{M}(\ell)'_{\mathbb{Q}}/\{\pm I\} \to \mathcal{M}'_{\mathbb{Q}} \tag{3-4-2}$$

where $-I \in \mathrm{SL}_2(\mathbb{F}_\ell)$ acts by negating the full level ℓ-structure.

Finally, note that relative to our free basis $\left[\begin{smallmatrix} 2 & -1 \\ -1 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & -1 \\ -1 & 2 \end{smallmatrix}\right]$ of $\Gamma(1)'$, the covering $\overline{\pi}_\ell$ corresponds to the point $[3,3,6] \in Y^*(\ell)$. By Proposition 3.3.2 and the calculation in Lemma A.1.1, this implies that $\overline{\pi}_\ell$ indeed corresponds to the unique unramified point above $j = 0$ in $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$.

Remark 3.4.2. In fact, the analysis shows that this point is defined over $\mathbb{Z}[1/|\mathrm{SL}_2(\mathbb{F}_\ell)|]$.

Remark 3.4.3. We will conclude this section by describing how the above geometric construction which yields the unique unramified point of $M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ may be deduced by "pure thought". We work over $\overline{\mathbb{Q}}$, and assume $\ell \geq 5$.

The completion of the étale local ring at a geometric point of a Deligne-Mumford stack is the universal deformation ring of that geometric point. Using the étale local structure of Deligne-Mumford stacks [AV02, Lemma 2.2.3], this implies that for a smooth separated 1-dimensional Deligne-Mumford stack $\mathcal{M}$ with coarse scheme $c : \mathcal{M} \to M$, then for any geometric point $x \in \mathcal{M}$, the map induced by c on étale local rings at x is a totally ramified extension of discrete valuation rings with ramification index $|G_x/K_x|$, where $G_x := \mathrm{Aut}_{\mathcal{M}}(x)$ and $K_x \subset G_x$ is the subgroup consisting of automorphisms which extend to the universal deformation of x. This implies in particular that at the level of étale local rings, the map $\mathcal{M}(1) \to M(1)$ has ramification index 3 at $j = 0$.

Now let $x \in M(\mathrm{PSL}_2(\mathbb{F}_\ell))_{-2}$ be a geometric point which is unramified over $j = 0$ in $M(1)$. Then the map $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))_{-2} \to M(\mathrm{PSL}_2(\mathbb{F}_\ell))_{-2}$ also has ramification index 3 above x. Such an x must correspond to a $\mathrm{PSL}_2(\mathbb{F}_\ell)$-torsor $p : X^\circ \to E^\circ$ where E is an elliptic curve over $\overline{\mathbb{Q}}$ with j-invariant 0. Viewing x as a geometric point of $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))_{-2}$, the fact that γ_{-I} acts trivially on $Y^*(\ell)$

implies that $[-1] \in \mathrm{Aut}(E)$ extends to the universal deformation of x.[14] The connection with deformation theory then implies that because $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))_{-2} \to M(\mathrm{PSL}_2(\mathbb{F}_\ell))_{-2}$ has ramification index 3 at x, x must have an automorphism group of order 6. Since $\mathrm{Aut}(E) \cong \mu_6$, this implies that if $\alpha \in \mathrm{Aut}(E)$ is a generator, then α lifts via p to a $\mathrm{PSL}_2(\mathbb{F}_\ell)$-equivariant automorphism $\tilde{\alpha}$ of X°. Since $\mathrm{PSL}_2(\mathbb{F}_\ell)$ has trivial center, any such lifting is unique, and hence we obtain an action of μ_6 on X°, commuting with the $\mathrm{PSL}_2(\mathbb{F}_\ell)$-action.

Next, let W be a cyclic group of order 12, and fix a surjection $f : W \to \mu_6$. Then W acts (non-faithfully) on X° and on E° via f, commuting with the $\mathrm{PSL}_2(\mathbb{F}_\ell)$-action on X°. Taking stacky quotients we obtain a diagram

$$\begin{tikzcd}
X^\circ \arrow[r] \arrow[d, "p"] & {[X^\circ/W]} \arrow[d, "\overline{p}"] \\
E^\circ \arrow[r] & {[E^\circ/W]}
\end{tikzcd}$$

where every map is finite étale. Since all objects in the diagram are connected, comparing degrees we find that the diagram is cartesian. Since the action of W on E° is isomorphic to the action of $\mathrm{Gal}(\mathcal{M}'/\mathcal{M}(1))$ on $\mathcal{M}'$, it follows that $[E^\circ/W] \cong \mathcal{M}(1)$ and that the monodromy representation of the $\mathrm{PSL}_2(\mathbb{F}_\ell)$-torsor $\overline{p}$ (viewed as a covering of $\mathcal{M}(1)$) is a surjection

$$\rho : \widehat{\mathrm{SL}_2(\mathbb{Z})} \to \mathrm{PSL}_2(\mathbb{F}_\ell).$$

At this point, if we take ρ to be the obvious surjection given by reduction mod ℓ, then pulling back the $\mathrm{PSL}_2(\mathbb{F}_\ell)$-cover of $\mathcal{M}(1)$ corresponding to ρ gives a cover of E° which by deformation theory must correspond to an "unramified point" in the sense described above. This establishes the existence of the unramified point.

To establish uniqueness, note that since the trace invariant of p is -2, all ramification indices of p and $\overline{p}$ above the puncture are ℓ. It is a group-theoretic fact that any surjection $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{PSL}_2(\mathbb{F}_\ell)$ which sends $\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$ (a generator of inertia around the cusp) to an element of order ℓ must have kernel the projective principal congruence subgroup $\langle -I, \Gamma(\ell)\rangle$. This implies that $\overline{p}$ is isomorphic to the map $\mathcal{M}(\ell)/\{\pm I\} \to \mathcal{M}(1)$, and p is isomorphic to the map $\overline{\pi}_\ell$ of (3-4-2). This proves uniqueness.

3.5. **Proof of Theorem B.** At this point we are ready to prove the "asymptotic part" of the main theorem, Theorem B. We begin by recalling the setup. Let F_2 be the free group on the generators a, b. For a prime $\ell \geq 3$, we have a diagram

(3-5-1)
$$\begin{tikzcd}
\mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{SL}_2(\mathbb{F}_\ell))/D(\ell) \arrow[d] & F(\ell)_{-2} \arrow[l, hook'] \arrow[r, "\mathrm{Tr}"] \arrow[d] & X^*(\ell) \arrow[d] \\
\mathrm{Epi}^{\mathrm{ext}}(F_2, \mathrm{PSL}_2(\mathbb{F}_\ell))/D(\ell) & \overline{F(\ell)}_{-2} \arrow[l, hook'] \arrow[r, "\overline{\mathrm{Tr}}"] & Y^*(\ell)
\end{tikzcd}$$

[14] We elaborate on this: By [MW13, §5], there are two conjugacy classes in $\mathrm{SL}_2(\mathbb{F}_\ell)$ with trace -2, and they are swapped by the action of $D(\ell)$. This implies that $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))_{-2}$ is a disjoint union of two open and closed substacks (corresponding to different Higman invariants) which are mapped isomorphically onto each other by the nontrivial element of $D(\ell)$. Thus, the degree 2 finite étale map $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))_{-2} \to \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ admits a section, hence induces isomorphisms on automorphism groups of geometric points. By Proposition 2.1.2(1), γ_{-I} acting trivially on $Y^*(\ell)$ implies that $[-1]$ fixes the absolute $\mathrm{PSL}_2(\mathbb{F}_\ell)$-structure determined by p, and we will say "$[-1] \in \mathrm{Aut}_{\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}}(x)$". By the above, this also means that "$[-1] \in \mathrm{Aut}_{\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))_{-2}}(x)$", so $[-1]$ fixes the $\mathrm{PSL}_2(\mathbb{F}_\ell)$-structure determined by p. Using Theorem 2.2.2(3), one can check that $[-1]$ must also fix the $\mathrm{PSL}_2(\mathbb{F}_\ell)$-structure attached to the universal deformation of x defined over $\overline{\mathbb{Q}}[\![t]\!]$, which has trivial π_1.

where Tr and $\overline{\mathrm{Tr}}$ are bijections. Recall from (3-1-1) that

$$|Y^*(\ell)| = n_\ell = \begin{cases} \frac{\ell(\ell+3)}{4} & \ell \equiv 1 \mod 4 \\ \frac{\ell(\ell-3)}{4} & \ell \equiv 3 \mod 4. \end{cases}$$

There are natural actions of $\mathrm{Out}(F_2)$ on each object on the left square, compatible with all the morphisms, which descends via Tr to the action of Γ on $X^*(\ell), Y^*(\ell)$ (see Proposition 3.2.3). We recall that the permutation images of the Γ action on $X^*(\ell)$ (resp. $Y^*(\ell)$) are denoted Γ_ℓ (resp. Q_ℓ). Let E be an elliptic curve over $\mathbb{Q}$, $x \in E^\circ(\mathbb{Q})$, and $x_\mathbb{C} : \operatorname{Spec}\mathbb{C} \to \operatorname{Spec}\mathbb{Q} \to E^\circ$ be the corresponding $\mathbb{C}$-point. Fixing an isomorphism $F_2 \cong \pi_1^{\mathrm{top}}(E^\circ(\mathbb{C}), x_0)$, then $F(\ell)_{-2}$ (resp. $\overline{F(\ell)}_{-2}$) is identified with the geometric fiber of $\mathcal{M}(\mathrm{SL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$ (resp. $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2}$) over $\mathcal{M}(1)_{\overline{\mathbb{Q}}}$ by Proposition 2.4.2. Moreover, since E is defined over $\mathbb{Q}$ we also obtain an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on these fibers. For any $p \nmid |\mathrm{PSL}_2(\mathbb{F}_\ell)|$ and any Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Frob_p acts on $Y^*(\ell)$. The parity of the Frob_p-action on $Y^*(\ell)$ does not depend on the choice of Frobenius element.

Let $\mathcal{E}$ be the set of "exceptional" primes ℓ for which Γ_ℓ does not act transitively on $X^*(\ell)$. We will refer to $\mathcal{E}$ as the "exceptional set". By Proposition 3.2.6, it makes sense to ask if a $\mathrm{PSL}_2(\mathbb{F}_\ell)$-torsor over a punctured elliptic curve over a $\mathbb{Z}[1/|\mathrm{PSL}_2(\mathbb{F}_\ell)|]$-scheme has trace invariant -2.

Let $c_\ell := |\mathrm{PSL}_2(\mathbb{F}_\ell)| = \frac{\ell(\ell^2-1)}{2}$, and note that $6 \mid c_\ell$. Recall that we defined $\mathbf{P}(\ell)$ as:

$$\mathbf{P}(\ell) := \begin{array}{c} \text{The property that either } \ell \equiv 1 \mod 4, \text{ or} \\ \text{the order of } \frac{3+\sqrt{5}}{2} \in \mathbb{F}_{\ell^2} \text{ is at least } 32\sqrt{\ell+1}. \end{array}$$

Theorem 3.5.1. *Let $\ell \geq 3$ be a prime such that $\ell \notin \mathcal{E}$ and the condition $\boldsymbol{P}(\ell)$ holds.*

1. *The substack $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2,\mathbb{Z}[1/c_\ell]} \subset \mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{\mathbb{Z}[1/c_\ell]}$ of objects of trace invariant -2 from Proposition 3.2.6 is finite étale over $\mathcal{M}(1)_{\mathbb{Z}[1/c_\ell]}$.*
2. *Its coarse scheme $M_\ell = (M(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}_{-2})_{\mathbb{Z}[1/c_\ell]}$ is smooth and geometrically connected over $\mathbb{Z}[1/c_\ell]$.*
3. *Let $M_\ell^\circ \subset M_\ell$ be the preimage of $M(1)^\circ_{\mathbb{Z}[1/c_\ell]} := M(1)_{\mathbb{Z}[1/c_\ell]} - \{j = 0, 1728\}$. Then there is an at most quadratic extension L of $\mathbb{Q}$ such that if B is the integral closure of $\mathbb{Z}[1/c_\ell]$ in L, then the Galois closure N_B of $M^\circ_{\ell,B} \to M(1)^\circ_B$ is geometrically connected over B with Galois group*
$$\mathrm{Gal}(N_B/M(1)^\circ_B) \cong \begin{cases} S_{n_\ell} & \text{if } \ell \equiv 5, 7, 9, 11 \mod 16 \\ A_{n_\ell} & \text{if } \ell \equiv 1, 3, 13, 15 \mod 16. \end{cases}$$
4. *If $\mathrm{Gal}(N_B/M(1)^\circ_B) \cong S_{n_\ell}$, then we may take $L = \mathbb{Q}$ and $B = \mathbb{Z}[1/c_\ell]$, and the fiber of $N_B \to M(1)^\circ_B$ at $p \nmid c_\ell$ is an S_{n_ℓ}-Galois cover of $\mathbb{P}^1_{\mathbb{F}_p} - \{0, 1728, \infty\}$.*
5. *If $\mathrm{Gal}(N_B/M(1)^\circ_B) \cong A_{n_\ell}$, then the fiber at any prime above $p \nmid c_\ell$ will yield an A_{n_ℓ}-cover of $\mathbb{P}^1_k - \{0, 1728, \infty\}$, where $k = \mathbb{F}_p$ if the action of Frob_p on $Y^*(\ell)$ is even, and $k = \mathbb{F}_{p^2}$ if the Frob_p-action is odd.*

Theorem B is a less precise version of Theorem 3.5.1.

Proof. The first statement follows from Theorem 2.2.2(1). Statements (2) and the existence of the at most quadratic L such that N_B is geometrically connected follow from Proposition 2.3.2. The description of the Galois groups in (3) follows from Corollary 3.3.4, and the exact fields of definitions for the fibers in (4) and (5) are a consequence of Proposition 2.3.2 and Remark 2.3.3. □

Remark 3.5.2. A subgroup A of a group B is G-defining if A is normal and $B/A \cong G$. Let E be an elliptic curve over $\mathbb{Q}$, and $x_0 \in E^\circ(\overline{\mathbb{Q}})$ a geometric point. Recall that

$$\overline{F(\ell)} := \mathrm{Epi}^{\mathrm{ext}}(\pi_1(E^\circ_{\overline{\mathbb{Q}}}, x_0), \mathrm{PSL}_2(\mathbb{F}_\ell))/D(\ell)$$

is in bijection with the set of $\mathrm{PSL}_2(\mathbb{F}_\ell)$-defining subgroups of $\pi_1(E^\circ_{\overline{\mathbb{Q}}}, x_0)$. Via this bijection, we may speak of the trace invariant of a $\mathrm{PSL}_2(\mathbb{F}_\ell)$-defining subgroup. In the notation of Theorem 3.5.1, if $[L : \mathbb{Q}] = 2$, then it follows from the Chebotarev density theorem that for a fixed $\ell \equiv 1, 3, 13, 15 \mod 16$, the set of primes p such that Frob_p acts as an even (resp. odd) permutation on the set of $\mathrm{PSL}_2(\mathbb{F}_\ell)$-defining subgroups of $\pi_1(E^\circ_{\overline{\mathbb{Q}}}, x_0)$ of trace invariant -2 each have density $\frac{1}{2}$.

4. Large Markoff orbits over finite fields

For a prime ℓ, we will adapt Meiri–Puder's method to apply to the maximal Q_ℓ-orbit of $Y^*(\ell)$, and show that Q_ℓ is the full alternating or symmetric group on the maximal orbit. In contrast to Theorem 3.5.1, this will remove the restriction coming from [BGS16a] that ℓ lies outside the small exceptional set $\mathcal{E}$ of primes. Since Q_ℓ acts transitively on the maximal orbit, many arguments from [MP18] can be adapted. This analysis will give Theorem C. Throughout this section, we assume that ℓ is odd.

4.1. **The Large Orbit.**

Definition 4.1.1. We let $\mathcal{O}(\ell)$ denote a Q_ℓ-orbit of maximal size in $Y^*(\ell)$, and denote by $\overline{Q}_\ell$ the permutation group induced by the Q_ℓ-action on $\mathcal{O}(\ell)$.

Although we do not know the size of a maximal orbit, we have a nice lower bound of its size given by Theorem 3.1.1 and the easy computation of $|Y^*(\ell)|$ recorded in [MP18, Lemmas 2.2 and 2.3]. In particular, for any $\varepsilon > 0$ there is a smallest integer N_ε such that for prime $\ell \geq N_\varepsilon$ we have that

$$|\mathcal{O}(\ell)| \geq |Y^*(\ell)| - \ell^\varepsilon = \begin{cases} \frac{\ell(\ell+3)}{4} - \ell^\varepsilon & \text{if } \ell \equiv 1 \mod 4 \\ \frac{\ell(\ell-3)}{4} - \ell^\varepsilon & \text{if } \ell \equiv 3 \mod 4. \end{cases} \tag{4-1-1}$$

In particular, this shows there is a unique maximal orbit for sufficiently large ℓ.

The main theorem in this section is the following.

Theorem 4.1.2. *Fix a prime ℓ for which $\boldsymbol{P}(\ell)$ holds. If $\ell \equiv 1 \mod 4$ then assume that $\ell \geq \max(N_{1/2}, 13)$, while if $\ell \equiv 3 \mod 4$ then $\ell \geq \max(N_{1/2}, 23)$. Then $\overline{Q}_\ell$ is the full alternating or symmetric group on $\mathcal{O}(\ell)$.*

The proof of this theorem is very similar to the proofs of [MP18, §4]. The strategy is to show that the permutation action of $\overline{Q}_\ell$ on $\mathcal{O}(\ell)$ is primitive, and then use a group-theoretic result classifying primitive permutation groups with extra conditions. The case that $\ell \equiv 1 \mod 4$ is significantly easier, and will be dealt with at the end in §4.5. When $\ell \equiv 3 \mod 4$, we first establish analogues of [MP18, Proposition 4.2 and 4.3] that work for the maximal $\overline{Q}_\ell$-orbit $\mathcal{O}(\ell)$, and use them to show the permutation action is primitive in §4.2. Then in §4.3 and §4.4 we use a classification of primitive permutation groups containing an element with a large number of fixed points, which is a consequence of the classification of finite simple groups. Our argument is significantly harder than that of [MP18, §4.3] as we do not know the exact size of $\mathcal{O}(\ell)$; this makes it more complicated to eliminate cases and conclude that $\overline{Q}_\ell$ contains the alternating group of permutations of the set $\mathcal{O}(\ell)$.

4.2. **Primitivity for $\ell \equiv 3 \mod 4$.** We briefly recall some further background about Markoff triples modulo ℓ. The conic $C_1(\pm a) \subset Y^*(\ell)$ is the set of elements $[x_1, x_2, x_3] \in Y^*(\ell)$ with $x_1 = a$. There is a very important rotation element $\mathrm{rot}_1 := R_3 \circ \tau_{23}$ sending (x, y, z) to $(x, z, xz - y)$ which visibly acts on $Y^*(\ell)$ and preserves the conics $C_1(\pm a)$.

Recall [MP18, Definition 2.1] that $x \in \mathbb{F}_\ell$ is called *hyperbolic*, *elliptic*, or *parabolic* if $x^2 - 4$ is a square in $\mathbb{F}_\ell^\times$, a non-square in $\mathbb{F}_\ell^\times$, or zero, respectively. This categorization is invariant under sign change. The cycle structure of rot_1 on $C_1(\pm a)$ depends on whether a is hyperbolic, elliptic, or parabolic: this is conveniently summarized in [MP18, Lemma 2.2 and 2.3, Tables 1 and 2]; we urge the reader to use them as reference.

We now begin our analysis of the maximal orbit $\mathcal{O}(\ell)$ when $\ell \equiv 3 \mod 4$.

Lemma 4.2.1. *Let $\ell \equiv 3 \mod 4$ be prime. If $\ell \geq N_{1/2}$ and $\boldsymbol{P}(\ell)$ holds, then $[3, 3, 3]$ is in $\mathcal{O}(\ell)$.*

Proof. When $\ell \equiv 3 \mod 4$, it is shown in the proof of [MP18, Thm. 4.1] that assuming the order of $\frac{3+\sqrt{5}}{2} \in \mathbb{F}_{\ell^2}$ is at least $32\sqrt{\ell + 1}$, the element $[3, 3, 3]$ belongs to a rot_1-cycle of length at least $16\sqrt{\ell + 1}$. As $\ell \geq N_{1/2}$, we know that $|Y^*(\ell)\backslash\mathcal{O}(\ell)| \leq \ell^{1/2}$ so this cycle must lie in $\mathcal{O}(\ell)$. □

Recall that a $\overline{Q}_\ell$-block is a subset $B \subseteq \mathcal{O}(\ell)$ such that for every $g \in \overline{Q}_\ell$, either $gB = B$ or $gB \cap B = \emptyset$. We say a coordinate $j \in \{1, 2, 3\}$ is homogenous in a block B if the jth coordinate of every triple in B has the same type (all hyperbolic, elliptic, or parabolic).

Remember that we say the $\overline{Q}_\ell$ action is *primitive* if the only blocks are singletons and $\mathcal{O}(\ell)$.

Proposition 4.2.2 (Analogue of [MP18, Prop 4.2]). *Let $\ell \equiv 3 \mod 4$ be a prime such that $\ell \geq N_{1/2}$ and $\boldsymbol{P}(\ell)$ holds, and let $B \subsetneq \mathcal{O}(\ell)$ be a proper $\overline{Q}_\ell$-block. Then at least two of the coordinates $\{1, 2, 3\}$ are homogeneous in B.*

Proof. In order to follow the proof of [MP18, Prop. 4.2], we use Lemma 4.2.1 to see that $[3, 3, 3]$ is in the maximal orbit $\mathcal{O}(\ell)$. The rest of the argument is the same. □

Recall that $d_\ell(\pm x)$ denotes the length of the cycles of rot_1 on $C_1(\pm x)$.

Proposition 4.2.3 (Analogue of [MP18, Prop. 4.3]). *Let $\ell \equiv 3 \mod 4$ be a prime such that $\ell \geq N_{1/2}$ and $\boldsymbol{P}(\ell)$ holds. Let $x \in \mathbb{F}_\ell\backslash\{0, \pm 2\}$ satisfy $d_\ell(\pm x) \geq 16\sqrt{\ell + 1}$. Then for every $j \in \{1, 2, 3\}$, every proper $\overline{Q}_\ell$-block $B \subsetneq \mathcal{O}(\ell)$ contains at most one solution with j-th coordinate $\pm x$.*

Proof. The proposition follows from the proof of [MP18, Prop. 4.3] and Proposition 4.2.2. □

Using Proposition 4.2.3, the analogue of [MP18, Cor. 4.4] immediately follows. That is, under the conditions in Proposition 4.2.3, if $B \subsetneq \mathcal{O}(\ell)$ is a proper $\overline{Q}_\ell$-block containing some solution with first coordinate $\pm x$, and another solution with first coordinates $\pm x'$, then $d_\ell(\pm x) = d_\ell(\pm x')$. With these ingredients, we obtain the analogue of [MP18, Thm. 4.1] by replacing $Y^*(\ell)$ by $\mathcal{O}(\ell)$ and remembering that $[3, 3, 3] \in \mathcal{O}(\ell)$ (Lemma 4.2.1).

Theorem 4.2.4 (Analogue of [MP18, Thm. 4.1]). *Let $\ell \equiv 3 \mod 4$ be a prime with $\ell \geq N_{1/2}$ and the property $\boldsymbol{P}(\ell)$. Then the $\overline{Q}_\ell$-action on $\mathcal{O}(\ell)$ is primitive.*

4.3. **Analyzing the Permutation Group for $\ell \equiv 3 \mod 4$.** In this section, we prove that $\overline{Q}_\ell$ contains the alternating group of permutations of the set $\mathcal{O}(\ell)$. This is the analog of [MP18, Proposition 4.15], but it is significantly harder to adapt the proof as we do not know the exact size of $\mathcal{O}(\ell)$. It relies on the following classification of primitive permutation groups containing an element which fixes at least half of the elements of the set it is acting on; Guralnick and Magaard obtain this result as a consequence of the classification of finite simple groups [GM98]. We record the convenient formulation of [MP18, Theorem 4.13].

Theorem 4.3.1. *Let $G \subset S_n$ be a primitive permutation group, and let $x \in G$ have at least $n/2$ fixed points. Then one of the following holds:*

(1) $G = \mathrm{Aff}^2(k)$ is the affine group acting on $\mathbb{F}_2^k$ and x is a transvection (and so in particular is an involution with $n/2$ fixed points).

(2) There are integers $r \geq 1$, $m \geq 5$, and $1 \leq k \leq m/4$ such that $n = \binom{m}{k}^r$, the group S_m acts on the set Δ of k-element subsets of $\{1, \ldots, m\}$ in the natural way, $G \subset S_m \wr S_r$ acts on Δ^r, and the socle $\mathrm{Soc}(G)$ of G is A_m^r.

(3) For some integer $r \geq 1$, $n = 6^r$, the group S_6 acts on $\Delta = \{1, \ldots, 6\}$ by applying an outer automorphism, $G \subset S_6 \wr S_r$ acts on Δ^r, and $\mathrm{Soc}(G) = A_6^r$.

(4) The group G is some variant of an orthogonal group over the field of two elements acting on some collection of 1-spaces of hyperplanes, and the element x is an involution.

Our ultimate goal is to show that $\overline{Q}_\ell$ occurs as Case (2) with $r = 1$ and $k = 1$; this shows that $\overline{Q}_\ell$ is the full alternating or symmetric group on $\mathcal{O}(\ell)$. To do so requires some non-trivial group theory involving wreath products; we briefly recall some background now, and then proceed with the proof of Theorem 4.1.2, making use of several technical results whose statements and proofs are deferred to §4.4.

Let G be a group acting on $\Delta = \{1, \ldots, m\}$, and r a positive integer. Let $\Omega = \{1, \ldots, r\}$, which has a natural action of S_r. Recall that the *wreath product* $G \wr S_r$ is defined to be the semi-direct product $G^r \rtimes S_r$, where S_r acts on $G^r = \prod_{i \in \Omega} G$ by permuting the coordinates. In particular, elements $\pi \in G \wr S_r$ are represented by pairs (σ, τ) where $\sigma = (\sigma_1, \ldots, \sigma_r) \in G^r$ and $\tau \in S_r$. There is a natural action of $G \wr S_r$ on Δ^r, given by

$$\pi(x_1, \ldots, x_r) = (\sigma_1(x_{\tau^{-1}(1)}), \ldots, \sigma_r(x_{\tau^{-1}(r)})). \tag{4-3-1}$$

This gives a natural embedding $\iota : G \wr S_r \hookrightarrow S_n$ where $n = m^r$.

Proof of Theorem 4.1.2 for $\ell \equiv 3 \mod 4$. We will follow the outline of [MP18, Prop. 4.15]. At the beginning, it shows that the permutation $\pi = \mathrm{rot}_1^{(\ell+1)/2}$ fixes exactly $\frac{(\ell+1)(\ell-3)}{8}$ elements of $Y^*(\ell)$. Therefore, since $\ell \geq N_{1/2}$, we have π fixes at least $\frac{(\ell+1)(\ell-3)}{8} - \ell^{1/2} > \frac{\ell(\ell-3)}{8} - \frac{\ell^{1/2}}{2} \geq \frac{|\mathcal{O}(\ell)|}{2}$ elements of $\mathcal{O}(\ell)$. Thus the $\overline{Q}_\ell$-action on $\mathcal{O}(\ell)$ together with the permutation π satisfies the assumptions in Theorem 4.3.1, and we need to rule out all options except for (2) with $k = r = 1$, so that $\overline{Q}_\ell = \mathrm{Alt}(\mathcal{O}(\ell))$ or $\mathrm{Sym}(\mathcal{O}(\ell))$.

Let q be a prime factor of $\frac{\ell-1}{2}$, and let s be a prime factor of $\frac{\ell+1}{2}$. By [MP18, Table 2], rot_1 contains $\frac{(\ell-1)(q-1)}{4q}$ cycles of size q and $\frac{(\ell+1)(s-1)}{4s}$ cycles of size s in $Y^*(\ell)$. So in $\mathcal{O}(\ell)$, rot_1 contains at least $\lceil \frac{(\ell-1)(q-1)}{4q} - \frac{\ell^{1/2}}{q} \rceil \geq 1$ cycles of size q and at least $\lceil \frac{(\ell+1)(s-1)}{4s} - \frac{\ell^{1/2}}{s} \rceil \geq 1$ cycles of size s. Because $\frac{\ell-1}{2}$ is odd and π has a cycle of size q, π is not an involution so the cases (1) and (4) cannot occur.

Again using [MP18, Table 2], notice that rot_1 does not contain any cycle of size divisible by qs; every cycle length divides either $\frac{\ell-1}{2}$ or $\frac{\ell+1}{2}$ which are relatively prime. There would be cycles of length divisible by qs if we were in case (2) with $k \geq 2$; [MP18, Lem. 4.14] shows that the hypotheses of Corollary 4.4.4 are satisfied (note the latter is applied with Δ the set of k element subsets of $\{1, \ldots, m\}$, so the m in Corollary 4.4.4 is $\binom{m}{k}$ in the notation of Theorem 4.3.1). Thus we can rule out case (2) with $k \geq 2$.

Similarly, we will rule out case (3). Note that $\frac{\ell-1}{2}$ is odd as $\ell \equiv 3 \mod 4$. If $\frac{\ell+1}{2}$ is a power of 2, then by the assumption $\ell \geq 23$ we have $\frac{\ell+1}{2} \equiv 0 \mod 8$, and hence $\frac{\ell-1}{2} \equiv 7 \mod 8$ cannot be a power of 3. Thus we may assume that $\{q, s\} \neq \{2, 3\}$. Then S_6 acting on $\{1, \ldots, 6\}$ satisfies the condition for G in Corollary 4.4.4 (no element of S_6 can contain a q-cycle and an s-cycle when $q + s > 6$) which implies there should be cycles of length divisible by qs. But there aren't, so case (3) can be ruled out.

Finally, we need to rule out case (2) with $r \geq 2$ and $k = 1$. So $\overline{Q}_\ell$ is a subgroup of $S_m \wr S_r$, and inherits the action of $S_m \wr S_r$ on $\{1, \ldots, m\}^r$. We may identify $\mathcal{O}(\ell)$ with a subset of r-tuples of elements of $\{1, \ldots, m\}$, and represent rot_1 by a tuple (σ, τ) where σ is a permutation of $\{1, \ldots, m\}$ and τ is a permutation of $\{1, \ldots, r\}$. We have seen that for any primes q and s with $q \mid \frac{\ell-1}{2}$ and $s \mid A := \frac{\ell+1}{2}$ there are rot_1-cycles of size q and of size s, but none of size divisible by qs. Notice that the rot_1-cycle of size A lies in $\mathcal{O}(\ell)$ as $|Y^*(\ell) \backslash \mathcal{O}(\ell)| \leq \ell^{1/2}$.

Fix a prime q dividing $\frac{\ell-1}{2}$ together with an element $(a_1, \ldots, a_r) \in \{1, \ldots, m\}^r = \mathcal{O}(\ell)$. Likewise let $(b_1, \ldots, b_r) \in \{1, \ldots, m\}^r$ be an element in the cycle of size exactly A. Then by Corollary 4.4.5, there exists $i \in \{1, \ldots, r\}$ such that $\tau(i) = i$ and such that the jth component of $\mathrm{rot}_1(b_1, \ldots, b_r)$ is b_j for any $j \neq i$.

In light of (4-3-1), the elements in the rot_1-cycle containing $(b_1, \ldots, b_r)$ only differ in the i-th component. Since the cycle has length $\frac{\ell+1}{2}$, we must have $m \geq \frac{\ell+1}{2}$. But $n = m^r$, and hence $n \geq \frac{(\ell+1)^2}{4}$. This contradicts the fact that $n = |\mathcal{O}(\ell)| \leq |Y^*(\ell)| = \frac{\ell(\ell-3)}{4}$.

Thus the only possibility is case (2) with $r = 1$ and $k = 1$, which shows that $\overline{Q}_\ell$ is the full alternating or symmetric group on $\mathcal{O}(\ell)$. □

4.4. **Arguments with Wreath Products.**

We continue the notation for wreath products introduced before the proof of Theorem 4.1.2, with $G \subset S_m$ and with $G \wr S_r$ acting on $\Delta^r = \{1, \ldots, m\}^r$. The action gives a natural inclusion $\iota : G \wr S_r \hookrightarrow S_n$, where $n = m^r$. We will need to work with powers in the wreath product: notice we have that $\pi^i = (\sigma_i, \tau^i)$ for some $\sigma_i = (\sigma_{i,1}, \ldots, \sigma_{i,r}) \in G^r$. Furthermore, we have

$$\pi^i(x_1, \ldots, x_r) = (\sigma_{i,1}(x_{\tau^{-i}(1)}), \ldots, \sigma_{i,r}(x_{\tau^{-i}(r)})). \tag{4-4-1}$$

Our main goal is to establish the following:

Proposition 4.4.1. *Let $\pi \in G \wr S_r$. Assume $(a_1, \ldots, a_r), (b_1, \ldots, b_r) \in \Delta^r$ belong to $\iota(\pi)$-cycles of size divisible by distinct primes q and s respectively. Then at least one of the following holds:*

(1) $\iota(\pi)$ has a cycle of size divisible by qs;

(2) There exist $i \in \{1, \ldots, r\}$ and an integer t relatively prime to qs such that $\tau^t(i) = i$ and for any $j \neq i$ we have that the j-th component of $\pi^t(a_1, \ldots, a_r)$ is a_j, and that the j-th component of $\pi^t(b_1, \ldots, b_r)$ is b_j.

In the proof, for convenience we will omit ι and also use π to denote the image of π in S_n.

Definition 4.4.2. Given a subset $S \subset \{1, \dots, r\}$ and $(x_1, \dots, x_r), (y_1, \dots, y_r) \in \Delta^r$ we say that

$$(x_1, \dots, x_r) = (y_1, \dots, y_r) \text{ at } S$$

provided that for all $j \in S$ we have $x_j = y_j$. Given a cycle C of an element of S_r, we say that two elements of Δ^r are equal at C if the elements are equal at elements appearing in the cycle.

We say that two elements of Δ^r are equal away from S if they are equal on $\{1, \dots, r\} - S$, and likewise for cycles.

For $\pi \in G \wr S_r$, we say that π fixes $(x_1, \dots, x_r)$ at S if $\pi(x_1, \dots, x_r)$ equals $(x_1, \dots, x_r)$ at S, and similarly for cycles and fixing away from.

For $\pi^i = (\sigma_i, \tau^i) \in G \wr S_r$ and $(x_1, \dots, x_r) \in \Delta^r$, notice that

$$\pi^i(x_1, \dots, x_r) = (x_1, \dots, x_r) \text{ at } S$$

provided for all $j \in S$

$$\sigma_{i,j}(x_{\tau^{-i}(j)}) = x_j. \tag{4-4-2}$$

We begin with a reduction.

Lemma 4.4.3. *It suffices to prove Proposition 4.4.1 when $(a_1, \dots, a_r)$ and $(b_1, \dots, b_r)$ belong to cycles with length a power of q and s respectively, and when, writing $\pi = (\sigma, \tau)$, there exists a cycle C of τ whose length is $d = q^{n_1} s^{n_2}$ and such that π fixes $(a_1, \dots, a_r)$ and $(b_1, \dots, b_r)$ away from C.*

Proof. We adopt the hypotheses of Proposition 4.4.1. Assume that $(a_1, \dots, a_r)$ (resp. $(b_1, \dots, b_r)$) belongs to a π-cycle of size Aq^* (resp. Bs^*), where A is prime to q (resp. B is prime to s) and q^* is a power of q (resp. s^* is a power of s). If $q \mid B$ or $s \mid A$, then the statement (1) in Proposition 4.4.1 holds. Otherwise, $\gcd(q, B) = \gcd(s, A) = 1$ and we set $\varpi := \pi^{AB}$, so $(a_1, \dots, a_r)$ and $(b_1, \dots, b_r)$ belong to ϖ-cycles of size exactly q^* and s^* respectively.

Write $\varpi = (\sigma', \tau')$. Suppose that there are disjoint cycles C_1 and C_2 for τ' such that ϖ does not fix $(a_1, \dots, a_r)$ at C_1 and ϖ does not fix $(b_1, \dots, b_r)$ at C_2. Then consider the element $(x_1, \dots, x_r) \in \Delta^r$ defined by $x_i = a_i$ if i appears in C_1, and $x_i = b_i$ otherwise. Looking at (4-4-1), it is clear that the j-th entry of $\varpi^i(x_1, \dots, x_r)$ will depend only on x_k such that k is in the same τ'-orbit as j. In particular, as $(x_1, \dots, x_r)$ equals $(a_1, \dots, a_r)$ at C_1, as ϖ does not fix $(a_1, \dots, a_r)$ at C_1, and as the ϖ-orbit of $(a_1, \dots, a_r)$ has size q^*, we deduce that

$$\varpi^i(x_1, \dots, x_r) = (x_1, \dots, x_r)$$

implies that $q \mid i$. Likewise, working with $(b_1, \dots, b_r)$ and C_2 we deduce that $s \mid i$. Thus the ϖ-orbit of $(x_1, \dots, x_r)$ is has size a multiple of qs. This establishes statement Proposition 4.4.1(1) in this case.

It remains to consider the case that there is a cycle C for τ' such that ϖ fixes both $(a_1, \dots, a_r)$ and $(b_1, \dots, b_r)$ away from C. Let e be the maximal divisor of $|C|$ that is not divisible by q or s. Then C breaks into e disjoint τ'^e-cycles of size $|C|/e$, and we will study the action of ϖ^e. If there are two cycles C_1 and C_2 for τ'^e on which ϖ^e doesn't fix $(a_1, \dots, a_r)$ and $(b_1, \dots, b_r)$ respectively, then we can repeat the argument of the previous paragraph, establishing statement Proposition 4.4.1(1).

Otherwise, there is a unique cycle C for τ'^e away from which ϖ^e fixes $(a_1, \dots, a_r)$ and $(b_1, \dots, b_r)$. The length of this cycle is $d := |C|/e = q^{n_1} s^{n_2}$. The sizes of the orbits of $(a_1, \dots, a_r)$ and $(b_1, \dots, b_r)$ under ϖ^e are a power of q and a power of s respectively, because e is relatively prime to q and s. A cycle for ϖ^e of size divisible by qs gives the same for π, and statement Proposition 4.4.1(2) for $\varpi^e = \pi^{ABe}$ gives the same for π as A, B, and e are coprime to q and s. This completes the reduction. □

Proof of Proposition 4.4.1. We may assume we are in the special case described in Lemma 4.4.3. Let $\pi = (\sigma, \tau)$. Without loss of generality, the cycle C consists of the integers $\{1, 2, \ldots, d\} \subset \Delta$ and that τ acts on C via

$$\tau(j) = (j \bmod d) + 1 \text{ for } 1 \leq j \leq d = q^{n_1}s^{n_2}.$$

Here $(j \bmod d) \in \{0, 1, \ldots, d-1\}$ indicates the remainder when j is divided by d. Furthermore, since π fixes $(a_1, \ldots, a_r)$ and $(b_1, \ldots, b_r)$ away from C, but the tuples lie in cycles of different lengths, they must differ at some element of C. So assume $a_1 \neq b_1$.

Case 1: Suppose $d = 1$. As π fixes $(a_1, \ldots, a_r)$ away from $C = (1)$, by (4-4-2) we see that

$$\sigma_{1,j}(a_{\tau^{-1}(j)}) = a_j \text{ for } j > 1.$$

Because $\tau(1) = 1$ and τ permutes $\{2, 3, \ldots, r\}$, we see that

$$\pi(a_1, a_2, \ldots, a_r) = (\sigma_{1,1}(a_1), \sigma_{1,2}(a_{\tau^{-1}(2)}), \ldots, \sigma_{1,r}(a_{\tau^{-1}(r)})) = (\sigma_{1,1}(a_1), a_2, \ldots, a_r).$$

We can make a similar calculation with $(b_1, b_2, \ldots, b_r)$, so statement Proposition 4.4.1(2) with $i = 1$ and $t = 1$ holds in this case.

Case 2: Suppose d is divisible by only one of q and s. Without loss of generality, we assume d is a power of q. We let q^* and s^* denote the size of the π-cycles that $(a_1, \ldots, a_r)$ and $(b_1, \ldots, b_r)$ belong to, and denote $q' := \max(d, q^*)$. Note that by construction we have $\tau^{q'}(j) = j$ for $1 \leq j \leq d$.

We write $\pi^i = ((\sigma_{i,1}, \ldots, \sigma_{i,r}), \tau^i)$, and first suppose $\sigma_{q',1}(b_1) = b_1$. We know that $\pi^{q's^*}$ fixes $(a_1, \ldots, a_r)$ and $(b_1, \ldots, b_r)$, and hence in light of (4-4-1) it fixes $(a_1, b_2, \ldots, b_r)$ since $\tau^{q's^*}(1) = 1$. As $\pi^{q'}$ does not fix $(b_1, \ldots, b_r)$ and

$$\pi^{q'}(b_1, \ldots, b_r) = (\sigma_{q',1}(b_{\tau^{-q'}(1)}), \ldots, \sigma_{q',r}(b_{\tau^{-q'}(r)})) = (b_1, \sigma_{q',2}(b_{\tau^{-q'}(2)}), \ldots, \sigma_{q',r}(b_{\tau^{-q'}(r)})),$$

there exists $i > 1$ such that $\sigma_{q',i}(b_{\tau^{-q'}(i)}) \neq b_i$. Therefore, it follows that

$$\pi^{q'}(a_1, b_2, \ldots, b_r) \neq (a_1, b_2, \ldots, b_r). \tag{4-4-3}$$

On the other hand, as $\gcd(d, s^*) = 1$, we see τ^{s^*} sends 1 to $\tau^{s^*}(1) \neq 1$. Then we obtain $b_{\tau^{s^*}(1)} = \sigma_{s^*,\tau^{s^*}(1)}(b_1)$, because π^{s^*} fixes $(b_1, \ldots, b_r)$. Thus we obtain

$$\pi^{s^*}(a_1, b_2, \ldots, b_r) \neq (a_1, b_2, \ldots, b_r) \tag{4-4-4}$$

because the $\tau^{s^*}(1)$-th component of the two sides are $\sigma_{s^*,\tau^{s^*}(1)}(a_1)$ and $b_{\tau^{s^*}(1)} = \sigma_{s^*,\tau^{s^*}(1)}(b_1)$, which are not equal by the assumption $a_1 \neq b_1$. By (4-4-3) and (4-4-4), $(a_1, b_2, \ldots, b_r)$ belongs to a π-cycle of size divisible by q and s since we knew $\pi^{q's^*}$ fixes $(a_1, b_2, \ldots, b_r)$, which proves Proposition 4.4.1(1).

Now suppose $\sigma_{q',1}(b_1) \neq b_1$. We consider the element $(b_1, a_2, \ldots, a_r)$, which, similarly as above, we will show belongs to a π-cycle of size divisible by $q's^*$. Note that

$$\pi^{q'}(b_1, a_2, \ldots, a_r) \neq (b_1, a_2, \ldots, a_r)$$

as the first components are $\sigma_{q',1}(b_1)$ and b_1 respectively. So in this case it suffices to show

$$\pi^{s^*}(b_1, a_2, \ldots, a_r) \neq (b_1, a_2, \ldots, a_r). \tag{4-4-5}$$

As $\gcd(q', s^*) = 1$, for each $1 < i \leq d$, there is a positive integer j such that $s^*j \equiv i-1 \mod q'$. If (4-4-5) does not hold, then π^{s^*j} fixes $(b_1, a_2, \dots, a_r)$. Then by studying the i-th component we have

$$\sigma_{s^*j,i}(b_1) = a_i, \tag{4-4-6}$$

and it implies $b_i = a_i$ for each $1 < i \leq d$ because $\sigma_{s^*j,i}(b_1)$ is also the i-th component of $\pi^{s^*j}(b_1, \dots, b_r)$ which is b_i. Consider

$$\begin{aligned} \pi^{q'}(b_1, \dots, b_r) &= \pi^{q'}(b_1, a_2, \dots, a_d, b_{d+1}, \dots, b_r) \\ &= (\sigma_{q',1}(b_1), a_2, \dots, a_d, \sigma_{q',d+1}(b_{\tau^{-q'}(d+1)}), \dots, \sigma_{q',r}(b_{\tau^{-q'}(r)})) \end{aligned}$$

where the second equality uses that $\sigma_{q',i}(a_i) = a_i$ for $1 \leq i \leq d$ since $\pi^{q'}$ fixes $(a_1, a_2, \dots, a_r)$. Notice that $\pi^{q'}(b_1, \dots, b_r)$ belongs to a cycle of size s^*. Then for j with $s^*j \equiv i-1 \mod q'$, looking at the ith components of $\pi^{s^*j} \circ \pi^{q'}(b_1, \dots, b_r)$ we conclude, for each $1 < i \leq d$, that

$$a_i = \sigma_{s^*j,i}(\sigma_{q',1}(b_1)), \tag{4-4-7}$$

Then (4-4-6) and (4-4-7) contradict the assumption $\sigma_{q',1}(b_1) \neq b_1$, establishing (4-4-5).

Case 3: Suppose $d = q^{n_1}s^{n_2}$ with $n_1, n_2 > 0$. We denote $q' := \max(q^*, q^{n_1})$ and $s' := \max(s^*, s^{n_2})$. We will show that statement (1) holds in this case. We begin by computing that

$$\pi^{q'}(b_1, a_2, \dots a_r) = (a_1, \dots, a_{\tau^{q'}(1)-1}, \sigma_{q',\tau^{q'}(1)}(b_1), a_{\tau^{q'}(1)+1}, \dots, a_r) \tag{4-4-8}$$

using (4-4-2) and the hypothesis that $\pi^{q^*}(a_1, \dots, a_r) = (a_1, \dots, a_r)$. As $a_1 \neq b_1$, we see that

$$\pi^{q'}(b_1, a_2, \dots, a_r) \neq (b_1, a_2, \dots a_r) \tag{4-4-9}$$

We next prove that

$$\pi^{s'}(b_1, a_2, \dots, a_r) \neq (b_1, a_2, \dots, a_r). \tag{4-4-10}$$

Assume otherwise, that $\pi^{s'}(b_1, a_2, \dots, a_r) = (b_1, a_2, \dots, a_r)$; by considering the $\tau^{s'}(1)$-th component of this equality we have that

$$\sigma_{s',\tau^{s'}(1)}(b_1) = a_{\tau^{s'}(1)}. \tag{4-4-11}$$

On the other hand, $\pi^{q'}(b_1, a_2, \dots, a_r)$ is also fixed by $\pi^{s'}$ by our assumption. So, similarly, by (4-4-8) and considering the $\tau^{s'}(1)$-th component of

$$\pi^{s'}(\pi^{q'}(b_1, a_2, \dots, a_r)) = \pi^{q'}(b_1, a_2, \dots, a_r),$$

we see that

$$\sigma_{s',\tau^{s'}(1)}(a_1) = a_{\tau^{s'}(1)}. \tag{4-4-12}$$

Then (4-4-11) and (4-4-12) contradict the assumption that $a_1 \neq b_1$, so we proved (4-4-10).

On the other hand, since $\tau^{q's'} = 1$ and $\pi^{q's'}$ fixes $(a_1, \dots, a_r)$ and $(b_1, \dots, b_r)$, we see that $\pi^{q's'}$ fixes $(b_1, a_2, \dots, a_r)$. Then (4-4-9) and (4-4-10) show that $(b_1, a_2, \dots, a_r)$ lies in a cycle of order divisible by qs.

□

Corollary 4.4.4. *Let m, r, n be positive integers with $n = m^r$, and let q, s be distinct primes. Assume that G is a permutation group acting on $\Delta = \{1, \dots, m\}$, such that if $g \in G$ has two cycles of sizes divisible by q and s respectively, then g has a cycle of size divisible by qs. Consider the embedding $\iota : G \wr S_r \hookrightarrow S_n$ defined by the natural action of $G \wr S_r$ on Δ^r. If, for some $\pi \in G \wr S_r$,* *the image $\iota(\pi)$ has a cycle of size divisible by q and a cycle of size divisible by s, then $\iota(\pi)$ also has a cycle of size divisible by qs.*

Proof. Assume that $(a_1, \dots, a_r)$ and $(b_1, \dots, b_r)$ belong to π-cycles of size divisible by q and s respectively. By Proposition 4.4.1, it's enough to consider the situation in the case (2). Let t and i be described in Proposition 4.4.1(2), and write $\pi = (\sigma, \tau)$. Then for $j \neq i$, π^t fixes the j-th component of $(a_1, \dots, a_r)$ and $(b_1, \dots, b_r)$, and τ^t fixes i. Therefore a_i and b_i belongs to $\sigma_{t,i}$-cycles in Δ of size divisible by q and s respectively. Then by the assumption in this corollary, we see that $\sigma_{t,i} \in G$ has a cycle of size divisible by qs, and hence π^t also has a cycle of size divisible by qs. □

Corollary 4.4.5. *Fix a prime q, an integer $A > 1$, and an element $\pi = (\sigma, \tau) \in S_m \wr S_r$. Assume $(a_1, \dots, a_r)$ and $(b_1, \dots, b_r)$ belong to π-cycles of length divisible by q and length exactly A respectively. Suppose that for every prime $s \mid A$, $\iota(\pi)$ does not have a cycle of size divisible by qs. Then there exists i such that $\tau(i) = i$ and $\pi(b_1, \dots, b_r)_j = b_j$ for any $j \neq i$.*

Here $\pi(b_1, \dots, b_r)_j$ represents the j-th coordinate of $\pi(b_1, \dots, b_r)$.

Proof. Let $\{s_1, s_2, \dots, s_e\}$ be the prime divisors of A, and write $\pi = (\sigma, \tau)$. By Proposition 4.4.1, for each s_j, we have t_{s_j} and i_{s_j} such that

$$\pi^{t_{s_j}}(a_1, \dots, a_r)_k = a_k, \text{ and } \pi^{t_{s_j}}(b_1, \dots, b_r)_k = b_k, \text{ for any } k \neq i_{s_j} \tag{4-4-13}$$

and such that $\tau^{t_{s_j}}(i_{s_j}) = i_{s_j}$. Notice that this last condition together with (4-4-1) shows that (4-4-13) continues to hold if we modify the i_{s_j}-th entry of $(a_1, \dots, a_r)$ or of $(b_1, \dots, b_r)$.

If $i_{s_j} \neq i_{s_{j'}}$, we would have that $\pi^{t_{s_j} t_{s_{j'}}}(a_1, \dots, a_r) = (a_1, \dots, a_r)$ which contradicts the fact that $q \nmid t_{s_j} t_{s_{j'}}$. So i_{s_j} does not depend on the choice of j and we define $i := i_{s_1}$.

Since $s_j \nmid t_{s_j}$ for each j, the integers $s_1, s_2, \dots, s_e$ are relatively prime and so by the Chinese Remainder Theorem there exists positive integers $c_1, \dots, c_e$ such that $\sum_{j=1}^{e} c_j t_{s_j} \equiv 1 \mod A$; as $(b_1, \dots, b_r)$ lies in a cycle of length A we conclude that

$$\pi^{\sum c_j t_{s_j}}(b_1, \dots, b_r) = \pi(b_1, \dots, b_r).$$

On the other hand, since each $\pi^{t_{s_j}}$ only modifies the ith entry of $(b_1, \dots, b_{i-1}, b, b_{i+1}, \dots, b_r)$ for any $b \in \{1, \dots, m\}$, we have $\pi^{\sum c_j t_{s_j}}(b_1, \dots, b_r)_k = b_k$ for $k \neq i$ as desired. □

4.5. The Case $\ell \equiv 1 \mod 4$.

We now give a short proof of the $\ell \equiv 1 \mod 4$ case of Theorem 4.1.2, following the strategy of [MP18, §3]. The idea is to apply Jordan's Theorem [MP18, Thm. 3.1], which states that every primitive permutation group on n elements which contains a cycle of length a prime p with $p \leq n - 3$ must contain the alternating group.

The key observation is that $C_1(\pm 2) \subset \mathcal{O}(\ell)$, as $C_1(\pm 2)$ is a single $\overline{Q}_\ell$ orbit and has size ℓ (see [MP18, Lem. 2.2]), while $|Y^*(\ell) - \mathcal{O}(\ell)| \leq \ell^{1/2}$ since $\ell \geq N_{1/2}$. By studying the action of rot_1, as in the original it can be deduced that an appropriate power is a ℓ-cycle $\mathcal{O}(\ell)$ containing the conic $C_1(\pm 2)$. We also see that $|\mathcal{O}(\ell)| \geq |Y^*(\ell)| - \ell^{1/2} = \frac{\ell(\ell+3)}{4} - \ell^{1/2} > \ell + 3$ since $\ell \geq 13$. Thus it suffices to check the permutation action is primitive and apply Jordan's theorem.

The proof then proceeds as in [MP18, S3], analyzing blocks of $\mathcal{O}(\ell)$ and again using that $C_1(\pm 2) \subset \mathcal{O}(\ell)$.

4.6. **Finishing the Proof.** Finally, we will deduce Theorem C from Theorem 4.1.2. Let ℓ be an odd prime with the property $\mathbf{P}(\ell)$. If $\ell \equiv 1 \mod 4$ then assume that $\ell \geq \max(N_{1/2}, 13)$, while if $\ell \equiv 3 \mod 4$ then $\ell \geq \max(N_{1/2}, 23)$. Let $\mathcal{M}(\overline{\pi_\ell})$ be the connected component of $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$ containing the $\mathbb{Q}$-rational point $\overline{\pi_\ell}$ from §3.4. In fact, $\overline{\pi_\ell}$ is defined over $\mathbb{Z}[1/|\mathrm{SL}_2(\mathbb{F}_\ell)|]$ (Remark 3.4.2). As $\mathcal{M}(\mathrm{PSL}_2(\mathbb{F}_\ell))^{\mathrm{abs}}$ is defined over $\mathbb{Z}[1/|\mathrm{SL}_2(\mathbb{F}_\ell)|]$, it follows that $\mathcal{M}(\overline{\pi_\ell})$ is also defined over $\mathbb{Z}[1/|\mathrm{SL}_2(\mathbb{F}_\ell)|]$.

Note that $R_3([3,3,3]) = [3,3,6]$, so $[3,3,6] \in \mathcal{O}(\ell)$. Using the identification of Propositions 2.4.2 and 3.2.3 and the Galois correspondence, we know from §3.4 that $\overline{\pi_\ell}$ corresponds to $[3,3,6]$, that the geometric fibers of $\mathcal{M}(\overline{\pi_\ell})$ are identified with $\mathcal{O}(\ell)$, and that the monodromy group is identified with $\overline{Q}_\ell^+$. From Theorem 4.1.2, we know that $\overline{Q}_\ell$ contains the alternating group on $\mathcal{O}(\ell)$. Since $\overline{Q}_\ell^+$ is a normal subgroup of $\overline{Q}_\ell$ of index 1 or 2 and the alternating group is simple, we deduce that $\overline{Q}_\ell^+$ is the alternating or symmetric group on $\mathcal{O}(\ell)$. Then applying Proposition 2.3.2 completes the proof of Theorem C. □

Appendix A. Explicit ramification calculations

A.1. **Details for the Proof of Proposition 3.3.2.** Note that $X^*(3)$ is empty, and Tr is not a bijection for $\ell = 2$ (see 3.2.3).

Lemma A.1.1. *Let $\ell \geq 5$ be a prime. We have the following descriptions of the automorphisms $r, s, t, \gamma_0, \gamma_{1728}$ and the permutations they induce on $X^*(\ell)$ via* Tr *(see 3.2.3):*

$$\begin{array}{rcl c rcl}
r:(a,b) & \mapsto & (a^{-1},b) & & \overline{r} = R_3 : (x,y,z) & \mapsto & (x,y,xy-z)\\
s:(a,b) & \mapsto & (b,a) & & \overline{s} = \tau_{12} : (x,y,z) & \mapsto & (y,x,z)\\
t:(a,b) & \mapsto & (a^{-1},ab) & \xrightarrow{\mathrm{Tr}_*} & \overline{t} = \tau_{23} : (x,y,z) & \mapsto & (x,z,y)\\
\gamma_0:(a,b) & \mapsto & (ab^{-1},a) & & \overline{\gamma}_0 : (x,y,z) & \mapsto & (xy-z,x,x^2y-xz-y)\\
\gamma_{1728}:(a,b) & \mapsto & (b^{-1},a) & & \overline{\gamma}_{1728} : (x,y,z) & \mapsto & (y,x,xy-z)
\end{array}$$

Moreover, we have

(1) γ_0 acts on $X^*(\ell)$ and $Y^*(\ell)$ as permutations of order 3 with exactly one fixed point. This fixed point is given by the triple $(3,3,6)$.

(2) γ_{1728} acts on $X^*(\ell)$ as a permutation of order 2 with exactly two fixed points if $\ell \equiv 1,7 \mod 8$ and with no fixed points otherwise. When $\ell \equiv 1,7 \mod 8$, the fixed points are given by $(\pm 2\alpha, \pm 2\alpha, 4)$, where α is a root of $x^2 - 2$ in $\mathbb{F}_\ell$. Thus in $Y^*(\ell)$, γ_{1728} acts as a permutation of order 2 with a unique fixed point if $\ell \equiv 1,7 \mod 8$ and no fixed points otherwise.

Proof. The formulas for r, s, t were checked in Proposition 3.2.3. For γ_0, γ_{1728}, one can check that the following equalities hold in $\mathrm{Aut}(F_2)$:

$$\gamma_0 = s \circ r \circ s \circ t \circ r \circ s, \qquad \gamma_{1728} = s \circ r$$

The descriptions of $\overline{\gamma}_0, \overline{\gamma}_{1728}$ then follow from those of $\overline{r}, \overline{s}, \overline{t}$, noting that Tr induces an *anti-homomorphism* $\mathrm{Tr}_* : \mathrm{Aut}(F_2) \to \mathrm{Aut}(\mathbb{A}^3)$.

Next, we show that γ_0 has the desired properties. The image of γ_0 in $\mathrm{GL}_2(F_2^{\mathrm{ab}})$ is the order 6 matrix $\left[\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right]$. However γ_0^3 is given by $(a,b) \mapsto (a^{-1}, b^{-1})$ (up to $\mathrm{Inn}(F_2)$) which visibly acts trivially on $X^*(\ell)$ and hence also on $Y^*(\ell)$. Thus, γ_0 acts with order 3 on $Y^*(\ell)$, and we wish to show that it has exactly one fixed point.

From the description of γ_0, we find that the image of (x,y,z) in $Y^*(\ell)$ is a fixed point if and only if

(a) $xy - z = \epsilon_1 x$

(b) $x = \epsilon_2 y$

(c) $x^2 y - xz - y = \epsilon_3 z$

where $\epsilon_i = \pm 1$ and $\epsilon_1\epsilon_2\epsilon_3 = 1$. Moreover (x, y, z) is a fixed point in $X^*(\ell)$ if (a),(b),(c) hold with $\epsilon_i = 1$. Substituting (a) into (c) we find

$$\epsilon_1 x^2 - y = \epsilon_3 z$$

Thus by (b), we find that the fixed points are of the form

$$P_{\epsilon_1,\epsilon_2,x} := (x, \epsilon_2 x, \epsilon_2 x^2 - \epsilon_1 x)$$

for x arbitrary and $\epsilon_1, \epsilon_2 = \pm 1$. We wish to count the number of points of this form which lie on $X^*(\ell) \subset \mathbb{F}_\ell^3$. Any such point must satisfy

$$\begin{aligned} x^2 + x^2 + (\epsilon_2 x^2 - \epsilon_1 x)^2 - x^2(x^2 - \epsilon_1\epsilon_2 x) &= 0 \\ x^2(\epsilon_1\epsilon_2 x + 3) &= 0 \end{aligned}$$

If $\epsilon_1 = \epsilon_2 = 1$ then the only solutions are $x = 0, -3$, corresponding to the points $P_{1,1,0} = (0, 0, 0)$ and $P_{1,1,-3} = (-3, -3, 6)$. The former does not lie on $X^*(\ell)$, so $(-3, -3, 6)$ is the unique fixed point in $X^*(\ell)$. If we allow ϵ_1, ϵ_2 to be arbitrary in $\{\pm 1\}$, then one obtains additionally the points $P_{-1,-1,-3} = (-3, 3, -6)$, $P_{1,-1,-3} = (-3, 3, -6)$, and $P_{-1,1,-3} = (-3, -3, 6)$ which all describe the same point in $Y^*(\ell)$.

Next we consider γ_{1728}. Again, in $\mathrm{Out}(F_2)$, γ_{1728} has order 4, with $\gamma_{1728}^2 = \gamma_0^3$ and hence γ_{1728} acts with order 2 on $X^*(\ell)$ and $Y^*(\ell)$.

Thus the image of (x, y, z) in $Y^*(\ell)$ is a fixed point if and only if

(a) $y = \epsilon_1 x$

(b) $x = \epsilon_2 y$

(c) $xy - z = \epsilon_3 z$

where again $\epsilon_i = \pm 1, \epsilon_1\epsilon_2\epsilon_3 = 1$, and (x, y, z) is a fixed point in $X^*(\ell)$ if (a),(b),(c) hold with $\epsilon_i = 1$. Substituting (a) into (c) we get

$$z + \epsilon_3 z = \epsilon_1 x^2$$

In this case we must have $\epsilon_3 = 1$, or else $x = y = 0$, which would not yield any solutions in $X^*(\ell)$. Thus, any solution in $X^*(\ell)$ has the form:

$$(x, \epsilon_1 x, \frac{\epsilon_1}{2} x^2)$$

Again the choice ϵ_1 is irrelevant in $Y^*(\ell)$, so we may take $\epsilon_1 = 1$, in which case $(x, x, \frac{1}{2}x^2) \in X^*(\ell)$ if and only if

$$x \neq 0 \quad \text{and} \quad x^2 + x^2 + \frac{1}{4}x^4 = \frac{1}{2}x^4$$

Rearranging, we get

$$\frac{1}{4}x^2(x^2 - 8) = 0$$

Since $x \neq 0$, we must have $x = \pm\alpha$ where $\alpha \in \mathbb{F}_\ell^\times$ is a root of $x^2 - 8$. Such an α exists if and only if $\left(\frac{2}{\ell}\right) = 1$, which occurs if and only if $\ell \equiv 1, 7 \mod 8$. In $Y^*(\ell)$ both $x = \alpha, x = -\alpha$ give the same point, whereas in $X^*(\ell)$, we obtain two fixed points. □

References

[Abh57] Shreeram Abhyankar, *Coverings of algebraic curves*, Amer. J. Math. **79** (1957), 825–856. MR 94354

[ACV03] Dan Abramovich, Alessio Corti, and Angelo Vistoli, *Twisted bundles and admissible covers*, Communications in Algebra **31** (2003), no. 8, 3547–3618.

[AM69] Michael Francis Atiyah and Ian Grant Macdonald, *Introduction to commutative algebra*, vol. 2, Addison-Wesley Reading, 1969.

[Asa01] Mamoru Asada, *The faithfulness of the monodromy representations associated with certain families of algebraic curves*, J. Pure Appl. Algebra **159** (2001), no. 2-3, 123–147. MR 1828935

[AV02] Dan Abramovich and Angelo Vistoli, *Compactifying the space of stable maps*, J. Amer. Math. Soc. **15** (2002), no. 1, 27–75. MR 1862797

[BEL18] David El-Chai Ben-Ezra and Alexander Lubotzky, *The congruence subgroup problem for low rank free and free metabelian groups*, J. Algebra **500** (2018), 171–192. MR 3765452

[BER11] Kai-Uwe Bux, Mikhail V. Ershov, and Andrei S. Rapinchuk, *The congruence subgroup property for* $\mathrm{Aut}\, F_2$*: a group-theoretic proof of Asada's theorem*, Groups Geom. Dyn. **5** (2011), no. 2, 327–353. MR 2782176

[Ber13] José Bertin, *Algebraic stacks with a view toward moduli stacks of covers*, Arithmetic and geometry around Galois theory, Progr. Math., vol. 304, Birkhäuser/Springer, Basel, 2013, pp. 1–148. MR 3408163

[BGS16a] Jean Bourgain, Alexander Gamburd, and Peter Sarnak, *Markoff surfaces and strong approximation: 1*, 2016.

[BGS16b] Jean Bourgain, Alexander Gamburd, and Peter Sarnak, *Markoff triples and strong approximation*, C. R. Math. Acad. Sci. Paris **354** (2016), no. 2, 131–135. MR 3456887

[BH95] G. W. Brumfiel and H. M. Hilden, $\mathrm{SL}(2)$ *representations of finitely presented groups*, Contemporary Mathematics, vol. 187, American Mathematical Society, Providence, RI, 1995. MR 1339764

[BR11] José Bertin and Matthieu Romagny, *Champs de hurwitz*, Mémoire de la Société mathématique de France (2011), no. 125-26, 3–219.

[CGMP16] Alois Cerbu, Elijah Gunther, Michael Magee, and Luke Peilen, *The cycle structure of a markoff automorphism over finite fields*, 2016.

[Che18] William Yun Chen, *Moduli interpretations for noncongruence modular curves*, Math. Ann. **371** (2018), no. 1-2, 41–126. MR 3788845

[DD97] Pierre Dèbes and Jean-Claude Douai, *Algebraic covers: field of moduli versus field of definition*, Ann. Sci. École Norm. Sup. (4) **30** (1997), no. 3, 303–338. MR 1443489

[DDH89] Steven Diaz, Ron Donagi, and David Harbater, *Every curve is a Hurwitz space*, Duke Math. J. **59** (1989), no. 3, 737–746. MR 1046746

[DR75] P. Deligne and M. Rapoport, *Correction to: "Les schémas de modules de courbes elliptiques" (modular functions of one variable, ii (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 143–316, Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973)*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1975, pp. p. 149. Lecture Notes in Math., Vol. 476. MR 0382292

[EM12] Jordan S. Ellenberg and D. B. McReynolds, *Arithmetic Veech sublattices of* $\mathrm{SL}(2, \mathbf{Z})$, Duke Math. J. **161** (2012), no. 3, 415–429. MR 2881227

[FM12] Benson Farb and Dan Margalit, *A primer on mapping class groups*, Princeton Mathematical Series, vol. 49, Princeton University Press, Princeton, NJ, 2012. MR 2850125

[GM71] Alexander Grothendieck and Jacob P. Murre, *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme*, Lecture Notes in Mathematics, Vol. 208, Springer-Verlag, Berlin-New York, 1971. MR 0316453

[GM98] Robert Guralnick and Kay Magaard, *On the minimal degree of a primitive permutation group*, J. Algebra **207** (1998), no. 1, 127–145. MR 1643074

[Gol03] William M. Goldman, *The modular group action on real* $\mathrm{SL}(2)$*-characters of a one-holed torus*, Geom. Topol. **7** (2003), 443–486. MR 2026539

[Gol04] William M Goldman, *An exposition of results of fricke*, arXiv preprint math/0402103 (2004).

[Gro71] Alexander Grothendieck, *Revêtements étales et groupe fondamental (SGA 1)*, Lecture notes in mathematics, vol. 224, Springer-Verlag, 1971.

[Hai11] Richard Hain, *Lectures on moduli spaces of elliptic curves*, Transformation groups and moduli spaces of curves, Adv. Lect. Math. (ALM), vol. 16, Int. Press, Somerville, MA, 2011, pp. 95–166. MR 2883686

[Har94] David Harbater, *Abhyankar's conjecture on Galois groups over curves*, Invent. Math. **117** (1994), no. 1, 1–25. MR 1269423

[Kan86] Ernst Kani, *The Galois-module structure of the space of holomorphic differentials of a curve*, J. Reine Angew. Math. **367** (1986), 187–206. MR 839131

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR 772569

[Kod63] Kunihiko Kodaira, *On compact analytic surfaces: Ii*, Annals of Mathematics (1963), 563–626.

[LP01] Alexander Lubotzky and Igor Pak, *The product replacement algorithm and Kazhdan's property (T)*, J. Amer. Math. Soc. **14** (2001), no. 2, 347–363. MR 1815215

[Mac69] Alexander M Macbeath, *Generators of the linear fractional groups*, Proc. Symp. Pure Math, vol. 12, 1969, pp. 14–32.

[Mar79] A. Markoff, *Sur les formes quadratiques binaires indéfinies*, Math. Ann. **15** (1879), 381–406.

[Mar80] ______, *Sur les formes quadratiques binaires indéfinies*, Math. Ann. **17** (1880), no. 3, 379–399. MR 1510073

[MP18] Chen Meiri and Doron Puder, *The Markoff group of transformations in prime and composite moduli*, Duke Math. J. **167** (2018), no. 14, 2679–2720, With an appendix by Dan Carmon. MR 3859362

[MW13] Darryl Mccullough and Marcus Wanderley, *Nielsen equivalence of generating pairs of $SL(2,q)$*, Glasgow Mathematical Journal **55** (2013), no. 03, 481–509.

[Noo04] B. Noohi, *Fundamental groups of algebraic stacks*, J. Inst. Math. Jussieu **3** (2004), no. 1, 69–103. MR 2036598

[Noo05] Behrang Noohi, *Foundations of topological stacks I*, arXiv preprint math/0503247 (2005).

[Obu17] Andrew Obus, *Good reduction of three-point Galois covers*, Algebr. Geom. **4** (2017), no. 2, 247–262. MR 3620638

[OZ81] R. P. Osborne and H. Zieschang, *Primitives in the free group on two generators*, Invent. Math. **63** (1981), no. 1, 17–24. MR 608526

[Pak01] Igor Pak, *What do we know about the product replacement algorithm?*, Groups and computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 301–347. MR 1829489

[Ray94] M. Raynaud, *Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar*, Invent. Math. **116** (1994), no. 1-3, 425–462. MR 1253200

[Ray99] Michel Raynaud, *Spécialisation des revêtements en caractéristique $p > 0$*, Ann. Sci. École Norm. Sup. (4) **32** (1999), no. 1, 87–126. MR 1670532

[RV15] David P. Roberts and Akshay Venkatesh, *Hurwitz monodromy and full number fields*, Algebra Number Theory **9** (2015), no. 3, 511–545. MR 3340543

[RZ10] Luis Ribes and Pavel Zalesskii, *Profinite groups*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 40, Springer-Verlag, Berlin, 2010. MR 2599132

[Sch04] Gabriela Schmithüsen, *An algorithm for finding the Veech group of an origami*, Experiment. Math. **13** (2004), no. 4, 459–472. MR 2118271

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

[Sta18] The Stacks Project Authors, *Stacks Project*, `https://stacks.math.columbia.edu`, 2018.

[Ste98] Katherine F. Stevenson, *Conditions related to π_1 of projective curves*, J. Number Theory **69** (1998), no. 1, 62–79. MR 1611097

[Ste16] Robert Steinberg, *Lectures on Chevalley groups*, University Lecture Series, vol. 66, American Mathematical Society, Providence, RI, 2016, Notes prepared by John Faulkner and Robert Wilson, Revised and corrected edition of the 1968 original [MR0466335], With a foreword by Robert R. Snapp. MR 3616493

[Sza09] Tamás Szamuely, *Galois groups and fundamental groups*, Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press, Cambridge, 2009. MR 2548205

Bât. 307, Université Paris-Sud, 91405 Orsay Cedex, France

Email address: renee.bell@universite-paris-saclay.fr

School of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand

Email address: jeremy.booher@canterbury.ac.nz

Department of Mathematics, Columbia University, 2990 Broadway, New York, NY 10027

Email address: wchen@math.columbia.edu

Department of Mathematics, University of Michigan, 530 Church Street, Ann Arbor, MI 48104, USA

Email address: yyyliu@umich.edu