

GALOIS EMBEDDING PROBLEMS AND NUMBER FIELD COUNTING

ANWESH RAY

ABSTRACT. Let p be a prime number and $1 \rightarrow H \rightarrow G \xrightarrow{q} T \rightarrow 1$ be an exact sequence of finite groups, where H is a nontrivial p -group. Fix a continuous surjection $\pi : G_{\mathbb{Q}} \twoheadrightarrow T$ and finitely many H -conjugation-invariant local conditions $\mathcal{D}$. Let $N_{G,\pi,\mathcal{D}}(X)$ count the continuous surjections $\rho : G_{\mathbb{Q}} \twoheadrightarrow G$ satisfying $q \circ \rho = \pi$ and these local conditions, with $|\Delta_{F_\rho}| \leq X$, where $F_\rho = \overline{\mathbb{Q}}^{\ker \rho}$.

If at least one such lift exists, we prove that, for every $\varepsilon > 0$,

$$X^{p/(|G|(p-1))} \ll_{G,\pi,\mathcal{D}} N_{G,\pi,\mathcal{D}}(X) \ll_{G,\pi,\mathcal{D},\varepsilon} X^{p/(|G|(p-1))+\varepsilon}$$

for all sufficiently large X . This establishes the power of X predicted by Alberts's conjecture for every finite p -group kernel, without any solvability assumption on T . If every element of order p in H lies in $Z(H)$, then every nonempty family satisfies the asymptotic predicted by Alberts:

$$N_{G,\pi,\mathcal{D}}(X) \sim C_{G,\pi,\mathcal{D}} X^{p/(|G|(p-1))} (\log X)^{b_V-1},$$

with $C_{G,\pi,\mathcal{D}} > 0$. As an application, for odd p and $m \geq 2$, we obtain discriminant asymptotics for surjective lifts of a fixed residual Galois representation to $\mathrm{GL}_d(\mathbb{Z}/p^m\mathbb{Z})$, subject to finitely many local conditions, whenever such a lift exists.

1. INTRODUCTION

Malle's conjectures concern the number of extensions of a number field with prescribed Galois group and bounded discriminant [12, 13]. Let k be a number field and let $1 \neq G \subseteq S_n$ be a transitive permutation group. Denote by $N_{k,G}(X)$ the number of k -isomorphism classes of degree- n extensions E/k such that $N_{k/\mathbb{Q}}(\mathfrak{d}_{E/k}) \leq X$ and the Galois group of the Galois closure of E/k , acting on the k -embeddings of E , is permutation isomorphic to G . Here $\mathfrak{d}_{E/k}$ is the relative discriminant ideal. For $g \in G$, define $\mathrm{ind}(g) = n - \#(\{1, \dots, n\}/\langle g \rangle)$, and put $a(G) = \min_{1 \neq g \in G} \mathrm{ind}(g)$. Thus $\mathrm{ind}(g)$ is n minus the number of orbits of g .

The weak form of Malle's conjecture [12] predicts that, for every $\varepsilon > 0$,

$$X^{1/a(G)} \ll_{k,G} N_{k,G}(X) \ll_{k,G,\varepsilon} X^{1/a(G)+\varepsilon}$$

for all sufficiently large X .

The strong form also specifies a logarithmic factor. Let $\mathcal{C}_{\min}(G)$ be the set of conjugacy classes of elements of index $a(G)$. Set $M = |G|$, write $G_k = \mathrm{Gal}(\overline{k}/k)$, and let $\chi_M : G_k \rightarrow (\mathbb{Z}/M\mathbb{Z})^\times$ be the mod- M cyclotomic character. The action $\sigma \cdot [g] = [g^{\chi_M(\sigma)^{-1}}]$ preserves $\mathcal{C}_{\min}(G)$. Set $b(k,G) = \#(G_k \backslash \mathcal{C}_{\min}(G))$. The original strong form [13, Conjecture 1.1] predicts a constant $c_{k,G} > 0$ such that

$$N_{k,G}(X) \sim c_{k,G} X^{1/a(G)} (\log X)^{b(k,G)-1}$$

Date: October 22, 2026.

2020 Mathematics Subject Classification. Primary 11R45, 11F80; Secondary 11R32, 11R34.

Key words and phrases. Galois representations, Malle's conjecture, embedding problems, discriminants, deformation theory.

as $X \rightarrow \infty$. Both invariants depend on the chosen permutation representation. Klüners [10] showed that the predicted logarithmic exponent is incorrect in general. His example is compatible with the weak form of the conjecture.

Throughout this paper, all homomorphisms between profinite groups are continuous, and finite groups have the discrete topology. We consider finite groups in their regular permutation representation. A surjection $\rho : G_{\mathbb{Q}} \twoheadrightarrow G$ cuts out the field $F_{\rho} = \overline{\mathbb{Q}}^{\ker \rho}$, which is Galois over $\mathbb{Q}$ with Galois group isomorphic to G . Conversely, each G -Galois extension gives $|\text{Aut}(G)|$ such surjections. An element $g \in G$ of order r has $|G|/r$ orbits in the regular action. Consequently, $\text{ind}_{\text{reg}}(g) = |G|(1 - \text{ord}(g)^{-1})$ and $a_{\text{reg}}(G) = |G|(1 - \ell_G^{-1})$, where ℓ_G is the smallest prime divisor of $|G|$.

Let p be a prime number and fix a surjection $\bar{\rho} : G_{\mathbb{Q}} \twoheadrightarrow \text{GL}_d(\mathbb{F}_p)$ and an integer $m \geq 2$. One can ask how many surjective lifts to $\text{GL}_d(\mathbb{Z}/p^m\mathbb{Z})$ have splitting field of discriminant at most X . Deformation theory provides methods for constructing lifts with prescribed properties. More generally, suppose that

$$1 \longrightarrow H \longrightarrow G \xrightarrow{q} T \longrightarrow 1 \quad (1.1)$$

is an exact sequence of finite groups in which H is a nontrivial p -group. Fix a surjection $\pi : G_{\mathbb{Q}} \twoheadrightarrow T$, and put $L = \overline{\mathbb{Q}}^{\ker \pi}$. A surjection $\rho : G_{\mathbb{Q}} \twoheadrightarrow G$ satisfying $q \circ \rho = \pi$ is called a proper solution of the embedding problem determined by (1.1) and π . For a proper solution ρ , the equality $\ker \pi = \rho^{-1}(H)$ gives $\ker \rho \subseteq \ker \pi$. Hence $L \subseteq F_{\rho}$, $\text{Gal}(F_{\rho}/\mathbb{Q}) \simeq G$, and $\text{Gal}(F_{\rho}/L) \simeq H$. In particular, $[F_{\rho} : \mathbb{Q}] = |G|$ and $[F_{\rho} : L] = |H|$. We order proper solutions by the absolute discriminant $|\Delta_{F_{\rho}}|$ of the full splitting field. We find that

$$|\Delta_{F_{\rho}}| = |\Delta_L|^{|H|} N_{L/\mathbb{Q}}(\mathfrak{d}_{F_{\rho}/L}),$$

where $\mathfrak{d}_{F_{\rho}/L}$ is the relative discriminant ideal. Since L and $|H|$ are fixed, this is equivalent (up to a fixed scaling) to ordering by the norm of the relative discriminant.

We first recall Alberts's conjecture [2, Conjecture 3.10]. Assume that a proper solution $\rho_0 : G_{\mathbb{Q}} \twoheadrightarrow G$ exists. Let $N_{G,\pi}(X)$ denote the number of surjections $\rho : G_{\mathbb{Q}} \twoheadrightarrow G$ satisfying $q \circ \rho = \pi$ and $|\Delta_{F_{\rho}}| \leq X$. For each nontrivial normal subgroup $N \trianglelefteq G$ contained in H , set

$$a(N) = \min_{1 \neq n \in N} \text{ind}_{\text{reg}}(n).$$

All indices here are computed in the regular permutation representation of G . Let $\mathcal{C}_{\min}(N)$ be the set of N -conjugacy classes of elements attaining this minimum. A continuous homomorphism $\varphi : G_{\mathbb{Q}} \rightarrow G$ defines an action on $\mathcal{C}_{\min}(N)$ by

$$\sigma \star [n]_N = [\varphi(\sigma)n^{\chi_M(\sigma)^{-1}}\varphi(\sigma)^{-1}]_N.$$

Denote the number of orbits by $b_{\varphi}(N)$.

Following [2, Definition 3.8], define

$$\mathcal{B}_{\rho_0} = \max_{\substack{1 \neq N \trianglelefteq G, N \subseteq H \\ a(N)=a(H)}} \max_{\substack{\varphi : G_{\mathbb{Q}} \rightarrow G \\ \varphi \equiv \rho_0 \pmod{N}}} b_{\varphi}(N).$$

The homomorphisms in the inner maximum are continuous and need not be surjective. The congruence means equality after composition with $G \rightarrow G/N$.

Alberts's conjecture predicts a constant $c_{G,\pi} > 0$ such that

$$N_{G,\pi}(X) \sim c_{G,\pi} X^{1/a(H)} (\log X)^{\mathcal{B}_{\rho_0}-1} \quad \text{as } X \rightarrow \infty. \quad (1.2)$$

Thus the predicted power of X is determined by the minimum index among the nonidentity elements of the kernel H . We now specialize Alberts's predicted exponent to our p -group kernel. In the regular representation, $\text{ind}_{\text{reg}}(h) = |G|(1 - \text{ord}(h)^{-1})$. Since every

nonidentity element of H has p -power order and H contains an element of order p , the minimum is

$$a(H) = |G|(1 - p^{-1}).$$

Thus the predicted power is X^α , where

$$\alpha = \frac{p}{(|G|(p-1))}.$$

The logarithmic invariant also simplifies in this setting. Let $\mathcal{C}_p(H)$ be the set of H -conjugacy classes of elements of order p . The fixed quotient π defines an action on this set by $\sigma \star [h]_H = [g_\sigma h^{\bar{\chi}_p(\sigma)^{-1}} g_\sigma^{-1}]_H$, where $q(g_\sigma) = \pi(\sigma)$ and $\bar{\chi}_p : G_{\mathbb{Q}} \rightarrow \mathbb{F}_p^\times$ is the mod- p cyclotomic character. The action is independent of the chosen lift g_σ , since conjugation by H acts trivially on H -conjugacy classes. Put $b_\pi = \#(G_{\mathbb{Q}} \backslash \mathcal{C}_p(H))$. Then

$$\mathcal{B}_{\rho_0} = b_{\rho_0}(H) = b_\pi.$$

Alberts's prediction specializes to

$$N_{G,\pi}(X) \sim c_{G,\pi} X^{p/(\ell|G|(p-1))} (\log X)^{b_\pi-1}.$$

Under the additional hypothesis that every element of order p in H is central in H , the group $V = \{h \in H : h^p = 1\}$ is elementary abelian, and $\mathcal{C}_p(H)$ identifies with $V \setminus \{0\}$. In this case, $\mathcal{B}_{\rho_0} = b_\pi = b_V$, where

$$b_V = \#(G_{\mathbb{Q}} \backslash (V(-1) \setminus \{0\}))$$

for the action $\sigma \star v = \bar{\chi}_p(\sigma)^{-1} \pi(\sigma)(v)$.

Alberts [2, Theorem 1.4 and Corollary 1.5] used the Greenberg–Wiles formula to prove the matching bounds $N_{G,\pi}(X) \asymp X^\alpha (\log X)^{b_\pi-1}$ for abelian H . Alberts and O'Dorney [4, 5] subsequently obtained the full asymptotic. Alberts [1] studied upper bounds obtained by successive abelian extensions. His results give the weak Malle upper bound for nilpotent groups. Koymans and Pagano [11] prove the strong form of Malle's conjecture in the regular representation for nilpotent groups whose elements of order ℓ are central, where ℓ is the smallest prime divisor of the group order. Alberts, Lemke Oliver, Wang and Wood [3] give an inductive framework for summing fixed-quotient counting formulas. Their applications are restricted to abelian normal subgroups and normal subgroups isomorphic to products of S_3 . In a related counting problem, lower bounds for unrestricted $\mathrm{GL}_2(\mathbb{F}_\ell)$ -extensions were obtained from elliptic curves in [18].

1.1. Main results. Fix a prime p and a finite group G with a nontrivial normal p -subgroup H . Put $T = G/H$, and let $q : G \twoheadrightarrow T$ be the quotient map. Fix a continuous surjection $\pi : G_{\mathbb{Q}} \twoheadrightarrow T$, and set $L = \overline{\mathbb{Q}}^{\ker \pi}$. Fix embeddings of decomposition groups $G_{\mathbb{Q}_v} \subset G_{\mathbb{Q}}$, and let S be a finite set of places containing p , ∞ , and every prime ramified in L . For each $v \in S$, choose a subset $\mathcal{D}_v$ of the continuous homomorphisms $\psi : G_{\mathbb{Q}_v} \rightarrow G$ satisfying $q \circ \psi = \pi|_{G_{\mathbb{Q}_v}}$. Assume that $\mathcal{D}_v$ is stable under conjugation by H , and write $\mathcal{D} = (\mathcal{D}_v)_{v \in S}$. There are no local restrictions outside S .

Define

$$N_{G,\pi,\mathcal{D}}(X) = \# \left\{ \rho \in \mathrm{Sur}(G_{\mathbb{Q}}, G) : \begin{array}{l} q \circ \rho = \pi, \\ \rho|_{G_{\mathbb{Q}_v}} \in \mathcal{D}_v \text{ for every } v \in S, \\ |\Delta_{F_\rho}| \leq X \end{array} \right\}. \quad (1.3)$$

Here Sur denotes continuous surjective homomorphisms. All the data G , H , π , S , and $\mathcal{D}$ remain fixed as $X \rightarrow \infty$.

Theorem 1.1. *Put $B = |H|^{[L:\mathbb{Q}]} - 1$. There is a constant $C > 0$ such that*

$$N_{G,\pi,\mathcal{D}}(X) \leq CX^\alpha (\log(X))^B$$

for every $X \geq 2$. If a proper solution satisfying the local conditions exists, then there are a constant $c > 0$ and an integer $b \geq 1$ such that

$$N_{G,\pi,\mathcal{D}}(X) \geq cX^\alpha(\log X)^{b-1}$$

for all sufficiently large X . In particular, every nonempty fiber satisfies

$$\lim_{X \rightarrow \infty} \frac{\log N_{G,\pi,\mathcal{D}}(X)}{\log X} = \frac{p}{|G|(p-1)}.$$

For the asymptotic, suppose that every element of order p in H belongs to $Z(H)$. Then

$$V = \{h \in H : h^p = 1\}. \quad (1.4)$$

Regard V as an $\mathbb{F}_p$ -vector space, and let $V(-1)$ denote the Galois module with action

$$\sigma \star v = \bar{\chi}_p(\sigma)^{-1} \pi(\sigma)(v). \quad (1.5)$$

Here $\pi(\sigma)(v)$ denotes conjugation by any lift of $\pi(\sigma)$ to G . This is independent of the lift because H centralizes V . Recall that $b_V = \#(G_{\mathbb{Q}} \backslash (V(-1) \setminus \{0\}))$.

Theorem 1.2. *Suppose that every element of order p in H is central in H . If the fiber in (1.3) contains a proper solution, then*

$$N_{G,\pi,\mathcal{D}}(X) \sim C_{G,\pi,\mathcal{D}} X^{p/(|G|(p-1))} (\log X)^{b_V-1} \quad (1.6)$$

for a finite positive constant $C_{G,\pi,\mathcal{D}}$.

For $T = 1$ and no local restrictions, our proof of Theorem 1.2 simplifies the proof of the p -group case over $\mathbb{Q}$ of Koymans and Pagano's theorem [11, Theorem 1.1]. Our arguments do not rely on their coordinate parametrization. Instead it uses the abelian counting theorem of Alberts and O'Dorney applied to a fibrewise argument.

The principal application concerns $G_j = \mathrm{GL}_d(\mathbb{Z}/p^j\mathbb{Z})$ for $j \geq 1$, with $m \geq 2$ and a fixed residual representation $\bar{\rho} : G_{\mathbb{Q}} \rightarrow G_1 = \mathrm{GL}_d(\mathbb{F}_p)$. For odd p , every element of order p in $H_m = \ker(G_m \rightarrow G_1)$ belongs to $V_m = \ker(G_m \rightarrow G_{m-1})$. This subgroup is central in H_m and is isomorphic to $M_d(\mathbb{F}_p)$.

Write $N_{\bar{\rho},m,\mathcal{D}}(X)$ for the count in (1.3) with $G = G_m$, $H = H_m$, $T = G_1$, and $\pi = \bar{\rho}$, where the quotient map $G_m \twoheadrightarrow G_1$ is reduction modulo p . Thus it counts surjective lifts of $\bar{\rho}$ satisfying $\mathcal{D}$ whose splitting fields have absolute discriminant at most X .

Corollary 1.3. *Let p be odd. If a surjective lift of $\bar{\rho}$ to G_m satisfying the finite local conditions exists, then*

$$N_{\bar{\rho},m,\mathcal{D}}(X) \sim C_{\bar{\rho},m,\mathcal{D}} X^{\alpha_m} (\log X)^{b_{\bar{\rho}}-1},$$

where $\alpha_m = p/(|G_m|(p-1))$ and $b_{\bar{\rho}}$ is the number of orbits on $M_d(\mathbb{F}_p) \setminus \{0\}$ for the action $\sigma \star A = \bar{\chi}_p(\sigma)^{-1} \bar{\rho}(\sigma) A \bar{\rho}(\sigma)^{-1}$. In particular, $b_{\bar{\rho}}$ is independent of m .

Let us make some remarks on the nonemptiness hypothesis and how it relates to well established lifting theorems for Galois representations. Ramakrishna [16] developed a method for constructing characteristic-zero lifts by allowing auxiliary ramification. In dimension two, his large-image theorem [17, Theorem 1.1] shows that, for $p \geq 7$, every surjective $\mathrm{GL}_2(\mathbb{F}_p)$ -representation admits a lift with image containing $\mathrm{SL}_2(\mathbb{Z}_p)$. A refined argument yields a lift surjective onto $\mathrm{GL}_2(\mathbb{Z}_p)$; see Proposition 8.3. Reduction modulo p^m therefore removes the nonemptiness hypothesis from Corollary 1.3.

Related constructions were developed by Khare, Larsen and Ramakrishna [9], who construct p -adic lifts with prescribed Frobenius properties. Fakhruddin, Khare and Patrikis [8] subsequently established lifting theorems for irreducible odd representations valued in general reductive groups over totally real fields, assuming sufficiently large residual characteristic and suitable local lifts. Whenever a lifting theorem supplies a

surjective lift realizing the prescribed local conditions, its reductions provide the proper solutions required by Corollary 1.3.

Declarations.

Conflict of interest: Not applicable; there is no conflict of interest to report.

Availability of data and materials: No data was generated or analyzed in obtaining the results in this article.

Funding: No funding was received during the preparation of this article.

Use of artificial intelligence: The author used ChatGPT 6 Astra as an exploratory tool to study related papers and to assist in correcting mistakes in the article. It was not used to generate the mathematical ideas or the main results of the article.

2. PRELIMINARY FACTS

In this short preliminary section we identify Alberts's logarithmic invariant, bound the number of surjections defining a fixed field, and recall the tame discriminant formula. Recall that $\alpha = p/(|G|(p-1))$, and write $a = \alpha^{-1}$. Let $\mathcal{B}_{\rho_0}$, $b_{\rho_0}(H)$ and b_{π} be the invariants defined in the introduction.

Lemma 2.1. *If a proper solution ρ_0 exists, then $\mathcal{B}_{\rho_0} = b_{\rho_0}(H) = b_{\pi}$.*

Proof. Every nontrivial subgroup $N \trianglelefteq G$ contained in H contains an element of order p , and all its elements have p -power order. Thus $a(N) = a(H)$. If $\varphi \equiv \rho_0 \pmod{N}$, their conjugation actions on N -conjugacy classes agree. Their twisted actions also agree, so $b_{\varphi}(N) = b_{\rho_0}(N)$.

Put $K = \ker \bar{\chi}_p$. Since ρ_0 is surjective, $\rho_0(K)$ is normal in G and $G/\rho_0(K)$ is a quotient of $G_{\mathbb{Q}}/K$. Its order therefore divides $p-1$. The image of the p -group H in this quotient is trivial, so $H \subseteq \rho_0(K)$.

Let Ω_N be the set of elements of order p in N . The action

$$\sigma \star x = \rho_0(\sigma) x^{\bar{\chi}_p(\sigma)^{-1}} \rho_0(\sigma)^{-1}$$

on Ω_H preserves Ω_N . For every $h \in H$, choose $\sigma \in K$ with $\rho_0(\sigma) = h$. The action of this σ is conjugation by h . In particular, each N -conjugacy class in Ω_N lies in a single $G_{\mathbb{Q}}$ -orbit. Consequently, passing to N -conjugacy classes induces a bijection on $G_{\mathbb{Q}}$ -orbit sets, and $b_{\rho_0}(N) = \#(G_{\mathbb{Q}} \backslash \Omega_N)$.

Since Ω_N is an invariant subset of Ω_H , $b_{\rho_0}(N) \leq b_{\rho_0}(H)$. The subgroup $N = H$ attains equality. The two maxima defining $\mathcal{B}_{\rho_0}$ therefore give $b_{\rho_0}(H)$. On H -conjugacy classes, the action through ρ_0 agrees with the action through π defined in the introduction. Thus $b_{\rho_0}(H) = b_{\pi}$. $\square$

Lemma 2.2. *A field $F/\mathbb{Q}$ occurs as F_{ρ} for at most $|\text{Aut}(G)|$ of the surjections in (1.3).*

Proof. Every surjection with kernel field F induces an isomorphism $\text{Gal}(F/\mathbb{Q}) \simeq G$. Fix one such isomorphism ι . Every other one is uniquely $\gamma \circ \iota$ with $\gamma \in \text{Aut}(G)$. $\square$

Lemma 2.3. *Let $F/\mathbb{Q}$ be Galois of degree g . At a tamely ramified rational prime ℓ with inertia order e ,*

$$v_{\ell}(\Delta_F) = g(1 - e^{-1}). \quad (2.1)$$

For a proper solution of (1.1), inertia at a ramified prime $\ell \notin S$ is tame and cyclic of order p^r , with $r \geq 1$. In particular, $v_{\ell}(\Delta_{F_{\rho}}) \geq a$.

Proof. The first assertion follows from [7, Corollary 4.16], since $F/\mathbb{Q}$ is Galois.

Now suppose that $\ell \notin S$ ramifies in F_{ρ} . Since $L/\mathbb{Q}$ is unramified at ℓ , we have $\pi(I_{\ell}) = 1$. The equality $q \circ \rho = \pi$ gives $\rho(I_{\ell}) \subseteq H$.

The image of wild inertia has ℓ -power order and is contained in the p -group H . Since $\ell \neq p$, this image is trivial. Thus $\rho(I_\ell)$ is a finite cyclic quotient of tame inertia. It is nontrivial because ℓ ramifies, so its order is p^r for some $r \geq 1$. Applying (2.1) gives

$$v_\ell(\Delta_{F_\rho}) = |G|(1 - p^{-r}) \geq |G|(1 - p^{-1}) = a.$$

□

3. A FIXED-FIELD UPPER BOUND

In this section, we bound the number of proper solutions with prescribed ramification support. This gives the upper bound in Theorem 1.1.

Let K be a number field and let Σ be a finite set of its finite places containing the places above p . Let K_Σ be the maximal extension of K unramified outside Σ and the infinite places. Set $G_{K,\Sigma} = \text{Gal}(K_\Sigma/K)$. Let $P_{K,\Sigma}$ be its maximal pro- p quotient, and put $X_{K,\Sigma} = \text{Hom}(G_{K,\Sigma}, \mathbb{F}_p) = \text{Hom}(P_{K,\Sigma}, \mathbb{F}_p)$. Here $\mathbb{F}_p$ is additive, with trivial action. Ramification at real places is allowed.

For a positive squarefree integer R , let Σ_R be obtained from Σ by adjoining the places above the prime divisors of R . Write $\omega(R)$ for the number of these prime divisors, and $d(P)$ for the minimum number of topological generators of a pro- p group P .

Lemma 3.1. *Let P be a pro- p group. If $r = \dim_{\mathbb{F}_p} \text{Hom}(P, \mathbb{F}_p) < \infty$, then P is finitely generated and $d(P) = r$.*

Proof. For the trivial P -module $\mathbb{F}_p$, we have $H^1(P, \mathbb{F}_p) = \text{Hom}(P, \mathbb{F}_p)$. The assertion follows from [15, Proposition 3.9.1]. □

Lemma 3.2. *The group $P_{K,\Sigma}$ is finitely generated. If $c_{K,\Sigma} = d(P_{K,\Sigma})$, then*

$$d(P_{K,\Sigma_R}) \leq c_{K,\Sigma} + [K : \mathbb{Q}]\omega(R). \quad (3.1)$$

Proof. By [15, Theorem 8.3.20(i)], with the infinite places included, the spaces $X_{K,\Sigma}$ and X_{K,Σ_R} are finite. Lemma 3.1 therefore shows that the corresponding pro- p groups are finitely generated and that their generator ranks equal the dimensions of these spaces.

Inflation identifies $X_{K,\Sigma}$ with a subspace of X_{K,Σ_R} . Restriction to inertia induces an injection

$$X_{K,\Sigma_R}/X_{K,\Sigma} \hookrightarrow \bigoplus_{\mathfrak{l} \in \Sigma_R \setminus \Sigma} \text{Hom}(I_{\mathfrak{l}}, \mathbb{F}_p).$$

Indeed, a character trivial on inertia at every new place is unramified outside Σ and the infinite places, and hence factors through $G_{K,\Sigma}$.

Every new place has residue characteristic different from p . Its wild inertia has trivial image in $\mathbb{F}_p$, and the maximal pro- p quotient of tame inertia is procyclic. Thus each summand has dimension at most one. There are at most $[K : \mathbb{Q}]\omega(R)$ new places, so

$$\begin{aligned} d(P_{K,\Sigma_R}) &= \dim_{\mathbb{F}_p} X_{K,\Sigma_R} \\ &\leq \dim_{\mathbb{F}_p} X_{K,\Sigma} + \#(\Sigma_R \setminus \Sigma) \\ &\leq c_{K,\Sigma} + [K : \mathbb{Q}]\omega(R). \end{aligned}$$

This proves (3.1). □

Lemma 3.3. *Put $A = |H|^{[L:\mathbb{Q}]}$. The number of proper solutions unramified outside $S \cup \text{supp}(R)$ is at most*

$$CA^{\omega(R)}, \quad (3.2)$$

where C depends only on the fixed data. If $V \subseteq H$ is normal in G , the same assertion holds for G/V , with $A_V = |H/V|^{[L:\mathbb{Q}]} \leq A$ in place of A .

Proof. Let Σ consist of the finite places of L above S . For every solution under consideration, F_ρ/L is an H -extension unramified outside Σ_R and the infinite places. Hence it is the kernel field of a surjection $P_{L,\Sigma_R} \twoheadrightarrow H$.

A continuous homomorphism from a group with d topological generators to H is determined by the d generator images. Indeed, two such homomorphisms agreeing on the generators agree on a dense subgroup and therefore everywhere. Thus there are at most $|H|^d$ homomorphisms. Distinct kernel fields give distinct kernels, so Lemma 3.2 bounds the number of possible fields by

$$|H|^{c_{L,\Sigma} + [L:\mathbb{Q}]\omega(R)} = |H|^{c_{L,\Sigma}} A^{\omega(R)}.$$

This counts all H -extensions of L with the stated ramification. Requiring Galoisness over $\mathbb{Q}$ only decreases their number. Lemma 2.2 bounds the number of surjections for each remaining field by $|\text{Aut}(G)|$, proving (3.2).

For G/V , the kernel over L is H/V . The same proof applies with H/V in place of H . If $H/V = 1$, the only quotient field is L , so the assertion also holds in this case. $\square$

Proposition 3.4. *The upper bound in Theorem 1.1 holds without a nonemptiness hypothesis.*

Proof. For a proper solution put $Q(\rho) = \prod_{\ell \notin S, \ell \text{ ramified in } F_\rho} \ell$. Lemma 2.3 gives $Q(\rho)^a \leq |\Delta_{F_\rho}|$. Thus $|\Delta_{F_\rho}| \leq X$ implies $Q(\rho) \leq Y = X^{1/a}$. Partitioning by $Q(\rho)$ and applying Lemma 3.3 gives

$$N_{G,\pi,D}(X) \leq C \sum_{n \leq Y} \mu^2(n) A^{\omega(n)}, \quad (3.3)$$

where μ is the Möbius function.

For the positive integer A , let $\tau_A(n)$ count ordered A -tuples of positive integers whose product is n . When n is squarefree, each prime factor is assigned to one of the A entries, so $\tau_A(n) = A^{\omega(n)}$. For all n , it follows that $\mu^2(n) A^{\omega(n)} \leq \tau_A(n)$.

We prove by induction on A that

$$D_A(Y) := \sum_{n \leq Y} \tau_A(n) \ll_A Y (\log(2Y))^{A-1} \quad (3.4)$$

where $Y \geq 1$. For $A = 1$, this is $\lfloor Y \rfloor \leq Y$. If $A \geq 2$, the convolution identity $\tau_A = 1 * \tau_{A-1}$ and the inductive bound give

$$\begin{aligned} D_A(Y) &= \sum_{m \leq Y} D_{A-1}(Y/m) \\ &\ll_A Y \sum_{m \leq Y} \frac{(\log(2Y/m))^{A-2}}{m} \\ &\ll_A Y (\log(2Y))^{A-2} \sum_{m \leq Y} \frac{1}{m} \\ &\ll_A Y (\log(2Y))^{A-1}. \end{aligned}$$

Here $\sum_{m \leq Y} m^{-1} \leq 1 + \log Y \ll \log(2Y)$. This proves (3.4).

Combining (3.3) and (3.4), and using $1/a = \alpha$ and $\log(2X^{1/a}) \ll_a \log(X)$, yields

$$N_{G,\pi,D}(X) \ll X^\alpha (\log(X))^{A-1}.$$

Since $A - 1 = B$, this is the asserted upper bound. $\square$

4. ABELIAN FIBERS AND THE LOWER BOUND

In this section, we parametrize lifts with an elementary abelian kernel in terms of Galois cocycles and apply the counting results of Alberts and O’Dorney. Choosing such a kernel inside $Z(H)$ then gives the lower bound in Theorem 1.1. Let V be any nonzero G -normal elementary abelian subgroup of $Z(H)$. Conjugation on V factors through T , so π makes V a Galois module. We set

$$b(V) = \#(G_{\mathbb{Q}} \backslash (V(-1) \setminus \{0\})).$$

This equals b_V when V is the subgroup in (1.4).

Let $q_V : G/V \rightarrow T$ be the map induced by q . Fix a surjection $\psi : G_{\mathbb{Q}} \rightarrow G/V$ satisfying $q_V \circ \psi = \pi$. Define $N_{\psi}(X)$ to be the number of surjections ρ counted by (1.3) whose composition with the quotient map $G \rightarrow G/V$ equals ψ .

Lemma 4.1. *Let $\rho_0 : G_{\mathbb{Q}} \rightarrow G$ lift ψ . The assignment*

$$f \mapsto \rho_f \quad \text{defined by} \quad \rho_f(\sigma) = f(\sigma)\rho_0(\sigma), \quad (4.1)$$

is a bijection from $Z^1(\mathbb{Q}, V)$ to the lifts of ψ . It induces a bijection from $H^1(\mathbb{Q}, V)$ to their V -conjugacy classes. Every class contains

$$|B^1(\mathbb{Q}, V)| = \frac{|V|}{|V^{G_{\mathbb{Q}}}|} \quad (4.2)$$

actual homomorphisms. These assertions also hold locally upon replacing $G_{\mathbb{Q}}$ by any decomposition group.

Proof. The proof is straightforward and thus is omitted. $\square$

Proposition 4.2. *If ψ has a surjective lift satisfying the local conditions, then there is a constant $c_{\psi} > 0$ such that*

$$N_{\psi}(X) \sim c_{\psi} X^{\alpha} (\log X)^{b(V)-1}. \quad (4.3)$$

Otherwise $N_{\psi}(X) = 0$ for every X .

Proof. Choose a surjective lift ρ_0 satisfying the local conditions. We apply the Alberts–O’Dorney theorem [6, Theorem 1.1 and Corollary 1.2]. We check the local conditions, the ordering, and surjectivity.

For $v \in S$, let $\mathcal{L}_v$ be the subset of $H^1(\mathbb{Q}_v, V)$ consisting of the classes whose twists of $\rho_0|_{G_{\mathbb{Q}_v}}$ belong to $\mathcal{D}_v$. This is well defined since changing a cocycle by a coboundary conjugates its twist by an element of $V \subset H$. For $v \notin S$, take $\mathcal{L}_v = H^1(\mathbb{Q}_v, V)$. Let $H_{\mathcal{L}}^1(\mathbb{Q}, V)$ denote the global classes satisfying these restrictions.

Set $g = |G|$, and let A_f be the degree- g étale algebra associated to ρ_f in the regular permutation representation. Define $D([f]) = |\text{disc}(A_f)|$. Conjugation does not change A_f , so this depends only on $[f]$. To describe it explicitly, set $U_f = \rho_f(G_{\mathbb{Q}})$ and $K_f = \overline{\mathbb{Q}}^{\ker \rho_f}$. The action of U_f on G is free, with $g/|U_f|$ orbits. We find that

$$A_f \simeq \prod_{j=1}^{g/|U_f|} K_f,$$

and consequently,

$$D([f]) = |\Delta_{K_f}|^{g/|U_f|}.$$

Enlarge S to a finite set S_0 containing the primes ramified in ρ_0 . For $\ell \notin S_0$, both ρ_0 and V are unramified, and $\ell \neq p$. Hence $\rho_f(I_{\ell}) = f(I_{\ell}) \subset V$. Wild inertia has trivial image in V . Its nontrivial tame image is cyclic of order p . Such an inertia generator acts on G as g/p cycles of length p . The tame discriminant formula gives $v_{\ell}(D([f])) = a$

for a ramified class and 0 for an unramified class. Thus the minimum exponent in the counting theorem is $a = \alpha^{-1}$.

We also compute its logarithmic exponent. Inflation–restriction at $\ell \notin S_0$ gives

$$0 \longrightarrow H_{\text{ur}}^1(\mathbb{Q}_\ell, V) \longrightarrow H^1(\mathbb{Q}_\ell, V) \longrightarrow V(-1)^{\text{Frob}_\ell} \longrightarrow 0.$$

Indeed, inertia acts trivially on V , its maximal pro- p tame quotient is $\mathbb{Z}_p(1)$, and the unramified quotient has p -cohomological dimension one. The inertia value w satisfies $\text{Frob}_\ell(w) = \ell w$, which gives the indicated inverse cyclotomic twist.

Every inertia value has $|H_{\text{ur}}^1(\mathbb{Q}_\ell, V)|$ preimages. This kernel is $V/(\text{Frob}_\ell - 1)V$, whose order is $|V^{\text{Frob}_\ell}| = |H^0(\mathbb{Q}_\ell, V)|$. The normalized local factor is consequently

$$\frac{1}{|H^0(\mathbb{Q}_\ell, V)|} \sum_{[f_\ell] \in H^1(\mathbb{Q}_\ell, V)} \ell^{-sv_\ell(D_\ell([f_\ell]))} = 1 + (|V(-1)^{\text{Frob}_\ell}| - 1)\ell^{-as}.$$

Here D_ℓ is the local discriminant formed by twisting $\rho_0|_{G_{\mathbb{Q}_\ell}}$.

The action on $V(-1)$ factors through $\Gamma = \text{Gal}(L(\mu_p)/\mathbb{Q})$. Thus these factors are Frobenian. The logarithmic parameter of the counting theorem is the Chebotarev average of their coefficients at ℓ^{-as} . Burnside’s lemma identifies it with

$$\frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} (|V(-1)^\gamma| - 1) = b(V).$$

Theorem 1.1 of [6] now gives a constant $C_\psi > 0$ such that

$$\#\{[f] \in H_{\mathcal{L}}^1(\mathbb{Q}, V) : D([f]) \leq X\} \sim C_\psi X^\alpha (\log X)^{b(V)-1}.$$

Since the chosen ρ_0 is surjective, [6, Corollary 1.2(i)(a)] states that the proportion of these classes whose twists are surjective converges to a positive number ϑ_ψ .

Surjectivity and the local conditions are invariant under V -conjugation. Apply Lemma 4.1 to convert the count of surjective cohomology classes to actual homomorphisms. This gives (4.3) with $c_\psi = |V|\vartheta_\psi C_\psi / |V^{G_{\mathbb{Q}}}| > 0$. If there is no surjective lift compatible with local conditions, the defining set for $N_\psi(X)$ is empty. $\square$

Lemma 4.3. *There is a nonzero G -normal elementary abelian subgroup of $Z(H)$.*

Proof. The proof of this lemma is straightforward and thus is left to the reader. $\square$

Proof of the lower bound in Theorem 1.1. Choose a compatible proper solution ρ_0 , and choose V as in Lemma 4.3. Put $\psi = \rho_0 \bmod V$. Every proper lift of ψ has quotient π , so Proposition 4.2 gives

$$N_{G,\pi,\mathcal{D}}(X) \geq N_\psi(X) \sim c_\psi X^\alpha (\log X)^{b(V)-1}.$$

The set $V(-1) \setminus \{0\}$ is nonempty, so $b(V) \geq 1$. Take $b = b(V)$ and $c = c_\psi/2$ for all sufficiently large X .

Together with Proposition 3.4, the lower bound gives $\log N_{G,\pi,\mathcal{D}}(X) = \alpha \log X + O(\log \log(X))$. Divide by $\log X$ to obtain the stated limit. $\square$

5. A UNIFORM ESTIMATE FOR ABELIAN FIBERS

In this section, we prove an upper bound for $N_\psi(X)$ whose constant is independent of ψ . Assume the hypothesis of Theorem 1.2, and use V from (1.4). In particular, V is normal in G , is elementary abelian, and is centralized by H . Its $G_{\mathbb{Q}}$ -action therefore depends only on π . Set

$$a' = |G|(1 - p^{-2}) \quad \text{and} \quad \frac{a'}{a} = 1 + \frac{1}{p}. \quad (5.1)$$

All constants in this section may depend on the fixed data and on S , but not on the quotient representation ψ . We let $G_{\mathbb{Q},S}$ be the Galois group of the maximal extension of $\mathbb{Q}$ unramified at all finite primes outside S .

Lemma 5.1. *The group $Z^1(G_{\mathbb{Q},S}, V)$ is finite.*

Proof. Since S is finite, $p \in S$, and V is a finite p -primary $G_{\mathbb{Q},S}$ -module, [15, Theorem 8.3.20(i)] shows that $H^1(G_{\mathbb{Q},S}, V)$ is finite.

The coboundary group $B^1(G_{\mathbb{Q},S}, V)$ is an image of V , so it is finite. Since $H^1(G_{\mathbb{Q},S}, V) = Z^1(G_{\mathbb{Q},S}, V)/B^1(G_{\mathbb{Q},S}, V)$, the cocycle group is also finite. $\square$

For each finite $\ell \notin S$, choose an arithmetic Frobenius ϕ_ℓ in the fixed decomposition group. Also choose $\tau_\ell \in I_\ell$ whose image generates the $\mathbb{Z}_p$ -quotient of tame inertia. Since $\ell \neq p$, every continuous homomorphism $I_\ell \rightarrow H$ kills wild inertia and factors through this procyclic quotient. It is therefore determined by the image of τ_ℓ .

In the tame quotient of the decomposition group, conjugation by ϕ_ℓ sends an inertia element to its ℓ th power. We use this relation only after applying a representation that kills wild inertia. The inertia action on V is trivial. Define

$$W_\ell = \{v \in V : \phi_\ell(v) = \ell v\}, \quad n_\ell = |W_\ell| - 1. \quad (5.2)$$

Since $\bar{\chi}_p(\phi_\ell) = \ell \pmod{p}$, the number n_ℓ is the number of fixed points of ϕ_ℓ on $V(-1) \setminus \{0\}$.

Lemma 5.2. *For every $Y \geq 1$,*

$$\sum_{\substack{Q \leq Y \\ Q \text{ squarefree} \\ (Q,S)=1}} \prod_{\ell|Q} n_\ell \ll Y(\log(2Y))^{b_V-1}. \quad (5.3)$$

Here $(Q, S) = 1$ means that no finite prime in S divides Q . The summand for $Q = 1$ is one.

Proof. Put $E = L(\mu_p)$ and $\Gamma = \text{Gal}(E/\mathbb{Q})$. The action on $V(-1)$ factors through Γ , and every prime ramified in E belongs to S . Decompose the finite Γ -set as

$$V(-1) \setminus \{0\} = \coprod_{j=1}^{b_V} \Gamma/J_j,$$

and put $E_j = E^{J_j}$. These fields remain fixed throughout the argument.

Let $a_K(n)$ be the number of nonzero integral ideals of a number field K with absolute norm n . For $\ell \notin S$, the cycles of ϕ_ℓ on Γ/J_j correspond to the primes of E_j above ℓ . Their lengths are the residue degrees. Thus a fixed point corresponds to a prime ideal of norm ℓ , and

$$n_\ell = \sum_{j=1}^{b_V} a_{E_j}(\ell). \quad (5.4)$$

For fixed K , put $A_K(Y) = \sum_{n \leq Y} a_K(n)$. The ideal-counting estimate is $A_K(Y) \ll_K Y$; see [14]. Partial summation gives

$$\sum_{n \leq Y} \frac{a_K(n)}{n} = \frac{A_K(Y)}{Y} + \int_1^Y \frac{A_K(t)}{t^2} dt \ll_K \log(2Y). \quad (5.5)$$

For $1 \leq r \leq b_V$, let $c_r = a_{E_1} * \cdots * a_{E_r}$, where $*$ denotes Dirichlet convolution. We claim that

$$\sum_{n \leq Y} c_r(n) \ll Y(\log(2Y))^{r-1}. \quad (5.6)$$

For $r = 1$ this is the ideal-counting estimate. Suppose $r \geq 2$ and that the assertion holds for $r - 1$. Then

$$\begin{aligned} \sum_{n \leq Y} c_r(n) &= \sum_{m \leq Y} a_{E_r}(m) \sum_{n \leq Y/m} c_{r-1}(n) \\ &\ll Y \sum_{m \leq Y} \frac{a_{E_r}(m)}{m} (\log(2Y/m))^{r-2} \\ &\leq Y (\log(2Y))^{r-2} \sum_{m \leq Y} \frac{a_{E_r}(m)}{m} \\ &\ll Y (\log(2Y))^{r-1}. \end{aligned}$$

The last estimate is (5.5). This proves (5.6) by induction.

The functions a_{E_j} are nonnegative and multiplicative. Their convolution is therefore nonnegative and multiplicative. By (5.4), $c_{b_V}(\ell) = n_\ell$ for $\ell \notin S$. Hence $c_{b_V}(Q) = \prod_{\ell \mid Q} n_\ell$ for every squarefree Q prime to S . The sum in (5.3) is at most $\sum_{n \leq Y} c_{b_V}(n)$, and (5.6) proves the lemma. $\square$

For a surjection $\psi : G_{\mathbb{Q}} \twoheadrightarrow G/V$ above π , write

$$R(\psi) = \prod_{\substack{\ell \notin S \\ \psi(I_\ell) \neq 1}} \ell. \quad (5.7)$$

This is squarefree and finite. As in Section 4, $N_\psi(X)$ counts the proper lifts of ψ satisfying the prescribed local conditions and the discriminant bound.

Proposition 5.3. *There is a constant C such that, for every ψ and every $X \geq 2$,*

$$N_\psi(X) \leq C |V|^{\omega(R(\psi))} R(\psi)^{-a'/a} X^{1/a} (\log(X))^{b_V-1}. \quad (5.8)$$

The constant is independent of ψ and of its restrictions at the places in S .

Proof. Write $R = R(\psi)$. For a lift ρ counted by $N_\psi(X)$, put

$$Q(\rho) = \prod_{\substack{\ell \notin S, \ell \nmid R \\ \rho(I_\ell) \neq 1}} \ell.$$

Then $Q(\rho)$ is squarefree and prime to R . By Lemma 2.3, each inertia image outside S is a cyclic p -subgroup of H generated by $\rho(\tau_\ell)$.

If $\ell \mid R$, the image of $\rho(\tau_\ell)$ in G/V is nontrivial. Thus $\rho(\tau_\ell) \notin V$. Every element of order p in H belongs to V , so $\text{ord}(\rho(\tau_\ell)) \geq p^2$. The tame discriminant formula gives $v_\ell(\Delta_{F_\rho}) \geq |G|(1 - p^{-2}) = a'$.

If $\ell \mid Q(\rho)$, the inertia image is a nontrivial cyclic subgroup of V . It has order p , so $v_\ell(\Delta_{F_\rho}) = a$. Consequently,

$$|\Delta_{F_\rho}| \geq R^{a'} Q(\rho)^a. \quad (5.9)$$

If $R^{a'} > X$, no lift is counted. Otherwise, set

$$Y = (X/R^{a'})^{1/a} \geq 1. \quad (5.10)$$

Every counted lift satisfies $Q(\rho) \leq Y$.

Fix a possible value Q of $Q(\rho)$. We first count the tuples $(\rho(\tau_\ell))_{\ell \notin S}$. For $\ell \mid R$, the element $\psi(\tau_\ell)$ is fixed. Its inverse image under $G \rightarrow G/V$ has $|V|$ elements, so there are at most $|V|$ choices for $\rho(\tau_\ell)$.

For $\ell \nmid R$ outside S , put $v_\ell = \rho(\tau_\ell) \in V$, using additive notation. The representation ρ kills wild inertia at ℓ . Applying it to the relation in the tame quotient gives

$$\rho(\phi_\ell)\rho(\tau_\ell)\rho(\phi_\ell)^{-1} = \rho(\tau_\ell)^\ell.$$

Conjugation on V factors through π , so this identity says $\phi_\ell(v_\ell) = \ell v_\ell$. Thus $v_\ell \in W_\ell$. It has at most n_ℓ choices if $\ell \mid Q$, and is zero if $\ell \nmid QR$. The number of possible tuples is therefore at most

$$|V|^{\omega(R)} \prod_{\ell \mid Q} n_\ell. \quad (5.11)$$

Fix one tuple and one lift ρ_1 having that tuple, if a lift exists. By Lemma 4.1, every other lift ρ_2 of ψ determines a unique $f \in Z^1(\mathbb{Q}, V)$ satisfying $\rho_2(\sigma) = f(\sigma)\rho_1(\sigma)$ for all $\sigma \in G_\mathbb{Q}$. The module action here is the fixed action through π ; it does not depend on ψ or ρ_1 .

Equal tuples give $f(\tau_\ell) = 0$ for every $\ell \notin S$. Since inertia acts trivially on V , the restriction of f to I_ℓ is a homomorphism. It kills wild inertia, whose finite quotients have ℓ -power order, and factors through the $\mathbb{Z}_p$ -quotient of tame inertia. Since τ_ℓ generates that quotient, $f|_{I_\ell} = 0$.

Let K_S be the kernel of $G_\mathbb{Q} \rightarrow G_{\mathbb{Q},S}$. The action on V factors through $G_{\mathbb{Q},S}$. If $i \in I_\ell$ and $\sigma \in G_\mathbb{Q}$, the cocycle identity therefore gives

$$f(\sigma i \sigma^{-1}) = f(\sigma) + \sigma f(i) + \sigma i f(\sigma^{-1}) = \sigma f(i) = 0.$$

Here the first and last terms cancel because i acts trivially on V . The restriction $f|_{K_S}$ is a homomorphism. The group K_S is the closed normal subgroup generated by the inertia groups outside S , so continuity implies $f|_{K_S} = 0$. Thus f descends to $Z^1(G_{\mathbb{Q},S}, V)$.

It follows that each tuple occurs for at most $C_S := |Z^1(G_{\mathbb{Q},S}, V)|$ global lifts. This is finite by Lemma 5.1. The estimate counts all lifts of ψ having the tuple, so it also applies after imposing surjectivity, the local conditions, and the discriminant bound.

By (5.11),

$$N_\psi(X) \leq C_S |V|^{\omega(R)} \sum_{\substack{Q \leq Y \\ Q \text{ squarefree} \\ (Q, RS)=1}} \prod_{\ell \mid Q} n_\ell. \quad (5.12)$$

Dropping the coprimality condition with R and applying Lemma 5.2 gives

$$N_\psi(X) \ll |V|^{\omega(R)} R^{-a'/a} X^{1/a} (\log(2Y))^{b_V - 1}.$$

Since $1 \leq Y \leq X^{1/a}$, we have $\log(2Y) \leq \max\{1, a^{-1}\} \log(X)$. Finally, $b_V \geq 1$ because $V \neq 0$. This proves (5.8). $\square$

6. SUMMING THE FIBERS

In this section, we use the uniform estimate from Section 5 to prove Theorem 1.2.

Proof of Theorem 1.2. The subgroup V in (1.4) satisfies the hypotheses of Proposition 5.3. Indeed, its elements are central in H , so $(vw)^p = v^p w^p = 1$ for $v, w \in V$. It is therefore an abelian subgroup of exponent p . Cauchy's theorem shows that it is nontrivial. Every automorphism of H preserves V , and H is normal in G , so V is normal in G . It contains every element of order p in H .

Let $\mathcal{P}$ be the set of surjections $\psi : G_\mathbb{Q} \twoheadrightarrow G/V$ whose further quotient is π . For each squarefree positive integer R , Lemma 3.3, applied with kernel H/V , gives

$$\#\{\psi \in \mathcal{P} : R(\psi) = R\} \leq C_0 A_0^{\omega(R)}, \quad (6.1)$$

where C_0 and $A_0 \geq 1$ are independent of R . If $H = V$, then $\mathcal{P} = \{\pi\}$ and we take $A_0 = 1$. Every ψ is ramified at only finitely many primes, so $R(\psi)$ is finite. There are

finitely many integers $R \leq Z$, and (6.1) bounds each corresponding set. Consequently $\mathcal{P}$ is countable and $\{\psi \in \mathcal{P} : R(\psi) \leq Z\}$ is finite for every Z .

Every representation counted by (1.3) has a unique quotient modulo V . Hence

$$N_{G,\pi,\mathcal{D}}(X) = \sum_{\psi \in \mathcal{P}} N_\psi(X). \quad (6.2)$$

For each fixed X , this sum has only finitely many nonzero terms, since the left side counts finitely many representations. Proposition 4.2 gives

$$\lim_{X \rightarrow \infty} \frac{N_\psi(X)}{X^{1/a}(\log X)^{b_V-1}} = c_\psi. \quad (6.3)$$

Here $c_\psi = 0$ for an empty fiber, and $c_\psi > 0$ whenever the fiber has a proper solution satisfying the local conditions. The action on V factors through π , so the integer b_V is the same in every fiber.

For $X \geq e$, write $F_\psi(X) = N_\psi(X)/(X^{1/a}(\log X)^{b_V-1})$. Proposition 5.3 and $a'/a = 1 + 1/p$ give

$$0 \leq F_\psi(X) \leq C_1 \frac{|V|^{\omega(R(\psi))}}{R(\psi)^{1+1/p}} =: M_\psi. \quad (6.4)$$

The constant is independent of X and ψ : the only additional factor after normalization is $(\log(X)/\log X)^{b_V-1}$, which is bounded for $X \geq e$.

Grouping by $R(\psi)$ and using (6.1), we obtain

$$\sum_{\psi \in \mathcal{P}} M_\psi \leq C_2 \sum_{R \text{ squarefree}} \frac{(A_0|V|)^{\omega(R)}}{R^{1+1/p}} = C_2 \prod_{\ell} \left(1 + \frac{A_0|V|}{\ell^{1+1/p}}\right) < \infty. \quad (6.5)$$

To justify the last two assertions, expand the product over a finite set of primes. Its terms are exactly those squarefree integers supported on that set. Increasing these finite sets gives the displayed equality by monotone convergence. The logarithm of each finite product is at most $A_0|V| \sum_{\ell} \ell^{-1-1/p}$, which is finite because it is bounded by $A_0|V| \sum_{n \geq 2} n^{-1-1/p}$.

Taking limits in (6.4) gives $0 \leq c_\psi \leq M_\psi$. Thus the sum $C_{G,\pi,\mathcal{D}} := \sum_{\psi \in \mathcal{P}} c_\psi$ converges. We verify the passage to the limit in (6.2). Given $\varepsilon > 0$, choose Z with $\sum_{R(\psi) > Z} M_\psi < \varepsilon$. For the finite set of ψ satisfying $R(\psi) \leq Z$, (6.3) implies

$$\lim_{X \rightarrow \infty} \sum_{R(\psi) \leq Z} (F_\psi(X) - c_\psi) = 0.$$

For every $X \geq e$, the two tails are bounded by $\sum_{R(\psi) > Z} F_\psi(X) < \varepsilon$ and $\sum_{R(\psi) > Z} c_\psi < \varepsilon$. Therefore

$$\left| \sum_{\psi \in \mathcal{P}} F_\psi(X) - C_{G,\pi,\mathcal{D}} \right| \leq \left| \sum_{R(\psi) \leq Z} (F_\psi(X) - c_\psi) \right| + 2\varepsilon.$$

First let $X \rightarrow \infty$, and then let $\varepsilon \rightarrow 0$. Together with (6.2), this proves

$$\lim_{X \rightarrow \infty} \frac{N_{G,\pi,\mathcal{D}}(X)}{X^{1/a}(\log X)^{b_V-1}} = C_{G,\pi,\mathcal{D}}.$$

Finally, the proper solution assumed in the theorem has a quotient $\psi_0 \in \mathcal{P}$ with a nonempty proper-lift fiber satisfying the local conditions. Proposition 4.2 gives $c_{\psi_0} > 0$. Hence $C_{G,\pi,\mathcal{D}} \geq c_{\psi_0} > 0$, which proves (1.6).

Lemma 2.1 gives $b_V = b_\pi = \mathcal{B}_{\rho_0}$ for every proper solution ρ_0 . Thus the logarithmic exponent agrees with (1.2). $\square$

7. GENERAL LINEAR CONGRUENCE GROUPS

In this section, we give an application to the asymptotic counting of lifts of Galois representations. We retain the notation of Corollary 1.3. For $1 \leq r \leq m$, put $K_r = \ker(G_m \rightarrow G_r)$, and set $K_r = 1$ for $r \geq m$. Thus $K_1 = H_m$ and $K_m = 1$.

Lemma 7.1. *For $1 \leq r < m$, the map*

$$\begin{aligned} K_r/K_{r+1} &\longrightarrow M_d(\mathbb{F}_p), \\ (I_d + p^r A)K_{r+1} &\longmapsto A \bmod p \end{aligned} \quad (7.1)$$

is an isomorphism of groups, where the target is additive. Conjugation on this quotient factors through G_1 and is given by $A \mapsto \bar{g}A\bar{g}^{-1}$ for $g \in G_m$. Moreover, for $r, s \geq 1$ one has

$$[K_r, K_s] \subseteq K_{r+s}. \quad (7.2)$$

In particular, H_m is a nontrivial p -group of order $p^{d^2(m-1)}$, and $V_m = K_{m-1}$ is elementary abelian and central in H_m .

Proof. The proof is an exercise which is left to the reader. $\square$

Lemma 7.2. *Suppose that p is odd. If $g \in H_m$ is nontrivial and $g = I_d + p^r A$ with $1 \leq r < m$ and $A \not\equiv 0 \pmod{p}$, then $\text{ord}(g) = p^{m-r}$. Consequently, $\{h \in H_m : h^p = 1\} = V_m$.*

Proof. Choose a lift $\tilde{A} \in M_d(\mathbb{Z}_p)$, and put $\tilde{g} = I_d + p^r \tilde{A}$. The binomial formula applies because every term is a power of the same matrix. It gives

$$\tilde{g}^p = I_d + p^{r+1} \tilde{A} + \sum_{j=2}^{p-1} \binom{p}{j} p^{rj} \tilde{A}^j + p^{rp} \tilde{A}^p.$$

For $2 \leq j \leq p-1$, the corresponding term is divisible entrywise by p^{1+rj} , hence by p^{r+2} . The last term is also divisible by p^{r+2} , since $rp \geq r+2$ for odd p and $r \geq 1$. Therefore

$$\tilde{g}^p = I_d + p^{r+1} A_1. \quad (7.3)$$

Here $A_1 \equiv \tilde{A} \pmod{p}$, so A_1 has an entry prime to p .

The same calculation can now be applied to $I_d + p^{r+1} A_1$. Induction gives matrices $A_t \in M_d(\mathbb{Z}_p)$ such that $\tilde{g}^{p^t} = I_d + p^{r+t} A_t$ and $A_t \equiv \tilde{A} \pmod{p}$ for every $t \geq 0$. Thus the least valuation of an entry of $\tilde{g}^{p^t} - I_d$ is exactly $r+t$.

Reduction modulo p^m gives $g^{p^{m-r}} = I_d$ and $g^{p^{m-r-1}} \neq I_d$. The order of g divides p^{m-r} and does not divide p^{m-r-1} , so it is p^{m-r} . Every nonidentity element of H_m admits such an expression by choosing r to be the least valuation of an entry of $g - I_d$. It has order p precisely when $r = m-1$. Adjoining the identity proves the final assertion. $\square$

Proof of Corollary 1.3. Apply Theorem 1.2 to the reduction map $G_m \rightarrow G_1$ and the fixed quotient $\bar{\rho}$. Lemma 7.1 shows that its kernel H_m is a nontrivial p -group. By Lemma 7.2, its elements of order dividing p form V_m . This subgroup centralizes H_m by Lemma 7.1. The assumed proper solution satisfies the prescribed local conditions, so the nonemptiness hypothesis of Theorem 1.2 holds.

Under the identification in (7.1), conjugation on V_m is the action $A \mapsto \bar{\rho}(\sigma)A\bar{\rho}(\sigma)^{-1}$. After the inverse cyclotomic twist, it is exactly the action defining $b_{\bar{\rho}}$ in Corollary 1.3. Theorem 1.2 therefore gives the asserted asymptotic with a positive constant and exponent $p/(|G_m|(p-1))$. The twisted action depends on $\bar{\rho}$ and $\bar{\chi}_p$, and hence its orbit number is independent of m . $\square$

8. AN APPLICATION IN DIMENSION TWO

We use Ramakrishna's large-image theorem [17, Theorem 1.1] to construct surjective lifts of $\bar{\rho}$ to $\mathrm{GL}_2(\mathbb{Z}_p)$ when $d = 2$ and $p \geq 7$. Reduction modulo p^m then removes the nonemptiness hypothesis from Corollary 1.3 for any finite local conditions satisfied by these reductions.

Lemma 8.1. *Let $p \geq 5$. The group $\mathrm{SL}_2(\mathbb{Z}_p)$ is generated by the matrices*

$$u(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad v(t) = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

for $t \in \mathbb{Z}_p$ and equals its commutator subgroup.

Proof. For $a \in \mathbb{Z}_p^\times$, we find that

$$w(a) = u(a)v(-a^{-1})u(a) = \begin{pmatrix} 0 & a \\ -a^{-1} & 0 \end{pmatrix}.$$

Thus $w(a)w(-1) = \mathrm{diag}(a, a^{-1})$ belongs to the subgroup generated by the elementary matrices.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_p)$. If a is a unit, then $ad - bc = 1$ gives

$$A = v(c/a) \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} u(b/a).$$

If a is not a unit, c must be a unit. The upper left entry of $w(1)A$ is then a unit, so the preceding factorization applies to $w(1)A$. Since $w(1)$ and its inverse belong to the generated subgroup, so does A .

Put $D = \mathrm{diag}(2, 2^{-1})$ and use the convention $[x, y] = xyx^{-1}y^{-1}$. Direct calculation gives $[D, u(t)] = u(3t)$ and $[D, v(t)] = v(-3t/4)$. The elements 3 and 4 are units in $\mathbb{Z}_p$. Consequently, $u(t) = [D, u(t/3)]$ and $v(t) = [D, v(-4t/3)]$. Every generator is a commutator, which proves the assertion. $\square$

In the result below, no parity assumption on $\det \bar{\rho}$ is required.

Theorem 8.2 (Ramakrishna [17, Theorem 1.1]). *Let $p \geq 7$, and let $\bar{\rho} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous representation whose image contains $\mathrm{SL}_2(\mathbb{F}_p)$. Put $\mathcal{A} = \mathbb{Z}_p[[T_1, T_2, \dots]]$. Then $\bar{\rho}$ admits a continuous lift $\tilde{r} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathcal{A})$ whose image contains $\mathrm{SL}_2(\mathcal{A})$.*

Proposition 8.3. *Suppose that $d = 2$ and $p \geq 7$. Then $\bar{\rho}$ admits a continuous surjective lift $\rho_{\infty} : G_{\mathbb{Q}} \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}_p)$.*

Proof. Theorem 8.2, followed by specialization $T_i = 0$, gives a continuous lift $r : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{Z}_p)$ whose image contains $\mathrm{SL}_2(\mathbb{Z}_p)$.

Let ω be the Teichmüller lift of $\det \bar{\rho}$, and let $\chi_{p,\infty}$ be the p -adic cyclotomic character. Put $\eta = \omega\chi_{p,\infty}^{p-1}$. This character lifts $\det \bar{\rho}$ and is surjective. Indeed, $\chi_{p,\infty}^{p-1}$ remains surjective onto $1 + p\mathbb{Z}_p$, when restricted to $\ker \omega$. The character $\eta(\det r)^{-1}$ takes values in $1 + p\mathbb{Z}_p$. Since squaring is an automorphism of this group, it has a unique continuous square-root character θ with $\theta \equiv 1 \pmod{p}$. Set $\rho_{\infty} = \theta r$. Then ρ_{∞} lifts $\bar{\rho}$ and $\det \rho_{\infty} = \eta$.

Put $J = \rho_{\infty}(G_{\mathbb{Q}})$. Since the twisting factors are scalar matrices, they cancel in commutators. Thus, for $\sigma, \tau \in G_{\mathbb{Q}}$,

$$[r(\sigma), r(\tau)] = [\rho_{\infty}(\sigma), \rho_{\infty}(\tau)] \in J.$$

Given $A, B \in \mathrm{SL}_2(\mathbb{Z}_p)$, choose $\sigma, \tau \in G_{\mathbb{Q}}$ with $r(\sigma) = A$ and $r(\tau) = B$. Such choices exist because the image of r contains $\mathrm{SL}_2(\mathbb{Z}_p)$. The displayed equality gives $[A, B] \in J$.

By Lemma 8.1, every element of $\mathrm{SL}_2(\mathbb{Z}_p)$ is a finite product of such commutators. Since $\det \rho_\infty$ is surjective, it then follows that ρ_∞ is surjective. $\square$

Corollary 8.4. *Suppose that $d = 2$ and $p \geq 7$. For every $m \geq 2$, the asymptotic in Corollary 1.3 holds with no local restrictions. More generally, let ρ_∞ be a surjective lift as in Proposition 8.3, and put $\rho_m = \rho_\infty \bmod p^m$. The same asymptotic holds with finite local conditions $\mathcal{D}$ whenever $\rho_m|_{G_{\mathbb{Q}_v}} \in \mathcal{D}_v$ for every $v \in S$.*

Proof. Proposition 8.3 provides a surjective lift ρ_∞ . Each reduction ρ_m is surjective and, under the stated compatibility condition, satisfies $\mathcal{D}$. Corollary 1.3 therefore applies. $\square$

REFERENCES

1. Brandon Alberts, *The weak form of Malle’s conjecture and solvable groups*, Research in Number Theory **6** (2020), no. 1, Paper No. 10.
2. ———, *Statistics of the first Galois cohomology group: A refinement of Malle’s conjecture*, Algebra & Number Theory **15** (2021), no. 10, 2513–2569.
3. Brandon Alberts, Robert J. Lemke Oliver, Jiuya Wang, and Melanie Matchett Wood, *Inductive methods for counting number fields*, Journal für die reine und angewandte Mathematik **835** (2026), 3–61.
4. Brandon Alberts and Evan O’Dorney, *Harmonic analysis and statistics of the first Galois cohomology group*, Research in the Mathematical Sciences **8** (2021), no. 3, Paper No. 50.
5. ———, *Corrigendum to “Harmonic analysis and statistics of the first Galois cohomology group”*, Research in the Mathematical Sciences **10** (2023), no. 3, Paper No. 31.
6. ———, *Harmonic analysis and statistics of the first Galois cohomology group*, arXiv:2102.11223v2 [math.NT], 2023, Corrected version incorporating the corrigendum.
7. Keith Conrad, *The different ideal*, Expository notes, <https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf>.
8. Najmuddin Fakhruddin, Chandrashekar Khare, and Stefan Patrikis, *Relative deformation theory, relative Selmer groups, and lifting irreducible Galois representations*, Duke Mathematical Journal **170** (2021), no. 16, 3505–3599.
9. Chandrashekar Khare, Michael Larsen, and Ravi Ramakrishna, *Constructing semisimple p -adic Galois representations with prescribed properties*, American Journal of Mathematics **127** (2005), no. 4, 709–734.
10. Jürgen Klüners, *A counter example to Malle’s conjecture on the asymptotics of discriminants*, Comptes Rendus. Mathématique **340** (2005), no. 6, 411–414.
11. Peter Koymans and Carlo Pagano, *On Malle’s conjecture for nilpotent groups*, Transactions of the American Mathematical Society, Series B **10** (2023), 310–354.
12. Gunter Malle, *On the distribution of Galois groups*, Journal of Number Theory **92** (2002), no. 2, 315–329.
13. ———, *On the distribution of Galois groups, II*, Experimental Mathematics **13** (2004), no. 2, 129–135.
14. Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999, Translated from the German by Norbert Schappacher.
15. Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2 ed., Grundlehren der mathematischen Wissenschaften, vol. 323, Springer-Verlag, Berlin, 2008.
16. Ravi Ramakrishna, *Deforming Galois representations and the conjectures of Serre and Fontaine–Mazur*, Annals of Mathematics. Second Series **156** (2002), no. 1, 115–154.
17. ———, *Constructing Galois representations with very large image*, Canadian Journal of Mathematics **60** (2008), no. 1, 208–221.
18. Anwesh Ray, *Lower bounds for the number of number fields with Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)$* , Forum Mathematicum **37** (2025), no. 5, 1589–1596.

CHENNAI MATHEMATICAL INSTITUTE, H1, SIPCOT IT PARK, KELAMBAKKAM, SIRUSERI, TAMIL NADU 603103, INDIA

Email address: anwesh@cmi.ac.in