FAMILIES OF ABELIAN VARIETIES AND LARGE GALOIS IMAGES

DAVID ZYWINA

ABSTRACT. Associated to an abelian variety A of dimension g over a number field K is a Galois representation $\rho_A\colon \operatorname{Gal}(\overline{K}/K) \to \operatorname{GL}_{2g}(\widehat{\mathbb{Z}})$. The representation ρ_A encodes the Galois action on the torsion points of A and its image is an interesting invariant of A that contains a lot of arithmetic information. We consider abelian varieties over K parametrized by the K-points of a nonempty open subvariety $U \subseteq \mathbb{P}^n_K$. We show that away from a set of density 0, the image of ρ_A will be very large; more precisely, it will have uniformly bounded index in a group obtained from the family of abelian varieties. This generalizes earlier results which assumed that the family of abelian varieties have "big monodromy". We also give a version for a family of abelian varieties with a more general base.

1. INTRODUCTION

Fix an abelian scheme $\pi\colon A \to U$ of relative dimension $g \geq 1$, where U is a non-empty open subvariety of $\mathbb{P}^n_K$ with K a number field and $n \geq 1$. Choose an algebraic closure $\overline{K}$ of K and define the absolute Galois group $\operatorname{Gal}_K := \operatorname{Gal}(\overline{K}/K)$.

Take any point $u \in U(K)$. The fiber of π over u is an abelian variety A_u over K of dimension g. For each positive integer m, let $A_u[m]$ be the m-torsion subgroup of $A(\overline{K})$. The group $A_u[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank m and has a natural Gal_K-action. This Galois action can expressed in terms of a representation

$$\bar{\rho}_{A,m}\colon \operatorname{Gal}_K \to \operatorname{Aut}_{\mathbb{Z}/m\mathbb{Z}}(A[m]).$$

Taking the inverse limit over all m, ordered by divisibility, we obtain a single representation

$$\rho_{A_u}\colon \operatorname{Gal}_K \to \operatorname{Aut}(\varprojlim A_u[m]) \cong \operatorname{GL}_{2g}(\widehat{\mathbb{Z}})$$

that encodes the Galois action on the torsion of A_u, where $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$. We are interested in describing how large the image of ρ_{A_u} can be as we vary the point $u \in U(K)$.

We first observe that the abelian scheme A imposes a constraint on the image of ρ_{A_u}. Let $\pi_1(U,\overline{\eta})$ be the étale fundamental group of U, where $\overline{\eta}$ is a fixed geometric generic point of U. For each positive integer m, let $A[m]$ be the m-torsion subscheme of A. The morphism $A[m] \to U$ can be viewed as locally constant sheaf of $\mathbb{Z}/m\mathbb{Z}$-modules on U that is free of rank $2g$; it thus corresponds to a representation $\bar{\rho}_{A,m}\colon \pi_1(U,\overline{\eta}) \to \operatorname{Aut}_{\mathbb{Z}/m\mathbb{Z}}(A[m]_{\overline{\eta}})$, where the group $A[m]_{\overline{\eta}}$ is the fiber of $A[m]$ above $\overline{\eta}$. Taking the inverse limit over all m, ordered by divisibility, we obtain a single representation

$$\rho_A\colon \pi_1(U,\overline{\eta}) \to \operatorname{Aut}(\varprojlim A[m]_{\overline{\eta}}) \cong \operatorname{GL}_{2g}(\widehat{\mathbb{Z}}).$$

Specialization at a point $u \in U(K)$ induces a homomorphism $u_*\colon \operatorname{Gal}_K \to \pi_1(U,\overline{\eta})$, uniquely defined up to conjugacy. Composing u_* with ρ_A, we obtain a representation $\operatorname{Gal}_K \to \operatorname{GL}_{2g}(\widehat{\mathbb{Z}})$ that agrees with ρ_{A_u} up to an inner automorphism of $\operatorname{GL}_{2g}(\widehat{\mathbb{Z}})$. So we may identity ρ_{A_u} with the specialization of ρ_A at u. In particular, we can view $\rho_{A_u}(\operatorname{Gal}_K)$ as a subgroup of $\rho_A(\pi_1(U,\overline{\eta}))$ that is uniquely defined up to conjugation. Suppressing the base point, we have

$$\rho_{A_u}(\operatorname{Gal}_K) \subseteq \rho_A(\pi_1(U))$$

for all $u \in U(K)$. Our main result is that the index $[\rho_A(\pi_1(U)) : \rho_{A_u}(\operatorname{Gal}_K)]$ is finite and bounded as we vary over "most" $u \in U(K)$. Our notion of "most" will be that of density. Let H be the absolute multiplicative

2010 *Mathematics Subject Classification.* Primary 11F80; Secondary 14K15.

height function on $\mathbb{P}^n(K)$. The density of a set $B \subseteq \mathbb{P}^n(K)$ is the value

$$\lim_{x\to+\infty} \frac{|\{u \in B : H(u) \le x\}|}{|\{u \in \mathbb{P}^n(K) : H(u) \le x\}|}$$

if the limit exists. For example, $U(K)$ has density 1. Our main theorem is the following:

Theorem 1.1. *Fix an abelian scheme $\pi\colon A \to U$ of positive relative dimension, where U is non-empty open subvariety of $\mathbb{P}^n_K$ for a number field K and $n \ge 1$. Then there is a constant C such that*

$$\left[\rho_A(\pi_1(U)) : \rho_{A_u}(\mathrm{Gal}_K)\right] \le C$$

holds for all $u \in U(K)$ in a set of density 1.

Theorem 1.1 shows that, up to bounded index, the image of the specializations are usually as large as possible when the geometric constraints are taken into account. This can thus be viewed as a variant of Hilbert's irreducibility theorem (and effective versions of Hilbert's irreducibility theorem will be a key component of our proof). This is useful since in practice, $\rho_A(\pi_1(U))$ is easier to compute that the images of the representations ρ_{A_u} (one reason is that there are geometric and topological approaches to computing the normal subgroup $\rho_A(\pi_1(U_{\overline{K}}))$).

However, note that our theorem is not a formal consequence of Hilbert's irreducibility theorem since $\rho_A(\pi_1(U))$ is not finitely generated when viewed as a topological group with the profinite topology. Moreover, the constant C cannot alway be taken to be 1. As an example, take $K = \mathbb{Q}$ and consider any abelian scheme $A \to U := \mathbb{A}^1_{\mathbb{Q}} - \{0, 1728\}$ of relative dimension 1 such that each fiber A_u is an elliptic curve with j-invariant u. In this case, we have $\rho_A(\pi_1(U)) = \mathrm{GL}_2(\widehat{\mathbb{Z}})$. The theorem cannot hold with $C = 1$ since from Serre we know that $\rho_E(\mathrm{Gal}_{\mathbb{Q}}) \ne \mathrm{GL}_2(\widehat{\mathbb{Z}})$ for all elliptic curves E over $\mathbb{Q}$, cf. Proposition 22 of [Ser72]. For this example, the theorem will hold with $C = 2$.

There are several special cases of Theorem 1.1 occurring in the literature and we will recall some in §1.3. These earlier results have a strong constraint on the image of ρ_A; more precisely, they assume that $\rho_A(\pi_1(U))$ is an open subgroup of $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$. The main novelty of Theorem 1.1 is the lack of restrictions on our abelian scheme $A \to U$. Since we have less control on the image of ρ_A, the group theory involved is much more complicated; for example, the ℓ-adic monodromy groups need not be connected and their derived subgroups need not be simply connected.

The constant C in Theorem 1.1 that occurs in our proof will be given in §1.2. We have not tried to determine the optimal C.

1.1. **General base.** Fix a number field K. Let $\pi\colon A \to X$ be an abelian scheme of relative dimension $g \ge 1$, where X is a smooth and geometrically integral variety defined over K of dimension $n \ge 1$. As before, we can define a representation

$$\rho_A\colon \pi_1(X) \to \mathrm{GL}_{2g}(\widehat{\mathbb{Z}}).$$

Take any closed point x of X. The residue field $k(x)$ of x is a finite extension of K. The fiber of A over x is an abelian variety A_x over $k(x)$. Associated to A_x, we have a representation $\rho_{A_x}\colon \mathrm{Gal}_{k(x)} \to \mathrm{GL}_{2g}(\widehat{\mathbb{Z}})$ whose image we may again view as a subgroup of $\rho_A(\pi_1(X))$. The following theorem says that there are infinitely many closed points x of X of bounded degree such that $\rho_{A_x}(\mathrm{Gal}_{k(x)})$ is large.

Theorem 1.2. *There are constants d and C such that there are infinitely many closed points x of X satisfying $[k(x) : K] \le d$ and $[\rho_A(\pi_1(X)) : \rho_{A_x}(\mathrm{Gal}_{k(x)})] \le C$.*

The theorem can fail if we insist that $d = 1$; for example, consider the case where X is a curve of genus at least 2 and hence $X(K)$ is finite.

We will deduce Theorem 1.2 from Theorem 1.1. The idea is to find, after possibly shrinking X, an étale map $X \to U$, where U is open in $\mathbb{P}^n_k$. We then apply Theorem 1.1 to the restriction of scalars of A from X to U.

1.2. **The constant C.** We now give a brief description of the constant C from Theorem 1.1 that occurs in our proof, see Remark 5.10. In particular, observe that the constant C can be computed directly from $H := \rho_A(\pi_1(U))$ and its normal subgroup $H_g := \rho_A(\pi_1(U_{\overline{K}}))$.

Take any prime ℓ and let $p_\ell \colon \operatorname{GL}_{2g}(\widehat{\mathbb{Z}}) \to \operatorname{GL}_{2g}(\mathbb{Z}_\ell)$ be the ℓ-adic projection. Let G_ℓ be the Zariski closure in $\operatorname{GL}_{2g,\mathbb{Q}_\ell}$ of $p_\ell(\rho_A(\pi_1(U)))$; it is an algebraic group over $\mathbb{Q}_\ell$ whose neutral component we denote by G_ℓ°. Let M be the kernel of the homomorphism

$$H \xrightarrow{p_\ell} G_\ell(\mathbb{Q}_\ell) \to G_\ell(\mathbb{Q}_\ell)/G_\ell^\circ(\mathbb{Q}_\ell).$$

We will show later that M does not depend on the choice of ℓ. The commutator subgroup M' of M is normal in H. We will see that the image of the quotient map

$$H_g \to H/M'$$

is finite and its cardinality is our constant C.

Example 1.3. As a special case, consider when $H = \operatorname{GSp}_{2g}(\widehat{\mathbb{Z}})$ and $H_g = \operatorname{Sp}_{2g}(\widehat{\mathbb{Z}})$; these are the largest that both H and H_g could possibly be, up to conjugation in $\operatorname{GL}_{2g}(\widehat{\mathbb{Z}})$, when the abelian scheme A is principally polarized. We have $M = H$ since $G_\ell = \operatorname{GSp}_{2g,\mathbb{Q}_\ell}$ is connected. Therefore, C is the cardinality of the group $\operatorname{Sp}_{2g}(\widehat{\mathbb{Z}})/\operatorname{GSp}_{2g}(\widehat{\mathbb{Z}})'$. One can show that $C = 1$ if $g \geq 3$ and $C = 2$ if $g = 1$ or 2.

1.3. **Some earlier results.** We now discuss special cases of Theorem 1.1 that have already been proved and some related results. Note that some of the results use integral points instead of rational points. In the results mentioned, the term *most* will refer to a suitable notion of density; the reader is encouraged to look at the corresponding articles for the precise definitions.

We first discuss the fundamental case $g = 1$, i.e., A is an elliptic curve. For a non-CM elliptic curve $E/\mathbb{Q}$, *Serre's open image theorem* says that $\rho_E(\operatorname{Gal}_\mathbb{Q})$ is an open subgroup of $\operatorname{GL}_2(\widehat{\mathbb{Z}})$, cf. [Ser72]. In particular, $\bar{\rho}_{E,\ell}(\operatorname{Gal}_K) = \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell \geq c_E$, where c_E is a constant depending on E. As a consequence of Serre's theorem, if A is non-isotrivial then $\rho_A(\pi_1(U))$ is an open subgroup of $\operatorname{GL}_2(\widehat{\mathbb{Z}})$.

The following are all with respect to the family $A \to U := \operatorname{Spec} \mathbb{Q}[a, b, (4a^3 + 27b^2)^{-1}]$ of elliptic curves given by the Weierstrass equation $y^3 = x^3 + ax + b$. In this case, we have $\rho_A(\pi_1(U)) = \operatorname{GL}_2(\widehat{\mathbb{Z}})$ and $\rho_A(\pi_1(U_{\overline{\mathbb{Q}}})) = \operatorname{SL}_2(\widehat{\mathbb{Z}})$.

Duke [Duk97] proved that for "most" elliptic curves $E/\mathbb{Q}$, we have $\bar{\rho}_{E,\ell}(\operatorname{Gal}_K) = \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for *all* primes. Building on this, Jones [Jon10] showed that for "most" elliptic curves $E/\mathbb{Q}$, $\rho_E(\operatorname{Gal}_\mathbb{Q})$ is an index 2 subgroup of $\operatorname{GL}_2(\widehat{\mathbb{Z}})$ (as already noted, ρ_E is never surjective for an elliptic curve over $\mathbb{Q}$). Similar results for one-parameter families of elliptic curves over $\mathbb{Q}$ can be found in [CGJ11].

For a number field $K \neq \mathbb{Q}$, Zywina showed that for "most" elliptic curves E/K, we have $\rho_E(\operatorname{Gal}_K) = \{B \in \operatorname{GL}_2(\widehat{\mathbb{Z}}) : \det(B) \in \chi_{\text{cyc}}(\operatorname{Gal}_K)\}$, where $\chi_{\text{cyc}} \colon \operatorname{Gal}_\mathbb{Q} \to \widehat{\mathbb{Z}}^\times$ is the cyclotomic character. In particular, if $K \neq \mathbb{Q}$ contains no non-trivial abelian extension of $\mathbb{Q}$, then there is an elliptic curve E/K with $\rho_E(\operatorname{Gal}_K) = \operatorname{GL}_2(\widehat{\mathbb{Z}})$. Greicius [Gre10] had previously constructed an explicit elliptic curve E over a number field with ρ_E surjective.

We now consider $g \geq 2$ and assume further that A is principally polarized. After possibly conjugating ρ_E by an element in $\operatorname{GL}_{2g}(\widehat{\mathbb{Z}})$ we may assume that $\rho_A(\pi_1(U))$ is a subgroup of $\operatorname{GSp}_{2g}(\widehat{\mathbb{Z}})$. Under the "big monodromy" assumption that $\rho_A(\pi_1(U))$ is an open subgroup of $\operatorname{GSp}_{2g}(\widehat{\mathbb{Z}})$, Landesman, Swaminathan, Tao and Xu proved Theorem 1.1 with an optimal C. Earlier, Wallace [Wal14] had proved a variant of this with $g = 2$; also see Remark 1.3 in [LSTX19]. The case $g = 1$ had been proved in [Zyw10].

When $K = \mathbb{Q}$, one can use the Kronecker–Weber theorem to show that $\rho_{A_u}(\operatorname{Gal}_\mathbb{Q}) \cap \operatorname{GSp}_{2g}(\widehat{\mathbb{Z}})$ agrees with the commutator subgroup of $\rho_{A_u}(\operatorname{Gal}_\mathbb{Q})$; this and the inclusion $\rho_{A_u}(\operatorname{Gal}_K) \subseteq \rho_A(\pi_1(U))$ are the only constraints on the image of ρ_{A_u} for "most" $u \in U(K)$. In the general setting of Theorem 1.1, there may be additional constraints on the image of all the representations ρ_{A_u}.

In the setting of Theorem 1.1, define the set

$$S := \{u \in U(K) : \rho_{A_u}(\mathrm{Gal}_K) \text{ is } \textit{not} \text{ an open subgroup of } \rho_A(\pi_1(U))\}.$$

An immediate consequence of Theorem 1.1 is that the set S density 0. Moreover, Cadoret proved that the set S is *thin* in $U(K)$, cf. Theorem 1.2 and §1.1 of [Cad15]. Recall that every thin subset of $U(K)$ has density 0, cf. §13.1 of [Ser97].

1.4. **Overview.** We now give a brief overview of the proof of Theorem 1.1.

For a rational prime ℓ, let $\rho_{A,\ell}\colon \pi_1(U) \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ be the representation obtained by composing ρ_A with the natural projection $\mathrm{GL}_{2g}(\widehat{\mathbb{Z}}) \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$. We define $\mathcal{G}_{A,\ell}$ be the $\mathbb{Z}_\ell$-group subscheme of $\mathrm{GL}_{2g,\mathbb{Z}_\ell}$ obtained by taking the Zariski closure of $\rho_{A,\ell}(\pi_1(U))$. These will agree with later definitions of $\rho_{A,\ell}$ and $\mathcal{G}_{A,\ell}$ after choosing an appropriate $\mathbb{Z}_\ell$-basis for the ℓ-adic Tate module $T_\ell(A)$. The generic fiber $G_{A,\ell}$ of $\mathcal{G}_{A,\ell}$ is an algebraic group over $\mathbb{Q}_\ell$ that we call the *ℓ-adic monodromy groups* of A. In §2, we recall several properties of $G_{A,\ell}$.

We have an easy inclusion $\bar{\rho}_{A,\ell}(\pi_1(U)) \subseteq \mathcal{G}_{A,\ell}(\mathbb{F}_\ell)$. Theorem 3.1, which is a generalization of Serre's open image theorem, implies that

$$[\mathcal{G}_{A,\ell}(\mathbb{F}_\ell) : \bar{\rho}_{A,\ell}(\pi_1(U))] \leq C$$

for a constant C that does not depend on ℓ. There is a constant b_A such that the neutral component of the algebraic group $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ over $\mathbb{F}_\ell$ is reductive for all $\ell \geq b_A$. For $\ell \geq b_A$, let H_ℓ is the derived subgroup of the neutral component of the group $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ and let S_ℓ be the commutator subgroup of $H_\ell(\mathbb{F}_\ell)$ (in the notation of §3, $S_\ell = \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$).

After possibly increasing b_A, we will observe that

$$S_\ell \subseteq \bar{\rho}_{A,\ell}(\pi_1(U))$$

holds for all $\ell \geq b_A$. In the special case of the examples in §1.3 where $\rho_A(\pi_1(U))$ is an open subgroup of $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$, we find that $\mathcal{G}_{A,\ell} = \mathrm{GSp}_{2g,\mathbb{Z}_\ell}$ and $S_\ell = \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ for all sufficiently large ℓ.

Fix a prime $\ell \geq b_A$ and a point $u \in U(K)$, specialization gives an inclusion $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \subseteq \bar{\rho}_{A,\ell}(\pi_1(U))$ uniquely determined up to conjugation. Since S_ℓ is a normal subgroup of $\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)$, and hence also of $\bar{\rho}_{A,\ell}(\pi_1(U))$, it makes sense to ask whether or not S_ℓ is a subgroup of $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K)$. Define the set

$$B := \{u \in U(K) : \bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \not\supseteq S_\ell \text{ for some prime } \ell \geq b_A\}.$$

One of the main tasks of this paper is to show that B has density 0; equivalently, that for "most" $u \in U(K)$, we have $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K) \supseteq S_\ell$ for *all* $\ell \geq b_A$. In §5, we prove that if the set B has density 0, then Theorem 1.1 will hold. This will require some information about the groups $\rho_{A,\ell}(\pi_1(U_{\bar{K}}))$ which we study in §4.

We will prove Theorem 1.1 in §9. Take any real number $x \geq 2$. Let $B(x)$ be the set of $u \in B$ satisfying $H(u) \leq x$. To prove that B has density 0, we need to show that $|B(x)| = o(x^{[K:\mathbb{Q}](n+1)})$ as $x \to \infty$. For each $\ell \geq b_A$, let $B_\ell(x)$ be the set of $u \in U(K)$ with $H(u) \leq x$ satisfying $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \not\supseteq S_\ell$. Using an effective open image theorem for abelian varieties, we will show that

$$B(x) \subseteq R(x) \cup T(x) \cup \bigcup_{b_A \leq \ell \leq c(\log x)^\gamma} B_\ell(x). \tag{1.1}$$

for some constant c, where the sets $R(x)$ and $T(x)$ are defined at the beginning of §9. The important aspect of the inclusion (1.1) is that the right hand side involves only a bounded number of primes ℓ while the definition of B requires considering all primes $\ell \geq b_A$. In §9.2 and §9.3, we show that $|R(x)| = o(x^{[K:\mathbb{Q}](n+1)})$ and $|T(x)| = o(x^{[K:\mathbb{Q}](n+1)})$. So from (1.1), we have

$$|B(x)| \leq \sum_{b_A \leq \ell \leq c(\log x)^\gamma} |B_\ell(x)| + o(x^{[K:\mathbb{Q}](n+1)}). \tag{1.2}$$

We thus need to find bounds for $|B_\ell(x)|$. The Hilbert Irreducibility Theorem (HIT) implies that $|B_\ell(x)| = o(x^{[K:\mathbb{Q}](n+1)})$ as $x \to \infty$. However, to use (1.2) to find meaningful bounds for $|B(x)|$, we need to find better bounds for $|B_\ell(x)|$ with an explicit dependency on ℓ.

In §6, we prove an effective version of HIT using the large sieve. In §8.1, we use it to give a more specialized version of HIT that is relevant to our application. To obtain the explicit bounds we require, we will need some group theoretic input which is discussed in §7. For each prime $\ell \geq b_A$ and $x \geq 2$, Theorem 8.1 says that

$$|B_\ell(x)| = O\Big((\ell+1)^{3g(2g+1)/2} \cdot x^{[K:\mathbb{Q}](n+1/2)} \log x + (\ell+1)^{(6n+15/2)g(2g+1)}\Big),$$

where the implicit constant depends only on A. Combining this with (1.2) gives $|B(x)| = o(x^{[K:\mathbb{Q}](n+1)})$ and hence B has density 0.

Finally in §10, we prove Theorem 1.2 by reducing to Theorem 1.1.

1.5. **Notation.** Consider a topological group G. The commutator subgroup of G is the closed subgroup G' generated by the set of commutators of G. We say that G is perfect if $G' = G$. Profinite groups, and in particular finite groups, will always be considered with their profinite topology.

For a scheme X over a commutative ring R and a commutative R-algebra S, we denote by X_S the base extension of X by $\operatorname{Spec} S$. Let M be a free module of finite rank over a commutative ring R. Denote by GL_M the R-scheme such that $\mathrm{GL}_M(S) = \mathrm{Aut}_S(M \otimes_R S)$ for any commutative R-algebra S with the obvious functoriality.

For an algebraic group G over a field F, we denote by G° the neutral component of G, i.e., the connected component of the identity of G. Note that G° is an algebraic subgroup of G.

For two real quantities f and g, the expression $f \ll_{\alpha_1,\ldots,\alpha_n} g$ means that the inequality $|f| \leq C|g|$ holds for some positive constant C depending only on $\alpha_1, \ldots, \alpha_n$. In particular, $f \ll g$ means that the implicit constant C is absolute. We denote by $O_{\alpha_1,\ldots,\alpha_n}(g)$ a quantity f satisfying $f \ll_{\alpha_1,\ldots,\alpha_n} g$. For two real valued functions f and g of a real variable x, with $g(x)$ non-zero for all sufficiently large x, the expression $f = o(g)$ means that $f(x)/g(x) \to 0$ as $x \to +\infty$.

For a number field K, we denote by $\mathcal{O}_K$ the ring of integers of K. For a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we define its residue field $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$. For a representation $\rho\colon \mathrm{Gal}_K \to G$ unramified at a prime $\mathfrak{p}$, we will view $\rho(\mathrm{Frob}_\mathfrak{p})$ as either a conjugacy class of G or as an element of G that is uniquely defined up to conjugacy. Throughout, ℓ will always denote a rational prime.

When talking about prime ideals of a number field K, density will always refer to *natural density*. From context, there should be no confusion with the notion of density of subsets of $\mathbb{P}^n(K)$.

1.6. **Acknowledgements.** Many thanks to David Zureick–Brown; this article was originally intended to be part of a joint work with him. Many parts of the original project have been greatly expanded on by his REU students in [LSTX19] and [LSTX17]. In particular, an examination of their papers will hopefully make up for the lack of examples in this article.

2. ℓ-ADIC MONODROMY GROUPS

Fix a number field K and an abelian scheme $\pi\colon A \to U$ of relative dimension $g \geq 1$, where U is a non-empty open subvariety of $\mathbb{P}^n_K$ for some integer $n \geq 0$.

Note that by including the case $n = 0$, the following notation and definitions will also hold for an abelian variety of dimension $g \geq 1$ defined over the number field K (when $n = 0$, we have $U = \mathbb{P}^n_K = \operatorname{Spec} K$ and we can identify $\pi_1(U)$ with Gal_K).

We now extend our notation from the introduction. For an integer $m \geq 2$, let $T_m(A)$ be the inverse limit of the groups $A[m^e]_{\bar{\eta}}$ over all $e \geq 1$, where the transition homomorphisms $A[m^{e+1}]_{\bar{\eta}} \to A[m^e]_{\bar{\eta}}$ are multiplication by m. The group $T_m(A)$ is a free $\mathbb{Z}_m$-module of rank $2g$, where $\mathbb{Z}_m := \varprojlim_e \mathbb{Z}/m^e\mathbb{Z} = \prod_{\ell | m} \mathbb{Z}_\ell$. The representations $\bar{\rho}_{A,m^e}$ combine to give a continuous representation

$$\rho_{A,m}\colon \pi_1(U) \to \mathrm{Aut}_{\mathbb{Z}_m}(T_m(A)).$$

Take any prime ℓ. Define $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$; it is a $\mathbb{Q}_\ell$-vector space of dimension $2g$. With notation as in §1.5, we have an algebraic group $\mathrm{GL}_{V_\ell(A)}$ defined over $\mathbb{Q}_\ell$. We can view $\mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A))$, and hence also $\rho_{A,\ell}(\pi_1(U))$, as a subgroup of $\mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) = \mathrm{GL}_{V_\ell(A)}(\mathbb{Q}_\ell)$.

2.1. **ℓ-adic monodromy groups.** For a prime ℓ, we have $\rho_{A,\ell}(\pi_1(U)) \subseteq \mathrm{GL}_{V_\ell(A)}(\mathbb{Q}_\ell)$. To study the image of $\rho_{A,\ell}$, we will study a related algebraic group defined over $\mathbb{Q}_\ell$.

Definition 2.1. The ℓ-adic monodromy group of A, which we denote by $G_{A,\ell}$, is the Zariski closure of $\rho_{A,\ell}(\pi_1(U))$ in $\mathrm{GL}_{V_\ell(A)}$; it is an algebraic group defined over $\mathbb{Q}_\ell$.

For any $m \geq 2$ and $u \in U(K)$, we can view $\rho_{A_u,m}(\mathrm{Gal}_K)$ as a closed subgroup of $\rho_{A,m}(\pi_1(U))$ that is uniquely determined up to conjugation. With $m = \ell$, we can thus identify $G_{A_u,\ell}$ with a closed algebraic subgroup of $G_{A,\ell}$ uniquely defined up to conjugation by an element in $G_{A,\ell}(\mathbb{Q}_\ell)$.

Lemma 2.2. *Assume that $n \geq 1$.*

(i) *For each integer $m \geq 2$, we have $\rho_{A_u,m}(\mathrm{Gal}_K) = \rho_{A,m}(\pi_1(U))$ for all $u \in U(K)$ away from a set of density 0.*

(ii) *For each prime ℓ, we have $G_{A_u,\ell} = G_{A,\ell}$ for all $u \in U(K)$ away from a set of density 0.*

Proof. Part (ii) is an easy consequence of (i) with $m = \ell$.

We now prove (i). Define $H := \rho_{A,m}(\pi_1(U))$. Let $\Phi(H)$ be the Frattini subgroup of H, i.e., the intersection of the maximal closed and proper subgroups of H. The kernel of $H \to \mathrm{Aut}_{\mathbb{Z}/m\mathbb{Z}}(T_m(A)/mT_m(A))$ is an open subgroup of H that is a product of finitely generated pro-ℓ groups with $\ell|m$. From the proposition of [Ser97, §10.5], we find that $\Phi(H)$ is an open, and hence finite index, subgroup of H.

So there is an integer $e \geq 1$ such that $\rho_{A_u,m}(\mathrm{Gal}_K) = H$ if and only if $\bar{\rho}_{A_u,m^e}(\mathrm{Gal}_K) = \bar{\rho}_{A,m^e}(\pi_1(U))$. The lemma follows since Hilbert's irreducibility theorem implies that $\bar{\rho}_{A_u,m^e}(\mathrm{Gal}_K) = \bar{\rho}_{A,m^e}(\pi_1(U))$ holds for all $u \in U(K)$ away from a set of density 0. □

Note that a priori the implicit set of density 0 in Lemma 2.2(ii) depends on ℓ. The following proposition, which we prove in §2.3, removes this dependence on ℓ.

Proposition 2.3. *Assume that $n \geq 1$. The set of $u \in U(K)$ for which $G_{A_u,\ell} = G_{A,\ell}$ holds for all primes ℓ has density 1.*

2.2. **Neutral component.** Let $G^\circ_{A,\ell}$ be the neutral component of $G_{A,\ell}$, i.e., the connected component of $G_{A,\ell}$ containing the identity. Note that $G^\circ_{A,\ell}$ is an algebraic subgroup of $G_{A,\ell}$. Let

$$\gamma_{A,\ell} \colon \pi_1(U) \to G_{A,\ell}(\mathbb{Q}_\ell)/G^\circ_{A,\ell}(\mathbb{Q}_\ell)$$

be the surjective homomorphism obtained by composing $\rho_{A,\ell}$ with the obvious quotient map. For any $u \in U(K)$ satisfying $G_{A_u,\ell} = G_{A,\ell}$, the specialization of $\gamma_{A,\ell}$ at u gives the homomorphism $\gamma_{A_u,\ell} \colon \mathrm{Gal}_K \to G_{A_u,\ell}(\mathbb{Q}_\ell)/G^\circ_{A_u,\ell}(\mathbb{Q}_\ell)$.

Lemma 2.4.

(i) *The kernel of $\gamma_{A,\ell}$ is independent of ℓ.*

(ii) *Suppose $n \geq 1$. Then there is a set $S \subseteq U(K)$ with density 1 such that the specialization of $\gamma_{A,\ell}$ at u is surjective for all ℓ and $u \in S$.*

Proof. If A is an abelian variety over K, then part (i) was proved by Serre [Ser00, 133]; see also [LP97]. We may now assume that $n \geq 1$.

Now suppose that there are primes ℓ and ℓ' such that $\ker \gamma_{A,\ell} \neq \ker \gamma_{A,\ell'}$. By Lemma 2.2(ii) and Hilbert's irreducibility theorem, there is a point $u \in U(K)$ such that $G_{A_u,\ell} = G_{A,\ell}$, $G_{A_u,\ell'} = G_{A,\ell'}$, and such that the kernel of the specializations of $\gamma_{A,\ell}$ and $\gamma_{A,\ell'}$ at u give different subgroups of Gal_K. So $\ker \gamma_{A_u,\ell} \neq \ker \gamma_{A_u,\ell'}$ which contradicts the case of (i) we have already proved. Therefore, $\ker \gamma_{A,\ell} = \ker \gamma_{A,\ell'}$ for any primes ℓ and ℓ'.

We now prove (ii). Let S be the set of $u \in U(k)$ for which the specialization of $\gamma_{A,2}$ at u is surjective. The set S has density 1 by Hilbert's irreducibility theorem. Take any point $u \in S$. Since each $\gamma_{A,\ell}$ is surjective and $\ker \gamma_{A,\ell}$ is independent of ℓ, we find that the specialization of $\gamma_{A,\ell}$ at u is surjective for one prime ℓ if and only if it is surjective for all primes ℓ. Therefore, the specialization of $\gamma_{A,\ell}$ at u is surjective for all ℓ by our definition of S. □

For an abelian variety A defined over K, we denote by K_A^{conn} the subfield of $\overline{K}$ fixed by the kernel of the homomorphism

$$\gamma_{A,\ell}\colon \mathrm{Gal}_K \xrightarrow{\rho_{A,\ell}} G_{A,\ell}(\mathbb{Q}_\ell) \to G_{A,\ell}(\mathbb{Q}_\ell)/G^\circ_{A,\ell}(\mathbb{Q}_\ell). \tag{2.1}$$

Equivalently, K_A^{conn} is the smallest extension of K in $\overline{K}$ that satisfies $\rho_{A,\ell}(\mathrm{Gal}_{K_A^{\mathrm{conn}}}) \subseteq G^\circ_{A,\ell}(\mathbb{Q}_\ell)$. By Lemma 2.4(i), the number field K_A^{conn} is independent of ℓ.

Proposition 2.5.

(i) *The group $G^\circ_{A,\ell}$ is reductive.*

(ii) *The rank of the reductive group $G^\circ_{A,\ell}$ is independent of ℓ.*

(iii) *Let R_ℓ be the commutant of $G^\circ_{A,\ell}$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$. The dimension of R_ℓ as a $\mathbb{Q}_\ell$-vector space is independent of ℓ.*

(iv) *Suppose that $n \geq 1$. The set of $u \in U(K)$ for which $G^\circ_{A_u,\ell} = G^\circ_{A,\ell}$ for all primes ℓ has density* 1.

Proof. We first consider the case where A is an abelian variety defined over a number field K. After replacing A/K by its base extension to K_A^{conn}, we may assume without loss of generality that $G_{A,\ell}$ is connected for all ℓ. From Faltings, cf. [Fal86], we know that:

(a) The $\mathbb{Q}_\ell[\mathrm{Gal}_K]$-module $V_\ell(A)$ is semisimple.

(b) The natural map $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_\ell(A))$ is an isomorphism.

From (a), we deduce that $G_{A,\ell}$ is reductive. From (b), the commutant R_ℓ of $G_{A,\ell}$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ is isomorphic to $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. In particular, the dimension of R_ℓ over $\mathbb{Q}_\ell$ is independent of ℓ and the center of R_ℓ is semisimple for all sufficiently large ℓ. Serre proved part (i) in [Ser00, 133]; this also follows from Theorem 1.2 of [LP97] since the dimension of the groups $H_{v,\ell}$ that occur there do not depend on ℓ.

It remains to consider the case where $n \geq 1$. For a fixed ℓ, Lemma 2.2(ii) implies that $G_{A_u,\ell} = G_{A,\ell}$ for some $u \in U(K)$. In particular, $G^\circ_{A_u,\ell} = G^\circ_{A,\ell}$. The group $G^\circ_{A,\ell} = G^\circ_{A_u,\ell}$ is thus reductive from part (i) in the case of an abelian variety defined over a number field. This proves (i).

Take any two distinct primes ℓ and ℓ'. By Lemma 2.2(ii), we have $G_{A_u,\ell} = G_{A,\ell}$ and $G_{A_u,\ell'} = G_{A,\ell'}$ for some $u \in U(K)$. In particular, $G^\circ_{A_u,\ell} = G^\circ_{A,\ell}$ and $G^\circ_{A_u,\ell'} = G^\circ_{A,\ell'}$. By part (ii) in the case of an abelian variety defined over a number field, the ranks of $G^\circ_{A_u,\ell} = G^\circ_{A,\ell}$ and $G^\circ_{A_u,\ell'} = G^\circ_{A,\ell'}$ are equal. Since ℓ and ℓ' are arbitrary primes, we deduce that the rank of $G^\circ_{A,\ell}$ does not depend on ℓ. This proves (ii).

Note that specialization gives an isomorphism $V_\ell(A_u) = V_\ell(A)$ for which the actions of the groups $G_{A_u,\ell} \subseteq G_{A,\ell}$ are compatible. Denote by R_ℓ the commutant of $G^\circ_{A,\ell}$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$. For $u \in U(K)$, denote by $R_{u,\ell}$ the commutant of $G^\circ_{A_u,\ell}$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$.

Take any two distinct primes ℓ and ℓ'. As above, we have $G^\circ_{A_u,\ell} = G^\circ_{A,\ell}$ and $G^\circ_{A_u,\ell'} = G^\circ_{A,\ell'}$ for some $u \in U(K)$. In particular, $R_{u,\ell} = R_\ell$ and $R_{u,\ell'} = R_{\ell'}$. By part (iii) in the case of an abelian variety defined over a number field, we deduce that $\dim_{\mathbb{Q}_\ell} R_\ell$ is independent of ℓ. This proves (iii).

It remains to prove that part (iv) holds; suppose $n \geq 1$. For each prime ℓ, let S_ℓ be the set of $u \in U(K)$ for which $G^\circ_{A_u,\ell} = G^\circ_{A,\ell}$; it has density 1 by Lemma 2.2(ii).

Take any $u \in S_2$ and prime ℓ. We have an inclusion of groups $G^\circ_{A_u,\ell} \subseteq G^\circ_{A,\ell}$ and they are reductive by part (i). The inclusion implies that $R_{u,\ell} \subseteq R_\ell$. We have $\dim_{\mathbb{Q}_2} R_{u,2} = \dim_{\mathbb{Q}_2} R_2$ since $u \in S_2$, and hence $\dim_{\mathbb{Q}_\ell} R_{u,\ell} = \dim_{\mathbb{Q}_\ell} R_\ell$ by part (iii). Therefore, $R_{u,\ell} = R_\ell$. The groups $G^\circ_{A_u,2}$ and $G^\circ_{A,2}$ have the same rank since $u \in S_2$, and hence $G^\circ_{A_u,\ell}$ and $G^\circ_{A,\ell}$ have the same rank by part (ii).

As noted above, we have $R_{u,\ell} \cong \mathrm{End}(A_u) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ and hence the $\mathbb{Q}_\ell$-algebra $R_\ell = R_{u,\ell}$, and it center, are semisimple for all ℓ greater than some constant $b \geq 2$.

Applying Lemma 2.6 below, we deduce that $G^\circ_{A_u,\ell} = G^\circ_{A,\ell}$ for all primes $\ell \geq b$. Therefore, $G^\circ_{A_u,\ell} = G^\circ_{A,\ell}$ holds for all primes ℓ with $u \in S := \bigcap_{\ell \leq b} S_\ell$. The set S has density 1 since it is a finite intersection of density 1 sets by Lemma 2.2(ii). Part (iv) now follows. □

Lemma 2.6. [Win02, Lemma 7] *Let F be a perfect field whose characteristic is 0 or at least 5. Let $G_1 \subseteq G_2$ be reductive groups defined over F that have the same rank. Suppose we have a faithful linear representation $G_2 \hookrightarrow \mathrm{GL}_V$, where V is a finite dimension F-vector space, such that the centers of the commutants of G_1 and G_2 in $\mathrm{End}_F(V)$ are the same F-algebra R. Suppose further that the commutative F-algebra R is semisimple. Then $G_1 = G_2$.* □

2.3. **Proof of Proposition 2.3.** Let S be the set of $u \in U(k)$ such that $G^\circ_{A_u,\ell} = G^\circ_{A,\ell}$ for all primes ℓ and such that the specialization of γ_ℓ at u is surjective for all primes ℓ. The set S has density 1 by Proposition 2.5(iv) and Lemma 2.4(ii).

Now take any $u \in S$ and any prime ℓ. Specialization gives an inclusion $G_{A_u,\ell} \subseteq G_{A,\ell}$ and we have $G^\circ_{A_u,\ell} = G^\circ_{A,\ell}$ since $u \in S$. The group $G_{A,\ell}(\mathbb{Q}_\ell)$ is Zariski dense in $G_{A,\ell}$ since $G_{A,\ell}$ is defined as the Zariski closure of a subgroup of $\mathrm{GL}_{V_\ell(A)}(\mathbb{Q}_\ell)$. So to prove that $G_{A_u,\ell} = G_{A,\ell}$, it suffices to show that the natural injective homomorphism $\varphi\colon G_{A_u,\ell}(\mathbb{Q}_\ell)/G^\circ_{A_u,\ell}(\mathbb{Q}_\ell) \hookrightarrow G_{A,\ell}(\mathbb{Q}_\ell)/G^\circ_{A,\ell}(\mathbb{Q}_\ell)$ is surjective. If φ was not surjective, then the specialization of γ_ℓ at u would not be surjective which is impossible since $u \in S$. Therefore, $G_{A_u,\ell} = G_{A,\ell}$. The proposition follows since S has density 1 and ℓ was arbitrary.

3. Big ℓ-adic images

Fix an abelian scheme $\pi\colon A \to U$ of relative dimension $g \geq 1$, where U is a non-empty open subvariety of $\mathbb{P}^n_K$ with K a number field and $n \geq 0$. As noted in §2, this includes the case that A is an abelian variety defined over K.

3.1. **More ℓ-adic monodromy groups.** Similar to our definition of $G_{A,\ell}$, we now define an ℓ-adic monodromy that is a group scheme over $\mathbb{Z}_\ell$. With notation as in §1.5, we have an algebraic group scheme $\mathrm{GL}_{T_\ell(A)}$ defined over $\mathbb{Z}_\ell$. Note that the generic fiber of $\mathrm{GL}_{T_\ell(A)}$ is $\mathrm{GL}_{V_\ell(A)}$.

We define $\mathcal{G}_{A,\ell}$ to be the Zariski closure of $\rho_{A,\ell}(\pi_1(U))$ in $\mathrm{GL}_{T_\ell(A)}$; it is a group scheme defined over $\mathbb{Z}_\ell$. The group schemes $G_{A,\ell}$ and $\mathcal{G}_{A,\ell}$ determine each other. More precisely, $G_{A,\ell}$ is the generic fiber of $\mathcal{G}_{A,\ell}$ and $\mathcal{G}_{A,\ell}$ is the Zariski closure of $G_{A,\ell}$ in $\mathrm{GL}_{T_\ell(A)}$.

Let $\mathcal{G}^\circ_{A,\ell}$ be the $\mathbb{Z}_\ell$-group subscheme of $\mathcal{G}_{A,\ell}$ that is the Zariski closure of $G^\circ_{A,\ell}$.

Let $\mathcal{S}_{A,\ell}$ be the $\mathbb{Z}_\ell$-group subscheme of $\mathcal{G}^\circ_{A,\ell}$ that is the Zariski closure of the derived subgroup of $G^\circ_{A,\ell}$.

3.2. **An open image theorem.** The following theorem says that the image of $\rho_{A,\ell}$ is "large" for all sufficiently large ℓ. More precisely, $\rho_{A,\ell}(\pi_1(U))$ contains $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ and its index in $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$ is uniformly bounded for all sufficiently large ℓ. The theorem also describes several important properties of the $\mathbb{Z}_\ell$-group schemes $\mathcal{G}^\circ_{A,\ell}$ and $\mathcal{S}_{A,\ell}$.

Theorem 3.1. *There is a constant b_A, depending only on A, such that the following hold for all primes $\ell \geq b_A$:*

(i) *The $\mathbb{Z}_\ell$-group scheme $\mathcal{G}^\circ_{A,\ell}$ is reductive and $\mathcal{S}_{A,\ell}$ is semisimple.*
(ii) *We have $\rho_{A,\ell}(\pi_1(U)) \supseteq \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ and $\bar{\rho}_{A,\ell}(\pi_1(U)) \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$.*
(iii) *We have $[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\pi_1(U))] \ll_A 1$.*
(iv) *The groups $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ and $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ are perfect and all of their finite simple quotients are of Lie type in characteristic ℓ. We have $\mathcal{G}^\circ_{A,\ell}(\mathbb{Z}_\ell)' = \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$.*
(v) *The cardinality of $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)/\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ is finite and can be bounded in terms of g.*
(vi) *Suppose that H is a closed subgroup of $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)$, in the ℓ-adic topology, whose image modulo ℓ contains $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$. Then $H \supseteq \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$.*

We will prove Theorem 3.1 in §3.4 by using the following lemma to reduce to the case of an abelian variety over a number field.

Lemma 3.2. *If Theorem 3.1 holds for abelian varieties over any number field K, then it holds in general.*

Proof. We can assume that $n \geq 1$. By Proposition 2.3, there is a $u \in U(K)$ such that $G_{A_u,\ell} = G_{A,\ell}$ for all ℓ. This implies that $\mathcal{G}_{A_u,\ell} = \mathcal{G}_{A,\ell}$ and $\mathcal{S}_{A_u,\ell} = \mathcal{S}_{A,\ell}$ hold for all ℓ. Specialization by u gives inclusions $\rho_{A_u,\ell}(\mathrm{Gal}_K) \subseteq \rho_{A,\ell}(\pi_1(U)) \subseteq \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$. It is now clear that Theorem 3.1 for the abelian variety A_u/K implies that Theorem 3.1 holds for A with $b_A := b_{A_u}$. □

3.3. **An effective open image theorem.** In this section, we assume that A is an abelian variety of dimension $g \geq 1$ defined over a number field K. We will state a version of Theorem 3.1 due to the author that gives a value of b_A in terms of various invariants of A. Before stating the results, we need to recall some quantities.

The algebraic group $G^\circ_{A,\ell}$ is reductive and its rank is independent of ℓ, cf. Proposition 2.5(ii). Denote the common rank of the groups $G^\circ_{A,\ell}$ by r.

Let $\mathfrak{p}$ be any non-zero prime ideal of $\mathcal{O}_K$ for which A has good reduction. Denote by $P_{A,\mathfrak{p}}(x)$ the Frobenius polynomial of A at $\mathfrak{p}$; it is a monic degree $2g$ polynomial with integer coefficients. For a prime ℓ satisfying $\mathfrak{p} \nmid \ell$, the representation $\rho_{A,\ell}$ is unramified at $\mathfrak{p}$ and we have

$$P_{A,\mathfrak{p}}(x) = \det(xI - \rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})).$$

Let $\Phi_{A,\mathfrak{p}}$ be the subgroup of $\mathbb{C}^\times$ generated by the roots of $P_{A,\mathfrak{p}}(x)$.

We denote by $h(A)$ the (logarithmic absolute) Faltings height of A obtained after base extending to any finite extension of K over which A has semistable reduction, see §5 of [Cha86]. In particular, note that $h(A_L) = h(A)$ for any finite extension L/K.

Theorem 3.3. *Let A be an abelian variety of dimension $g \geq 1$ defined over a number field K. Let $\mathfrak{q}$ be a non-zero prime ideal of $\mathcal{O}_K$ for which A has good reduction and $\Phi_{A,\mathfrak{q}}$ is a free abelian group of rank r. Then there are positive constants c and γ, depending only on g, such that Theorem 3.1 holds with*

$$b_A = c \cdot (\max\{[K:\mathbb{Q}], h(A), N(\mathfrak{q})\})^\gamma.$$

Proof. Take any prime $\ell \geq b_A$. Parts (i) and (iii) follow from parts (c) and (a), respectively, of Theorem 1.2 in [Zyw19]. Theorem 1.2(d) in [Zyw19] implies that $\rho_{A,\ell}(\mathrm{Gal}_K) \supseteq \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$. Reducing modulo ℓ and using that $\mathcal{S}_{A,\ell}$ is smooth, we find that $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K) \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$; this proves (ii). Parts (iv) and (v) of Theorem 3.1 are shown to hold in the proof of Theorem 1.2 in [Zyw19], cf. Proposition 4.25 of [Zyw19]. Part (vi) of Theorem 3.1 is also shown to hold in the proof of Theorem 1.2 in [Zyw19], cf. Lemmas 4.23 and 4.24 of [Zyw19]. □

Remark 3.4. From Lemma 2.7 of [Zyw19], the set of non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ for which A has good reduction and $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank r has density $1/[K_A^{\mathrm{conn}} : K]$. In particular, there do exists prime ideals $\mathfrak{q}$ as in the statement of Theorem 3.3.

3.4. **Proof of Theorem 3.1.** The theorem follows immediately from Lemma 3.2 and Theorem 3.3 (with Remark 3.4 to show that the assumptions are not vacuous).

4. Geometric monodromy

Fix an abelian scheme $\pi\colon A \to U$ of relative dimension $g \geq 1$, where K is a number field and U is a non-empty open subvariety of $\mathbb{P}^n_K$ for some $n \geq 1$. Fix notation as in §2 and §3. Take a constant b_A as in Theorem 3.1.

In this section, we will prove the following constraints on the images of the representations $\rho_{A,\ell}$ when restricted to the geometric fundamental group $\pi_1(U_{\bar{K}})$; there is no harm in suppressing base points below since $\pi_1(U_{\bar{K}})$ is a normal subgroup of $\pi_1(U)$.

Proposition 4.1. *There is an open subgroup H of $\pi_1(U_{\bar{K}})$ such that the following hold:*

(a) *$\rho_{A,\ell}(H)$ lies in the group of $\mathbb{Q}_\ell$-points of the derived subgroup of $G^\circ_{A,\ell}$ for all primes ℓ,*
(b) *$\rho_{A,\ell}(H) \subseteq \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ for all primes $\ell \geq b_A$.*

4.1. **The algebraic monodromy group.** Fix a field embedding $\bar{K} \subseteq \mathbb{C}$. Let $\mathcal{A} \to U_\mathbb{C}$ be the fiber of $A \to U$ over $U_\mathbb{C}$. Associated to $\pi\colon \mathcal{A}(\mathbb{C}) \to U(\mathbb{C})$, we define the local system $\mathcal{F} := R^1\pi_*\mathbb{Z}$ of $\mathbb{Z}$-modules on $U(\mathbb{C})$, where we are viewing $U(\mathbb{C})$ with its familiar analytic topology. For each $u \in U(\mathbb{C})$, the fiber $\mathcal{F}_u$ of $\mathcal{F}$ at u is the cohomology group $H^1(A_u(\mathbb{C}), \mathbb{Z})$. Fix a point $u_0 \in U(\mathbb{C})$ and define $\Lambda := H^1(A_{u_0}(\mathbb{C}), \mathbb{Z})$; it is a free abelian group of rank $2g$. The local system $\mathcal{F}$ gives rise to a monodromy representation

$$\varrho\colon \pi_1^{\mathrm{top}}(U(\mathbb{C}), u_0) \to \mathrm{Aut}_\mathbb{Z}(\Lambda) \cong \mathrm{GL}_{2g}(\mathbb{Z}),$$

where we are now using the usual topological fundamental group. Let $\mathcal{G}$ be the $\mathbb{Z}$-group subscheme of $\mathrm{GL}_{2g,\mathbb{Z}}$ obtained by taking the Zariski closure of the image of ϱ; we call it the *algebraic monodromy group* of the abelian scheme A.

Lemma 4.2. *The neutral component $(\mathcal{G}_\mathbb{Q})^\circ$ of the linear algebraic group $\mathcal{G}_\mathbb{Q}$ is semisimple.*

Proof. It suffices to prove that the neutral component of $\mathcal{G}_\mathbb{C}$ is semisimple. From Deligne [Del71, Corollaire 4.2.9], the neutral component of $\mathcal{G}_\mathbb{C}$ is semisimple; this uses that $U_\mathbb{C}$ is smooth and connected and that $\pi\colon \mathcal{A}\to U_\mathbb{C}$ is smooth and proper. □

Lemma 4.3. *There is an open and normal subgroup H of $\pi_1(U_{\overline{K}})$ such that the Zariski closure of $\rho_{A,\ell}(H)$ in $\mathrm{GL}_{V_\ell(A)}$ is connected and semisimple for all ℓ.*

Proof. The homomorphism $\pi_1(U_\mathbb{C})\to\pi_1(U_{\overline{K}})$ induced by the embedding $\overline{K}\subseteq\mathbb{C}$ is an isomorphism, so it suffices to prove the lemma with $\overline{K}$ replaced by $\mathbb{C}$. Recall that there is a natural isomorphism between the profinite completion of $\pi_1^{\mathrm{top}}(U(\mathbb{C}),u_0)$ and $\pi_1(U_\mathbb{C})$ (only uniquely defined up to an inner automorphism since we are suppressing base points in our étale fundamental groups).

Take any integer $e\geq 1$. Let $\bar\rho_{\mathcal{A},\ell^e}\colon \pi_1(U_\mathbb{C})\to\mathrm{GL}_{2g}(\mathbb{Z}/\ell^e\mathbb{Z})$ be the representation arising from the locally constant sheaf $\mathcal{A}[\ell^e]$ of $\mathbb{Z}/\ell^e\mathbb{Z}$-modules on $U_\mathbb{C}$. By choosing compatible bases, these representation combine to give a single representation $\rho_{\mathcal{A},\ell}\colon\pi_1(U_\mathbb{C})\to\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$. Let S be the Zariski closure of $\rho_{\mathcal{A},\ell}(\pi_1(U_\mathbb{C}))$ in $\mathrm{GL}_{2g,\mathbb{Q}_\ell}$. Since $\mathcal{A}$ is the fiber of A above $U_\mathbb{C}$, it suffices to prove the lemma with $\rho_{A,\ell}$ replaced by $\rho_{\mathcal{A},\ell}$.

Note that $\mathcal{A}[\ell^e]$ gives a local system of $\mathbb{Z}/\ell^e\mathbb{Z}$-modules on $U(\mathbb{C})$ that is dual to $R^1\pi_*(\mathbb{Z}/\ell^e\mathbb{Z})$, where $\pi\colon\mathcal{A}(\mathbb{C})\to U(\mathbb{C})$; the ℓ^e-torsion of $\mathcal{A}_u(\mathbb{C})$ for a point $u\in U(\mathbb{C})$ is isomorphic to the homology group $H_1(\mathcal{A}_u(\mathbb{C}),\mathbb{Z}/\ell^e\mathbb{Z})$ which is dual to the corresponding cohomology group. Since $R^1\pi_*(\mathbb{Z}/\ell^e\mathbb{Z})$ is isomorphic to $\mathcal{F}/\ell^e\mathcal{F}$, we find that the representation $\bar\rho_{\mathcal{A},\ell^e}\colon\pi_1(U_\mathbb{C})\to\mathrm{GL}_{2g}(\mathbb{Z}/\ell^e\mathbb{Z})$ is isomorphic to the dual of the representation obtained by taking the profinite completion of

$$\pi_1^{\mathrm{top}}(U(\mathbb{C}),u_0)\xrightarrow{\varrho}\mathrm{GL}_{2g}(\mathbb{Z})\to\mathrm{GL}_{2g}(\mathbb{Z}/\ell^e\mathbb{Z}).$$

Therefore, $\rho_{\mathcal{A},\ell}$ is isomorphic to the dual of the representation obtained from $\pi_1^{\mathrm{top}}(U(\mathbb{C}),u_0)\xrightarrow{\varrho}\mathrm{GL}_{2g}(\mathbb{Z})\subseteq\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ by taking the profinite completion and extending using continuity.

Let H_0 be the kernel of $\pi_1^{\mathrm{top}}(U(\mathbb{C}),u_0)\xrightarrow{\varrho}\mathcal{G}(\mathbb{Q})/\mathcal{G}^\circ_\mathbb{Q}(\mathbb{Q})$. The Zariski closure of $\varrho(H_0)$ in $\mathrm{GL}_{2g,\mathbb{Q}_\ell}$ is $\mathcal{G}^\circ_{\mathbb{Q}_\ell}$ which is connected and semisimple by Lemma 4.2. The lemma will then hold by taking H to be the profinite completion of H_0. □

4.2. **Proof of Proposition 4.1.** By Lemma 4.3, there is an open and normal subgroup H of $\pi_1(U_{\overline{K}})$ such that the Zariski closure S_ℓ of $\rho_{A,\ell}(H)$ in $\mathrm{GL}_{V_\ell(A)}$ is connected and semisimple for all ℓ. We have $S_\ell\subseteq G_{A,\ell}$ and hence $S_\ell\subseteq G^\circ_{A,\ell}$ since S_ℓ is connected. Since $G^\circ_{A,\ell}$ is reductive, we find that S_ℓ is contained in the derived subgroup of $G^\circ_{A,\ell}$. This proves (a).

Now take any prime $\ell\geq b_A$. By part (a) and $\rho_{A,\ell}(\pi_1(U))\subseteq\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$, we have $\rho_{A,\ell}(H)\subseteq\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)$. Define the homomorphism

$$\beta_\ell\colon H\to\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)\to B_\ell,$$

where $B_\ell:=\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)/\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$. By Theorem 3.1(v), the group B_ℓ is abelian and its cardinality divides a positive integer Q that depends only on g. In particular, Q is independent of ℓ. So to prove (a), it suffices to show that H has only finitely many abelian quotients whose cardinality divides Q.

The group H is the étale fundamental group of a connected variety X of finite type over $\overline{K}$ (let $X\to U_{\overline{K}}$ be an étale cover corresponding the subgroup H of $\pi_1(U_{\overline{K}})$). From [SGA7.1], II.2.3.1, we find that H is finitely generated as a topological group. In particular, the abelianization H^{ab} of H, i.e, the quotient of H by its commutator subgroup, is a finitely generated topological group. Viewing H^{ab} as an additive group, the quotient $H^{\mathrm{ab}}/QH^{\mathrm{ab}}$ is a finitely generated abelian group whose exponent divides Q. Therefore, $H^{\mathrm{ab}}/QH^{\mathrm{ab}}$ has finite order and hence H has only finitely abelian quotients whose cardinality divides Q.

5. Main reduction

Let K be a number field. Fix an abelian scheme $\pi\colon A \to U$ of relative dimension $g \geq 1$, where U is a non-empty open subvariety of $\mathbb{P}^n_K$ for some $n \geq 1$. Fix notation as in §2 and §3. Take a constant b_A as in Theorem 3.1.

Define the set

$$B := \{u \in U(K) : \bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \not\supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)' \text{ for some prime } \ell \geq b_A\}.$$

The goal of this section is to prove the following proposition which reduces the proof of Theorem 1.1 to showing that the set $B \subseteq \mathbb{P}^n(K)$ has density 0.

Proposition 5.1. *Suppose that B has density 0. Then there is a constant C such that $[\rho_A(\pi_1(U)) : \rho_{A_u}(\mathrm{Gal}_K)] \leq C$ holds for all $u \in U(K)$ away from a set of density 0.*

Remark 5.2. Note that $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ is a normal subgroup of $\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)$ while $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K)$ is a subgroup of $\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)$ uniquely defined up to conjugation. It thus makes sense to ask whether the inclusion $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ holds or not.

5.1. **Proof of Proposition 5.1.** Let $W \subseteq \pi_1(U)$ be the kernel of $\gamma_{A,\ell}$ from §2.2; it is a normal and open subgroup of $\pi_1(U)$ and is independent of ℓ by Lemma 2.4(i). The group $\rho_A(W)'$ is thus normal in $\rho_A(\pi_1(U))$. The homomorphism $\gamma_{A,\ell}$ is surjective so the integer $[G_{A,\ell}(\mathbb{Q}_\ell) : G^\circ_{A,\ell}(\mathbb{Q}_\ell)]$ is independent of ℓ.

For a prime $\ell \geq b_A$, we have $\bar{\rho}_{A,\ell}(\pi_1(U)) \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$. Hilbert's irreducibility theorem implies that $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ for all $u \in U(K)$ away from a set of density 0. Thus there is no harm in replacing b_A by a larger integer. In particular, we may assume that $b_A > 7$ and $b_A > [\pi_1(U) : W]$.

Lemma 5.3. *Take any $u \in U(K)$ satisfying $G_{A_u,\ell} = G_{A,\ell}$ for all ℓ. Then for any integer $m > 1$, we have $\rho_{A_u,m}(\mathrm{Gal}_{K^{\mathrm{conn}}_{A_u}}) = \rho_{A_u,m}(\mathrm{Gal}_K) \cap \rho_{A,m}(W)$.*

Proof. Fix a prime $\ell | m$. The kernel of the homomorphism $\rho_{A,m}(\pi_1(U)) \to G_{A,\ell}(\mathbb{Q}_\ell)/G^\circ_{A,\ell}(\mathbb{Q}_\ell)$ obtained by composing the ℓ-adic projection with the obvious quotient map is equal to $\rho_{A,m}(W)$. Similarly the kernel of the homomorphism $\rho_{A_u,m}(\mathrm{Gal}_K) \to G_{A_u,\ell}(\mathbb{Q}_\ell)/G^\circ_{A_u,\ell}(\mathbb{Q}_\ell)$ obtained by composing the ℓ-adic projection with the obvious quotient map is equal to $\rho_{A_u,m}(\mathrm{Gal}_{K^{\mathrm{conn}}_{A_u}})$. From $G_{A_u,\ell} = G_{A,\ell}$ and the inclusion $\rho_{A_u,m}(\mathrm{Gal}_K) \subseteq \rho_{A,m}(\pi_1(U))$, we deduce that $\rho_{A_u,m}(\mathrm{Gal}_{K^{\mathrm{conn}}_{A_u}}) = \rho_{A_u,m}(\mathrm{Gal}_K) \cap \rho_{A,m}(W)$. □

Lemma 5.4. *The set of $u \in U(K)$ that satisfy*

$$\rho_{A_u,\ell}(\mathrm{Gal}_{K^{\mathrm{conn}}_{A_u}})' = \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$$

for all primes $\ell \geq b_A$ has density 1. For all $\ell \geq b_A$, we have $\rho_{A,\ell}(W)' = \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$.

Proof. Let B_1 be the set of $u \in U(K)$ satisfying the following conditions:

(a) $G_{A_u,\ell} = G_{A,\ell}$ for all primes ℓ,
(b) $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ for all primes $\ell \geq b_A$.

The set of $u \in U(K)$ satisfying (a) has density 1 by Proposition 2.3. The set of $u \in U(K)$ that satisfy (b) has density 1 since the set B in the statement of Proposition 5.1 has density 0 by assumption. Therefore, B_1 has density 1.

Take any $u \in B_1$ and set $L := K^{\mathrm{conn}}_{A_u}$. Take any prime $\ell \geq b_A$. It suffices to prove that $\rho_{A_u,\ell}(\mathrm{Gal}_L)'$ and $\rho_{A,\ell}(W)'$ both equal $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$.

We claim that $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_L)' \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$. Since L/K is a Galois extension and $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ is a (normal) subgroup of $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K)$, the group $H := \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)' \cap \bar{\rho}_{A_u,\ell}(\mathrm{Gal}_L)$ is a normal subgroup of $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ of index at most

$$[L:K] = [G_{A_u,\ell}(\mathbb{Q}_\ell) : G^\circ_{A_u,\ell}(\mathbb{Q}_\ell)] = [G_{A,\ell}(\mathbb{Q}_\ell) : G^\circ_{A,\ell}(\mathbb{Q}_\ell)] = [\pi_1(U) : W].$$

By our choice of b_A and $\ell \geq b_A$, we have $[\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)' : H] \leq [\pi_1(U) : W] < b_A \leq \ell$. Now suppose that $H \neq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$. So there is a simple group S that is a quotient of $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ and satisfies $|S| < \ell$. Theorem 3.1(iv) implies that S is of Lie type type in characteristic ℓ and hence ℓ divides $|S|$. This contradicts

$|S| < \ell$, so we deduce that $H = \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$. Therefore, $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_L) \supseteq H = \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$. Since $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ is perfect by Theorem 3.1(iv), we have $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_L)' \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'' = \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ which proves the claim.

Since $u \in B_1$, Lemma 5.3 implies that $\rho_{A_u,\ell}(\mathrm{Gal}_L)$ is a subgroup of $\rho_{A,\ell}(W) \subseteq \mathcal{G}^\circ_{A,\ell}(\mathbb{Z}_\ell)$. Therefore,

$$\rho_{A_u,\ell}(\mathrm{Gal}_L)' \subseteq \rho_{A,\ell}(W)' \subseteq \mathcal{G}^\circ_{A,\ell}(\mathbb{Z}_\ell)' = \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)',$$

where the last equality uses Theorem 3.1(iv). So to prove the lemma it thus suffices to show that $\rho_{A_u,\ell}(\mathrm{Gal}_L)' \supseteq \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$. The image of $\rho_{A_u,\ell}(\mathrm{Gal}_L)'$ in $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)$ is $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_L)'$ and hence contains $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ by our claim. Theorem 3.1(vi) implies that $\rho_{A_u,\ell}(\mathrm{Gal}_L)' \supseteq \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ as desired □

Lemma 5.5. *Take any prime p, any subgroup G of $\mathrm{GL}_{2g}(\mathbb{F}_p)$, and any composition factor S of G. There is an integer J, depending only on g, such that S is abelian, S is of Lie type in characteristic p, or $|S| < J$.*

Proof. This is an immediate consequence of Theorem 0.2 of [LP11]. □

Let M be the product of all primes $\ell \leq \max\{b_A, J\}$, where J is as in Lemma 5.5. Define the group

$$\mathcal{B} := \rho_{A,M}(W)' \times \prod_{\ell \nmid M} \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'.$$

After the following lemma, we will prove that $\rho_A(W)'$ is equal to $\mathcal{B}$.

Lemma 5.6. *Let H be a closed subgroup of $\mathcal{B}$. Suppose that the projection maps $H \to \rho_{A,M}(W)'$ and $H \to \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$, with $\ell \nmid M$, are surjective. Then $H = \mathcal{B}$.*

Proof. After choosing bases of the $\mathbb{Z}_\ell$-modules $T_\ell(A)$, one can identify $\mathcal{B}$ with a closed subgroup of $\mathrm{GL}_{2g}(\widehat{\mathbb{Z}})$. For each integer $e \geq 2$, let $\mathcal{B}_e$ be the kernel of the reduction modulo e homomorphism $\mathcal{B} \subseteq \mathrm{GL}_{2g}(\widehat{\mathbb{Z}}) \to \mathrm{GL}_{2g}(\mathbb{Z}/e\mathbb{Z})$. We have $\mathcal{B} = \varprojlim_e \mathcal{B}/\mathcal{B}_e$, where e is ordered by divisibility. Since H is a closed subgroup of $\mathcal{B}$, it suffices to prove that $H \to \mathcal{B}/\mathcal{B}_e$ is surjective for all $e \geq 2$.

Suppose that $H \to \mathcal{B}/\mathcal{B}_e$ is not surjective for some $e \geq 2$. We have an isomorphism $\mathcal{B}/\mathcal{B}_e \cong Q_M \times \prod_{\ell \nmid M} Q_\ell$ of groups for which all the following hold:

- Q_M and Q_ℓ (with $\ell \nmid M$) are finite quotients of $\rho_{A,M}(W)'$ and $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$, respectively,
- $Q_\ell = 1$ for all but finitely many primes $\ell \nmid M$,
- the projection maps $H \to \mathcal{B}/\mathcal{B}_e \to Q_M$ and $H \to \mathcal{B}/\mathcal{B}_e \to Q_\ell$ (with $\ell \nmid M$) are surjective.

The last condition uses our assumptions on H in the statement of the lemma.

Since $H \to \mathcal{B}/\mathcal{B}_e$ is not surjective, there is an integer $b > 1$ relatively prime to M and a proper subgroup H_0 of $Q_M \times \prod_{\ell | b} Q_\ell$ such that the projection map $H_0 \to Q_m$ is surjective for all $m \in \{M\} \cup \{\ell : \ell | b\}$. So there are non-empty and disjoint subsets I_1 and I_2 of $\{M\} \cup \{\ell : \ell | b\}$ and a proper subgroup H_1 of $\prod_{m \in I_1} Q_m \times \prod_{m \in I_2} Q_m$ such that the projection map $H_1 \to \prod_{m \in I_i} Q_m$ is surjective for each $i \in \{1, 2\}$.

Set $G_i := \prod_{m \in I_i} Q_m$ for $1 \leq i \leq 2$. Let N and N' be the kernel of the projection maps $H_1 \to G_2$ and $H_1 \to G_1$, respectively. We have $H_1 \subseteq G_1 \times G_2$ and hence $N \subseteq G_1 \times \{1\}$ and $N' \subseteq \{1\} \times G_2$. We can thus identify N and N' with normal subgroups of G_1 and G_2, respectively. By Goursat's lemma (see [Rib76, Lemma 5.2.1]), the image of H_1 in $G_1/N \times G_2/N'$ is the graph of an isomorphism $G_1/N \cong G_2/N'$.

Suppose that G_1/N and G_2/N' are both trivial. We have $N = G_1$ and $N' = G_2$ and hence $H_1 = G_1 \times G_2$. However, this contradicts that H_1 is a proper subgroup of $G_1 \times G_2$. Therefore, there is a simple group S that is isomorphic to a quotient of both G_1 and G_2. In particular, there are distinct $m_1, m_2 \in \{M\} \cup \{\ell : \ell | b\}$ such that S is isomorphic to a quotient of both Q_{m_1} and Q_{m_2}. We may assume that $m_2 = \ell$ is a prime not dividing M.

Since $\ell \nmid M$, every simple quotient of $Q_{m_2} = Q_\ell$ is non-abelian and of Lie type in characteristic ℓ by Theorem 3.1(iv). Therefore, S is a non-abelian simple group of Lie type in characteristic ℓ.

Suppose that m_1 is a prime p that does not M. By the same argument, S is also a non-abelian simple group of Lie type in characteristic p. However, there are no simple groups that are of Lie type in both characteristic ℓ and p, where ℓ and p are distinct primes with $\ell > 7$ (we have $\ell > 7$ since $\ell \nmid M$). This contradiction implies that $m_1 = M$. In particular, S is a non-abelian group that is a quotient of Q_M and hence also of $\rho_{A,M}(W)'$.

Define $m := \prod_{\ell|M} \ell$. The kernel of the quotient homomorphism

$$\rho_{A,M}(W)' \subseteq \mathrm{Aut}_{\mathbb{Z}_m}(T_m(A)) \to \mathrm{Aut}_{\mathbb{Z}/m\mathbb{Z}}(T_m(A)/mT_m(A)) \cong \prod_{p|M} \mathrm{GL}_{2g}(\mathbb{F}_p)$$

is a product of pro-p groups with $p|M$; in particular, it is prosolvable. So there is a prime $p|M$ and a subgroup G of $\mathrm{GL}_{2g}(\mathbb{F}_p)$ such that S is isomorphic to a composition factor of G. Since S is non-abelian, Lemma 5.5 implies that S is of Lie type in characteristic p or satisfies $|S| < J$. The group S cannot be of Lie type in characteristic p since again there are no simple groups that are of Lie type in both characteristic ℓ and p, where ℓ and p are distinct primes with $\ell > 7$. Therefore, $|S| < J$. Since S is of Lie type in characteristic ℓ, it has an element of order ℓ and hence $\ell \leq |S| < J$. However, this contradicts that $\ell \nmid M$. This contradiction proves that $H \to \mathcal{B}/\mathcal{B}_e$ is surjective for all $e \geq 2$ as desired. □

Lemma 5.7. *We have $\rho_A(W)' = \mathcal{B}$.*

Proof. Take any prime $\ell \geq b_A$. By Theorem 3.1(ii), we have $\rho_{A,\ell}(\pi_1(U)) \supseteq \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$. We thus have inclusions

$$\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)' \subseteq \rho_{A,\ell}(W) \subseteq \mathcal{G}^\circ_{A,\ell}(\mathbb{Z}_\ell). \tag{5.1}$$

By Theorem 3.1(iv), the commutators subgroups of both $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ and $\mathcal{G}^\circ_{A,\ell}(\mathbb{Z}_\ell)$ are equal to $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$. Taking commutators of the groups in (5.1), we deduce that $\rho_{A,\ell}(W)' = \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$.

We can identify $\rho_A(W)'$ with a closed subgroup of $\rho_{A,M}(W)' \times \prod_{\ell\nmid M} \rho_{A,\ell}(W)' = \mathcal{B}$. Since the projections of $\rho_A(W)'$ to $\rho_{A,M}(W)'$ and $\rho_{A,\ell}(W)' = \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$, with $\ell \nmid M$, are surjective, we deduce that $\rho_A(W)' = \mathcal{B}$ by Lemma 5.6. □

Lemma 5.8. *The set of $u \in U(K)$ for which $\rho_{A_u}(\mathrm{Gal}_K) \supseteq \rho_A(W)'$ holds has density* 1.

Proof. Take any $u \in U(K)$ that satisfies all the following conditions with $L := K^{\mathrm{conn}}_{A_u}$:

(a) $G_{A_u,\ell} = G_{A,\ell}$ for all ℓ,
(b) $\rho_{A_u,M}(\mathrm{Gal}_K) = \rho_{A,M}(\pi_1(U))$
(c) $\rho_{A_u,\ell}(\mathrm{Gal}_L)' = \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ for all $\ell \geq b_A$

By Lemma 5.3 with (a) and (b), we have $\rho_{A_u,M}(\mathrm{Gal}_L) = \rho_{A_u,M}(\mathrm{Gal}_K) \cap \rho_{A,M}(W) = \rho_{A,M}(W)$. In particular, $\rho_{A_u,M}(\mathrm{Gal}_L)' = \rho_{A,M}(W)'$. From this and (c), we deduce that $\rho_{A_u}(\mathrm{Gal}_L)'$ is a closed subgroup of $\mathcal{B} = \rho_{A,M}(W)' \times \prod_{\ell\nmid M} \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ for which the projection maps to $\rho_{A,M}(W)'$ and $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$, with $\ell \nmid M$, are all surjective. By Lemmas 5.6 and 5.7, we have $\rho_{A_u}(\mathrm{Gal}_L)' = \mathcal{B} = \rho_A(W)'$.

To complete the lemma, it thus suffices to show that the set of $u \in U(K)$ that satisfy each of the conditions (a), (b) and (c) has density 1. The set of $u \in U(K)$ that satisfy (a) has density 1 by Proposition 2.3. The set of $u \in U(K)$ that satisfy (b) has density 1 by Lemma 2.2(i). The set of $u \in U(K)$ that satisfy (c) has density 1 by Lemma 5.4. □

Let

$$\beta_A \colon \pi_1(U) \to \rho_A(\pi_1(U))/\rho_A(W)'$$

be the surjective homomorphism obtained by composing ρ_A with the obvious quotient map.

Lemma 5.9. *The group $\beta_A(\pi_1(U_{\overline{K}}))$ is finite.*

Proof. We need to prove that there is an open subgroup H of $\pi_1(U_{\overline{K}})$ such that $\rho_A(H)$ is contained in $\rho_A(W)' = \mathcal{B} = \rho_{A,M}(W)' \times \prod_{\ell\nmid M} \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$. By Proposition 4.1, there is an open subgroup H of $\pi_1(U_{\overline{K}})$ such that $\rho_{A,\ell}(H) \subseteq \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ for all $\ell \geq b_A$. It thus suffices to show that there is an open subgroup H of $\pi_1(U_{\overline{K}})$ such that $\rho_{A,M}(H) \subseteq \rho_{A,M}(W)'$.

The group $\rho_{A,M}(W)$ is open in $\prod_{\ell|M} G^\circ_{A,\ell}(\mathbb{Q}_\ell)$ since $\rho_{A,\ell}(W)$ is open in $G^\circ_{A,\ell}(\mathbb{Q}_\ell)$ for all $\ell|M$ (note that each $\rho_{A,\ell}(W)$ has an open pro-ℓ subgroup). For each ℓ, let $S_{A,\ell}$ be the derived subgroup of $G^\circ_{A,\ell}$. Note that for every open subgroup H of $G^\circ_{A,\ell}(\mathbb{Q}_\ell)$, the commutator subgroup H' is open in $S_{A,\ell}(\mathbb{Q}_\ell)$, cf. [HL15, Proposition 3.2]. Therefore, $\rho_{A,M}(W)'$ is an open subgroup of $\prod_{\ell|M} S_{A,\ell}(\mathbb{Q}_\ell)$.

By Proposition 4.1, there is an open subgroup H of $\pi_1(U_{\overline{K}})$ such that $\rho_{A,M}(H) \subseteq \prod_{\ell|M} S_{A,\ell}(\mathbb{Q}_\ell)$. Since $\rho_{A,M}(H)$ is compact in $\prod_{\ell|M} S_{A,\ell}(\mathbb{Q}_\ell)$ and $\rho_{A,M}(W)'$ is open in $\prod_{\ell|M} S_{A,\ell}(\mathbb{Q}_\ell)$, we find that $\rho_{A,M}(H) \cap$

$\rho_{A,M}(W)'$ is a finite index subgroup of $\rho_{A,M}(H)$. So after replacing H by a suitable open subgroup, we will have $\rho_{A,M}(H) \subseteq \rho_{A,M}(W)'$. □

Let C be the cardinality of $\beta_A(\pi_1(U_{\overline{K}}))$; it is finite by Lemma 5.9. Take any $u \in U(K)$ for which $\rho_{A_u}(\mathrm{Gal}_K) \supseteq \rho_A(W)'$. We will now show that $[\rho_A(\pi_1(U)) : \rho_{A_u}(\mathrm{Gal}_K)] \leq C$. Since the set of $u \in U(K)$ satisfying $\rho_{A_u}(\mathrm{Gal}_K) \supseteq \rho_A(W)'$ has density 1 by Lemma 5.8, this will complete the proof of the proposition.

Let $\beta_{A,u}\colon \mathrm{Gal}_K \to \rho_A(\pi_1(U))/\rho_A(W)'$ be the homomorphism obtained by specializing β_A at u. We have

$$[\rho_A(\pi_1(U))/\rho_A(W)' : \beta_{A,u}(\mathrm{Gal}_K)] \leq C$$

since the homomorphism

$$\pi_1(U) \xrightarrow{\rho_A} (\rho_A(\pi_1(U))/\rho_A(W)')/\beta_A(\pi_1(U_{\overline{K}}))$$

is surjective and factors through Gal_K (in particular, its specialization at a point $u \in U(K)$ is independent of the choice u). Since $\rho_{A_u}(\mathrm{Gal}_K) \supseteq \rho_A(W)'$, we have

$$\begin{aligned}[\rho_A(\pi_1(U)) : \rho_{A_u}(\mathrm{Gal}_K)] &= [\rho_A(\pi_1(U))/\rho_A(W)' : \rho_{A_u}(\mathrm{Gal}_K)/\rho_A(W)'] \\ &= [\rho_A(\pi_1(U))/\rho_A(W)' : \beta_{A,u}(\mathrm{Gal}_K)] \\ &\leq C.\end{aligned}$$

This completes the proof of Proposition 5.1.

Remark 5.10. The above constant C is precisely the one described in §1.2. With notation as in §1.2, the group M is equal to $\rho_A(W)$. In §9, we will show that the set B has density 0 and this will imply, by Proposition 5.1, that Theorem 1.1 holds with this particular constant C.

6. Explicit Hilbert irreducibility

Let U be a nonempty open subvariety of $\mathbb{P}^n_K$ for some integer $n \geq 1$, where K is a number field. Let

$$\rho\colon \pi_1(U) \to G$$

be a continuous and surjective homomorphism, where G is a finite group. For each point $u \in U(K)$, we obtain a homomorphism $\rho_u\colon \mathrm{Gal}_K \to G$ by specializing ρ at u; it is uniquely defined up to conjugation by an element of G.

Let G_g be the image of $\pi_1(U_{\overline{K}})$ under ρ; it is a well-defined normal subgroup of G. Let L be the minimal extension of K in $\overline{K}$ for which G_g is the image of $\pi_1(U_L)$. We have a natural short exact sequence

$$1 \to G_g \to G \xrightarrow{\varphi} \mathrm{Gal}(L/K) \to 1.$$

Let $\mathcal{U}$ be the open subscheme of $\mathbb{P}^n_{\mathcal{O}_K}$ that is the complement of the Zariski closure of $\mathbb{P}^n_K - U$ in $\mathbb{P}^n_{\mathcal{O}_K}$. The $\mathcal{O}_K$-scheme $\mathcal{U}$ has generic fiber U. Fix a finite set $\mathscr{S}$ of non-zero prime ideals of $\mathcal{O}_K$ such that ρ arises from a continuous homomorphism $\varrho\colon \pi_1(\mathcal{U}_{\mathcal{O}}) \to G$, where $\mathcal{O}$ is the ring of $\mathscr{S}$-integers in K.

Theorem 6.1. *With notation as above, fix a Galois extension $F \subseteq L$ of K and a set $C \subseteq G$ that is stable under conjugation by G. Define*

$$\delta := \max_{\kappa} \frac{|C \cap \kappa|}{|G_g|},$$

where κ varies over the G_g-cosets of $\varphi^{-1}(\mathrm{Gal}(L/F))$. Assume that $\delta < 1$. Then for $x \geq 2$,

$$|\{u \in U(K) : H(u) \leq x,\, \rho_u(\mathrm{Gal}_K) \subseteq C\}| \ll_{U,F,\delta} x^{(n+1/2)[K:\mathbb{Q}]} \log x + |\mathscr{S}|^{4n+4} + |C|^{2n+2} \cdot |G_g|^{4n+4}.$$

Recall that Hilbert's irreducibility theorem implies that $\rho_u(\mathrm{Gal}_K) = G$ for all $u \in U(K)$ away from a set of density 0. Corollary 6.2 shows how Theorem 6.1 can be viewed as an explicit version of Hilbert's irreducibility theorem.

Corollary 6.2. *For $x \geq 2$, we have*

$$|\{u \in U(K) : H(u) \leq x,\, \rho_u(\mathrm{Gal}_K) \neq G\}| \ll_{U,L,|G|} x^{[K:\mathbb{Q}](n+1/2)} \log x + |\mathscr{S}|^{4n+4}.$$

Proof. For each $u \in U(K)$, the quotient map $\rho_u(\mathrm{Gal}_K) \to G/G_g$ is surjective. So if $\rho_u(\mathrm{Gal}_K) \neq G$, then $\rho_u(\mathrm{Gal}_K)$ is contained in a maximal subgroup M of G for which $M \to G/G_g$ is surjective. It thus suffices to bound $|\{u \in U(K) : H(u) \leq x,\, \rho_u(\mathrm{Gal}_K) \subseteq \bigcup_{g\in G} gMg^{-1}\}|$ for any such M; the corollary will then follow by summing over all M (the number of such maximal subgroups can be bounded in terms of $|G|$).

Take any maximal subgroup M of G for which the quotient map $M \to G/G_g$ is surjective. Define $C := \cup_{g\in G}\, gMg^{-1} = \cup_{g\in G_g} gMg^{-1}$, where the last equality uses our assumption that $M \to G/G_g$ is surjective. We have $C \cap G_g = \cup_{g\in G_g} g(M\cap G_g)g^{-1}$ since G_g is normal in G. The group $M \cap G_g$ is a proper subgroup of G_g since $M \neq G$ and $M \to G/G_g$ is surjective. Jordan's lemma ([Ser03, Theorem 4']) implies that $C \cap G_g \neq G_g$. In particular, $\delta := |C\cap G_g|/|G_g| \leq 1 - 1/|G_g| < 1$. Applying Theorem 6.1 with $F = L$, we have

$$|\{u \in U(K) : H(u) \leq x,\, \rho_u(\mathrm{Gal}_K) \subseteq C\}| \ll_{U,L,|G|} x^{[K:\mathbb{Q}](n+1/2)}\log x + |\mathscr{S}|^{4n+4}$$

as desired. □

6.1. **Equidistribution over finite fields.** Fix a finite field $\mathbb{F}_q$ of cardinality q and denote its characteristic by p. In this section, we denote by U a smooth affine variety over $\mathbb{F}_q$ that is geometrically irreducible and has dimension $d \geq 1$. Take positive integers N, r and δ such that $U_{\overline{\mathbb{F}}_q}$ is isomorphic to a closed subscheme of $\mathbb{A}^N_{\overline{\mathbb{F}}_q}$ defined by the vanishing of r polynomials of degree at most δ.

Consider a surjective continuous homomorphism

$$\varrho\colon \pi_1(U) \to G,$$

where G is a finite group. Define $G_g := \varrho(\pi_1(U_{\overline{\mathbb{F}}_q}))$; it is a normal subgroup of G. We have a natural short exact sequence

$$1 \to G_g \to G \xrightarrow{\varphi} \mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q) \to 1$$

for some $e \geq 1$. Let κ be the G_g-coset of G that is the inverse image of the q-th power Frobenius automorphism $\mathrm{Frob}_q \in \mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$ under φ. If $U(\mathbb{F}_q) \neq \emptyset$, we can also characterize κ as the unique G_g-coset of G that contains $\rho(\mathrm{Frob}_u)$ for all $u \in U(\mathbb{F}_q)$.

Theorem 6.3. *Fix notation as above and assume that $p \nmid |G_g|$. Let $C \subseteq \kappa$ be a set stable under conjugation by G. Then*

$$|\{u \in U(\mathbb{F}_q) : \varrho(\mathrm{Frob}_u) \in C\}| = \frac{|C|}{|G_g|}\,|U(\mathbb{F}_q)| + O_{N,r,\delta}\big(|C|^{1/2}|G_g|q^{d-1/2}\big).$$

Proof. (Sketch) This is essentially Theorem 1.1 of [Kow06a] due to Kowalski; the key difference is that we are more explicit with the dependencies in the implicit constant (we also have $|G_g|$ in our error term instead of $|G|$). We now sketch the minor changes that need to be made in Kowalski's proof.

Choose any prime $\ell \neq p$. Let $V \to \mathcal{U}_{\overline{\mathbb{F}}_q}$ be the finite étale Galois covering with group G_g corresponding to the surjective homomorphism $\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_q}) \xrightarrow{\rho} G_g$. By Propositions 4.5 and 4.4 of [Kow06b] and using $p \nmid |G_g|$, we have

$$\sigma_c(V, \mathbb{Q}_\ell) := \sum_i \dim H^i_c(V,\mathbb{Q}_\ell) \leq c(N,r,\delta)\cdot|G_g|,$$

where $c(N,r,\delta)$ is a constant depending only on N, r and δ. Moreover, [Kow06b] gives an explicit value of $c(N,r,d)$. Proposition 4.7 of [Kow06b] and its proof imply that

$$\sigma_c(U_{\overline{\mathbb{F}}_q}, \pi(\rho)) := \sum_i H^i_c(U_{\overline{\mathbb{F}}_q}, \pi(\rho)) \leq c(N,r,\delta)\cdot|G_g|\cdot\dim\pi \tag{6.1}$$

for any representation $\pi\colon G_g \to \mathrm{GL}_{\dim\pi}(\overline{\mathbb{Q}}_\ell)$, where $\pi(\rho)$ denotes the lisse $\overline{\mathbb{Q}}_\ell$-sheaf corresponding to $\pi\circ\rho\colon \pi_1(U_{\overline{\mathbb{F}}_q}) \to \mathrm{GL}_{\dim\pi}(\overline{\mathbb{Q}}_\ell)$. Examining the proof of Theorem 1.1 of [Kow06a] with the bound (6.1), we have

$$\left|\,|\{u \in U(\mathbb{F}_q) : \rho(\mathrm{Frob}_u) \in C\}| - \frac{|C|}{|G_g|}\,|U(\mathbb{F}_q)|\right| \leq c(N,r,\delta)\cdot|C|^{1/2}|G_g|^{3/2}q^{d-1/2}$$

which gives the theorem. □

6.2. **Sieving.** Fix a subset $B \subseteq \mathbb{P}^n(K)$ with $n \geq 1$. Let Σ be a set of non-zero primes ideals $\mathfrak{p}$ of $\mathcal{O}_K$ with positive density. Let $\mathscr{S}$ be a finite subset of Σ. Suppose that there are real numbers $0 \leq \delta < 1$ and $c \geq 1$ such that the image of the reduction modulo $\mathfrak{p}$ map $B \to \mathbb{P}^n(\mathbb{F}_\mathfrak{p})$ has cardinality at most $\delta N(\mathfrak{p})^n + cN(\mathfrak{p})^{n-1/2}$ for all $\mathfrak{p} \in \Sigma - \mathscr{S}$.

The follow proposition uses the large sieve to bound $|\{u \in B : H(u) \leq x\}|$; we will use it later to prove Theorem 6.1.

Proposition 6.4. *Fix notation and assumptions as above. For $x \geq 2$, we have*

$$|\{u \in B : H(u) \leq x\}| \ll_{K,n,\Sigma} (1-\delta)^{-1} \cdot x^{(n+1/2)[K:\mathbb{Q}]} \log x + |\mathscr{S}|^{4n+4} + ((1-\delta)^{-1}c)^{4n+4}.$$

Proof. For each $a = (a_1, \ldots, a_{n+1}) \in \mathcal{O}_K^{n+1}$, define

$$\|a\| := \max_{1\leq i\leq n+1} \max_\sigma |\sigma(a_i)|,$$

where σ runs over the field embeddings $K \hookrightarrow \mathbb{C}$. Note that $\|\cdot\|$ extends uniquely to a norm on $\mathcal{O}_K^{n+1} \otimes_\mathbb{Z} \mathbb{R}$.

Let B' be the set of $a \in \mathcal{O}_K^{n+1} - \{0\}$ for which the image of a in $\mathbb{P}^n(K)$ lies in B. We first bound the number of $a \in B'$ for which $\|a\| \leq x$. For a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, let $B'_\mathfrak{p}$ be the the image of B' under the reduction modulo $\mathfrak{p}$ map $\mathcal{O}_K^{n+1} \to \mathbb{F}_\mathfrak{p}^{n+1}$. Define $\omega_\mathfrak{p} := 1 - |B'_\mathfrak{p}|/N(\mathfrak{p})^{n+1}$. We may assume $\omega_\mathfrak{p} < 1$ since otherwise $B = \emptyset$ and the proposition is trivial.

Now suppose $\mathfrak{p} \in \Sigma - \mathscr{S}$. Using our assumption on the image of B modulo $\mathfrak{p}$ and $c \geq 1$, we find that

$$|B'_\mathfrak{p}| \leq (\delta N(\mathfrak{p})^n + cN(\mathfrak{p})^{n-1/2}) \cdot |\mathbb{F}_\mathfrak{p}^\times| + 1 \leq \delta N(\mathfrak{p})^{n+1} + cN(\mathfrak{p})^{n+1/2}$$

and hence $|B'_\mathfrak{p}|/N(\mathfrak{p})^{n+1} \leq \delta + c/N(\mathfrak{p})^{1/2}$. If $N(\mathfrak{p}) \geq 4c^2/(1-\delta)^2$, then

$$|B'_\mathfrak{p}|/N(\mathfrak{p})^{n+1} \leq \delta + c/(4c^2/(1-\delta)^2)^{1/2} = (1+\delta)/2$$

and hence $\omega_\mathfrak{p} \geq (1-\delta)/2$.

Since Σ has positive density, there is a constant $b \geq 1$ depending only on Σ such that

$$\#\{\mathfrak{p} \in \Sigma - \mathscr{S} : y/2 \leq N(\mathfrak{p}) \leq y\} \gg_\Sigma y/\log y$$

holds for all real y satisfying $y \geq b$ and $y \geq |\mathscr{S}|^2$.

- First take any $x \geq 2$ satisfying

$$x^{[K:\mathbb{Q}]/2} \geq \max\{b, |\mathscr{S}|^2, 8c^2/(1-\delta)^2\}.$$

The large sieve ([Ser97, §12.1]) implies that for any $Q \geq 1$, we have

$$|\{a \in B' : \|a\| \leq x\}| \ll_{K,n} \frac{\max\{x^{(n+1)[K:\mathbb{Q}]}, Q^{2(n+1)}\}}{L(Q)}, \tag{6.2}$$

where

$$L(Q) := \sum_\mathfrak{a} \prod_{\mathfrak{p}|\mathfrak{a}} \frac{\omega_\mathfrak{p}}{1-\omega_\mathfrak{p}}$$

and the sum is over the square-free ideals $\mathfrak{a}$ of $\mathcal{O}_K$ with norm at most Q. We interpret (6.2) as being the trivial bound $+\infty$ when $L(Q) = 0$.

Set $Q := x^{[K:\mathbb{Q}]/2}$. Take any prime $\mathfrak{p} \in \Sigma - \mathscr{S}$ with $Q/2 \leq N(\mathfrak{p}) \leq Q$. We have $N(\mathfrak{p}) \geq \frac{1}{2}x^{[K:\mathbb{Q}]/2} \geq 4c^2/(1-\delta)^2$ and hence $\omega_\mathfrak{p} \geq (1-\delta)/2$. Since $t/(1-t)$ is increasing on the interval $[0,1)$, we have $\omega_\mathfrak{p}/(1-\omega_\mathfrak{p}) \geq ((1-\delta)/2)/(1-(1-\delta)/2) = (1-\delta)/(1+\delta)$. Therefore,

$$L(Q) \geq \sum_{\substack{\mathfrak{p}\in\Sigma-\mathscr{S} \\ Q/2\leq N(\mathfrak{p})\leq Q}} \frac{1-\delta}{1+\delta} \geq \frac{1-\delta}{2} \cdot \#\{\mathfrak{p} \in \Sigma - \mathscr{S} : Q/2 \leq N(\mathfrak{p}) \leq Q\}.$$

We have $Q = x^{[K:\mathbb{Q}]/2} \geq \max\{b, |\mathscr{S}|^2\}$ and hence $L(Q) \gg_\Sigma (1-\delta)Q/\log Q \gg_K (1-\delta)\, x^{[K:\mathbb{Q}]/2}/\log x$. From (6.2), we deduce that

$$|\{a \in B' : \|a\| \leq x\}| \ll_{K,n,\Sigma,} (1-\delta)^{-1} \cdot x^{(n+1/2)[K:\mathbb{Q}]} \log x.$$

- Now suppose that $x \geq 2$ satisfies $x^{[K:\mathbb{Q}]/2} \leq \max\{b, |\mathscr{S}|^2, 8c^2/(1-\delta)^2\}$. Therefore,

$$\begin{aligned} |\{a \in B' : \|a\| \leq x\}| &\leq |\{a \in \mathcal{O}_K^{n+1} : \|a\| \leq x\}| \\ &\ll_{K,n} x^{(n+1)[K:\mathbb{Q}]} \\ &\leq (\max\{b, |\mathscr{S}|^2, 8c^2/(1-\delta)^2\})^{2n+2}. \end{aligned}$$

Combining both cases for $x \geq 2$ and using $b \ll_\Sigma 1$ gives

$$|\{a \in B' : \|a\| \leq x\}| \ll_{K,n,\Sigma} (1-\delta)^{-1} \cdot x^{(n+1/2)[K:\mathbb{Q}]} \log x + |\mathscr{S}|^{4n+4} + ((1-\delta)^{-1}c)^{4n+4}. \tag{6.3}$$

By the proposition in §13.4 of [Ser97], there is a constant c', depending only on K and n, such that each $u \in \mathbb{P}^n(K)$ is represented by a tuple $a \in \mathcal{O}_K^{n+1}$ with $\|a\| \leq c'H(u)$. In particular, we have $|\{u \in B : H(u) \leq x\}| \leq |\{a \in B' : \|a\| \leq c'x\}|$. The proposition now follows directly from (6.3) and $c' \ll_{K,n} 1$. □

6.3. **Proof of Theorem 6.1.** We may assume that the set C is non-empty since otherwise the bound in the theorem is trivial.

Lemma 6.5. *There is a finite set $\mathscr{S}_1$ of non-zero prime ideals of $\mathcal{O}_K$, depending only on $U \subseteq \mathbb{P}^n_K$, such that $\varrho(\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_\mathfrak{p}})) = G_g$ for all non-zero prime ideals $\mathfrak{p} \notin \mathscr{S} \cup \mathscr{S}_1$ of $\mathcal{O}_K$ satisfying $\mathfrak{p} \nmid |G_g|$.*

Proof. Define the closed subvariety $Z := \mathbb{P}^n_K - U$ of $\mathbb{P}^n_K$. Let $\mathcal{Z}$ be the Zariski closure of Z in $\mathbb{P}^n_{\mathcal{O}_K}$; its complement in $\mathbb{P}^n_{\mathcal{O}_K}$ is $\mathcal{U}$. For a commutative ring R, let $\mathrm{Gr}_R(1,n)$ be the Grassmannian of lines in $\mathbb{P}^n_R$. In §4H1 of [LSTX19], a closed subscheme $\mathcal{W}$ of $\mathrm{Gr}_{\mathcal{O}_K}(1,n)$ is constructed such that for each $\mathcal{O}_K$-algebra R and line $\mathcal{L} \in (\mathrm{Gr}_{\mathcal{O}_K}(1,n) - \mathcal{W})(R)$, the scheme theoretic intersection $\mathcal{L} \cap \mathcal{Z}_R$ is finite and étale over $\operatorname{Spec} R$. We have $\mathcal{W} \neq \mathrm{Gr}_{\mathcal{O}_K}(1,n)$ by Bertini's theorem. Let $\mathscr{S}_1$ be the (finite) set consisting of all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ for which $\mathcal{W}_{\mathbb{F}_\mathfrak{p}} \neq \mathrm{Gr}_{\mathcal{O}_K}(1,n)_{\mathbb{F}_\mathfrak{p}}$. Note that $\mathscr{S}_1$ depends only on $U \subseteq \mathbb{P}^n_K$.

Now take any non-zero prime ideal $\mathfrak{p} \notin \mathscr{S} \cup \mathscr{S}_1$ of $\mathcal{O}_K$ satisfying $\mathfrak{p} \nmid |G_g|$. Let $\mathcal{O}_\mathfrak{p}^{\mathrm{un}}$ be the ring of integers in the maximal unramified extension of $K_\mathfrak{p}^{\mathrm{un}}$ of $K_\mathfrak{p}$ in a fixed algebraic closure $\overline{K}_\mathfrak{p}$. The ring $\mathcal{O}_\mathfrak{p}^{\mathrm{un}}$ is a complete discrete valuation ring with residue field $\overline{\mathbb{F}}_\mathfrak{p}$. Take any line $L \in (\mathrm{Gr}_{\mathcal{O}_K}(1,n) - \mathcal{W})(\overline{\mathbb{F}}_\mathfrak{p})$. Since $\mathrm{Gr}_{\mathcal{O}_K}(1,n)$ is smooth and $\mathcal{W}$ is a closed subscheme, there is a line $\mathcal{L} \in (\mathrm{Gr}_{\mathcal{O}_K}(1,n) - \mathcal{W})(\mathcal{O}_\mathfrak{p}^{\mathrm{un}})$ whose image in $(\mathrm{Gr}_{\mathcal{O}_K}(1,n) - \mathcal{W})(\overline{\mathbb{F}}_\mathfrak{p})$ is L. Define the $\mathcal{O}_\mathfrak{p}^{\mathrm{un}}$-scheme $\mathcal{V} := \mathcal{U}_{\mathcal{O}_\mathfrak{p}^{\mathrm{un}}} \cap \mathcal{L}$. We have $\mathcal{V} = \mathcal{L} - \mathcal{D}$, where $\mathcal{D} := \mathcal{L} \cap \mathcal{Z}_{\mathcal{O}_\mathfrak{p}^{\mathrm{un}}}$. Observe that $\mathcal{D}$ is finite étale over $\operatorname{Spec} \mathcal{O}_\mathfrak{p}^{\mathrm{un}}$ since $\mathcal{L} \notin \mathcal{W}(\mathcal{O}_\mathfrak{p}^{\mathrm{un}})$.

We claim that the homomorphism

$$\pi_1(\mathcal{V}_{\overline{K}_\mathfrak{p}}) = \pi_1(\mathcal{U}_{\overline{K}_\mathfrak{p}} \cap \mathcal{L}_{\overline{K}_\mathfrak{p}}) \to \pi_1(\mathcal{U}_{\overline{K}_\mathfrak{p}}) \xrightarrow{\varrho} G$$

has image G_g. Fix an embedding $\overline{K}_\mathfrak{p} \subseteq \mathbb{C}$. To prove the claim there is no harm in replacing $\overline{K}_\mathfrak{p}$ by the larger algebraically closed field $\mathbb{C}$. By Bertini's theorem, the homomorphism $\pi_1(\mathcal{U}_\mathbb{C} \cap L) \to \pi_1(\mathcal{U}_\mathbb{C}) \xrightarrow{\varrho} G$ has image G_g for a generic line $L \in \mathrm{Gr}_\mathbb{C}(1,n)(\mathbb{C})$. The above claim follows by (topologically) deforming $\mathcal{L}$ in $\mathrm{Gr}_\mathbb{C}(1,n)(\mathbb{C})$ to a generic line; note that small changes in $\mathcal{L}$ do not change the image of the representation since $\mathcal{L}$ intersects $\mathcal{Z}(\mathbb{C})$ only at smooth points and transversally at each of these points.

Choose a point $a_0 \in \mathcal{V}(\overline{\mathbb{F}}_\mathfrak{p})$ with a lift $a_1 \in \mathcal{V}(\mathcal{O}_\mathfrak{p}^{\mathrm{un}})$. Since $\mathcal{D}$ is finite étale over $\operatorname{Spec} \mathcal{O}_\mathfrak{p}^{\mathrm{un}}$, the Grothendieck specialization theorem implies that the natural homomorphisms

$$\pi_1(\mathcal{V}_{K_\mathfrak{p}^{\mathrm{un}}}, a_1) \to \pi_1(\mathcal{V}_{\mathcal{O}_\mathfrak{p}^{\mathrm{un}}}, a_1) \leftarrow \pi_1(\mathcal{V}_{\overline{\mathbb{F}}_\mathfrak{p}}, a_0)$$

induce an isomorphism between the prime to $p = \operatorname{char} \mathbb{F}_\mathfrak{p}$ quotients of $\pi_1(\mathcal{V}_{\overline{K}_\mathfrak{p}}, a_1)$ and $\pi_1(\mathcal{V}_{\overline{\mathbb{F}}_\mathfrak{p}}, a_0)$. In the present setting, an accessible proof of Grothendieck's theorem can be found in [Wew99, §4]. Therefore, the homomorphism

$$\pi_1(\mathcal{V}_{\overline{\mathbb{F}}_\mathfrak{p}}, a_0) \to \pi_1(\mathcal{V}_{\mathcal{O}_\mathfrak{p}^{\mathrm{un}}}, a_1) \to \pi_1(\mathcal{U}, a_1) \xrightarrow{\varrho} G \tag{6.4}$$

has the same image as $\pi_1(\mathcal{V}_{\overline{K}_\mathfrak{p}}, a_1) \to \pi_1(\mathcal{V}_{\mathcal{O}_\mathfrak{p}^{\mathrm{un}}}, a_1) \to \pi_1(\mathcal{U}, a_1) \xrightarrow{\varrho} G$ which is G_g by our claim (we have $p \nmid |G_g|$ since $\mathfrak{p} \nmid |G_g|$ by assumption).

We have thus proved that the image of $\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_\mathfrak{p}} \cap L) \to \pi_1(\mathcal{U}_{\overline{\mathbb{F}}_\mathfrak{p}}) \xrightarrow{\varrho} G$ is G_g for all lines $L \in (\mathrm{Gr}_{\mathcal{O}_K}(1,n) - \mathcal{W})(\overline{\mathbb{F}}_\mathfrak{p})$. Since $\mathfrak{p} \notin \mathscr{S}_1$, $(\mathrm{Gr}_{\mathcal{O}_K}(1,n) - \mathcal{W})_{\overline{\mathbb{F}}_\mathfrak{p}}$ is a non-empty open subvariety of $\mathrm{Gr}_{\mathcal{O}_K}(1,n)_{\overline{\mathbb{F}}_\mathfrak{p}}$. By Bertini's theorem, we deduce that $\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_\mathfrak{p}}) \xrightarrow{\varrho} G$ has image G_g. □

Let Σ be the set of non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ that split completely in F; it has positive density by the Chebotarev density theorem.

Lemma 6.6. *For any non-zero prime ideal $\mathfrak{p} \in \Sigma - \mathscr{S}$ of $\mathcal{O}_K$ satisfying $\mathfrak{p} \nmid |G_g|$, we have*

$$|\{u \in \mathbb{P}^n(\mathbb{F}_\mathfrak{p}) : u \notin \mathcal{U}(\mathbb{F}_\mathfrak{p}) \text{ or } \varrho(\mathrm{Frob}_u) \in C\}| \leq \delta N(\mathfrak{p})^n + O_U(|C|^{1/2}|G_g|N(\mathfrak{p})^{n-1/2}).$$

Proof. We can view $\mathbb{A}^n_{\mathcal{O}_K} = \operatorname{Spec} \mathcal{O}_K[x_1,\ldots,x_n]$ as an open subscheme of $\mathbb{P}^n_{\mathcal{O}_K}$ via the morphism $(a_1,\ldots,a_n) \mapsto [a_1,\ldots,a_n,1]$. There is a non-zero polynomial $f \in \mathcal{O}_K[x_1,\ldots,x_n]$ that is squarefree in $K[x_1,\ldots,x_n]$ such that $\mathcal{U}' := \operatorname{Spec}(\mathcal{O}_K[x_1,\ldots,x_n][f^{-1}])$ is an open $\mathcal{O}_K$-subscheme of $\mathcal{U}$. There is a finite set $\mathscr{S}_2$ of non-zero prime ideals $\mathcal{O}_K$ such that for all non-zero prime ideals $\mathfrak{p} \notin \mathscr{S}_2$ of $\mathcal{O}_K$:

- $\mathcal{U}'_{\mathbb{F}_\mathfrak{p}}$ is an open affine subvariety of $\mathbb{P}^n_{\mathbb{F}_\mathfrak{p}}$ of dimension n that is geometrically irreducible,
- $\mathcal{U}'_{\mathbb{F}_\mathfrak{p}}$ is isomorphic to the closed subscheme of $\mathbb{A}^{n+1}_{\mathbb{F}_\mathfrak{p}} = \operatorname{Spec} \mathbb{F}_\mathfrak{p}[x_1,\ldots,x_n,x_{n+1}]$ defined by the equation $\bar{f}(x_1,\ldots,x_n)\cdot x_{n+1} = 1$, where $\bar{f}$ is obtained from f by reducing its coefficients modulo $\mathfrak{p}$.

Note that f and $\mathscr{S}_2$ are choices that depends only on $U \subseteq \mathbb{P}^n_K$.

Now take any prime ideal $\mathfrak{p} \in \Sigma - \mathscr{S}$ satisfying $\mathfrak{p} \nmid |G_g|$. Let $\mathscr{S}_1$ be a set of prime ideals from Lemma 6.5. Since $\mathscr{S}_1$ and $\mathscr{S}_2$ depend only on $U \subseteq \mathbb{P}^n_K$, we may further assume that $\mathfrak{p} \notin \mathscr{S}_1 \cup \mathscr{S}_2$; the lemma holds for the finite number of excluded prime ideals by suitably increasing the implicit constant. Similarly, we may also assume that $\mathcal{U}'(\mathbb{F}_\mathfrak{p})$ is non-empty.

From ϱ, we obtain a continuous homomorphism $\varrho_\mathfrak{p} \colon \pi_1(\mathcal{U}_{\mathbb{F}_\mathfrak{p}}) \to G$. We have $\varrho_\mathfrak{p}(\mathcal{U}_{\overline{\mathbb{F}}_\mathfrak{p}}) = G_g$ by Lemma 6.5 and $\mathfrak{p} \nmid |G_g|$. Since $\mathcal{U}'_{\mathbb{F}_\mathfrak{p}}$ is a non-empty open subvariety of $\mathcal{U}_{\mathbb{F}_\mathfrak{p}}$, we can restrict $\varrho_\mathfrak{p}$ to obtain a homomorphism $\pi_1(\mathcal{U}'_{\overline{\mathbb{F}}_\mathfrak{p}}) \to G$ that satisfies $\varrho_\mathfrak{p}(\pi_1(\mathcal{U}'_{\overline{\mathbb{F}}_\mathfrak{p}})) = \varrho_\mathfrak{p}(\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_\mathfrak{p}})) = G_g$.

There is a unique G_g-coset κ of G such that $\varrho_\mathfrak{p}(\mathrm{Frob}_u) \in \kappa$ for all $u \in \mathcal{U}'(\mathbb{F}_\mathfrak{p})$. By Theorem 6.3, applied to the affine variety $\mathcal{U}'_{\mathbb{F}_\mathfrak{p}}$ and the representation $\rho_\mathfrak{p}$ (and using $\mathfrak{p} \nmid |G_g|$), we have

$$\begin{aligned}|\{u \in \mathcal{U}'(\mathbb{F}_\mathfrak{p}) : \varrho(\mathrm{Frob}_u) \in C\}| &= |\{u \in \mathcal{U}'(\mathbb{F}_\mathfrak{p}) : \varrho_\mathfrak{p}(\mathrm{Frob}_u) \in C \cap \kappa\}| \\ &= \frac{|C \cap \kappa|}{|G_g|}\,|\mathcal{U}'(\mathbb{F}_\mathfrak{p})| + O_U(|C|^{1/2}|G_g|N(\mathfrak{p})^{n-1/2});\end{aligned}$$

note that the implicit term depends only on $U \subseteq \mathbb{P}^n_K$ since $\mathcal{U}'_{\mathbb{F}_\mathfrak{p}}$ is isomorphic to a closed subscheme of $\mathbb{A}^{n+1}_{\mathbb{F}_\mathfrak{p}}$ defined by the polynomial equation $\bar{f}(x_1,\ldots,x_n)\cdot x_{n+1} = 1$, where f is a choice depending only on U.

Take any $u \in \mathcal{U}(\mathbb{F}_\mathfrak{p})$. Since $\mathfrak{p}$ splits completely in F, we have $(\varphi \circ \varrho_\mathfrak{p})(\mathrm{Frob}_\mathfrak{p}) \in \mathrm{Gal}(L/F)$. Therefore, $\kappa \subseteq \varphi^{-1}(\mathrm{Gal}(L/F))$. We thus have $|C \cap \kappa|/|G_g| \leq \delta$ by the definition of δ. Using this and $|\mathcal{U}'(\mathbb{F}_\mathfrak{p})| = N(\mathfrak{p})^n + O_U(N(\mathfrak{p})^{n-1/2})$, we find that

$$\begin{aligned}&|\{u \in \mathbb{P}^n(\mathbb{F}_\mathfrak{p}) : u \notin \mathcal{U}(\mathbb{F}_\mathfrak{p}) \text{ or } \varrho(\mathrm{Frob}_u) \in C\}| \\ &\leq |\{u \in \mathcal{U}'(\mathbb{F}_\mathfrak{p}) : \varrho(\mathrm{Frob}_u) \in C\}| + |\mathbb{P}^n(\mathbb{F}_\mathfrak{p}) - \mathcal{U}'(\mathbb{F}_\mathfrak{p})| \\ &\leq \delta N(\mathfrak{p})^n + O_U(|C|^{1/2}|G_g|N(\mathfrak{p})^{n-1/2}),\end{aligned}$$

where since $C \neq \emptyset$ we can absorb the various error terms. □

Define the set

$$B := \{u \in U(K) : \rho_u(\mathrm{Gal}_K) \subseteq C\}.$$

For each $\mathfrak{p} \in \Sigma - \mathscr{S}$, denote by $B_\mathfrak{p}$ the image of B under the reduction modulo $\mathfrak{p}$ map $U(K) \subseteq \mathbb{P}^n(K) \to \mathbb{P}^n(\mathbb{F}_\mathfrak{p})$. Let $\mathscr{S}'$ be the finite set of primes $\mathfrak{p} \in \Sigma$ that lie in $\mathscr{S}$ or divide $|G_g|$.

Take any $\mathfrak{p} \in \Sigma - \mathscr{S}'$ and $u \in B$. Denote by $u_\mathfrak{p} \in \mathbb{P}^n(\mathbb{F}_\mathfrak{p})$ the image of u modulo $\mathfrak{p}$. If $u_\mathfrak{p} \in \mathcal{U}(\mathbb{F}_\mathfrak{p})$, then $\rho_u(\mathrm{Frob}_\mathfrak{p}) = \varrho(\mathrm{Frob}_{u_\mathfrak{p}})$. Since $u \in B$, we deduce that $u_\mathfrak{p} \notin \mathcal{U}(\mathbb{F}_\mathfrak{p})$ or $\varrho(\mathrm{Frob}_{u_\mathfrak{p}}) \in C$. By Lemma 6.6, we deduce that

$$|B_{\mathfrak{p}}| \le \delta N(\mathfrak{p})^n + O_U(|C|^{1/2}|G_g|N(\mathfrak{p})^{n-1/2})$$

for all $\mathfrak{p} \in \Sigma - \mathscr{S}'$. Take any $x \ge 2$. By Proposition 6.4, we have

$$\begin{aligned} |\{u \in B : H(u) \le x\}| &\ll_{U,F} (1-\delta)^{-1} \cdot x^{(n+1/2)[K:\mathbb{Q}]} \log x + |\mathscr{S}'|^{4n+4} + ((1-\delta)^{-1}|C|^{1/2}|G_g|)^{4n+4} \\ &\ll_\delta x^{(n+1/2)[K:\mathbb{Q}]} \log x + |\mathscr{S}'|^{4n+4} + |C|^{2n+2} \cdot |G_g|^{4n+4} \\ &\ll_n x^{(n+1/2)[K:\mathbb{Q}]} \log x + |\mathscr{S}|^{4n+4} + |C|^{2n+2} \cdot |G_g|^{4n+4}, \end{aligned}$$

where the last inequality uses that $|\mathscr{S}'| = |\mathscr{S}| + O(\log |G_g|)$ and $C \neq \emptyset$.

7. Derangements

Let G be a linear algebraic group defined over a finite field $\mathbb{F}_\ell$ for which its neutral component G° is semisimple and adjoint. Let S be the commutator subgroup of $G^\circ(\mathbb{F}_\ell)$. Fix a group H satisfying

$$S \subseteq H \subseteq G(\mathbb{F}_\ell)$$

and fix a normal subgroup H_g of H. Define $H_0 := H \cap G^\circ(\mathbb{F}_\ell)$; it is a normal subgroup of H that contains S. Let r be the rank of G° and define $m = [G(\mathbb{F}_\ell) : G^\circ(\mathbb{F}_\ell)]$.

Proposition 7.1. *With notation as above, let M be a subgroup of H for which $M \not\supseteq S$ and for which the natural homomorphisms $M \to H/H_g$ and $M \to H/H_0$ are surjective. Define the subset*

$$C := \bigcup_{h \in H} hMh^{-1}$$

of H. Then there is a constant $0 \le \delta < 1$, depending only on r and m, satisfying

$$\frac{|C \cap \kappa|}{|H_g|} \le \delta + O_{r,m}(1/\ell) \tag{7.1}$$

for every H_g-coset κ in $H_0 \cdot H_g$.

We will prove Proposition 7.1 by repeated reducing to simpler cases. Proposition 7.1 will be used to prove a specialized version of Hilbert's irreducibility theorem (Theorem 8.3). The notation H_g is chosen because in our applications, H will be the image of an arithmetic fundamental group and H_g will be the image of its geometric subgroup.

7.1. A theorem of Fulman and Guralnick.

Consider a finite group H acting on a set Ω. An element $h \in H$ is called a derangement on Ω if it has no fixed points. For a non-empty subset $B \subseteq H$, let $\delta(B, \Omega)$ be the proportion of elements in B that are derangements on Ω.

The following is a slight variant of a result of Fulman and Guralnick.

Theorem 7.2 (Fulman–Guralnick)**.** *Let G be a connected, geometrically simple and adjoint linear algebraic group of rank r defined over a finite field $\mathbb{F}_q$. Let S be the commutator subgroup of $G(\mathbb{F}_q)$ and fix a group $S \subseteq H \subseteq G(\mathbb{F}_q)$. Fix a maximal subgroup M of H satisfying $M \not\supseteq S$ and define $\Omega = H/M$ with H acting by left multiplication. Then for every S-coset κ in H, we have*

$$\delta(\kappa, \Omega) \ge \delta + O_r(1/q)$$

with $0 < \delta \le 1$ a constant that depends only on r.

Proof. Since G is geometrically simple and adjoint group, by taking q sufficiently large in terms of r, we may assume that S is a non-abelian simple group and that H has socle S. Conjugation on S allows us to view $G(\mathbb{F}_q)$, and hence also H, as a subgroup of the automorphism group of S. Our theorem is then a consequence of Corollary 7.4 in [FG12] and the remark following it; note that since $H \subseteq G(\mathbb{F}_q)$, H lies in the group of inner-diagonal automorphisms of S. □

Remark 7.3. With notation as in Theorem 7.2, define the set $C := \bigcup_{h \in H} hMh^{-1}$. Left multiplication gives a transitive action of H on $\Omega = H/M$. Note that an element $x \in H$ fixes a coset $hM \in H/M$ if and only if $x \in hMh^{-1}$. So an element $x \in H$ is a derangement on Ω if and only if it does not lie in C. In particular, for any S-coset κ in H, we have $\delta(\kappa, \Omega) = 1 - |C \cap \kappa|/|S|$.

Similarly, we could reformulate Proposition 7.1 in terms of derangements.

7.2. **Proof of Proposition 7.1.** Since G° is a connected and adjoint, we have $G^\circ = \prod_{i=1}^n G_i$, where the G_i are connected, adjoint and simple groups defined over $\mathbb{F}_\ell$. We have $S = S_1 \times \cdots \times S_n$, where S_i is the commutator subgroup of $G_i(\mathbb{F}_\ell)$.

By excluding a finite number of primes ℓ that depend only on r and m, we may assume that all the groups S_i are non-abelian and simple and that $\ell > m$. Since S_i contains an element of order ℓ, we have $|S_i| \geq \ell > m \geq [H : H_0]$. Note that the proposition holds for the finite number of excluded primes by increasing the implicit constant.

Lemma 7.4. *The natural map $M \cap S \to S/(S \cap H_g)$ is surjective.*

Proof. We claim that S_i is not isomorphic to a composition factor of $M/(M \cap S)$ for any $1 \leq i \leq n$. Take any $1 \leq i \leq n$. To prove the claim it suffices to show that neither of the groups $M/(M \cap H_0)$ or $(M \cap H_0)/(M \cap S)$ have a composition factor isomorphic to S_i; note that H_0 is a normal subgroup of H that contains S. The group S_i is not a composition factor of $M/(M \cap H_0)$ since $[M : M \cap H_0] \leq [H : H_0] \leq m < |S_i|$. The group S_i is not a composition factor of $(M \cap H_0)/(M \cap S)$ since we have an injective homomorphism $(M \cap H_0)/(M \cap S) \hookrightarrow H_0/S$ and H_0/S is abelian. This proves the claim.

Let $B_1, \ldots, B_m$ be the composition factors of $S/(S \cap H_g) \cong (SH_g)/H_g$. Note that each B_j is isomorphic to some S_i.

Let $\varphi \colon M \to H/H_g$ be the quotient homomorphism. We have $\varphi(M \cap S) \subseteq (SH_g)/H_g$. The groups $B_1, \ldots, B_m$ occur, with multiplicity, as composition factors of $\varphi(M)$ since φ is surjective by our assumptions on M and $(SH_g)/H_g$ is normal in H/H_g. By the claim, the group $M/(M \cap S)$, and hence also $\varphi(M)/\varphi(M \cap S)$, has no composition factors isomorphic to any B_i. Therefore, the groups $B_1, \ldots, B_m$ occur, with multiplicity, as composition factors of $\varphi(M \cap S)$. In particular, $|\varphi(M \cap S)| \geq |B_1| \cdots |B_m| = |(SH_g)/H_g|$. Since $\varphi(M \cap S) \subseteq (SH_g)/H_g$, this implies that $\varphi(M \cap S) = (SH_g)/H_g$. The lemma follows by noting that $(SH_g)/H_g \cong S/(S \cap H_g)$. □

Define the subgroup $M_0 := M \cap H_0$ of H_0 and the subset

$$C_0 := \bigcup_{h \in H_0} hM_0h^{-1} \tag{7.2}$$

of H_0. We have $M \cap S = M_0 \cap S$ since S is a subgroup of H_0. Therefore, $M_0 \not\supseteq S$. The natural homomorphism $M_0 \cap S \to S/(S \cap H_g)$ is surjective by Lemma 7.4. This surjectivity and $M_0 \not\supseteq S$ implies that $S \cap H_g \neq 1$. The following lemma will be used to reduce to a setting where the group G is connected.

Lemma 7.5. *Let κ be any coset of H_g in $H_0 \cdot H_g$. Then there is a coset κ_0 of $S \cap H_g$ in H_0 such that*

$$\frac{|C \cap \kappa|}{|H_g|} \leq 1 - \frac{1}{e} + \frac{1}{e} \cdot \frac{|C_0 \cap \kappa_0|}{|S \cap H_g|}, \tag{7.3}$$

where $e := [H_g : S \cap H_g]$.

Proof. We have $\kappa \cap H_0 \neq \emptyset$ since κ is a H_g-coset in $H_0 \cdot H_g$. Therefore, there is a $S \cap H_g$-coset κ_0 of H_0 satisfying $\kappa_0 \subseteq \kappa$. Since κ is the disjoint union of e different $S \cap H_g$-cosets, one of which is κ_0, we have

$$|C \cap \kappa| \leq (e-1)|S \cap H_g| + |C \cap \kappa_0| = |H_g| - |S \cap H_g| + |C \cap \kappa_0|,$$

where the inequality uses the trivial upper bound for the $S \cap H_g$-cosets that are not κ_0. Dividing by $|H_g|$, we deduce that $|C \cap \kappa|/|H_g| \leq 1 - 1/e + 1/e \cdot |C \cap \kappa_0|/|S \cap H_g|$. So to prove (7.3), it suffices to show that $C \cap \kappa_0 = C_0 \cap \kappa_0$.

Since $\kappa_0 \subseteq H_0$ and $C_0 \subseteq H_0$, it thus suffices to show that $C \cap H_0 = C_0$. Using that $M \to H/H_0$ is surjective, we find that $C = \cup_{h \in H_0} hMh^{-1}$. Therefore, $C \cap H_0 = \cup_{h \in H_0} h(M \cap H_0)h^{-1} = C_0$ as desired. □

Proposition 7.6. *Take any subgroup M_1 of H_0 satisfying $M_1 \not\supseteq S$ for which $M_1 \cap S \to S/(S \cap H_g)$ is surjective. Define the subset $C_1 := \bigcup_{h \in H_0} hM_1h^{-1}$ of H_0. Then for any coset κ_0 of $S \cap H_g$ in H_0, we have*

$$\frac{|C_1 \cap \kappa_0|}{|S \cap H_g|} \leq \delta_0 + O_r(1/\ell)$$

with $0 \leq \delta_0 < 1$ depending only on r.

Suppose that Proposition 7.6 holds. Take any H_g-coset κ in $H_0 \cdot H_g$. By Lemma 7.5, there is a $(S \cap H_g)$-coset κ_0 in H_0 such that (7.3) holds. Proposition 7.6, with $M_1 = M_0$, implies that $|C_0 \cap \kappa_0|/|S \cap H_g| \leq \delta_0 + O_r(1/\ell)$ holds with a constant $0 \leq \delta_0 < 1$ depending only on r. From (7.3), we deduce that

$$\frac{|C \cap \kappa|}{|H_g|} \leq \delta + O_r(1/\ell)$$

with $\delta := 1 - 1/e + \delta_0/e = 1 + (-1+\delta_0)/e$. We have $0 \leq \delta < 1$ since $0 \leq \delta_0 < 1$. We have

$$e \leq [G(\mathbb{F}_\ell) : S] \leq m \cdot [G^\circ(\mathbb{F}_\ell) : S] \ll_r m.$$

So $\delta < 1$ depends only on r and m. This completes the proof of Proposition 7.1 assuming Proposition 7.6.

It thus remains to prove Proposition 7.6. Note that the only role that H_g plays in the proposition is through its subgroup $S \cap H_g$, so without loss generality assume that H_g is a normal subgroup of S. Take any subgroup $M_1 \subseteq H_0$ such that $M_1 \not\supseteq S$ and such that $M_1 \cap S \to S/(S \cap H_g) = S/H_g$ is surjective. We thus have $H_g \neq 1$. Define $C_1 := \bigcup_{h \in H_0} hM_1h^{-1}$. Since the proposition now only concerns subgroups of $G^\circ(\mathbb{F}_\ell)$, we may assume without loss of generality that G is connected and hence that $H = H_0$.

Lemma 7.7. *It suffices to prove Proposition 7.6 with the additional assumption that the projection homomorphism $M_1 \cap S \hookrightarrow S \to \prod_{j \in J} S_j$ is surjective for all proper subsets $J \subsetneq \{1, \ldots, n\}$.*

Proof. Since $M_1 \not\supseteq S$, there is a minimal (non-empty) subset $I \subseteq \{1, \ldots, n\}$ for which the projection $M_1 \cap S \to \prod_{i \in I} S_i$ is not surjective. Define the projection

$$\varphi \colon G(\mathbb{F}_\ell) \to \prod\nolimits_{i \in I} G_i(\mathbb{F}_\ell) = \tilde{G}(\mathbb{F}_\ell),$$

where $\tilde{G} := \prod_{i \in I} G_i$. Define the groups $\tilde{H} := \varphi(H)$, $\tilde{H}_g := \varphi(H_g)$ and $\tilde{M}_1 := \varphi(M_1)$. The group $\varphi(S)$ equals $\tilde{S} := \prod_{i \in I} S_i$. By our choice of I, we have $\tilde{M}_1 \not\supseteq \tilde{S}$. The natural homomorphism $M_1 \cap S \to S/H_g$ is surjective and hence so is $\tilde{M}_1 \cap \tilde{S} \to \tilde{S}/\tilde{H}_g$.

Take any coset κ_0 of $S \cap H_g = H_g$ in H. Define $\tilde{\kappa}_0 := \varphi(\kappa_0)$; it is a coset of $\tilde{H}_g$ in $\tilde{H}$. The map $\kappa_0 \to \tilde{\kappa}_0$, $x \mapsto \varphi(x)$ is b-to-1 with $b := |H_g|/|\tilde{H}_g|$. Therefore,

$$\frac{|C_1 \cap \kappa_0|}{|H_g|} \leq \frac{|\varphi(C_1) \cap \varphi(\kappa_0)| \cdot b}{|H_g|} = \frac{|\varphi(C_1) \cap \tilde{\kappa}_0| \cdot b}{|\tilde{H}_g| \cdot b} = \frac{|\tilde{C}_1 \cap \tilde{\kappa}_0|}{|\tilde{H}_g|}, \tag{7.4}$$

where $\tilde{C}_1 := \cup_{h \in \tilde{H}} h\tilde{M}_1h^{-1}$.

The inequality (7.4) shows that is suffices to prove Proposition 7.6 with (G, H, H_g, M_1) replaced by $(\tilde{G}, \tilde{H}, \tilde{H}_g, \tilde{M}_1)$; note that we have already verified the required properties and that the rank of $\tilde{G}$ is at most the rank of G. By the minimality of our choice of I, the projection $\tilde{M}_1 \cap \tilde{S} \to \prod_{j \in J} S_j$ is surjective for each proper subset $J \subsetneq I$. The lemma is now immediate. □

By Lemma 7.7, we may now assume that the projection $M_1 \cap S \to \prod_{j \in J} S_j$ is surjective for every proper subset $J \subsetneq \{1, \ldots, n\}$.

Lemma 7.8. *To prove Proposition 7.6, it suffices to assume that $n = 1$ or that $n = 2$ and there is a group isomorphism $f \colon S_1 \to S_2$ such that $M_1 \cap S = \{(s, f(s)) : s \in S_1\}$.*

Proof. Suppose that $n \geq 3$. Then the projection $M_1 \cap S \to S_i \times S_j$ is surjective for all distinct $i, j \in \{1, \ldots, n\}$. Since the groups S_i have no nontrivial abelian quotients, Lemma 5.2.2 of [Rib76] implies that $M_1 \cap S = S$. However, this is a contradiction since $M_1 \not\supseteq S$ by assumption. Therefore, $n \leq 2$.

Suppose that $n = 2$. The projection $M_1 \cap S \to S_i$ is surjective for $i \in \{1, 2\}$. Using that $M_1 \not\supseteq S$ and that the non-abelian groups S_i are simple, Goursat's lemma ([Rib76, Lemma 5.1.1]) implies that $M_1 \cap S = \{(s, f(s)) : s \in S_1\}$ for some group isomorphism $f \colon S_1 \to S_2$. □

By Lemma 7.8, we may assume that $n \leq 2$.

- First consider the case $n = 1$. Since H_g is a non-trivial normal subgroup of $S = S_1$ and S_1 is simple, we have $H_g = S$. Take any coset κ_0 of $S \cap H_g = S$ in H_0.

Since $n = 1$, the connected and adjoint group G is simple. There is an integer $e \geq 1$ and a connected, geometrically simple and adjoint linear algebraic group $\mathcal{G}$ defined over $\mathbb{F}_{\ell^e}$ such that G is isomorphic to the Weil restriction $\operatorname{Res}_{\mathbb{F}_{\ell^e}/\mathbb{F}_\ell}(\mathcal{G})$, cf. [KMRT98, Theorem 26.8]. Without loss of generality, we may assume that $G = \operatorname{Res}_{\mathbb{F}_{\ell^e}/\mathbb{F}_\ell}(\mathcal{G})$ and hence $G(\mathbb{F}_\ell) = \mathcal{G}(\mathbb{F}_{\ell^e})$. In particular, we can view S as the commutator subgroup of $\mathcal{G}(\mathbb{F}_{\ell^e})$, and H_0 and M_1 as subgroups of $\mathcal{G}(\mathbb{F}_{\ell^e})$.

Define $C_1 = \bigcup_{h \in H_0} hM_1h^{-1}$. Let H_1 be the subgroup of H_0 generated by M_1 and S; it is a normal subgroup of H_0. If $\kappa_0 \cap H_1 = \emptyset$, then $C_1 \cap \kappa_0 = \emptyset$ and the bound of Proposition 7.6 is trivial for the coset κ_0. So we may assume that κ_0 is an S-coset in H_1. Since $M_1 \to H_1/S$ is surjective, we can replace M_1 by a maximal subgroup of H_1; it still will satisfy the conditions of Proposition 7.6 and the set C_1 will only get larger.

Note that the rank of $\mathcal{G}$ is at most r. By Theorem 7.2 and Remark 7.3, applied with the algebraic group $\mathcal{G}/\mathbb{F}_{\ell^e}$, we have

$$\frac{|C_1 \cap \kappa_0|}{|S \cap H_g|} = \frac{|C_1 \cap \kappa_0|}{|S|} = 1 - \delta(\kappa_0, H_1/M_1) \leq 1 - \delta + O_r(1/\ell)$$

with a constant $0 < \delta \leq 1$ depending only on r. This completes the proof of Proposition 7.6 in the case $n = 1$.

• Finally, consider the case $n = 2$. Since $H_g \neq 1$ is a normal subgroup of S, H_g is equal to $\{1\} \times S_2$, $S_1 \times \{1\}$ or $S_1 \times S_2$. The following lemma allows us to make some further reductions.

Lemma 7.9. *It suffices to prove Proposition 7.6 in the case $n = 2$ with $G_1 = G_2$, $H_g = S_1 \times \{1\}$ and $M_1 = \{(g, g) : g \in G_1(\mathbb{F}_\ell)\}$.*

Proof. Using Lemma 7.8, we make an identification $S_1 = S_2$ of abstract groups so that $M_1 \cap S = \{(s, s) : s \in S_1\}$. Since the groups G_i are adjoint, we find that conjugation gives a faithful action of $G_i(\mathbb{F}_\ell)$ on $S_1 = S_2$. So we may identify $G_i(\mathbb{F}_\ell)$ with a subgroup of $\operatorname{Aut}(S_1)$.

Take any $(g_1, g_2) \in M_1$. Since $M_1 \cap S$ is a normal subgroup of M_1, we have $g_1sg_1^{-1} = g_2sg_2^{-1}$ for all $s \in S_1 = S_2$. Therefore, g_1 and g_2 are equal elements of $\operatorname{Aut}(S_1)$. Therefore, M_1 is a subgroup of $\{(g, g) : g \in G_1(\mathbb{F}_\ell)\}$. To prove the claim, there is no harm in increasing M_1 to be equal to $\{(g, g) : g \in G_1(\mathbb{F}_\ell)\}$; it also does not contain $S = S_1 \times S_2$. We may thus assume that $G_1 = G_2$.

We have already observed that $H_g \in \{\{1\} \times S_2, S_1 \times \{1\}, S_1 \times S_2\}$. By symmetry, we may assume that H_g is $S_1 \times \{1\}$ or $S_1 \times S_2$. From our explicit description of M_1, the homomorphism $M_1 \cap S \to S/(S_1 \times \{1\})$ is surjective. So we may assume that $H_g = S_1 \times \{1\}$; note that the $S_1 \times S_2$ cosets can be broken up into $S_1 \times \{1\}$-cosets. □

We finally assume that we are in the setting of Lemma 7.9. Take any coset κ_0 of $S_1 \times \{1\}$ in $G(\mathbb{F}_\ell)$. We have $\kappa_0 = \alpha S_1 \times \{\beta\}$ for some $\alpha, \beta \in G_1(\mathbb{F}_\ell)$. Using our explicit description of M_1, we have

$$C_1 \cap \kappa_0 \subseteq \{(g, \beta) : g \in G_1(\mathbb{F}_\ell) \text{ is conjugate to } \beta \text{ in } G_1(\mathbb{F}_\ell)\}.$$

Therefore, $|C_1 \cap \kappa_0| \leq |G_1(\mathbb{F}_\ell)|/|\mathcal{C}_\beta|$, where $\mathcal{C}_\beta$ is the centralizer of β in $G_1(\mathbb{F}_\ell)$. If β is semisimple in G_1, then it lies in a maximal torus (of rank r) and hence $|\mathcal{C}_\beta| \gg_r \ell^r$. If β is not semisimple, then it commutes with a non-trivial unipotent element of $G_1(\mathbb{F}_\ell)$ (whose order is a power of ℓ). Therefore,

$$|C_1 \cap \kappa_0| \leq |G_1(\mathbb{F}_\ell)|/|\mathcal{C}_\beta| \ll_r |G_1(\mathbb{F}_\ell)|/\ell \ll_r |S_1|/\ell,$$

where the last inequality uses that $[G_1(\mathbb{F}_\ell) : S_1]$ can be bounded in terms of r.

We deduce that $|C_1 \cap \kappa_0|/|H_g| = |C_1 \cap \kappa_0|/|S_1| \ll_r 1/\ell$. This completes our proof of Proposition 7.6.

8. Hilbert irreducibility

Fix an abelian scheme $A \to U$ of relative dimension $g \geq 1$, where U is a non-empty open subscheme of $\mathbb{P}^n_K$ with $n \geq 1$ and K a number field. Take any constant b_A as in Theorem 3.1. For each prime $\ell \geq b_A$, we have $\bar{\rho}_{A,\ell}(\pi_1(U)) \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$. For a prime $\ell \geq b_A$ and real x, define the set

$$B_\ell(x) := \{u \in U(K) : H(u) \leq x, \bar{\rho}_{A_u,\ell}(\operatorname{Gal}_K) \not\supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'\}.$$

In this section, we will prove the following.

Theorem 8.1. *For each prime $\ell \geq b_A$ and $x \geq 2$, we have*

$$|B_\ell(x)| \ll_A \ (\ell+1)^{3g(2g+1)/2} \cdot x^{[K:\mathbb{Q}](n+1/2)} \log x + (\ell+1)^{(6n+15/2)g(2g+1)}.$$

Remark 8.2. In our application, we will use Theorem 8.1 when $\ell \leq c(\log x)^\gamma$ for some positive constants c and γ depending only on A. For such ℓ, we obtain a bound $|B_\ell(x)| \ll_A x^{[K:\mathbb{Q}](n+1/2)}(\log x)^{\gamma'}$ for a constant γ'.

8.1. **A special version of Hilbert irreducibility.** We now state a specialized version of Hilbert's irreducibility theorem. To ease notation and make it suitable for future use, we keep it separate from our abelian variety application.

Let K be a number field. Fix a non-empty open subvariety U of $\mathbb{P}^n_K$ with $n \geq 1$ and a continuous representation

$$\rho\colon \pi_1(U) \to G(\mathbb{F}_\ell),$$

where G is a linear algebraic group defined over $\mathbb{F}_\ell$ for which the neutral component G° is reductive. Let S be the commutator subgroup of $G^\circ(\mathbb{F}_\ell)$. Assume further that ρ satisfies $\rho(\pi_1(U)) \supseteq S$.

For each point $u \in U(K)$, we obtain a homomorphism $\rho_u\colon \operatorname{Gal}_K \to G(\mathbb{F}_\ell)$ by specializing ρ at u; it is uniquely defined up to conjugation by an element of $G(\mathbb{F}_\ell)$. Hilbert's irreducibility theorem implies that $\rho_u(\operatorname{Gal}_K) \supseteq S$ for all $u \in U(K)$ away from a set of density 0; Theorem 8.3 below gives a quantitative version.

We first define some quantities for which the implicit constant of our theorem depends on. Let $\mathcal{U}$ be the open subscheme of $\mathbb{P}^n_{\mathcal{O}_K}$ that is the complement of the Zariski closure of $\mathbb{P}^n_K - U$ in $\mathbb{P}^n_{\mathcal{O}_K}$. The $\mathcal{O}_K$-scheme $\mathcal{U}$ has generic fiber U. Fix a finite set $\mathscr{S}$ of non-zero prime ideals of $\mathcal{O}_K$ such that ρ arises from a homomorphism $\pi_1(\mathcal{U}_\mathcal{O}) \to G(\mathbb{F}_\ell)$, where $\mathcal{O}$ is the ring of $\mathscr{S}_\ell$-integers in K and $\mathscr{S}_\ell$ is the set of non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ that lie in $\mathscr{S}$ or divide ℓ.

Let $\alpha\colon \pi_1(U) \to G(\mathbb{F}_\ell)/G^\circ(\mathbb{F}_\ell)$ be the homomorphism obtained by composing ρ with the obvious quotient map. Let $F \subseteq \overline{K}$ be the minimal extension of K for which $\alpha(\pi_1(U_F)) = \alpha(\pi_1(U_{\overline{K}}))$.

Let G^{ad} be the quotient of G by the center of G°. The group $(G^{\mathrm{ad}})^\circ$ is an adjoint algebraic group over $\mathbb{F}_\ell$. Denote the rank and dimension of $(G^{\mathrm{ad}})^\circ$ by r and d, respectively. Define the index $m = [G(\mathbb{F}_\ell) : G^\circ(\mathbb{F}_\ell)]$.

Theorem 8.3. *Fix notation and assumptions as above and take any $x \geq 2$. There is a constant c, depending only on r and m, such that if $\ell \geq c$, then*

$$\begin{aligned}&|\{u \in U(K) : H(u) \leq x,\, \rho_u(\operatorname{Gal}_K) \not\supseteq S\}|\\ &\ll_{U,F,|\mathscr{S}|,r,m} \ (\ell+1)^{3d/2} \cdot x^{[K:\mathbb{Q}](n+1/2)} \log x + (\ell+1)^{(6n+15/2)d}.\end{aligned}$$

8.2. **Proof of Theorem 8.3.** We assume that $\ell \geq c$, where c is a constant that depends only on r and m; we will allow ourselves to appropriately increase c throughout the proof while maintaining the dependencies.

Let G^{ad} be the quotient of G by the center of G° and let $\pi\colon G \to G^{\mathrm{ad}}$ be the quotient map. The morphism π gives rise to homomorphisms $G(\mathbb{F}_\ell) \to G^{\mathrm{ad}}(\mathbb{F}_\ell)$ and $S \to S^{\mathrm{ad}}$, where S^{ad} is the commutator subgroup of $(G^{\mathrm{ad}})^\circ(\mathbb{F}_\ell)$. Let

$$\rho^{\mathrm{ad}}\colon \pi_1(U) \to G^{\mathrm{ad}}(\mathbb{F}_\ell),$$

be the representation obtained by composing ρ with π.

Before proceeding, the following lemma gives an alternate description of S and S^{ad} for all sufficiently large ℓ.

Lemma 8.4. *Let G be a connected reductive group over $\mathbb{F}_\ell$. Let H be the derived subgroup of G and let $\varphi\colon H^{\mathrm{sc}} \to H$ be its simply connected cover. Then $G(\mathbb{F}_\ell)'$ is perfect and equal to $\varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell))$ for all $\ell \gg_r 1$, where r is the rank of H.*

Proof. Since H^{sc} is simply connected, it is a product of simply connected and simple groups $H_1, \ldots, H_m$. We know that each group $H_i(\mathbb{F}_\ell)$ is perfect for $\ell \gg 1$ (moreover, the quotient by its center is a non-abelian simple group). In particular, we may assume that the group $H^{\mathrm{sc}}(\mathbb{F}_\ell)$ is perfect. Therefore, $\varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell)) = \varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell)') \subseteq H(\mathbb{F}_\ell)'$. The group $\varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell))$ is perfect since $H^{\mathrm{sc}}(\mathbb{F}_\ell)$ is perfect.

Let Y be the kernel of φ; it is commutative since the isogeny φ is central. The degree of φ, and hence also the cardinality of $Y(\overline{\mathbb{F}}_\ell)$, can be bounded in terms of r. Galois cohomology gives an injective homomorphism $H(\mathbb{F}_\ell)/\varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell)) \hookrightarrow H^1(\mathrm{Gal}_{\mathbb{F}_\ell}, Y(\overline{\mathbb{F}}_\ell))$ of groups, so $H(\mathbb{F}_\ell)/\varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell))$ is abelian and its cardinality can be bounded in terms of r. In particular, we have $\varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell)) \supseteq H(\mathbb{F}_\ell)'$.

We thus have $\varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell)) = H(\mathbb{F}_\ell)'$ since we have shown both inclusions and we have seen that $\varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell))$ is perfect. We clearly have $H(\mathbb{F}_\ell)' \subseteq G(\mathbb{F}_\ell)'$ so it suffices to show that $G(\mathbb{F}_\ell)' \subseteq \varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell))$ for all $\ell \gg_r 1$.

Let $G(\mathbb{F}_\ell)^+$ be the (normal) subgroup of $G(\mathbb{F}_\ell)$ generated by its elements of order ℓ. We have $G(\mathbb{F}_\ell)^+ \subseteq H(\mathbb{F}_\ell)$ since G/H is a torus over $\mathbb{F}_\ell$ and hence has no $\mathbb{F}_\ell$-points of order ℓ. We have already shown that $[H(\mathbb{F}_\ell) : \varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell))] \leq C_r$, where C_r is a constant depending only on r. By taking $\ell > C_r$, we find that $G(\mathbb{F}_\ell)^+ \subseteq \varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell))$. The group $G(\mathbb{F}_\ell)/G(\mathbb{F}_\ell)^+$ is abelian by [Pet16, Proposition 1.1] and hence $G(\mathbb{F}_\ell)' \subseteq G(\mathbb{F}_\ell)^+$. Therefore, $G(\mathbb{F}_\ell)' \subseteq G(\mathbb{F}_\ell)^+ \subseteq \varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell))$. □

Lemma 8.5. *If $\ell \gg_r 1$ and M is a subgroup of $G(\mathbb{F}_\ell)$, then S is a subgroup of M if and only if S^{ad} is a subgroup $\pi(M)$.*

Proof. Let H be the derived subgroup of G°; it has rank r Let $\varphi\colon H^{\mathrm{sc}} \to H$ be the simply connected cover of H. Define $\varphi^{\mathrm{ad}} := \pi \circ \varphi\colon H^{\mathrm{sc}} \to (G^{\mathrm{ad}})^\circ$; it is the simply connected cover of $(G^{\mathrm{ad}})^\circ$. By assuming ℓ is sufficiently large in terms of r, Lemma 8.4 implies that $S = \varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell))$, $S^{\mathrm{ad}} = \varphi^{\mathrm{ad}}(H^{\mathrm{sc}}(\mathbb{F}_\ell))$, and that S and S^{ad} are perfect. If M is a subgroup of $G(\mathbb{F}_\ell)$ containing S, then

$$\pi(M) \supseteq \pi(S) = \pi(\varphi(H^{\mathrm{sc}}(\mathbb{F}_\ell))) = \varphi^{\mathrm{ad}}(H^{\mathrm{sc}}(\mathbb{F}_\ell)) = S^{\mathrm{ad}}.$$

Now let M be a subgroup of $G(\mathbb{F}_\ell)$ that satisfies $\pi(M) \supseteq S^{\mathrm{ad}}$. We need to show that $M \supseteq S$. We have $\pi^{-1}((G^{\mathrm{ad}})^\circ) \subseteq G^\circ$, so there is no harm in replacing M by the smaller group $M \cap G^\circ(\mathbb{F}_\ell)$. In particular, we may assume that $M \subseteq G^\circ(\mathbb{F}_\ell)$. We have $\pi(M') = \pi(M)' \supseteq (S^{\mathrm{ad}})' = S^{\mathrm{ad}}$. So after replacing M by the smaller group M', we may further assume that $M \subseteq S$. We thus have $\pi(M) = S^{\mathrm{ad}}$ since $\pi(S) = S^{\mathrm{ad}}$. The homomorphism $S \xrightarrow{\pi} S^{\mathrm{ad}}$ is surjective and its kernel Z lies in the center of $G(\mathbb{F}_\ell)$ since π is a central isogeny, so we have $S = M \cdot Z$. Taking commutator subgroups, we find that $S = S' = (M \cdot Z)' = M'$. Since $M' \subseteq M \subseteq S$, we deduce that $M = S$. □

Take any $u \in U(K)$. Specializing ρ^{ad} at u gives a representation $\rho_u^{\mathrm{ad}}\colon \mathrm{Gal}_K \to G^{\mathrm{ad}}(\mathbb{F}_\ell)$. Up to an inner automorphism, ρ_u^{ad} agrees with $\pi \circ \rho_u$. By suitably increasing the constant c, Lemma 8.5 implies that $\rho_u(\mathrm{Gal}_K) \supseteq S$ if and only $\rho_u^{\mathrm{ad}}(\mathrm{Gal}_K) \supseteq S^{\mathrm{ad}}$. So to prove the theorem, we need to bound the cardinality of the set

$$\{u \in U(K) : H(u) \leq x,\, \rho_u^{\mathrm{ad}}(\mathrm{Gal}_K) \not\supseteq S^{\mathrm{ad}}\}.$$

We now show that the assumptions of Theorem 8.3 hold for ρ^{ad} and relate its basic invariants to those of ρ. Lemma 8.5 and the assumption $\rho(\pi_1(U)) \supseteq S$ implies that $\rho^{\mathrm{ad}}(\pi_1(U)) \supseteq S^{\mathrm{ad}}$. By our assumption on ρ, the representation ρ^{ad} arises from the homomorphism $\pi_1(\mathcal{U}_{\mathcal{O}}) \to G(\mathbb{F}_\ell) \xrightarrow{\pi} G^{\mathrm{ad}}(\mathbb{F}_\ell)$, where $\mathcal{O}$ is the ring of $\mathscr{S}_\ell$-integers in K. The quantities r and d associated to ρ and ρ^{ad} are the same.

There is no harm in replacing G by the algebraic subgroup generated by G° and $\rho(\pi_1(U))$. In particular, we may assume that G is generated by G° and $G(\mathbb{F}_\ell)$. From this we find that the natural map $G(\mathbb{F}_\ell)/G^\circ(\mathbb{F}_\ell) \to G^{\mathrm{ad}}(\mathbb{F}_\ell)/(G^{\mathrm{ad}})^\circ(\mathbb{F}_\ell)$ is an isomorphism. Therefore, α, F and m are the same for ρ and ρ^{ad}.

It is now clear that proving Theorem 8.3 for ρ^{ad} will give the desired bound for ρ.

Without loss of generality, we may now assume that the group G° is adjoint. Define the subgroups

$$H := \rho(\pi_1(U)), \quad H_g := \rho(\pi_1(U_{\overline{K}})) \quad \text{and} \quad H_0 := H \cap G^\circ(\mathbb{F}_\ell)$$

of $G(\mathbb{F}_\ell)$. Let $\mathcal{M}$ be the set of subgroups M of H for which $M \not\supseteq S$ and for which the quotient maps $M \to H/H_g$ and $M \to H/H_0$ are surjective.

Lemma 8.6. *Take any $x \geq 2$. There is a constant c, depending only on r and m, such that if $\ell \geq c$, then*

$$|\{u \in U(K) : \rho_u(\mathrm{Gal}_K) \in \mathcal{M}\}| \ll_{U,F,|\mathscr{S}|,r,m} (\ell+1)^{3d/2} \cdot x^{[K:\mathbb{Q}](n+1/2)} \log x + (\ell+1)^{(6n+15/2)d}.$$

Proof. Let L be the minimal extension of K in $\overline{K}$ for which H_g is the image of $\pi_1(U_L)$ under ρ. We have a natural short exact sequence

$$1 \to H_g \to H \xrightarrow{\varphi} \mathrm{Gal}(L/K) \to 1.$$

Observe that F is the subfield of L that satisfies $\varphi^{-1}(\mathrm{Gal}(L/F)) = \rho(\pi_1(U_F)) = H_0 \cdot H_g$.

Fix $x \geq 2$. Let $\widetilde{\mathcal{M}}$ be the set of maximal elements of $\mathcal{M}$ with respect to inclusion. Take any group $M \in \widetilde{\mathcal{M}}$ and define the subset $C := \bigcup_{h \in H} hMh^{-1}$ of H. By appropriately increasing the constant c, Proposition 7.1 says that there is a constant $0 \leq \delta < 1$, depending only on r and m, such that $|C \cap \kappa|/|H_g| \leq \delta$ holds for every coset κ of H_g in $H_0 \cdot H_g$. By Theorem 6.1, we have

$$|\{u \in U(K) : H(u) \leq x,\ \rho_u(\mathrm{Gal}_K) \subseteq C\}| \ll_{U,F,\delta} x^{(n+1/2)[K:\mathbb{Q}]} \log x + |\mathscr{S}_\ell|^{4n+4} + |C|^{2n+2} \cdot |H_g|^{4n+4}.$$

Since $|\mathscr{S}_\ell| \leq |\mathscr{S}| + [K : \mathbb{Q}]$ and δ depends only on r and m, we deduce that

$$\begin{aligned}&|\{u \in U(K) : H(u) \leq x,\ \rho_u(\mathrm{Gal}_K) \text{ is conjugate in } H \text{ to a subgroup of } M\}| \\ &\ll_{U,F,r,m} x^{(n+1/2)[K:\mathbb{Q}]} \log x + |\mathscr{S}|^{4n+4} + |G(\mathbb{F}_\ell)|^{6n+6}.\end{aligned}$$

By summing over all $M \in \widetilde{\mathcal{M}}$ and using that the implicit constant depends on m, we have

$$|\{u \in U(K) : \rho_u(\mathrm{Gal}_K) \in \mathcal{M}\}| \ll_{U,F,r,m} |\widetilde{\mathcal{M}}| \cdot \big(x^{(n+1/2)[K:\mathbb{Q}]} \log x + |\mathscr{S}|^{4n+4} + |G^\circ(\mathbb{F}_\ell)|^{6n+6}\big).$$

We now bound $|\widetilde{\mathcal{M}}|$. Take any $M \in \widetilde{\mathcal{M}}$ and define the subgroup $\widetilde{H} := M \cdot S$ of $G(\mathbb{F}_\ell)$. Observe that M is a maximal subgroup of $\widetilde{H}$ (if not, then it would give rise to a larger group in the set $\mathcal{M}$). By [LPS07], the group $\widetilde{H}$ has at most $O(|\widetilde{H}|^{3/2})$ maximal subgroups, where the constant is absolute. Therefore,

$$|\widetilde{\mathcal{M}}| \ll |G(\mathbb{F}_\ell)|^{3/2} \cdot |\{\widetilde{H} : \widetilde{H} \text{ subgroup of } G(\mathbb{F}_\ell) \text{ containing } S\}|.$$

We obtain $|\widetilde{\mathcal{M}}| \ll_{r,m} |G(\mathbb{F}_\ell)|^{3/2} \leq m \cdot |G^\circ(\mathbb{F}_\ell)|^{3/2}$ by using that the order of the quotient group $G(\mathbb{F}_\ell)/S$ can be bounded in terms of r and m. Therefore,

$$|\{u \in U(K) : \rho_u(\mathrm{Gal}_K) \in \mathcal{M}\}| \ll_{U,F,r,m} |G^\circ(\mathbb{F}_\ell)|^{3/2} \big(x^{(n+1/2)[K:\mathbb{Q}]} \log x + |\mathscr{S}|^{4n+4} + |G^\circ(\mathbb{F}_\ell)|^{6n+6}\big).$$

The bound in the lemma follows by noting that $|G^\circ(\mathbb{F}_\ell)| \leq (\ell+1)^d$, cf. [Nor87, Lemma 3.5]. □

Let $\beta\colon \pi_1(U) \to H/H_0$ be the surjective representation obtained by composing ρ with the obvious quotient map. As usual, we have a specialization $\beta_u\colon \mathrm{Gal}_k \to H/H_0$ for each $u \in U(k)$.

Lemma 8.7. *We have*

$$|\{u \in U(K) : H(u) \leq x,\ \beta_u(\mathrm{Gal}_k) \neq H/H_0\}| \ll_{U,F,|\mathscr{S}|,m} x^{[k:\mathbb{Q}](n+1/2)} \log x + |\mathscr{S}|^{4n+4}.$$

Proof. To ease notation, define $Y := H/H_0 = \beta(\pi_1(U))$ and its normal subgroup $Y_g := \beta(\pi_1(U_{\overline{K}}))$. The field F is the smallest extension of K in $\overline{K}$ for which $\beta(\pi_1(U_F)) = Y_g$. The homomorphism β arises from a continuous homomorphism $\pi_1(\mathcal{U}_{\mathcal{O}}) \to Y$, where $\mathcal{O}$ is the ring of $\mathscr{S}_\ell$-integers (since ρ arises from a representation of $\pi_1(\mathcal{U}_{\mathcal{O}})$). By Corollary 6.2, we have

$$|\{u \in U(K) : H(u) \leq x,\ \beta_u(\mathrm{Gal}_K) \neq Y\}| \ll_{U,F,|Y|} x^{[K:\mathbb{Q}](n+1/2)} \log x + |\mathscr{S}_\ell|^{4n+4}.$$

The lemma follows by noting that $|\mathscr{S}_\ell| \leq |\mathscr{S}| + [K : \mathbb{Q}]$ and $|Y| \leq m$. □

Take any $u \in U(K)$ for which S is *not* a subgroup of $\rho_u(\mathrm{Gal}_K)$. The natural map $\rho_u(\mathrm{Gal}_K) \to H/H_g$ is always surjective. If $\beta_u(\mathrm{Gal}_K) = H/H_0$ (equivalently, if the natural map $\rho_u(\mathrm{Gal}_K) \to H/H_0$ is surjective), then we must have $\rho_u(\mathrm{Gal}_K) \in \mathcal{M}$. Therefore, $|\{u \in U(K) : H(u) \leq x,\ \rho_u(\mathrm{Gal}_K) \not\supseteq S\}|$ is less than or equal to

$$|\{u \in U(K) : \beta_u(\mathrm{Gal}_K) \neq H/H_0\}| + |\{u \in U(K) : \rho_u(\mathrm{Gal}_K) \in \mathcal{M}\}|.$$

The theorem is now a direct consequence of Lemmas 8.6 and 8.7.

8.3. **Proof of Theorem 8.1.** Take any prime $\ell \geq b_A$. Corollary 6.2 with our assumption $\bar{\rho}_{A,\ell}(\pi_1(U)) \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ implies that $|B_\ell(x)| \ll_{A,\ell} x^{[K:\mathbb{Q}](n+1/2)} \log x$, where the implicit constant depends on ℓ. So during our proof we may exclude a finite number of primes ℓ.

Define the linear algebraic group $G := (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ over $\mathbb{F}_\ell$. By Theorem 3.1(i), $G^\circ = (\mathcal{G}^\circ_{A,\ell})_{\mathbb{F}_\ell}$ is reductive with derived subgroup $(\mathcal{S}_{A,\ell})_{\mathbb{F}_\ell}$. The rank of G° is bounded in terms of g since it is isomorphic to an algebraic subgroup of $\mathrm{GL}_{2g,\mathbb{F}_\ell}$.

Let S be the commutator subgroup of $G^\circ(\mathbb{F}_\ell)$. By first excluding a finite number of primes, Lemma 8.4 implies that $S = G^\circ(\mathbb{F}_\ell)'$ equals $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$. We have a representation

$$\rho := \bar{\rho}_{A,\ell} \colon \pi_1(U) \to G(\mathbb{F}_\ell).$$

For each $u \in U(K)$, specializing ρ at u gives a representation $\rho_u \colon \mathrm{Gal}_K \to G(\mathbb{F}_\ell)$ that is uniquely defined up to an inner automorphism of $G(\mathbb{F}_\ell)$ and agrees with $\bar{\rho}_{A_u,\ell}$. In particular, we have

$$B_\ell(x) = \{u \in U(K) : H(u) \leq x,\, \rho_u(\mathrm{Gal}_K) \not\supseteq S\}.$$

We are thus in the setting of §8.1 and hence we can define $\mathcal{U}$, r, d, m and F as in that section.

Lemma 8.8. *There is a finite set $\mathscr{S}$ of non-zero prime ideals of $\mathcal{O}_K$, not depending on ℓ, such that $\bar{\rho}_{A,\ell}$ arises from a homomorphism $\pi_1(\mathcal{U}_\mathcal{O}) \to G(\mathbb{F}_\ell)$, where $\mathscr{S}_\ell$ is the set of prime ideals of $\mathcal{O}_K$ that lies in $\mathscr{S}$ or divides ℓ and $\mathcal{O}$ is the ring of $\mathscr{S}_\ell$-integers in K.*

Proof. We first "spread out" A. There is an abelian scheme $\mathcal{A}' \to \mathcal{U}_{\mathcal{O}'}$, where $\mathcal{O}'$ is the ring of $\mathscr{S}$-integers in K for some finite set $\mathscr{S}$ of nonzero prime ideals of $\mathcal{O}_K$ such that the fiber over $(\mathcal{U}_{\mathcal{O}'})_K = U$ is the abelian scheme $A \to U$.

Let $\mathcal{O}$ be the ring of $\mathscr{S}_\ell$-integers in K, where $\mathscr{S}_\ell$ is the set of prime ideals of $\mathcal{O}_K$ that lie in $\mathscr{S}$ or divide ℓ. Let $\mathcal{A}$ be the abelian scheme over $\mathcal{U}_\mathcal{O}$ obtained from $\mathcal{A}'$ by base change. The ℓ-torsion subscheme $\mathcal{A}[\ell]$ of $\mathcal{A}$ can be viewed as locally constant sheaf of $\mathbb{Z}/\ell\mathbb{Z}$-modules on $\mathcal{U}_\mathcal{O}$ that is free of rank $2g$. The fiber of $\mathcal{A}[\ell]$ over $U = (\mathcal{U}_\mathcal{O})_K$ is $A[\ell]$. Since $\rho = \bar{\rho}_{A,\ell}$ is the representation associated to $A[\ell]$, we find that ρ arises via base change from a representation of $\pi_1(\mathcal{U}_\mathcal{O})$. □

Let $\mathscr{S}$ be a set of prime ideals as in Lemma 8.8. We may assume that $\mathscr{S}$ is chosen so that $|\mathscr{S}|$ is minimal and hence $|\mathscr{S}| \ll_A 1$.

Lemma 8.9. *As the prime $\ell \geq b_A$ varies, there are only finitely many possibilities for F, r and m.*

Proof. Let $\alpha \colon \pi_1(U) \to G(\mathbb{F}_\ell)/G^\circ(\mathbb{F}_\ell)$ be the homomorphism obtained by composing ρ with the obvious quotient map. The field $F \subseteq \overline{K}$ is the minimal extension of K for which $\alpha(\pi_1(U_F)) = \alpha(\pi_1(U_{\overline{K}}))$.

Using that $G_{A,\ell}$ is the Zariski closure of a subset of $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$, we find that the natural map $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)/\mathcal{G}^\circ_{A,\ell}(\mathbb{Z}_\ell) \to G_{A,\ell}(\mathbb{Q}_\ell)/G^\circ_{A,\ell}(\mathbb{Q}_\ell)$ is an isomorphism. Using Hensel's lemma, we find that the reduction module ℓ homomorphism $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)/\mathcal{G}^\circ_{A,\ell}(\mathbb{Z}_\ell) \to G(\mathbb{F}_\ell)/G^\circ(\mathbb{F}_\ell)$ is surjective. Therefore, α can be obtained by composing the homomorphism $\gamma_{A,\ell}$ of §2.2 with a surjective homomorphism $G_{A,\ell}(\mathbb{Q}_\ell)/G^\circ_{A,\ell}(\mathbb{Q}_\ell) \to G(\mathbb{F}_\ell)/G^\circ(\mathbb{F}_\ell)$. In particular, m is at most $[G_{A,\ell}(\mathbb{Q}_\ell) : G^\circ_{A,\ell}(\mathbb{Q}_\ell)]$ which is independent of ℓ by Lemma 2.4(i). The field F is contained in the minimal extension $F' \subseteq \overline{K}$ of K for which $\gamma_{A,\ell}(\pi_1(U_{F'})) = \gamma_{A,\ell}(\pi_1(U_{\overline{K}}))$. By Lemma 2.4(i), F' is independent of ℓ and hence there are only finitely many possibilities for F. We can bound r in terms of the rank of G° which we have already noted can be bounded in terms of g. □

Take any $x \geq 2$. After first excluding a finite number of primes ℓ, Theorem 8.3 implies that

$$\begin{aligned} |B_\ell(x)| &= |\{u \in U(K) : H(u) \leq x,\, \rho_u(\mathrm{Gal}_K) \not\supseteq S\}| \\ &\ll_{U,F,|\mathscr{S}|,r,m} \ (\ell+1)^{3d/2} \cdot x^{[K:\mathbb{Q}](n+1/2)} \log x + (\ell+1)^{(6n+15/2)d}. \end{aligned}$$

By Lemma 8.9 and $|\mathscr{S}| \ll_A 1$, we have

$$|B_\ell(x)| \ll_A \ (\ell+1)^{3d/2} \cdot x^{[K:\mathbb{Q}](n+1/2)} \log x + (\ell+1)^{(6n+15/2)d}.$$

It remains to bound d. By choosing a polarization of A and combining with the Weil pairing on the ℓ-torsion of A, we find that G is isomorphic to an algebraic subgroup of $\mathrm{GSp}_{2g,\mathbb{F}_\ell}$ by taking ℓ sufficiently large. Since d is equal to the dimension of the derived subgroup of G° it is at most $\dim \mathrm{Sp}_{2g,\mathbb{F}_\ell} = g(2g+1)$ and hence

$$|B_\ell(x)| \ll_A \ (\ell+1)^{3g(2g+1)/2} \cdot x^{[K:\mathbb{Q}](n+1/2)} \log x + (\ell+1)^{(6n+15/2)g(2g+1)}.$$

9. Proof of Theorem 1.1

Take any constant b_A as in Theorem 3.1 and define the set

$$B := \{u \in U(K) : \bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \not\supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)' \text{ for some prime } \ell \geq b_A\}.$$

To prove the theorem, it suffices by Proposition 5.1 to show that B has density 0.

Take any real number $x \geq 2$. We now define some finite sets that we will use to study B. Let r be the common rank of the groups $G^\circ_{A,\ell}$, cf. Proposition 2.5(ii). Fix a $b > 0$ for which $\mathcal{O}_K$ has a prime ideal of norm at most $b \log 2$.

- Let $B(x)$ be the set of $u \in B$ for which $H(u) \leq x$.
- For a prime ℓ, let $B_\ell(x)$ be the set of $u \in U(K)$ with $H(u) \leq x$ satisfying $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \not\supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$.
- Let $R(x)$ be the set of $u \in U(K)$ with $H(u) \leq x$ such that $G_{A_u,\ell} \neq G_{A,\ell}$ for some prime ℓ.
- Let $T(x)$ be the set of $u \in U(K)$ with $H(u) \leq x$ such that for any non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ satisfying $N(\mathfrak{p}) \leq b \log x$, the abelian variety A_u has bad reduction at $\mathfrak{p}$ or the roots of the polynomial $P_{A_u,\mathfrak{p}}$ in $\mathbb{C}^\times$ generate a group that is not isomorphic to $\mathbb{Z}^r$.

Lemma 9.1. *Take any $u \in U(K)$ with $H(u) \leq x$ satisfying $u \notin R(x) \cup T(x)$. There are positive constants γ and c, with γ depending only on g and c depending only on K and g, such that if $\ell \geq c(\max\{[K:\mathbb{Q}], h(A_u), \log x\})^\gamma$, then $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$.*

Proof. Since $u \notin T(x)$, there is a non-zero prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$ satisfying $N(\mathfrak{q}) \leq b \log x$ for which A_u has good reduction at $\mathfrak{q}$ and for which the subgroup $\Phi_{A_u,\mathfrak{q}}$ of $\mathbb{C}^\times$ generated by the roots of $P_{A_u,\mathfrak{q}}$ is isomorphic to $\mathbb{Z}^r$. This uses our choice of b and $x \geq 2$. By Theorem 3.3 and Theorem 3.1(ii), we have $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \supseteq \mathcal{S}_{A_u,\ell}(\mathbb{F}_\ell)'$ for all primes

$$\ell \geq c \cdot \max(\{[K:\mathbb{Q}], h(A_u), N(\mathfrak{q})\})^\gamma, \tag{9.1}$$

where c and γ are positive constants that depend only on g. Since $u \notin R(x)$, we have $G_{A_u,\ell} = G_{A,\ell}$. In particular, we have $\mathcal{G}_{A_u,\ell} = \mathcal{G}_{A,\ell}$ and $\mathcal{S}_{A_u,\ell} = \mathcal{S}_{A,\ell}$. Therefore, we have $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ for all primes ℓ satisfying (9.1). Finally, since $N(\mathfrak{q}) \leq b \log x$, we can replace $N(\mathfrak{q})$ by $b \log x$ in (9.1) and adjust the constant c to obtain the lemma. □

We now bound the Faltings height $h(A_u)$ in terms of $H(u)$.

Lemma 9.2. *We have $\max\{1, h(A_u)\} \ll_A \log H(u) + 1$ for all $u \in U(K)$.*

Proof. We recall some results of Faltings [Fal86]. Let A_g be the coarse moduli space of the moduli stack $\mathfrak{A}_g$ of principally polarized abelian varieties of relative dimension g; it is a variety defined over $\mathbb{Q}$. There is an integer $r > 0$ for which $(\omega_{\mathcal{A}/\mathfrak{A}_g})^{\otimes r}$ defines a very ample line bundle on A_g, where $\mathcal{A} \to \mathfrak{A}_g$ is the universal abelian variety. Using this line bundle, we will identify A_g with a subvariety of a projective space $\mathbb{P}^m_{\mathbb{Q}}$. Let $\bar{\mathsf{A}}_g$ be the Zariski closure of A_g in $\mathbb{P}^m_{\mathbb{Z}}$ and let $\mathcal{M}$ be the induced line bundle $\mathcal{O}(1)$ on $\bar{\mathsf{A}}_g$. In [Fal86, §3], Faltings defines a hermitian metric $\|\cdot\|$ on the line bundle induced by $\mathcal{M}$ on $(\mathsf{A}_g)_{\mathbb{C}}$; it gives rise to a height function $h\colon \mathsf{A}_g(\bar{K}) \to \mathbb{R}$. Choose any hermitian metric $\|\cdot\|_1$ on the line bundle induced by $\mathcal{M}$ on $(\bar{\mathsf{A}}_g)_{\mathbb{C}}$; it gives rise to a height function $h_1\colon \bar{\mathsf{A}}_g(\bar{K}) \to \mathbb{R}$. For our implicit constants below, we note that the choices of r, $\mathcal{M}$ and $\|\cdot\|_1$ depend only on g.

Faltings observes that the metric $\|\cdot\|$ has logarithmic singularities along $\bar{\mathsf{A}}_g - \mathsf{A}_g$, cf. [Fal86, p. 15]. This implies that

$$|h(x) - h_1(x)| \ll_g \log h_1(x) + 1$$

for all $x \in \mathsf{A}_g(\bar{K})$; see the proof of [Fal86, Lemma 3] or [Sil86, Proposition 8.2]. Therefore, we have

$$\max\{1, h(x)\} \ll_g \max\{1, h_1(x)\} \ll_g \log H(x) + 1$$

for all $x \in \mathsf{A}_g(\bar{K})$, where H is the usual absolute height on $\mathbb{P}^m(\bar{K})$.

Consider a semistable abelian variety A defined over K that has a principal polarization ξ (the connected Néron model of A is a scheme over the ring of integers of K that is semiabelian). Denote by $x \in \mathsf{A}_g(K)$ the point on the moduli space corresponding to the pair (A, ξ). Then we have

$$h(A) = r \cdot h(x) + O_g(1);$$

this is noted in the proof of [Fal86, Theorem 1]. Combining the bounds above, we have

$$\max\{1, h(A)\} \ll_g \log H(x) + 1;$$

note that this remains true without the semistable hypothesis since both sides are stable under replacing K by a finite extension.

We finally consider our abelian scheme $A \to U$. First suppose that $A \to U$ has a principal polarization ξ. There is thus a morphism $\varphi\colon U \to (\mathsf{A}_g)_K$ such that the pair (A_u, ξ_u) represents the point $\varphi(u) \in \mathsf{A}_g(K)$ for each $u \in U(K)$, where ξ_u is the specialization of ξ at u. So from above, we find that

$$\max\{1, h(A_u)\} \ll_g \log H(\varphi(u)) + 1.$$

The lemma now follows since $\log H(\varphi(u)) \ll_\varphi \log H(u) + 1$ for all $u \in U(K)$, where the implicit constant depends only on the morphism $\varphi\colon U \to (\mathsf{A}_g)_K \subseteq \mathbb{P}^m_K$, cf. [Ser97, §2.6].

It remains to consider a general $A \to U$ that need not have a principal polarization. Define the abelian scheme $B := (A \times A^\vee)^4 \to U$, where $A^\vee$ is the dual of A. Using Zarhin's trick [FWG+92, Ch. IV Proposition 3.8], one finds that the abelian scheme $B \to U$ is principally polarized. So by the case of the lemma already proved, we have $\max\{1, h(B_u)\} \ll_A \log H(u) + 1$ for all $u \in U(K)$. The lemma follows since $h(B_u) = 8h(A_u)$ for all $u \in U(K)$, cf. the remarks after Propositions 3.7 and 3.8 in Ch. IV of [FWG+92] (recall we are using the stable Faltings height). □

Take $x \geq 2$. Take any $u \in U(K)$ satisfying $H(u) \leq x$ and $u \notin R(x) \cup T(x)$. We have $\max\{1, h(A_u)\} \ll_A \log x$ by Lemma 9.2. So by Lemma 9.1, there are positive constants c and γ such that $\bar{\rho}_{A_u,\ell}(\mathrm{Gal}_K) \supseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ holds for all $\ell \geq c(\log x)^\gamma$, where γ depends only on g and c depends only on A. Therefore,

$$B(x) \subseteq R(x) \cup T(x) \cup \bigcup_{b_A \leq \ell \leq c(\log x)^\gamma} B_\ell(x).$$

In particular, we have

$$|B(x)| \leq |R(x)| + |T(x)| + \sum_{b_A \leq \ell \leq c(\log x)^\gamma} |B_\ell(x)|. \tag{9.2}$$

We now bound the terms on the right hand side of (9.2).

9.1. **Bounding the sum of the $|B_\ell(x)|$.** Take c and γ as in (9.2). For each prime $b_A \leq \ell \leq c(\log x)^\gamma$, Theorem 8.1 implies that $|B_\ell(x)| \ll_A x^{[K:\mathbb{Q}](n+1/2)}(\log x)^{\gamma'}$, where γ' is a positive constant depending only on g. Therefore,

$$\sum_{b_A \leq \ell \leq c(\log x)^\gamma} |B_\ell(x)| \ll_A x^{[K:\mathbb{Q}](n+1/2)}(\log x)^{\gamma'+\gamma} = o(x^{[K:\mathbb{Q}](n+1)}). \tag{9.3}$$

9.2. **Bounding $|R(x)|$.** Let R be the set of $u \in U(K)$ such that $G_{A_u,\ell} \neq G_{A,\ell}$ for some ℓ. Note that $R(x)$ is the set of $u \in R$ with $H(u) \leq x$. The set R has density 0 by Proposition 2.3 and hence

$$|R(x)| = o(x^{[K:\mathbb{Q}](n+1)}). \tag{9.4}$$

9.3. **Bounding $|T(x)|$.** We fix a prime $\ell \geq b_A$. Let $\mathcal{U}$ be the open subscheme of $\mathbb{P}^n_{\mathcal{O}_K}$ that is the complement of the Zariski closure of $\mathbb{P}^n_K - U$ in $\mathbb{P}^n_{\mathcal{O}_K}$. There is an abelian scheme $\mathcal{A} \to \mathcal{U}_{\mathcal{O}}$, where $\mathcal{O}$ is the ring of $\mathscr{S}$-integers in K for some finite set $\mathscr{S}$ of nonzero prime ideals of $\mathcal{O}_K$, such that the fiber over $(\mathcal{U}_{\mathcal{O}})_K = U$ is our abelian scheme $A \to U$. By increasing $\mathscr{S}$, we may further assume that it contains all prime ideals that divide $\ell \cdot |\mathcal{G}_{A,\ell}(\mathbb{Z}/\ell\mathbb{Z})|$ and that $\mathcal{U}(\mathbb{F}_\mathfrak{p})$ is non-empty for all $\mathfrak{p} \notin \mathscr{S}$. There is no harm in replacing U by a non-empty open subvariety since this only removes a density 0 set of rational points. So after replacing U and increasing $\mathscr{S}$, we may further assume that $\mathcal{U}_{\mathbb{F}_\mathfrak{p}}$ is affine and geometrically irreducible for all non-zero prime ideals $\mathfrak{p} \notin \mathscr{S}$ of $\mathcal{O}_K$.

For each integer $e \geq 1$, the ℓ^e-torsion subscheme $\mathcal{A}[\ell^e]$ of $\mathcal{A}$ can be viewed as locally constant sheaf of $\mathbb{Z}/\ell^e\mathbb{Z}$-modules on $\mathcal{U}$ that is free of rank $2g$. The fiber of $\mathcal{A}[\ell^e]$ over $U = (\mathcal{U})_K$ is $A[\ell^e]$. Since $\bar{\rho}_{A,\ell^e}$ is the representation associated to $A[\ell^e]$, we find that it arises via base change from a representation of $\pi_1(\mathcal{U})$. Combining these representations together appropriately, we obtain a representation $\varrho_{\mathcal{A},\ell}$ of $\pi_1(\mathcal{U})$ such that base change gives rise to our representation $\rho_{A,\ell}\colon \pi_1(U) = \pi_1(\mathcal{U}_K) \to \mathrm{GL}_{V_\ell(A)}(\mathbb{Q}_\ell)$. Since $\varrho_{\mathcal{A},\ell}$ and $\rho_{A,\ell}$ have the same image, we have $\varrho_{\mathcal{A},\ell}\colon \pi_1(\mathcal{U}) \to \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$.

For a non-zero prime ideal $\mathfrak{p} \notin \mathscr{S}$ of $\mathcal{O}_K$ and a point $u \in \mathcal{U}(\mathbb{F}_\mathfrak{p})$, let $\mathcal{A}_u$ be the abelian variety over $\mathbb{F}_\mathfrak{p}$ that is the fiber of $\mathcal{A}$ over u. Since $\mathfrak{p} \nmid \ell$, we have $P_{\mathcal{A}_u}(x) = \det(xI - \varrho_{\mathcal{A},\ell}(\mathrm{Frob}_u))$, where $P_{\mathcal{A}_u}(x)$ is the Frobenius polynomial of $\mathcal{A}_u$. Let $\Phi_{\mathcal{A}_u}$ be the subgroup of $\mathbb{C}^\times$ generated by the roots of the Frobenius polynomial $P_{\mathcal{A}_u}(x)$.

Lemma 9.3. *There is a closed subvariety $Y \subsetneq G^\circ_{A,\ell}$, stable under conjugation by $G_{A,\ell}$, such that if $\varrho_{\mathcal{A},\ell}(\mathrm{Frob}_u) \in G^\circ_{A,\ell}(\mathbb{Q}_\ell) - Y(\mathbb{Q}_\ell)$ for a prime ideal $\mathfrak{p} \notin \mathscr{S}$ of $\mathcal{O}_K$ and a point $u \in \mathcal{U}(\mathbb{F}_\mathfrak{p})$, then $\Phi_{\mathcal{A}_u} \cong \mathbb{Z}^r$.*

Proof. This essentially follows from Theorem 1.2 [LP97]; we give a few extra details since this theorem was only stated for representations of Gal_K.

Take any prime ideal $\mathfrak{p} \notin \mathscr{S}$ and $u \in \mathcal{U}(\mathbb{F}_\mathfrak{p})$. Let $H_{u,\ell}$ be the Zariski closure of the subgroup of $G_{A,\ell}$ generated by $\varrho_{\mathcal{A},\ell}(\mathrm{Frob}_u)$. The proof of Lemma 1.3(b) of [LP97] shows that there are only finitely many possibilities for $(H_{u,\ell})_{\overline{\mathbb{Q}}_\ell}$ up to conjugation by $\mathrm{GL}_{V_\ell(A)}(\overline{\mathbb{Q}}_\ell)$ as we vary over all $\mathfrak{p}$ and u; note that the proof only uses that $\varrho_{\mathcal{A},\ell}(\mathrm{Frob}_u)$ is semisimple along with information about the valuations of the roots of $P_{\mathcal{A}_u}(x)$. The end of the proof of Theorem 1.2 [LP97] then shows how to construct a closed subvariety $Y \subsetneq G^\circ_{A,\ell}$, stable under conjugation by $G_{A,\ell}$, such that if $\varrho_{\mathcal{A},\ell}(\mathrm{Frob}_u) \in G^\circ_{A,\ell}(\mathbb{Q}_\ell) - Y(\mathbb{Q}_\ell)$ for a prime ideal $\mathfrak{p} \notin \mathscr{S}$ of $\mathcal{O}_K$ and a point $u \in \mathcal{U}(\mathbb{F}_\mathfrak{p})$, then $H_{u,\ell}$ is a maximal torus of $G^\circ_{A,\ell}$.

Now suppose that $T := H_{u,\ell}$ is a maximal torus of $G^\circ_{A,\ell}$; it remains to show that $\Phi_{\mathcal{A}_u} \cong \mathbb{Z}^r$. Let $X(T)$ be the group of characters $T_{\overline{\mathbb{Q}}_\ell} \to \mathbb{G}_{m,\overline{\mathbb{Q}}_\ell}$; it is a free abelian group whose rank is equal to $\dim T = \mathrm{rank} G^\circ_{A,\ell} = r$. Define the homomorphism $\varphi\colon X(T) \to \mathbb{C}^\times$, $\alpha \mapsto \iota(\alpha(\varrho_{\mathcal{A},\ell}(\mathrm{Frob}_u)))$, where ι is any embedding of $\overline{\mathbb{Q}}_\ell$ into $\mathbb{C}$. The homomorphism φ is injective since otherwise $H_{u,\ell} \neq T$. Since $\varrho_{\mathcal{A},\ell}(\mathrm{Frob}_u)$ is semisimple with characteristic polynomial $P_{\mathcal{A}_u}(x)$, we find that the image of φ is generated by the roots of $P_{\mathcal{A}_u}(x)$. Therefore, we have isomorphisms $\Phi_{\mathcal{A}_u} \cong X(T) \cong \mathbb{Z}^r$. □

For each non-zero prime ideal $\mathfrak{p} \notin \mathscr{S}$ of $\mathcal{O}_K$, let $D_\mathfrak{p}$ be the set of $u \in \mathbb{P}^n(\mathbb{F}_\mathfrak{p})$ for which $u \notin \mathcal{U}(\mathbb{F}_\mathfrak{p})$ or for which $\Phi_{\mathcal{A}_u} \not\cong \mathbb{Z}^r$. Define $\delta_\mathfrak{p} := |D_\mathfrak{p}|/|\mathbb{P}^n(\mathbb{F}_\mathfrak{p})|$.

Lemma 9.4. *There is a constant $0 \leq \delta < 1$ such that $\delta_\mathfrak{p} \leq \delta$ holds for infinitely many prime ideals $\mathfrak{p} \notin \mathscr{S}$ of $\mathcal{O}_K$.*

Proof. Fix an integer $e \geq 1$. Take Y as in Lemma 9.3 and define $\mathcal{Y} = Y(\mathbb{Q}_\ell) \cap \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$; it is stable under conjugation by $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$. Let $\mathcal{Y}_e$ be the image of $\mathcal{Y}$ in $\mathcal{G}_{A,\ell}(\mathbb{Z}/\ell^e\mathbb{Z})$. Let $\bar{\varrho}_{\mathcal{A},\ell^e}\colon \pi_1(\mathcal{U}) \to \mathcal{G}_{A,\ell}(\mathbb{Z}/\ell^e\mathbb{Z})$ be the representation obtained by composing $\varrho_{\mathcal{A},\ell}$ with the reduction map $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) \to \mathcal{G}_{A,\ell}(\mathbb{Z}/\ell^e\mathbb{Z})$.

Define the finite group $G := \bar{\varrho}_{\mathcal{A},\ell^e}(\pi_1(\mathcal{U})) = \bar{\rho}_{A,\ell^e}(\pi_1(U)) \subseteq \mathcal{G}_{A,\ell}(\mathbb{Z}/\ell^e\mathbb{Z})$. Define $G_g := \bar{\varrho}_{\mathcal{A},\ell^e}(\pi_1((\mathcal{U}_\mathcal{O})_{\overline{K}})) = \bar{\rho}_{A,\ell^e}(\pi_1(U_{\overline{K}}))$; it is a normal subgroup of G. After possibly increasing the finite set $\mathscr{S}$, we may assume that

$$\bar{\varrho}_{\mathcal{A},\ell^e}(\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_\mathfrak{p}})) = G_g$$

holds for all non-zero prime ideals $\mathfrak{p} \notin \mathscr{S}$ of $\mathcal{O}_K$, see Lemma 6.5.

Take a non-zero prime ideal $\mathfrak{p} \notin \mathscr{S}$ of $\mathcal{O}_K$. From $\bar{\varrho}_{\mathcal{A},\ell^e}$, base change to $\mathbb{F}_\mathfrak{p}$ gives a homomorphism we will denote by $\varrho_\mathfrak{p}\colon \pi_1(\mathcal{U}_{\mathbb{F}_\mathfrak{p}}) \to G$; uniquely defined up to conjugation by G and satisfying $\varrho_\mathfrak{p}(\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_\mathfrak{p}})) = G_g$. Let $\kappa_\mathfrak{p}$ be the unique G_g-coset of G that contains $\varrho_\mathfrak{p}(\mathrm{Frob}_u)$ for all $u \in \mathcal{U}(\mathbb{F}_\mathfrak{p})$. Note that the set $\mathcal{Y}_e \cap \kappa_\mathfrak{p}$ is stable under conjugation by G.

If $\varrho_\mathfrak{p}(\mathrm{Frob}_u) \in \kappa_\mathfrak{p} - (\mathcal{Y}_e \cap \kappa_\mathfrak{p})$ for a point $u \in \mathcal{U}(\mathbb{F}_\mathfrak{p})$, then $\varrho_{\mathcal{A},\ell}(\mathrm{Frob}_u) \notin Y(\mathbb{Q}_\ell)$ and hence $\Phi_{\mathcal{A}_u} \cong \mathbb{Z}^r$ by Lemma 9.3. Therefore,

$$\{u \in \mathcal{U}(\mathbb{F}_\mathfrak{p}) : \varrho_\mathfrak{p}(\mathrm{Frob}_u) \in \kappa_\mathfrak{p} - (\mathcal{Y}_e \cap \kappa_\mathfrak{p})\} \subseteq \mathbb{P}^n(\mathbb{F}_\mathfrak{p}) - D_\mathfrak{p}.$$

By Theorem 6.3, this implies that

$$\Big(1 - \frac{|\mathcal{Y}_e \cap \kappa_\mathfrak{p}|}{|G_g|}\Big)\, |\mathcal{U}(\mathbb{F}_\mathfrak{p})| + O_{\mathcal{A},\ell^e}(N(\mathfrak{p})^{n-1/2}) \leq |\mathbb{P}^n(\mathbb{F}_\mathfrak{p})| - |D_\mathfrak{p}|.$$

Dividing by $|\mathbb{P}^n(\mathbb{F}_\mathfrak{p})|$ and using that $|\mathbb{P}^n(\mathbb{F}_\mathfrak{p}) - \mathcal{U}(\mathbb{F}_\mathfrak{p})| \ll_A N(\mathfrak{p})^{n-1/2}$, we deduce that

$$\delta_\mathfrak{p} \leq \frac{|\mathcal{Y}_e \cap \kappa_\mathfrak{p}|}{|G_g|} + O_{A,\ell^e}(N(\mathfrak{p})^{-1/2}). \tag{9.5}$$

Now suppose that $\mathcal{Y}_e \cap G$ is a proper subset of G. Then there is a G_g-coset κ_0 of G such that $\mathcal{Y}_e \cap \kappa_0$ is a proper subset of κ_0. Let C be the conjugacy class of G/G_g that contains the image of κ_0. Define the homomorphism

$$\alpha\colon \pi_1(\mathcal{U}) \xrightarrow{\bar{\varrho}_{\mathcal{A},\ell^e}} G \to G/G_g.$$

The homomorphism α factors through Gal_K; moreover, for $u \in \mathcal{U}(\mathbb{F}_\mathfrak{p})$ with $\mathfrak{p} \notin \mathscr{S}$, the conjugacy class of $\alpha(\mathrm{Frob}_u)$ is represented by the image of $\kappa_\mathfrak{p}$ in G/G_g. By the Chebotarev density theorem, there are infinitely many $\mathfrak{p} \notin \mathscr{S}$ for which the image of $\kappa_\mathfrak{p}$ in G/G_g lies in C; now take any such $\mathfrak{p}$. The cosets $\kappa_\mathfrak{p}$ and κ_0 are conjugate in G. Since $\mathcal{Y}_e \cap G$ is stable under conjugation by G, we have

$$\frac{|\mathcal{Y}_e \cap \kappa_\mathfrak{p}|}{|G_g|} = \frac{|\mathcal{Y}_e \cap \kappa_0|}{|G_g|} < 1,$$

where the inequality uses our choice of κ_0. In particular, $|\mathcal{Y}_e \cap \kappa_\mathfrak{p}|/|G_g| \leq 1 - 1/|G_g|$. After first excluding a finite number of $\mathfrak{p}$, we deduce that $\delta_\mathfrak{p} < 1$ by (9.5).

So to prove the lemma, it suffices to show that $\mathcal{Y}_e \cap G$ is a proper subset of G. Since $Y \subsetneq G^\circ_{A,\ell}$, the variety Y has dimension at most $d-1$, where $d := \dim G^\circ_{A,\ell}$. So $\mathcal{Y}$ is a p-adic analytic manifold of dimension at most $d-1$ and hence $|\mathcal{Y}_e| \ll_\mathcal{Y} \ell^{e(d-1)}$, cf. [Ser81, Theéorème 8]. Since $\ell \geq b_A$, $\mathcal{G}_{A,\ell}$ is smooth and $[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\pi_1(U))] \ll_A 1$ by Theorem 3.1(i) and (iii). Therefore, $[\mathcal{G}_{A,\ell}(\mathbb{Z}/\ell^e\mathbb{Z}) : \bar{\rho}_{A,\ell^e}(\pi_1(U))] \ll_A 1$ and hence $|G| \gg_A |\mathcal{G}_{A,\ell}(\mathbb{Z}/\ell^e\mathbb{Z})| \gg_A \ell^{ed}$. We have not imposed any conditions on the integer $e \geq 1$ yet. So using $|G| \gg_A \ell^{ed}$ and $|\mathcal{Y}_e| \ll_\mathcal{Y} \ell^{e(d-1)}$, we choose $e \geq 1$ large enough so that $|G| > |\mathcal{Y}_e|$ and hence $\mathcal{Y}_e \cap G$ is a proper subset of G. □

By Lemma 9.4, there are infinitely many non-zero prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ of $\mathcal{O}_K$ that are not in $\mathscr{S}$ and satisfy $\delta_{\mathfrak{p}_i} \leq \delta$ for some $0 \leq \delta < 1$. Take any integer $m \geq 1$.

Let D be the set of $u \in \mathbb{P}^n(K)$ for which the image in $\mathbb{P}^n(\mathbb{F}_{\mathfrak{p}_i})$ under the reduction modulo $\mathfrak{p}_i$ lies in $D_{\mathfrak{p}_i}$ for all $1 \leq i \leq m$. The subset D of $\mathbb{P}^n(K)$ has density $\prod_{i=1}^m \delta_{\mathfrak{p}_i}$. Note that if the reduction $\bar{u}$ of a point $u \in U(K)$ modulo $\mathfrak{p}_i$ lies in $\mathbb{P}^n(\mathbb{F}_{\mathfrak{p}_i}) - D_{\mathfrak{p}_i}$, then $A_u = \mathcal{A}_u$ has good reduction at $\mathfrak{p}_i$ and $\Phi_{A_u,\mathfrak{p}} = \Phi_{\mathcal{A}_{\bar{u}}} \cong \mathbb{Z}^r$. Therefore, we have $T(x) \subseteq D$ for all sufficiently large x. Since D has density $\prod_{i=1}^m \delta_{\mathfrak{p}_i}$, we deduce that

$$\limsup_{x\to+\infty} \frac{|T(x)|}{|\{u \in \mathbb{P}^n(K) : H(u) \leq x\}|} \leq \prod_{i=1}^m \delta_{\mathfrak{p}_i} \leq \delta^m.$$

Since $0 \leq \delta < 1$ and since $m \geq 1$ was arbitrary, this implies that $\lim_{x\to+\infty} |T(x)|/|\{u \in \mathbb{P}^n(K) : H(u) \leq x\}| = 0$. Equivalently, we have

$$|T(x)| = o(x^{[K:\mathbb{Q}](n+1)}). \tag{9.6}$$

9.4. **End of the proof.** Using (9.2) with (9.3), (9.4) and (9.6), we deduce that $|B(x)| = o(x^{[K:\mathbb{Q}](n+1)})$ and hence B has density 0. As already noted, the theorem now follows directly from Proposition 5.1.

10. Proof of Theorem 1.2

After replacing X by a non-empty open subvariety, and restricting A, we may assume that there is an étale morphism $\varphi\colon X \to U$, where U is a non-empty open subvariety of $\mathbb{P}^n_K$ and n is the dimension of X.

We first consider the special case where $\varphi\colon X \to U$ is a Galois cover. Denote the degree of φ by d. Define

$$B := \mathrm{Res}_{X/U}(A),$$

i.e., the Weil restriction of A along the morphism φ; it is an abelian scheme of relative dimension $g \cdot d$ over U. Note that for any U-scheme S, we have $B(S) = A(S \times_U X)$.

Using φ, we can identify $\pi_1(X)$ with a normal subgroup of $\pi_1(U)$. Let G be the Galois group of φ, i.e., the group of automorphisms σ of X such that $\varphi \circ \sigma = \varphi$. For each $\sigma \in G$, let A^σ be the abelian scheme over X obtained by composing $A \to X$ with σ^{-1}. Using that φ is a Galois cover, we have a natural isomorphism

$$B \times_U X = \prod_{\sigma \in G} A^\sigma \tag{10.1}$$

of abelian schemes over X and hence an isomorphism $\rho_B|_{\pi_1(X)} = \prod_{\sigma \in G} \rho_{A^\sigma}$ of representations of $\pi_1(X)$.

For any number field L/K and point $x \in X(L)$, taking the fiber of (10.1) above x gives a natural isomorphism

$$B_{\varphi(x)} = \prod_{\sigma \in G} A_{\sigma(x)}$$

of abelian varieties over L; the fiber of A^σ over x is $A_{\sigma(x)}$. Therefore, we have an equality $\rho_{B_{\varphi(x)}} = \prod_{\sigma \in G} \rho_{A_{\sigma(x)}}$ of representations of Gal_L. By considering specializations, we find that

$$[\rho_B(\pi_1(X)) : \rho_{B_{\varphi(x)}}(\mathrm{Gal}_L)] = \Big[(\prod_{\sigma \in G} \rho_{A_\sigma})(\pi_1(X)) : (\prod_{\sigma \in G} \rho_{A_{\sigma(x)}})(\mathrm{Gal}_L)\Big].$$

Therefore, $[\rho_A(\pi_1(X)) : \rho_{A_x}(\mathrm{Gal}_L)] \leq [\rho_B(\pi_1(X)) : \rho_{B_{\varphi(x)}}(\mathrm{Gal}_L)] \leq [\rho_B(\pi_1(U)) : \rho_{B_{\varphi(x)}}(\mathrm{Gal}_L)]$.

By Theorem 1.1, there is a constant C such that $[\rho_B(\pi_1(U)) : \rho_{B_u}(\mathrm{Gal}_K)] \leq C$ holds for infinitely many $u \in U(K)$. Take any such $u \in U(K)$. There is a field L/K with $[L : K] \leq d$ and a point $x \in X(L)$ such that $\varphi(x) = u$. Therefore,

$$[\rho_A(\pi_1(X)) : \rho_{A_x}(\mathrm{Gal}_L)] \leq [\rho_B(\pi_1(U)) : \rho_{B_{\varphi(x)}}(\mathrm{Gal}_L)] \leq [\rho_B(\pi_1(U)) : \rho_{B_u}(\mathrm{Gal}_K)] \cdot [L : K] \leq C \cdot d.$$

This proves that $[\rho_A(\pi_1(X)) : \rho_{A_{\tilde{x}}}(\mathrm{Gal}_{k(\tilde{x})})] \leq C \cdot d$ and $[k(\tilde{x}) : K] \leq d$, where $\tilde{x}$ is the closed point of X corresponding to x (one can identify $\tilde{x}$ with the Gal_K-orbit of x in $X(\overline{K})$). There are infinitely many such closed points $\tilde{x}$ since we have infinitely many $u \in U(K)$ for which $[\rho_B(\pi_1(U)) : \rho_{B_u}(\mathrm{Gal}_K)] \leq C$. This completes the proof in the case where φ is a Galois cover.

We now consider the general case. There is an étale morphism $\psi \colon X' \to X$ such that its composition with φ gives a Galois cover $\varphi' \colon X' \to U$. To prove Theorem 1.2 there is no harm in replacing K by a finite extension K' and A by its base change over $X_{K'}$. So without loss of generality, we may assume that X' is a geometrically irreducible variety defined over K.

Let $A' \to X'$ be the base change of A by ψ; it is an abelian scheme over X'. Since φ' is Galois, the case of Theorem 1.2 already proved shows that there are integers d and C such that $[\rho_{A'}(\pi_1(X')) : \rho_{A'_{x'}}(\mathrm{Gal}_{k(x')})] \leq C$ holds for infinitely many closed points x' of X' satisfying $[k(x') : K] \leq d$. Take any such closed point x' of X' and define the closed point $x = \varphi(x')$ of X. Using ψ, we can view $k(x')$ as an extension of $k(x)$ of degree at most $\deg \psi$. In particular, $[k(x) : K] \leq [k(x') : K] \leq d$. We have an isomorphism A_x between $A'_{x'}$ as abelian varieties over $k(x')$. Therefore, we have

$$[\rho_A(\pi_1(X')) : \rho_{A_x}(\mathrm{Gal}_{k(x')})] = [\rho_{A'}(\pi_1(X')) : \rho_{A'_{x'}}(\mathrm{Gal}_{k(x')})].$$

and hence

$$\begin{aligned} [\rho_A(\pi_1(X)) : \rho_{A_x}(\mathrm{Gal}_{k(x)})] &\leq [\rho_A(\pi_1(X')) : \rho_{A_x}(\mathrm{Gal}_{k(x')})] \cdot \deg \psi \\ &= [\rho_{A'}(\pi_1(X')) : \rho_{A'_{x'}}(\mathrm{Gal}_{k(x')})] \cdot \deg \psi \\ &\leq C \cdot \deg \psi. \end{aligned}$$

Therefore, $[k(x) : k] \leq d$ and $[\rho_A(\pi_1(X)) : \rho_{A_x}(\mathrm{Gal}_{k(x)})] \leq C \cdot \deg \psi$. Finally, there are infinitely many such closed points x of X since they arose from infinitely many closed points x' of X'.

References

[Cad15] Anna Cadoret, *An open adelic image theorem for abelian schemes*, Int. Math. Res. Not. IMRN **20** (2015), 10208–10242, DOI 10.1093/imrn/rnu259. MR3455865 ↑1.3

[Cha86] Ching-Li Chai, *Siegel moduli schemes and their compactifications over* **C**, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 231–251. ↑3.3

[CGJ11] Alina-Carmen Cojocaru, David Grant, and Nathan Jones, *One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations*, Proc. Lond. Math. Soc. (3) **103** (2011), no. 4, 654–675. ↑1.3

[Del71] Pierre Deligne, *Théorie de Hodge. II*, Inst. Hautes Études Sci. Publ. Math. **40** (1971), 5–57 (French). ↑4.1

[Duk97] William Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818 (English, with English and French summaries). ↑1.3

[Fal86] Gerd Faltings, *Finiteness theorems for abelian varieties over number fields*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 9–27. Translated from the German original [Invent. Math. **73** (1983), no. 3, 349–366; ibid. **75** (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz. ↑2.2, 9

[FWG$^+$92] Gerd Faltings, Gisbert Wüstholz, Fritz Grunewald, Norbert Schappacher, and Ulrich Stuhler, *Rational points*, 3rd ed., Aspects of Mathematics, E6, Friedr. Vieweg & Sohn, Braunschweig, 1992. Papers from the seminar held at the Max-Planck-Institut für Mathematik, Bonn/Wuppertal, 1983/1984; With an appendix by Wüstholz. ↑9

[FG12] Jason Fulman and Robert Guralnick, *Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements*, Trans. Amer. Math. Soc. **364** (2012), no. 6, 3023–3070. ↑7.1

[GM88] Mark Goresky and Robert MacPherson, *Stratified Morse theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 14, Springer-Verlag, Berlin, 1988. ↑

[Gre10] Aaron Greicius, *Elliptic curves with surjective adelic Galois representations*, Experiment. Math. **19** (2010), no. 4, 495–507. ↑1.3

[HL15] Chun Yin Hui and Michael Larsen, *Adelic openness without the Mumford-Tate conjecture* (2015), available at https://arxiv.org/abs/1312.3812v2. arXiv:1312.3812v2. ↑5.1

[Jon10] Nathan Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570. ↑1.3

[KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits. ↑7.2

[Kow06a] E. Kowalski, *On the rank of quadratic twists of elliptic curves over function fields*, Int. J. Number Theory **2** (2006), no. 2, 267–288. ↑6.1, 6.1

[Kow06b] ———, *The large sieve, monodromy and zeta functions of curves*, J. Reine Angew. Math. **601** (2006), 29–69. ↑6.1

[LSTX19] Aaron Landesman, Ashvin Swaminathan, James Tao, and Yujie Xu, *Surjectivity of Galois representations in rational families of abelian varieties*, Algebra Number Theory **13** (2019), no. 5, 995–1038. With an appendix by Davide Lombardo. ↑1.3, 1.6, 6.3

[LSTX17] ———, *Hyperelliptic curves with maximal Galois action on the torsion points of their Jacobians* (2017), available at https://arxiv.org/abs/1705.08777. arXiv:1011.6465. ↑1.6

[LP97] Michael Larsen and Richard Pink, *A connectedness criterion for l-adic Galois representations*, Israel J. Math. **97** (1997), 1–10. ↑2.2, 2.2, 9.3

[LP11] ———, *Finite subgroups of algebraic groups*, J. Amer. Math. Soc. **24** (2011), 1105–1158. ↑5.1

[LPS07] Martin W. Liebeck, Laszlo Pyber, and Aner Shalev, *On a conjecture of G. E. Wall*, J. Algebra **317** (2007), no. 1, 184–197. ↑8.2

[Lom15] Davide Lombardo, *Explicit open image theorems for abelian varieties with trivial endomorphism ring* (2015), available at https://arxiv.org/abs/1508.01293. arXiv:1508.01293. ↑

[Nor87] Madhav V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$, Invent. Math. **88** (1987), no. 2, 257–275. ↑8.2

[Pet16] Sebastian Petersen, *Group-theoretical independence of ℓ-adic Galois representations*, Acta Arith. **176** (2016), no. 2, 161–176. ↑8.2

[Rib76] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804. ↑5.1, 7.2

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331 (French). ↑1, 1.3

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401 (French). ↑9.3

[Ser97] ———, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt; With a foreword by Brown and Serre. ↑1.3, 2.1, 6.2, 6.2, 9

[Ser00] ———, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000. 1985–1998. ↑2.2, 2.2

[Ser03] ———, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) **40** (2003), no. 4, 429–440 (electronic). ↑6

[SGA7.1] *Groupes de monodromie en géométrie algébrique. I*, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, Berlin-New York, 1972 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I); Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. MR0354656 ↑4.2

[Sil86] Joseph H. Silverman, *The theory of height functions*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 151–166. ↑9

[Wal14] Erik Wallace, *Principally polarized abelian surfaces with surjective Galois representations on l-torsion*, J. Lond. Math. Soc. (2) **90** (2014), no. 2, 451–471. ↑1.3

[Wew99] Stefan Wewers, *Deformation of tame admissible covers of curves*, Aspects of Galois theory (Gainesville, FL, 1996), 1999, pp. 239–282. ↑6.3

[Win02] J.-P. Wintenberger, *Démonstration d'une conjecture de Lang dans des cas particuliers*, J. Reine Angew. Math. **553** (2002), 1–16. ↑2.6

[Zyw10] David Zywina, *Hilbert's irreducibility theorem and the larger sieve* (2010), available at https://arxiv.org/abs/1011.6465. arXiv:1011.6465. ↑1.3

[Zyw19] ———, *An effective open image theorem for abelian varieties* (2019), available at https://arxiv.org/abs/1910.14171. arXiv:1910.14171. ↑3.3, 3.4

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
Email address: `zywina@math.cornell.edu`
URL: `http://www.math.cornell.edu/~zywina`