GALOIS GROUPS ARISING FROM FAMILIES WITH BIG ORTHOGONAL MONODROMY

DAVID ZYWINA

Abstract. We study the Galois groups of polynomials arising from a compatible family of representations with big orthogonal monodromy. We show that the Galois groups are usually as large as possible given the constraints imposed on them by a functional equation and discriminant considerations. As an application, we consider the Frobenius polynomials arising from the middle étale cohomology of hypersurfaces in $\mathbb{P}^{2n+1}_{\mathbb{F}_q}$ of degree at least 3. We also consider the L-functions of quadratic twists of fixed degree of an elliptic curve over a function field $\mathbb{F}_q(t)$. To determine the typical Galois group in the elliptic curve setting requires using some known cases of the Birch and Swinnerton-Dyer conjecture. This extends and generalizes work of Chavdarov, Katz and Jouve.

1. Introduction

1.1. **Constraint on the Galois group of reciprocal polynomials.** We first define some of the groups that will arise as Galois groups in our applications.

For each integer $n \geq 1$, let W_{2n} be the subgroup of signed permutations in $\mathrm{GL}_n(\mathbb{Z})$, i.e., permutation matrices whose non-zero entries are allowed to be ± 1. Let W_{2n}^+ be the subgroup of W_{2n} consisting of those elements that act evenly on the set $\{\pm e_1, \ldots, \pm e_n\}$. The group W_{2n} has order $2^n n!$ and is isomorphic to the Weyl group of the root systems B_n and C_n. The group W_{2n}^+ has order $2^{n-1}n!$ and is isomorphic to the Weyl group of the root system D_n.

Now consider a polynomial $P \in \mathbb{Q}[T]$ of degree $N > 2$ that satisfies

$$T^N P(1/T) = \varepsilon P(T) \tag{1.1}$$

for some $\varepsilon \in \{\pm 1\}$. Setting $T = 1$ and $T = -1$ in the above equation, we find that $P(1) = 0$ if $\varepsilon \neq 1$ and $P(-1) = 0$ if $\varepsilon \neq (-1)^N$. So by removing these obvious linear factors from P, we obtain a polynomial

$$f(T) := \begin{cases} P(T)/(1+\varepsilon T) & \text{if } N \text{ is odd,} \\ P(T)/(1-T^2) & \text{if } N \text{ is even and } \varepsilon = -1, \\ P(T) & \text{if } N \text{ is even and } \varepsilon = 1 \end{cases} \tag{1.2}$$

with rational coefficients and even degree $2n \geq 2$. From (1.1), we deduce that the polynomial f is reciprocal, i.e., it satisfies $T^{2n} f(1/T) = f(T)$.

Let $\mathrm{Gal}(P)$ be the Galois group of a splitting field of P, equivalently of f, over $\mathbb{Q}$. Since f is reciprocal, its distinct roots in $\overline{\mathbb{Q}} - \{\pm 1\}$ are of the form $\alpha_1, \ldots, \alpha_m, \alpha_1^{-1}, \ldots, \alpha_m^{-1}$ for an integer $1 \leq m \leq n$. Let $\iota\colon \{\alpha_1^{\pm 1}, \ldots, \alpha_m^{\pm 1}\} \to \{\pm e_1, \ldots, \pm e_m\}$ be the bijection satisfying $\iota(\alpha_i) = e_i$ and $\iota(\alpha_i^{-1}) = -e_i$. There is a unique injective homomorphism $\psi\colon \mathrm{Gal}(P) \hookrightarrow W_{2m}$ satisfying $\iota(\sigma(\alpha)) = \psi(\sigma) \cdot \iota(\alpha)$ for each root $\alpha \in \overline{\mathbb{Q}} - \{\pm 1\}$ of P and $\sigma \in \mathrm{Gal}(P)$. So $\mathrm{Gal}(P)$ is isomorphic to a subgroup of W_{2m} and hence also a subgroup of W_{2n}. So $\mathrm{Gal}(P)$ is isomorphic to a subgroup of W_{N-1} if N is odd, W_{N-2} if N is even and $\varepsilon = -1$, and W_N if N is even and $\varepsilon = 1$.

2020 *Mathematics Subject Classification.* Primary 11F80; Secondary 11G05, 14D05.

Key words and phrases. Galois representations; big monodromy, elliptic curves over function fields.

Suppose that P is separable, N is even and $\varepsilon = 1$. If the discriminant of P is a square, then $\mathrm{Gal}(P)$ will be isomorphic to a subgroup of W_N^+.

1.2. **Example: smooth hypersurfaces over finite fields.** Fix an even integer $n \geq 2$ and an integer $d \geq 3$ with $(n,d) \neq (2,3)$. Fix a finite field $\mathbb{F}_q$ with cardinality q. We define $U(\mathbb{F}_q)$ to be the set of homogeneous polynomials in $\mathbb{F}_q[x_0, \ldots, x_{n+1}]$ of degree d, up to scalar multiplication by $\mathbb{F}_q^\times$, that define a *smooth* hypersurface in $\mathbb{P}^{n+1}_{\mathbb{F}_q}$.

Take any $f \in U(\mathbb{F}_q)$. The zeta function of the hypersurface H_f in $\mathbb{P}^{n+1}_{\mathbb{F}_q}$ defined by f is the power series

$$Z_f(T) = \exp\Big(\sum_{n=1}^{\infty} |H_f(\mathbb{F}_{q^n})| \cdot T^n/n\Big).$$

One can show that $Z_f(T)$ is a rational function in T and moreover that

$$Z_f(T) = 1/\Big(P_f(q^nT) \cdot \prod\nolimits_{i=0}^{2n}(1 - q^iT)\Big)$$

for a unique polynomial $P_f(T) \in \mathbb{Q}[T]$ of degree $N := (d-1)((d-1)^{n+1}+1)/d$. Note that the integer N depends only on n and d. The functional equation for $Z_f(T)$ implies that we have the relation $T^N P_f(1/T) = \varepsilon_f\, P_f(T)$ for a unique $\varepsilon_f \in \{\pm 1\}$.

We will describe the Galois group $\mathrm{Gal}(P_f)$ for a "random" $f \in U(\mathbb{F}_q)$. From §1.1, and using that N is even if and only if d is odd, we find that $\mathrm{Gal}(P_f)$ is isomorphic to a subgroup of W_{N-1} if d is even, W_{N-2} if d is odd and $\varepsilon_f = -1$, and W_N if d is odd and $\varepsilon_f = 1$.

There is an additional constraint on the Galois group of P_f. Suppose that d is odd, $\varepsilon_f = 1$ and P_f is separable. We will show later that the discriminant of P_f is in $(-1)^{(d-1)/2} d \cdot (\mathbb{Q}^\times)^2$. Since d is odd, we deduce that the discriminant of P_f is a square if and only if d is a square. So if d is odd, $\mathrm{Gal}(P_f)$ will be isomorphic to a subgroup of W_N^+.

The following theorem says that the Galois group of P_f is as large as possible, given the above constraints, for a "random" polynomial $f \in U(\mathbb{F}_q)$.

Theorem 1.1. *For each prime power $q > 1$, let $\delta(q)$ be the proportion of $f \in U(\mathbb{F}_q)$ for which we have an isomorphism*

$$\mathrm{Gal}(P_f) \cong \begin{cases} W_{N-1} & \text{if } d \text{ is even,} \\ W_{N-2} & \text{if } d \text{ is odd and } \varepsilon_f = -1, \\ W_N^+ & \text{if } d \text{ is odd, } \varepsilon_f = 1, \text{ and } d \text{ is a square,} \\ W_N & \text{if } d \text{ is odd, } \varepsilon_f = 1, \text{ and } d \text{ is not a square.} \end{cases}$$

Then $\delta(q) \to 1$ as $q \to \infty$.

We will prove Theorem 1.1 in §8 by showing that it satisfies the general framework of Theorem 1.4. We will use some Hodge theory to compute the field K of §1.3.4 which is needed to distinguish the cases when d is odd and $\varepsilon_f = 1$.

Remark 1.2. Let us briefly mention the excluded case where $n \geq 2$ is *odd*. Take any $d \geq 3$ and define $U(\mathbb{F}_q)$ as before. For any $f \in U(\mathbb{F}_q)$, the zeta function of the hypersurface defined by f will now be of the form $P_f(T)/\prod_{i=0}^{2n}(1-q^iT)$ for a unique polynomial $P_f(T) \in \mathbb{Q}[T]$ of degree $N := (d-1)((d-1)^{n+1}-1)/d$.

The description of the Galois group of P_f for a "random" $f \in U(\mathbb{F}_q)$ is now much more straightforward. We have $\delta(q) \to 1$ as $q \to \infty$, where $\delta(q)$ is the proportion of $f \in U(\mathbb{F}_q)$ for which $\mathrm{Gal}(P_f)$ is isomorphic to W_N. This can be proved with the techniques of this paper and using the computations of Chavdarov (the work of Chavdarov will be described in §1.7).

For both even and odd n, the polynomial P_f can be obtained from the characteristic polynomial of the q-th power Frobenius automorphism acting on the middle étale cohomology group $V := H^n_{\text{ét}}((H_f)_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ for a prime $\ell \nmid q$. The important difference between the two cases is that the cup product $V \times V \to H^{2n}((H_f)_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell(-n)$ is symmetric when n is even and skew-symmetric when n is odd.

Remark 1.3. The sign ε_f can be $+1$ or -1 and both occur with essentially equal likelihood. More precisely, for a fixed $\varepsilon \in \{\pm 1\}$, we have $|\{f \in U(\mathbb{F}_q) : \varepsilon_f = \varepsilon\}|/|U(\mathbb{F}_q)| \to 1/2$ as $q \to \infty$.

1.3. **General setup.** Let R be either a finite field or the ring of S-units in a number field F with S a finite set of non-zero prime ideals of $\mathcal{O}_F$. Let U be a smooth scheme over R of relative dimension at least 1 with geometrically connected fibers.

1.3.1. *Representations.* Fix a set of rational primes Σ with Dirichlet density 1 such that each $\ell \in \Sigma$ is not equal to the characteristic of R and satisfies $\ell \geq 5$. For each prime $\ell \in \Sigma$, we fix a continuous representation

$$\rho_\ell \colon \pi_1(U_{R[1/\ell]}) \to \mathrm{O}(M_\ell),$$

where M_ℓ is an orthogonal space[1] over $\mathbb{Z}_\ell$. Here, and throughout this article, π_1 will always refer to the étale fundamental group. We will suppress the base point in our fundamental groups and hence its elements and representations will only be determined up to conjugacy. Equivalent to giving ρ_ℓ is to give a lisse $\mathbb{Z}_\ell$-sheaf $\mathcal{H}_\ell$ on $U_{R[1/\ell]}$ of free $\mathbb{Z}_\ell$-modules of finite rank with a symmetric autoduality pairing $\mathcal{H}_\ell \times \mathcal{H}_\ell \to \mathbb{Z}_\ell$.

From M_ℓ, we obtain orthogonal spaces $V_\ell := M_\ell/\ell M_\ell$ and $\mathcal{V}_\ell := M_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ over $\mathbb{F}_\ell$ and $\mathbb{Q}_\ell$, respectively. Let

$$\bar{\rho}_\ell \colon \pi_1(U_{R[1/\ell]}) \to \mathrm{O}(V_\ell)$$

be the representation obtained by composing ρ_ℓ with the obvious reduction map.

1.3.2. *Compatibility.* Take any R-algebra k that is a finite field and take any point $u \in U(k)$. Let $\bar{k}$ be a fixed algebraic closure of k. For a prime $\ell \in \Sigma$ that is invertible in k, we have $u \in U(k) = U_{R[1/\ell]}(k)$. Viewing u as a morphism $\operatorname{Spec} k \to U_{R[1/\ell]}$, we obtain a group homomorphism $\operatorname{Gal}(\bar{k}/k) = \pi_1(\operatorname{Spec} k) \to \pi_1(U_{R[1/\ell]})$ and we denote by Frob_u the image of the Frobenius automorphism of the extension $\bar{k}/k$. Observe that Frob_u lies in a well-defined conjugacy class of $\pi_1(U_{R[1/\ell]})$. In particular, the polynomial

$$P_u(T) := \det(I - \rho_\ell(\operatorname{Frob}_u)T)$$

is well-defined and has coefficients in $\mathbb{Z}_\ell$.

We shall further assume that the family of representations $\{\rho_\ell\}_{\ell \in \Sigma}$ are compatible, i.e., the above polynomial $P_u(T)$ lies in $\mathbb{Q}[T]$ and does not depend on the choice of ℓ. From our compatibility assumption, the rank of M_ℓ as a $\mathbb{Z}_\ell$-module does not depend on ℓ; denote this common rank by N. We shall assume that $N > 2$.

Since $\rho_\ell(\operatorname{Frob}_u)$ lies in $\mathrm{O}(M_\ell)$, we have

$$T^N P_u(1/T) = \varepsilon_u P_u(T), \tag{1.3}$$

where $\varepsilon_u := \det(-\rho_\ell(\operatorname{Frob}_u)) \in \{\pm 1\}$. From our compatibility assumption, the sign ε_u does not depend on the choice of ℓ.

[1] The definitions of orthogonal spaces and orthogonal groups are recalled in §2.1.

1.3.3. *Big monodromy.* For each prime $\ell \in \Sigma$, let $\mathrm{O}_{\mathcal{V}_\ell}$ be the orthogonal group of $\mathcal{V}_\ell$ as an algebraic group over $\mathbb{Q}_\ell$. For each field k that is an $R[1/\ell]$-algebra, we can view $\rho_\ell(\pi_1(U_{\bar{k}}))$ as a subgroup of $\mathrm{O}_{\mathcal{V}_\ell}(\mathbb{Q}_\ell) = \mathrm{O}(\mathcal{V}_\ell)$, where $\bar{k}$ is a fixed algebraic closure of k.

We now make an additional "big monodromy" assumption. Assume that one of the following holds:

(a) The ring R has characteristic 0 and for any finite field k that is a an R-algebra, the Zariski closure of $\rho_\ell(\pi_1(U_{\bar{k}}))$ in $\mathrm{O}_{\mathcal{V}_\ell}$ is either $\mathrm{SO}_{\mathcal{V}_\ell}$ or $\mathrm{O}_{\mathcal{V}_\ell}$ for a set of primes $\ell \in \Sigma$ with Dirichlet density 1.

(b) There is a subset $\Lambda \subseteq \Sigma$ with Dirichlet density 1 such that for any finite field k that is an R-algebra, we have
$$\bar{\rho}_\ell(\pi_1(U_{\bar{k}})) \supseteq \Omega(V_\ell)$$
for all primes $\ell \in \Lambda$ that are not equal to the characteristic of k, where $\Omega(V_\ell)$ is the commutator subgroup of $\mathrm{O}(V_\ell)$.

In fact, condition (a) implies condition (b), see Corollary 3.4.

1.3.4. *The field K.* Suppose that N is even. We shall prove in §4 that there is a unique extension $K/\mathbb{Q}$ of degree at most 2 such that for all sufficiently large $\ell \in \Sigma$, the prime ℓ splits in K if and only if the orthogonal space V_ℓ is split (in the sense of §2.2).

Consider any point $u \in U(k)$ with k a finite field that is an R-algebra. Let Δ_u be the discriminant of P_u. If $\varepsilon_u = 1$ and P_u is separable, then $K = \mathbb{Q}(\sqrt{\Delta_u})$, cf. Proposition 4.1.

1.4. **Main result.** Fix notation and assumptions as in §1.3. Take any $u \in U(k)$, where k is an R-algebra that is a finite field. Let $\mathrm{Gal}(P_u)$ be the Galois group of a splitting field of P_u over $\mathbb{Q}$. From §1.1 and (1.3), we find that $\mathrm{Gal}(P)$ is isomorphic to a subgroup of W_{N-1} if N is odd, W_{N-2} if N is even and $\varepsilon_u = -1$, and W_N if N is even and $\varepsilon_u = 1$.

Suppose that N is even, $\varepsilon_u = 1$ and P_u is separable. If $K = \mathbb{Q}$, then the discriminant Δ_u of P_u is a square and hence $\mathrm{Gal}(P_u)$ is isomorphic to a subgroup of W_N^+.

The following theorem describes the Galois group $\mathrm{Gal}(P_u)$ for a "random" $u \in U(k)$. The group $\mathrm{Gal}(P_u)$ is usually as large as possible given the constraints discussed above.

Theorem 1.4. *For a finite field k that is an R-algebra, we define $\delta(k)$ to be the proportion of $u \in U(k)$ for which we have*
$$\mathrm{Gal}(P_u) \cong \begin{cases} W_{N-1} & \text{if } N \text{ is odd,} \\ W_{N-2} & \text{if } N \text{ is even and } \varepsilon_u = -1, \\ W_N & \text{if } N \text{ is even, } \varepsilon_u = 1 \text{ and } K \neq \mathbb{Q}, \\ W_N^+ & \text{if } N \text{ is even, } \varepsilon_u = 1 \text{ and } K = \mathbb{Q} \end{cases} \tag{1.4}$$
(and set $\delta(k) = 0$ when $U(k)$ is empty). Then
$$\lim_{k,\,|k|\to\infty} \delta(k) = 1,$$
where the limit is over finite fields k that are R-algebras with increasing cardinality.

Remark 1.5.

(i) Theorem 1.4 answers a question of Katz on what the maximal Galois groups are, see the end of §1 of [Kat12] where it is asked in the setting of elliptic curves (which we will discuss in §1.6). Katz's guess is the same as (1.4) except he predicts that W_N^+ is the group for N even and $\varepsilon_u = 1$.

(ii) Jouve proved a special case of Theorem 1.4, in the context of elliptic curves, where he showed that $\mathrm{Gal}(P_u)$ is either equal to W_{2n} or W_{2n}^+ for the appropriate n. See Remark 1.11 for the precise result.

1.5. **An effective version.** Fix notation and assumptions as in §1.3. Now assume that $R = \mathbb{F}_q$ is a finite field with odd cardinality and that U is a smooth affine curve over $\mathbb{F}_q$ that is geometrically integral. Let $C/\mathbb{F}_q$ be the smooth projective curve that contains U as a Zariski open subvariety. Let g be the genus of C and let b be the number of points in the set $C(\overline{\mathbb{F}}_q) - U(\overline{\mathbb{F}}_q)$.

We also assume that condition (b) of §1.3 holds with a set of primes Λ having *natural* density 1. Finally, we assume that the representations $\{\bar{\rho}_\ell\}_{\ell \in \Sigma}$ are all tamely ramified.

In this special setting, the following gives an effective version of Theorem 1.4.

Theorem 1.6. *For all $n \geq 1$, we have*

$$\delta(\mathbb{F}_{q^n}) = 1 + O\Big(2^{2g+b}(2g+b)\, q^{-n/(N^2-N+6)} \log(q^n)\Big),$$

where the implicit constant depends only on Σ.

In particular, note that $1 - \delta(\mathbb{F}_{q^n})$ decays exponentially as a function of $n \geq 1$. This strengthens a result of Jouve that we will recall in Remark 1.11.

1.6. **Example: L-functions of twists of an elliptic curve.** Fix an elliptic curve E defined over the function field $\mathbb{F}_q(t)$, where q is a power of a prime $p \geq 5$. Assume that E has multiplicative reduction at some place $v \neq \infty$ of $\mathbb{F}_q(t)$, where ∞ is the place of $\mathbb{F}_q(t)$ with uniformizer t^{-1}. Let $m(t)$ be the monic squarefree polynomial in $\mathbb{F}_q[t]$ whose irreducible factors correspond to the places $v \neq \infty$ for which $E/\mathbb{F}_q(t)$ has bad reduction.

Fix an integer $d \geq 1$. For each integer $n \geq 1$, define the set

$$U_d(\mathbb{F}_{q^n}) = \Big\{ u \in \mathbb{F}_{q^n}[t] : u \text{ squarefree},\ \deg(u) = d,\ \gcd(u, m) = 1 \Big\};$$

it will serve as a parameter space for quadratic twists of E. Identifying a polynomial with the tuple of its coefficients, we can view $U_d(\mathbb{F}_{q^n})$ as the $\mathbb{F}_{q^n}$-points of an open subvariety U_d of $\mathbb{A}^{d+1}_{\mathbb{F}_q}$.

Take any $u \in U_d(\mathbb{F}_{q^n})$ and let E_u be an elliptic curve over $\mathbb{F}_{q^n}(t)$ obtained by taking a quadratic twist of E by u (so if E is defined by a Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_q(t)$, then $E_u/\mathbb{F}_{q^n}(t)$ can be defined by $u \cdot y^2 = x^3 + ax + b$). Let v be a place of $\mathbb{F}_{q^n}(t)$ and let $\mathbb{F}_v$ be the corresponding residue field. When E_u has good reduction at v, we define the integer $a_v = q^{\deg v} + 1 - |E_u(\mathbb{F}_v)|$, where $E_u(\mathbb{F}_v)$ is the $\mathbb{F}_v$-points of a good model of E_u over the local ring at v and $\deg v$ is the degree of the field extension $\mathbb{F}_v/\mathbb{F}_q$. If E_u has bad reduction at v, define $a_v = 1$, -1 or 0 if E_u has split multiplicative, non-split multiplicative or additive reduction, respectively, at v. The L-function of the elliptic curve E_u over $\mathbb{F}_{q^n}(t)$ is the power series

$$L(T, E_u) := \prod_{v \text{ good}} (1 - a_v T^{\deg v} + q^{\deg v} T^{2\deg v})^{-1} \cdot \prod_{v \text{ bad}} (1 - a_v T^{\deg v})^{-1},$$

where the product is over the places v of $\mathbb{F}_{q^n}(t)$. Moreover, one can show that $L(T, E_u)$ is a polynomial (note that E_u is non-isotrivial since it is a quadratic twist of E which has multiplicative reduction at some place). Define the polynomial

$$P_u(T) := L(T/q^n, E_u) \in \mathbb{Q}[T].$$

The degree N_d of $P_u(T)$ depends only on E and d; we will give an explicit formula below. The functional equation of $L(T, E_u)$ says that

$$T^{N_d} P_u(1/T) = \varepsilon_u P_u(T)$$

for a unique $\varepsilon_u \in \{\pm 1\}$ called the root number of E_u.

For each place v of $\mathbb{F}_q(t)$, we can assign a Kodaira symbol to the elliptic curve E after base extending to the local field $\mathbb{F}_q(t)_v$; the symbol can be computed quickly using Tate's algorithm. For each place v of $\mathbb{F}_q(t)$, we define integers $f_v(E)$, $\gamma_v(E)$ and $b_v(E)$ using the following table.

Kodaira symbol at v	I_0	I_n $(n \geq 1)$	II	III	IV	I_0^*	I_n^* $(n \geq 1)$	IV^*	III^*	II^*
f_v	0	1	2	2	2	2	2	2	2	2
γ_v	1	$n/\gcd(2,n)$	1	1	3	1	$2/\gcd(2,n)$	3	1	1
b_v	0	0	1	1	1	0	1	1	1	1

The common degree of the polynomials $P_u(T)$ is

$$N_d = f_\infty(E_{t^d}) + \sum_{v \neq \infty} f_v(E) \deg v - 4 + 2d,$$

where the sum is over the places $v \neq \infty$ of $\mathbb{F}_q(t)$ and $E_{t^d}/\mathbb{F}_q(t)$ is the quadratic twist of E by t^d. We also define the integers

$$D_d := \gamma_\infty(E_{t^d}) \cdot \prod_{v \neq \infty} \gamma_v(E)^{\deg v} \quad \text{and} \quad B := \sum_{v \neq \infty} b_v(E) \deg v.$$

The following describes the Galois group of the L-function of $E_u/\mathbb{F}_{q^n}(t)$ when E is twisted by a "random" $u \in U_d(\mathbb{F}_{q^n})$.

Theorem 1.7. *Fix an integer $d \geq 1$ so that $N_d \geq \max\{6B, 3\}$. Assume further that $d \geq 2$ or that there is a place $v \neq \infty$ of $\mathbb{F}_q(t)$ for which E has Kodaira symbol I_0^*. For each $n \geq 1$, let $\delta(q^n)$ be the proportion of $u \in U_d(\mathbb{F}_{q^n})$ for which we have an isomorphism*

(1.5)
$$\mathrm{Gal}(P_u) = \mathrm{Gal}(L(T, E_u)) \cong \begin{cases} W_{N_d - 1} & \text{if } N_d \text{ is odd,} \\ W_{N_d - 2} & \text{if } N_d \text{ is even and } \varepsilon_u = -1, \\ W_{N_d} & \text{if } N_d \text{ is even, } \varepsilon_u = 1, \text{ and } (-1)^{N_d/2} D_d \text{ is not a square,} \\ W_{N_d}^+ & \text{if } N_d \text{ is even, } \varepsilon_u = 1, \text{ and } (-1)^{N_d/2} D_d \text{ is a square} \end{cases}$$

(and set $\delta(q^n) = 0$ when $U_d(\mathbb{F}_{q^n})$ is empty). Then $\delta(q^n) \to 1$ as $n \to \infty$.

Remark 1.8.

(i) Note that the conditions on d in Theorem 1.7 hold for all sufficiently large d; our constraint on d is used to apply a big monodromy theorem of Hall.

(ii) Using the work of Katz and Hall, we will verify that the polynomials P_u arise from representations as in the axiomatic setup of §1.3. The remaining task is to compute the associated field K from §1.3.4 when N_d is even; this is needed to distinguish the two possible cases when $\varepsilon_u = 1$.

(iii) Suppose that N_d is even and take any polynomial $u \in U_d(\mathbb{F}_{q^n})$ for which $\varepsilon_u = 1$ and P_u is separable. Denote the discriminant of P_u by Δ_u. One can show that the square class $\Delta_u \cdot (\mathbb{Q}^\times)^2$ is independent of the choice of u. Distinguishing the last two cases of (1.5) is a result of this square class being $(-1)^{N_d/2} D_d \cdot (\mathbb{Q}^\times)^2$.

How does one prove this? Using that P_u is reciprocal and separable, one can prove that

$$\begin{aligned} \Delta_u \cdot (\mathbb{Q}^\times)^2 &= (-1)^{N_d/2} P_u(1) P_u(-1) (\mathbb{Q}^\times)^2 \\ &= (-1)^{N_d/2} L(1/q^n, E_u)\, L(-1/q^n, E_u) \cdot (\mathbb{Q}^\times)^2 \\ &= (-1)^{N_d/2} L(1/q^n, E_u)\, L(1/q^n, E_{\alpha u}) \cdot (\mathbb{Q}^\times)^2, \end{aligned}$$

where $\alpha \in \mathbb{F}_{q^n}^\times$ is any choice of non-square. Since the values $L(1/q^n, E_u)$ and $L(1/q^n, E_{\alpha u})$ are non-zero, the Birch and Swinnerton-Dyer conjecture (BSD) give an explicit expression for them in terms of interesting invariants of E_u and $E_{\alpha u}$, respectively. This part of BSD for elliptic curves over global function fields has been proved by Tate and Milne. Several of the invariants that arise, like the cardinality of the (finite!) Tate–Shafarevich group, are squares and hence do not need to be computed. Proving that $(-1)^{N_d/2}L(1/q^n, E_u)L(1/q^n, E_{\alpha u}) \in (-1)^{N_d/2}D_d \cdot (\mathbb{Q}^\times)^2$ is then essentially an application of the Tate algorithm. For details and background, see [Zyw14, §2.4]. The paper [Zyw14], which proves the Inverse Galois Problem for several groups of the form $\Omega(V_\ell)$, were motivated by these computations.

(iv) If N_d is even, then the integer $(-1)^{N_d/2}D_d$ depends only on the parity of d.

(v) Both possibilities for ε_u occur. Moreover, we have $|\{u \in U_d(\mathbb{F}_{q^n}) : \varepsilon_u = \varepsilon\}|/|U(\mathbb{F}_{q^n})| \to 1/2$ as $n \to \infty$ for each $\varepsilon \in \{\pm 1\}$, cf. Remark 9.2.

Example 1.9. As an example consider a prime $q = p \geq 5$ and let $E/\mathbb{F}_p(t)$ be the elliptic curve defined by $y^2 = x(x-1)(x-t)$. Fix an integer $d \geq 2$.

The only places $v \neq \infty$ of $\mathbb{F}_p(t)$ for which E has bad reduction are those with uniformizers t and $t-1$, and the Kodaira symbol is I_2 at both places. The elliptic curve E_{t^d} has bad reduction at ∞ and the Kodaira symbol is I_2 when d is odd and I_2^* when d is even. We thus have $N_d = 2d-1$ if d is odd and $N_d = 2d$ if d is even. We have $B = 0$ and $d \geq 2$, so the conditions of Theorem 1.7 hold. When N_d is even, equivalently d is even, we have $D_d = 1$ and hence $(-1)^{N_d/2}D_d = (-1)^d = 1$.

The set $U_d(\mathbb{F}_{p^n})$ consists of all separable degree d polynomials $u \in \mathbb{F}_{p^n}[t]$ with $u(0)u(1) \neq 0$. If d is even and $u \in U_d(\mathbb{F}_{p^n})$, one can show that $\varepsilon_u = 1$ if and only if $u(0)u(1)$ is a square in $\mathbb{F}_{p^n}^\times$; we can express ε_u as a product of local root numbers that are easy to compute, cf. [CCH05, Theorem 3.1]. For each $n \geq 1$, let $\delta(p^n)$ be the proportion of $u \in U_d(\mathbb{F}_{p^n})$ for which we have an isomorphism

$$\mathrm{Gal}(P_u) \cong \begin{cases} W_{2d-2} & \text{if } d \text{ is odd or if } d \text{ is even and } u(0)u(1) \text{ is not a square in } \mathbb{F}_{p^n}^\times, \\ W_{2d}^+ & \text{if } d \text{ is even and } u(0)u(1) \text{ is a square in } \mathbb{F}_{p^n}^\times. \end{cases}$$

Theorem 1.7 in this case says that $\delta(p^n) \to 1$ as $n \to \infty$.

We now give an explicit version where we restrict to certain 1 dimension subvarieties of U_d.

Theorem 1.10. *Fix an integer $d \geq 1$ as in Theorem 1.7 and fix a polynomial $g(t) \in U_{d-1}(\mathbb{F}_q)$. Let $\delta(q^n)$ be the proportion of $c \in \mathbb{F}_{q^n}$ for which the polynomial $u := (t-c)g(t) \in \mathbb{F}_{q^n}[t]$ is squarefree and relatively prime to $m(t)$, and for which the Galois group $\mathrm{Gal}(P_u) = \mathrm{Gal}(L(T, E_u))$ satisfies (1.5). Then*

$$\delta(q^n) = 1 + O\Big(2^{\deg m + d}(\deg m + d)\, q^{-n/(N_d^2 - N_d + 6)} \log(q^n)\Big),$$

where the implicit constant depends only on the j-invariant of E.

Remark 1.11. Theorem 1.10 is a strengthening of the main result of Jouve, cf. [Jou09, Theorem 4.3]. Jouve bounds the number of $c \in \mathbb{F}_q$ with $m(c)g(c) \neq 0$ such that $\mathrm{Gal}\Big(L(T, E_{(t-c)g(t)}/\mathbb{F}_q(t))\Big)$ does not equal the appropriate Galois group W_{2n} or its subgroup W_{2n}^+. Jouve obtains a bound of the form

$$O\Big(N_d^2\, |G|\, q^{1-1/(3.5N_d^2 - 3.5N_d + 2)} \log q\Big)$$

for d sufficiently large, where the implicit constant depends only on the j-invariant of E and G is a certain finite group. A bound for $|G|$ is not given in [Jou09] but one can show that $|G| \leq 2^{\deg m + d}$ using the approach of Lemma 7.1.

We will prove Theorems 1.7 and 1.10 in §9 by applying the axiomatic setup of §1.3 and §1.5.

1.7. **Some related results.** This paper was motivated by the work of Chavdarov for which we now recall a special case. Let U be a geometrically irreducible variety over $\mathbb{F}_q$ of positive dimension. Consider a compatible family of continuous representations $\{\rho_\ell\}_\ell$ with $\rho_\ell\colon \pi_1(U) \to \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. For each $u \in U(\mathbb{F}_{q^n})$, let $P_u \in \mathbb{Q}[T]$ be the corresponding polynomial of degree $2g$ arising from the representations ρ_ℓ. We also make a *big monodromy* assumption: suppose that the image of $\rho_\ell(\pi_1(U_{\overline{\mathbb{F}}_q}))$ modulo ℓ is $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ for all sufficiently large ℓ.

Let $\delta(q^n)$ be the proportion of $u \in U(\mathbb{F}_{q^n})$ for which the Galois group of P_u is isomorphic to W_{2g}. We then have $\delta(q^n) \to 1$ as $n \to \infty$ by [Cha97, Theorem 2.1]. Note the description of $\mathrm{Gal}(P_u)$ for a "random" u is much simpler than that of Theorem 1.4. One key reason is that the algebraic groups GSp_{2g} and Sp_{2g} that arise in Chavdarov's work are connected, while orthogonal groups are not connected. Also the group Sp_{2g} is simply connected, while special orthogonal groups are not.

Katz has proved a theorem similar to Theorem 1.4, in the setting of L-functions of elliptic curves, except showing that P_u with the obvious linear factors removed is irreducible, cf. [Kat12, Theorem 4.1].

As noted in Remark 1.11, Jouve proved an analogue of Theorem 1.6, in the setting of L-functions of elliptic curves, showing that the Galois group of P_u for a "random" u is isomorphic to either W_{2n}^+ or W_{2n} for an appropriate n. One of the main motivations of this paper is to distinguish between these two cases.

1.8. **Overview.** We now give a brief overview. In §2, we describe some basic facts about orthogonal spaces and groups. In particular in §2.4, we study the cardinality of certain conjugacy classes of orthogonal groups over finite fields. When N is even, the field K from §1.3.4 will be discussed in §4.

Fix notation and assumptions as in §1.3. Consider a polynomial $P_u \in \mathbb{Q}[T]$. At the beginning of §1.4, we have given some constraint on the group $\mathrm{Gal}(P_u)$. How do we show that $\mathrm{Gal}(P_u)$ satisfies (1.4), i.e., is as large as possible? The idea is fundamental to Galois theory; we will consider the reduction of P_u modulo various primes ℓ and compute how it factors in $\mathbb{F}_\ell[T]$. If we see enough different kinds of factorizations, we will be able to prove that $\mathrm{Gal}(P_u)$ is as large as possible. The following proposition, which we will prove in §5, is a key ingredient in the proof of our main theorems.

Proposition 1.12. *For each $\ell \in \Sigma$, there are subsets $C_1(V_\ell), \ldots, C_6(V_\ell)$ of $\mathrm{O}(V_\ell)$ such that the following hold:*

(i) *$C_i(V_\ell)$ is stable under conjugation by $\mathrm{O}(V_\ell)$.*

(ii) *There are positive absolute constants c_1 and c_2 such that if $\ell \in \Sigma$ satisfies $\ell \geq c_1$, then*

$$\frac{|C_i(V_\ell) \cap \kappa|}{|\kappa|} \geq \frac{c_2}{N^2}$$

for all cosets κ of $\Omega(V_\ell)$ in $\mathrm{O}(V_\ell)$ and all integers $1 \leq i \leq 6$.

(iii) *Take any $u \in U(k)$, where k is a finite field that is an R-algebra. Suppose that for each $1 \leq i \leq 6$ there is a prime $\ell \in \Sigma$, not equal to the characteristic of k, such that $\bar{\rho}_\ell(\mathrm{Frob}_u) \subseteq C_i(V_\ell)$. Then the Galois group of $P_u(T)$ satisfies (1.4).*

The representations $\{\rho_\ell\}$ are not independent, i.e., a condition imposed on P_u modulo one prime can restrict the possible reductions modulo other primes. In §3, we use our big monodromy assumption, and some group theory, to show that the image of the representation $\prod_{\ell \in D} \bar{\rho}_\ell$ is large for all finite subsets $D \subseteq \Lambda$, where Λ is an appropriate subset of Σ with Dirichlet density 1. This controls how dependent the representations ρ_ℓ are.

Theorem 1.4 and Theorem 1.6 will be proved in §6 and §7, respectively. Our examples from §1.2 and §1.6, will be proved in §8 and §9, respectively. In Appendix A, we state a general version of Selberg's sieve. For convenience, we state some equidistribution bounds in Appendix B.

Acknowledgements. Thanks to the referee who made several suggestions that have improved the exposition.

2. Orthogonal groups and characteristic polynomials

2.1. **Orthogonal spaces.** Let R be an integral domain whose characteristic is not 2. An orthogonal space M over R is a free R-module M of finite rank equipped with a symmetric R-bilinear pairing $\langle\ ,\ \rangle\colon M \times M \to R$ which induces an isomorphism $M \to \operatorname{Hom}_R(M,R)$, $m \mapsto \langle m, \cdot\rangle$.

A homomorphism of orthogonal spaces is an R-module homomorphism that is compatible with the respective pairings. The orthogonal group of M, denoted by $\mathrm{O}(M)$, is the group of automorphisms of the orthogonal space M. Let $\mathrm{SO}(M)$ be the kernel of the determinant map $\det\colon \mathrm{O}(M) \to \{\pm 1\}$.

2.2. **Finite fields.** Fix a finite field $\mathbb{F}$ with odd characteristic. Let V be an orthogonal space over $\mathbb{F}$ of dimension $N \geq 1$. For each $v \in V$ with $\langle v, v\rangle \neq 0$, we have a reflection $r_v \in \mathrm{O}(V)$ defined by $x \mapsto x - 2\langle x, v\rangle / \langle v, v\rangle \cdot v$. Let

$$\mathrm{sp}_V\colon\ \mathrm{O}(V) \to \mathbb{F}^\times/(\mathbb{F}^\times)^2$$

be the spinor norm. The spinor norm is a homomorphism that can be characterized by the property that it is satisfies $\mathrm{sp}_V(r_v) = \langle v, v\rangle \cdot (\mathbb{F}^\times)^2$ for all $v \in V$ with $\langle v, v\rangle \neq 0$. We will denote sp_V by sp if V is clear from context. We define $\Omega(V)$ to be the subgroup of $\mathrm{O}(V)$ that is the simultaneous kernels of the homomorphisms $\det\colon \mathrm{O}(V) \to \{\pm 1\}$ and $\mathrm{sp}_V\colon\ \mathrm{O}(V) \to \mathbb{F}^\times/(\mathbb{F}^\times)^2$.

The discriminant of V, denoted by $\operatorname{disc}(V)$, is the coset in $\mathbb{F}^\times/(\mathbb{F}^\times)^2$ represented by $\det(\langle v_i, v_j\rangle)$, where $v_1, \ldots, v_N$ is any basis of V over $\mathbb{F}$. Up to isomorphism, there are two orthogonal spaces of dimension N over $\mathbb{F}$; these orthogonal spaces are distinguishable by their discriminants. When N is even, it will be especially important to distinguish these two spaces (for example when N is odd, the group $\Omega(V)$, up to isomorphism, depends only on N and $\mathbb{F}$; this fails for even N). If N is even, we say that V is split if $\operatorname{disc}(V) = (-1)^{N/2}(\mathbb{F}^\times)^2$ and non-split otherwise.

Lemma 2.1. *We have* $\operatorname{disc}(V) = \mathrm{sp}_V(-I)$.

Proof. Let $v_1, \ldots, v_N$ be an orthogonal basis of V. We have $-I = r_{v_1} r_{v_2} \cdots r_{v_N}$, so

$$\operatorname{disc}(V) = \det(\langle v_i, v_j\rangle) \cdot (\mathbb{F}^\times)^2 = \textstyle\prod_i \langle v_i, v_i\rangle \cdot (\mathbb{F}^\times)^2 = \prod_i \mathrm{sp}(r_{v_i}) = \mathrm{sp}(-I). \qquad \square$$

The following lemma recalls some basic facts about these groups; see [ATLAS, §2.4] for a good exposition of the groups $\Omega(V)$; proofs can be found in §3.7 and §3.11 of [Wil09] for $N \neq 5$ and $N = 4$, respectively.

Lemma 2.2. *Suppose that $N \geq 3$ and $q > 3$. Let Z be the center of $\Omega(V)$.*

(i) *The map* $\det \times \mathrm{sp}\colon\ \mathrm{O}(V)/\Omega(V) \to \{\pm 1\} \times \mathbb{F}^\times/(\mathbb{F}^\times)^2$ *is an isomorphism.*
(ii) *The group Z is either $\{I\}$ or $\{\pm I\}$.*
(iii) *The group $\Omega(V)/Z$ is simple except when $N = 4$ and V is split.*
(iv) *If $N = 4$ and V is split, then* $\Omega(V)/Z \cong \mathrm{PSL}_2(\mathbb{F}) \times \mathrm{PSL}_2(\mathbb{F})$.
(v) *The group $\Omega(V)$ is perfect, i.e., it equals its own commutator subgroup. In particular, $\Omega(V)$ is the commutator subgroup of* $\mathrm{O}(V)$.

Remark 2.3. We now give an alternate description of the group $\Omega(V)$. Let SO_V be the obvious algebraic group over $\mathbb{F}$; it is semisimple and has a simply connected cover $\pi\colon G \to \mathrm{SO}_V$. The group $\Omega(V)$ is equal to $\pi(G(\mathbb{F}))$.

Remark 2.4. We gave an alternate definition of $\Omega(V_\ell)$ in condition (b) in §1.3.3. Since $\ell \geq 5$ and $N > 2$, these definitions agree by Lemma 2.2(v).

The following lemma allows to compute the spinor norm for some elements in $\mathrm{O}(V)$ directly from their characteristic polynomials.

Lemma 2.5. *Take any $A \in \mathrm{O}(V)$ and set $P(T) = \det(I - AT)$.*

(i) *If $P(-1) \neq 0$, then $\mathrm{sp}(A) = 2^N P(-1)(\mathbb{F}^\times)^2$.*
(ii) *If $P(1) \neq 0$, then $\mathrm{sp}(A) = 2^N P(1)\,\mathrm{disc}(V)$.*
(iii) *If $P(1) \neq 0$ and $P(-1) \neq 0$, then $\mathrm{disc}(V) = P(1)P(-1)(\mathbb{F}^\times)^2$.*

Proof. If $P(-1) \neq 0$, then Zassenhaus [Zas62, p.446] shows that $\mathrm{sp}(A)$ equals

$$\det((I+A)/2)(\mathbb{F}^\times)^2 = 2^N \det(I+A)(\mathbb{F}^\times)^2 = 2^N P(-1)(\mathbb{F}^\times)^2.$$

This gives (i), and part (ii) follows by applying (i) with the matrix $-A$ and using Lemma 2.1. Finally, (iii) follows directly from (i) and (ii). □

Take any $A \in \mathrm{O}(V)$ and define $P(T) = \det(I - AT)$. We have

$$T^N P(1/T) = \det(-A)P(T) = (-1)^N \det(A)P(T). \tag{2.1}$$

Substituting 1 and -1 into (2.1), we have $P(1) = (-1)^N \det(A)P(1)$ and $P(-1) = \det(A)P(-1)$. So P is divisibly by $1-T$ if $\det(A) = (-1)^{N+1}$ and by $1+T$ if $\det(A) = -1$. Removing these obvious linear factors from P, we have the polynomial

$$f(T) := \begin{cases} P(T) & \text{if } N \text{ is even and } \det(A) = 1, \\ P(T)/(1-T^2) & \text{if } N \text{ is even and } \det(A) = -1, \\ P(T)/(1-\det(A)T) & \text{if } N \text{ is odd.} \end{cases}$$

Using (2.1), we find that $f(T) \in \mathbb{F}[T]$ is reciprocal, i.e., $T^{\deg f} f(1/T) = f(T)$. The polynomial $f(T)$ is monic and has even degree.

2.3. **Reciprocal polynomials.**

Lemma 2.6. *Fix a field K whose characteristic is not 2. Let $f \in K[T]$ be a monic reciprocal polynomial of even degree $2n \geq 2$.*

(i) *We have $f(T) = T^n h(T + 1/T)$ for a unique polynomial $h \in K[T]$. The polynomial h is monic of degree n.*
(ii) *We have*

$$\mathrm{disc}(f) = (-1)^n f(1)f(-1)\,\mathrm{disc}(h)^2 = h(2)h(-2)\,\mathrm{disc}(h)^2. \tag{2.2}$$

In particular, f is separable if and only if h is separable and $h(2)h(-2) \neq 0$.

(iii) *Suppose that $K = \mathbb{F}$ is a finite field. Further suppose that h is irreducible and $h(2)h(-2) \neq 0$.*
   - *If $h(2)h(-2)$ is not a square in $\mathbb{F}$, then f is irreducible of degree $2n$ in $\mathbb{F}[T]$.*
   - *If $h(2)h(-2)$ is a square in $\mathbb{F}$, then f is the product of two irreducible polynomials of degree n in $\mathbb{F}[T]$.*

Proof. See [AV08, Lemma 6] for the existence in part (i); the uniqueness is clear. Denote the discriminant of f and h by $\mathrm{disc}(f)$ and $\mathrm{disc}(h)$, respectively. It is straightforward to show that

$$\mathrm{disc}(f) = (-1)^n f(1)f(-1)\,\mathrm{disc}(h)^2 = h(2)h(-2)\,\mathrm{disc}(h)^2, \tag{2.3}$$

see [AV08, §3] for example. Part (ii) is now immediate from (2.3)

Now suppose that $h \in \mathbb{F}[T]$ is irreducible and satisfies $h(\pm 2) \neq 0$. From part (ii), f is separable. Let $\alpha \in \overline{\mathbb{F}}$ be any root of f; we have $\alpha \neq 0$ since f is reciprocal. The extension $\mathbb{F}(\alpha + \alpha^{-1})/\mathbb{F}$

has degree n since $\alpha + \alpha^{-1}$ is a root of h and h is irreducible of degree n. The extension $\mathbb{F}(\alpha)/\mathbb{F}$ thus has degree n or $2n$. Since α was an arbitrary root of f, we find that f is either irreducible of degree $2n$ or the product of two irreducible polynomials of degree n. From [AV08, Theorem 7], we deduce that f is irreducible if and only if $(-1)^n f(1)f(-1) = h(2)h(-2)$ is not a square in $\mathbb{F}$. □

2.4. **Counting elements with a given separable characteristic polynomial.** Fix an orthogonal space V of dimension $N \geq 2$ over a finite field $\mathbb{F}$ with odd cardinality q.

In this section, we give an explicit formula for the number of $A \in \mathrm{O}(V)$ for which $\det(I - AT)$ is equal to a fixed *separable* polynomial in $\mathbb{F}[T]$. These computations are of independent interest.

Fix an integer $n \geq 1$ and a monic, separable and reciprocal polynomial $f \in \mathbb{F}[T]$ of degree $2n$. There is a unique (monic) polynomial $h \in \mathbb{F}[T]$ of degree n such that $f(T) = T^n h(T + 1/T)$. From Lemma 2.6(ii) and the assumption that f is separable, we find that h is separable and $h(2)h(-2) = (-1)^n f(1)f(-1)$ is non-zero.

Let $h_1, \ldots, h_r \in \mathbb{F}[T]$ be the monic irreducible factors of h. Define $e_i = 1$ if $h_i(2)h_i(-2) \in \mathbb{F}$ is a square, otherwise set $e_i = -1$.

Proposition 2.7. *Let V be an orthogonal space of even dimension $N = 2n$ over $\mathbb{F}$. Let C be the set of $A \in \mathrm{O}(V)$ for which $\det(I - AT) = f(T)$.*

(i) *If $\mathrm{disc}(V) \neq f(1)f(-1)(\mathbb{F}^\times)^2$, then $C = \emptyset$.*

(ii) *If $\mathrm{disc}(V) = f(1)f(-1)(\mathbb{F}^\times)^2$, then C is a conjugacy class of $\mathrm{O}(V)$ and*

$$|C|/|\mathrm{O}(V)| = q^{-n} \prod_{i=1}^{r} (1 - e_i/q^{\deg h_i})^{-1}.$$

We have $\det(A) = 1$ and $\mathrm{sp}(A) = f(-1)(\mathbb{F}^\times)^2$ for all $A \in C$.

Proof. We use the background material in Appendix A of [GM02] which holds for a general field whose characteristic is not 2. Any $A \in \mathrm{O}(V)$ with $\det(I - A) = f(T)$ has determinant 1 since $f(T)$ is reciprocal.

Consider pairs (V, A) consisting of an orthogonal space V over $\mathbb{F}$ with an automorphism $A \in \mathrm{SO}(V)$. We say that two such pairs (V, A) and (V', A') are *equivalent* if there is an isomorphism $B\colon V \to V'$ of orthogonal spaces for which $A' = B \circ A \circ B^{-1}$. Let $\mathcal{V}(f)$ be the set of equivalence classes of pairs (V, A) for which $\det(I - AT) = f(T)$.

We have an extension of $\mathbb{F}$-algebras K/k, where $K = \mathbb{F}[x]/(f(x))$, $k = \mathbb{F}[y]/(h(y))$ and $y = x + x^{-1}$. Since $f(x)$ and $h(y)$ are separable, the algebras K and k will be products of finite extensions of $\mathbb{F}$. Let $\iota\colon K \to K$ be the automorphism which fixes k and satisfies $\iota(x) = x^{-1}$. Let $N_{K/k}\colon K \to k$ be the norm map $\alpha \mapsto \alpha \cdot \overline{\alpha}$, where we set $\overline{\alpha} = \iota(\alpha)$.

For each $\xi \in k^\times$, define the $\mathbb{F}$-vector space $V_\xi := K$ and endow it with the $\mathbb{F}$-valued pairing $\langle \alpha, \beta \rangle_\xi = \mathrm{Tr}_{K/\mathbb{F}}(\xi \alpha \overline{\beta})$. With this bilinear form, V_ξ is an orthogonal space of dimension $2n$ over $\mathbb{F}$. The map $A_\xi\colon K \to K$ defined by $A_\xi(\alpha) = x\alpha$ is an automorphism of the orthogonal space V_ξ. By construction, we have $\det(I - A_\xi T) = f(T)$. If $\xi, \lambda \in k^\times$ satisfy $\xi\lambda^{-1} = N_{K/k}(\delta)$ for some $\delta \in K^\times$, then the map $B : K \to K$ defined by $B(\alpha) = \delta\alpha$ gives an equivalence between (V_ξ, A_ξ) and (V_λ, A_λ). We thus have a well-defined map

$$\phi\colon k^\times / N_{K/k}(K^\times) \to \mathcal{V}(f), \quad \xi \mapsto (V_\xi, A_\xi).$$

The map ϕ is a bijection by [GM02, Theorem A.2].

Since $\mathbb{F}$ is finite and K and k are the product of finite extension fields of $\mathbb{F}$, we know that $N_{K/k}\colon K^\times \to k^\times$ is surjective and hence $|\mathcal{V}(f)| = 1$. So there is a pair (V, A), unique up to equivalence, that satisfies $\det(I - AT) = f(T)$. In particular, the set C of $B \in \mathrm{SO}(V)$ with $\det(I - BT) = f(T)$ is the conjugacy class of A in $\mathrm{O}(V)$. By Lemma 2.5(iii), we have $\mathrm{disc}(V) =$

$f(1)f(-1)(\mathbb{F}^\times)^2$ and hence the uniqueness of the equivalence class (V,A) gives part (i). We have $\operatorname{sp}(A) = f(-1)(\mathbb{F}^\times)^2$ by Lemma 2.5(i). It remains to compute $|C|/|\operatorname{O}(V)|$.

Since C is the conjugacy class of A in $\operatorname{O}(V)$, we have

$$|C|/|\operatorname{O}(V)| = |\{B \in \operatorname{O}(V) : \det(I - BT) = f(T)\}|/|\operatorname{O}(V)| = 1/|\operatorname{Cent}_{\operatorname{O}(V)}(A)|.$$

We have $\operatorname{Cent}_{\operatorname{O}(V)}(A) \cong \ker(N_{K/k}\colon K^\times \to k^\times)$ by [GM02, Theorem A.2] . For $1 \le i \le r$, define $f_i(T) := T^{\deg h_i} h_i(T + 1/T)$. We thus have

$$\operatorname{Cent}_{\operatorname{O}(V)}(A) \cong \prod\nolimits_{i=1}^r \ker(N_{K_i/k_i}\colon K_i^\times \to k_i^\times),$$

where we have the extension of $\mathbb{F}$-algebras K_i/k_i with $K_i := \mathbb{F}[x]/(f_i(x))$ and $k_i := \mathbb{F}[y]/(h_i(y))$. Since $N_{K/k}\colon K^\times \to k^\times$ is surjective, we have $|\operatorname{Cent}_{\operatorname{O}(V)}(A)| = \prod_{i=1}^r |K_i^\times|/|k_i^\times|$.

Suppose that $e_i = -1$, and hence $f_i(T)$ is irreducible by Lemma 2.6(iii). Then K_i/k_i is a quadratic extension of finite fields, so $|K_i^\times|/|k_i^\times| = |k_i| + 1 = q^{\deg h_i} + 1 = q^{\deg h_i}(1 - e_i/q^{\deg h_i})$.

Suppose that $e_i = 1$, and hence $f_i(T)$ is the product of two irreducible polynomials of degree $\deg h_i$ by Lemma 2.6(iii). Then K_i is isomorphic to the product of two fields isomorphic to k_i, so $|K_i^\times|/|k_i^\times| = |k_i| - 1 = q^{\deg h_i} - 1 = q^{\deg h_i}(1 - e_i/q^{\deg h_i})$.

Therefore, $|C|/|\operatorname{O}(V)|$ equals

$$1/|\operatorname{Cent}_{\operatorname{O}(V)}(A)| = \Big(\prod\nolimits_{i=1}^r q^{\deg h_i}(1 - e_i/q^{\deg h_i})\Big)^{-1} = q^{-n}\prod\nolimits_{i=1}^r (1 - e_i/q^{\deg h_i})^{-1}. \qquad \square$$

Proposition 2.8. *Let V be an orthogonal space of dimension $2n+2$ over $\mathbb{F}$ and fix a coset $\beta \in \mathbb{F}^\times/(\mathbb{F}^\times)^2$. Let C_β be the set of $A \in \operatorname{O}(V)$ for which $\det(I - AT) = (1 - T^2)f(T)$ and $\operatorname{sp}(A) = \beta$. Then C_β is a conjugacy class of $\operatorname{O}(V)$ and*

$$|C_\beta|/|\operatorname{O}(V)| = \frac{1}{4} q^{-n} \prod_{i=1}^r (1 - e_i/q^{\deg h_i})^{-1}.$$

Proof. Let V_1 be the orthogonal space of dimension $2n$ over $\mathbb{F}$ with $\operatorname{disc}(V_1) = f(1)f(-1)(\mathbb{F}^\times)^2$. Let V_2 and V_3 be orthogonal spaces of dimension 1 over $\mathbb{F}$ such that $\operatorname{disc}(V_2) = f(-1)\beta$ and $\operatorname{disc}(V_3) = f(1)\beta\operatorname{disc}(V)$. We have $\operatorname{disc}(V_1 \oplus V_2 \oplus V_3) = f(1)f(-1) \cdot f(-1)\beta \cdot f(1)\beta \operatorname{disc}(V) = \operatorname{disc}(V)$. Therefore, the orthogonal spaces V and $V_1 \oplus V_2 \oplus V_3$ are isomorphic; without loss of generality, assume that $V = V_1 \oplus V_2 \oplus V_3$.

By Proposition 2.7(ii), there is an $A_1 \in \operatorname{SO}(V_1)$ such that $\det(I - A_1T) = f(T)$ and $\operatorname{sp}(A_1) = f(-1)(\mathbb{F}^\times)^2$. Let $A \in \operatorname{O}(V)$ be the automorphism that acts as A_1 on V_1, $-I$ on V_2, and I on V_3. Therefore, $\det(I - AT) = f(T)(1+T)(1-T) = f(T)(1-T^2)$. We have

$$\operatorname{sp}(A) = \operatorname{sp}(A_1)\operatorname{sp}(-I_{V_2})\operatorname{sp}(I_{V_3}) = f(-1) \cdot \operatorname{sp}(-I_{V_2}) \cdot 1 = f(-1)\operatorname{disc}(V_2) = \beta,$$

where we have used Lemma 2.1. So A belongs to C_β.

Now take any $B \in C_\beta$. Let W_2 and W_3 be the (one-dimensional) eigenspaces of B corresponding to the eigenvalues -1 and 1, respectively. Let W_1 be the subspace of V perpendicular to W_2 and W_3. With the pairing from V, the W_i are orthogonal spaces and $V = W_1 \oplus W_2 \oplus W_3$. The automorphism B acts on W_1; denote by $B_1 \in \operatorname{O}(W_1)$ the restriction of B to W_1. We have $\beta = \operatorname{sp}(B) = \operatorname{sp}(B_1)\operatorname{sp}(-I_{W_2})\operatorname{sp}(I_{W_3}) = \operatorname{sp}(B_1)\operatorname{sp}(-I_{W_2}) = \operatorname{sp}(B_1)\operatorname{disc}(W_2)$. By Lemma 2.5, we have $\operatorname{sp}(B_1) = f(-1)(\mathbb{F}^\times)^2$ and $\operatorname{disc}(W_1) = f(1)f(-1)(\mathbb{F}^\times)^2$. Therefore, $\operatorname{disc}(W_2) = f(-1)\beta$ and $\operatorname{disc}(W_3) = \operatorname{disc}(V)\operatorname{disc}(W_1)\operatorname{disc}(W_2) = f(1)\beta\operatorname{disc}(V)$.

By comparing discriminants, we have isomorphisms $\varphi_1\colon V_1 \xrightarrow{\sim} W_1$, $\varphi_2\colon V_2 \xrightarrow{\sim} W_2$ and $\varphi_3\colon V_3 \xrightarrow{\sim} W_3$ of orthogonal spaces. By Proposition 2.7, we may take φ_1 so that $B_1 = \varphi_1 \circ A_1 \circ \varphi_1^{-1}$. The automorphisms $\varphi_1, \varphi_2, \varphi_3$ give rise to an automorphism $\varphi \in \operatorname{O}(V)$ such that $B = \varphi \circ A \circ \varphi^{-1}$. Therefore, C_β is a conjugacy class of $\operatorname{O}(V)$.

Since C_β is a conjugacy class of $\mathrm{O}(V)$, it has cardinality $|\mathrm{O}(V)|/|\operatorname{Cent}_{\mathrm{O}(V)}(A)|$. The above argument shows that $\operatorname{Cent}_{\mathrm{O}(V)}(A)$ is equal to

$$\operatorname{Cent}_{\mathrm{O}(V_1)}(A_1)\times\operatorname{Cent}_{\mathrm{O}(V_2)}(-I)\times\operatorname{Cent}_{\mathrm{O}(V_3)}(I)=\operatorname{Cent}_{\mathrm{O}(V_1)}(A_1)\times\{\pm I\}\times\{\pm I\}.$$

Therefore,

$$|C_\beta|/|\mathrm{O}(V)|=1/|\operatorname{Cent}_{\mathrm{O}(V)}(A)|=1/|\operatorname{Cent}_{\mathrm{O}(V_1)}(A_1)|\cdot 1/2\cdot 1/2=\tfrac{1}{4}q^{-n}\prod_{i=1}^{r}(1-e_i/q^{\deg h_i})^{-1},$$

where the last equality uses Proposition 2.7. □

Finally, we consider orthogonal spaces of odd dimension.

Proposition 2.9. *Let V be an orthogonal space of dimension $2n+1$ over $\mathbb{F}$. Fix an $\varepsilon\in\{\pm1\}$. Let C be the set of $A\in\mathrm{O}(V)$ for which $\det(I-AT)=(1-\varepsilon T)f(T)$. Then C is a conjugacy class of $\mathrm{O}(V)$ and*

$$|C|/|\mathrm{O}(V)|=\frac{1}{2}q^{-n}\prod_{i=1}^{r}(1-e_i/q^{\deg h_i})^{-1}.$$

For $A\in C$, we have $\det(A)=\varepsilon$, $\operatorname{sp}(A)=f(-1)(\mathbb{F}^\times)^2$ if $\varepsilon=1$ and $\operatorname{sp}(A)=f(1)\operatorname{disc}(V)$ if $\varepsilon=-1$.

Proof. Let V_1 and V_2 be the orthogonal spaces of dimension $2n$ and 1, respectively, over $\mathbb{F}$ with $\operatorname{disc}(V_1)=f(1)f(-1)(\mathbb{F}^\times)^2$ and $\operatorname{disc}(V_2)=f(1)f(-1)\operatorname{disc}(V)$. We have $\operatorname{disc}(V_1\oplus V_2)=\operatorname{disc}(V)$, so V and $V_1\oplus V_2$ are isomorphic. Without loss of generality, we may assume that $V=V_1\oplus V_2$.

By Proposition 2.7, there is an $A_1\in\mathrm{SO}(V_1)$ such that $\det(I-A_1T)=f(T)$. Let $A\in\mathrm{O}(V)$ be the automorphism that acts as A_1 on V_1 and as scalar multiplication by ε on V_2. Therefore, $\det(I-AT)=f(T)(1-\varepsilon T)$ and hence $A\in C$.

Now take any $B\in C$. Let W_2 be the (one-dimensional) eigenspace of B corresponding to the eigenvalue ε. Let W_1 be the subspace of V perpendicular to W_2. With the pairing from V, W_1 and W_2 are orthogonal spaces and $V=W_1\oplus W_2$. The automorphism B acts on W_1; denote by $B_1\in\mathrm{O}(W_1)$ the restriction of B to W_1.

By Proposition 2.7, we have $\operatorname{disc}(W_1)=f(1)f(-1)(\mathbb{F}^\times)^2$, so $\operatorname{disc}(V_1)=\operatorname{disc}(W_1)$. Therefore, $\operatorname{disc}(V_2)=\operatorname{disc}(V)\operatorname{disc}(V_1)$ equals $\operatorname{disc}(W_2)=\operatorname{disc}(V)\operatorname{disc}(W_1)$. So there are isomorphisms $\varphi_1\colon V_1\xrightarrow{\sim}W_1$ and $\varphi_2\colon V_2\xrightarrow{\sim}W_2$ of orthogonal spaces. By Proposition 2.7, we may take φ_1 so that $B_1=\varphi_1\circ A_1\circ\varphi_1^{-1}$. The automorphisms φ_1 and φ_2 give rise to an automorphism $\varphi\in\mathrm{O}(V)$ such that $B=\varphi\circ A\circ\varphi^{-1}$.

Therefore, C is a conjugacy class of $\mathrm{O}(V)$ containing A and hence has cardinality equal to $|\mathrm{O}(V)|/|\operatorname{Cent}_{\mathrm{O}(V)}(A)|$. The above argument shows that $\operatorname{Cent}_{\mathrm{O}(V)}(A)$ is equal to

$$\operatorname{Cent}_{\mathrm{O}(V_1)}(A_1)\times\operatorname{Cent}_{\mathrm{O}(V_2)}(\varepsilon I_{V_2})=\operatorname{Cent}_{\mathrm{O}(V_1)}(A_1)\times\{\pm I\}.$$

Therefore,

$$|C|/|\mathrm{O}(V)|=1/|\operatorname{Cent}_{\mathrm{O}(V_1)}(A_1)|\cdot 1/2=\tfrac{1}{2}q^{-n}\prod_{i=1}^{r}(1-e_i/q^{\deg h_i})^{-1},$$

where the last equality uses Proposition 2.7.

Finally, we compute $\operatorname{sp}(A)$. We have $\operatorname{sp}(A)=\operatorname{sp}(A_1)\operatorname{sp}(\varepsilon I_{V_2})=f(-1)\operatorname{sp}(\varepsilon I_{V_2})$, where the last equality uses Proposition 2.7. If $\varepsilon=1$, then $\operatorname{sp}(A)=f(-1)(\mathbb{F}^\times)^2$. We have $\operatorname{sp}(-I_{V_2})=\operatorname{disc}(V_2)=f(1)f(-1)\operatorname{disc}(V)$, so if $\varepsilon=-1$, then $\operatorname{sp}(A)=f(1)\operatorname{disc}(V)$. □

3. Big monodromy

Fix notation and assumptions as in §1.3. Let F be the fraction field of R. When R has characteristic 0, and hence F is a number field, we have $R = \mathcal{O}_F[S^{-1}]$ for a finite set S of non-zero prime ideals of $\mathcal{O}_F$.

For each finite subset D of Σ, define the representation

$$\bar{\rho}_D := \prod_{\ell \in D} \bar{\rho}_\ell \colon \pi_1(U_{R[D^{-1}]}) \to \prod_{\ell \in D} \mathrm{O}(V_\ell)$$

and the subgroup $G_D^g := \bar{\rho}_D(\pi_1(U_{\overline{F}}))$ of $\prod_{\ell \in D} \mathrm{O}(V_\ell)$. The goal of this section is to prove the following two propositions.

Proposition 3.1. *There is a subset $\Lambda \subseteq \Sigma$ with Dirichlet density 1 such that the inclusion*

$$\bar{\rho}_D(\pi_1(U_{\bar{k}})) \supseteq \prod_{\ell \in D} \Omega(V_\ell) \tag{3.1}$$

holds for all finite subsets $D \subseteq \Lambda$ and all finite fields k that are R-algebras with characteristic not in D. Moreover, $G_D^g \supseteq \prod_{\ell \in D} \Omega(V_\ell)$.

If R is a finite field and condition (b) in §1.3 holds, then we may take Λ to be the set of primes from condition (b).

Proposition 3.2. *Suppose that R has characteristic 0. There is a finite set $S' \supseteq S$ of non-zero prime ideals of $\mathcal{O}_F$ and a subset $\Lambda \subseteq \Sigma$ with Dirichlet density 1 such that*

$$\bar{\rho}_D(\pi_1(U_{\bar{k}})) = G_D^g \tag{3.2}$$

holds for all finite subsets $D \subseteq \Lambda$ and all finite fields k that are $\mathcal{O}_F[S'^{-1}]$-algebras with characteristic not in D.

Remark 3.3. Note that any subgroup of $\prod_{\ell \in D} \mathrm{O}(V_\ell)$ containing $\prod_{\ell \in D} \Omega(V_\ell)$ is a normal subgroup. This explains why (3.1) and (3.2) are well-defined without the fundamental groups have explicit base points.

Corollary 3.4. *Condition (a) of §1.3 implies condition (b).*

Proof. We obtain condition (b) by taking singleton sets D in Proposition 3.1. □

3.1. Proof of Propositions 3.1 and 3.2.

Lemma 3.5. *Fix a finite field k that is an R-algebra. There is a subset $\Lambda \subseteq \Sigma$ with Dirichlet density 1 such that $\bar{\rho}_\ell(\pi_1(U_{\bar{k}})) \supseteq \Omega(V_\ell)$ holds for all primes $\ell \in \Lambda$ that are not equal to the characteristic of k. If condition (b) in §1.3 holds, then we may take Λ to be the set of primes from condition (b).*

Proof. The lemma is immediate if condition (b) holds, so we may assume that condition (a) in §1.3.3 holds. For $\ell \in \Sigma$ not equal to the characteristic of k, let

$$\varrho_\ell \colon \pi_1(U_k) \to \mathrm{O}_{\mathcal{V}_\ell}(\mathbb{Q}_\ell)$$

be the representation obtained by specializing ρ_ℓ. By condition (a), there is a subset $\Lambda \subseteq \Sigma$ with Dirichlet density 1, that does not contain the characteristic of k, such that the neutral component of the Zariski closure of $\varrho_\ell(\pi_1(U_k))$ is $\mathrm{SO}_{\mathcal{V}_\ell}$ for all $\ell \in \Lambda$.

Now take any $\ell \in \Lambda$. We have a connected and semisimple group scheme $H_\ell := \mathrm{SO}_{M_\ell}$ over $\mathbb{Z}_\ell$ and base extension by $\mathbb{Q}_\ell$ gives $\mathrm{SO}_{\mathcal{V}_\ell}$. Let H_ℓ^{ad} be the quotient of H_ℓ by its center and let H_ℓ^{sc} be the simply connected cover of H_ℓ. Denote by $\pi \colon H_\ell^{\mathrm{sc}} \to H_\ell$ and $\sigma \colon H_\ell \to H_\ell^{\mathrm{ad}}$ the natural homomorphisms. Define

$$\Gamma_\ell := \varrho_\ell(\pi_1(U_k)) \cap \mathrm{SO}_{\mathcal{V}_\ell}(\mathbb{Q}_\ell);$$

it is a compact subgroup of $H_\ell(\mathbb{Z}_\ell) = \mathrm{SO}_{M_\ell}(\mathbb{Z}_\ell)$. Define the subgroup

$$\Gamma_\ell^{\mathrm{sc}} := \{g \in H_\ell^{\mathrm{sc}}(\mathbb{Q}_\ell) : \sigma(\pi(g)) \in \sigma(\Gamma_\ell)\}$$

of $H_\ell^{\mathrm{sc}}(\mathbb{Q}_\ell)$. Observe that $\Gamma_\ell^{\mathrm{sc}} \subseteq H_\ell^{\mathrm{sc}}(\mathbb{Z}_\ell)$.

We now apply a theorem of Larsen. By [Lar95, Theorem 3.17], there is a subset $\Lambda' \subseteq \Lambda$ with Dirichlet density 1 such that $\Gamma_\ell^{\mathrm{sc}}$ is a maximal compact subgroup of $H_\ell^{\mathrm{sc}}(\mathbb{Q}_\ell)$ for all $\ell \in \Lambda'$. Therefore, $\Gamma_\ell^{\mathrm{sc}} = H_\ell^{\mathrm{sc}}(\mathbb{Z}_\ell)$ for all $\ell \in \Lambda'$ since $H_\ell^{\mathrm{sc}}(\mathbb{Z}_\ell)$ is a compact subgroups of $H_\ell^{\mathrm{sc}}(\mathbb{Q}_\ell)$.

Take any $\ell \in \Lambda'$ with $\ell \geq 11$ and let $\bar{\Gamma}_\ell$ be the image of Γ_ℓ in $\mathrm{SO}(V_\ell)$. Since σ is a central isogeny, we have $\pi(\Gamma_\ell^{\mathrm{sc}}) \subseteq \Gamma_\ell \cdot Z$, where $Z \subseteq H_\ell(\mathbb{Z}_\ell)$ lies in the center of H_ℓ. By our choice of ℓ, we have $\pi(H_\ell^{\mathrm{sc}}(\mathbb{Z}_\ell)) = \pi(\Gamma_\ell^{\mathrm{sc}}) \subseteq \Gamma_\ell \cdot Z$. Reducing modulo ℓ, we find that $\pi(H_\ell^{\mathrm{sc}}(\mathbb{F}_\ell)) \subseteq \bar{\Gamma}_\ell \cdot \bar{Z}$, where $\bar{Z}$ is a subgroup of the center of $\mathrm{SO}(V_\ell)$. The group $\pi(H_\ell^{\mathrm{sc}}(\mathbb{F}_\ell))$ is equal to the commutator subgroup of $H_\ell(\mathbb{F}_\ell) = \mathrm{SO}(V_\ell)$; for example, see [Lar95, §1.2] and note that a simply connected group is a product of simple simply connected groups (this is where we are using $\ell \geq 11$). So by Lemma 2.2(v), we have $\Omega(V_\ell) = \pi(H_\ell^{\mathrm{sc}}(\mathbb{F}_\ell)) \subseteq \bar{\Gamma}_\ell \cdot \bar{Z}$. The group $\Omega(V_\ell)$ is perfect and the commutator subgroup of $\bar{\Gamma}_\ell \cdot \bar{Z}$ lies in $\bar{\Gamma}_\ell$. So by starting with $\Omega(V_\ell) \subseteq \bar{\Gamma}_\ell \cdot \bar{Z}$ and taking commutator subgroups, we deduce that $\Omega(V_\ell) \subseteq \bar{\Gamma}_\ell$. In particular, $\Omega(V_\ell) \subseteq \bar{\rho}_\ell(\pi_1(U_k))$. Since $\bar{k}/k$ is an abelian extension and $\Omega(V_\ell)$ is perfect, this implies that $\Omega(V_\ell) \subseteq \bar{\rho}_\ell(\pi_1(U_{\bar{k}}))$. □

Lemma 3.6. *Take any finite field k that is an R-algebra. Let Λ be the set of primes from Lemma 3.5. Then for any finite subset $D \subseteq \Lambda$ not containing the characteristic of k, we have*

$$\bar{\rho}_D(\pi_1(U_{\bar{k}})) \supseteq \prod_{\ell \in D} \Omega(V_\ell).$$

Proof. Let H be the commutator subgroup of $\bar{\rho}_D(\pi_1(U_{\bar{k}}))$; it is a subgroup of $\prod_{\ell \in D} \Omega(V_\ell)$ which is the commutator subgroup of $\prod_{\ell \in D} \mathrm{O}(V_\ell)$ by Lemma 2.2(v).

For each $\ell \in D$, we have inclusions $\Omega(V_\ell) \subseteq \bar{\rho}_\ell(\pi_1(U_{\bar{k}})) \subseteq \mathrm{O}(V_\ell)$, where the first inclusion uses our choice of Λ and Lemma 3.5. By taking commutator subgroups and using Lemma 2.2(v), we deduce that the commutator subgroup of $\bar{\rho}_\ell(\pi_1(U_{\bar{k}}))$ is $\Omega(V_\ell)$ for all $\ell \in D$. Therefore, the projection homomorphism $H \to \Omega(V_\ell)$ is surjective for all $\ell \in D$.

Fix $\ell \in D$. Lemma 2.2 implies that the only non-abelian simple group in the composition series of $\Omega(V_\ell)$ is $\Omega(V_\ell)/Z_\ell$ where Z_ℓ is the center, *except* when $N = 4$ and V_ℓ is split, then the only one is $\mathrm{PSL}_2(\mathbb{F}_\ell)$. For distinct $\ell, \ell' \in D$, the non-abelian simple groups occurring in the composition series of $\Omega(V_\ell)$ and $\Omega(V_{\ell'})$ have different cardinalities (see [ATLAS, §2.4]) and hence are not isomorphic. Since H is a subgroup of $\prod_{\ell \in D} \Omega(V_\ell)$ such that the projection $H \to \Omega(V_\ell)$ is surjective for all $\ell \in D$, Goursat's lemma (for example, [Zyw10a, Lemma A.4]) implies that $H = \prod_{\ell \in D} \Omega(V_\ell)$. The lemma follows since $\bar{\rho}_D(\pi_1(U_{\bar{k}})) \supseteq H$. □

If R is a finite field, then Proposition 3.1 follows from Lemma 3.6 since the group $\bar{\rho}_D(\pi_1(U_{\bar{k}}))$, for a finite extension k of R, depends only on an algebraic closure $\bar{k}$ of R.

For the rest of the proof, we may thus assume that R has characteristic 0. Let R' be an integral domain that is an R-algebra. We say that the R'-scheme $U_{R'}$ is nicely compactifiable if $U_{R'}$ is open in a proper smooth R'-scheme X and $\mathcal{D} := X - U_{R'}$ is a divisor of X that has normal crossings relative to R'.

Lemma 3.7. *There is a finite set $S' \supseteq S$ of non-zero prime ideals of $\mathcal{O}_F$ such that the R'-scheme $U_{R'}$ is nicely compactifiable, where $R' = \mathcal{O}_F[S'^{-1}]$.*

Proof. By resolution of singularities, the variety U_F over F is nicely compactifiable (note that F is a field of characteristic 0). The lemma follows by choosing integral models for $\mathcal{D}$ and X and inverting enough primes. □

Fix a set $S' \supseteq S$ as in Lemma 3.7 and define $R' = \mathcal{O}_F[S'^{-1}]$. By enlarging S' if necessary, we may assume that $U(\mathbb{F}_\mathfrak{p})$ is non-empty for all maximal ideals $\mathfrak{p} \notin S'$ of $\mathcal{O}_F$ (since U is a smooth R-scheme with geometric irreducible fibers of dimension at least 1).

Lemma 3.8. *Take any finite set $D \subseteq \Sigma$. For any finite field k that is an R'-algebra with characteristic not in D, the group $\bar{\rho}_D(\pi_1(U_{\bar{k}}))$ is conjugate to G_D^g in $\prod_{\ell\in D} \mathrm{O}(V_\ell)$.*

Proof. Take any finite set $D \subseteq \Sigma$. Since the conclusion only involves the algebraic closure of k, we may assume that $k = \mathbb{F}_\mathfrak{p}$ for a maximal ideal $\mathfrak{p} \notin S'$ of $\mathcal{O}_F$, where $\mathfrak{p}$ does not divide any prime in D.

Let $F_\mathfrak{p}$ be the completion of F at $\mathfrak{p}$ and denote by $\mathcal{O}_\mathfrak{p}$ its valuation ring. For an algebraic closure $\overline{F}$ of F, choose an algebraic closure $\overline{F}_\mathfrak{p}$ of $F_\mathfrak{p}$ containing $\overline{F}$. Since the set $U(\mathbb{F}_\mathfrak{p})$ is non-empty and U is smooth, we have $U(\mathcal{O}_\mathfrak{p}) \neq \emptyset$. The $\mathcal{O}_\mathfrak{p}$-scheme $U_{\mathcal{O}_\mathfrak{p}}$ is nicely compactifiable since $U_{R'}$ has this property and $\mathcal{O}_\mathfrak{p}$ is an R'-algebra. So $U_{\mathcal{O}_\mathfrak{p}}$ is open in a proper smooth $\mathcal{O}_\mathfrak{p}$-scheme X for which $\mathcal{D} := X - U_{\mathcal{O}_\mathfrak{p}}$ is a divisor of X that has normal crossings relative to $\mathcal{O}_\mathfrak{p}$. Let

$$\bar{\varrho}_D \colon \pi_1(U_{\mathcal{O}_\mathfrak{p}}) \to \prod_{\ell\in D} \mathrm{O}(V_\ell)$$

be the representation obtained from $\bar{\rho}_D$ by base extension. By Abhyankar's Lemma [SGA1, XIII, 5.5], the representation $\pi_1(U_{\overline{\mathbb{F}}_\mathfrak{p}}) \to \prod_{\ell\in D} \mathrm{O}(V_\ell)$ obtained from $\bar{\varrho}_D$ is tamely ramified at each maximal point of the scheme $\mathcal{D}_{\overline{\mathbb{F}}_\mathfrak{p}}$. The Tame Specialization Theorem [Kat90, Theorem 8.17.14] then implies that the group $\bar{\rho}_D(\pi_1(U_{\overline{\mathbb{F}}_\mathfrak{p}}))$ is conjugate to $\bar{\rho}_D(\pi_1(U_{\overline{F}_\mathfrak{p}}))$ in $\prod_{\ell\in D} \mathrm{O}(V_\ell)$. Finally, observe that $\bar{\rho}_D(\pi_1(U_{\overline{F}_\mathfrak{p}}))$ is conjugate to G_D^g in $\prod_{\ell\in D} \mathrm{O}(V_\ell)$. □

Lemma 3.9. *There is a subset $\Lambda \subseteq \Sigma$ with Dirichlet density 1 such that $G_D^g \supseteq \prod_{\ell\in D} \Omega(V_\ell)$ for all finite subsets $D \subseteq \Lambda$.*

Proof. Fix a finite field k that is an R'-algebra. Take $\Lambda \subseteq \Sigma$ as in Lemma 3.6. For any finite $D \subseteq \Lambda$, the group $\bar{\rho}_D(\pi_1(U_{\bar{k}}))$ contains $\prod_{\ell\in D} \Omega(V_\ell)$ by Lemma 3.6 and is conjugate to G_D^g by Lemma 3.8. The lemma is now immediate. □

Proposition 3.1 (in the characteristic 0 case) and Proposition 3.2 are now direct consequences of Lemmas 3.8 and 3.9.

4. The field K

Fix notation and assumptions as in §1.3 and assume that N is even. In this section, we describe the field K from §1.3.

Proposition 4.1.

(i) *There is a unique extension $K/\mathbb{Q}$ with $[K:\mathbb{Q}] \leq 2$ such that for all sufficiently large $\ell \in \Sigma$, ℓ splits in K if and only if the orthogonal space V_ℓ is split.*

(ii) *Take any $u \in U(k)$, where k is a finite field that is an R-algebra. If $P_u(\pm1) \neq 0$, then*
$$K = \mathbb{Q}\Big(\sqrt{(-1)^{N/2} P_u(1) P_u(-1)}\Big).$$

(iii) *Take any $u \in U(k)$, where k is a finite field that is an R-algebra. If $\varepsilon_u = 1$ and $P_u(T)$ is separable, then $K = \mathbb{Q}(\sqrt{\Delta_u})$ where Δ_u is the discriminant of $P_u(T)$.*

Proof. We claim that there is a point $u \in U(k)$ such that $P_u(\pm1) \neq 0$, where k is a finite field that is an R-algebra. By Corollary 3.4, there is a subset $\Lambda \subseteq \Sigma$ of Dirichlet 1 for which condition (b) of §1.3.3 holds. Fix a prime $\ell \in \Lambda$ and choose an element $g \in \Omega(V_\ell)$ such that $\det(I+g) \neq 0$ and $\det(I-g) \neq 0$. Since $\ell \in \Lambda$, there is a finite field k that is an R-algebra with characteristic not equal to ℓ such that $\bar{\rho}_\ell(\pi_1(U_{\bar{k}})) \supseteq \Omega(V_\ell)$. By equidistribution, there is a finite extension k'/k and a point $u \in U(k')$ such that $\bar{\rho}_\ell(\mathrm{Frob}_u)$ is conjugate to g in $\mathrm{O}(V_\ell)$. So $P_u(\pm 1) \equiv \det(I \mp g) \not\equiv 0 \pmod{\ell}$. In particular, $P_u(\pm 1) \neq 0$ which proves the claim.

Now take any $u \in U(k)$ such that $P_u(\pm 1) \neq 0$, where k is a finite field that is an R-algebra (such a point u exists by the above claim). The polynomial P_u is reciprocal since $P_u(\pm 1) \neq 0$. Define the field

$$K := \mathbb{Q}\Big(\sqrt{(-1)^{N/2} P_u(1) P_u(-1)}\Big).$$

Let Σ_0 be the set of odd primes $\ell \in \Sigma$ for which $P_u(\pm 1) \not\equiv 0 \pmod{\ell}$. Take any prime $\ell \in \Sigma_0$ and define $A := \bar{\rho}_\ell(\mathrm{Frob}_u) \in \mathrm{O}(V_\ell)$. We have $\det(I - TA) \equiv P_u(T) \pmod{\ell}$, so $A \in \mathrm{SO}(V_\ell)$ since P_u is reciprocal. By Lemma 2.5(iii), V_ℓ is split if and only if $(-1)^{N/2} P_u(1) P_u(-1)$ modulo ℓ is a (non-zero) square in $\mathbb{F}_\ell$. So for any $\ell \in \Sigma_0$, we deduce that ℓ splits in K if and only if V_ℓ is split. In particular, for all sufficiently large $\ell \in \Sigma$, we find that ℓ splits in K if and only if V_ℓ is split. Since Σ has density 1, this gives a characterization of K that does not depend on our choice of u. Parts (i) and (ii) now follow since K does not depend on u.

Finally, take any $u \in U(k)$ for which $\varepsilon_u = 1$ and $P_u(T)$ is separable, where k is a finite field that is an R-algebra. Let Δ_u be the discriminant of P_u; it is non-zero since P_u is separable. The polynomial P_u has even degree and is reciprocal by (1.3) since $\varepsilon_u = 1$. By Lemma 2.6(ii), we have $\Delta_u \in (-1)^{N/2} P_u(1) P_u(-1) \cdot (\mathbb{Q}^\times)^2$. Therefore, $\mathbb{Q}(\sqrt{\Delta_u}) = \mathbb{Q}(\sqrt{(-1)^{N/2} P_u(1) P_u(-1)})$. Part (iii) now follows from (ii). □

5. Proof of Proposition 1.12

Fix notation and assumptions as in §1.3. In this section, we prove Proposition 1.12 which will be used to apply the sieve theory in the proofs of Theorems 1.4 and 1.6.

5.1. Big subgroups of W_{2n}.

We first give a criterion to prove that a subgroup of W_{2n} contains W_{2n}^+. We shall assume that $n \geq 2$; the case $n = 1$ is not interesting since $W_2^+ = 1$.

We may view W_{2n} as a subgroup of the group of permutations $\mathfrak{S}_X$ of the set $X = \{\pm e_1, \ldots, \pm e_n\}$. Let $\varepsilon_1 \colon W_{2n} \to \{\pm 1\}$ be the homomorphism obtained by composing the inclusion $W_{2n} \hookrightarrow \mathfrak{S}_X$ with the signature map. The kernel of ε_1 is the subgroup W_{2n}^+. By considering the action of W_{2n} on the n pairs $p_i := \{e_i, -e_i\}$ with $1 \leq i \leq n$, we obtain a homomorphism $\varphi \colon W_{2n} \to \mathfrak{S}_n$. Let $\varepsilon_2 \colon W_{2n} \to \{\pm 1\}$ be the homomorphism obtained by composing φ with the signature map.

Lemma 5.1. *Let G be a subgroup of W_{2n}. Suppose that there exist g_1, g_2, g_3, g_4 and g_5 in G such that the following hold:*

- *$\varphi(g_1) \in \mathfrak{S}_n$ is an n-cycle,*
- *$\varphi(g_2) \in \mathfrak{S}_n$ is a p-cycle for some prime $p > n/2$,*
- *$\varphi(g_3) \in \mathfrak{S}_n$ is a transposition,*
- *$g_4 \in \mathfrak{S}_X$ satisfies $\varphi(g_4) = 1$ and is a product of one or two disjoint transpositions,*
- *$\varepsilon_1(g_5)\varepsilon_2(g_5) = -1$.*

Then G equals W_{2n}^+ or W_{2n}.

Proof. A lemma of Bauer, see [Gal73, p.98], says that $\mathfrak{S}_n$ has no proper transitive subgroups that contain a transposition and a cycle of prime order greater than $n/2$. The properties of g_1, g_2 and g_3 thus ensure that $\varphi(G) = \mathfrak{S}_n$.

Let H be the kernel of $\varphi \colon W_{2n} \to \mathfrak{S}_n$; these are the permutations of X that fix all the pairs $p_i = \{e_i, -e_i\}$. Let H^+ be the kernel of $\varepsilon_1|_H \colon H \to \{\pm 1\}$.

First suppose that g_4 is the product of two disjoint transpositions. We have $g_4 \in H$ since $\varphi(g_4) = 1$. Without loss of generality, we may assume that g_4 interchanges e_1 and $-e_1$, interchanges e_2 and $-e_2$, and fixes all the other $\pm e_j$.

Take any $1 \leq i \leq n$. Since $\varphi(G) = \mathfrak{S}_n$, there is an element $\sigma \in G$ satisfying $\varphi(\sigma) = (1i)$. Then $\sigma g_4 \sigma^{-1} \in G$ interchanges e_2 and $-e_2$, e_i and $-e_i$, and fixes all the other $\pm e_j$. Therefore, $h_i := \sigma g_4 \sigma^{-1} g_4^{-1} \in G$ interchanges e_1 and $-e_1$, e_i and $-e_i$, and fixes all the other $\pm e_j$. Observe that h_i is in the commutator subgroup $[G, G]$ of G.

The elements of H that are the product of two disjoint transpositions are precisely the elements h_i with $1 < i \leq n$ or $h_i h_j$ with $1 < i < j \leq n$. We thus have $H^+ \subseteq G$ since the group H^+ is generated by the elements in H that are the product of two disjoint transpositions. Moreover, $H^+ \subseteq [G, G]$.

Since $\varphi(G) = \mathfrak{S}_n$, the group $\varphi([G, G])$ equals the commutator subgroup of $\mathfrak{S}_n$; this is the alternating group $\mathfrak{A}_n$ since $n \geq 2$. Therefore, the cardinality of the group $[G, G]$ is divisible by $|H^+| \cdot |\mathfrak{A}_n| = 2^{n-1} \cdot n!/2 = 2^{n-2} n!$. We have $|W_{2n}| = 2^n n!$, so $[W_{2n} : [G, G]] \leq 4$. Since $[G, G]$ is contained in the commutator subgroup $[W_{2n}, W_{2n}]$, we have

$$m := [W_{2n} : [W_{2n}, W_{2n}]] \leq [W_{2n} : [G, G]] \leq 4.$$

However, we have $m \geq 4$ since the quotient of W_{2n} by $\ker(\varepsilon_1) \cap \ker(\varepsilon_2)$ is isomorphic to $\{\pm 1\} \times \{\pm 1\}$. Therefore, $m = 4$ and hence

$$[G, G] = [W_{2n}, W_{2n}] = \ker(\varepsilon_1) \cap \ker(\varepsilon_2).$$

We have $\varepsilon_2(G) = \{\pm 1\}$ since $\varphi(G) = \mathfrak{S}_n$. Therefore, G must be one of the groups $\ker(\varepsilon_1 \varepsilon_2)$, $\ker(\varepsilon_1) = W_{2n}^+$ or W_{2n}. The existence of g_5 rules out the case $G = \ker(\varepsilon_1 \varepsilon_2)$. Therefore, G equals W_{2n}^+ or W_{2n}.

Now suppose that $g_4 \in G$ is a transposition. We have $g_4 \in H$ since $\varphi(g_4) = 1$. Using that $\varphi(G) = \mathfrak{S}_n$, an argument similar to the one above shows that G contains every transposition in H. We have $H \subseteq G$ since H is generated by transpositions. Therefore, G is a group of order $|H| \cdot |\mathfrak{S}_n| = 2^n n!$. Since G has the same cardinality as W_{2n}, we conclude that $G = W_{2n}$. □

Remark 5.2. Note that in [Jou09, Lemma 4.4(ii)], which is an analogue of our Lemma 5.1, one needs to add another condition to rule out the case where the subgroup of W_{2n} is $\ker(\epsilon_1 \epsilon_2)$.

5.2. **A criterion for a maximal Galois group.** Fix an integer $n \geq 1$ and let $\mathbb{F}$ be a finite field of odd characteristic. Let $\mathcal{P}_n(\mathbb{F})$ be the set of monic polynomials $h \in \mathbb{F}[T]$ of degree n which are separable and satisfy $h(\pm 2) \neq 0$.

If $n \geq 2$, define the following sets:

- Let $H_{n,1}(\mathbb{F})$ be the set of irreducible $h \in \mathcal{P}_n(\mathbb{F})$.
- Let $H_{n,2}(\mathbb{F})$ be the set of $h \in \mathcal{P}_n(\mathbb{F})$ that have an irreducible factor whose degree is a prime greater than $n/2$.
- Let $H_{n,3}(\mathbb{F})$ be the set of $h \in \mathcal{P}_n(\mathbb{F})$ that factor as a product of an irreducible polynomial of degree 2 and irreducible polynomials of odd degree.
- Let $H_{n,4}(\mathbb{F})$ be the set of $h \in \mathcal{P}_n(\mathbb{F})$ that have no irreducible factors of even degree, and for which the polynomial $T^n h(T + 1/T)$ is the product of one or two quadratic irreducible polynomials and irreducible polynomials of odd degree.
- Let $H_{n,5}(\mathbb{F})$ be the set of $h \in \mathcal{P}_n(\mathbb{F})$ such that the polynomial $h(T) \cdot T^n h(T + 1/T)$ has an odd number of irreducible factors of even degree (counted with multiplicity).
- Let $H_{n,6}(\mathbb{F})$ be the set of $h \in \mathcal{P}_n(\mathbb{F})$ such that the polynomial $T^n h(T + 1/T)$ is the product of a quadratic irreducible polynomial and irreducible polynomials of odd degree.

If $n = 1$, define $H_{n,i}(\mathbb{F}) = \mathcal{P}_1(\mathbb{F})$ for all $1 \leq i \leq 5$ and let $H_{n,6}(\mathbb{F})$ be the set of $h \in \mathcal{P}_1(\mathbb{F})$ such that the quadratic polynomial $Th(T + 1/T)$ is irreducible.

For $1 \leq i \leq 6$, we define $F_{2n,i}(\mathbb{F})$ to be the set of polynomials $T^n h(T + 1/T)$ with $h \in H_{n,i}(\mathbb{F})$; they are monic, reciprocal and have degree $2n$. By Lemma 2.6(ii), the condition that h is separable and $h(\pm 2) \neq 0$ ensures that each polynomials $f \in F_{2n,i}(\mathbb{F})$ is separable and $f(\pm 1) \neq 0$.

The above definitions are justified by the following criterion.

Proposition 5.3. *Fix a monic, reciprocal and separable polynomial $f \in \mathbb{Q}[T]$ of even degree $2n \geq 2$. Let Δ be the discriminant of f. Denote by $\operatorname{Gal}(f)$ the Galois group of a splitting field of f over $\mathbb{Q}$. Assume that for each $1 \leq i \leq 5$, there is an odd prime ℓ such that the coefficients of f are integral at ℓ and $f \bmod \ell \in \mathbb{F}_\ell[T]$ lies in $F_{2n,i}(\mathbb{F}_\ell)$.*

(i) *If Δ is a square in $\mathbb{Q}$, then $\operatorname{Gal}(f) \cong W_{2n}^+$.*
(ii) *If Δ is a non-square in $\mathbb{Q}$, then $\operatorname{Gal}(f) \cong W_{2n}$.*
(iii) *If there is an odd prime ℓ such that the coefficients of f are integral at ℓ and $f \bmod \ell \in \mathbb{F}_\ell[T]$ lies in $F_{2n,6}(\mathbb{F}_\ell)$, then $\operatorname{Gal}(f) \cong W_{2n}$.*

Proof. If $n = 1$, then (i) and (ii) are immediate since f is a separable quadratic polynomial and the groups W_2^+ and W_2 have cardinality 1 and 2, respectively. So assume that $n \geq 2$. As in §1.1, we have an injective homomorphism

$$\psi\colon \operatorname{Gal}(f) \hookrightarrow W_{2n}.$$

Take any prime ℓ for which the coefficients of f are integral at ℓ and f modulo ℓ is separable with the same degree as f. Then ψ is unramified at ℓ and the cycle type of $\psi(\operatorname{Frob}_\ell)$ in $\mathfrak{S}_X$ is given by the degrees of the irreducible factors of f modulo ℓ. The cycle type of $\varphi(\psi(\operatorname{Frob}_\ell))$ in $\mathfrak{S}_n$ is given by the degrees of the irreducible factors of h modulo ℓ.

- Since $h \bmod \ell_1$ is irreducible in $\mathbb{F}_{\ell_1}[T]$, we find that $\varphi(\psi(\operatorname{Frob}_{\ell_1}))$ is a n-cycle in $\mathfrak{S}_n$.
- Since $h \bmod \ell_2 \in \mathbb{F}_{\ell_2}[T]$ has an irreducible factor of prime degree $p > n/2$, we find that some power of $\varphi(\psi(\operatorname{Frob}_{\ell_2}))$ is a p-cycle in $\mathfrak{S}_n$.
- Since $h \bmod \ell_3 \in \mathbb{F}_{\ell_3}[T]$ is the product of an irreducible quadratic polynomial and irreducibles of odd degree, we find that some power of $\varphi(\psi(\operatorname{Frob}_{\ell_3}))$ is a transposition in $\mathfrak{S}_n$.
- Since $h \bmod \ell_4$ has no irreducible factors of even degree and $f \bmod \ell_4$ is the product of one or two quadratic irreducible polynomials and irreducible polynomials of odd degree, we find that there is a power g of $\psi(\operatorname{Frob}_{\ell_4})$ such that $\varphi(g) = 1$ and g is a product of one or two disjoint transpositions in $\mathfrak{S}_X$.
- Since $hf \bmod \ell_5$ has an odd number of irreducible factors of even degree, we find that
$$\epsilon_1(\psi(\operatorname{Frob}_{\ell_5}))\epsilon_2(\psi(\operatorname{Frob}_{\ell_5})) = -1.$$

By Lemma 5.1, the group $\psi(\operatorname{Gal}(f))$ is either W_{2n}^+ or W_{2n}. The image of ψ is a subgroup of W_{2n}^+ if and only if the discriminant Δ of f is a square in $\mathbb{Q}$. So $\psi(\operatorname{Gal}(f)) = W_{2n}^+$ if Δ is a square in $\mathbb{Q}$ and $\psi(\operatorname{Gal}(f)) = W_{2n}$ if Δ is not a square in $\mathbb{Q}$. This proves parts (i) and (ii).

Finally, suppose there is a prime ℓ as in the statement of part (iii). Then ψ is unramified at ℓ and the permutation $\psi(\operatorname{Frob}_\ell)$ in $\mathfrak{S}_X$ is the product of disjoint cycles where one is a transposition and the rest have odd length. Therefore, $\varepsilon_1(\psi(\operatorname{Frob}_\ell)) = -1$ and hence $\psi(\operatorname{Gal}(f)) \neq W_{2n}^+$. So, $\psi(\operatorname{Gal}(f)) = W_{2n}$. □

For cosets $\alpha, \beta \in \mathbb{F}^\times/(\mathbb{F}^\times)^2$, we define $F_{2n,i}^{\alpha,\beta}(\mathbb{F})$ to be the set of $f \in F_{2n,i}(\mathbb{F})$ such that $f(\pm 1) \neq 0$, $f(1) \in \alpha$, $f(-1) \in \beta$, and f has at most eight irreducible factors. The following lower bounds for the cardinality of $F_{2n,i}^{\alpha,\beta}(\mathbb{F})$ will be important later for counting certain subsets of orthogonal groups.

Proposition 5.4. *Fix $\alpha, \beta \in \mathbb{F}^\times/(\mathbb{F}^\times)^2$ and an integer $1 \le i \le 6$. Assume that $\alpha\beta \ne (-1)^n(\mathbb{F}^\times)^2$ if $i = 6$. Then*

$$|F^{\alpha,\beta}_{2n,i}(\mathbb{F})| \ge \frac{c}{n^2} q^n \Big(1 + O(1/q)\Big), \tag{5.1}$$

where q is the cardinality of $\mathbb{F}$, and the constant $c > 0$ and the implicit constant are absolute.

Before proving the proposition, we need a lemma. For $m \ge 1$ and cosets $\alpha, \beta \in \mathbb{F}^\times/(\mathbb{F}^\times)^2$, let $\mathcal{I}^{\alpha,\beta}_m$ be the set of irreducible $h \in \mathcal{P}_m(\mathbb{F})$ such that $h(2) \in \alpha$ and $h(-2) \in \beta$. Set $\mathcal{I}^{\alpha,\beta}_0 = \{1\}$.

Lemma 5.5. *For $m \ge 1$ and cosets $\alpha, \beta \in \mathbb{F}^\times/(\mathbb{F}^\times)^2$, we have $|\mathcal{I}^{\alpha,\beta}_m| = \frac{1}{4m}\Big(q^m + O(q^{m/2})\Big)$, where the implicit constant is absolute.*

Proof. For each $d \ge 1$, let $\mathbb{F}_{q^d}$ be the degree d extension of $\mathbb{F}$. Choose elements $a \in \alpha$ and $b \in \beta$. The map

$$\{\zeta \in \mathbb{F}_{q^m} : \mathbb{F}(\zeta) = \mathbb{F}_{q^m}\} \to \{h \in \mathbb{F}[T] : h \text{ monic and irreducible of degree } m\}$$

defined by $\zeta \mapsto N_{\mathbb{F}_{q^m}/\mathbb{F}}(T - \zeta) := \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F})}(T - \sigma(\zeta))$ is surjective and m-to-1.

Fix $\zeta \in \mathbb{F}_{q^m}$ such that $\mathbb{F}(\zeta) = \mathbb{F}_{q^m}$, and set $h(T) = N_{\mathbb{F}_{q^m}/\mathbb{F}}(T - \zeta)$. We have $h(\pm 2) \ne 0$ if and only if $\zeta \ne \pm 2$. Since $N_{\mathbb{F}_{q^m}/\mathbb{F}}$ induces an isomorphism $\mathbb{F}^\times_{q^m}/(\mathbb{F}^\times_{q^m})^2 \to \mathbb{F}^\times/(\mathbb{F}^\times)^2$, we have $h(2) \in \alpha$ and $h(-2) \in \beta$ if and only if $2 - \zeta \in a(\mathbb{F}^\times_{q^m})^2$ and $-2 - \zeta \in b(\mathbb{F}^\times_{q^m})^2$. Therefore,

$$\begin{aligned} m|\mathcal{I}^{\alpha,\beta}_m(\mathbb{F})| &= |\{\zeta \in \mathbb{F}_{q^m} - \{\pm 2\} : \mathbb{F}(\zeta) = \mathbb{F}_{q^m},\ 2 - \zeta = ax^2 \text{ and } -2 - \zeta = by^2 \text{ for some } x, y \in \mathbb{F}_{q^m}\}| \\ &= \tfrac{1}{4}|\{(x,y) \in \mathbb{F}^2_{q^m} : ax^2 - by^2 = 4\}| + O(|\{\zeta \in \mathbb{F}_{q^m} : \mathbb{F}(\zeta) \ne \mathbb{F}_{q^m}\}| + 1). \end{aligned}$$

The projective closure of the plane curve $ax^2 - by^2 = 4$ is smooth of genus 0. So $m|\mathcal{I}^{\alpha,\beta}_m(\mathbb{F})|$ equals $q^m/4 + O(|\{\zeta \in \mathbb{F}_{q^m} : \mathbb{F}(\zeta) \ne \mathbb{F}_{q^m}\}| + 1)$. Finally, note that

$$|\{\zeta \in \mathbb{F}_{q^m} : \mathbb{F}(\zeta) \ne \mathbb{F}_{q^m}\}| \le \sum_{d|m, d<m} |\mathbb{F}_{q^d}| \le \sum_{d \le m/2} q^d = (q^{\lfloor m/2 \rfloor + 1} - 1)/(q - 1) = O(q^{m/2}). \qquad \square$$

Proof of Proposition 5.4. For cosets $\alpha, \beta \in \mathbb{F}^\times/(\mathbb{F}^\times)^2$, we define $H^{\alpha,\beta}_{n,i}(\mathbb{F})$ to be the set of $h \in H_{n,i}(\mathbb{F})$ such that $h(\pm 2) \ne 0$, $h(2) \in \alpha$, $h(-2) \in \beta$, and h has at most four irreducible factors. By Lemma 2.6(iii), the polynomial $T^n h(T + 1/T) \in \mathbb{F}[T]$ has at most eight irreducible factors for all $h \in H_{n,i}(\mathbb{F})$. We thus have an injective map

$$H^{\alpha,\beta}_{n,i}(\mathbb{F}) \hookrightarrow F^{\alpha,(-1)^n\beta}_{2n,i}(\mathbb{F}), \quad h \mapsto T^n h(T + 1/T).$$

It thus suffices to show that

$$|H^{\alpha,\beta}_{n,i}(\mathbb{F})| \ge \frac{c}{n^2} \cdot (q^n + O(q^{n-1})),$$

where $c > 0$ and the implicit constant are absolute, and $\alpha\beta \ne (\mathbb{F}^\times)^2$ if $i = 6$.

The following inclusions involving $H^{\alpha,\beta}_{n,i}(\mathbb{F})$ make use of Lemma 2.6(iii) when $i \in \{4, 5, 6\}$. Let γ be the non-identity coset of $\mathbb{F}^\times/(\mathbb{F}^\times)^2$. When $n = 1$, we have $H^{\alpha,\beta}_{n,i}(\mathbb{F}) = \mathcal{I}^{\alpha,\beta}_n$ for $1 \le i \le 5$. We also have $H^{\alpha,\beta}_{1,6}(\mathbb{F}) = \mathcal{I}^{\alpha,\beta}_1$ when $\alpha\beta = \gamma$.
Now suppose that $n \ge 2$.

- We have $\mathcal{I}^{\alpha,\beta}_n = H^{\alpha,\beta}_{n,1}(\mathbb{F})$.
- By Bertrand's postulate, there exists a prime $n/2 < p \le n$ and hence

$$\{h_1 h_2 : (h_1, h_2) \in \mathcal{I}^{\alpha,\beta}_p \times \mathcal{I}^{1,1}_{n-p} \text{ and } h_1 \ne h_2\} \subseteq H^{\alpha,\beta}_{n,2}(\mathbb{F}).$$

- If n is odd, then $\{h_1h_2 : (h_1,h_2) \in \mathcal{I}_2^{\alpha,\beta} \times \mathcal{I}_{n-2}^{1,1}\} \subseteq H_{n,3}^{\alpha,\beta}(\mathbb{F})$.
  If $n \geq 4$ is even, then $\{h_1h_2h_3 : (h_1,h_2,h_3) \in \mathcal{I}_2^{\alpha,\beta} \times \mathcal{I}_1^{1,1} \times \mathcal{I}_{n-3}^{1,1}$ and $h_2 \neq h_3\} \subseteq H_{n,3}^{\alpha,\beta}(\mathbb{F})$.
  If $n = 2$, then $\mathcal{I}_2^{\alpha,\beta} \subseteq H_{n,3}^{\alpha,\beta}(\mathbb{F})$.
- If $\alpha\beta = 1$ and n is odd, then
  $$\{h_1h_2h_3 : (h_1,h_2,h_3) \in \mathcal{I}_1^{\alpha,\beta\gamma} \times \mathcal{I}_1^{1,\gamma} \times \mathcal{I}_{n-2}^{1,1} \text{ and } h_1,h_2,h_3 \text{ distinct}\} \subseteq H_{n,4}^{\alpha,\beta}(\mathbb{F})$$
  and $\{h_1h_2 : (h_1,h_2) \in \mathcal{I}_2^{\alpha,\beta} \times \mathcal{I}_{n-2}^{1,1}\} \subseteq H_{n,5}^{\alpha,\beta}(\mathbb{F})$.
- If $\alpha\beta = 1$ and $n = 2$, then
  $$\{h_1h_2 : (h_1,h_2) \in \mathcal{I}_1^{\alpha,\beta\gamma} \times \mathcal{I}_1^{1,\gamma} \text{ and } h_1 \neq h_2\} \subseteq H_{n,4}^{\alpha,\beta}(\mathbb{F})$$
  and $\mathcal{I}_2^{\alpha,\beta} \subseteq H_{n,5}^{\alpha,\beta}(\mathbb{F})$.
- If $\alpha\beta = 1$ and $n \geq 4$ is even, then
  $$\{h_1h_2h_3h_4 : (h_1,h_2,h_3,h_4) \in \mathcal{I}_1^{\alpha,\beta\gamma} \times \mathcal{I}_1^{1,\gamma} \times \mathcal{I}_1^{1,1} \times \mathcal{I}_{n-3}^{1,1} : h_1,h_2,h_3,h_4 \text{ distinct}\} \subseteq H_{n,4}^{\alpha,\beta}(\mathbb{F})$$
  and $\{h_1h_2h_3 : (h_1,h_2,h_3) \in \mathcal{I}_2^{\alpha,\beta} \times \mathcal{I}_1^{1,1} \times \mathcal{I}_{n-3}^{1,1} : h_2 \neq h_3\} \subseteq H_{n,5}^{\alpha,\beta}(\mathbb{F})$.
- If $\alpha\beta = \gamma$ and n is odd, then
  $$\{h_1h_2h_3 : (h_1,h_2,h_3) \in \mathcal{I}_1^{\alpha,\beta} \times \mathcal{I}_1^{1,1} \times \mathcal{I}_{n-2}^{1,1},\ h_1,h_2,h_3 \text{ distinct}\}$$
  is a subset of $H_{n,4}^{\alpha,\beta}(\mathbb{F})$ and $H_{n,5}^{\alpha,\beta}(\mathbb{F})$.
- If $\alpha\beta = \gamma$ and n is even, then
  $$\{h_1h_2 : (h_1,h_2) \in \mathcal{I}_1^{\alpha,\beta} \times \mathcal{I}_{n-1}^{1,1} \text{ and } h_1 \neq h_2\}$$
  is a subset of $H_{n,4}^{\alpha,\beta}(\mathbb{F})$ and $H_{n,5}^{\alpha,\beta}(\mathbb{F})$.
- If $\alpha\beta = \gamma$ and n is odd, then
  $$\{h_1h_2h_3 : (h_1,h_2,h_3) \in \mathcal{I}_1^{\alpha,\beta} \times \mathcal{I}_1^{1,1} \times \mathcal{I}_{n-2}^{1,1} \text{ and } h_2 \neq h_3\} \subseteq H_{n,6}^{\alpha,\beta}(\mathbb{F}).$$
  If $\alpha\beta = \gamma$ and n is even, then $\{h_1h_2 : (h_1,h_2) \in \mathcal{I}_1^{\alpha,\beta} \times \mathcal{I}_{n-1}^{1,1}\} \subseteq H_{n,6}^{\alpha,\beta}(\mathbb{F})$.

The proposition follows immediately from the above inclusions and Lemma 5.5. □

5.3. **Proof of Proposition 1.12.** First fix a prime $\ell \in \Sigma$. Let κ be any coset of $\Omega(V_\ell)$ in $\mathrm{O}(V_\ell)$. There are unique $\varepsilon \in \{\pm 1\}$ and $\delta \in \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$ such that $\det(\kappa) = \{\varepsilon\}$ and $\mathrm{sp}(\kappa) = \{\delta\}$.

Take any $1 \leq i \leq 6$. We now define a subset $C_i(\kappa) \subseteq \kappa$ that is stable under conjugacy by $\mathrm{O}(V_\ell)$ (the sets of polynomials $F_{2n,i}(\mathbb{F}_\ell)$ are those from §5.2):

- If N is odd, let $C_i(\kappa)$ be the set of $A \in \kappa$ such that $\det(I - AT)/(1 - \varepsilon T)$ lies in $F_{N-1,i}(\mathbb{F}_\ell)$.
- If N is even and $\varepsilon = -1$, let $C_i(\kappa)$ be the set of $A \in \kappa$ such that $\det(I - AT)/(1 - T^2)$ lies in $F_{N-2,i}(\mathbb{F}_\ell)$.
- If N is even, $\varepsilon = 1$ and $i \neq 6$, let $C_i(\kappa)$ be the set of $A \in \kappa$ such that $\det(I - AT)$ lies in $F_{N,i}(\mathbb{F}_\ell)$.
- If N is even, $\varepsilon = 1$ and $i = 6$, define $C_i(\kappa) = \kappa$.

Lemma 5.6. *There is a positive constant c such that*
$$\frac{|C_i(\kappa)|}{|\Omega(V_\ell)|} \geq \frac{c}{N^2} \cdot (1 + O(1/\ell))$$
holds for all $1 \leq i \leq 6$, where c and the implicit constant are absolute.

Proof. • *Suppose that N is odd.*
Fix any $\alpha, \beta \in \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$ satisfying $\alpha\beta \neq (-1)^{(N-1)/2}(\mathbb{F}_\ell^\times)^2$ such that $\delta = \beta$ if $\varepsilon = 1$ and $\delta = \alpha\operatorname{disc}(V_\ell)$ if $\varepsilon = -1$. Take any $f \in F_{N-1,i}^{\alpha,\beta}(\mathbb{F}_\ell)$. Proposition 2.9 implies that

$$C_f := \{A \in \mathrm{O}(V_\ell) : \det(I - AT) = (1-\varepsilon)f(T)\}$$

is a conjugacy class of $\mathrm{O}(V_\ell)$ and

$$|C_f|/|\Omega(V_\ell)| \geq 2\ell^{-(N-1)/2}(1 + O(1/\ell))$$

with an absolute implicit constant. Note that for the constant to be absolute, we have used that f has at most eight irreducible factors.

By Proposition 2.9 and our choice of α and β, we have $\det(C_f) = \{\varepsilon\}$ and $\operatorname{sp}(C_f) = \{\delta\}$, and thus $C_f \subseteq \kappa$. Therefore,

$$|C_i(\kappa)|/|\Omega(V_\ell)| \geq |F_{N-1,i}^{\alpha,\beta}(\mathbb{F}_\ell)| \cdot 2\ell^{-(N-1)/2}(1 + O(1/\ell)) \gg 1/N^2 \cdot (1 + O(1/\ell))$$

with absolute constants, where the last inequality uses Proposition 5.4.
• *Suppose that N is even and $\varepsilon = -1$.*
Take any $\alpha, \beta \in \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$ and any $f \in F_{N-2,i}^{\alpha,\beta}(\mathbb{F}_\ell)$. Proposition 2.8 implies that

$$C_f := \{A \in \mathrm{O}(V_\ell) : \det(I - AT) = (1 - T^2)f(T) \text{ and } \operatorname{sp}(A) = \delta\}$$

is a conjugacy class of $\mathrm{O}(V_\ell)$ and $|C_f|/|\Omega(V_\ell)| \geq \ell^{-(N-2)/2}(1 + O(1/\ell))$ with an absolute constant. We have $C_f \subseteq \kappa$, so

$$|C_i(\kappa)|/|\Omega(V_\ell)| \geq |F_{N-2,i}^{\alpha,\beta}(\mathbb{F}_\ell)| \cdot \ell^{-(N-2)/2}(1 + O(1/\ell)) \gg 1/N^2 \cdot (1 + O(1/\ell))$$

with absolute constants, where the last inequality uses Proposition 5.4.
• *Suppose that N is even and $\varepsilon = 1$.*
If $i = 6$, we have $C_i(\kappa) = \kappa$ and the lemma is easy.

Now suppose that $1 \leq i \leq 5$. Take $\alpha, \beta \in \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$ such that $\delta = \beta$ and $\operatorname{disc}(V_\ell) = \alpha\beta$. Take any $f \in F_{N,i}^{\alpha,\beta}(\mathbb{F}_\ell)$. Proposition 2.7(ii) implies that

$$C_f := \{A \in \mathrm{O}(V) : \det(I - AT) = f(T)\}$$

is a conjugacy class of $\mathrm{O}(V_\ell)$ and $|C_f|/|\Omega(V_\ell)| \geq 4\ell^{-N/2}(1 + O(1/\ell))$ with an absolute constant. By Proposition 2.7(ii), we have $\det(C_f) = \{1\}$ and $\operatorname{sp}(C_f) = \{f(-1)(\mathbb{F}_\ell^\times)^2\} = \{\beta\}$. Therefore,

$$|C_i(\kappa)|/|\Omega(V_\ell)| \geq |F_{N,i}^{\alpha,\beta}(\mathbb{F}_\ell)| \cdot 4\ell^{-(N-2)/2}(1 + O(1/\ell)) \gg 1/N^2 \cdot (1 + O(1/\ell))$$

with absolute constants, where the last inequality uses Proposition 5.4 (recall that $i \neq 6$). □

For any integer $1 \leq i \leq 6$, define

$$C_i(V_\ell) := \bigcup_\kappa C_i(\kappa),$$

where the union is over the four cosets κ of $\Omega(V_\ell)$ in $\mathrm{O}(V_\ell)$. The set $C_i(V_\ell)$ is stable under conjugation by $\mathrm{O}(V_\ell)$. By Lemma 5.6, we have $|C_i(V_\ell) \cap \kappa|/|\kappa| = |C_i(\kappa)|/|\Omega(V_\ell)| \gg 1/N^2 \cdot (1 + O(1/\ell))$ for each coset κ. There are thus positive absolute constants c_1 and c_2 such that if $\ell \geq c_1$, then $|C_i(V_\ell) \cap \kappa|/|\kappa| \geq c_2/N^2$ for all cosets κ of $\Omega(V_\ell)$ in $\mathrm{O}(V_\ell)$.

We have now constructed sets $\{C_i(V_\ell)\}_{\ell \in \Sigma}$ for all $1 \leq i \leq 6$. It thus remains to verify that (iii) holds with these sets. Take any $u \in U(k)$, where k is a finite field that is an R-algebra. Suppose that for each $1 \leq i \leq 6$, there is a prime $\ell_i \in \Sigma$ for which $\bar{\rho}_{\ell_i}(\mathrm{Frob}_u) \in C_i(V_{\ell_i})$.

Let f_u be the polynomial obtained from P_u by the formula (1.2). Set $n = \deg(f_u)/2$. If N is odd, we have $N = 2n + 1$. If N is even, then N is $2n$ or $2n + 2$ when ε_u is 1 or -1, respectively.

For each $1 \leq i \leq 6$, with $i \neq 6$ when N is even and $\varepsilon_u = 1$, the inclusion $\bar{\rho}_{\ell_i}(\mathrm{Frob}_u) \subseteq C_i(V_{\ell_i})$ implies that f_u modulo ℓ_i lies in $F_{2n,i}(\mathbb{F}_\ell)$. If N is odd or $\varepsilon_u = -1$, Proposition 5.3(iii) implies that the Galois group of f_u, and hence also P_u, is isomorphic to W_{2n}.

Finally, suppose that N is even and $\varepsilon_u = 1$. The polynomial $P_u = f_u$ is separable since its reduction modulo ℓ_1 is separable. By Proposition 4.1(iii), the discriminant of P_u is a square in $\mathbb{Q}$ if and only if $K = \mathbb{Q}$. From Proposition 5.3(i) and (ii), we deduce that the Galois group of P_u is isomorphic to W_N^+ if $K = \mathbb{Q}$ and W_N if $K \neq \mathbb{Q}$.

6. Proof of Theorem 1.4

Fix notations and assumptions as in §1.3.

Suppose that R has characteristic 0 and hence $R = \mathbb{Z}[S^{-1}]$ for a finite set S of non-zero prime ideals of $\mathcal{O}_F$. Take $S' \supseteq S$ and $\Lambda \subseteq \Sigma$ as in Proposition 3.2. For the finite number of $\mathfrak{p} \in S' - S$, we can base extend everything to $\mathbb{F}_\mathfrak{p}$ and the assumptions of §1.3 still hold with the base ring $\mathbb{F}_\mathfrak{p}$. So Theorem 1.4 in the finite field case, would imply that $\delta(k) \to 1$ as we vary over all finite extensions k of $\mathbb{F}_\mathfrak{p}$ for some $\mathfrak{p} \in S' - S$. So assuming Theorem 1.4 in the finite field case, we can reduce to the case where we base extend everything to $R[S'^{-1}] = \mathbb{Z}[S'^{-1}]$. So without loss of generality, we may assume that Proposition 3.2 holds with $S' = S$ and $\Lambda \subseteq \Sigma$ a set of Dirichlet density 1. By replacing Λ by an appropriate subset with Dirichlet density 1, we may further assume that it satisfies Proposition 3.1.

If R is a finite field, we take Λ as in Proposition 3.1.

Let $c_1 \geq 5$ and c_2 be positive absolute constants as in Proposition 1.12(ii). By replacing c_2 with a smaller value, we may assume that $0 < c_2/N^2 < 1$. By removing a finite number of primes from Λ, we may also assume that each prime $\ell \in \Lambda$ is greater than c_1.

Take any $\varepsilon > 0$. We will prove that

$$1 - \delta(k) < \varepsilon + O(|k|^{-1/2}) \tag{6.1}$$

holds for all finite fields k that are R-algebras, where the implicit constant does not depend on k. This will imply that $0 \leq \limsup_{k,\,\#k\to\infty}(1-\delta(k)) \leq \varepsilon$ where k varies over finite fields that are R-algebras with increasing cardinality. Since $\varepsilon > 0$ was arbitrary, we will then have $\lim_{k,\,\#k\to\infty}\delta(k) = 1$ which will complete the proof of Theorem 1.4.

Since $0 < c_2/N^2 < 1$, we can choose an integer $M \geq 1$ satisfying $(1 - c_2/N^2)^M < \varepsilon/6$. Since Λ is infinite, we can choose a finite set $D \subseteq \Lambda$ of cardinality M. It suffices to prove that (6.1) holds when the characteristic of k does not lie in D (we can then repeat the proof with a different set $D \subseteq \Lambda$ of cardinality M that is disjoint from the original one).

Take any finite field k that is an R-algebra and whose characteristic does not lie in D. If $U(k)$ is empty, then $|k|$ is bounded and hence (6.1) holds for an appropriate implicit constant. We may thus assume that $U(k)$ is non-empty

For each integer $1 \leq i \leq 6$, define the set

$$\mathcal{S}_i = \{u \in U(k) : \bar{\rho}_\ell(\mathrm{Frob}_u) \not\subseteq C_i(V_\ell) \text{ for all } \ell \in D\},$$

where the sets $C_i(V_\ell)$ are from Proposition 1.12. Proposition 1.12(iii) implies that

$$\{u \in U(k) : P_u(T) \text{ does not satisfy } (1.4)\} \subseteq \bigcup\nolimits_{i=1}^{6} \mathcal{S}_i.$$

Therefore,

$$1 - \delta(k) = \frac{|\{u \in U(k) : P_u(T) \text{ does not satisfy } (1.4)\}|}{|U(k)|} \leq \sum_{i=1}^{6} |\mathcal{S}_i|/|U(k)|. \tag{6.2}$$

Now fix any $1 \leq i \leq 6$. Define $\bar{\rho}_D$ as in §3. We have

$$\mathcal{S}_i = \{u \in U(k) : \bar{\rho}_D(\mathrm{Frob}_u) \subseteq \mathcal{B}_i\},$$

where $\mathcal{B}_i = \prod_{\ell \in D}(\mathrm{O}(V_\ell) - C_i(V_\ell))$. Define $G = \bar{\rho}_D(\pi_1(U_k))$ and $G^g = \bar{\rho}_D(\pi_1(U_{\bar{k}}))$. Note that G^g is a normal subgroup of G and G/G^g is cyclic. Let hG^g be the G^g-coset of G that contains $\bar{\rho}_D(\mathrm{Frob}_u)$ for all $u \in U(k)$.

Lemma 6.1. *We have*

$$\frac{|\mathcal{S}_i|}{|U(k)|} = \frac{|\mathcal{B}_i \cap hG^g|}{|G^g|} + O(|k|^{-1/2}),$$

where the implicit constant does not depend on the choice of k.

Proof. Define the group $G^g_D := \bar{\rho}_D(\pi_1(U_{\bar{F}}))$, where F is the fraction field of R.

We claim that the groups G^g and G^g_D are conjugate in $\prod_{\ell \in D} \mathrm{O}(V_\ell)$. The claim is easy if R is a finite field since then k is a finite extension of F and the groups G^g and G^g_D depend only on the common algebraic closure of these fields. The case where R has characteristic 0 follows from Proposition 3.2; recall that we have reduced to the case where the proposition holds with $S' = S$.

The lemma follows from an equidistribution result with enough control over the error terms, for example [KS99, Theorem 9.7.13]. The above claim is needed to verify condition 9.7.2 (4) in [KS99]. □

By (6.2) and Lemma 6.1, we deduce that

$$1 - \delta(k) \leq \sum_{i=1}^{6} \frac{|\mathcal{B}_i \cap hG^g|}{|G^g|} + O(|k|^{-1/2}), \tag{6.3}$$

where the implicit constant does not depend on k.

We now bound $|\mathcal{B}_i \cap hG^g|/|G^g|$ for $1 \leq i \leq 6$. By Proposition 3.1 and our choice of Λ, we have $G^g \supseteq \prod_{\ell \in D}\Omega(V_\ell)$. Denote by m the index of $\prod_{\ell \in D}\Omega(V_\ell)$ in G^g. The G^g-coset hG^g is the disjoint union of m cosets of $\prod_{\ell \in D}\Omega(V_\ell)$; let κ be any of these m cosets. We have $\kappa = \prod_{\ell \in D} \kappa_\ell$, where κ_ℓ is a $\Omega(V_\ell)$-coset in $\mathrm{O}(V_\ell)$. Therefore,

$$\frac{|\mathcal{B}_i \cap \kappa|}{|\kappa|} = \prod_{\ell \in D}\left(1 - \frac{|C_i(V_\ell) \cap \kappa_\ell|}{|\kappa_\ell|}\right) \leq (1 - c_2/N^2)^{|D|} = (1 - c_2/N^2)^M < \varepsilon/6,$$

where the first inequality uses Proposition 1.12(ii) (note that $\ell \geq c_1$ for all $\ell \in \Sigma$) and the second inequality uses our choice of M. Therefore,

$$\frac{|\mathcal{B}_i \cap hG^g|}{|G^g|} = \sum_{\kappa \subseteq hG^g} \frac{|\mathcal{B}_i \cap \kappa|}{m|\kappa|} = \frac{1}{m} \sum_{\kappa \subseteq hG^g} \frac{|\mathcal{B}_i \cap \kappa|}{|\kappa|} < \varepsilon/6,$$

where the sums are over the m cosets of $\prod_{\ell \in D}\Omega(V_\ell)$ contained in hG^g. We deduce (6.1) from (6.3) and the above bound for $|\mathcal{B}_i \cap hG^g|/|G^g|$.

7. Proof of Theorem 1.6

Fix notations and assumptions as in §1.3 and §1.5. Let Λ be the set of natural density 1 that satisfies condition (b) of §1.3.3. Let $c_1 \geq 5$ and c_2 be positive absolute constants as in Proposition 1.12(ii). We may assume that each prime $\ell \in \Lambda$ is greater than c_1.

Take any $n \geq 1$. After base extending everything to $\mathbb{F}_{q^n}$, we find that the setup and assumptions of §1.3 and §1.5 still hold. Moreover, we may take the same sets Σ and Λ, and the integers g, b and N do not change. So to prove Theorem 1.6, we may assume without loss of generality that $n = 1$. We may further assume that $U(\mathbb{F}_q)$ is non-empty.

For each subset D of Λ, define the representation

$$\bar\rho_D = \prod_{\ell\in D} \bar\rho_\ell \colon \pi_1(U) \to \prod_{\ell \in D} \mathrm{O}(V_\ell);$$

note that the set D may be infinite now. Define the group $G_D := \bar\rho_D(\pi_1(U)) \subseteq \prod_{\ell\in D} \mathrm{O}(V_\ell)$ and its normal subgroup $G_D^g := \bar\rho_D(\pi_1(U_{\overline{\mathbb{F}}_q}))$. We have $G_D^g \supseteq \prod_{\ell\in D}\Omega(V_\ell)$; this follows for finite D by Proposition 3.1 and hence infinite D since the groups involved are profinite.

Denote the index of $\prod_{\ell\in\Lambda}\Omega(V_\ell)$ in G_Λ^g by m.

Lemma 7.1. *The value m is finite and satisfies $m \leq 2^{2g+b-1}$. We have $[G_\Lambda : G_\Lambda^g] \leq 2$.*

Proof. Since the groups $\prod_{\ell\in\Lambda}\Omega(V_\ell)$ and G_Λ^g are profinite, to bound m it suffices to prove that

$$[G_D^g : \textstyle\prod_{\ell\in D}\Omega(V_\ell)] \leq 2^{2g+b-1}$$

for any fixed finite $D \subseteq \Lambda$. Define $H = G_D^g / \prod_{\ell\in D}\Omega(V_\ell)$; it is a subgroup of $(\prod_{\ell\in D} \mathrm{O}(V_\ell))/(\prod_{\ell\in D}\Omega(V_\ell)) \cong (\mathbb{Z}/2\mathbb{Z})^{2|D|}$. Therefore, H is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ for some integer r. Let G be a finite group with cardinality relatively prime to q that is a quotient of $\pi_1(U_{\overline{\mathbb{F}}_q})$. The group G can be generated by a set of cardinality at most $2g+b-1$ by [SGA1, XIII Corollaire 2.12] . Since q is odd, we deduce that the group H is generated by $2g+b-1$ elements. Therefore, $r \leq 2g+b-1$ and hence $|H| \leq 2^{2g+b-1}$.

The group G_Λ/G_Λ^g is pro-cyclic since it is a quotient of the absolute Galois group of $\mathbb{F}_q$. However, every element in G_Λ/G_Λ^g has order 1 or 2 since it is a quotient of

$$G_\Lambda/(\prod_{\ell\in\Lambda}\Omega(V_\ell)) \subseteq (\prod_{\ell\in\Lambda}\mathrm{O}(V_\ell))/(\prod_{\ell\in\Lambda}\Omega(V_\ell)) \cong \prod_{\ell\in\Lambda}(\mathbb{Z}/2\mathbb{Z})^2.$$

Therefore, G_Λ/G_Λ^g is cyclic of order 1 or 2. □

Let hG_Λ^g be the coset of G_Λ^g in G_Λ which contains $\bar\rho_\Lambda(\mathrm{Frob}_u)$ for all $u \in U(\mathbb{F}_q)$. Fix one of the m cosets κ of $\prod_{\ell\in\Lambda}\Omega(V_\ell)$ in G_Λ that is also a subset of hG_Λ^g. We have $\kappa = \prod_{\ell\in\Lambda}\kappa_\ell$ for unique cosets κ_ℓ of $\Omega(V_\ell)$ in $\mathrm{O}(V_\ell)$. We also fix an integer $1 \leq i \leq 6$.

With κ and i fixed, let A be the set of $u \in U(\mathbb{F}_q)$ that satisfy $\bar\rho_\Lambda(\mathrm{Frob}_u) \subseteq \kappa$. Let $\{C_i(V_\ell)\}_{\ell\in\Lambda}$ be the sets from Proposition 1.12. For a prime $\ell \in \Lambda$, let A_ℓ be the set of $u \in A$ for which $\bar\rho_\ell(\mathrm{Frob}_u) \subseteq C_i(V_\ell)$ and define $\omega_\ell := |C_i(V_\ell) \cap \kappa_\ell|/|\kappa_\ell|$. For a subset $D \subseteq \Lambda$, define $A_D = \cap_{\ell\in D} A_\ell$; it is the set of $u \in A$ satisfying $\bar\rho_\ell(\mathrm{Frob}_u) \subseteq C_i(V_\ell)$ for all $\ell \in D$.

Lemma 7.2. *For every finite subset $D \subseteq \Lambda$, we have*

$$|A_D| = \frac{|U(\mathbb{F}_q)|}{m} \cdot \prod_{\ell\in D}\omega_\ell + r_D,$$

where $|r_D| \leq (\prod_{\ell\in D}\ell)^{N(N-1)/4}(2g+b)q^{1/2}$.

Proof. Take any finite subset $D \subseteq \Lambda$. Since m is finite by Lemma 7.1, there is a non-empty finite set $D \subseteq E \subseteq \Lambda$ such that the projection map

$$G_\Lambda/\textstyle\prod_{\ell\in\Lambda}\Omega(V_\ell) \to G_E/\prod_{\ell\in E}\Omega(V_\ell)$$

is an isomorphism. In particular, for $u \in U(\mathbb{F}_q)$, we have $\bar\rho_\Lambda(\mathrm{Frob}_u) \subseteq \kappa$ if and only if $\bar\rho_E(\mathrm{Frob}_u) \subseteq \prod_{\ell\in E}\kappa_\ell$.

Define

$$B := \prod_{\ell\in D}(C_i(V_\ell)\cap\kappa_\ell) \times \prod_{\ell\in E-D}\kappa_\ell;$$

it is a subset of G_E that is stable under conjugation. Observe that

$$A_D = \{u \in U(\mathbb{F}_q) : \bar{\rho}_E(\mathrm{Frob}_u) \subseteq B\}.$$

Define the subgroup $H := \prod_{\ell\in D}\{I\} \times \prod_{\ell\in E-D}\Omega(V_\ell)$ of G_E^g; it is a normal subgroup of G_E and satisfies $B \cdot H \subseteq B$. The representation $\bar{\rho}_E$ is tamely ramified since the representations $\{\bar{\rho}_\ell\}_{\ell\in\Lambda}$ are tamely ramified by assumption. By Theorem B.1(ii) in Appendix B, we have

$$|A_D| = \frac{|B|}{|G_E^g|} \cdot |U(\mathbb{F}_q)| + r_D,$$

where r_D satisfies $|r_D| \le |B|^{1/2}/|H|^{1/2} \cdot (2g+b)q^{1/2}$. By our choice of E, the index $[G_E^g : \prod_{\ell\in E}\Omega(V_\ell)]$ equals m. Therefore,

$$\frac{|B|}{|G_E^g|} = \frac{1}{m}\prod_{\ell\in D}\frac{|C_i(V_\ell)\cap\kappa_\ell|}{|\Omega(V_\ell)|} = \frac{1}{m}\prod_{\ell\in D}\omega_\ell$$

and it thus remains to prove the correct bound for $|r_D|$. We have $|B|/|H| \le (\prod_{\ell\in E}|\Omega(V_\ell)|)/|H| = \prod_{\ell\in D}|\Omega(V_\ell)|$ and hence $|r_D| \le \prod_{\ell\in D}|\Omega(V_\ell)|^{1/2}\cdot(2g+b)q^{1/2}$. It thus remains to prove that $|\Omega(V_\ell)| \le \ell^{N(N-1)/2}$ for all $\ell \in D$.

Take any $\ell \in D$. The possible cardinality for $|\mathrm{O}(V_\ell)|$ is given in [Wil09, §3.7.2]. If $N = 2n+1$ is odd, we find that $|\mathrm{O}(V_\ell)| \le 2\ell^{m^2+2+4+\cdots+2m} = 2\ell^{N(N-1)/2}$. If $N = 2n$ is even, we find that $|\mathrm{O}(V_\ell)| \le 2\ell^{m(m-1)+(2+4+\cdots+2(m-1))+m} = 2\ell^{N(N-1)/2}$. Therefore, $|\Omega(V_\ell)| \le \ell^{N(N-1)/2}/2$. □

We will now use Selberg's sieve, as described in Appendix A, to bound the cardinality of the set

$$S_{\kappa,i} := \{u \in A : \bar{\rho}_\ell(\mathrm{Frob}_u) \not\subseteq C_i(V_\ell) \text{ for all } \ell \in \Lambda\}.$$

Lemma 7.3. *We have*

$$|S_{\kappa,i}| \ll \Big(m^{-1}|U(\mathbb{F}_q)|\log q + (2g+b)q\Big)q^{-1/(N^2-N+6)},$$

where the implicit constant depends only on Λ*.*

Proof. For each $Q \ge 1$, let $\Lambda(Q)$ be the set of primes $\ell \in \Lambda$ with $\ell \le Q$. Since Λ has positive natural density, there is a constant $c_3 \ge 1$ such that

$$|\Lambda(Q)| \gg Q/\log Q$$

for all $Q \ge c_3$, where c_3 and the implicit constant depend only on Λ.

Set $X := |U(\mathbb{F}_q)|/m$. For each finite $D \subseteq \Lambda$, we have $|A_D| = (\prod_{\ell\in D}\omega_\ell)X + r_D$, where r_D satisfies the inequality from Lemma 7.2. We may assume that $\omega_\ell < 1$ for all $\ell \in \Lambda$ since otherwise $S_{\kappa,i} = \emptyset$ and the desired upper bound is trivial. We have $\ell \ge c_1$, and hence $\omega_\ell \ge c_2/N^2$, for all $\ell \in \Lambda$. In particular, $\omega_\ell > 0$ for all $\ell \in \Lambda$.

Fix a number $Q \ge c_3$. Observe that $S_{\kappa,i}$ is a subset of $A - (\cup_{\ell\in\Lambda(Q)}A_\ell)$. Let $\mathscr{X}(Q)$ be the set of finite subsets D of Λ, equivalently of $\Lambda(Q)$, such that $\prod_{\ell\in D}\ell \le Q$. We have $|\mathscr{X}(Q)| \le Q$. Therefore,

$$\sum_{D,D'\in\mathscr{X}(Q)}|r_{D\cup D'}| \le |\mathscr{X}(Q)|^2\cdot(Q^2)^{N(N-1)/4}(2g+b)q^{1/2} \le Q^{N(N-1)/2+2}(2g+b)q^{1/2}.$$

By the Selberg sieve (Theorem A.1), we obtain the bound

$$|S_{\kappa,i}| \le X/H(Q) + Q^{N(N-1)/2+2}(2g+b)q^{1/2},$$

where $H(Q) := \sum_{D\in\mathscr{X}(Q)}\prod_{\ell\in D}\omega_\ell/(1-\omega_\ell)$. Since $Q \ge c_3$, we have

$$H(Q) \ge \sum_{\ell\in\Lambda(Q)}\omega_\ell \ge \frac{c_2}{N^2}\cdot|\Lambda(Q)| \gg \frac{1}{N^2}Q/\log Q,$$

where we have used Proposition 1.12(ii). Therefore,

$$|S_{\kappa,i}| \ll m^{-1}|U(\mathbb{F}_q)|\cdot N^2\log(Q)/Q + Q^{N(N-1)/2+2}(2g+b)q^{1/2}.$$

Set $Q := q^{1/(N^2-N+6)}$. If $Q \geq c_3$, then

$$|S_{\kappa,i}| \ll \Big(m^{-1}|U(\mathbb{F}_q)|\log q + (2g+b)q\Big)q^{-1/(N^2-N+6)}. \tag{7.1}$$

If $Q < c_3$, then the bound (7.1) is immediate since

$$(2g+b)q\cdot q^{-1/(N^2-N+6)} \gg (2g+b)q \gg q + 2g\sqrt{q}+1 \geq |U(\mathbb{F}_q)| \geq |S_{\kappa,i}|. \qquad \square$$

Since hG_Λ^g is the union of m cosets $\kappa_1,\dots,\kappa_m$ of $\prod_{\ell\in\Lambda}\Omega(V_\ell)$, we have

$$\begin{aligned}&|\{u\in U(\mathbb{F}_q) : \bar\rho_\ell(\mathrm{Frob}_u)\not\subseteq C_i(V_\ell) \text{ for all } \ell\in\Lambda\}|\\ &\leq \sum_{j=1}^m |S_{\kappa_j,i}| \ll \Big(|U(\mathbb{F}_q)|\log q + m(2g+b)q\Big)q^{-1/(N^2-N+6)},\end{aligned}$$

where the last inquality uses Lemma 7.3. By Proposition 1.12(iii) and Lemma 7.1, we deduce that

$$\begin{aligned}1-\delta(\mathbb{F}_q) &= \frac{|\{u\in U(\mathbb{F}_q) : P_u(T) \text{ does not satisfies } (1.4)\}|}{|U(\mathbb{F}_q)|}\\ &\ll \Big(\log q + 2^{2g+b}(2g+b)q/|U(\mathbb{F}_q)|\Big)q^{-1/(N^2-N+6)}.\end{aligned}$$

If $g\leq\sqrt{q}/4$ and $b\leq q/4$, then $|U(\mathbb{F}_q)|\geq q+1-2g\sqrt{q}-b\geq q/4$ and hence

$$1-\delta(\mathbb{F}_q) \ll \Big(\log q + 2^{2g+b}(2g+b)\Big)q^{-1/(N^2-N+6)} \ll 2^{2g+b}(2g+b)\,q^{-1/(N^2-N+6)}\log q.$$

Finally suppose that $g\geq\sqrt{q}/4$ or $b\geq q/4$. Using $N\geq 3$, we find that

$$2^{2g+b}(2g+b)q^{-1/(N^2-N+6)}\log q \geq 2^{2g+b}q^{-1/12} \geq 2^{\sqrt{q}/4}q^{-1/12} \gg 1 \geq 1-\delta(\mathbb{F}_q).$$

8. Proof of Theorem 1.1

Let $\mathbb{P}$ be the projective space over $\mathbb{Z}$ consisting of non-zero homogenous polynomials of degree d in variables $x_0,\dots,x_{n+1}$ up to scalars. By ordering the monomials in $x_0,\dots,x_{n+1}$ of degree d, we obtain an isomorphism $\mathbb{P}\cong\mathbb{P}^m_{\mathbb{Z}}$ where $m=\binom{n+1+d}{d}-1$. Let $U\subseteq\mathbb{P}$ be the open subscheme corresponding to homogeneous polynomials that define a *smooth* hypersurface. From [KS99, §11.4.7], we know that U is smooth, connected, and that $U(k)$ is nonempty for all fields k. Let $H\subseteq U\times\mathbb{P}^{n+1}$ be the subscheme defined by pairs consisting of a homogeneous polynomial and a point on the corresponding hypersurface. The projection

$$\pi\colon H\to U$$

gives the *universal family of degree d hypersurfaces* in $\mathbb{P}^{n+1}$. For each point $f\in U(k)$, with k a field, we denote by H_f the fiber of π over f. Note that H_f is the hypersurface of $\mathbb{P}^{n+1}_k$ corresponding to f and agrees with the notation introduced in §1.2.

We now show that the setup of §1.3 applies with $R=\mathbb{Z}$. The following simply summarizes material presented by Katz in [Kat12, §8] with $X=\mathbb{P}^{n+1}_{\mathbb{Z}}$. Take a prime $\ell\geq 5$. We have a lisse $\mathbb{Z}_\ell$-sheaf $R^n\pi_*\mathbb{Z}_\ell(n)$ on $U_{\mathbb{Z}[1/\ell]}$. The cup product

$$R^n\pi_*\mathbb{Z}_\ell(n)\times R^n\pi_*\mathbb{Z}_\ell(n)\to R^{2n}\pi_*\mathbb{Z}_\ell(2n)\cong\mathbb{Z}_\ell$$

is an orthogonal autoduality modulo torsion (that the pairing is symmetric uses that n is even). On $\operatorname{Spec}\mathbb{Z}[1/\ell]$ we have the lisse $\mathbb{Z}_\ell$-sheaf $R^n\gamma_*\mathbb{Z}_\ell(n)$, where $\gamma\colon\mathbb{P}^{n+1}_{\mathbb{Z}[1/\ell]}\to\operatorname{Spec}\mathbb{Z}[1/\ell]$ is the structure morphism. The sheaf $R^n\gamma_*\mathbb{Z}_\ell(n)$ pulls back to a sheaf $\mathcal{F}_\ell$ on $U_{\mathbb{Z}[1/\ell]}$. We can view $\mathcal{F}_\ell$ as a subsheaf of $R^n\pi_*\mathbb{Z}_\ell(n)$, and we define $\mathrm{Ev}_{\mathbb{Z}_\ell}$ to be the orthogonal to $\mathcal{F}_\ell$ under the cup product pairing.

For ℓ sufficiently large, the lisse sheaf $\mathrm{Ev}_{\mathbb{Z}_\ell}$ is torsion free and the cup product makes $\mathrm{Ev}_{\mathbb{Z}_\ell}$ self dual over $\mathbb{Z}_\ell$. With such ℓ, let M_ℓ be the fiber of $\mathrm{Ev}_{\mathbb{Z}_\ell}$ at a geometric fiber of U; it gives rise to a representation

$$\rho_\ell\colon \pi_1(U_{\mathbb{Z}[1/\ell]}) \to \mathrm{O}(M_\ell)$$

These representations ρ_ℓ are compatible and the corresponding polynomials $P_f(T)$ are those described in §1.2. Note that the description of the zeta function of H_f from §1.2 is given in the second half of [Kat12, §8]. The zeta functions are also described in [KS99, §11.4] where it is observed that their common degree is $N := (d-1)((d-1)^{n+1}+1)/d$. So the M_ℓ have common rank N over $\mathbb{Z}_\ell$ and $N > 2$.

In [Kat12, §8], Katz observes that the representations ρ_ℓ satisfy condition (a) in §1.3.3. Moreover, he notes that the Zariski closure in condition (a) is always the full group $\mathrm{O}_{\mathcal{V}_\ell}$; using this and equidistribution, one can prove Remark 1.3. For this big monodromy result, we need our assumptions $d \geq 3$ and $(n, d) \neq (2, 3)$.

Using $N = (d-1)((d-1)^{n+1}+1)/d$ and n even, we find that N is even if and only if d is odd. The following, which we will prove in §8.1, describes the field K from §1.3.4 when N is even.

Lemma 8.1. *Suppose that N is even (equivalently, d is odd). Then $K = \mathbb{Q}(\sqrt{(-1)^{(d-1)/2}d})$. Moreover, $K = \mathbb{Q}$ if and only if d is a square.*

We have verified the axiomatic setup of §1.3. Lemma 8.1 describes the field K when N is even and in particular describes when $K = \mathbb{Q}$. Theorem 1.1 now follows from Theorem 1.4.

8.1. **Proof of Lemma 8.1.** Let $\mathcal{X}$ be a smooth hypersurface of degree d in $\mathbb{P}^{n+1}_{\mathbb{C}}$ and define the complex manifold $X := \mathcal{X}(\mathbb{C})$. Let h in $H^n(X, \mathbb{Z})$ be the class of a linear section of codimension $n/2$; we have $h^2 = d$. Let $L := H^n(X, \mathbb{Z})_\circ$ be the *primitive cohomology lattice*, i.e., the orthogonal complement in $H^n(X, \mathbb{Z})$ of the class h with respect to the usual intersection pairing. Note that L is a lattice, i.e., an orthogonal space over $\mathbb{Z}$, and so the discriminant of L is a well-defined integer. Beauville [Bea09, Theorem 4] describes the structure of L from which it is clear that $\mathrm{disc}(L) = \pm d$.

We can take M_ℓ to be the fiber of the sheaf $\mathrm{Ev}_{\mathbb{Z}_\ell}$ above the complex point corresponding to $\mathcal{X}$. For ℓ sufficiently large, the orthogonal space M_ℓ will be isomorphic to $L \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. So for ℓ sufficiently large, the orthogonal space $V_\ell := M_\ell/\ell M_\ell$ over $\mathbb{F}_\ell$ will have discriminant $\mathrm{disc}(L) \cdot (\mathbb{F}_\ell^\times)^2$.

From the description of K in §1.3.4, a sufficiently large prime ℓ splits in K if and only if $(-1)^{N/2}\,\mathrm{disc}(L)$ is a square modulo ℓ. Therefore, $K = \mathbb{Q}(\sqrt{(-1)^{N/2}\,\mathrm{disc}(L)})$. Using that $N = (d-1)((d-1)^{n+1}+1)/d$ and d is odd, we find that $N \equiv (d-1)/d \equiv d-1 \pmod 4$. Therefore, $K = \mathbb{Q}(\sqrt{(-1)^{(d-1)/2}\,\mathrm{disc}(L)})$.

We will show that $\mathrm{disc}(L) = d$ and hence $K = \mathbb{Q}(\sqrt{(-1)^{(d-1)/2}d})$. For K to be $\mathbb{Q}$, we certainly need d to be a square. If d is a square, then $d \equiv 1 \pmod 4$ since it is odd and thus $K = \mathbb{Q}$.

It remains to prove that $\mathrm{disc}(L) = d$. Since $\mathrm{disc}(L) = \pm d$, we need only show that $\mathrm{disc}(L)$ is positive.

We now consider the cohomology group $H^n(X, \mathbb{R})$. The cup product gives a non-degenerate symmetric pairing $H^n(X, \mathbb{R}) \times H^n(X, \mathbb{R}) \to \mathbb{R}$. So $H^n(X, \mathbb{R})$ is an orthogonal space over $\mathbb{R}$ and we will now compute its discriminant; there are two possibilities $(\mathbb{R}^\times)^2$ and $-1 \cdot (\mathbb{R}^\times)^2$. We claim that $\mathrm{disc}(H^n(X, \mathbb{R})) = (\mathbb{R}^\times)^2$. Since $H^n(X, \mathbb{R}) = L \otimes_{\mathbb{Z}} \mathbb{R} \oplus \mathbb{R}h$ and $h^2 = d > 0$, this claim will prove that $\mathrm{disc}(L)$ is positive. There is an orthogonal basis $v_1, \ldots, v_m$ over $\mathbb{R}$ of $H^n(X, \mathbb{R})$. By scaling the vectors, we may assume that $\langle v_i, v_i\rangle = \pm 1$. Let b^+ and b^- be the number of v_i for which $\langle v_i, v_i\rangle$ is 1 and -1, respectively. The discriminant of $H^n(X,\mathbb{R})$ is thus equal to $(-1)^{b_-}(\mathbb{R}^\times)^2$; so to complete the proof of Lemma 8.1, it suffices to show that b_- is even.

Lemma 8.2. *We have* $b_+ - b_- \equiv d \pmod 4$.

Proof. The Hodge index theorem [Voi02, Theorem 6.33] shows that

$$b_+ - b_- = \sum_{p,q} (-1)^p h^{p,q}(X),$$

where $h^{p,q}(X)$ is the (p,q)-Hodge number of X. For $0 \le i \le 2n$ with $i \ne n$, $\dim_{\mathbb{R}} H^i(X,\mathbb{R})$ is 0 if i is odd and 1 if i is even, cf. [KS99, §11.4.2]. So when $p+q \ne n$, we have $h^{p,q}(X) = 1$ if $0 \le p = q \le n$ and $h^{p,q}(X) = 0$ otherwise. Therefore,

$$b_+ - b_- = \sum_{p+q=n} (-1)^p h^{p,q}(X) + \sum_{0\le i\le n,\, i\ne n/2} (-1)^i = \sum_{p+q=n} (-1)^p h^{p,q}(X) + 1 - (-1)^{n/2}.$$

By Hirzebruch's formula for Hodge numbers, cf. [SGA7 II, Exposé XI Théorème 2.3], we have the following equality

$$\sum_{p\ge 0, q\ge 0} h_\circ^{p,q}\, y^p z^q = \frac{1}{(1+y)(1+z)}\left(\frac{(1+y)^d - (1+z)^d}{-(1+y)^d z + (1+z)^d y} - 1\right)$$

in $\mathbb{Z}[\![y,z]\!]$, where $h_\circ^{p,q} := h^{p,q} - \delta_{p,q}$ and $h^{p,q}$ is the (p,q)-Hodge number of any smooth hypersurface of degree d in $\mathbb{P}_{\mathbb{C}}^{2(p+q)+1}$. Setting $y = -x$ and $z = x$, we have

$$\sum_{m\ge 0}\left(\sum_{p+q=m} (-1)^p h_0^{p,q}\right) x^m = \frac{1}{(1-x)(1+x)}\left(\frac{(1-x)^d - (1+x)^d}{-(1-x)^d x - (1+x)^d x} - 1\right) = \frac{1}{1-x^2}(\alpha/\beta - 1),$$

where $\alpha := -\Big((1-x)^d - (1+x)^d\Big)/(2x)$ and $\beta := ((1-x)^d + (1+x)^d)/2$. Expanding out α and β, we find that

$$\begin{aligned} \alpha &= -\tfrac{1}{2}\textstyle\sum_{i\ge 0}\binom{d}{i}((-1)^i - 1)x^{i-1} = \sum_{k\ge 0}\binom{d}{2k+1}x^{2k} \quad \text{and} \\ \beta &= \tfrac{1}{2}\textstyle\sum_{i\ge 0}\binom{d}{i}((-1)^i + 1)x^i = \sum_{k\ge 0}\binom{d}{2k}x^{2k}. \end{aligned}$$

In particular, we have $\alpha, \beta \in \mathbb{Z}[\![x]\!]$. For each $k \ge 0$, we have

$$\binom{d}{2k+1} - d\binom{d}{2k} = \binom{d}{2k}\left(\frac{d-2k}{2k+1} - d\right) = \binom{d}{2k}\cdot\frac{-2k(d+1)}{2k+1} \equiv 0 \pmod 4,$$

where the congruence uses that d is odd. Therefore, $\alpha \equiv d\beta \pmod 4$. The constant term of β is 1, so $\beta^{-1} \in \mathbb{Z}[\![x]\!]$ and hence $\alpha/\beta \equiv d \pmod 4$. So

$$\sum_{m\ge 0}\left(\sum_{p+q=m} (-1)^p h_0^{p,q}\right) x^m \equiv \frac{1}{1-x^2}(d-1) = (d-1)(1 + x^2 + x^4 + x^6 + \cdots) \pmod 4$$

and hence

$$\sum_{p+q=n} (-1)^p h^{p,q} = \sum_{p+q=n} (-1)^p h_\circ^{p,q} + (-1)^{n/2} \equiv d - 1 + (-1)^{n/2} \pmod 4.$$

Therefore, $b_+ - b_- \equiv (d - 1 + (-1)^{n/2}) + 1 - (-1)^{n/2} \equiv d \pmod 4$. □

We have $b_+ + b_- = N + 1 = (d-1)((d-1)^{n+1}+1)/d + 1$. Using that d is odd and $n+1 \geq 2$, we find that $b_+ + b_- \equiv (d-1)/d + 1 \equiv d \pmod 4$. By Lemma 8.2. we deduce that

$$2b_- = (b_+ + b_-) - (b_+ - b_-) \equiv d - d = 0 \pmod 4.$$

This implies that b_- is even as desired.

9. Proof of Theorems 1.7 and 1.10

We first check the axiomatic setup of §1.3 with $R = \mathbb{F}_q$ and $U = U_d$. Let Σ be the set of primes $\ell \geq 5$ that do not divide q.

Take any $\ell \in \Sigma$. Following Katz, Hall constructs in [Hal08, §6.2] a representation

$$\bar{\rho}_\ell \colon \pi_1(U_d) \to \mathrm{O}(V_\ell),$$

with V_ℓ an orthogonal space over $\mathbb{F}_\ell$, satisfying

$$P_u(T) \equiv \det(I - \bar{\rho}_\ell(\mathrm{Frob}_u)T) \pmod \ell$$

for all $n \geq 1$ and $u \in U_d(\mathbb{F}_{q^n})$. One can easily see that $\bar{\rho}_\ell$ arises from a representation $\rho_\ell \colon \pi_1(U_d) \to \mathrm{O}(M_\ell)$, with M_ℓ an orthogonal space over $\mathbb{Z}_\ell$ and $V_\ell \cong M_\ell/\ell M_\ell$, satisfying

$$P_u(T) = \det(I - \rho_\ell(\mathrm{Frob}_u)T) \tag{9.1}$$

for all $n \geq 1$ and $u \in U_d(\mathbb{F}_{q^n})$ (in Hall's construction, simply replace $\mathcal{T}_{d,\ell}$ with the $\mathbb{Z}_\ell$-sheaf $\mathcal{T}_{d,\ell^\infty}$ described in [Hal08, §6.6]). The common dimension of the V_ℓ is our integer N_d by [Hal08, Lemma 6.2]. We have $N_d \geq 3$ by assumption.

It remains to verify that condition (b) in §1.3.3 holds. To do this, we will restrict to a subvariety of U_d; after possibly replacing $\mathbb{F}_q$ by a finite extension, one can further assume that $U_{d-1}(\mathbb{F}_q)$ is non-empty.

Now fix a polynomial $g \in U_{d-1}(\mathbb{F}_q)$. We let U be the subvariety of $\mathbb{A}^1_{\mathbb{F}_q}$ consisting of c for which $(t-c)g(t)$ is separable and relatively prime to $m(t)$. We can identify U with a closed subvariety of U_d via the map $c \mapsto (t-c)g(t)$. Restricting ρ_ℓ and $\bar{\rho}_\ell$ to $\pi_1(U)$ gives representations $\varrho_\ell \colon \pi_1(U) \to \mathrm{O}(M_\ell)$ and $\bar{\varrho}_\ell \colon \pi_1(U) \to \mathrm{O}(V_\ell)$. These representations satisfy the axiomatic setup of §1.3.1 and §1.3.2 with $R = \mathbb{F}_q$ and the same set Σ from the above discussion. Moreover, each representation ϱ_ℓ is tamely ramified, cf. [Hal08, §6.3].

Let Λ be the set of $\ell \in \Sigma$ which do not divide $\max\{1, -\mathrm{ord}_v(j_E)\}$ for any place v of $\mathbb{F}_q(t)$, where $j_E \in \mathbb{F}_q(t)$ is the j-invariant of E. We now show that condition (b) holds for the representations $\{\varrho_\ell\}_{\ell \in \Lambda}$.

Lemma 9.1. *For each prime $\ell \in \Lambda$, we have $\bar{\varrho}_\ell(\pi_1(U_{\overline{\mathbb{F}}_q})) \supseteq \Omega(V_\ell)$ and $\bar{\varrho}_\ell(\pi_1(U_{\overline{\mathbb{F}}_q}))$ is not a subgroup of* $\mathrm{SO}(V_\ell)$.

Proof. After replacing E by its quadratic twist by $g(t)$, we may assume without loss of generality that $d = 1$. Note that performing this twist leaves the integer B unchanged. Using the assumptions of the theorems, there will be a place $v \neq \infty$ of $\mathbb{F}_q(t)$ for which E has Kodaira symbol I_0^*. There is also a place $v \neq \infty$ for which E has multiplicative reduction, i.e., E has Kodaira symbol I_n at v for some $n \geq 1$. The lemma is now a direct consequence of [Zyw14, Theorem 3.4] which is an explicit version of [Hal08, Theorem 6.4]. □

An immediate consequence of Lemma 9.1 is that $\bar{\rho}_\ell(\pi_1(U_{d,\overline{\mathbb{F}}_q})) \supseteq \Omega(V_\ell)$ for all $\ell \in \Lambda$ and $\bar{\rho}_\ell(\pi_1(U_{d,\overline{\mathbb{F}}_q}))$ is not a subgroup of $\mathrm{SO}(V_\ell)$.

Remark 9.2. Using that $\bar{\rho}_\ell(\pi_1(U_{d,\overline{\mathbb{F}}_q}))$ is not a subgroup of $\mathrm{SO}(V_\ell)$ and equidistribution, one can prove Remark 1.8(v) which says that $|\{u \in U_d(\mathbb{F}_{q^n}) : \varepsilon_u = \varepsilon\}|/|U(\mathbb{F}_{q^n})| \to 1/2$ as $n \to \infty$ for each $\varepsilon \in \{\pm 1\}$

We have now verified enough to apply Theorems 1.4 and 1.6 to the representations $\{\rho_\ell\}_{\ell\in\Lambda}$. Note that U is open in $\mathbb{A}^1_{\mathbb{F}_q} \subseteq \mathbb{P}^1_{\mathbb{F}_q}$ and $|(\mathbb{P}^1 - U)(\overline{\mathbb{F}}_q)| = d + \deg m$.

Theorems 1.7 and 1.10 are now immediate if we can prove that $K = \mathbb{Q}(\sqrt{(-1)^{N_d/2} D_d})$ if N_d is even.

Now suppose that N_d is even. It remains to compute the field K from §1.3.4 and determine when $K = \mathbb{Q}$. The following lemma depends on a result from [Zyw14] which uses known cases of the Birch and Swinnerton-Dyer conjecture for elliptic curves over global function fields.

Lemma 9.3. *For $\ell \in \Lambda$, we have* $\mathrm{disc}(V_\ell) = D_d \cdot (\mathbb{F}_\ell^\times)^2$.

Proof. Take any $\ell \in \Lambda$. By Lemma 9.1, there is an element $g \in \bar{\varrho}_\ell(\pi_1(U))$ such that $\det(I \pm g) \neq 0$. By equidistribution, there is some $c \in U(\mathbb{F}_{q^n})$ such that $\bar{\varrho}_\ell(\mathrm{Frob}_c)$ is conjugate to g in $\mathrm{O}(V_\ell)$. By [Zyw14, Proposition 3.2(e)], we have $\mathrm{disc}(V_\ell) = D \cdot (\mathbb{F}_\ell^\times)^2$, where $D := \prod_v \gamma_v(E_{t-c})^{\deg v}$ and the product is over places v of $\mathbb{F}_{q^n}(t)$. We have $D = \gamma_\infty(E_{t^d}) \prod_{v\neq\infty} \gamma_v(E_{t-c})^{\deg v}$, where the product is over places v of $\mathbb{F}_{q^n}(t)$. We have $D = D_d$ by noting that the integer $\gamma_\infty(E_{t^d}) \prod_{v\neq\infty} \gamma_v(E_{t-c})^{\deg v}$ does not change if we consider v running over places of $\mathbb{F}_q(t)$ instead of $\mathbb{F}_{q^n}(t)$. □

By Lemma 9.3, we have $K = \mathbb{Q}(\sqrt{(-1)^{N_d/2} D_d})$. In particular, $K = \mathbb{Q}$ if and only if $(-1)^{N_d/2} D_d$ is a square.

Appendix A. The Selberg sieve

In this appendix, we give a version of Selberg's sieve. This elegant and useful method was introduced by Selberg in [Sel47] to sieve integers by congruences modulo primes. For background, see [IK04, §6.5] or [CM06, §7.2]. For future reference, we give a version that is more general than what is required for our application.

Theorem A.1. *Let A be a measure space with a bounded measure μ. Let Λ be a finite set, and for each $\lambda \in \Lambda$ fix a measurable subset A_λ of A. Define the set*

$$S := A - \Big(\cup_{\lambda\in\Lambda} A_\lambda\Big).$$

Fix real numbers $\{\omega_\lambda\}_{\lambda\in\Lambda}$ with $0 < \omega_\lambda < 1$ and $X \geq 0$. Define $A_D := \cap_{\lambda\in D} A_\lambda$ for each non-empty $D \subseteq \Lambda$ and set $A_\emptyset := A$. Let r_D be the real number satisfying

$$\mu(A_D) = \Big(\prod_{\lambda\in D} \omega_\lambda\Big) \cdot X + r_D. \tag{A.1}$$

Let $\mathscr{X}$ be a set of subsets of Λ such that if $D \in \mathscr{X}$ and $E \subseteq D$, then $E \in \mathscr{X}$. Then

$$\mu(S) \leq \frac{X}{H} + \sum_{D,D'\in\mathscr{X}} |r_{D\cup D'}| \tag{A.2}$$

where $H := \sum_{D\in\mathscr{X}} \prod_{\lambda\in D} \frac{\omega_\lambda}{1-\omega_\lambda}$. (When $H = 0$, we interpret this as giving the trivial bound $\mu(S) \leq +\infty$.)

Before proceeding, let us first give some context. After normalizing the measure, we may assume that (A, μ) is a probability space and hence use the language of probability. For each $\lambda \in \Lambda$, we have fixed an event A_λ. So S is the set of outcomes that do not belong to any of the elements A_λ.

Consider the special case where the events $\{A_\lambda\}_{\lambda\in\Lambda}$ are independent. We have $\mu(S)=\prod_{\lambda\in\Lambda}(1-\omega_\lambda)$. Set $\omega_\lambda=\mu(A_\lambda)$ and $X=1$. In (A.1), we take $r_D=0$ for $D\subseteq\Lambda$. With $\mathscr{X}$ the power set of Λ, we have $H=\prod_{\lambda\in\Lambda}(1+\omega_\lambda/(1-\omega_\lambda))=\prod_{\lambda\in\Lambda}(1-\omega_\lambda)^{-1}$ and hence our sieve gives the optimal bound $\mu(S)\leq\prod_{\lambda\in\Lambda}(1-\omega_\lambda)$.

In the general setting, we think of the sets A_λ as being "almost independent" and hence the number r_D should be relatively small (at least for some D of small cardinality). Inclusion-exclusion gives

$$\mu(S)=\sum_{D\subseteq\Lambda}(-1)^{|D|}\mu(A_D)=\sum_{D\subseteq\Lambda}(-1)^{|D|}\Big(\prod_{\lambda\in D}\omega_\lambda\Big)X+R=\prod_{\lambda\in\Lambda}(1-\omega_\lambda)\cdot X+R$$

with $R:=\sum_{D\subseteq\Lambda}(-1)^{|D|}r_D$. In practice, the "error term" R can be difficult to control and may in fact exceed the "main term". To find upper bounds for $\mu(S)$ using our sieve, one need to prudently select the sieve support $\mathscr{X}$ so that "error term" in (A.2) is not too large.

A.1. **Proof of Theorem A.1.** For $D\subseteq\Lambda$, define $\omega_D=\prod_{\lambda\in D}\omega_\lambda$. For each non-empty $D\in\mathscr{X}$, we fix a real number λ_D that will be chosen later. Set $\lambda_\emptyset=1$. For any $U\subseteq A$, let $\chi_U\colon A\to\{0,1\}$ be the characteristic function of U, i.e., $\chi_U(a)=1$ if and only if $a\in U$. The set U is measurable if and only if $\chi_U\colon A\to\{0,1\}$ is measurable. For each $a\in A$, we claim that

$$\chi_S(a)\leq\Big(\sum_{D\in\mathscr{X}}\chi_{A_D}(a)\lambda_D\Big)^2.$$

If $a\notin S$, then $\chi_S(a)=0$ and the above inequality is immediate since the square of a real number is non-negative. If $a\in S$, then $\sum_{D\in\mathscr{X}}\chi_{A_D}(a)\lambda_D=\lambda_\emptyset=1$. Therefore,

$$\mu(S)=\int_A\chi_S(a)d\mu(a)\leq\int_A\Big(\sum_{D\in\mathscr{X}}\chi_{A_D}(a)\lambda_D\Big)^2d\mu(a)=\sum_{D,D'\in\mathscr{X}}\Big(\int_A\chi_{A_D}(a)\chi_{A_{D'}}(a)d\mu(a)\Big)\lambda_D\lambda_{D'}$$

and thus $\mu(S)\leq\sum_{D,D'\in\mathscr{X}}\mu(A_{D\cup D'})\lambda_D\lambda_{D'}$. Using (A.1), this inequality becomes

$$\mu(S)\leq\Delta\cdot X+R$$

where

$$\Delta=\sum_{D,D'\in\mathscr{X}}\omega_{D\cup D'}\lambda_D\lambda_{D'}\quad\text{and}\quad R=\sum_{D,D'\in\mathscr{X}}r_{D\cup D'}\lambda_D\lambda_{D'}.$$

We first study Δ. By the multiplicative definition of ω_D, we have

$$\Delta=\sum_{D,D'\in\mathscr{X}}\frac{\omega_D\omega_{D'}}{\omega_{D\cap D'}}\lambda_D\lambda_{D'}.$$

For $D,D'\in\mathscr{X}$, we have

$$\frac{1}{\omega_{D\cap D'}}=\prod_{\lambda\in D\cap D'}\Big(1+\frac{1-\omega_\lambda}{\omega_\lambda}\Big)=\sum_{E\subseteq D\cap D'}\prod_{\lambda\in E}\frac{1-\omega_\lambda}{\omega_\lambda}$$

and thus

$$\Delta=\sum_{D,D'\in\mathscr{X}}\omega_D\omega_{D'}\Big(\sum_{E\subseteq D\cap D'}\prod_{\lambda\in E}\frac{1-\omega_\lambda}{\omega_\lambda}\Big)\lambda_D\lambda_{D'}=\sum_{E\in\mathscr{X}}\Big(\prod_{\lambda\in E}\frac{1-\omega_\lambda}{\omega_\lambda}\Big)\sum_{\substack{D,D'\in\mathscr{X}\\E\subseteq D,E\subseteq D'}}\omega_D\omega_{D'}\lambda_D\lambda_{D'}.$$

So

$$\Delta=\sum_{E\in\mathscr{X}}\Big(\prod_{\lambda\in E}\frac{1-\omega_\lambda}{\omega_\lambda}\Big)\xi_E^2\tag{A.3}$$

where $\xi_E := (-1)^{|E|} \sum_{E\subseteq D \in \mathscr{X}} \omega_D \lambda_D$ for $E \in \mathscr{X}$. By Möbius inversion, for $D \in \mathscr{X}$ we have

$$\omega_D \lambda_D = \sum_{D\subseteq E\in\mathscr{X}} (-1)^{|E|-|D|} \cdot (-1)^{|E|} \xi_E = (-1)^{|D|} \sum_{D\subseteq E\in\mathscr{X}} \xi_E \tag{A.4}$$

and in particular, $\sum_{E\in\mathscr{X}} \xi_E = \lambda_\emptyset = 1$.

Since Δ shows up in our upper bound for $\mu(S)$, we now minimize its value. With (A.3) we view Δ as a quadratic form in the variables $(\xi_E)_{E\in\mathscr{X}}$ subject to the constraint $\sum_{E\in\mathscr{X}} \xi_E = 1$; it is not hard to show that Δ obtains its minimum value of $H^{-1} = \left(\sum_{D\in\mathscr{X}} \prod_{\lambda\in D} \frac{\omega_\lambda}{1-\omega_\lambda}\right)^{-1}$ when

$$\xi_E = \frac{1}{H} \prod_{\lambda\in E} \frac{\omega_\lambda}{1-\omega_\lambda}$$

for $E \in \mathscr{X}$. With these optimized values of ξ_E and (A.4), we now *define*

$$\lambda_D := \frac{1}{H} \frac{(-1)^{|D|}}{\omega_D} \sum_{D\subseteq E\in\mathscr{X}} \prod_{\lambda\in E} \frac{\omega_\lambda}{1-\omega_\lambda} \tag{A.5}$$

for each $D \in \mathscr{X}$. By our choice, we have $\Delta = H^{-1}$ and hence $\mu(S) \leq X/H + R$. It remains to bound R. For each $D \in \mathscr{X}$,

$$0 \leq (-1)^{|D|}\lambda_D = \frac{1}{H} \prod_{\lambda\in D}\left(1 + \frac{\omega_\lambda}{1-\omega_\lambda}\right) \sum_{D\subseteq E\in\mathscr{X}} \prod_{\lambda\in E-D} \frac{\omega_\lambda}{1-\omega_\lambda} \leq \frac{1}{H} \sum_{E\in\mathscr{X}} \prod_{\lambda\in E} \frac{\omega_\lambda}{1-\omega_\lambda} = 1.$$

Therefore,

$$R \leq \sum_{D,D'\in\mathscr{X}} |r_{D\cup D'}||\lambda_D||\lambda_{D'}| \leq \sum_{D,D'\in\mathscr{X}} |r_{D\cup D'}|.$$

Appendix B. Equidistribution

Let U be an affine variety of dimension $d \geq 1$ over a finite field $\mathbb{F}_q$ that is geometrically smooth and irreducible. Let $\rho\colon \pi_1(U) \to G$ be a surjective and continuous homomorphism, where $\pi_1(U)$ is the étale fundamental group and G is a finite group. Let G^g be the image of $\pi_1(U_{\overline{\mathbb{F}}_q})$ under ρ and define $m = [G : G^g]$. We have an exact sequence of groups

$$1 \to G^g \hookrightarrow G \xrightarrow{\varphi} \mathbb{Z}/m\mathbb{Z} \to 1$$

such that $\varphi(\mathrm{Frob}_u) \equiv n \pmod m$ for all $u \in U(\mathbb{F}_{q^n})$.

Theorem B.1. *Fix an integer $n \geq 1$. Let C be a subset of G that is stable under conjugation and satisfies $\varphi(C) = \{n \bmod m\}$.*

(i) *Then*

$$\frac{|\{u \in U(\mathbb{F}_{q^n}) : \rho(\mathrm{Frob}_u) \subseteq C\}|}{|U(\mathbb{F}_{q^n})|} = \frac{|C|}{|G^g|} + O(q^{-n/2}),$$

where the implicit constant does not depend on n.

(ii) *Assume further that U is of dimension 1 and ρ is tamely ramified. Let $X/\mathbb{F}_q$ be the smooth projective curve obtained by completing U. Let g be the genus of X and define $b = |X(\overline{\mathbb{F}}_q) - U(\overline{\mathbb{F}}_q)|$. Suppose that $H \subseteq G^g$ is a normal subgroup of G that satisfies $C \cdot H \subseteq C$. Then*

$$\left| |\{u \in U(\mathbb{F}_q) : \rho(\mathrm{Frob}_u) \subseteq C\}| - \frac{|C|}{|G^g|}|U(\mathbb{F}_q)| \right| \leq \frac{|C|^{1/2}}{|H|^{1/2}} (1 - |H|/|G^g|)^{1/2} (2g - 2 + b) q^{1/2}.$$

Proof. Both parts are applications of the machinery of Grothendieck and Deligne used to prove the Weil conjectures. Part (i) is well known; a proof can be found in [Cha97, §4]. For (ii), one can replace ρ with the representation $\pi_1(U,\eta) \xrightarrow{\rho} G \to G/H$ and reduce to the case where $H = 1$. This case has already been dealt with by the author, cf. [Zyw10b, Proposition 5.1]. □

References

[ATLAS] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray. ↑2.2, 3.1

[AV08] Omran Ahmadi and Gerardo Vega, *On the parity of the number of irreducible factors of self-reciprocal polynomials over finite fields*, Finite Fields Appl. **14** (2008), no. 1, 124–131. ↑2.3, 2.3

[Bea09] Arnaud Beauville, *The primitive cohomology lattice of a complete intersection*, C. R. Math. Acad. Sci. Paris **347** (2009), no. 23-24, 1399–1402 (English, with English and French summaries). ↑8.1

[Cha97] Nick Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. **87** (1997), no. 1, 151–180. ↑1.7, B

[CM06] Alina Carmen Cojocaru and M. Ram Murty, *An introduction to sieve methods and their applications*, London Mathematical Society Student Texts, vol. 66, Cambridge University Press, Cambridge, 2006. ↑A

[CCH05] B. Conrad, K. Conrad, and H. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. Math. **198** (2005), no. 2, 684–731. ↑1.9

[Gal73] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), 1973, pp. 91–101. ↑5.1

[GM02] Benedict H. Gross and Curtis T. McMullen, *Automorphisms of even unimodular lattices and unramified Salem numbers*, J. Algebra **257** (2002), no. 2, 265–290. ↑2.4

[Hal08] Chris Hall, *Big symplectic or orthogonal monodromy modulo ℓ*, Duke Math. J. **141** (2008), no. 1, 179–203. ↑9, 9, 9

[IK04] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. ↑A

[Jou09] Florent Jouve, *Maximal Galois group of L-functions of elliptic curves*, Int. Math. Res. Not. IMRN **19** (2009), 3557–3594. ↑1.11, 5.2

[Kat90] Nicholas M. Katz, *Exponential sums and differential equations*, Annals of Mathematics Studies, vol. 124, Princeton University Press, Princeton, NJ, 1990. ↑3.1

[Kat12] Nicholas M. Katz, *Report on the irreducibility of L-functions*, Number theory, analysis and geometry, 2012, pp. 321–353. ↑i, 1.7, 8

[KS99] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999. ↑6, 8, 8.1

[Lar95] M. Larsen, *Maximality of Galois actions for compatible systems*, Duke Math. J. **80** (1995), no. 3, 601–630. ↑3.1

[Sel47] Atle Selberg, *On an elementary method in the theory of primes*, Norske Vid. Selsk. Forh., Trondhjem **19** (1947), no. 18, 64–67. ↑A

[SGA1] *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3, Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)]. ↑3.1, 7

[SGA7 II] *Groupes de monodromie en géométrie algébrique. II*, Lecture Notes in Mathematics, Vol. 340, Springer-Verlag, Berlin-New York, 1973 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II); Dirigé par P. Deligne et N. Katz. ↑8.1

[Voi02] Claire Voisin, *Hodge theory and complex algebraic geometry. I*, Cambridge Studies in Advanced Mathematics, vol. 76, Cambridge University Press, Cambridge, 2002. Translated from the French original by Leila Schneps. ↑8.1

[Wil09] Robert A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London Ltd., London, 2009. ↑2.2, 7

[Zas62] Hans Zassenhaus, *On the spinor norm*, Arch. Math. **13** (1962), 434–451. ↑2.2

[Zyw10a] David Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. London Math. Soc. **42** (2010), no. 5, 811–826. ↑3.1

[Zyw10b] ______, *Hilbert's irreducibility theorem and the larger sieve* (2010), available at https://arxiv.org/abs/1011.6465. arXiv:1011.6465. ↑B

[Zyw14] ______, *The inverse Galois problem for orthogonal groups* (2014), available at https://arxiv.org/abs/1409.1151. arXiv:1409.1151. ↑iii, 9, 9, 9

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
Email address: zywina@math.cornell.edu