AN OPEN IMAGE THEOREM FOR A GENERAL CLASS OF ABELIAN VARIETIES

CHRIS HALL

ABSTRACT. Let K be a number field and A/K be a polarized abelian variety with absolutely trivial endomorphism ring. We show that if the Néron model of A/K has at least one fiber with potential toric dimension one, then for almost all rational primes ℓ, the Galois group of the splitting field of the ℓ-torsion of A is $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell)$.

1. Introduction

Let K be a number field and A/K a polarized abelian g-fold with trivial $\overline{K}$-endomorphism ring. For each rational prime ℓ, let A_ℓ denote the ℓ-torsion of A and G_ℓ the Galois group of the splitting-field extension $K(A_\ell)/K$. If $g = 1$, then A/K is an elliptic curve and a well-known theorem of Serre asserts that G_ℓ is isomorphic to $\mathrm{GSp}_2(\mathbb{Z}/\ell) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell)$ for all sufficiently large ℓ [S2, Theorem 2]. In a series of lectures and letters Serre (cf. [S4, Corollaire au Théorème 3]) later showed how to extend the result to the case when g is odd, 2, or 6: if ℓ is sufficiently large, then $G_\ell \simeq \mathrm{GSp}_{2g}(\mathbb{Z}/\ell)$. However, for general g it is an open problem to show that G_ℓ is as big as possible for almost all ℓ. In this paper we show that this is true when we assume an additional hypothesis on the reduction of A, and our main theorem is the following.

Theorem 1. *Suppose A/K satisfies the following property:*

(T) : there is a finite extension L/K so that the Néron model of A/L over the ring of integers $\mathcal{O}_L$ has a semistable fiber with toric-dimension one.

If ℓ is sufficiently large with respect to A and K, then $G_\ell \simeq \mathrm{GSp}_{2g}(\mathbb{Z}/\ell)$.

The rest of this paper is devoted to a proof of the theorem. In section 2 we prove the theorem modulo a result of Serre on the rigidity of inertial tori, and in section 3 we prove the necessary rigidity result.

An example due to Mumford shows that one cannot remove hypothesis (T) from the statement of our theorem [M, Section 4]. More precisely, Mumford constructed

2000 *Mathematics Subject Classification.* 11G10,14K15.

an abelian 4-fold with absolutely trivial endomorphism ring such that G_ℓ does not contain $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell)$ for infinitely many ℓ. His 4-fold does not satisfy hypothesis (T) because it has potentially good reduction everywhere; for infinitely many ℓ there are no non-trivial unipotent elements $u \in G_\ell$ satisfying $(u-1)^2 = 0$, while potential positive-dimension toric reduction would give rise to such elements. More importantly, Mumford's example fails to satisfy the conclusion of the theorem because its so-called Mumford-Tate group is strictly smaller than for those 4-folds addressed in the theorem (cf. [S3, annotation 4]). However, the groups G_ℓ are as big as possible for almost all ℓ once one takes into consideration the upper bound imposed by the Mumford-Tate group, and for a general polarized abelian g-fold A/K it is conjectured that G_ℓ is almost always as big as possible given the constraints imposed by the endomorphism ring and Mumford-Tate group.

While Mumford's example shows that an arbitrary abelian g-fold will not satisfy the hypothesis (nor the conclusion) of the theorem, one can ask for the likelihood that a "random" A/K will have absolutely trivial endomorphism ring and satisfy hypothesis (T). For $g = 1$, a necessary and sufficient condition is that j-invariant does not lie in the ring of integers of K. For $g > 1$, if $n = 2g + 2$ or $2g + 1$ and $f(x)$ is a degree-n polynomial in $K[x]$ whose splitting field has Galois group S_n, then Zarhin showed that the endomorphism ring of the Jacobian of the hyperelliptic curve $y^2 = f(x)$ is absolutely trivial [Z, Theorem 2.1]. If moreover there is a prime $\mathfrak{p}$ in K such that the reduction of $f(x)$ modulo $\mathfrak{p}$ (is defined and) has $n-1$ distinct zeros (over an algebraic closure), one of which is a double zero, then the Jacobian satisfies (T).

In an appendix to this paper E. Kowalski shows that most monic polynomials in $K[x]$ with integral coefficients satisfy both these properties, thus for most hyperelliptic curves over K the Jacobian satisfies the hypotheses of the theorem. Of course, for $g > 2$ most polarized abelian g-folds A/K do not arise as the Jacobians of hyperelliptic curves, so it is an open problem to determine how often the hypotheses of the theorem are satisfied in general.

1.1. **Notation.** We use the notation $\ell \gg_X 0$ to mean that there is a constant $\ell_0(X)$ which depends on the object X and ℓ satisfies $\ell \geq \ell_0(X)$.

2. Proof of Main Theorem

Up to replacing K by a finite extension L/K we may assume A/K satisfies (T) for $L = K$. We fix an odd prime ℓ which is relatively prime to the polarization degree of A. We regard $V = A_\ell$ as a vector space over $\mathbb{Z}/\ell$ and write $\langle\,,\rangle : V \times V \to \mu_\ell$ for the Weil pairing; the pairing exists because A is polarized and it is non-degenerate because ℓ is prime to the polarization degree. If $W \leq V$ is a subspace, then we write $W^\perp$ for the complement of W with respect to $\langle\,,\rangle$. We identify $\Gamma = \mathrm{GSp}(V) \leq \mathrm{GL}(V)$ with the similitude subgroup of $\langle\,,\rangle$ and $\mathrm{Sp}(V) \leq \Gamma$ with the isometry group.

There is short exact sequence

$$1 \to \mathrm{Sp}(V) \to \mathrm{GSp}(V) \xrightarrow{m} (\mathbb{Z}/\ell)^\times \to 1$$

such that, for every $\gamma \in \Gamma$ and $x, y \in V$, we have $\langle \gamma x, \gamma y \rangle = \langle x, y \rangle^{m(\gamma)}$. The action of $G = G_\ell$ is compatible with $\langle\, , \rangle$, so there is an embedding $G \to \Gamma$ and the theorem asserts it is an isomorphism if $\ell \gg_A 0$. To prove the theorem we will construct a subgroup $R \leq G$ which we can show satisfies $R = \mathrm{Sp}(V)$ for $\ell \gg_A 0$, from which it will follow easily that $G = \Gamma$ for $\ell \gg_{A,K} 0$.

Lemma 2. *If $\ell \gg_A 0$, then V is an irreducible G-module.*

Proof. If $W \leq V$ is a G-submodule, then the isogeny $A \to B = A/W$ is defined over K. If $\phi_1, \phi_2 : A \to B$ were isogenies for distinct ℓ, then $\psi = \phi_1 \circ \phi_2^t$ would be an endomorphism outside of $\mathbb{Z}$ because $\deg(\psi) \notin \deg(\mathbb{Z})$, so distinct ℓ give rise to distinct elements of the K-isogeny class of A. However, Faltings' theorem implies there can only be finitely many abelian varieties in the K-isogeny class of A (cf. [D, Corollaire 2.8]), so there are only finitely many ℓ such that V is reducible. □

We say $\gamma \in \Gamma$ is a *transvection* if it is unipotent and $V^{\gamma=1}$ has codimension one. The Γ-conjugate of a transvection is a transvection, and we write $R \leq G$ for the normal subgroup generated by the subset of transvections in G. The proof of the following lemma shows that condition (T) is sufficient, but not necessary, to show that R is non-trivial for almost all ℓ.

Lemma 3. *If $\ell \gg_A 0$, then R is non-trivial.*

Proof. Suppose $\mathfrak{p}$ is a prime in $\mathcal{O}_K$ over which A has toric-dimension one; $\mathfrak{p}$ exists because A satisfies (T) for $L = K$. Then the monodromy about $\mathfrak{p}$ is a transvection provided ℓ does not divide the order of the component group of the Néron model of A over $\mathfrak{p}$ (cf. 2.1, 2.5 and 3.5 of [G]). □

Suppose R is non-trivial. Let $W \leq V$ be a non-trivial irreducible R-submodule and $H \leq G$ be the stabilizer of W.

Lemma 4. *If V is an irreducible G-module, then $W \cap W^\perp = W^R = 0$ and $V = \bigoplus_{G/H} gW$.*

Proof. This follows from (the proof of) lemma 3.2 of [H] because $(gW)^\perp = g(W^\perp)$ for all $g \in \Gamma$. □

Suppose V is an irreducible G-module, and let $R_g \leq R$ be the subgroup generated by the transvections which act non-trivially on gW. The image of $R_g = gR_1g^{-1}$ in $\mathrm{Sp}(gW)$ is non-trivial, irreducible, and generated by transvections, so is all of $\mathrm{Sp}(gW)$ by [ZS, Main Theorem].

Lemma 5. *If $g_1H \neq g_2H$ as cosets, then the commutator $[R_{g_1}, R_{g_2}]$ is trivial.*

Proof. Note, $g_1W = g_2W$ if and only if $g_1H = g_2H$. If $\gamma \in R$ is a transvection which acts non-trivially on g_1W, then $(\gamma - 1)V \leq g_1W$. Thus if $g_1W \neq g_2W$, then $(\gamma - 1)g_2W$ lies in $g_1W \cap g_2W = 0$, so R_{g_1} acts trivially on g_2W. In particular, if $\gamma_1 \in R_{g_1}$, $\gamma_2 \in R_{g_2}$ are transvections and $g_1W \neq g_2W$, then for each gW, at least one of γ_1, γ_2 acts trivially on gW, so the restrictions of γ_1, γ_2 to gW commute (for every coset gH), hence they commute on all of V. □

The lemma implies $R_g = \mathrm{Sp}(gW)$ for all gH and R is the central product $\prod_{G/H} R_g$. Therefore, if we write $n = [V : W]$, then $N_\Gamma(R)$ is isomorphic to the wreath product $\mathrm{GSp}(W) \wr S_n$ and $G \leq N_\Gamma(R)$. The next step is to show that $n = 1$.

Let $N_0 \leq N_\Gamma(R)$ be the kernel of $N_\Gamma(R) \to S_n$.

Lemma 6. *Let π be a prime in $\mathcal{O}_K$ and let e be the ramification index of π over $\mathbb{Q}$. If $\ell > en + 1$ and $I \leq G$ is the inertia subgroup of a prime in $K(A_\ell)$ over π, then the image of I in S_n is trivial.*

Proof. If $\ell > n$, then S_n has no elements of order ℓ, so the image in S_n of the ℓ-Sylow subgroup of I must be trivial. In particular, if π does not lie over ℓ, then I is an ℓ-group because it is trivial or generated by a unipotent element, so the image of I in S_n is trivial. Therefore we may suppose π lies over ℓ. Let $C \leq I$ be a complement of the ℓ-Sylow subgroup; it is a cyclic subgroup of order prime to ℓ. By section 1.13 of [S1] (following [R]), there is a finite extension $\mathbb{F}_{\ell^d}/\mathbb{F}_\ell$ and a surjective homomorphism $T = \mathbb{F}_{\ell^d}^\times \to C$ so that the representation $T \to \mathrm{GL}(V)$ has amplitude at most e; see section 3 for the definition of amplitude. The kernel of $T \to S_n$ has index at most n in T and it commutes with $Z(N_0)$ (because it lies in N_0), so lemma 9 of section 3 implies all of T commutes with $Z(N_0)$ because $\ell > en + 1$. In particular, the centralizer of $Z(N_0)$ in $N_\Gamma(R)$ is N_0, so C, the image of $T \to \mathrm{GL}(V)$, and I lie in N_0. □

The lemma implies that the fixed field of the kernel of $G \to S_n$ is unramified and has uniformly bounded degree over K. By a theorem of Hermite, there are only finitely many such extensions, so up to replacing K by a finite extension we may assume that the image of G in S_n is trivial (for all $\ell \gg_A 0$). Therefore $G \leq N_0 = \prod_{G/H} \mathrm{GSp}(gW)$ and hence $n = 1$ because G acts irreducibly, so $W = V$ and $R = \mathrm{Sp}(V)$. Once we know that R is big, the following lemma completes the proof of the theorem.

Lemma 7. *If $R = \mathrm{Sp}(V)$ and $\ell \gg_K 0$, then $G = \Gamma$.*

Proof. If $\ell \gg_K 0$, then K and $\mathbb{Q}(\mu_\ell)$ are disjoint extensions of $\mathbb{Q}$. On the other hand, if $R = \mathrm{Sp}(V)$, then G/R is the Galois group of $K(\mu_\ell)/K$, so must be all of $(\mathbb{Z}/\ell)^\times$ for $\ell \gg_K 0$. □

Remark: Most of the above carries through if we replace K by a global field of characteristic $p > 0$. One key difference is that G_ℓ is no longer equal to $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell)$

for all $\ell \gg_A 0$, but it does contain $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell)$ for all $\ell \gg_A 0$. Another difference is that the argument in lemma 6 is made simpler by the fact that there are no inertial tori to contend with for $\ell \neq p$.

3. Rigidity of Tori

Let T be the multiplicative group of a finite extension $\mathbb{F}_{\ell^d}/\mathbb{F}_\ell$. We regard T as the set of $\mathbb{F}_\ell$-points of the algebraic torus $\underline{T}/\mathbb{F}_\ell$ given by the Weil restriction of scalars of the split one-dimensional torus $\mathbb{G}_m/\mathbb{F}_{\ell^d}$. The d fundamental characters $\psi_1, \ldots, \psi_d : \underline{T} \to \mathbb{G}_m$ corresponding to the d embeddings $\mathbb{F}_{\ell^d} \to \overline{\mathbb{F}}_\ell$ form a basis for the character group $\mathrm{Hom}_{\overline{\mathbb{F}}_\ell}(\underline{T}, \mathbb{G}_m)$. We define the amplitude of a character $\chi = \prod_i \psi_i^{e_i}$ as $\max_i(e_i)$, and we say χ is ℓ-restricted if $0 \leq e_i \leq \ell - 1$ for all i and $e_i < \ell - 1$ for some i (cf. [S1, section 1.7] and [S4, annotation 5]).

Let $\mathbb{F}_\lambda/\mathbb{F}_\ell$ be a finite extension and $V/\mathbb{F}_\lambda$ be a finite-dimensional vector space. We say a representation $\rho : \underline{T} \to \underline{\mathrm{GL}}(V)$ of algebraic groups over $\mathbb{F}_\lambda$ is ℓ-restricted if all its characters are ℓ-restricted. Every representation $\rho : T \to \mathrm{GL}(V)$ extends uniquely to an ℓ-restricted representation $\rho : \underline{T} \to \underline{\mathrm{GL}}(V)$, and we define the amplitude of ρ as the maximum of the amplitudes of its characters.

Lemma 8. *Let $s \in \mathrm{GL}(V)$ be a semisimple element and $\rho : T \to \mathrm{GL}(V)$ be a representation of amplitude $e < \ell - 1$. If $\rho(T)$ commutes with s, then $\rho(\underline{T})$ commutes with s in $\underline{\mathrm{GL}}(V)$.*

Proof. Up to a base change by a finite extension of $\mathbb{F}_\lambda$, we may assume that s is diagonalizable in $\mathrm{GL}(V)$. Thus there is a decomposition $V = \oplus_j V_j$ so that s acts on V_j via an element $s_j \in Z(\mathrm{GL}(V_j))$ and T preserves the decomposition because it commutes with s. The amplitude of the restriction $\rho_j : T \to \mathrm{GL}(V_j)$ is at most e. If we write $\rho_j : \underline{T} \to \underline{\mathrm{GL}}(V_j)$ for the ℓ-restricted representation corresponding to ρ_j, then $\rho_j(\underline{T})$ commutes with s_j because s_j is a scalar. In particular, the composition of the product representation $\underline{T} \to \prod_j \underline{\mathrm{GL}}(V_j)$ with the obvious embedding $\prod_j \underline{\mathrm{GL}}(V_j) \to \underline{\mathrm{GL}}(V)$ is an ℓ-restricted representation extending $\rho : T \to \mathrm{GL}(V)$, so it must be $\rho : \underline{T} \to \underline{\mathrm{GL}}(V)$ and hence $\rho(\underline{T})$ commutes with s. □

The power of the previous lemma is that it allows us to show that representations $\rho : T \to \mathrm{GL}(V)$ are 'rigid' if they have sufficiently small amplitude (cf. [S4]).

Lemma 9. *Let $s \in \mathrm{GL}(V)$ be a semisimple element and $\rho : T \to \mathrm{GL}(V)$ be a representation of amplitude e. If $S \leq T$ is a subgroup such that $\rho(S)$ commutes with s in $\mathrm{GL}(V)$ and $e \cdot [T : S] < \ell - 1$, then $\rho(T)$ commutes with s in $\underline{\mathrm{GL}}(V)$.*

Proof. Let $c = [T : S]$ and $\rho^c : T \to \mathrm{GL}(V)$ denote the composition of ρ with the cth-power-map $c : T \to T$. By assumption ρ^c has amplitude $e \cdot c < \ell - 1$, hence the corresponding ℓ-restricted representation $\rho^c : \underline{T} \to \underline{\mathrm{GL}}(V)$ is the composition of the ℓ-restricted representation $\rho : \underline{T} \to \underline{\mathrm{GL}}(V)$ with the cth-power-map $c : \underline{T} \to \underline{T}$.

Moreover, $\rho^c(T) \leq \rho(S)$ commutes with s in $\mathrm{GL}(V)$, so by the previous lemma $\rho^c(\underline{T})$ commutes with s in $\underline{\mathrm{GL}}(V)$. In particular, $c : \underline{T} \to \underline{T}$ is surjective because $0 < c < \ell - 1$, hence $\rho(\underline{T})$ and a foriori $\rho(T)$ commute with s. □

4. Acknowledgements

We gratefully acknowledge helpful conversations with Serre, and in particular, for clarifications with regard to initial tori. We also acknowledge helpful conversations with N.M. Katz and E. Kowalski.

References

[D] P. Deligne, "Preuve des conjectures de Tate et de Shafarevitch (d'après G. Faltings)," Seminar Bourbaki, Vol. 1983/84, *Astérisque* No. 121-122 (1985), 25–41.

[G] A. Grothendieck, "Modèles de Néron et monodromie", SGA 7 Part I, exposé IX, Springer Lecture Notes in Mathematics, Vol. 288, 1972.

[H] C. Hall, "Big symplectic or orthogonal monodromy modulo ℓ," Duke Math. Journal 141 (2008), 179–203.

[M] D. Mumford, "A note of Shimura's paper "Discontinuous groups and abelian varieties"," *Math. Ann.* 181 (1969), 345–351.

[R] M. Raynaud, "Schémas en groupes de type $(p, \ldots, p)$," Bull. Soc. Math. France 102 (1974), 241–280.

[S1] J-P Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques," Invent. Math. 15 (1972), no. 4, 259–331.

[S2] J-P Serre, *Abelian ℓ-adic Representations and Elliptic Curves*, 2nd ed., Adv. Book Classics, Addison-Wesley, Redwood City, Calif., 1989.

[S3] J-P Serre, letter to Daniel Bertrand, 8/6/1984, *Collected Papers*, Vol. 4.

[S4] J-P Serre, Lettre à Marie-France Vignéras du 10/2/1986, *Collected Papers*, Vol. 4.

[ZS] A.E. Zalesskiĭ, V.N. Serežkin, "Linear groups generated by transvections," (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 40 (1976), no. 1, 26–49, 221; translation in Math. USSR Izvestija, Vol. 10 (1976), no. 1, 25–46.

[Z] Y.G. Zarhin, "Hyperelliptic Jacobians without complex multiplication," Math. Res. Lett. 7 (2000), no. 1, 123–132.

Appendix: Most hyperelliptic curves have big monodromy

Emmanuel Kowalski[1]

Let $k/\mathbb{Q}$ be a number field and $\mathbb{Z}_k$ its ring of integers. Let $f \in \mathbb{Z}_k[X]$ be a monic squarefree polynomial of degree $n = 2g+2$ or $2g+1$ for some integer $g \geq 1$, and let C_f/k be the (smooth, projective) hyperelliptic curve of genus g with affine equation

$$C_f \, : \, y^2 = f(x),$$

and J_f its jacobian.

[1]ETH Zürich - DMATH, kowalski@math.ethz.ch

In the previous text, C. Hall has shown that the image of the Galois representation

$$\rho_{f,\ell} : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}(J_f[\ell](\bar{k})) \simeq \mathbf{F}_\ell^{2g}$$

on the ℓ-torsion points of J_f is as big as possible for almost all primes ℓ, if the following two (sufficient) conditions hold:

(1) the endomorphism ring of J_f is $\mathbb{Z}$;

(2) for some prime ideal $\mathfrak{p} \subset \mathbb{Z}_k$, the fiber over $\mathfrak{p}$ of the Néron model of C_f is a smooth curve except for a single ordinary double point.

These conditions can be translated concretely in terms of the polynomial f, and are implied by:

(1') the Galois group of the splitting field of f is the full symmetric group $\mathfrak{S}_n$ (this is due to a result of Zarhin [Z], which shows that this condition implies (1));

(2') for some prime ideal $\mathfrak{p} \subset \mathbb{Z}_k$, f factors in $\mathbf{F}_\mathfrak{p} = \mathbb{Z}_k/\mathfrak{p}\mathbb{Z}_k$ as $f = f_1 f_2$ where $f_i \in \mathbf{F}_\mathfrak{p}[X]$ are relatively prime polynomials such that $f_1 = (X-\alpha)^2$ for some $\alpha \in \mathbf{F}_\mathfrak{p}$ and f_2 is squarefree of degree $n-2$; indeed, this implies (2).

In this note, we show that, in some sense, "most" polynomials f satisfy these two conditions, hence "most" jacobians of hyperelliptic curves have maximal monodromy modulo all but finitely many primes (which may, a priori, depend on the polynomial, of course!).

More precisely, for k and $\mathbb{Z}_k$ as above, let us denote

$$\mathcal{F}_n = \{f \in \mathbb{Z}_k[X] \mid f \text{ is monic of degree } n\},$$

and let the height be defined on $\mathcal{F}_n$ by

$$H(a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + X^n) = \max_{0 \le i \le n-1} H(a_i),$$

where N is the norm from k to $\mathbb{Q}$ and H is any reasonable height function on k, e.g., choose a $\mathbb{Z}$-basis $(\omega_i)_{1 \le i \le d}$ of $\mathbb{Z}_k$, where $d = [k:\mathbb{Q}]$, and let

$$H(\alpha_1\omega_1 + \cdots + \alpha_d\omega_d) = \max |\alpha_i|,$$

for all $(\alpha_i) \in \mathbb{Z}^d$.

Let $\mathcal{F}_n(T)$ denote the finite set

$$\mathcal{F}_n(T) = \{f \in \mathcal{F}_n \mid H(f) \le T\}. \tag{4.1}$$

We have $|\mathcal{F}_n(T)| = N_k(T)^n$, where

$$N_k(T) = |\{x \in \mathbb{Z}_k \mid H(x) \le T\}| \asymp T^d, \text{ where } d = [k:\mathbb{Q}].$$

Say that f has *big monodromy* if the Galois group of its splitting field is $\mathfrak{S}_n$. We will show:

Proposition 10. *Let k and $\mathbb{Z}_k$ be as above. Then*

$$|\{f \in \mathcal{F}_n(T) \mid f \text{ does not have big monodromy}\}| \ll N_k(T)^{n-1/2}(\log N_k(T)),$$

for all $T \geq 2$, where the implied constant depends on k and n.

Say that $f \in \mathcal{F}_n$ has *ordinary ramification* if it satisfies condition (2') above.

Proposition 11. *Let k and $\mathbb{Z}_k$ be as above, and assume $n \geq 2$. There exists a constant $c > 0$, depending on n and k, such that we have*

$$|\{f \in \mathcal{F}_n(T) \mid f \text{ does not have ordinary ramification}\}| \ll \frac{N_k(T)^n}{(\log N_k(T))^c}$$

for $T \geq 3$, where the implied constant depends on k and n.

Finally, say that J_f has *big monodromy* if the image of $\rho_{f,\ell}$ is as big as possible for almost all primes ℓ.

Corollary 12. *Assume that $n \geq 2$. Then we have*

$$\lim_{T \to +\infty} \frac{1}{|\mathcal{F}_n(T)|} |\{f \in \mathcal{F}_n(T) \mid J_f \text{ does not have big monodromy}\}| = 0.$$

Remark 13. Quantitatively, we have proved that the rate of decay of this probability is at least a small power of power of logarithm, because of Proposition 11. With more work, one should be able to get c equal or very close to 1, but it seems hard to do better with the current ideas (the problem being in part that we must avoid f for which the discriminant is a unit in $\mathbb{Z}_k$, which may well exist, and sieve can not detect them better than it does discriminants which generate prime ideals, the density of which could be expected to be about $(\log N_k(T))^{-1}$).

For both propositions, in the language of [K1], we consider a sieve with data

$$(\mathcal{F}_n, \{\text{prime ideals in } \mathbb{Z}_k\}, \{\text{reduction modulo } \mathfrak{p}\}), \quad (\mathcal{F}_n(T), \text{counting measure}),$$

and we claim that the "large sieve constant" Δ for the sifting range

$$\mathcal{L}^* = \{\mathfrak{p} \subset \mathbb{Z}_k \mid N\mathfrak{p} \leq L\}$$

satisfies

$$\Delta \ll N_k(T)^n + L^{2n},$$

where the implied constant depends only on k. Indeed, this follows from the work of Huxley [Hu], by combining in an obvious manner his Theorem 2 (which is the case $n = 1$, k arbitrary) with his Theorem 1 (which is the case $k = \mathbb{Q}$, n arbitrary).

Concretely, this implies that for arbitrary subsets $\Omega_\mathfrak{p}$ in the image of $\mathcal{F}_n$ under reduction modulo $\mathfrak{p}$ — the latter is simply the set of monic polynomials of degree n in $\mathbf{F}_\mathfrak{p}[X]$, and has cardinality $(N\mathfrak{p})^n$ — we have

(4.2)

$$|\{f \in \mathcal{F}(T) \mid f \,(\mathrm{mod}\,\mathfrak{p}) \notin \Omega_\mathfrak{p} \text{ for } N\mathfrak{p} \leq L\}| \ll (N_k(T)^n + L^{2n}) \Big(\sum_{N\mathfrak{a} \leq L}{}^\flat \prod_{\mathfrak{p} \mid \mathfrak{a}} \frac{|\Omega_\mathfrak{p}|}{(N\mathfrak{p})^n - |\Omega_\mathfrak{p}|} \Big)^{-1},$$

where the sum is over squarefree ideals in $\mathbb{Z}_k$ with norm at most L, and therefore also

(4.3)
$$|\{f \in \mathcal{F}(T) \mid f \,(\mathrm{mod}\,\mathfrak{p}) \notin \Omega_{\mathfrak{p}} \text{ for } N\mathfrak{p} \leq L\}| \ll (N_k(T)^n + L^{2n})\Big(\sum_{N\mathfrak{p}\leq L} \frac{|\Omega_{\mathfrak{p}}|}{(N\mathfrak{p})^n}\Big)^{-1}.$$

Proposition 10 is a result of S.D. Cohen [C]; it is also a simple application of the methods of Gallagher [G] (one only needs (4.3) here), the basic idea being that elements of the Galois group of the splitting field of a polynomial f are detected using the factorization of f modulo prime ideals. We recall that the first quantitative result of this type (for $k = \mathbb{Q}$) is due to van der Waerden [vdW], whose weaker result would be sufficient here (though the proof is not simpler than Gallagher's).

Proof of Proposition 11. Let $\mathfrak{p} \subset \mathbb{Z}_k$ be a prime ideal, and let $\Omega_{\mathfrak{p}}$ be the set of polynomials $f \in \mathbf{F}_{\mathfrak{p}}[X]$ which are monic of degree n and factor as described in Condition (2'). We claim that, for some constant $c > 0$, $c \leq 1$ (depending on k and n), we have

$$\frac{|\Omega_{\mathfrak{p}}|}{(N\mathfrak{p})^n} \geq \frac{c}{N\mathfrak{p}} \tag{4.4}$$

for all prime ideals with norm $N\mathfrak{p} \geq P_0$, for some P_0 depending on k and n.

Indeed, for $n \geq 4$, we have clearly

$$|\Omega_{\mathfrak{p}}| \geq (N\mathfrak{p}) \times |\{f \in \mathbf{F}_{\mathfrak{p}}[X] \mid \deg(f) = n-2,\ f \text{ monic irreducible}\}|;$$

for $n = 2$, this holds with the convention that 1 is irreducible of degree 0, and for $n = 3$, we must subtract 1 from the second term on the right. If $n = 2$, we are done, otherwise it is well-known that

$$|\{f \in \mathbf{F}_q[X] \mid \deg(f) = n-2,\ f \text{ monic irreducible}\}| \sim \frac{q^{n-2}}{n-2}$$

as $q \to +\infty$, hence the lower bound (4.4) follows by combining these two facts (showing we can take for c any constant $< (n-2)^{-1}$ if P_0 is chosen large enough; using more complicated factorizations of the squarefree factor of degree $n-2$, one could get c arbitrarily close to 1).

Now we apply (4.3) with this choice of subsets for $\mathfrak{p}$ with norm $> P_0$, and with $\Omega_{\mathfrak{p}} = \emptyset$ for other $\mathfrak{p}$. We take $L = N_k(T)^{d/2}$, assuming that $L > P_0$, i.e., that T is large enough. Since, if $f \in \mathcal{F}_n(T)$ does not have ordinary ramification, we have by definition $f \,(\mathrm{mod}\,\mathfrak{p}) \notin \Omega_{\mathfrak{p}}$ for any $\mathfrak{p}$, it follows by simple computations that

$$|\{f \in \mathcal{F}_n(T) \mid f \text{ does not have ordinary ramification}\}| \ll N_k(T)^n H^{-1}$$

where the implied constant depends on k and

$$H = \sum_{N\mathfrak{a}\leq L}{}^{\flat} c^{\omega(\mathfrak{a})}(N\mathfrak{a})^{-1},$$

where now $\sum^{\flat}$ restricts the sum to squarefree ideals not divisible by a prime ideal of norm $\leq P_0$, and where $\omega(\mathfrak{a})$ is the number of prime ideals dividing $\mathfrak{a}$.

It is then a standard fact about sums of multiplicative functions that

$$H \gg (\log L)^c$$

for L large enough (depending on P_0; recall that $0 < c \leq 1$), and this leads to the proposition, since L and $N_k(T)$ are comparable in logarithmic scale. □

References

[C] S.D. Cohen: *The distribution of the Galois groups of integral polynomials*, Illinois J. Math. 23 (1979), 135–152.

[G] P.X. Gallagher: *The large sieve and probabilistic Galois theory*, in Proc. Sympos. Pure Math., Vol. XXIV, Amer. Math. Soc. (1973), 91–101.

[Hu] M.N. Huxley: *The large sieve inequality for algebraic number fields*, Mathematika 15 (1968) 178–187.

[K1] E. Kowalski: *The large sieve and its applications: arithmetic geometry, random walks, discrete groups*, Cambridge Univ. Tracts (to appear).

[vdW] B.L. van der Waerden: *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monath. Math. Phys. 43 (1936), 133–147.

[Z] Y.G. Zarhin: *Hyperelliptic Jacobians without complex multiplication*, Math. Res. Lett. 7 (2000), no. 1, 123–132.

Department of Mathematics, University of Michigan at Ann Arbor

E-mail address: hallcj@umich.edu