SPLITTING FIELDS OF ELEMENTS IN ARITHMETIC GROUPS

ALEXANDER GORODNIK AND AMOS NEVO

ABSTRACT. We prove that the number of unimodular integral $n \times n$ matrices in a norm ball whose characteristic polynomial has Galois group different than the full symmetric group S_n is of strictly lower order of magnitude than the number of all such matrices in the ball, as the radius increases. More generally, we prove a similar result for the Galois groups associated with elements in any connected semisimple linear algebraic group defined and simple over a number field F. Our method is based on the abstract large sieve method developed by Kowalski, and the study of Galois groups via reductions modulo primes developed by Jouve, Kowalski and Zywina. The two key ingredients are a uniform quantitative lattice point counting result, and a non-concentration phenomenon for lattice points in algebraic subvarieties of the group variety, both established previously by the authors. The results answer a question posed by Rivin and by Jouve, Kowalski and Zywina, who have considered Galois groups of random products of elements in algebraic groups.

1. INTRODUCTION

Let $P(x) = x^d + a_1 x^{d-1} + \cdots + a_{d-1}x + a_d$ be an irreducible polynomial with integral coefficients. We denote by $\mathbb{Q}_P$ the splitting field of P. Since the Galois group $\mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q})$ acts on the roots of $P(x)$, it can be realised as a subgroup of the symmetric group S_d. P. Gallagher has shown in [1] that typically the Galois group is, in fact, isomorphic to symmetric group S_d. Namely,

$$\left| \left\{ P(x) : \begin{array}{c} \max\{|a_1|, \dots, |a_d|\} \le T \\ \mathrm{Gal}(\mathbb{Q}_P/\mathbb{Q}) \simeq S_d \end{array} \right\} \right| = (2T+1)^d + O_d\left(T^{d-1/2}\log T\right).$$

The goal of this paper is to establish an analogous result for Galois groups of splitting fields of elements in arithmetic groups. Let us consider, for instance, $\Gamma = \mathrm{SL}_d(\mathbb{Z})$. We denote by $\mathbb{Q}_\gamma$ the field generated

Date: July 15, 2011.

The first author was supported in part by EPSRC, ERC, and RCUK.

The second author was supported by ISF grant.

by the eigenvalues of γ (or, equivalently, the splitting field of the characteristic polynomial $\det(x \cdot \mathrm{Id} - \gamma)$). Let $\|\cdot\|$ be a norm on $\mathrm{Mat}_d(\mathbb{R})$, and $N_T(\Gamma) := |\{\gamma \in \Gamma : \|\gamma\| \le T\}|$. Then our main result below implies that

$$|\{\gamma \in \Gamma : \|\gamma\| \le T, \mathrm{Gal}(\mathbb{Q}_\gamma/\mathbb{Q}) \simeq S_d\}| = N_T(\Gamma) + O_{d,\varepsilon}\left(N_T(\Gamma)^{1-\delta_d+\varepsilon}\right)$$

for all $\varepsilon > 0$, where $\delta_2 = 1/56$, $\delta_d = d^{-3}(4d^2-2)^{-1}$ for even d, and $\delta_d = d^{-2}(d-1)^{-1}(4d^2-2)^{-1}$ for odd d.

More generally, our standing assumptions will be that $\mathsf{G} \subset \mathrm{GL}_m$ is a connected semisimple algebraic group defined over a number field F, and that G is simply connected and F-simple. Let S be a finite set of places of F that contains all Archimedean places such that G is isotropic over S. We denote by O_S the ring of S-integers in F, and consider the arithmetic group $\Gamma := \mathsf{G}(O_S)$. For $\gamma \in \Gamma$, we denote by F_γ the field generated by the eigenvalues of γ. We shall analyse the Galois groups $\mathrm{Gal}(F_\gamma/F)$ for $\gamma \in \Gamma$ with γ's indexed by the height function H, which is defined by

$$\mathrm{H}(\gamma) := \prod_{v \in S} \mathrm{H}_v(\gamma),$$

where the local heights H_v are

$$\mathrm{H}_v(\gamma) := \begin{cases} \left(\sum_{i,j} |\gamma_{ij}|_v^2\right)^{1/2} & \text{for Archimedean places } v \in S, \\ \max_{ij} |\gamma_{ij}|_v & \text{for non-Archimedean places } v \in S. \end{cases}$$

We set

$$N_T(\Gamma) := |\{\gamma \in \Gamma : \mathrm{H}(\gamma) \le T\}|.$$

Let $F_\mathsf{G} := \cap_\mathsf{T} F_\mathsf{T}$ where the intersection is taken over all maximal tori T of G defined over F, and F_T denotes the splitting field of the torus T. We also denote by $W(\mathsf{G}) \simeq N_\mathsf{G}(\mathsf{T})/C_\mathsf{G}(\mathsf{T})$ the Weyl group of G. Our first result shows that typically the Galois groups $\mathrm{Gal}(F_\gamma/(F_\gamma \cap F_\mathsf{G}))$ are isomorphic to the Weyl groups $W(\mathsf{G})$.

Theorem 1. *For the group Γ as above, there exists $\delta > 0$ such that*

$$\left|\left\{\gamma \in \Gamma : \begin{array}{l} \mathrm{H}(\gamma) \le T,\ F_\gamma \supset F_\mathsf{G} \\ \mathrm{Gal}(F_\gamma/F_\mathsf{G}) \simeq W(\mathsf{G}) \end{array}\right\}\right| = N_T(\Gamma) + O\left(N_T(\Gamma)^{1-\delta}\right).$$

The implied constant here and in Theorem 2 depends only on G, S, and choice of the embedding of G in GL_m (i.e., the choice of an integral model of G over O_S).

In general, the Galois groups $\mathrm{Gal}(F_\gamma/F)$ are typically isomorphic to a larger group $\Pi(\mathsf{G})$ which we now define. Let T be a maximal torus of G defined over F, and let $X(\mathsf{T})$ be the character group of T which is a

free abelian group of rank $\dim(\mathsf{T})$. We denote by $\Pi(\mathsf{G})$ the subgroup of $\mathrm{Aut}(X(\mathsf{T}))$ generated by the action of the Weyl group $W(\mathsf{G})$ and the action of the Galois group $\mathrm{Gal}(F_{\mathsf{T}}/F)$. We note that the definition of the group $\Pi(\mathsf{G})$ does not depend on the choice of the torus T.

Theorem 2. *For the group Γ as above, there exists $\delta > 0$ such that*

$$\left|\left\{\gamma \in \Gamma : \begin{array}{c} \mathrm{H}(\gamma) \leq T \\ \mathrm{Gal}(F_\gamma/F) \simeq \Pi(\mathsf{G}) \end{array}\right\}\right| = N_T(\Gamma) + O\left(N_T(\Gamma)^{1-\delta}\right).$$

Remark 3. The exponent δ can given explicitly, and Theorems 1 and 2 hold with

$$\delta < a(a + [F:\mathbb{Q}]\dim(\mathsf{G}))^{-1}(2n_e(p_S))^{-1}(2\dim(\mathsf{G})+1)^{-1}, \qquad (1)$$

where a is the Hölder exponent of the height balls, p_S is the integrability exponent of the relevant automorphic representations, and $n_e(p)$ is the least even integer $\geq p/2$ if $p > 2$ and 1 if $p = 2$. We refer to [3, Sec. 4] for this notation. We note that in many cases we have $a = 1$ (see [3, Rem. 4.2] and [2, Th. 3.15]); for instance, this is so when S contains only Archimedean places. Also, when the local height functions H_v, $v \in S$, are bi-invariant under a good special subgroup of $\mathsf{G}(F_v)$, one can replace $2n_e(p_S)$ by p_S (see [3, Rem. 4.2]).

We note that I. Rivin [12] has raised a number of important questions on genericity properties in arithmetic lattices and mapping class groups. The present paper is motivated also by the works of F. Jouve, E. Kowalski, and D. Zywina [5, 6, 7] who studied Galois groups of elements generated by random walks and have established definitive results in this setting. We are not aware of previous results about Galois groups of elements indexed by the height function, a question that was raised explicitly in [12] and [6, §7]. The method of constructing elements with prescribed properties using reduction modulo primes has been also developed in the works of G. Prasad and A. Rapinchuk [9, 10, 11].

The proofs of the theorems utilize the abstract large sieve method developed in Kowalski's book [7], and rely also on the technique of studying Galois groups via reductions modulo primes that has been developed in great generality in [6]. Our arguments are based on the general counting results for congruence subgroups proved in [3], which provide the crucial spectral estimate necessary for the large sieve method to proceed (see equation (6) below). In addition, the non-concentration phenomenon established for subvarieties of semisimple group varieties in [4] is used to immediately reduce the computation of splitting fields to regular semisimple elements only, as non-regular elements have a-priori lower rate of growth.

Acknowledgement. We would like to thank Emmanuel Kowalski for useful discussions, and the referee for helping us to improve the estimate in Proposition 4.

2. The large sieve for arithmetic groups

For a prime ideal $\mathfrak{p}$ of the ring of integers of F, we denote by $\mathsf{G}^{(\mathfrak{p})}$ the reduction of G modulo $\mathfrak{p}$. For almost all $\mathfrak{p}$, $\mathsf{G}^{(\mathfrak{p})}$ is a smooth connected algebraic group defined over the residue field $\mathbf{F}_\mathfrak{p}$. We set $Y_\mathfrak{p} := \mathsf{G}^{(\mathfrak{p})}(\mathbf{F}_\mathfrak{p})$, and more generally, for a square-free ideal $\mathfrak{a}$, we set $Y_\mathfrak{a} := \prod_{\mathfrak{p}|\mathfrak{a}} Y_\mathfrak{p}$. When the ideal $\mathfrak{a}$ is coprime to S, we have a well-defined reduction map

$$\pi_\mathfrak{p} : \Gamma = \mathsf{G}(O_S) \to Y_\mathfrak{p}.$$

Given a family of subsets $\Omega_\mathfrak{p} \subset Y_\mathfrak{p}$ with $\mathfrak{p} \in \mathcal{L}^*$, we define the sifted set by

$$S_T\left(\Gamma, \{\Omega_\mathfrak{p}\}_{\mathfrak{p}\in\mathcal{L}^*}; \mathcal{L}^*\right) := |\{\gamma \in \Gamma : \ \mathrm{H}(\gamma) \le T,\, \pi_\mathfrak{p}(\gamma) \notin \Omega_\mathfrak{p} \text{ for } \mathfrak{p} \in \mathcal{L}^*\}|.$$

A fundamental problem in sieve theory is to produce an upper estimate on the cardinality of this set.

Proposition 4. *There exist a finite set R of prime ideals containing S and constants $C, T_0, \rho > 0$, depending only on Γ, such that for any choice of*

- *a set $\mathcal{L}^*$ of prime ideals coprime to R,*
- *a set $\mathcal{L}$ of square-free ideals divisible by only prime ideals in $\mathcal{L}^*$,*
- *a family of subsets $\Omega_\mathfrak{p} \subset Y_\mathfrak{p}$ with $\mathfrak{p} \in \mathcal{L}^*$,*

the following estimate holds

$$|S_T\left(\Gamma, \{\Omega_\mathfrak{p}\}_{\mathfrak{p}\in\mathcal{L}^*}; \mathcal{L}^*\right)| \le \frac{N_T(\Gamma) + C\, N_T(\Gamma)^{1-\rho} M(\mathcal{L})}{V\left(\{\Omega_\mathfrak{p}\}_{\mathfrak{p}\in\mathcal{L}^*}\right)},$$

for all $T \ge T_0$, where

$$M(\mathcal{L}) := \max_{\mathfrak{a}\in\mathcal{L}} \sum_{\mathfrak{b}\in\mathcal{L}} |Y_{[\mathfrak{a},\mathfrak{b}]}|, \tag{2}$$

$$V\left(\{\Omega_\mathfrak{p}\}_{\mathfrak{p}\in\mathcal{L}^*}\right) := \sum_{\mathfrak{a}\in\mathcal{L}} \prod_{\mathfrak{p}|\mathfrak{a}} \frac{|\Omega_\mathfrak{p}|}{|Y_\mathfrak{p}| - |\Omega_\mathfrak{p}|}. \tag{3}$$

Remark 5. The exponent ρ in Proposition 4 can be estimated by

$$\rho < a(a + [F:\mathbb{Q}]\dim(\mathsf{G}))^{-1}(2n_e(p_S))^{-1}, \tag{4}$$

with notation as in [3, Sec. 4]. This exponent comes from [3, Th. 5.1] (see (7) below).

Proof. We use the general version of the large sieve developed in [7, Ch. 2]. We equip the spaces $Y_{\mathfrak{a}}$ with the uniform probability measure and choose an orthonormal basis of $\mathcal{B}_{\mathfrak{a}}$ of $L^2(Y_{\mathfrak{a}})$ that contains the constant function 1. We follow the convention of [7] and construct the basis elements of $L^2(Y_{\mathfrak{a}})$ as products of basis elements of $L^2(Y_{\mathfrak{p}})$ with prime ideals $\mathfrak{p}$ dividing $\mathfrak{a}$.

It will be convenient to introduce a measure $\mu_T = \sum_{\gamma\in\Gamma:\,\mathrm{H}(\gamma)\leq T} \delta_\gamma$ on Γ, where δ_γ denotes the Dirac measure at γ. According to the general large sieve inequality (see [7, Prop. 2.3]), we have the estimate

$$|S_T\left(\Gamma, \{\Omega_{\mathfrak{p}}\}_{\mathfrak{p}\in\mathcal{L}^*}; \mathcal{L}^*\right)| \leq \Delta \cdot V\left(\{\Omega_{\mathfrak{p}}\}_{\mathfrak{p}\in\mathcal{L}^*}\right)^{-1}, \tag{5}$$

where $\Delta = \Delta(T, \mathcal{L})$ is the large sieve constant, namely, the smallest number such that

$$\sum_{\mathfrak{a}\in\mathcal{L}} \sum_{\phi\in\mathcal{B}_{\mathfrak{a}}\setminus\{1\}} \left|\int_\Gamma \alpha(\gamma)\phi(\pi_{\mathfrak{p}}(\gamma))\, d\mu_T(\gamma)\right|^2 \leq \Delta \int_\Gamma |\alpha(\gamma)|^2\, d\mu_T(\gamma) \tag{6}$$

for all $\alpha \in L^2(\Gamma, \mu_T)$. As observed in [7, Rem. 2.5], the estimate (6) is independent of the choices of orthonormal bases of $L^2(Y_{\mathfrak{a}})$. We pick our bases, so that $\|\phi\|_2 = \|\phi\|_\infty$ for $\phi \in \mathcal{B}_{\mathfrak{a}}$. This can be done using finite Fourier analysis (see, for instance, [8, Prop. 2]).

For an ideal $\mathfrak{a}$ coprime with S, we set

$$\Gamma(\mathfrak{a}) = \{\gamma \in \Gamma :\ \gamma = \mathrm{Id} \mod \mathfrak{a}\}.$$

Then by [3, Th. 5.1], there exist $T_0, \rho > 0$ such that for all ideals $\mathfrak{a}$ of O_S, $\gamma_0 \in \Gamma$ and $T \geq T_0$, we have

$$|\{\gamma \in \gamma_0\Gamma(\mathfrak{a}) :\ \mathrm{H}(\gamma) \leq T\}| = \frac{N_T(\Gamma)}{|\Gamma : \Gamma(\mathfrak{a})|} + O\left(N_T(\Gamma)^{1-\rho}\right), \tag{7}$$

where ρ is as in (4). It follows from the strong approximation property of G that excluding a finite set of primes R, we may assume that the reduction map $\pi_{\mathfrak{a}}$ is surjective for all $\mathfrak{a} \in \mathcal{L}$. In particular, this implies that $Y_{\mathfrak{a}} \simeq \Gamma/\Gamma(\mathfrak{a})$, and we deduce that for all $\mathfrak{a} \in \mathcal{L}$, $y \in Y_{\mathfrak{a}}$ and $T \geq T_0$, we have

$$\mu_T\left(\{\pi_{\mathfrak{a}}(\gamma) = y\}\right) = \frac{N_T(\Gamma)}{|Y_{\mathfrak{a}}|} + O\left(N_T(\Gamma)^{1-\rho}\right). \tag{8}$$

The implied constant depends only on Γ.

Given ideals $\mathfrak{a}, \mathfrak{b} \in \mathcal{L}$, we denote by $\mathfrak{d}$ their greatest common divisor and by $[\mathfrak{a}, \mathfrak{b}]$ their least common multiple. Then

$$Y_{\mathfrak{a}} \simeq Y_{\mathfrak{a}'} \times Y_{\mathfrak{d}}, \quad Y_{\mathfrak{b}} \simeq Y_{\mathfrak{d}} \times Y_{\mathfrak{b}'}, \quad Y_{[\mathfrak{a},\mathfrak{b}]} \simeq Y_{\mathfrak{a}'} \times Y_{\mathfrak{d}} \times Y_{\mathfrak{b}'}$$

where we write $\mathfrak{a} = \mathfrak{a}'\mathfrak{d}$ and $\mathfrak{b} = \mathfrak{d}\mathfrak{b}'$. Then every $\phi \in \mathcal{B}_\mathfrak{a}$ and $\psi \in \mathcal{B}_\mathfrak{b}$ can be written as

$$\phi = \phi_1 \otimes \phi_0 \quad \text{and} \quad \psi = \psi_0 \otimes \psi_1$$

for some elements $\phi_1 \in \mathcal{B}_{\mathfrak{a}'}$, $\phi_0, \phi_1 \in \mathcal{B}_\mathfrak{d}$, $\psi_1 \in \mathcal{B}_{\mathfrak{b}'}$. Given $\phi \in \mathcal{B}_\mathfrak{a}$ and $\psi \in \mathcal{B}_\mathfrak{b}$, we define a function on $Y_{[\mathfrak{a},\mathfrak{b}]}$ by

$$[\phi, \bar\psi] = \phi_1 \otimes (\phi_0 \bar\psi_0) \otimes \bar\psi_1.$$

Now to estimate the large sieve constant Δ, we apply [7, Cor. 2.13]. Using (8), we obtain for some $C > 0$ and all $T \ge T_0$,

$$\Delta \le N_T(\Gamma) + C\, N_T(\Gamma)^{1-\rho} \max_{\mathfrak{a}\in\mathcal{L}, \phi\in\mathcal{B}_\mathfrak{a}} \sum_{\mathfrak{b}\in\mathcal{L}} |Y_{[\mathfrak{a},\mathfrak{b}]}| \left(\sum_{\psi\in\mathcal{B}_\mathfrak{b}} \|[\phi,\bar\psi]\|_\infty \right).$$

Since $\|\phi\|_\infty = \|\psi\|_\infty = 1$, we obtain

$$\begin{aligned}\|[\phi,\bar\psi]\|_\infty &\le \|\phi_1\|_\infty \cdot \|\phi_0\bar\psi_0\|_\infty \cdot \|\psi_1\|_\infty \le \|\phi_1\|_\infty \cdot \|\phi_0\|_\infty \cdot \|\bar\psi_0\|_\infty \cdot \|\psi_1\|_\infty \\ &\le \|\phi\|_\infty \cdot \|\psi\|_\infty = 1,\end{aligned}$$

and it follows that

$$\Delta \le N_T(\Gamma) + C\, N_T(\Gamma)^{1-\rho} \left(\max_{\mathfrak{a}\in\mathcal{L}} \sum_{\mathfrak{b}\in\mathcal{L}} |Y_{[\mathfrak{a},\mathfrak{b}]}| \right),$$

which completes the proof. □

3. Proof of the main theorems

For $\gamma \in \Gamma$, we denote by D_γ the algebraic group generated by γ. Let $\Gamma^* \subset \Gamma$ be the subsets of γ's such that D_γ is a maximal torus in G. In particular, every element in Γ^* is semisimple and regular. By [6, Lem. 2.5], there exists a regular function h on G defined over F such that for $\gamma \in \Gamma$, the condition $h(\gamma) \ne 0$ implies that $\gamma \in \Gamma^*$. Therefore, applying [4, Th. 1.8] to the variety $\{h = 0\}$, we deduce that for some $\sigma > 0$,

$$|\{\gamma \in \Gamma^* : \mathrm{H}(\gamma) \le T\}| = N_T(\Gamma) + O\left(N_T(\Gamma)^{1-\sigma}\right). \tag{9}$$

In fact, [4, Th. 1.8] gives $\sigma < \rho/\dim(\mathsf{G})$ with ρ as in (4). This shows that it will be sufficient to produce a favourable estimate for the set Γ^*. We note that for $\gamma \in \Gamma^*$, the maximal torus D_γ is split over F_γ, and hence $F_\gamma \supset F_\mathsf{G}$.

Let T be a maximal torus of G defined over F. The Galois group $\mathrm{Gal}(F_\mathsf{T}/F)$ acts faithfully on the character group $X(\mathsf{T})$, and we denote by

$$\phi_\mathsf{T} : \mathrm{Gal}(F_\mathsf{T}/F) \to \mathrm{Aut}(X(\mathsf{T}))$$

the corresponding injective homomorphism. For $\gamma \in \Gamma^*$, we also use notation

$$\phi_\gamma : \mathrm{Gal}(F_\gamma/F) \to \mathrm{Aut}(X(\mathsf{D}_\gamma)).$$

The Weyl group $W(\mathsf{G},\mathsf{T}) := N_{\mathsf{G}}(\mathsf{T})/C_{\mathsf{G}}(\mathsf{T})$ also acts on $X(\mathsf{T})$. Let $\Pi(\mathsf{G},\mathsf{T})$ be the subgroup of $\mathrm{Aut}(X(\mathsf{T}))$ generated by $\phi_{\mathsf{T}}(\mathrm{Gal}(F_{\mathsf{T}}/F))$ and $W(\mathsf{G},\mathsf{T})$. Using that all maximal tori are conjugate, one can check (see [6, Prop. 2.1]) that all groups $\Pi(\mathsf{G},\mathsf{T})$ and all groups $W(\mathsf{G},\mathsf{T})$ are isomorphic, and moreover that the corresponding isomorphisms are defined uniquely up to inner automorphisms, so that the bijections between the conjugacy classes are canonically defined. Because of this, we use the simple notation $\Pi(\mathsf{G})$ and $W(\mathsf{G})$.

By [6, Lem. 2.2], for $\gamma \in \Gamma^*$, we have

$$\phi_\gamma(\mathrm{Gal}(F_\gamma/F_{\mathsf{G}})) \subset W(\mathsf{G}).$$

Therefore, $\mathrm{Gal}(F_\gamma/F_{\mathsf{G}})$ is isomorphic to a subgroup of $W(\mathsf{G})$, and to prove Theorem 1, it remains to show that 'typically' the map ϕ_γ is onto.

Let E be a finite extension of F such that G is split over E. To show that 'typically' $\phi_\gamma(\mathrm{Gal}(E_\gamma/E)) = W(\mathsf{G})$, we verify that the subgroup $\phi_\gamma(\mathrm{Gal}(E_\gamma/E))$ intersects each conjugacy class of $W(\mathsf{G})$. Then the claim would follow from a classical lemma in group theory: no proper subgroup of a finite group intersects all conjugacy classes. Moreover, since $E \supset F_{\mathsf{G}}$, this also implies that $\phi_\gamma(\mathrm{Gal}(F_\gamma/F_{\mathsf{G}})) = W(\mathsf{G})$.

For a prime ideal $\mathfrak{p}$ of the ring of integers of E, we denote by $\mathsf{G}^{(\mathfrak{p})}$ the reduction of G modulo $\mathfrak{p}$. For all but finitely many $\mathfrak{p}$, the group $\mathsf{G}^{(\mathfrak{p})}$ is geometrically irreducible and split. Let $Y_{\mathfrak{p}} = \mathsf{G}^{(\mathfrak{p})}(\mathbf{F}_{\mathfrak{p}})$ and $Y_{\mathfrak{p}}^*$ be the subset of regular semisimple elements in $Y_{\mathfrak{p}}$. Every $g \in Y_{\mathfrak{p}}^*$ is contained in a unique maximal torus of $\mathsf{G}^{(\mathfrak{p})}$, which we denote by D_g. As above, for $g \in Y_{\mathfrak{p}}^*$, we have a homomorphism

$$\phi_g : \mathrm{Gal}(\overline{\mathbf{F}}_{\mathfrak{p}}/\mathbf{F}_{\mathfrak{p}}) \to \mathrm{Aut}(X(\mathsf{D}_g)),$$

and

$$\phi_g\left(\mathrm{Gal}(\overline{\mathbf{F}}_{\mathfrak{p}}/\mathbf{F}_{\mathfrak{p}})\right) \subset W\left(\mathsf{G}^{(\mathfrak{p})}\right)$$

for all but finitely many $\mathfrak{p}$. We denote by $\mathrm{Frob}_{\mathfrak{p}}$ the conjugacy class in $\mathrm{Gal}(\overline{\mathbf{F}}_{\mathfrak{p}}/\mathbf{F}_{\mathfrak{p}})$ generated by the Frobenius automorphism $x \mapsto x^{N\mathfrak{p}}$. For a prime ideal $\mathfrak{p}$ of E which is unramified over E_γ we denote by $\mathrm{Frob}_{\mathfrak{p}}^{E_\gamma/E}$ the Frobenius conjugacy class in $\mathrm{Gal}(E_\gamma/E)$. By [6, Prop. 3.1], there exists a finite set R of prime ideals $\mathfrak{p}$ and a nonzero regular function h on G defined over E such that for all $\mathfrak{p} \notin R$ and every $\gamma \in \Gamma^*$ satisfying $h(\gamma) \neq 0 \mod \mathfrak{p}$, we have

- $\pi_{\mathfrak{p}}(\gamma) \in Y_{\mathfrak{p}}^*$,

- $\mathfrak{p}$ is unramified in F_γ,
- $W(\mathsf{G}) \simeq W(\mathsf{G}^{(\mathfrak{p})})$, and there is a canonical bijection between the sets of conjugacy classes in $W(\mathsf{G})$ and $W(\mathsf{G}^{(\mathfrak{p})})$ such that the conjugacy classes $\phi_\gamma\left(\mathrm{Frob}_\mathfrak{p}^{E_\gamma/E}\right)$ and $\phi_{\pi_\mathfrak{p}(\gamma)}\left(\mathrm{Frob}_\mathfrak{p}\right)$ correspond to each other.

Moreover, enlarging R if necessary, we may assume that for $\mathfrak{p} \notin R$, $h \neq 0 \mod \mathfrak{p}$, and for prime ideals $\mathfrak{q}$ of F dividing $\mathfrak{p}$, $\mathsf{G}^{(\mathfrak{p})} \simeq \mathsf{G}^{(\mathfrak{q})}$, and Proposition 4 applies.

Let $\mathcal{L} = \mathcal{L}^*$ be the set of prime ideals $\mathfrak{p}$ which are not in R, split completely in the extension E/F, and satisfy $N\mathfrak{p} \le L$ for a parameter $L \ge 2$ that will be chosen later. We note that by Chebotarev density theorem and Landau prime ideal theorem in E, $\frac{L}{\log L} \ll |\mathcal{L}| \ll \frac{L}{\log L}$. The assumption that a prime ideal $\mathfrak{p} \in \mathcal{L}$ splits completely guarantees that for every prime ideal $\mathfrak{q}$ of F that divides $\mathfrak{p}$, we have $Y_\mathfrak{p} \simeq Y_\mathfrak{q}$, and hence Proposition 4 applies to the maps $\pi_\mathfrak{p} : \Gamma \to Y_\mathfrak{p}$. We fix a conjugacy class $\mathcal{C} \subset W(\mathsf{G}) \simeq W(\mathsf{G}^{(\mathfrak{p})})$ and for $\mathfrak{p} \in \mathcal{L}$ consider a set

$$\Omega_\mathfrak{p}^\mathcal{C} = Y_\mathfrak{p} \setminus \left\{ g \in Y_\mathfrak{p}^* : \ h(g) \neq 0,\, \phi_g(\mathrm{Frob}_\mathfrak{p}) = \mathcal{C} \right\}.$$

In order to estimate $S_T\left(\Gamma, \left\{\Omega_p^\mathcal{C}\right\}_{\mathfrak{p}\in\mathcal{L}}; \mathcal{L}\right)$, we need to establish a lower bound for $V\left(\left\{\Omega_p^\mathcal{C}\right\}_{\mathfrak{p}\in\mathcal{L}}\right)$ and an upper bound for $M(\mathcal{L})$.

Since $\{h = 0\}$ is a subvariety of $\mathsf{G}^{(\mathfrak{p})}$ with smaller dimension, it follows that

$$\left|\left\{ g \in \mathsf{G}^{(\mathfrak{p})}(\mathbf{F}_\mathfrak{p}) : \ h(g) = 0 \right\}\right| \ll |\mathbf{F}_\mathfrak{p}|^{\dim(\mathsf{G})-1} \ll |Y_\mathfrak{p}|/|\mathbf{F}_\mathfrak{p}|.$$

Also, by [6, Prop. 4.1],

$$|\{ g \in Y_\mathfrak{p}^* : \, \phi_g(\mathrm{Frob}_\mathfrak{p}) = \mathcal{C}\}| = \frac{|\mathcal{C}|}{|W(\mathsf{G})|}|Y_\mathfrak{p}| \left(1 + O\left(|\mathbf{F}_\mathfrak{p}|^{-1}\right)\right).$$

This estimate is crucial for our argument, and it allows to detect that most splitting fields have Galois groups that intersect each conjugacy class in the Weyl group. We note that in the case of SL_d, the Weyl group is the symmetric group S_d whose conjugacy classes are indexed by partitions of d. This exactly corresponds to factorisation patterns of polynomials over $\mathbf{F}_\mathfrak{p}$.

Now we deduce from the above estimates that

$$\frac{|\Omega_\mathfrak{p}^\mathcal{C}|}{|Y_\mathfrak{p}|} = \frac{|W(\mathsf{G}) - \mathcal{C}|}{|W(\mathsf{G})|} + O\left(|\mathbf{F}_\mathfrak{p}|^{-1}\right),$$

and hence,

$$V\left(\left\{\Omega_p^{\mathcal{C}}\right\}_{\mathfrak{p}\in\mathcal{L}}\right) \geq \sum_{\mathfrak{p}\in\mathcal{L}} \frac{|\Omega_{\mathfrak{p}}^{\mathcal{C}}|}{|Y_{\mathfrak{p}}|} \gg |\mathcal{L}| \gg \frac{L}{\log L}. \tag{10}$$

Next we estimate $M(\mathcal{L})$. For $\mathfrak{p},\mathfrak{q}\in\mathcal{L}$, we have

$$|Y_{\mathfrak{p}}| \ll |\mathbf{F}_{\mathfrak{p}}|^{\dim(\mathsf{G})} \leq L^{\dim(\mathsf{G})},$$
$$\left|Y_{[\mathfrak{p},\mathfrak{q}]}\right| \leq |Y_{\mathfrak{p}}|\cdot|Y_{\mathfrak{q}}| \ll L^{2\dim(\mathsf{G})},$$

and it follows that

$$M(\mathcal{L}) \leq L^{2\dim(\mathsf{G})}|\mathcal{L}| \ll \frac{L^{2\dim(\mathsf{G})+1}}{\log L}. \tag{11}$$

Now Proposition 4, together with (10) and (11), implies that

$$S_T\left(\Gamma, \left\{\Omega_p^{\mathcal{C}}\right\}_{\mathfrak{p}\in\mathcal{L}}; \mathcal{L}\right) \ll \left(N_T(\Gamma) + N_T(\Gamma)^{1-\rho}\frac{L^{2\dim(\mathsf{G})+1}}{\log L}\right)\frac{\log L}{L}.$$

Taking $L = N_T(\Gamma)^{\rho/(2\dim(\mathsf{G})+1)}$, we deduce that for $\delta < \rho/(2\dim(\mathsf{G})+1)$, we have

$$S_T\left(\Gamma, \left\{\Omega_p^{\mathcal{C}}\right\}_{\mathfrak{p}\in\mathcal{L}}; \mathcal{L}\right) \ll N_T(\Gamma)^{1-\delta}.$$

Combining this estimate with (9), we deduce that

$$\left|\left\{\gamma\in\Gamma^* : \begin{array}{c}\mathrm{H}(\gamma)\leq T\\ \exists\,\mathfrak{p}:\ \phi_\gamma\left(\mathrm{Frob}_{\mathfrak{p}}^{E_\gamma/E}\right)=\mathcal{C}\end{array}\right\}\right| = N_T(\Gamma) + O(N_T(\Gamma)^{1-\delta}),$$

since $\delta<\sigma$. This estimate holds for all conjugacy classes $\mathcal{C}$ of the Weyl group $W(\mathsf{G})$. Therefore,

$$\left|\left\{\gamma\in\Gamma^* : \begin{array}{c}\mathrm{H}(\gamma)\leq T\\ \forall\,\mathcal{C}:\ \phi_\gamma(\mathrm{Gal}(E_\gamma/E))\cap\mathcal{C}\neq\emptyset\end{array}\right\}\right| = N_T(\Gamma)+O(N_T(\Gamma)^{1-\delta}).$$

As it was remarked above, this implies that

$$\left|\left\{\gamma\in\Gamma^* : \begin{array}{c}\mathrm{H}(\gamma)\leq T\\ \mathrm{Gal}(E_\gamma/E)\simeq W(\mathsf{G})\end{array}\right\}\right| = N_T(\Gamma) + O(N_T(\Gamma)^{1-\delta}),$$

and

$$\left|\left\{\gamma\in\Gamma^* : \begin{array}{c}\mathrm{H}(\gamma)\leq T\\ \mathrm{Gal}(F_\gamma/F_{\mathsf{G}})\simeq W(\mathsf{G})\end{array}\right\}\right| = N_T(\Gamma) + O(N_T(\Gamma)^{1-\delta}).$$

Now Theorem 1 follows from (9).

To prove Theorem 2, we observe that if for $\gamma\in\Gamma^*$, we have

$$\phi_\gamma(\mathrm{Gal}(F_\gamma/F_{\mathsf{G}})) = W(\mathsf{G}),$$

then

$$\phi_\gamma(\mathrm{Gal}(F_\gamma/F)) = \Pi(\mathsf{G}),$$

and ϕ_γ defines an isomorphism $\mathrm{Gal}(F_\gamma/F) \simeq \Pi(\mathsf{G})$. Therefore, it follows from the above argument that

$$\left|\left\{\gamma \in \Gamma^* : \begin{array}{c} \mathrm{H}(\gamma) \le T \\ \mathrm{Gal}(F_\gamma/F) \simeq \Pi(\mathsf{G}) \end{array}\right\}\right| = N_T(\Gamma) + O(N_T(\Gamma)^{1-\delta}),$$

and finally Theorem 2 follows from (9). The estimate (1) on δ follows from (4).

References

[1] 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), pp. 91–101. Amer. Math. Soc., Providence, R.I., 1973.

[2] A. Gorodnik and A. Nevo, The ergodic theory of lattice subgroups, Annals of Mathematics Studies 172, Princeton University Press, 2010.

[3] A. Gorodnik and A. Nevo, Counting lattice points, to appear in J. reine angew. Math., arXiv:0903.1515.

[4] A. Gorodnik and A. Nevo, Lifting, restricting and sifting integral points on affine homogeneous varieties, to appear in Compositio Math., arXiv:1009.5217.

[5] F. Jouve, The large sieve and random walks on left cosets of arithmetic groups, Comment. Math. Helv. 85 (2010), no. 3, 647–704.

[6] F. Jouve, E. Kowalski, D. Zywina, Splitting fields of characteristic polynomials of random elements in arithmetic groups, to appear in Israel J. Math., arXiv:1008.3662.

[7] E. Kowalski, The large sieve and its applications. Arithmetic geometry, random walks and discrete groups. Cambridge Tracts in Mathematics, 175. Cambridge University Press, Cambridge, 2008.

[8] E. Kowalski, Pointwise bounds for orthonormal basis elements in Hilbert spaces, http://www.math.ethz.ch/∼kowalski/bounds-orthonormal-basis.pdf

[9] G. Prasad and A. Rapinchuk, Zariski-dense subgroups and transcendental number theory. Math. Res. Lett. 12 (2005), no. 2–3, 239–249.

[10] G. Prasad and A. Rapinchuk, Existence of irreducible R-regular elements in Zariski-dense subgroups. Math. Res. Lett. 10 (2003), no. 1, 21–32.

[11] G. Prasad and A. Rapinchuk, Weakly commensurable arithmetic groups and isospectral locally symmetric spaces. Publ. Math. Inst. Hautes Études Sci. No. 109 (2009), 113–184.

[12] I. Rivin, Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms. Duke Math. J. 142 (2008), no. 2, 353–379.

School of Mathematics, University of Bristol, Bristol, U.K.
E-mail address: a.gorodnik@bristol.ac.uk

Department of Mathematics, Technion, Haifa, Israel
E-mail address: anevo@tx.technion.ac.il