Math. Proc. Camb. Phil. Soc.: page 1 of 16
doi:10.1017/S0305004126102126

Galois groups of random integer matrices

BY THERESA C. ANDERSON AND EVAN M. O'DORNEY
Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, PA, USA
e-mails: tanders2@andrew.cmu.edu, emo916math@gmail.com

(*Received* 10 *July* 2025 *UTC; revised* 04 *June* 2026 *UTC; accepted* 10 *June* 2026 *UTC*)

Abstract

We study the number $M_n(T)$ of integer $n \times n$ matrices A with entries bounded in absolute value by T such that the Galois group of the characteristic polynomial of A is not the full symmetric group S_n. One knows $M_n(T) \gg T^{n^2-n+1} \log T$, which we conjecture is sharp. We first use the large sieve to get $M_n(T) \ll T^{n^2-1/2} \log T$. Using Fourier analysis and the geometric sieve, as in Bhargava's proof of van der Waerden's conjecture, we improve this bound for some classes of A.

2020 Mathematics Subject Classification: 11R32, 15A18 (Primary); 12F12 (Secondary)

1. *Introduction*

In recent years there has been a resurgence in the study of polynomials with non-generic Galois group, in particular the following noted breakthrough.

THEOREM 1·1 (Bhargava [7, theorem 1]; conjectured by van der Waerden [32]). *For an integer $n \geq 2$, let $E_n(T)$ be the number of monic integer polynomials*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n, \quad |a_i| \leq T$$

with Galois group strictly smaller than the full symmetric group S_n, where $T \to \infty$. Then

$$E_n(T) \asymp T^{n-1}.$$

Theorem 1·1 follows decades of incremental advances on the problem [2, 10, 15, 22, 32]. The dominant contribution comes from f having a rational root. The asymptotic probability is unaffected by whether or not we require f to be monic.

This breakthrough concerns the "large box model" where n is fixed and the height $T \to \infty$. Work has also been fruitful for the complementary "restricted coefficient model" where the coefficients a_i are drawn from a fixed set and $n \to \infty$ [4, 5, 9].

Many directions of generalisation are possible. In a recent preprint [1], the authors and Bertelli proved the analogue of the van der Waerden–Bhargava theorem for *reciprocal* polynomials, where the generic Galois group is the wreath product $S_2 \wr S_n$. We found that the most common non-generic Galois group is the index-2 subgroup $(S_2 \wr S_n) \cap A_{2n} < S_{2n}$, which also yields the best known bounds for occurrence of non-generic Galois groups in the restricted coefficient model [20].

© The Author(s), 2026. Published by Cambridge University Press on behalf of The Cambridge Philosophical Society. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

In this paper, we pursue a different direction: we look at the Galois groups of the characteristic polynomials χ_A of random $n \times n$ matrices A. These were considered by Eberhard [12] under a natural analogue of the restricted coefficient model, showing that if the entries a_{ij} are drawn independently from a finitely supported measure on $\mathbb{Z}$ satisfying some conditions, then with high probability as $n \to \infty$, the Galois group of χ_A is either S_n or A_n. A follow-up paper of Ferber, Jain, Sah and Sawhney [14] specialises to symmetric matrices, showing again that irreducibility of χ_A holds almost surely as $n \to \infty$. We recently learned of work of Bary-Soroker, Garzoni and Sodin [3] that shows a similar result for tridiagonal matrices. While these papers address the restricted entry model, we think it timely to revisit the large box model. Define $M_n(T)$ to be the number of integer $n \times n$ matrices A with entries in $[-T, T]$ such that the characteristic polynomial χ_A of A does not have Galois group the full S_n. We wish to improve upon the trivial bound $M_n(T) \ll T^{n^2}$ from counting all matrices.

One way that χ_A can fail to be of type S_n is if it is reducible, that is, the action of A on $\mathbb{Q}^n$ has an invariant subspace defined over $\mathbb{Q}$. We conjecture that this is the most common way for the Galois group to drop:

CONJECTURE 1·2. *Let $M_n(T)$ be the number of integer $n \times n$ matrices A such that the characteristic polynomial χ_A of A does not have Galois group the full S_n. Let $R_n(T) \leq M_n(T)$ be the number of A for which χ_A is reducible. Then as $T \to \infty$,*

$$R_n(T) \sim M_n(T) \asymp T^{n^2-n+1} \log T.$$

For $R_n(T)$, this asymptotic was conjectured by Rivin [26, conjecture 12]. Similarly to the van der Waerden–Bhargava theorem, the lower bound is known and comes from counting matrices with an integer eigenvalue, as we explain in Section 2 below. It is interesting to note the necessity of the log factor, which is also present in [1] when counting reciprocal polynomials, but absent in the van der Waerden–Bhargava theorem. Refining these estimates into precise asymptotic formulae would be an exciting (and lofty) goal for future work.

1·1. *Notation*

In this paper, the norm of a matrix or vector is the ∞-norm, $\|[a_{ij}]\| = \max_{i,j}|a_{ij}|$, except where otherwise noted. Some literature uses the 2-norm (Euclidean norm) instead; this only affects outlying constants, which are outside the scope of this paper.

If A is a matrix, we denote by $\chi_A(x)$ its characteristic polynomial, $\det(xI - A)$. If χ_A is irreducible over $\mathbb{Q}$, we denote by K_A the attached number field $\mathbb{Q}[x]/\chi_A(x)$. We let G_A be the Galois group of χ_A, a subgroup of S_n that permutes the roots of χ_A (transitively if and only if χ_A is irreducible).

As usual, if $f(T)$, $g(T)$ are real-valued functions of a sufficiently large real number T, then the notations

$$f(T) \ll g(T), \quad g(T) \gg f(T), \quad f(T) = O(g(T))$$

mean that $|f(T)| < c \cdot |g(T)|$ for sufficiently large T and some constant c, while the notations

$$f(T) \asymp g(T), \quad f(T) = \Theta(g(T))$$

mean that $f(T) \ll g(T)$ and $f(T) \gg g(T)$. Finally, $f(T) = o\big(g(T)\big)$ means that $\lim_{T \to \infty} f(T)/g(T) = 0$. The implied constants c may depend on the degree n but

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

not on the height T; if they depend on any other variables, we will include these variables in a subscript.

1·2. *Results*

In this paper we make progress toward proving Conjecture 1·2, which appears to be very hard to prove in general. We use a number of techniques, which are effective for different classes of matrices. In Section 3, we use the Cohen–Serre irreducibility theorem (an application of the large sieve) to get a power saving upon the trivial bound $M_n(T) \ll T^{n^2}$:

THEOREM 1·3. *We have the bound*

$$M_n(T) \ll T^{n^2-1/2} \log T. \tag{1·1}$$

In Section 4, we reduce modulo a prime of suitable size and apply Fourier analysis, modeled after the work of a group including the first author [**2**], to get a bound on the number of matrices A such that χ_A is reducible with an irreducible factor of low degree:

THEOREM 1·4. *The number $R_{n,k}(T)$ of $n \times n$ matrices A with $\|A\| \le T$ and characteristic polynomial χ_A having an irreducible factor of degree $k \le n/2$ is bounded by*

$$R_{n,k}(T) \ll T^{n^2-\frac{n-k}{n+k-1}}.$$

This improves on the large sieve when $k \le n/3$. For $k \gg \sqrt{n}$, it also improves on the bound $R_{n,k}(T) \ll T^{n^2-n+k(k+1)/2} \log T$ due to Ostafe and Shparlinski [**24**, equation (3·2)]. When k is fixed and n is large, we obtain a savings of $1 - O(1/n)$ over the trivial bound.

In Section 5, we use a combinatorial argument to get the full upper bound $T^{n^2-n+1} \log T$ but for a rather restricted class of matrices A, namely those which preserve a subspace generated by vectors of low height:

THEOREM 1·5. *For integers $1 \le k \le n/2$, let $S_{n,k}(T) \le R_{n,k}(T)$ be the number of $n \times n$ matrices A with $\|A\| \le T$ satisfying the following properties*:

(*a*) *a preserves a lattice $\Lambda \subset \mathbb{Z}^n$ of dimension k*;

(*b*) *the characteristic polynomial of $A|_\Lambda$ is irreducible*;

(*c*) *the orthogonally complementary lattice $\Lambda^\perp$ is generated by vectors of length $\le T$.*

Then

$$S_{n,k}(T) \ll T^{n^2-n+1} \log T.$$

Observe that conditions (*a*) and (*b*) force χ_A to have an irreducible factor $\chi_{A|_\Lambda}$ of degree k. Also, $\Lambda^\perp$ is an invariant lattice of dimension $n-k$ for the transpose $A^\top$, with $\chi_{A^\top|_{\Lambda^\perp}} \cdot \chi_{A|_\Lambda} = \chi_A$.

Finally, in Section 6, we use a geometric sieve modeled after Bhargava's proof of Theorem 1·1 to obtain a bound on the number of A for which χ_A defines a primitive number field of large discriminant. Our main new twist used in the proof is to take a double discriminant with respect to the direction of translation by a diagonal matrix with separable characteristic polynomial. Recall that a field extension $K/\mathbb{Q}$ is *primitive* if it has no proper intermediate

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

extensions $K \supsetneq L \supsetneq \mathbb{Q}$; this is equivalent to the Galois group $G_A \subseteq S_n$ not lying in any of the wreath products $S_a \wr S_b \subset S_n$, where $a, b > 1$ are integers with $ab = n$.

THEOREM 1·6. *Let $L_n(T) \leq M_n(T)$ be the number of matrices A with $\|A\| \leq T$ such that χ_A is a defining polynomial for a primitive degree n number field K_A with discriminant $D := |\mathrm{disc}\, K_A| \geq T^2$ with Galois group $G_A \subsetneq S_n$. Then*

$$L_n(T) \ll_\varepsilon T^{n^2-1+\varepsilon}. \tag{1·2}$$

Just as in [7], it is plausible that using Fourier analysis, one could remove the ε from the bound (1·2) and also extend the region of applicability to $D \geq T^{2-\delta}$ for some small constant δ. However, we do not attempt this strengthening, which is of doubtful value in the absence of a complementary result for small discriminants $D \leq T^{2-\delta}$. In [7], the needed bound for small discriminants (Case II therein) is quickly proved by multiplying Schmidt's upper bound on the number of number fields of bounded discriminant [28] by Lemke Oliver–Thorne's upper bound on the number of polynomials of bounded height cutting out a given field [23, proposition 2·2]. However, to apply such a technique in our setting would require a third factor, namely, the number $M_n(T; f)$ of matrices A with a given characteristic polynomial f. For fixed irreducible f and $T \to \infty$, Eskin–Mozes–Shah [13] show that

$$M_n(T; f) = (C_f + o_f(1))T^{n(n-1)/2}, \tag{1·3}$$

but the constant C_f and the rate of convergence depend heavily on f. The best uniform bound is due to Habegger, Ostafe and Shparlinski [18, theorems 2·1–2·2]:

$$M_n(T; f) \ll_n T^{n^2-n-1+o(1)}.$$

Observe that this result can be applied to at most T^{n+1} polynomials f if we want to obtain nontrivial bounds. It is believed that [18, conjecture 1·1]

$$M_n(T; f) \ll_n T^{n(n-1)/2+o(1)},$$

but this conjecture is apparently hard. We expect that progress in the small discriminant case will require a sharper error term in (1·3) by careful analysis of the spectral and ergodic theory on the manifolds involved, inspired by the recently improved error terms due to Blomer–Lutsko [8] for the related question of counting matrices of bounded norm in $\mathrm{SL}_n\mathbb{Z}$.

2. *Integer eigenvalue and the lower bound of Conjecture 1·2*

In the van der Waerden–Bhargava setting, the main term was for polynomials with a rational root. Analogously, we conjecture that the dominant contribution to $M_n(T)$ comprises matrices with an integer eigenvalue. As pointed out by Rivin [26, corollary 11], the count of such matrices is a consequence of work of Katznelson [21, theorem 1]. We can easily get T^{n^2-n+1} such matrices by setting all but the last entry in the last column to 0, which makes $[0 \cdots 0\ 1]^\top$ an eigenvector. The true order of magnitude is only slightly larger:

THEOREM 2·1. *The number $R_{n,1}(T)$ of integer $n \times n$ matrices with entries bounded by T and at least one integer eigenvalue is given asymptotically by*

$$R_{n,1}(T) \asymp T^{n^2-n+1} \log T.$$

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

Proof. Let A be such a matrix with eigenvalue λ. Then $|\lambda| \leq nT$, and $B = A - \lambda I$ is singular. Counting singular matrices in an expanding box was done by Katznelson [**21**, theorem 1], who showed that for any bounded convex open set $\mathcal{B} \subset \mathrm{Mat}_n(\mathbb{R})$ containing the origin, there is a constant $c_{\mathcal{B}} > 0$ for which

$$|\{A \in T\mathcal{B} \cap \mathrm{Mat}_n(\mathbb{Z}) : \det A = 0\}| = c_{\mathcal{B}} T^{n^2-n} \log T + O(T^{n^2-n}). \tag{2·1}$$

In our case, we can simply take $\mathcal{B}$ to be the box $\{A \in \mathrm{Mat}_n(\mathbb{R}) : \|A\|_\infty \leq 1\}$ consisting of matrices whose entries are bounded in absolute value by 1. Summing over $\lambda \ll T$, we get $R_{n,1}(T) \ll T^{n^2-n+1} \log T$, which is the desired upper bound.

For the lower bound, note that if $\lambda \leq T/2$ and $\|B\|_\infty \leq T/2$, then $\|A\|_\infty = \|B + \lambda I\| \leq T$. Moreover, each A counted by $R_{n,1}(T)$ has at most n integer eigenvalues and so is expressible in at most n ways as $B + \lambda I$ with B singular.

Remark 2·2. A different proof for the upper bound may be found in Shparlinski [**30**, theorem 6].

3. *The Cohen–Serre irreducibility theorem and Theorem 1·3*

The Cohen–Serre quantitative Hilbert irreducibility theorem, proved in special cases by Cohen [**11**] and generalised by Serre [**29**, section 13·1; theorem 1] is a tool that applies quite generally to the Galois group of any family of polynomials whose coefficients are themselves polynomials in a family of variables. We follow the presentation of Zywina [**32**, theorem 1·2], specialising to $k = \mathbb{Q}$:

THEOREM 3·1 (Cohen–Serre). *Let $F = F(x, Y_1, \ldots, Y_m) \in \mathbb{Q}(Y_1, \ldots, Y_m)[x]$ be a separable polynomial of degree n having Galois group $\Gamma \subseteq S_n$ over the rational function field $\mathbb{Q}(Y_1, \ldots, Y_m)$. For $y = (y_1, \ldots, y_m) \in \mathbb{Q}^m$, let $\Gamma_y \subseteq \Gamma$ be the Galois group of $F(x, y_1, \ldots, y_m)$ as a polynomial in x. Denote by Ω_F the subvariety of those $(y_1, \ldots, y_m)$ for which Γ_t is undefined (because f has a multiple root or one of its coefficients has a pole). Then as $T \to \infty$,*

$$|\{y \in \mathbb{Z}^m \setminus \Omega_F : |y_i| \leq T, \Gamma_y \neq \Gamma\}| \ll_{m,F} T^{m-1/2} \log T.$$

In our situation, we take $Y_1, \ldots, Y_m = Y_{n^2}$ to be the entries of the matrix A and $F = \chi_A$. We have $\Gamma = S_n$ since any integer polynomial can be realised as a characteristic polynomial. The exceptional set Ω_F comprises matrices with a repeated eigenvalue, of which there are at most $O(T^{n^2-1})$ of norm up to T. Hence we obtain Theorem 1·3.

Remark 3·2. For some subgroups $\Gamma \subsetneq S_n$, the number of matrices A with Galois group Γ has a better bound $T^{n^2-1+\delta(\Gamma)} \log T$, where $0 < \delta(\Gamma) < 1$ is determined combinatorially from Γ; see Zywina [**32**, theorem 1·4]. Unfortunately, it does not seem possible to tighten the exponent below $n^2 - 1$ with these methods.

4. *Reducible matrices and Theorem 1·4*

If the characteristic polynomial $\chi_A(x)$ is reducible but does not have an integer root, it has a factor $g(x)$ of degree k, $2 \leq k \leq n/2$. In this section we estimate the number $R_{n,k}(T)$ of matrices A having this kind of decomposition.

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

It is not so hard to show that reducibility of χ_A is equivalent to the existence of a nontrivial invariant subspace $W \subsetneq \mathbb{Q}^n$ for the action of A. With care, the volume of the corresponding invariant lattice $\Lambda = W \cap \mathbb{Z}^n$ can also be bounded:

LEMMA 4·1. *Let $g(x)$ be an irreducible factor of $\chi_A(x)$ of degree k, $1 \le k < n$. There is a subspace W of $\mathbb{Q}^n$ such that*:

(*a*) *A preserves W, and $A|_W$ has characteristic polynomial g;*

(*b*) *The lattice $\Lambda = W \cap \mathbb{Z}^n$ has volume*

$$\operatorname{covol}(\Lambda) \ll \|A\|^{k^2(n-k)+\binom{k}{2}},$$

the implicit constant depending only on n.

Proof. Our strategy is to find a short vector $v \in \ker g(A)$ and take W to be the $\mathbb{Q}$-span $\mathbb{Q}\langle v, Av, \dots, A^{k-1}v\rangle$.

Let $T = \|A\|$. Since $g \mid \chi_A$, the matrix $g(A)$ has rank at most $n-k$. To estimate $\|g(A)\|$, we write $g(x) = \sum b_i x^i$ and note that since all eigenvalues of A have absolute value at most $n\,T$, we have $b_i \ll T^{k-i}$. Therefore $g(A)$ is a sum of $k+1$ matrices $b_i A^i$ of norm $\ll T^{k-i}T^i = T^k$, so $\|g(A)\| \ll T^k$. Now to find a kernel vector v of $g(A)$, we set up a system of n linear equations in the n coordinates of v. The requirement $g(A)v = 0$ can be expressed in at most $n-k$ linear equations (one for each linearly independent row of $g(A)$), and then we fill out the system by setting one coordinate equal to 1 and the others to 0 in such a way that there is a unique solution. The solution (up to scaling) is a vector of cofactors of the coefficient matrix, which has $n-k$ rows of norm $\ll T^k$ and k rows of norm 1, so all cofactors are $\ll T^{k(n-k)}$, yielding $\|v\| \ll T^{k(n-k)}$.

Now take $W = \mathbb{Q}\langle v, Av, \dots, A^{k-1}v\rangle$, noting that since g is irreducible, W has dimension k and $A|_W$ has characteristic polynomial g. Lastly,

$$\begin{aligned}\operatorname{covol}(\Lambda) &\le \operatorname{covol}\left(\mathbb{Z}\langle v, Av, \dots, A^{k-1}v\rangle\right)\\ &\le \|v\| \cdot \|Av\| \cdots \left\|A^{k-1}v\right\|\\ &\ll T^{k(n-k)} \cdot T^{k(n-k)+1} \cdots T^{k(n-k)+k-1}\\ &= T^{k^2(n-k)+\binom{k}{2}},\end{aligned}$$

as claimed.

Remark 4·2. It is an interesting follow-up question to improve the exponent $k^2(n-k)+\binom{k}{2}$. For this paper, any bound $\|A\|^{O_n(1)}$ will do.

Proof of Theorem 1·4. Straightforward adaptation of Katznelson's methods leads to difficulties in which the error terms swamp the main term. Instead, we use a Fourier-analytic method inspired by recent successes in counting problems of this type [**1, 2, 6**]. Let $p > T$ be a large prime to be specified more precisely later. We sieve out A based on the fact that, if $\chi_A(x)$ has an irreducible factor $g(x)$ of degree k, the same is true modulo p, and this factor g must still have the form

$$g(x) = \sum_i a_i x^{k-i}, \quad a_i \ll T^i.$$

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

By Lemma 4·1, there is a subspace $W \subset \mathbb{Q}^n$ on which the characteristic polynomial of $A|_W$ is g. Let $\Lambda = W \cap \mathbb{Z}^n$ be the corresponding primitive lattice. Then the image $\overline{\Lambda}$ of Λ in $\mathbb{F}_p^n$ is a k-dimensional subspace such that $A|_{\overline{\Lambda}}$ has characteristic polynomial $\overline{g} = g \bmod p$. If $p \nmid \operatorname{disc} g$ (as holds for all but at most $O(1)$ primes $p > T$), then $\overline{g}$ has no repeated roots, so there is a unique linear operator on $\mathbb{F}_p^k$ up to conjugacy that has characteristic polynomial $\overline{g}$, namely the companion matrix $C_{\overline{g}}$. For each particular choice of conjugate $C : \overline{\Lambda} \to \overline{\Lambda}$ of the companion matrix, let $\Psi_C : \operatorname{Mat}_n(\mathbb{F}_p) \to \mathbb{Z}$ be the selector that sends a matrix $A : \mathbb{F}_p^n \to \mathbb{F}_p^n$ to 1 if $A|_{\overline{\Lambda}} = C$, and 0 otherwise. Let Ψ_g be the sum of the Ψ_C, over all distinct Λ and C. Then for A with $g \mid \chi_A$, we have shown that

$$\Psi_g(A) \geq 1.$$

Let $\Phi : \operatorname{Mat}_n(\mathbb{R}) \to \mathbb{C}$ be a Schwartz bump function that is identically 1 on matrices of norm at most 1. Then the count $R_{n,g}(T)$ of $n \times n$ matrices of norm at most T whose characteristic polynomial is divisible by g is bounded by

$$R_{n,g}(T) \leq \sum_{A \in \operatorname{Mat}_n(\mathbb{Z})} \Phi\left(\frac{A}{T}\right) \Psi_g(A).$$

We now apply twisted Poisson summation [**1**, proposition 5·2], taking the inner product of two matrices A, B to be $\operatorname{tr}(AB)$, and get

$$R_{n,g}(T) \leq \sum_{A \in \operatorname{Mat}_n(\mathbb{Z})} \Phi\left(\frac{A}{T}\right) \Psi_g(A) = T^{n^2} \sum_{B \in \operatorname{Mat}_n(\mathbb{Z})} \widehat{\Phi}\left(\frac{TB}{p}\right) \widehat{\Psi}_g(B).$$

We first compute the main term $\widehat{\Phi}(0)\widehat{\Psi}_g(0)$. To compute $\widehat{\Psi}_g(0)$, we multiply:

(1) there are $\binom{n}{k}_p \asymp p^{kn-k^2}$ subspaces $\bar{\Lambda}$, where $\binom{n}{k}_p$ is the Gaussian q-binomial coefficient;

(2) for each $\bar{\Lambda}$, the number of C is $\asymp p^{k^2-k}$, because we can conjugate C by any of the $\asymp p^{k^2}$ matrices in $\mathrm{GL}_k(\mathbb{F}_p)$, but the centraliser of C has order $\left|\left(\mathbb{F}_p[X]/g(X)\right)^\times\right| \asymp p^k$;

(3) for fixed C, Ψ_C is supported on an $n(n-k)$-dimensional affine subspace of $\operatorname{Mat}_n(\mathbb{F}_p)$.

Hence

$$\begin{aligned} \widehat{\Psi}_C(0) &= p^{n(n-k)-n^2} = p^{-kn} \\ \widehat{\Psi}_g(0) &\asymp p^{kn-k^2} \cdot p^{k^2-k} \cdot p^{-kn} = p^{-k} \\ \widehat{\Phi}(0)\widehat{\Psi}_g(0) &\asymp p^{-k}. \end{aligned}$$

(Note that the probability that $g \mid \chi_A$ is $p^{-k}\big(1 + O(1/p)\big)$, because the characteristic polynomials of matrices over a finite field are equidistributed modulo p up to $O(1/p)$ as $p \to \infty$ for fixed n by Proposition 6·4. Thus, the loss due to those A for which $\Psi_g > 1$ is of low order.)

As to the error terms $\widehat{\Phi}(B/p)\widehat{\Psi}_g(B)$, we may assume that $\|B\| \ll p/T$, as $\widehat{\Phi}(BT/p)$ drops precipitously to zero outside this range. Observe that Ψ_C is the selector for a coset of

$$N_{\bar{\Lambda}} = \{A : A|_{\overline{\Lambda}} = 0\},$$

the subspace of matrices $A \in \operatorname{Mat}_n(\mathbb{F}_p)$ whose rows belong to $\Lambda^\perp$. Hence the support of $\widehat{\Psi}_C$ is the orthogonal complement $N_{\bar{\Lambda}}^\perp$, the subspace of matrices A whose columns belong

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

to $\bar{\Lambda}$. In particular, $\widehat{\Psi}_g(B) = 0$ unless the rank r of $B \in \mathrm{Mat}_n(\mathbb{F}_p)$ satisfies $r \le k$. If $r = 0$, then $B \equiv 0 \mod p$, and hence $B = 0$ since $\|B\| \ll p/T < p$. For fixed B and r $(1 \le r \le k)$, observe that there are $\binom{n-r}{k-r}_p \asymp p^{kn-k^2-rn+rk}$ subspaces $\bar{\Lambda}$ containing the column space of B. The remaining factors are unchanged from the main term, so

$$\widehat{\Phi}(TB/p)\widehat{\Psi}_g(B) \ll p^{kn-k^2-rn+rk} \cdot p^{k^2-k} \cdot p^{-kn} = p^{-k-rn+rk}.$$

To sum these terms, we must estimate the number of matrices B having each rank r modulo p. Note that B is determined by $2rn - r^2$ coefficients: an $r \times r$ submatrix, nonsingular modulo p, and all entries in those r rows and r columns. Hence the number of B is

$$\ll \left(\frac{p}{T}\right)^{2rn-r^2} \ll \left(\frac{p}{T}\right)^{2rn-r},$$

since $p \gg T$, for a total

$$R_{n,g}(T) \ll \sum_{r=0}^{k} T^{n^2-2rn+r} p^{rn+rk-r-k}.$$

At this point, we must take $p \ll T^2$ or else the $r = 1$ term will start to outpace the main term. We take $p \asymp T^{\frac{2n-1}{n+k-1}}$ to equalise the $r = 0$ and $r = 1$ terms and get

$$R_{n,g}(T) \ll T^{n^2} p^{-k}.$$

Lastly, we sum over g. Note that modulo p, the trace-coefficient a_1 of g is bounded by $O(T)$, whereas the other coefficients admit no bound better than p, so we sum over $O(Tp^{k-1})$ polynomials g over $\mathbb{F}_p$ (and also over $O(1)$ primes $p \asymp T^{\frac{2n-1}{n+k-1}}$, to ensure at least one prime not dividing disc g for each g over $\mathbb{Z}$) to bound the desired quantity

$$\begin{aligned} R_{n,k}(T) &\ll Tp^{k-1} \cdot T^{n^2} p^{-k} \\ &= T^{n^2+1} p^{-1} \\ &\ll T^{n^2+1-\frac{2n-1}{n+k-1}} \\ &= T^{n^2-\frac{n-k}{n+k-1}}. \end{aligned}$$

5. *Reducible matrices fixing a lattice of short vectors and Theorem 1·5*

Each lattice Λ defines a subspace $\mathrm{Inv}_\Lambda \mathbb{R} \subset \mathrm{Mat}_n \mathbb{R}$ of linear maps on $\mathbb{R}^n$ that fix Λ. Hence one approach to bounding $R_n(T)$ is to count lattice points of norm $\ll T$ in the integer lattice $\mathrm{Inv}_\Lambda \mathbb{Z} = \mathrm{Inv}_\Lambda \mathbb{R} \cap \mathrm{Mat}_n \mathbb{Z}$ and then sum over Λ. For instance, if $\Lambda = \langle e_1, \ldots, e_k \rangle$ is the primitive lattice in a coordinate hyperplane, then

$$\mathrm{Inv}_\Lambda \mathbb{Z} = \left\{ \left[\begin{array}{c|c} * & * \\ \hline 0 & * \end{array}\right] : * \in \mathbb{Z} \right\}$$

is the set of matrices with an $(n-k) \times k$ lower left block of zeros, and thus

$$R_\Lambda(T) := |\mathrm{Inv}_\Lambda \mathbb{Z} \cap T\mathcal{B}| \asymp T^{n^2-k(n-k)},$$

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

which is evidently the maximum-order contribution to $R_n(T)$ among lattices Λ, since we always have $\dim \mathrm{Inv}_\Lambda \mathbb{Z} = n^2 - k(n-k)$.

We take a reduced basis for Λ, as in [21, §2]. Namely, a reduced basis is a $\mathbb{Z}$-basis $\{v_1, \dots, v_k\}$ for Λ that minimises the product of the Euclidean lengths $\ell_i = \|v_i\|_2$, arranged in increasing order of length: $\ell_1 \le \cdots \le \ell_k$.

Let $G = [g_{ij}]_{i,j=1}^k$ be the matrix describing the action of $A|_\Lambda$ with respect to the basis $\{v_i\}$. Our approach to estimating $R_\Lambda(T)$ is by two steps: we count G, that is, $A|_\Lambda$; then we count A given $A|_\Lambda$. One might hope that there are $\ll T^{k^2}$-many G and $\ll T^{n(n-k)}$-many A for each G, with equality when Λ spans a coordinate hyperplane. The bound on the number of A given G indeed holds, but there may be more G for some lattices:

Example 5·1. Let Λ be the primitive lattice in $n = 6$ dimensions spanned by the $k = 3$ vectors

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ 1 \\ T \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ T \\ T^2 \end{bmatrix}.$$

Observe that any matrix A of the shape

$$A = \left[\begin{array}{ccc|ccc} a & b & c & d & e & f \\ \hline & g & & h & i & \\ & & g & & h & i \\ \hline & & & j & & \\ & & & & j & \\ & & & & & j \end{array}\right]$$

fixes Λ. Moreover, each choice of integers $a, b, \dots, j$ in the range $[0, T)$ yields a different choice of the corresponding restriction

$$G = \begin{bmatrix} a & b + Tc & d + Te + T^2 f \\ & g & h + Ti \\ & & j \end{bmatrix}.$$

So there are at least T^{10} (in fact, $\asymp T^{10}$) matrices G, more than the $\asymp T^{k^2} = T^9$ that appear for $\Lambda = \langle e_1, e_2, e_3 \rangle$.

Generalising this example appropriately, we find that there is a lattice Λ for $n = \binom{k+1}{2}$ with $\gg T^{\binom{k+2}{3}}$ choices for G. The exponent $\binom{k+2}{3}$ is of higher order than k^2, and indeed is smaller only by a constant factor than the bound $\#G \ll T^{kn}$, which arises by noting that G is determined by the k rows of A describing the projection of outputs of A onto any coordinate k-plane whose projection to W is faithful.

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

5·1. *Counting G*

Our first lemma limits the possibilities for G.

LEMMA 5·2. *The matrix G as above has entries*

$$g_{ij} \ll \frac{T\ell_j}{\ell_i}. \tag{5·1}$$

Proof. A reduced basis $v_1, \dots, v_k$ for a lattice Λ has the useful property that, for any decomposition of a vector $v = a_1 v_1 + \cdots + a_k v_k$, we have

$$\|a_i v_i\| \ll \|v\|,$$

where the implied constant depends only on k. Thus, we can write

$$\begin{aligned} |g_{ij}| &= \frac{\|g_{ij} v_i\|}{\|v_i\|} \\ &\ll \frac{\left\|\sum_h g_{hj} v_h\right\|}{\|v_i\|} \\ &= \frac{\|Av_j\|}{\|v_i\|} \\ &\ll \frac{\|A\| \, \|v_j\|}{\|v_i\|} \\ &\ll \frac{T\ell_j}{\ell_i}, \end{aligned}$$

proving the assertion.

LEMMA 5·3. *The number of possible G, for a given* Λ, *is* $\ll T^{kn-n+1}$.

Proof. Let c be the implied constant in (5·1), so that $|g_{ij}| \le cT\ell_j/\ell_i$. Note that if $cT\ell_i/\ell_j < 1$, then $g_{ij} = 0$; in this case, we say that (i, j) is a *pinch point*. For instance, in Example 5·1, there is a pinch point at (3,1). Let $P \subseteq [n]^2$ be the set of pinch points. If (i, j) is not a pinch point, the number of possibilities for g_{ij} is $\ll T\ell_j/\ell_i$. Multiplying,

$$\begin{aligned} \#G &\ll \prod_{(i,j)\notin P} \frac{T\ell_j}{\ell_i} \\ &= \prod_{i,j=1}^{k} \frac{T\ell_j}{\ell_i} \prod_{(i,j)\in P} \frac{\ell_i}{T\ell_j} \\ &= T^{k^2} \prod_{(i,j)\in P} \frac{\ell_i}{T\ell_j}. \end{aligned} \tag{5·2}$$

Since Λ is k-dimensional, the projection of Λ onto some k-dimensional coordinate subspace, WLOG the first k coordinates, is full-dimensional. Then the first k rows of A determine G. Moreover, each pinch point imposes an independent linear condition on the entries in the first k rows of A. Hence G is determined by $kn - |P|$ entries of A, each of

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

which is $\ll T$, so we get the bound

$$\#G \ll T^{kn-|P|}. \tag{5·3}$$

If $|P| \geq n-1$, then (5·3) proves the lemma. Hence we may assume that $|P| \leq n-2$.

Note that if (i,j) is a pinch point, $i' \geq i$, and $j' \leq j$, then (i',j') is also a pinch point. In other words, the pinch points form a lower left corner of the $k \times k$ array. Clearly there are no pinch points (i,j) with $i \leq j$. Also, $(i+1,i)$ is never a pinch point: if it is, it forces the entire lower left $i \times (k-i)$ submatrix of G to be zero, so that G is block upper triangular, contradicting our hypothesis that its characteristic polynomial g is irreducible! So we have the bound

$$\ell_{i+1} \ll T\ell_i. \tag{5·4}$$

Let row i have p_i pinch points $(i,1),\dots,(i,p_i)$. For $(i,j) \in P$, each factor in (5·2) is bounded by

$$\frac{\ell_i}{T\ell_j} \ll T^{p_i+1-j}\frac{\ell_i}{T\ell_{p_i+1}} \ll T^{p_i+1-j},$$

yielding a bound $\#G \ll T^r$ where

$$\begin{aligned}
r &= k^2 + \sum_{i=3}^{k}\sum_{j=1}^{p_i}(p_i+1-j)\\
&= k^2 + \sum_{i=3}^{k}\frac{p_i(p_i+1)}{2}\\
&\leq k^2 + \sum_{i=3}^{k}\frac{p_i(k-1)}{2}\\
&= k^2 + \frac{k-1}{2}\sum_{i=3}^{k}p_i\\
&= k^2 + \frac{k-1}{2}|P|\\
&\leq k^2 + \frac{k-1}{2}(n-2)\\
&\leq k^2 + \frac{k-1}{2}(2n-2k-2)\\
&= nk - n + 1.
\end{aligned}$$

5·2. *Counting A given G*

Proof of Theorem 1·5. If Λ and G are fixed, then A is determined up to translation by the lattice N_Λ of matrices each of whose rows is in $\Lambda^\perp$. If $\Lambda^\perp$ is generated by vectors of length $\leq T$, we get

$$\#A \ll \#G \cdot \frac{T^{n(n-k)}}{\operatorname{covol}(N_\Lambda)} = \#G \cdot \frac{T^{n(n-k)}}{\operatorname{covol}(\Lambda^\perp)^n}.$$

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

Now the covolumes of a pair of mutually orthogonal primitive lattices Λ, $\Lambda^\perp$ are equal (see Schmidt [27, equation (6)]), so

$$\#A \ll \#G \cdot \frac{T^{n(n-k)}}{\operatorname{covol}(\Lambda)^n} \ll \frac{T^{n^2-n+1}}{\operatorname{covol}(\Lambda)^n}.$$

Finally, we have Λ with $\operatorname{covol}(\Lambda) \ll T^{O(1)}$ (by Lemma 4·1). From Schmidt's asymptotic for the number of primitive lattices of bounded volume [27, theorem 1]

$$|\{\Lambda : \operatorname{covol}(\Lambda) \le H\}| \sim a(n,k)H^n,$$

we get

$$\sum_{\operatorname{covol}(\Lambda) \ll T^{O(1)}} \operatorname{covol}(\Lambda)^{-n} = O(\log T),$$

so $\#A \ll T^{n^2-n+1} \log T$, as claimed.

Note that the restriction on the length of the vectors (bounded by T) is closely related to the difficult "large value problem" [17] that appears in multiple fields of mathematics and computer science. Essentially, this problem asks: for a given matrix A and bounded input vector v, how many entries of Av can be large? The lack of control of large entries of $\Lambda^\perp$ leads to our restriction on the length of its generating vectors, which then leads to the overall savings from counting these matrices. It is possible that developments in large value problems could be useful in similar matrix counting problems.

6. *Primitive groups with large field discriminant and Theorem 1·6*

In this section, we bound the number $L_n(T)$ of matrices such that χ_a defines a primitive number field K_A of discriminant $D = \operatorname{disc} K_A \ge T^2$. Our methods are direct adaptations of Bhargava's.

Let $C = \prod_{p|D, p>n} p$. First, we note that D is squarefull (apart from the small primes which we ignore here):

LEMMA 6·1 ([7, remark following proposition 11]). *If a prime p divides C, then $p^2 \mid D$.*

Recall [7, proposition 21] that if $f \in \mathbb{F}_p[x]$ is a polynomial of degree n, we factor $f = \prod_i f_i^{e_i}$ into powers of distinct irreducibles and define the *index* of f to be

$$\operatorname{ind} f = \sum_i (e_i - 1) \deg f_i = n - \sum_i \deg f_i.$$

The index has the following useful properties:

LEMMA 6·2 (see [1, lemma 5·3]). *If $p > n$ is a prime and $p^k \mid D$, then the index of χ_A mod p is at least k.*

LEMMA 6·3 (see [7, proposition 21]). *The fraction of polynomials modulo p having index at least k is $O(p^{-k})$.*

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

We need the approximate equidistribution of characteristic polynomials of matrices over $\mathbb{F}_p$. Indeed, an exact formula for the number of matrices with a given characteristic polynomial is given in [16] and [25]:

PROPOSITION 6·4 (Reiner [25, theorem 2], and Gerstenhaber [16]). *For any monic $f \in \mathbb{F}_q[x]$ of degree n over a finite field $\mathbb{F}_q$, the number of matrices $A \in \mathrm{Mat}_n(\mathbb{F}_q)$ having characteristic polynomial f is*

$$q^{n^2-n}\left(1 + O\left(\frac{1}{q}\right)\right).$$

(Here the implied constant depends on n, but not q or f.)

Observe that Lemma 6·3 and Proposition 6·4 together imply that the fraction of matrices $A \in \mathrm{Mat}_n \mathbb{F}_p$ with $\mathrm{ind}\,(\chi_A \bmod p) \geq k$ is $O(p^{-k})$. We are now ready to prove Theorem 1·6.

Proof of Theorem 1·6. We separate the cases $C \leq T$ and $C > T$, corresponding to Bhargava's Cases I and III respectively.

If $C \leq T$, then the A having any particular value of D satisfy congruence conditions modulo C for which the solution set has density $O(1/D)$. Therefore, there are at most $O(T^{n^2}/D)$ such A. Summing, the total contribution to $L_n(T)$ is

$$\ll \sum_{D \geq T^2} \frac{T^{n^2}}{D} \ll T^{n^2-1}.$$

We now assume $C \geq T$. Let $S = \mathrm{Diag}\,(1, 2, \ldots, n)$; note that χ_S is separable modulo every prime $p > n$. For a matrix A, define the *double discriminant* of A to be

$$\mathrm{DD}(A) = \mathrm{disc}_t\, \mathrm{disc}_x\, \chi_{A+tS}(x) = \mathrm{disc}_t\, \mathrm{disc}_x \det(xI - tS - A).$$

Note that $\mathrm{DD}(A)$ is an integer polynomial in the entries of A that is invariant under translation by multiples of S. We can check that DD is not identically zero modulo any prime $p > n$ by observing that for a general diagonal matrix A over $\overline{\mathbb{F}_p}$, there are the full $\binom{n}{2} = \deg_t \mathrm{disc}_x \det(xI - tS - A)$ values of t that cause two of the diagonal entries of $A + tS$ to coincide.

If $p > n$ is a prime dividing C, so that $\mathrm{ind}\,(\chi_A \bmod p) \geq 2$, we claim that $p \mid \mathrm{DD}(A)$ (compare [6, proposition 4]). This is an easy consequence of the following lemma:

LEMMA 6·5. *If $f_0 \in K[x]$ is a polynomial of index k over a field K, then the point f_0 has multiplicity at least k on the hypersurface of polynomials of discriminant* 0; *that is,* $\mathrm{disc}\,(f)$ *and all its derivatives of order up to $k-1$ with respect to the coefficients vanish at $f = f_0$.*

Remark 6·6. In fact, the multiplicity is exactly k, at least in characteristic zero, by a Riemann–Hurwitz argument; see the MathOverflow post by user `Harambe` and the answers therein [19].

Proof of Lemma 6·5. Without loss of generality, assume that K is algebraically closed and factor $f_0 = c\prod_{j=1}^{n-k}(x - r_i)^{m_i}$, noting that there are $n-k$ distinct roots. The discriminant $\mathrm{disc}\,(f)$ is given (up to sign) by the determinant of the $(2n-1) \times (2n-1)$ resultant matrix of f and f'. Note that this matrix has corank at least k because all its rows, viewed as

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

polynomials, are divisible by the degree k polynomial

$$\prod_{j=1}^{n-k} (x - r_i)^{m_i - 1}.$$

It remains to prove that if a matrix M_0 has corank k, then the determinant (viewed as a polynomial in the entries) vanishes to order at least k at M_0. But this is easy: after a coordinate transformation we have

$$M_0 = \mathrm{Diag}\,(\overbrace{1, \ldots, 1}^{n-k}, \overbrace{0, \ldots, 0}^{k}),$$

and every transversal of M_0 includes at least k zero entries, hence vanishes to order at least k at M_0.

In our situation, $\mathrm{ind}\,(\chi_A \mod p) \geq 2$, and Lemma 6·5 tells us that $\mathrm{disc}_x \det(xI - A)$ vanishes to order at least 2 modulo p. In particular, $\mathrm{disc}_x \det(xI - tS - A)$ has a double root modulo p at $t = 0$, so

$$\mathrm{DD}(A) = \mathrm{disc}_t \,\mathrm{disc}_x \det(xI - tS - A) \equiv 0 \mod p.$$

Therefore, the A having a given D are constrained by the relations

$$\mathrm{disc}\ \chi_A \equiv \mathrm{DD}(A) \equiv 0 \mod C. \tag{6·1}$$

There are $O(T^{n^2-1})$ congruence classes of matrices A modulo $\mathbb{Z}S$, because the $n-1$ linear combinations of diagonal entries

$$2a_{11} - a_{22}, \quad 3a_{11} - a_{33}, \quad \ldots, \quad na_{11} - a_{nn},$$

together with the $n^2 - n$ off-diagonal entries, determine A up to $\mathbb{Z}S$ and are $O(T)$ in size. Also, in each congruence class there are $O(T)$ matrices of norm $\leq T$ because a_{11} determines A. Since $\mathrm{DD}(A)$ is a nonzero polynomial, there are $O(T^{n^2-1})$ matrices A lying in congruence classes on which $\mathrm{DD}(A) = 0$. Excluding these, when $A = A_0 + tS$ is in a fixed congruence class, there are at most $2^{\omega(\mathrm{DD}(A))} \ll_\varepsilon T^\varepsilon$ choices of $C > T$ that divide $\mathrm{DD}(A)$. Then t is constrained by

$$\mathrm{disc}\ \chi_A = \mathrm{disc}_x \det(xI - tS - A_0) \equiv 0 \mod C. \tag{6·2}$$

We claim that (6·2) is a nonzero polynomial equation in t modulo every prime $p \mid C$ with $p > n$. For this, note that $\det(xI - tS - A_0)$ is a polynomial of degree n in x and t whose leading homogeneous piece is

$$\det(xI - tS) = \chi_{tS}(x) = (x - t)(x - 2t) \cdots (x - nt).$$

Hence

$$\mathrm{DD}(A) = \mathrm{DD}(A_0) = \mathrm{disc}_x \det(xI - tS - A_0)$$

has leading term $t^{n^2-n}\,\mathrm{disc}\ \chi_S \not\equiv 0 \mod p$ and in particular is not identically 0 modulo p.

Now (6·2) has $O(1)$ solutions modulo every prime $p \mid C$, and so $O(1)^{\omega(C)} \ll_\varepsilon T^\varepsilon$ solutions overall. Hence the total number of matrices A in this case is $O_\varepsilon(T^{n^2-1} \cdot T^\varepsilon \cdot T^\varepsilon) = O_\varepsilon(T^{n^2-1+\varepsilon})$, as desired.

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

Acknowledgements. This research was supported by the NSF. We thank Alina Ostafe, Igor Shparlinski, Daniele Garzoni and Ofir Gorodetsky for insightful comments and Robert J. Lemke Oliver for helpful conversations about this work.

REFERENCES

[1] T. C. Anderson, A. Bertelli, and E. M. O'Dorney. Galois groups of reciprocal polynomials and the van der Waerden–Bhargava theorem. *Preprint:* arXiv:2406.18970 (2024).
[2] T. C. Anderson, A. Gafni, R. J. Lemke Oliver, D. Lowry-Duda, G. Shakan, and R. Zhang. Quantitative Hilbert irreducibility and almost prime values of polynomial discriminants. *Int. Math. Res. Not. IMRN* **2023** (2023), 2188–2214.
[3] L. Bary-Soroker, D. Garzoni, and S. Sodin. Irreducibility of the characteristic polynomials of random tridiagonal matrices. *Preprint:* arXiv:2502.17218 (2025).
[4] L. Bary-Soroker, D. Koukoulopoulos, and G. Kozma. Irreducibility of random polynomials: general measures. *Invent. Math.* **233** (2023), 1041–1120.
[5] L. Bary-Soroker and G. Kozma. Irreducible polynomials of bounded height. *Duke Math. J.* **169** (2020), 579–598.
[6] M. Bhargava. A proof of van der Waerden's conjecture on random Galois groups of polynomials. *Pure Appl. Math. Q.* **19** (2023), 45–60.
[7] M. Bhargava. Galois groups of random integer polynomials and van der Waerden's conjecture. *Ann. of Math. (2)* **201** (2025), 339–377.
[8] V. Blomer and C. Lutsko. Hyperbolic lattice point counting in unbounded rank. *J. Reine Angew. Math.* **2024** (2024), 257–274.
[9] E. Breuillard and P. P. Varjú. Irreducibility of random polynomials of large degree. *Acta Math.* **223** (2019), 195–249.
[10] S. Chow and R. Dietmann. Enumerative Galois theory for cubics and quartics. *Adv. Math.* **372** (2020), 107282, 37.
[11] S. D. Cohen. The distribution of the Galois groups of integral polynomials. *Illinois J. Math.* **23** (1979), 135–152.
[12] S. Eberhard. The characteristic polynomial of a random matrix. *Combinatorica* **42** (2022), 491–527.
[13] A. Eskin, S. Mozes, and N. Shah. Unipotent flows and counting lattice points on homogeneous varieties. *Ann. of Math. (2)* **143** (1996), 253–299.
[14] A. Ferber, V. Jain, A. Sah, and M. Sawhney. Random symmetric matrices: rank distribution and irreducibility of the characteristic polynomial. *Math. Proc. Camb. Phil. Soc.* **174** (2023), 233–246.
[15] P. X. Gallagher. The large sieve and probabilistic Galois theory. In *Analytic number theory (Proc. Sympos. Pure Math., Vol.* **XXIV**, *St. Louis Univ., St. Louis, Mo.,* 1972). *Proc. Sympos. Pure Math.,* vol. XXIV (Amer. Math. Soc., Providence, RI, 1973), pp. 91–101.
[16] M. Gerstenhaber. On the number of nilpotent matrices with coefficients in a finite field. *Illinois J. Math.* **5** (1961), 330–333.
[17] L. Guth. Large value estimates in number theory, harmonic analysis, and computer science. *Preprint:* arXiv:2503.07410 (2025).
[18] P. Habegger, A. Ostafe, and I. E. Shparlinski. Integer matrices with a given characteristic polynomial and multiplicative dependence of matrices. *Preprint:* arXiv:2203.03880 (2024).
[19] Harambe 2024. What relationship is there between repeated roots of discriminants and orders of roots of the original polynomials? MathOverflow question, https://mathoverflow.net/questions/466758 (accessed Jun 3, 2026).
[20] D. Hokken. Counting (skew-)reciprocal Littlewood polynomials with square discriminant. *Preprint:* arXiv:2301.05656 (2023).
[21] Y. R. Katznelson. Singular matrices and a uniform bound for congruence groups of $\mathrm{SL}_n(\mathbf{Z})$. *Duke Math. J.* **69** (1993), 121–136.
[22] H.-W. Knobloch. Zum Hilbertschen Irreduzibilitätssatz. *Abh. Math. Sem. Univ. Hamburg* **19** (1955), 176–190.
[23] R. J. Lemke Oliver and F. Thorne. Upper bounds on number fields of given degree and bounded discriminant. *Duke Math. J.* **171** (2022), 3077–3087.

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press

[24] A. OSTAFE and I. E. SHPARLINSKI. On the sparsity of non-diagonalisable integer matrices and matrices with a given discriminant. *Preprint:* arXiv:2312.12626 (2024).
[25] I. REINER. On the number of matrices with given characteristic polynomial. *Illinois J. Math.* **5** (1961), 324–329.
[26] I. RIVIN. Counting reducible matrices, polynomials, and surface and free group automorphisms. Preliminary version of [27]. *Preprint:* arxiv:math/0604489 (2006).
[27] W. M. SCHMIDT. Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height. *Duke Math. J.* **35** (1968), 327–339.
[28] W. M. SCHMIDT. Number fields of given degree and bounded discriminant. *Astérisque* **4** (1995), 189–195. Columbia University Number Theory Seminar (New York, 1992).
[29] J.-P. SERRE. *Lectures on the Mordell-Weil Theorem*. *Aspects of Mathematics*. (Vieweg+Teubner Verlag, Wiesbaden, 3rd edition, 2013).
[30] I. E. SHPARLINSKI. Some counting questions for matrices with restricted entries. *Linear Algebra Appl.* **432** (2010), 155–160.
[31] B. L. VAN DER WAERDEN. Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt. *Monatsh. Math. Phys.* **43** (1936), 133–147.
[32] D. ZYWINA. Hilbert's irreducibility theorem and the larger sieve. *Preprint:* arXiv:1011.6465 (2010).

https://doi.org/10.1017/S0305004126102126 Published online by Cambridge University Press