Math. Res. Lett.
Volume 25, Number 4, 1151–1172, 2018

Counting G-extensions by discriminant

Evan P. Dummit

The problem of analyzing the number of number field extensions L/K with bounded (relative) discriminant has been the subject of renewed interest in recent years, with significant advances made by Schmidt, Ellenberg-Venkatesh, Bhargava, Bhargava-Shankar-Wang, and others. In this paper, we use the geometry of numbers and invariant theory of finite groups, in a manner similar to Ellenberg and Venkatesh, to give an upper bound on the number of extensions L/K with fixed degree, bounded relative discriminant, and specified Galois closure.

1. Overview

Over a century ago, Hermite showed that the number of number fields of a given degree whose (absolute) discriminant is less than X is finite. Thus, ordering number fields of a fixed degree (or fixed Galois closure) by discriminant provides us with a variety of well-posed counting problems.

For a fixed number field K, our primary interest is in analyzing the asymptotics, as $X \to \infty$, of the number of extensions L/K, of fixed degree and Galois closure, whose discriminant (norm) is less than X. Providing exact asymptotics is quite difficult and has been carried out in only a few cases.

In Section 2, we briefly review a number of results on counting number fields by discriminant, and then in Section 3 we review some necessary background on polynomial invariants attached to representations of finite groups.

In Section 4, we then prove a general theorem bounding from above the number of extensions of a given degree, bounded discriminant, and specified Galois closure. We give a prototypical example in Section 5, and then finish with some concluding remarks.

2010 Mathematics Subject Classification: Primary 11R21 ; Secondary 11R29, 13A50, 11H06.

Key words and phrases: Discriminants, number field counting, G-extensions, discriminant counting, polynomial invariant theory, geometry of numbers.

2. Notation and background

To introduce some notation, let K be a number field and L/K be an extension of degree n. Also let $\mathcal{O}_L$ and $\mathcal{O}_K$ be the rings of integers, and D_L and D_K be the absolute discriminants, of L and K respectively. We also take $\mathrm{Nm}_{K/\mathbb{Q}}$ to be the absolute norm on ideals and $\mathcal{D}_{L/K}$ to be the relative discriminant ideal.

We will understand $f(X) \sim g(X)$ to mean that $\lim_{X\to\infty} \dfrac{g(X)}{f(X)} = 1$, and $f(X) \ll g(X)$ to mean that $f(x) < c\, g(X)$ for some constant $c > 0$ and X sufficiently large (where c may depend on other parameters such as n and ϵ that will be clear from the context). The group G will also always refer to a finite group equipped with an embedding into S_n, and is to be interpreted as the Galois group of the Galois closure of L/K.

2.1. Counting extensions of fixed degree

Our central problem is to count extensions L/K where $[L : K] = n$.

Definition 1. For a fixed K and n, we define $N_{K,n}(X)$ to be the number of number fields L (up to K-isomorphism) with extension degree $[L : K] = n$ and absolute discriminant norm $\mathrm{Nm}_{K/\mathbb{Q}}(\mathcal{D}_{L/K}) < X$.

A folk conjecture, sometimes attributed to Linnik, says that

$$N_{K,n}(X) \sim C_{K,n} X$$

for fixed n and as $X \to \infty$, for some positive constant $C_{K,n}$ depending on K and n. Even for the base field $K = \mathbb{Q}$, the best known results for large n are far away from this conjectured result. Only in some low-degree cases ($n \leq 5$) is this conjecture proven: for general K, the case $n = 2$ is an exercise in Kummer theory, and the case $n = 3$ for $K = \mathbb{Q}$ is due to Davenport and Heilbronn [14], while for general K it is due to Datskovsky and Wright [13]. For $K = \mathbb{Q}$, the results for $n = 4$ and $n = 5$ are also known and due to Cohen-Diaz y Diaz-Olivier and Bhargava [4, 5, 9], (a slightly weaker exponent was first established by Kable-Yukie [20, 33]), and for general K they are due to Bhargava-Shankar-Wang [7]. However, these techniques are not expected to extend to higher-degree extensions.

Our starting point for counting extensions of higher degree is the following theorem of Schmidt [27]:

Theorem (Schmidt). *For all n and all base fields K,*

$$N_{K,n}(X) \ll X^{(n+2)/4}. \tag{2.1}$$

The approach of Schmidt can be broadly interpreted as follows: if L/K is an extension of degree n, first use Minkowski's Lattice Theorems to obtain an element $\alpha \in \mathcal{O}_L$ whose archimedean norms are small (in terms of X). This gives bounds on the coefficients of the minimal polynomial of α; counting the number of possibilities for α yields the upper bound on the number of possible extensions L/K. We will note that some care is necessary in the above argument: in fact, Schmidt actually counts chains of primitive extensions $K \subset L_1 \subset \cdots \subset L_{t-1} \subset L$ to avoid possible issues arising from the existence of large-degree subfields. (The overall exponent in X, ultimately, is independent of any assumption of primitivity.)

The best upper bound for general n was established by Ellenberg and Venkatesh [18]:

Theorem (Ellenberg-Venkatesh). *For all $n > 2$ and all base fields K,*

$$N_{K,n}(X) \ll (X\, D_K^n\, A_n^{[K:\mathbb{Q}]})^{\exp(C\sqrt{\log\, n})},$$

where A_n is a constant depending only on n and C is an absolute constant.

Although the constants are not explicitly computed in the paper, after some effort one can show that for sufficiently large n (roughly on the order of $n = 200$), the result becomes stronger than Schmidt's bound.

By taking logarithms, one may recast Theorem 2.1 as showing that

$$\limsup_{X\to\infty} \frac{\log\, N_{K,n}(X)}{\log\, X} \ll n^{\epsilon}$$

for any $\epsilon > 0$. For comparison, Schmidt's result is that this limit is at most $\dfrac{n+2}{4}$, while Linnik's conjecture is that this limit is 1.

Ellenberg-Venkatesh use a modification of Schmidt's technique: rather than counting the number of possibilities for a single element of $\mathcal{O}_L$, they instead count linearly-independent r-tuples of elements of $\mathcal{O}_L$, where r is chosen at the end so as to optimize the resulting bound. Then by using properties of the invariant theory of products of symmetric groups, they rephrase the problem into one about counting integral points on a scheme which is a generically-finite cover of affine space.

2.2. Counting extensions with specified Galois closure

We may refine the basic counting problem by restricting our attention to extensions L/K whose Galois closure $\hat{L}/K$ has Galois group isomorphic to a particular finite permutation group G.

Definition 2. For fixed K and n, and a transitive permutation group $G \hookrightarrow S_n$ with a given embedding into S_n, we define $N_{K,n}(X;G)$ to be the number of number fields L (up to K-isomorphism) such that

1) The degree $[L:K] = n$,
2) The absolute norm of the relative discriminant $\mathrm{Nm}_{K/\mathbb{Q}}(\mathcal{D}_{L/K})$ is less than X, and
3) The action of the Galois group of the Galois closure of L/K on the complex embeddings of L is permutation-isomorphic to G.

Extensions satisfying these conditions are referred to as G-extensions. It is also common to abuse terminology and refer to G as the "Galois group" of the extension L/K, despite the fact that this extension is not typically Galois.

A series of conjectures of Malle [25, 26] give expected growth rates for $N_{K,n}(X;G)$ depending on the group G. Explicitly, for G a transitive subgroup acting on $\Omega = \{1, 2, \ldots, n\}$, and for g in G, define the index of an element

$$\mathrm{ind}(g) = n - [\text{number of orbits of } g \text{ on } \Omega],$$

which is also equal to the sum, over all cycles in the cycle decomposition of g in S_n, of the length of the cycle minus 1. Next define the index of G to be

$$\mathrm{ind}(G) = \min\{\mathrm{ind}(g) \,:\, 1 \neq g \in G\}.$$

We also set

$$a(G) = 1/\mathrm{ind}(G).$$

Note that the index of a transposition is equal to 1, and (since an element with index 1 has $n-1$ orbits) the transpositions are the only elements of index 1.

The absolute Galois group of K acts on the conjugacy classes of G via the action on $\bar{\mathbb{Q}}$-characters of G. We define the orbits (of that action) to be the "K-conjugacy classes" of G. Since all elements in a K-conjugacy class

have the same index, we define the index of a conjugacy class to be the index of any element in that class.

The strong form of Malle's conjecture is as follows:

Conjecture 3. *(Malle, strong form) There exists a constant $c(k,G) > 0$ such that*

$$N_{K,n}(X;G) \sim c(K,G) \cdot X^{a(G)} \cdot \log(X)^{b(K,G)-1},$$

where

$$a(G) = \frac{1}{\mathrm{ind}(G)} \quad \textit{and}$$
$$b(K,G) = \#\{C : C \textit{ a } K\textit{-conjugacy class of minimal index ind}(G)\}.$$

Remark. We would expect by Linnik's conjecture that for any group G, the asymptotics should not exceed X^1, and indeed it is not hard to see (cf. Lemma 2.2 of [26]) that if $a(G) = 1$ then $b(K,G)$ is also 1.

The strong form of Malle's conjecture holds for all abelian groups; this is a result of Wright [32]. However, Klüners [21] has constructed a counterexample to the $\log(X)$ part of the conjecture for the nonabelian group $G = C_3 \wr C_2$ of order 18 embedded in S_6. (Klüners also notes that this is not a unique example, and that all groups of the form $C_p \wr C_2$ yield counterexamples to Malle's conjecture as formulated above.) The ultimate difficulty is the potential existence of an intermediate cyclotomic subfield inside the extension: in this case, $\mathbb{Q}(\zeta_3)$ (or $\mathbb{Q}(\zeta_p)$ in the general family).

There is a recent refinement of the exponent of the log-term in Malle's conjecture over function fields, due to Türkelli [31], which appears to avoid all of the known counterexamples. Türkelli's refinement is motivated by counting points on components of non-connected Hurwitz schemes. The question of counting points on connected Hurwitz schemes was related to counting extensions of function fields in a paper of Ellenberg-Venkatesh [17], and their heuristics (subject to some assumptions) aligned with Malle's. Türkelli extended their arguments to cover non-connected Hurwitz schemes, and the difference in the results compared to those of Ellenberg-Venkatesh suggested a modification to Malle's conjecture.

It is generally believed that the power of X in Malle's conjecture is essentially correct. Explicitly:

Conjecture 4. *(Malle, weak form) For any $\epsilon > 0$ and any number field K, $X^{a(G)} \ll N_{K,n}(X;G) \ll X^{a(G)+\epsilon}$, where $a(G) = \frac{1}{\mathrm{ind}(G)}$.*

If true, Malle's conjecture, even when we restrict to the "weak form" that only considers the power of X, and only for extensions of $\mathbb{Q}$, would for example imply that every finite group is a Galois group over $\mathbb{Q}$. As such, even this weak version (let alone the full version) is naturally considered to be entirely out of reach of current methods.

An upper bound at least as strong as that in Conjecture 4 is known to hold in the following cases over general number fields K:

1) For any abelian group [24, 32], with the asymptotic constants (in principle).

2) For any nilpotent group [1, 23]. For a nilpotent group in its regular representation, the lower bound is also known.

3) For S_3 [13, 14], with the asymptotic constants. In fact, in this case there is a second main term, and its asymptotic constant is also known [6, 30].

4) For D_4 and S_4 [2, 4, 7, 9]. The asymptotic constants are also known. A power savings in the error term is also known [3] when $K = \mathbb{Q}$.

5) For S_5 [5, 7, 20], as well as the asymptotic constant. A power savings in the error term is also known [28] when $K = \mathbb{Q}$.

6) For degree-6 S_3 extensions [8], as well as the asymptotic constant.

7) Under mild restrictions, for wreath products of the form $C_2 \wr H$ where H is nilpotent [22].

Note that the results in degree 4 provide a stark contrast for the situation with counting polynomials by the maximum height of their coefficients: if we let a_i for $1 \leq i \leq n$ be indeterminates, then the polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K(a_1, \ldots, a_n)$ has Galois group S_n over $K(a_1, \ldots, a_n)$. Hilbert's Irreducibility Theorem then implies that almost all specializations (when ordered by the coefficient height) of this polynomial still have Galois group S_n.

However, the results of Cohen et al. [10] collectively show that, when ordered by discriminant, a positive proportion (roughly 17%) of extensions of degree 4 have an associated Galois group isomorphic to the dihedral group D_4: the difference is entirely caused by ordering the fields by discriminant. Malle's conjectures, moreover, indicate that the non-S_n extensions should have a positive density for any composite n, but should have zero density for prime n, though this is not known to be true for any $n > 5$.

2.3. Outline of results

The overarching goal of this paper is to generalize the results of Schmidt and Ellenberg-Venkatesh to arbitrary G-extensions. In Section 4, we prove the following theorem:

Theorem 7. Let $n \geq 2$, let K be any number field, and let G be a proper transitive subgroup of S_n. Also, let t be such that if G' is the intersection of any point stabilizer in S_n with G, then any subgroup of G properly containing G' has index at most t. Then for any $\epsilon > 0$,

$$N_{K,n}(X;G) \ll X^{\frac{1}{2(n-t)}\left[\sum_{i=1}^{n-1}\deg(f_{i+1})-\frac{1}{[K:\mathbb{Q}]}\right]+\epsilon},$$

where the f_i for $1 \leq i \leq n$ are a set of primary invariants for G, whose degrees (in particular) satisfy $\deg(f_i) \leq i$.

We note here that for every primitive group covered by the Theorem, the result is always strictly better than the result offered by Schmidt's bound $N_{K,n}(X) \ll X^{(n+2)/4}$, and the savings (see Appendix A) are often significant.

Our proof follows the same general approach as that of Schmidt and generalizes Example 2.7 from Ellenberg-Venkatesh [18], which gives a rough outline of the technique for a single group. The technique is as follows:

1) Apply Minkowski's Theorems to obtain an algebraic integer generating L whose archimedean valuations are small.
2) Use a counting argument to establish an upper bound on the number of such algebraic integers.

The goal of Proposition 5 is to accomplish (1). We modify the basic argument in (2) by rephrasing the counting argument in scheme-theoretic language, and then invoke invariant theory and the large sieve (see Lemma 6) to save in the counting part.

3. Polynomial invariants of finite groups

In this section we briefly discuss some standard results in the theory of polynomial invariants; we freely refer to results from this section in the main text. The following discussion is condensed from Derksen-Kemper [15].

Let G be a finite group and $\rho : G \to GL_n(\mathbb{C})$ be a (faithful) complex representation, and let G act on $\mathbb{C}[x_1, \ldots, x_n]$ via ρ. If $f_1, \ldots, f_n$ are algebraically independent, homogeneous elements of $\mathbb{C}[x_1, \ldots, x_n]$ with the property that $\mathbb{C}[x_1, \ldots, x_n]^G$, the ring of G-invariant polynomials, is a finitely-generated module over $\mathbb{C}[f_1, \ldots, f_n]$, we say these polynomials f_i are a set of "primary invariants" for G. The Noether normalization lemma implies that such polynomials exist; that there are n of them follows from comparing transcendence degrees.

The primary invariants are not unique: one can (for example) take linear combinations or powers of the f_i and still retain the finite-generation property. When we speak of primary invariants, we generally mean a set of primary invariants which are homogeneous and of minimal degree, arranged in nondecreasing order by degree. However, all results discussed will hold for any set of primary invariants.

Denote $A = \mathbb{C}[f_1, \ldots, f_n]$, and $R = \mathbb{C}[x_1, \ldots, x_n]^G$. The theorem of Hochster-Roberts (Theorem 2.5.5 of [15]) implies that R is a Cohen-Macaulay ring and, moreover, that there exist homogeneous G-invariant polynomials g_1, $g_2, \ldots,$ g_k with $g_1 = 1$ such that $R = A \cdot g_1 + \cdots + A \cdot g_k$. These polynomials g_i are called "secondary invariants" of G and will depend intrinsically on the choice of primary invariants, and are not uniquely determined even for a fixed set of primary invariants.

Example. Let $G = S_n$ and ρ be the regular representation of G (which acts by index permutation on $\mathbb{C}[x_1, \ldots, x_n]$). It is easy to see that the elementary symmetric polynomials are invariants under the action of G on $\mathbb{C}[x_1, \ldots, x_n]$, and that they are algebraically independent: thus, they form a set of primary invariants for G. In fact, for *any* subgroup of S_n, the elementary symmetric polynomials form a set of (possibly non-minimal-degree) primary invariants: hence, for any permutation representation ρ of degree n, there exists a set of primary invariants of ρ such that $\deg(f_i) \leq i$ for each $1 \leq i \leq n$.

Associated to any (usually G-invariant) graded submodule M of $\mathbb{C}[x_1, \ldots, x_n]$ is the generating function $H(M, t) = \sum_{j=0}^{\infty} a_j t^j$, where $a_j = \dim_{\mathbb{C}}(M^{(j)})$, the vector space dimension of the degree-j polynomials in M. This generating function is called (variously) the Hilbert series or the Molien series of M.

Example. For $A = \mathbb{C}[f_1, \ldots, f_d]$, one has $H(A, t) = \prod_{i=1}^{n} (1 - t^{\deg(f_i)})^{-1}$ by the algebraic independence of the f_i.

For $R = \mathbb{C}[x_1, \ldots, x_m]^G$, there is a formula, due to Molien, which says

$$H(R,t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - t\rho(g))}. \tag{3.1}$$

(In fact the formula applies to any linear representation $\rho : G \to GL(V)$, over any field of characteristic relatively prime to $|G|$.) By looking at the free resolution of $R = A \cdot g_1 + \cdots + A \cdot g_k$ arising from the secondary invariants in tandem with 3.1, we can write

$$H(R,t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - t\rho(g))} = \frac{\sum_{j=1}^{k} t^{\deg(g_i)}}{\prod_{i=1}^{n} (1 - t^{\deg(f_i)})}. \tag{3.2}$$

By examining the Hilbert series identity 3.2 with sufficient care, one can deduce a number of facts about the primary invariants: for example, the product of the degrees of any set of primary invariants is divisible by $|G|$, and the quotient is equal to the number of associated secondary invariants (cf. Proposition 3.3.5 of [15]). Also, the least common multiple of the degrees of the primary invariants is divisible by the exponent of G.

For any particular representation ρ, one can compute the Hilbert series as a rational function using Molien's formula, and then factor the denominator to generate possibilities for the degrees for the primary invariants. One might hope that this will immediately give the degrees of the primary invariants, but this is not the case: for general linear representations (or even permutation representations), the minimal degrees possible from the Hilbert series will not always give the degrees of an actual set of primary invariants.

The computer algebra system MAGMA computes minimal primary invariants by using Molien's formula to generate possible degree vectors for the primary invariants, then generates independent ρ-invariant polynomials of those degrees, and finally applies a Hilbert-driven Buchberger algorithm to verify that the resulting ideal is zero-dimensional. For a number of reasons, most algorithms for primary invariant computation in general settings generally seek to minimize the product of the invariant degrees rather than their sum. In general, we would also not expect there to be a way to compute the degrees of a set of primary invariants without essentially having to compute the invariants themselves; see the discussion following Algorithm 3.3.4 of [15] for further details.

4. Proof of main counting theorem

Given an extension L/K, we start by constructing a generator of small size.

Proposition 5. *Let K be a number field of degree l over $\mathbb{Q}$, and L/K an extension of degree n such that $\mathrm{Nm}_{K/\mathbb{Q}}(\mathcal{D}_{L/K}) < X$, and such that any proper subfield K' of L containing K has $[K' : K] \leq t$. Then there exists an $\alpha \in \mathcal{O}_L$ with $\mathrm{Tr}_{L/K}(\alpha) = 0$, all of whose archimedean valuations have absolute value $\ll X^{\frac{1}{2l(n-t)}}$, and such that $L = K(\alpha)$.*

Proof. If L has r real embeddings $\rho_1, \ldots, \rho_r$ and s complex embeddings $\sigma_1, \bar{\sigma}_1, \ldots, \sigma_s, \bar{\sigma}_s$ (where $r + 2s = nl$), for $\alpha \in L$ we define the "Minkowski map" $\varphi_L : L \to \mathbb{R}^{nl} = \mathbb{R}^{r+2s}$ sending

$$\alpha \mapsto \Big(\rho_1(\alpha), \ldots, \rho_r(\alpha), \sqrt{2}\,\mathrm{Re}\,\sigma_1(\alpha),\ \sqrt{2}\,\mathrm{Im}\,\sigma_1(\alpha), \ldots, \sqrt{2}\,\mathrm{Re}\,\sigma_s(\alpha),\ \sqrt{2}\,\mathrm{Im}\,\sigma_s(\alpha)\Big).$$

Recall that the image $\Lambda_L = \varphi_L(\mathcal{O}_L)$ is the so-called Minkowski lattice of rank nl in $\mathbb{R}^{nl}$.

Let $\beta_1, \ldots, \beta_{nl}$ be the successive minima of the gauge function $f(x_1, \ldots, x_{nl}) = \max(x_1, \ldots, x_{nl})$ on Λ_L, and denote $f(\varphi(\beta_i)) = ||\beta_i||$ for shorthand. (Note that $||\beta_i||$ is essentially just the maximum archimedean valuation of β_i up to a factor of 2.) Minkowski's Second Theorem [29] says

$$\prod_{i=1}^{nl} ||\beta_i|| \ll |D_L|^{1/2}, \tag{4.1}$$

where the implied constant depends only on nl.

Now since the β_i are nondecreasing, for any k we may use the bound given by 4.1 to write

$$||\beta_k||^{nl+1-k} \leq \prod_{i=k}^{nl} ||\beta_i|| \leq \prod_{i=1}^{nl} ||\beta_i|| \ll D_L^{1/2}$$

whence

$$||\beta_k|| \ll D_L^{1/2(nl+1-k)}. \tag{4.2}$$

For all k with $1 \leq k \leq t+1$, 4.2 implies

$$||\beta_k|| \ll D_L^{1/2l(n-t)} \ll X^{1/2l(n-t)}. \tag{4.3}$$

Now, by our assumption about intermediate subfields, we know that $S = \{\beta_1, \ldots, \beta_{t+1}\}$ will generate L/K, since S spans a vector subspace of L of dimension greater than any proper subfield. By a pigeonhole argument, we see that if $\mathrm{sub}(L/K)$ denotes the number of subfields of L/K (which by Galois theory can be bounded above in terms of n only), there exists a linear combination $\alpha_1 = \sum_S c_i\beta_i$, with integral coefficients bounded in absolute value by $\mathrm{sub}(L/K)$, that generates L/K.

Since K is fixed, we may choose a basis B of $\mathcal{O}_K$ and observe that $S' = S \cup B$ still has the property that $||\beta|| \ll X^{1/2l(n-t)}$ for every $\beta \in S'$. If π is the projection of $\varphi(\langle S' \rangle)$ onto the sublattice of the Minkowski lattice generated by B, then $\alpha = l\alpha_1 - \pi(\alpha_1)$ lies in $\mathcal{O}_L$, has trace zero, generates L/K, and its archimedean norms satisfy

$$||\alpha|| \ll X^{1/2l(n-t)}. \tag{4.4}$$

□

We also require a sieving lemma:

Lemma 6. *Suppose $\Pi : Z \mapsto \mathbb{A}^d$ is a finite map of schemes of degree ≥ 2 and Z is irreducible. Then, for any $\epsilon > 0$, the number of integral points of Z whose images lie in the box centered at 0 whose sides have lengths $(X^{a_1}, X^{a_2}, \ldots, X^{a_d})$ is $\ll X^{(\sum a_i) - \frac{1}{2}a_1 + \epsilon}$, where $a_1 \leq a_2 \leq \cdots \leq a_d$ are positive rational numbers.*

Proof. First, by changing variables for X, we may assume that the a_i are integers. Our starting point is a multivariable version of Hilbert's Irreducibility Theorem due to S.D. Cohen [11]: if $X \to \mathbb{P}^n$ is a morphism of degree ≥ 2, then the number of integral points of $\mathbb{A}^n$ of height $\leq N$ which lift to X is $\ll N^{n-1/2+\epsilon}$.

The side length of the box in that theorem is N, and the result gives a savings of $N^{1/2-\epsilon}$ on the box. The result is also stated for a box centered at 0, but the bound (with a uniform constant) still holds even if we translate to center the box at an arbitrary point.

Now we tile our large box of side lengths $(X^{a_1}, X^{a_2}, \ldots, X^{a_d})$ with square boxes each of which has size $(X^{a_1}, X^{a_1}, \ldots, X^{a_1})$: each square box yields $\ll X^{da_1 - \frac{1}{2}a_1 + \epsilon}$ points of Z having an image in that square box, and we

require a total of $X^{(\sum a_i)-da_1}$ such square boxes to cover the large box. The result follows. □

Remark. There are sieving methods that work directly with non-square boxes, and these would presumably give an additional small savings, although we do not expect the gain to be particularly significant.

We can now prove the main theorem:

Theorem 7. *Let $n \geq 2$, let K be any number field, and let G be a proper transitive subgroup of S_n. Also, let t be such that if G' is the intersection of a point stabilizer in S_n with G, then any subgroup of G properly containing G' has index at most t. Then for any $\epsilon > 0$,*

$$N_{K,n}(X;G) \ll X^{\frac{1}{2(n-t)}\left[\sum_{i=1}^{n-1}\deg(f_{i+1})-\frac{1}{[K:\mathbb{Q}]}\right]+\epsilon}, \tag{4.5}$$

where the f_i for $1 \leq i \leq n$ are a set of primary invariants for G, whose degrees (in particular) satisfy $\deg(f_i) \leq i$.

Remark. The condition about the point stabilizer is (by the Galois correspondence) equivalent to the following: if L/K is a G-extension, then any proper subfield K' of L containing K has $[K' : K] \leq t$. (The criterion in the theorem statement is stated the way it is in order to avoid any reference to L.) We note in particular that if G is a primitive subgroup of S_n, then $t = 1$.

Proof. Let G act on the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ by index permutation, and let $f_1, \ldots, f_n$ be primary invariants of G with associated secondary invariants $1 = g_1, g_2, \ldots, g_k$, each set arranged in order of nondecreasing degree. Observe that because G is transitive, the only primary invariant of degree 1 is $f_1 = x_1 + \cdots + x_n$, and that because G is proper, there is at least one secondary invariant besides $g_1 = 1$.

Denote $A = \mathbb{C}[f_1, \ldots, f_n]$ and $R = \mathbb{C}[x_1, \ldots, x_n]^G$, and observe that $\bar{R} = R/f_1R$ is an integral domain. Let S be the subring of $\bar{R}$ generated by $\bar{f}_2, \ldots, \bar{f}_n$ and $\bar{g}_2$, and let $Z = \mathrm{Spec}(S)$. Observe that S is an integral domain (since $\bar{R}$ is) so Z is irreducible.

The natural map $\mathbb{C}[f_2, \ldots, f_n] \to S$ induces a projection $\Pi : Z \to \mathbb{A}^{n-1}$ (namely, evaluation of the polynomials $f_2, \ldots, f_n$ at the given point), and the map Π is finite because R is a finitely-generated A-module (whence $\bar{R}$ is finite over $\mathbb{C}[f_2, \ldots, f_n]$). Also notice that, by construction, we have $\bar{g}_2 \notin \mathbb{C}[\bar{f}_2, \ldots, \bar{f}_n]$, and so Π has degree at least 2.

Now suppose L/K is an extension of number fields with $[K:\mathbb{Q}] = l$, $[L:K] = n$, such that the Galois group of the Galois closure $\hat{L}/K$ is permutation-isomorphic to G, and such that $\mathrm{Nm}_{K/\mathbb{Q}}(\mathcal{D}_{L/K}) < X$. As noted in Remark 4, the condition on the group G implies that any field K' intermediate between K and L has $[K':K] \leq t$. By Proposition 5, there exists a nonzero element $\alpha \in \mathcal{O}_L$ of trace zero such that all archimedean valuations of α are $\ll X^{\frac{1}{2l(n-t)}}$ and with $L = K(\alpha)$. This element α gives rise to an integral point $\mathbf{x} = (\alpha^{(1)}, \ldots, \alpha^{(n)}) \in Z$, where the $\alpha^{(i)}$ are the archimedean embeddings of α. (Note that we are using the fact that α has trace zero to say that $f_1(\mathbf{x}) = 0$, so that $\mathbf{x}$ is actually well-defined on Z.)

We may then obtain an upper bound on the total possible number of fields L by bounding the number of possible $\mathbf{x}$. But since Π is finite (and its degree is independent of L), we may equivalently bound the number of possibilities for $\Pi(\mathbf{x})$.

Since Π is simply evaluation of the primary invariant polynomials f_i on the point $\mathbf{x}$, the coordinates of $\Pi(\mathbf{x}) = (y_2, \ldots, y_n)$ obey the bounds

$$|y_i| \ll X^{\frac{\deg(f_i)}{2l(n-t)}},$$

for $2 \leq i \leq n$, which forms a "box" B in $\mathbb{A}^n(K)$. By choosing an integral basis of $\mathcal{O}_K$, this box becomes a box in $\mathbb{A}^{nl}(\mathbb{Q})$ with the same dimensions (up to fixed constants), each occurring l times, and the image of $\Pi(\mathbf{x})$ is integral. We now apply Lemma 6 to see that the number of possible integral points $\mathbf{x}$ is $\ll X^{\frac{1}{2(n-t)l}\left[l\sum_{i=1}^{n-1}\deg(f_{i+1}) - \frac{1}{2}\deg(f_2)\right]+\epsilon}$. Finally, since $\deg(f_2) = 2$ and each $\mathbf{x}$ gives rise to at most one distinct extension L/K, we obtain

$$\begin{aligned} N_{K,n}(X;G) &\leq \#\{\text{integral } \mathbf{x} \in Z \text{ with } \Pi(\mathbf{x}) \in B\} \\ &\ll X^{\frac{1}{2(n-t)}\left[\sum_{i=1}^{n-1}\deg(f_{i+1}) - \frac{1}{l}\right]+\epsilon}, \end{aligned}$$

which is precisely the desired result. □

Remark. Note that we require the existence of a secondary invariant in order to apply Lemma 6. Without a secondary invariant, we lose the power savings and instead obtain the upper bound $X^{\frac{1}{2(n-t)}\left[\sum_{i=1}^{n-1}\deg(f_{i+1})\right]}$. This will only occur when $G = S_n$, whose primary invariants are the usual symmetric polynomials (with degrees $2, 3, \ldots, n$): it is then easy to see that our upper

bound is

$$X^{\frac{1}{2(n-1)}[\sum_{i=1}^{n-1}(i+1)]} = X^{\frac{1}{2(n-1)}[n(n+1)/2-1]} = X^{\frac{n+2}{4}},$$

which is precisely Schmidt's bound. Since the symmetric polynomials are a set of primary invariants for any permutation group, we therefore see that for any primitive proper transitive subgroup of S_n, our theorem always beats the bound of Schmidt (due to the power-savings from the sieving and the fact that $t = 1$). However, in practice for most primitive groups G, the majority of the actual savings comes from the primary invariants, whose degrees tend to be much smaller than the degrees of the symmetric polynomials.

5. A prototypical example: $PSL_2(\mathbb{F}_7)$ in S_7

In this section we give an explicit example of a primary invariant computation, for the group $G = PSL_2(\mathbb{F}_7) \cong GL_3(\mathbb{F}_2)$, which is the simple group of order 168, and appears as 7T5 in the tables in Appendix A.

Corollary 8. *For any $\epsilon > 0$, $N_{\mathbb{Q},7}(X; G) \ll X^{11/6+\epsilon}$.*

For comparison, Schmidt's bound (for general degree-7 extensions) gives an upper bound of $X^{9/4}$, and the Ellenberg-Venkatesh bound is weaker.

Proof. Let $G = \langle (1\,2\,3\,4\,5\,6\,7),\ (1\,2)(3\,6)\rangle$; it is a primitive permutation group on $\{1, 2, 3, 4, 5, 6, 7\}$ whose action is conjugate to the action of $PSL_2(\mathbb{F}_7)$ on $\mathbb{P}^1(\mathbb{F}_7)$. A computation with MAGMA shows that primary invariants can be chosen as

$$\begin{aligned}
f_1 &= x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7\\
f_2 &= x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2\\
f_3 &= x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 + x_6^3 + x_7^3\\
f_4 &= x_1x_2x_3 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_4 + x_1x_3x_6 + x_1x_3x_7\\
&\quad + x_1x_4x_5 + x_1x_4x_6 + x_1x_4x_7 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_4 + x_2x_3x_5\\
&\quad + x_2x_3x_7 + x_2x_4x_5 + x_2x_4x_6 + x_2x_4x_7 + x_2x_5x_6 + x_2x_6x_7\\
&\quad + x_3x_4x_5 + x_3x_4x_6 + x_3x_5x_6 + x_3x_5x_7 + x_3x_6x_7 + x_4x_5x_7\\
&\quad + x_4x_6x_7 + x_5x_6x_7
\end{aligned}$$

$$
\begin{aligned}
f_5 &= x_1^4 + x_2^4 + x_3^4 + x_4^4 + x_5^4 + x_6^4 + x_7^4 \\
f_6 &= x_1^2x_2x_3 + x_1^2x_2x_5 + x_1^2x_2x_6 + x_1^2x_2x_7 + x_1^2x_3x_4 + x_1^2x_3x_6 + x_1^2x_3x_7 \\
&\quad + x_1^2x_4x_5 + x_1^2x_4x_6 + x_1^2x_4x_7 + x_1^2x_5x_6 + x_1^2x_5x_7 + x_1x_2^2x_3 + x_1x_2^2x_5 \\
&\quad + x_1x_2^2x_6 + x_1x_2^2x_7 + x_1x_2x_3^2 + x_1x_2x_5^2 + x_1x_2x_6^2 + x_1x_2x_7^2 + x_1x_3^2x_4 \\
&\quad + x_1x_3^2x_6 + x_1x_3^2x_7 + x_1x_3x_4^2 + x_1x_3x_6^2 + x_1x_3x_7^2 + x_1x_4^2x_5 + x_1x_4^2x_6 \\
&\quad + x_1x_4^2x_7 + x_1x_4x_5^2 + x_1x_4x_6^2 + x_1x_4x_7^2 + x_1x_5^2x_6 + x_1x_5^2x_7 + x_1x_5x_6^2 \\
&\quad + x_1x_5x_7^2 + x_2^2x_3x_4 + x_2^2x_3x_5 + x_2^2x_3x_7 + x_2^2x_4x_5 + x_2^2x_4x_6 + x_2^2x_4x_7 \\
&\quad + x_2^2x_5x_6 + x_2^2x_6x_7 + x_2x_3^2x_4 + x_2x_3^2x_5 + x_2x_3^2x_7 + x_2x_3x_4^2 + x_2x_3x_5^2 \\
&\quad + x_2x_3x_7^2 + x_2x_4^2x_5 + x_2x_4^2x_6 + x_2x_4^2x_7 + x_2x_4x_5^2 + x_2x_4x_6^2 + x_2x_4x_7^2 \\
&\quad + x_2x_5^2x_6 + x_2x_5x_6^2 + x_2x_6^2x_7 + x_2x_6x_7^2 + x_3^2x_4x_5 + x_3^2x_4x_6 + x_3^2x_5x_6 \\
&\quad + x_3^2x_5x_7 + x_3^2x_6x_7 + x_3x_4^2x_5 + x_3x_4^2x_6 + x_3x_4x_5^2 + x_3x_4x_6^2 + x_3x_5^2x_6 \\
&\quad + x_3x_5^2x_7 + x_3x_5x_6^2 + x_3x_5x_7^2 + x_3x_6^2x_7 + x_3x_6x_7^2 + x_4^2x_5x_7 + x_4^2x_6x_7 \\
&\quad + x_4x_5^2x_7 + x_4x_5x_7^2 + x_4x_6^2x_7 + x_4x_6x_7^2 + x_5^2x_6x_7 + x_5x_6^2x_7 + x_5x_6x_7^2 \\
f_7 &= x_1^7 + x_2^7 + x_3^7 + x_4^7 + x_5^7 + x_6^7 + x_7^7
\end{aligned}
$$

of degrees 1, 2, 3, 3, 4, 4, 7 respectively. Invoking Theorem 7 yields the stated bound. (Note here that $t = 1$.) □

We will note that the group $G = PSL_2(\mathbb{F}_7)$ also appears as a transitive subgroup of S_8 (it is 8T37 in the tables in Appendix A), but the upper bounds obtained are different: as a subgroup of S_7 we obtain the bound $X^{11/6+\epsilon}$, while as a subgroup of S_8 we obtain $X^{29/14+\epsilon}$. This should not be surprising, as the fields being counted are different (though related): in the S_7 case we are counting fields of degree 7 whose Galois action on the 7 complex embeddings is that of G, whereas in the S_8 case we are counting fields of degree 8 whose Galois action on the 8 complex embeddings is that of G. Indeed, the predictions from Malle's heuristics also differ for these fields: the number of degree-7 G-extensions is expected to be approximately $X^{1/2+\epsilon}$ while the number of degree-8 G-extensions is expected to be approximately $X^{1/4+\epsilon}$.

6. Closing remarks

Per Malle's heuristics, we would expect the actual number of integral points to be (much) lower than the bound given by Theorem 7. There are three ways in which we lose accuracy:

1) The map associating an element $\mathbf{x}$ to an extension L/K is not injective: any extension has many different generators. Worse still, there is no uniform way to account for this non-injectivity: an extension of small discriminant will have many generators of small archimedean norm, and thus it will show up in the count much more frequently than an extension of larger discriminant.

2) The simple techniques employed above for counting integral points on the scheme Z give weaker bounds than could be hoped for. Most points in affine space are not actually the image of an integral point on Z, so we would not expect that the sieving lemma 6 is sharp: it is likely only extracting a small amount of the potential savings that should be realizable.

3) If L/K has any intermediate extensions, the bound given in Lemma 5 on the archimedean norm of a generator is weaker than for a primitive extension. The worst losses occur when L/K has a subfield of small index (e.g., index 2), in which case the exponent obtained in Theorem 7 is nearly doubled.

One technique by which we could address the issues in (1) is that of Ellenberg-Venkatesh [18]: rather than counting the number of possibilities for the single element $\mathbf{x}$ of trace zero and whose archimedean valuations are small, we could instead count the number of possibilities for an r-tuple of elements $(\mathbf{x}_1, \ldots, \mathbf{x}_r)$, each of whose archimedean valuations is small. This would provide a stronger way of separating extensions of differing discriminants and reduce the amount of duplication in the counting (though it cannot entirely erase duplicate counting).

In order to address the deficiencies of (2), we would require the use of stronger point-counting techniques. To do this, however, would require understanding the geometry of the scheme Z in a much deeper way. For particular groups G with low-degree permutation representations, this is (at least, theoretically) feasible, since the primary invariants are explicitly computable. However, for large n this seems very unlikely to succeed, since the invariant theory becomes extremely computationally demanding for $n > 10$.

To deal with the deficiencies of (3), it seems likely that a more direct analysis of the possible extension towers for extensions of small degree over general base fields could yield significant savings, but we will not pursue this avenue here.

As a concluding remark, one way of reinterpreting Theorem 7 is to view it as a result about permutation representations of groups. The invariant theory involved in the proof carries over to general representations ρ, and so one could ask: is there a way to construct an analogue of these results attached to an arbitrary faithful representation ρ? As we show in a forthcoming paper [16], the answer to this question is also "yes".

Appendix A. Tabulation of results

In the following tables, we give the results of the invariant computations, performed using the algebra system MAGMA, for all proper transitive subgroups of S_n for $n = 5, 6, 7, 8$, along with a small number of subgroups of S_9 for which it was possible to finish the invariant computations within 2 days on a 4Ghz desktop computer with 1GB of memory. We observe that for primitive transitive subgroups, the result of Theorem 7 is significantly better than the overall bound of Schmidt, although the results generally do not get close to X^1 nor (a fortiori) to the bounds in Malle's Conjecture 4. For imprimitive extensions, and especially in even degree (where many extensions have an index-2 subfield), the results are frequently worse than Schmidt's bound.

The labeling of the transitive subgroups is the standard one originally given by Conway-Hulpke-McKay [12]. Subfield information was obtained from John Jones' page on transitive group data [19], which also contains additional detailed information about the transitive subgroups.

For brevity in the tables below, we quote the results of Theorem 7 only for the base field $K = \mathbb{Q}$, and we write the results as $X^{\#}$ rather than $X^{\#+\epsilon}$ (including the bounds conjectured by Malle). The upper bound over a general base field K of degree l over $\mathbb{Q}$ is (for an entry of $X^{\#}$) equal to $X^{\#+1-\frac{1}{l}+\epsilon}$. Rows marked with an asterisk are groups for which Malle's weak conjecture is known to hold. For subgroups of S_5, we compare the results to the bound of Bhargava; for other symmetric groups, we compare our results to that of Schmidt.

We also remark that for certain classes of groups such as the dihedral groups, there are bounds available (e.g., from class field theory) that are far better than Schmidt's bound.

Proper transitive subgroups of S_5							
#	Order	Isom. to	Subfield?	Invariant Degrees	Result	Malle	Bhargava
5T1	5*	C_5	none	1,2,2,3,5	$X^{11/8}$	$X^{1/4}$	X^1
5T2	10	D_5	none	1,2,2,3,5	$X^{11/8}$	$X^{1/2}$	X^1

Proper transitive subgroups of S_5 (continued)							
#	Order	Isom. to	Subfield?	Invariant Degrees	Result	Malle	Bhargava
5T3	20	F_{20}	none	1,2,3,4,5	$X^{13/8}$	$X^{1/2}$	X^1
5T4	60	A_5	none	1,2,3,4,5	$X^{13/8}$	$X^{1/2}$	X^1

Proper transitive subgroups of S_6							
#	Ord	Isom. to	Subfield?	Invariant Degrees	Result	Malle	Schmidt
6T1	6*	C_6	Deg. 3	1,2,2,2,3,6	$X^{7/3}$	$X^{1/3}$	X^2
6T2	6*	S_3	Deg. 3	1,2,2,2,3,3	$X^{11/6}$	$X^{1/3}$	X^2
6T3	12	$S_3 \times C_2$	Deg. 3	1,2,2,2,3,6	$X^{7/3}$	$X^{1/2}$	X^2
6T4	12	A_4	Deg. 3	1,2,2,3,3,4	X^2	$X^{1/2}$	X^2
6T5	18	F_{18}	Deg. 2	1,2,2,3,3,6	$X^{7/4}$	$X^{1/2}$	X^2
6T6	24	$A_4 \times C_2$	Deg. 3	1,2,2,3,4,6	$X^{8/3}$	X^1	X^2
6T7	24	S_4	Deg. 3	1,2,2,3,3,4	$X^{13/6}$	$X^{1/2}$	X^2
6T8	24	S_4	Deg. 3	1,2,2,3,4,6	$X^{8/3}$	$X^{1/2}$	X^2
6T9	36	$S_3 \times S_3$	Deg. 2	1,2,2,3,4,6	X^2	$X^{1/2}$	X^2
6T10	36	F_{36}	Deg. 2	1,2,3,3,4,6	$X^{17/8}$	$X^{1/2}$	X^2
6T11	48	$S_4 \times C_2$	Deg. 3	1,2,2,3,4,6	$X^{8/3}$	X^1	X^2
6T12	60	A_5	none	1,2,3,3,4,5	$X^{8/5}$	$X^{1/2}$	X^2
6T13	72	$F_{36} \rtimes C_2$	Deg. 2	1,2,2,3,4,6	X^2	X^1	X^2
6T14	120	S_5	none	1,2,3,4,5,6	$X^{19/10}$	$X^{1/2}$	X^2
6T15	360	A_6	none	1,2,3,4,5,6	$X^{19/10}$	$X^{1/2}$	X^2

Proper transitive subgroups of S_7							
#	Order	Isom. to	Subfield?	Invariant Degrees	Result	Malle	Schmidt
7T1	7*	C_7	none	1,2,2,2,3,4,7	$X^{19/12}$	$X^{1/6}$	$X^{9/4}$
7T2	14	D_7	none	1,2,2,2,3,4,7	$X^{19/12}$	$X^{1/3}$	$X^{9/4}$
7T3	21	F_{21}	none	1,2,3,3,3,4,7	$X^{7/4}$	$X^{1/4}$	$X^{9/4}$
7T4	42	F_{42}	none	1,2,3,3,4,6,7	X^2	$X^{1/3}$	$X^{9/4}$
7T5	168	$PSL_2(\mathbb{F}_7)$	none	1,2,3,3,4,4,7	$X^{11/6}$	$X^{1/2}$	$X^{9/4}$
7T6	2520	A_7	none	1,2,3,4,5,6,7	$X^{13/6}$	$X^{1/2}$	$X^{9/4}$

Proper transitive subgroups of S_8							
#	Order	Isom. to	Subfield?	Invariant Degrees	Result	Malle	Schmidt
8T1	8*	C_8	Deg. 4	1,2,2,2,2,3,4,8	$X^{11/4}$	$X^{1/4}$	$X^{5/2}$
8T2	8*	$C_4 \times C_2$	Deg. 4	1,2,2,2,2,2,4,4	$X^{17/8}$	$X^{1/4}$	$X^{5/2}$
8T3	8*	$(C_2)^3$	Deg. 4	1,2,2,2,2,2,2,2	$X^{13/8}$	$X^{1/4}$	$X^{5/2}$
8T4	8*	D_4	Deg. 4	1,2,2,2,2,2,4,4	$X^{17/8}$	$X^{1/4}$	$X^{5/2}$
8T5	8*	Q_8	Deg. 4	1,2,2,2,2,4,4,4	$X^{19/8}$	$X^{1/4}$	$X^{5/2}$
8T6	16*		Deg. 4	1,2,2,2,2,3,4,8	$X^{11/4}$	$X^{1/3}$	$X^{5/2}$
8T7	16*		Deg. 4	1,2,2,2,3,4,4,8	X^3	$X^{1/2}$	$X^{5/2}$
8T8	16*		Deg. 4	1,2,2,2,3,4,4,8	X^3	$X^{1/3}$	$X^{5/2}$

Proper transitive subgroups of S_8 (continued)							
#	Order	Isom. to	Subfield?	Invariant Degrees	Result	Malle	Schmidt
8T9	16*	$D_4 \rtimes C_2$	Deg. 4	1,2,2,2,2,2,4,4	$X^{17/8}$	$X^{1/2}$	$X^{5/2}$
8T10	16*		Deg. 4	1,2,2,2,2,3,4,4	$X^{9/4}$	$X^{1/2}$	$X^{5/2}$
8T11	16*		Deg. 4	1,2,2,2,2,4,4,4	$X^{19/8}$	$X^{1/2}$	$X^{5/2}$
8T12	24	$SL_2(\mathbb{F}_3)$	Deg. 4	1,2,2,3,3,4,4,6	$X^{23/8}$	$X^{1/4}$	$X^{5/2}$
8T13	24	$A_4 \times C_2$	Deg. 4	1,2,2,2,3,3,4,6	$X^{21/8}$	$X^{1/4}$	$X^{5/2}$
8T14	24	S_4	Deg. 4	1,2,2,2,3,4,4,6	$X^{11/4}$	$X^{1/4}$	$X^{5/2}$
8T15	32*		Deg. 4	1,2,2,2,3,4,4,8	X^3	$X^{1/2}$	$X^{5/2}$
8T16	32*		Deg. 4	1,2,2,2,3,4,4,8	X^3	$X^{1/2}$	$X^{5/2}$
8T17	32*		Deg. 4	1,2,2,2,3,4,4,8	X^3	$X^{1/2}$	$X^{5/2}$
8T18	32*		Deg. 4	1,2,2,2,2,3,4,4	$X^{9/4}$	$X^{1/2}$	$X^{5/2}$
8T19	32*		Deg. 4	1,2,2,2,3,4,4,4	$X^{5/2}$	$X^{1/2}$	$X^{5/2}$
8T20	32*		Deg. 4	1,2,2,2,3,4,4,4	$X^{5/2}$	$X^{1/2}$	$X^{5/2}$
8T21	32*		Deg. 4	1,2,2,2,2,4,4,4	$X^{19/8}$	$X^{1/2}$	$X^{5/2}$
8T22	32*		Deg. 4	1,2,2,2,2,4,4,4	$X^{19/8}$	$X^{1/2}$	$X^{5/2}$
8T23	48	$GL_2(\mathbb{F}_3)$	Deg. 4	1,2,2,3,3,4,6,8	$X^{27/8}$	$X^{1/3}$	$X^{5/2}$
8T24	48	$S_4 \times C_2$	Deg. 4	1,2,2,2,3,4,4,6	$X^{11/4}$	$X^{1/2}$	$X^{5/2}$
8T25	56	F_{56}	none	1,2,3,4,4,4,4,7	$X^{27/14}$	$X^{1/4}$	$X^{5/2}$
8T26	64*		Deg. 4	1,2,2,2,3,4,4,8	X^3	$X^{1/2}$	$X^{5/2}$
8T27	64*		Deg. 4	1,2,2,2,3,4,4,8	X^3	X^1	$X^{5/2}$
8T28	64*		Deg. 4	1,2,2,2,3,4,4,8	X^3	$X^{1/2}$	$X^{5/2}$
8T29	64*		Deg. 4	1,2,2,2,3,4,4,4	$X^{5/2}$	$X^{1/2}$	$X^{5/2}$
8T30	64*		Deg. 4	1,2,2,2,3,4,4,8	X^3	$X^{1/2}$	$X^{5/2}$
8T31	64*		Deg. 4	1,2,2,2,2,4,4,4	$X^{19/8}$	X^1	$X^{5/2}$
8T32	96		Deg. 4	1,2,2,3,3,4,4,6	$X^{23/8}$	$X^{1/2}$	$X^{5/2}$
8T33	96	$(C_2)^2 \rtimes C_6$	Deg. 2	1,2,2,3,4,4,4,6	X^2	$X^{1/2}$	$X^{5/2}$
8T34	96	$(E_4)^2 \rtimes D_6$	Deg. 2	1,2,2,3,4,4,4,6	X^2	$X^{1/2}$	$X^{5/2}$
8T35	128*		Deg. 4	1,2,2,2,3,4,4,8	X^3	X^1	$X^{5/2}$
8T36	168	$(C_2)^3 \rtimes F_{21}$	none	1,2,3,4,4,5,6,7	$X^{15/7}$	$X^{1/4}$	$X^{5/2}$
8T37	168	$PSL_2(\mathbb{F}_7)$	none	1,2,3,4,4,4,6,7	$X^{29/14}$	$X^{1/4}$	$X^{5/2}$
8T38	192		Deg. 4	1,2,2,3,3,4,6,8	$X^{27/8}$	X^1	$X^{5/2}$
8T39	192		Deg. 4	1,2,2,3,3,4,4,6	$X^{23/8}$	$X^{1/2}$	$X^{5/2}$
8T40	192		Deg. 4	1,2,2,3,3,4,6,8	$X^{27/8}$	$X^{1/2}$	$X^{5/2}$
8T41	192	$(C_2)^3 \rtimes S_4$	Deg. 2	1,2,2,3,4,4,4,6	X^2	$X^{1/2}$	$X^{5/2}$
8T42	288		Deg. 2	1,2,2,3,4,4,6,6	$X^{13/6}$	$X^{1/2}$	$X^{5/2}$
8T43	336	$PGL_2(\mathbb{F}_7)$	none	1,2,3,4,4,6,7,8	$X^{33/14}$	$X^{1/3}$	$X^{5/2}$
8T44	384		Deg. 4	1,2,2,3,3,4,6,8	$X^{27/8}$	X^1	$X^{5/2}$
8T45	$2^6 3^2$		Deg. 2	1,2,2,3,4,4,6,8	$X^{7/3}$	$X^{1/2}$	$X^{5/2}$
8T46	$2^6 3^2$		Deg. 2	1,2,2,3,4,4,6,8	$X^{7/3}$	$X^{1/2}$	$X^{5/2}$
8T47	$2^7 3^2$		Deg. 2	1,2,2,3,4,4,6,8	$X^{7/3}$	X^1	$X^{5/2}$
8T48	$2^6 3^1 7^1$	$AL(8)$	none	1,2,3,4,4,5,6,7	$X^{15/7}$	$X^{1/2}$	$X^{5/2}$
8T49	8!/2	A_8	none	1,2,3,4,5,6,7,8	$X^{17/7}$	$X^{1/2}$	$X^{5/2}$

Some transitive subgroups of S_9							
#	Order	Isom. to	Subfield?	Invariant Degrees	Result	Malle	Schmidt
9T3	18	D_9	Deg. 3	1,2,2,2,2,3,3,5,8	$X^{13/6}$	$X^{1/4}$	$X^{11/4}$
9T4	18	$S_3 \times C_3$	Deg. 3	1,2,2,2,3,3,3,3,6	$X^{23/12}$	$X^{1/3}$	$X^{11/4}$
9T5	18*	$(C_3)^2 \rtimes C_2$	Deg. 3	1,2,2,2,2,3,3,3,3	$X^{19/12}$	$X^{1/4}$	$X^{11/4}$
9T8	36	$S_3 \times S_3$	Deg. 3	1,2,2,2,3,3,3,4,6	X^2	$X^{1/3}$	$X^{11/4}$

Acknowledgements

The author would like to thank Jordan Ellenberg and Akshay Venkatesh for their work which inspired this paper, John Voight for computing assistance with MAGMA, David Dummit and Dinesh Thakur for their helpful editorial comments, and Jordan Ellenberg in particular for his comments and persistent encouragement.

References

[1] B. Alberts, *The weak form of Malle's conjecture and solvable groups*, preprint (2018), `arXiv:1804.11318`.

[2] A. M. Baily, *On the density of discriminants of quartic fields*, J. reine angew. Math **315** (1980), 190–210.

[3] K. Belabas, M. Bhargava, and C. Pomerance, *Error estimates for the Davenport-Heilbronn theorems*, Duke Mathematical Journal **153** (2010), no. 1, 173–210.

[4] M. Bhargava, *The density of discriminants of quartic rings and fields*, Annals of Mathematics (2005), 1031–1063.

[5] M. Bhargava, *The density of discriminants of quintic rings and fields*, Annals of Mathematics (2010), 1559–1591.

[6] M. Bhargava, A. Shankar, and J. Tsimerman, *On the Davenport–Heilbronn theorems and second order terms*, Inventiones Mathematicae **193** (2013), no. 2, 439–499.

[7] M. Bhargava, A. Shankar, and X. Wang, *Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces*, preprint (2015), `arXiv:1512.03035`.

[8] M. Bhargava and M. Wood, *The density of discriminants of S_3-sextic number fields*, Proceedings of the American Mathematical Society **136** (2008), no. 5, 1581–1587.

[9] H. Cohen, *Constructing and Counting Number Fields*, Proceedings of the ICM **2** (2002), 129–138.

[10] H. Cohen, F. D. y Diaz, and M. Olivier, *A survey of discriminant counting*, in: International Algorithmic Number Theory Symposium, 80–94, Springer (2002).

[11] S. D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proceedings of the London Mathematical Society **3** (1981), no. 2, 227–250.

[12] J. H. Conway, A. Hulpke, and J. McKay, *On transitive permutation groups*, LMS Journal of Computation and Mathematics **1** (1998), 1–8.

[13] B. Datskovsky and D. J. Wright, *Density of discriminants of cubic extensions*, J. reine angew. Math **386** (1988), 116–138.

[14] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences (1971), 405–420.

[15] H. Derksen and G. Kemper, Computational invariant theory, Springer (2015).

[16] E. P. Dummit, *The ρ-discriminant and applications*, unpublished preprint.

[17] J. S. Ellenberg and A. Venkatesh, *Counting extensions of function fields with bounded discriminant and specified Galois group*, in: Geometric methods in algebra and number theory, 151–168, Springer (2005).

[18] J. S. Ellenberg and A. Venkatesh, *The number of extensions of a number field with fixed degree and bounded discriminant*, Annals of Mathematics (2006), 723–741.

[19] J. Jones, Transitive Group Data (accessed October 2016). `http://hobbes.la.asu.edu/Groups/`.

[20] A. C. Kable and A. Yukie, *On the number of quintic fields*, Inventiones Mathematicae **160** (2005), no. 2, 217–259.

[21] J. Klüners, *A counter example to Malle's conjecture on the asymptotics of discriminants*, Comptes Rendus Mathematique **340** (2005), no. 6, 411–414.

[22] J. Klüners, *The distribution of number fields with wreath products as Galois groups*, International Journal of Number Theory **8** (2012), no. 03, 845–858.

[23] J. Klüners and G. Malle, *Counting nilpotent Galois extensions*, J. reine angew. Math (2004), 1–26.

[24] S. Mäki, On the density of abelian number fields, Vol. 54, Suomalainen tiedeakatemia (1985).

[25] G. Malle, *On the distribution of Galois groups*, Journal of Number Theory **92** (2002), no. 2, 315–329.

[26] G. Malle, *On the distribution of Galois groups, II*, Experimental Mathematics **13** (2004), no. 2, 129–135.

[27] W. M. Schmidt, *Number fields of given degree and bounded discriminant*, Astérisque **228** (1995), no. 4, 189–195.

[28] A. Shankar and J. Tsimerman, *Counting S_5-fields with a power-saving error term*, in: Forum of Mathematics, Sigma, Vol. 2, e13, Cambridge Univ Press (2014).

[29] C. L. Siegel, Lectures on the Geometry of Numbers, Springer Science & Business Media (2013).

[30] T. Taniguchi and F. Thorne, *Secondary terms in counting functions for cubic fields*, Duke Mathematical Journal **162** (2013), no. 13, 2451–2508.

[31] S. Türkelli, *Connected components of Hurwitz Schemes and Malle's conjecture*, Journal of Number Theory **155** (2015), 163–201.

[32] D. J. Wright, *Distribution of discriminants of abelian extensions*, Proceedings of the London Mathematical Society **3** (1989), no. 1, 17–50.

[33] A. Yukie, Shintani Zeta Functions, Vol. 183, Cambridge University Press (1993).

School of Mathematical and Statistical Sciences
Wexler Hall, Arizona State University, Tempe AZ 85287, USA
E-mail address: evan.dummit@asu.edu

Received October 29, 2016