Counting Number Field Extensions of Given Degree, Bounded Discriminant, and Specified Galois Closure

By

Evan P. Dummit

A dissertation submitted in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

(Mathematics)

at the

UNIVERSITY OF WISCONSIN – MADISON

2014

Date of final oral examination: August 7th, 2014

The dissertation is approved by the following members of the Final Oral Committee:

Jordan S. Ellenberg, Full Professor, Mathematics

Melanie Matchett Wood, Assistant Professor, Mathematics

Nigel Boston, Full Professor, Mathematics

Daniel Erman, Assistant Professor, Mathematics

Richard Kent, Assistant Professor, Mathematics

Abstract

For a given number field K, this dissertation focuses on counting the number of extensions L/K of a fixed degree, specified Galois closure, and bounded discriminant.

We begin in Chapter 1 with a historical overview of counting number fields by discriminant and outline a number of prior results on this and related problems.

In Chapter 2, we prove an upper-bound asymptotic on the number $N_{K,n}(X;G)$ of extensions L/K having the Galois group of the Galois closure of L/K isomorphic to G, and such that the classical discriminant $\mathrm{Nm}_{K/\mathbb{Q}}(\mathscr{D}_{L/K})$ is at most X. We then give a tabulation of explicit upper bounds for particular Galois groups.

In Chapter 3, we generalize the results of Chapter 2 to general representations by introducing a new counting metric called the ρ-discriminant, and we then prove an analogue of the counting theorem from Chapter 2 in this setting.

We conclude with a discussion of questions left open for future work.

The main techniques involved in establishing the results are from the geometry of numbers, polynomial invariant theory, integral-point counting on schemes, and representation theory of finite groups.

Acknowledgements

I would like to thank the following individuals for their personal contributions to the mathematics contained herein:

- My advisor Jordan Ellenberg, for his persistent support and encouragement, and for originally bringing the problem that ultimately became this thesis to my attention. Without him, this work would not exist.
- Daniel Ross and Lalit Jain for their gracious help in generalizing their work on a closely-related counting problem for dihedral extensions.
- Melanie Matchett Wood for her help in understanding her work with the tuning submodule.
- Rob Harron for his help with Sage and computations with Malle's conjectures.
- Silas Johnson for his help with technical aspects of discriminant counting.
- Marci Hablicsek for his help in algebraic geometry and typesetting.
- David Zureick-Brown and John Voight for their help with MAGMA.
- David Dummit, for typography, editing, and general mathematical help.
- All of my other friends and colleagues for the countless conversations I had on every aspect of my work.

I dedicate this text to my family, especially Kathleen, David, Janice, and Krysta, whose love and support have guided my life.

Contents

Chapter 1

Introduction and Background

1.1. Overview

Among the most fundamental objects of study in number theory are algebraic number fields and extensions of number fields.

A very basic question is: how many number fields (with some particular set of properties) are there?

A fundamental invariant attached to a number field is its degree over $\mathbb{Q}$, but there are infinitely many number fields of any degree greater than 1: so if we wish to put them in some kind of order, we must filter them in a more careful manner. An invariant that refines the degree is the Galois group of its Galois closure $\mathsf{G} = \mathrm{Gal}(\hat{\mathsf{L}}/\mathbb{Q})$, which encapsulates the structure of the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on L and its subfields. However, even if the Galois group G of this Galois closure is fixed, there may still be infinitely many possible number fields L.

Another natural invariant attached to an extension $\mathsf{L}/\mathbb{Q}$ is the discriminant D_{L}, which (roughly speaking) measures how complicated the extension is. For example, the discriminant of the quadratic number field $\mathbb{Q}(\sqrt{\mathsf{D}})$ is either D or $4\mathsf{D}$ (where D is or is not, respectively, congruent to 1 modulo 4), which grows as D increases.

Over a century ago, Hermite [19] showed that the number of number fields of a given

degree whose (absolute) discriminant is less than X is finite (see Section 1.3 for a brief summary). Thus, ordering number fields of a fixed degree (or fixed Galois closure) by discriminant provides us with a variety of well-posed counting problems.

Our primary interest is in analyzing the asymptotics, as $X \to \infty$, of the number of extensions (of fixed degree and Galois closure) of discriminant less than X. As we discuss further in Section 1.6, providing exact asymptotics is quite difficult and has been carried out in only a few cases; thus, our goal in the present work is to give upper bounds on this quantity.

In the remainder of this introduction, we will briefly outline some necessary preliminaries regarding lattices and invariant theory, and then discuss a number of historical results on counting number fields ordered by discriminant.

In Chapter 2, we will prove a general theorem bounding from above the number of extensions of a given degree, bounded discriminant, and specified Galois closure. (We note in particular that the result is better than any previously known, for almost all Galois groups.) We then tabulate a number of corollaries and detailed examples.

In Chapter 3, we will consider other counting metrics aside from the standard discriminant D_L and introduce a new metric attached to a faithful representation $\rho : G \to GL_d(K)$ called the ρ-discriminant. We will then generalize the counting theorem and results from Chapter 2 into this setting.

We close with a discussion of a number of related open problems.

1.2. Notation and Background

To introduce some notation, let K be a number field and L/K be an extension of degree n. We will let $\mathscr{O}_L$ and $\mathscr{O}_K$ be the rings of integers, and D_L and D_K be the absolute discriminants of L and K respectively, and $D_{L/K}$ be the relative discriminant ideal in $\mathscr{O}_K$. We also take $\mathrm{Nm}_{K/\mathbb{Q}}$ to be the absolute norm on ideals or elements (as appropriate).

We will employ the standard notations $f(X) \sim g(X)$ to mean $\lim_{X\to\infty} \frac{g(X)}{f(X)} = 1$, 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 subgroup of S_n (unless otherwise specified).

Definition 1.1. *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* $\mathrm{Nm}_{K/\mathbb{Q}}(\mathscr{D}_{L/K}) < X$.

A folk conjecture, sometimes attributed to Linnik, says that

$$N_{K,n}(X) \sim C_{K,n} X \tag{1.2.1}$$

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 [13], and Datskovsky and Wright [12] for general K. For $K = \mathbb{Q}$, the results for $n = 4$ and $n = 5$ are known and due to Bhargava and Kable-Yukie [3, 41, 5, 21], and in principle these results should extend to general

base fields.

The best upper bound for general n was established by Ellenberg and Venkatesh in 2006 [18]. For sufficiently large n (roughly on the order of $n = 20$), their results improve on the only previous result for general n, due to Schmidt [33].

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

Definition 1.2. *For fixed* K *and* n*, and a transitive permutation group* $G \hookrightarrow S_n$ *with a particular 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 $\mathrm{Nm}_{K/\mathbb{Q}}(\mathscr{D}_{L/K})$ 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.

For shorthand, we refer to extensions satisfying these conditions as G-extensions. We will also frequently 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 [26, 27] give expected growth rates for $N_{K,n}(X; G)$ depending on the group G. One such statement is as follows:

Conjecture 1.3. *(Malle, weak form) For any number field* K *and any* $\epsilon > 0$*,*

$$c_K(G)\, X^{a(G)} < N_{K,n}(X; G) < X^{a(G)+\epsilon}, \tag{1.2.2}$$

where $0 < a(G) \leq 1$ *is a computable constant depending on* G *(but not* K*) that is contained in* $\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right\}$*, and* $c_K(G)$ *is a positive constant. Furthermore, if* $a(G) = 1$ *then the upper bound can be replaced by* $c'_K X$ *for some (other) positive constant* c'_K*.*

For example, Malle's conjecture says that for the Klein 4-group $V_4 = C_2 \times C_2$ (embedded in S_4), and any $\epsilon > 0$, then for sufficiently large X,

$$c\, X^{1/2} < N_{\mathbb{Q},n}(X; V_4) < d_\epsilon X^{1/2+\epsilon}$$

for some constants c and d_ϵ. (In fact, much more is known about the growth of $N_{\mathbb{Q},n}(X; V_4)$: see Theorem 1.12.)

There are various stronger versions of this conjecture; see the the discussion in 1.6.1 for more detail. We also remark that similar counting asymptotics are expected to hold for arbitrary global fields (not just number fields).

If true, Malle's conjecture, even when we restrict to this weak form and only consider extensions of $\mathbb{Q}$, would (for example) imply that every finite group is a Galois group over $\mathbb{Q}$ – as such, it is considered to be completely unattainable with current methods.

As we discuss in more detail in Section 1.6, an upper bound at least as strong as the weak form of Malle's conjecture 1.2.2 is known to hold in the following cases over general number fields K:

1. For any abelian group [39], with the asymptotic constants (in principle).
2. For any nilpotent group [25]. For a nilpotent group in its regular representation, the lower bound is also known.
3. For S_3 [12, 13], with the specified asymptotic constants. In fact, there is a second main term, and the asymptotic constant is also known [6, 36].
4. For D_4 and S_4 (in principle over general K) [1, 3, 8]. The asymptotic constants are also known.
5. For S_5 (in principle over general K) [21, 5], as well as the asymptotic constant.
6. For degree-6 S_3 extensions [7], as well as the asymptotic constant.

7. Under mild restrictions, for wreath products of the form $C_2 \wr H$ where H is nilpotent [24].

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 $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K(a_1, \cdots, a_n)$ has Galois group S_n over $K(a_1, \ldots, a_n)$. Then Hilbert's Irreducibility Theorem 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. 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 $n > 5$. (For more detail, see the discussion in Section 1.6.1.)

1.3. Lattices and Minkowski's Theorems

In this section we briefly discuss the classical theory of lattices and Minkowski's Theorems in number theory. The discussion of this material is primarily adapted from Siegel [35], Neukirch [30], and Narkiewicz [29].

A lattice Γ in $\mathbb{R}^n$ is a discrete subgroup of $\mathbb{R}^n$; equivalently, $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$ for some linearly independent vectors $v_1, \cdots, v_m$. We will primarily be interested in lattices of the maximal rank n – in such a case, we say that the fundamental domain of this

lattice is the set $\Phi = \{x_1\nu_1 + \cdots + x_n\nu_n : 0 \leq x_i < 1\}$. By basic linear algebra, we have $\mathrm{covol}(\Gamma) = \mathrm{vol}(\Phi) = \det(A)$, where A is the base-change matrix from the standard basis of $\mathbb{R}^n$ to $\nu_1, \cdots, \nu_n$.

We take for granted the following theorem of Minkowski, whose proof is nothing more than a geometric version of the pigeonhole principle:

Theorem 1.4. *(Minkowski's First Theorem) If Γ is a lattice of rank n in $\mathbb{R}^n$ and X is a centrally symmetric, convex set such that $\mathrm{vol}(X) > 2^n\mathrm{covol}(\Gamma)$, then X contains at least one nonzero element of Γ.*

Now let K be a number field of degree n over $\mathbb{Q}$ having r real embeddings $\rho_1, \ldots, \rho_r : K \to \mathbb{R}$ and s complex embeddings $\sigma_1, \bar{\sigma}_1, \ldots, \sigma_s, \bar{\sigma}_s$ (where $r + 2s = n$). For $\alpha \in K$, we then define the injective map $\varphi : K \to \mathbb{R}^n = \mathbb{R}^{r+2s}$ by sending

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

We will note here that some authors choose to omit the factors of $\sqrt{2}$ (and thus, the canonical measure on this space differs from the Lebesgue measure on $\mathbb{R}^n$ by a factor of 2^s). If φ' is the map that lacks the factors of the $\sqrt{2}$ on the complex-embedding terms, then it is straightforward to see that φ' is the natural map embedding K into $K \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^n$. (In the main body of the thesis, these differences are essentially irrelevant.)

Since $\mathcal{O}_K$ has an integral basis, we see that the image of the ring of integers $\mathcal{O}_K$ under φ is a lattice of rank n whose covolume is $2^s\,|D_K|^{1/2}$ (this is merely a rewriting of the definition of the discriminant). We refer to the image $\varphi(\mathcal{O}_K) \subset \mathbb{R}^n$ as the Minkowski lattice of K.

By considering the convex bounded set in $\mathbb{R}^n$ defined by the condition

$$\sum_{i=1}^{r} |\rho_i(\alpha)| + 2\sum_{j=1}^{s} |\sigma_j(\alpha)| \leq t$$

for an appropriate t, and applying Minkowski's First Theorem to the lattice $\varphi(M)$ for any finite-index module M in $\mathscr{O}_K$, we can deduce the following result often referred to as the "Minkowski bound" [28]:

Theorem 1.5. *(Minkowski) If M is a $\mathbb{Z}$-module of finite index in $\mathscr{O}_K$, then there is a nonzero $a \in M$ such that*

$$\left|\mathrm{Nm}_{K/\mathbb{Q}}(a)\right| \leq [\mathscr{O}_K : M] \cdot \left(\frac{4}{\pi}\right)^s \left(\frac{n!}{n^n}\right) \left|d_{K/\mathbb{Q}}\right|^{1/2}.$$

A pleasant application of the Minkowski bound is to prove the finiteness of the class group of K; however, this is not our goal here. If we apply the Minkowski bound to $M = \mathscr{O}_K$, then since an element of $\mathscr{O}_K$ has norm at least 1, Stirling's formula yields the lower bound

$$\left|d_{K/\mathbb{Q}}\right| \geq \left(\frac{\pi}{4}\right)^{2s} \left(\frac{n^n}{n!}\right) \geq \left(\frac{11}{12}\right)^2 \left(\frac{\pi e^2}{4}\right)^n \frac{1}{2\pi n},$$

which is clearly increasing for positive integers n. By constructing appropriate convex bounded sets in $\mathbb{R}^n$ (see Theorem 2.24 of [29]), one can show that for fixed r, s, n there is an upper bound on the archimedean norms on a generator of such an extension. This yields the following result of Hermite [19]:

Theorem 1.6. *(Hermite) Up to isomorphism, only finitely many number fields have any fixed discriminant D.*

Hermite's Theorem demonstrates the well-posedness of all of the counting problems discussed in the main body of the thesis. We now turn our attention to Minkowski's Second Theorem, which requires a brief discussion of gauge functions.

Recall that a convex body is an open, bounded, convex region in $\mathbb{R}^n$. Given a convex body B containing the origin, we define its gauge function $f : \mathbb{R}^n \to [0, \infty)$ as follows:

1. If $x \in \partial B$ then $f(x) = 1$.
2. For all scalars $\mu > 0$ and $x \in \mathbb{R}^n$, it is true that $f(\mu x) = \mu f(x)$.

An equivalent way of writing the second criterion is: for any nonzero x, draw the ray from the origin to x. Since B is a convex body containing 0, this ray intersects ∂B exactly once, at some point y. Then for the λ with $x = \lambda y$, we set $f(x) = \lambda$. This also makes it clear that f is well-defined. If f is even, then B is (clearly) symmetric about the origin.

For f an even gauge function on $\mathbb{R}^n$, let B denote the convex body $\{x : f(x) < 1\}$ – which we call the convex body of f – and for $\lambda > 0$ let λB be the stretched set $\{x : f(x) < \lambda\}$, which is just the region B scaled about the origin by a factor of λ.

If Λ is a rank-n lattice in $\mathbb{R}^n$, then if we consider the intersection $\Lambda \cap \lambda B$ as λ varies, for small λ the intersection will only be the origin, and as λ increases we will start including other points of Λ. This motivates the definition of the <u>successive minima</u> of an even gauge function f, which are constructed as follows: μ_1 is the minimum value of $f(x)$ over all nonzero $x \in \Lambda$. If μ_1 is attained at the vector x_1 then define μ_2 to be the minimum value of $f(x)$ over all $x \in \Lambda$ linearly independent from x_1. We continue in this way, defining μ_k for $2 \leq k \leq n$ to be the minimum of f over the points in Λ linearly independent from $\text{span}(x_1, \cdots, x_{k-1})$.

We may now state Minkowski's Second Theorem:

Theorem 1.7. *(Minkowski's Second Theorem) If $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_n$ are the successive minima of the even gauge function f on the lattice Λ, and V is the volume of the convex body of f, then $V \cdot \mu_1 \mu_2 \cdots \mu_n \leq 2^n \, \text{covol}(\Lambda)$.*

The idea of the proof is to apply a transformation to the region B that makes the successive minima all equal to one another, and then to invoke Minkowski's First Theorem.

Our primary interest is, naturally, to apply this Theorem in the setting where the lattice Λ is the image of the ring of integers of a number field. Roughly speaking, the successive minima and Minkowski's Second Theorem in this setting provide us with tools to analyze collections of elements in the extension $K/\mathbb{Q}$, rather than only the single element produced by Minkowski's First Theorem.

1.4. Invariant Theory

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 $\mathbb{C}[x_1, \cdots, x_n]$ via ρ. If $f_1, \cdots, f_n$ are algebraically independent, homogeneous elements of $\mathbb{C}[x_1, \cdots, x_n]$ with the property that $\mathbb{C}[x_1, \cdots, x_n]^G$, the ring of G-invariant polynomials, is a finitely-generated module over $\mathbb{C}[f_1, \cdots, f_n]$, 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, and we will arrange them in nondecreasing order of degree. However, all results discussed will hold for any set of primary invariants.

Denote $A = \mathbb{C}[f_1, \cdots, f_n]$, and $R = \mathbb{C}[x_1, \cdots, x_n]^G$. The theorem of Hochster-Roberts (see Theorem 2.5.5 of [15]) implies that R is a Cohen-Macaulay ring and, moreover, that there exist homogeneous G-invariant polynomials $g_1, g_2, \cdots, g_k$ 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 1.8. Let $G = S_n$ and ρ be the regular representation of G (which acts by index permutation on $\mathbb{C}[x_1, \cdots, x_n]$). It is easy to see that the elementary symmetric polynomials are invariants under the action of G on $\mathbb{C}[x_1, \cdots, x_n]$, 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 $\mathbb{C}[x_1, \cdots, x_n]$ 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 1.9. For $A = \mathbb{C}[f_1, \cdots, f_d]$, one has $H(A, t) = \prod_{i=1}^{n} (1 - t^{\deg(f_i)})^{-1}$ by the algebraic independence of the f_i.

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

$$H(R,t) = \frac{1}{|G|}\sum_{g\in G} \frac{1}{\det(I - t\rho(g))}. \tag{1.4.1}$$

(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 1.4.1, we can write

$$H(R,t) = \frac{1}{|G|}\sum_{g\in G} \frac{1}{\det(I - t\rho(g))} = \frac{\sum_{j=1}^{k} t^{\deg(g_i)}}{\prod_{i=1}^{n}(1 - t^{\deg(f_i)})}. \tag{1.4.2}$$

By examining the Hilbert series identity 1.4.2 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 isn't 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.

1.5. Goals

The overarching goal of this thesis is to generalize the results of Schmidt and Ellenberg-Venkatesh to arbitrary G-extensions. The central theorem of Chapter 2, generalizing Example 2.7 of [18], is the following:

Theorem 2.4. 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 least 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 $\deg(f_i) \leq i$.

One way of reinterpreting Theorem 2.4 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 a lattice attached to an arbitrary faithful representation ρ? The central goal of Chapter 3 is to show that the answer to this question is "yes", to construct a new counting function $N_{K,n}(X;\rho)$ associated to ρ, and then to prove the following theorem:

Theorem 3.10. Let K be any number field, G be a finite group of order n, and $\rho : G \to GL_d(\mathscr{O}_K)$ be a faithful d-dimensional representation of G on $\mathscr{O}_K$. Also define $t(\rho)$ to be the smallest positive integer such that for any nontrivial subgroup H of G, $(\mathscr{O}_K^d)^{\rho(H)}$ has rank $\leq t(\rho)$ as an $\mathscr{O}_K$-module. Then

$$N_{K,n}(X;\rho) \ll X^{\frac{1}{2(d-t(\rho))}\left[\sum_{i=1}^{d} \deg(f_i)\right]},$$

where the f_i for $1 \leq i \leq d$ are a set of primary invariants for ρ. Furthermore, if ρ has a nontrivial secondary invariant, then we can replace the upper bound by $X^{\frac{1}{2(d-t(\rho))}\left[\sum_{i=1}^{d} \deg(f_i) - \frac{\deg(f_1)}{2[K:\mathbb{Q}]}\right]+\epsilon}$.

Finally, in Chapter 4, we briefly discuss a number of open problems that are related to our results.

1.6. Detailed Outline of Prior Results

The goal of this section is to discuss in more detail the central results outlined in Section 1.2. Our intent is to contrast the methods and techniques with one another, and to put the results of Chapters 2 and 3 in a historical context. Much of our treatment here is drawn from the expository portions of the papers being discussed.

1.6.1. Conjectural Results: Malle, Kluners

To state the full version of Malle's conjecture, we first need a few definitions.

For G a transitive subgroup acting on $\Omega = \{1, 2, \cdots, n\}$, 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 of the lengths of all the cycles, minus the number of cycles, in the cycle decomposition of g in S_n. Next we 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. Since S_n contains transpositions, we see that $a(S_n) = 1$. If n is prime then it is a standard exercise that the only transitive subgroup G containing a transposition is S_n itself. If $n = d_1 d_2$ is composite, then the subgroup $G = S_{d_1} \wr S_{d_2}$ is a proper subgroup of S_n which contains a transposition and hence has $a(H) = 1$. (We note in particular that the group $S_2 \wr S_2$ is simply the dihedral group of order 8.)

Note that 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 1.10. *(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 $a(G) = \dfrac{1}{\mathrm{ind}(G)}$ *and* $b(K, G) = \#\{C : C \text{ a } K\text{-conjugacy class of minimal index } \mathrm{ind}(G)\}$.

Remark 1.11. We would expect by Linnik's conjecture 1.2.1 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 [27]) 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 [39]. However, Klüners [22] 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 Turkelli [37], which appears to avoid all of the known counterexamples. Turkelli'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. Turkelli 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.

1.6.2. Abelian, Solvable, and Nilpotent Extensions

The goal of this section is to briefly discuss techniques for counting G-extensions in the cases where G is solvable or nilpotent, using the simple case when $n = 2$ as a starting point. This general type of approach is the one used by Wright [39] for general abelian extensions, Baily [1] and Cohen et al. [8, 9] for degree-4 extensions, and Klüners-Malle [25, 24] for nilpotent extensions and wreath products thereof. Our discussion primarily follows the treatment in Cohen's paper [8].

In the sequel, whenever we write $\zeta_K(1)$, we intend this to mean the residue at $s = 1$.

If $n = 2$, the extension is trivially Galois with Galois group C_2, and is of the form $L = K(\sqrt{D})$ where D is a nonsquare element of $\mathcal{O}_K$. The fact that the growth rate of $N_{\mathbb{Q},2}(X; C_2)$ is on the order of X^1 follows immediately, and it is only somewhat harder to compute the constant on the first term, though obtaining a strong bound on the error term is more difficult. The result over a general number field K is

$$N_{K,2}(X; C_2) = \frac{1}{2^{r_2}} \cdot \frac{\zeta_K(1)}{\zeta_K(2)} \cdot X + O(X^{\alpha}),$$

where K has signature (r_1, r_2) and $\alpha < 1$ can be given explicitly depending on $[K : \mathbb{Q}]$; in particular $\alpha = 1/2$ for $K = \mathbb{Q}$ is known, and by assuming the generalized Riemann hypothesis this value can be lowered further. The answer over $K = \mathbb{Q}$ (where the leading coefficient is $\frac{1}{\zeta(2)}$) can be obtained using a standard counting argument, since the question reduces to counting squarefree integers.

At this point, it is worthwhile summarizing Cohen's argument for why class field theory does not immediately give the answer in this case (which one might assume given the purview of that subject): a direct application of class field theory does yield an exact

formula

$$N_{K,2}(X; C_2) = -1 + \sum_{\mathrm{Nm}(\mathfrak{a}) \leq X} 2^{\mathrm{rank}_2(\mathrm{Cl}_{\mathfrak{a}}^+(K))} M_K\left(\frac{X}{\mathrm{Nm}(\mathfrak{a})}\right), \tag{1.6.1}$$

where $\mathrm{Cl}_{\mathfrak{a}}^+(K)$ denotes the narrow ray class group modulo $\mathfrak{a}$, $\mathrm{rank}_2(\cdot)$ denotes the 2-rank of the given abelian group, and $M_K(n)$ is the number-field version of the summation $M(n)$ of the Möbius function. The derivation of this formula stems from the observation that if $\mathfrak{a}$ is the conductor of the quadratic extension L/K, then L is isomorphic to the fixed field of a ray class field by an index-2 subgroup of the ray class group. Then one is reduced to counting the number of possibilities for each of these objects, and subtracting duplicates.

Although the formula 1.6.1 is completely explicit, and all of the quantities are effectively computable, it is quite difficult to use this formula for asymptotic estimation. As is plain, in order to study the asymptotics as $X \to \infty$, one needs to know (i) information about the 2-rank of narrow ray class groups, and (ii) information about the summatory Möbius function. Although one can glean some information about the ray class groups, it is harder to give a good bound on the growth rate of $M_K(n)$ – indeed, the statement that the growth rate of $M_K(n)$ is on the order of $X^{1/2}$ is equivalent to the Riemann hypothesis! (Thus making it rather inadvisable as a starting point.)

The classical starting point for the Kummer theory / class field theory approach is to introduce the Dirichlet series

$$\Phi_{K,n}(s; G) = \sum_{L/K \cong G} \left[\mathrm{Nm}_{K/\mathbb{Q}}(\mathscr{D}_{L/K})\right]^{-s},$$

where the sum is over all G-extensions L/K of degree n. Then the goal is to study the analytic continuation and poles of this function, and use a Tauberian theorem to extract information about the growth rate of $N_{K,n}(X; G)$.

Wright [39] applies this technique, and then invokes the conductor-discriminant relation to convert the problem into one of analyzing a number of related L-series, which is in turn converted to a local problem. The end result is that the asymptotic constant of the leading term can be written as a sum of Euler products, although the actual computation of the value requires a significant additional effort.

Cohen et al. [8, 9] study carefully the case $n = 2$ and obtain an efficiently computable formula for $\Phi_{K,2}(s; C_2)$, which then allows them (after additional work) to analyze the cases of degree-4 extensions L/K whose Galois closure is obtained as a tower of quadratic extensions – namely, $G = C_4$, V_4, and D_4. A similar, though less technical, method is used in the earlier work of Baily [1], who counts the number of quadratic ray class characters after building an A_4-extension from a cubic extension. A typical example of these results, given in Section 2.3 of [8], is as follows:

Theorem 1.12. *(Cohen et al.) For a general base field* K*,*

$$N_{K,4}(X; V_4) \sim c_K(V_4) X^{1/2} \log^2 X,$$

with

$$\begin{aligned} C_K(V_4) &= \frac{\zeta_K(1)^3}{48 \cdot 4^{r_2}} \prod_{\mathfrak{p}} \left(1 + \frac{3}{\mathrm{Nm}\,\mathfrak{p}}\right)\left(1 - \frac{1}{\mathrm{Nm}\,\mathfrak{p}}\right)^3, \\ &\quad \cdot \prod_{\mathfrak{p} \mid 2\mathcal{O}_K} \frac{1 + \frac{4}{\mathrm{Nm}\,\mathfrak{p}} + \frac{2}{\mathrm{Nm}\,\mathfrak{p}^2} + \frac{1}{\mathrm{Nm}\,\mathfrak{p}^3} - \frac{(1 - \mathrm{Nm}\,\mathfrak{p}^2)e(\mathfrak{p}) + (1 + 1/\mathrm{Nm}\,\mathfrak{p})^2}{\mathrm{Nm}\,\mathfrak{p}^{e(\mathfrak{p})+1}}}{1 + 3/\mathrm{Nm}\,\mathfrak{p}} \end{aligned}$$

where $e(\mathfrak{p})$ *denotes the absolute ramification index of* $\mathfrak{p}$ *above its corresponding prime in* $\mathbb{Z}$*.*

Klüners-Malle [25] analyze nilpotent extensions in a similar way – namely, by showing that all such extensions can be constructed by solving a central embedding problem and

controlling the additional ramification that occurs. (In other words, by building larger extensions from smaller ones and bounding the growth of the discriminant.) Klüners [24] extends these results to wreath products of the form $C_2 \wr H$ where H is nilpotent by combining the techniques of the prior results for degree-2 extensions and nilpotent extensions (since an extension with Galois group $C_2 \wr H$ is obtained by a quadratic extension of one of Galois group H), using the Dirichlet series approach.

1.6.3. Counting n-ic Rings: Extensions of Degree 3, 4, and 5

The goal of this section is to give a brief overview of the number-field counting techniques that involve counting cubic, quartic, or quintic rings. This general type of approach is the one used by Davenport-Heilbronn [13] for degree-3 S_3 extensions, and Bhargava [3, 5] for degree-4 S_4 and degree-5 S_5 extensions. These approaches typically deal with only the base field $K = \mathbb{Q}$, although they are expected to extend to general base fields K – this extension has been done by Datskovsky-Wright [12] in degree 3, by Yukie in degree 4, and by Kable-Yukie [21] in degree 5 (although in this last case, only a slightly weaker result was obtained).

The starting point for counting degree-3 S_3-extensions is the observation that the ring of integers of such a field is a cubic ring (a commutative ring with 1 that is a free rank-3 $\mathbb{Z}$-module) – and in fact is a maximal cubic ring (a cubic ring that is not contained in any other cubic ring). The so-called Delone-Faddeev correspondence [14] relates cubic rings to equivalence classes of binary cubic forms:

Theorem 1.13. *(Delone-Faddeev) There is a natural bijection between the set of* $GL_2(\mathbb{Z})$*-equivalence classes of integral binary cubic forms and the set of isomorphism classes of*

cubic rings.

The bijection underlying this theorem, as related in an especially simple manner in the paper of Bhargava-Shankar-Tsimerman [6], can be made entirely concrete: if $\langle 1, \omega, \theta \rangle$ is an integral basis for the cubic ring R where $w\theta$ is chosen to be in $\mathbb{Z}$ (by an appropriate change of variables), then specifying the multiplication in the ring is equivalent to giving constants $a, b, c, d, l, m, n \in \mathbb{Z}$ such that

$$\begin{aligned} \omega\theta &= n \\ \omega^2 &= m - b\omega + a\theta \\ \theta^2 &= l - d\omega + c\theta. \end{aligned}$$

where the associativity of multiplication (e.g., $(\omega\theta)\theta = \omega(\theta^2)$ and so forth) also fixes n, m, l in terms of the free parameters a, b, c, d. Then the associated binary cubic form is defined to be $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$. It is then essentially straightforward to write down the inverse map sending a binary cubic form to a cubic ring, and to verify that the possible changes of coordinates on each side correspond precisely with taking cubic forms up to $GL_2(\mathbb{Z})$-equivalence.

The association $f \leftrightarrow R$ has a number of extremely useful properties. For example, it preserves the discriminant (where the natural definition of discriminant of a cubic ring R is the determinant of the trace pairing $\mathrm{tr}(\alpha\beta)$ on R). Also, R is an integral domain if and only if f is irreducible (over $\mathbb{Q}$).

So, in order to count degree-3 S_3-extensions of bounded discriminant, it is enough to analyze maximal cubic rings of bounded discriminant. Now the observation to make is that the question of whether a given cubic ring R is maximal is equivalent to whether $R_p = R \otimes \mathbb{Z}_p$ is maximal for every prime p. As shown originally by Davenport-Heilbronn

and simplified by Bhargava-Shankar-Tsimerman, the question of local maximality turns out to have a nice answer:

Theorem 1.14. *(Davenport-Heilbronn) The cubic ring* $R(f)$ *fails to be maximal at* p *if and only if its associated cubic form* $f = ax^3 + bx^2y + cxy^2 + dy^3$ *is either a multiple of* p*, or there exists some* $GL_2(\mathbb{Z})$ *transformation such that* a *is a multiple of* p^2 *and* b *is a multiple of* p*.*

The procedure for computing the desired count of degree-3 S_3-extensions is now as follows: first, count lattice points in the fundamental region for the action of $GL_2(\mathbb{Z})$ bounded by $|\mathrm{Disc}(\alpha)| < X$, excluding the points corresponding to reducible rings. Then, exclude the non-maximal orders via the local maximality conditions using a sieving procedure.

Bhargava-Shankar-Tsimerman improve on this procedure in a number of ways to show the existence of a second main term (the existence and form of which was originally conjectured by Roberts [31] following numerical and theoretical calculations). For example, instead of counting points in a single fundamental domain, they average over a range of fundamental domains. The second main term arises from the geometry of the cusps of the fundamental regions, which they also analyze in a deeper way. They also develop stronger sieving methods to preserve the second-order terms even after sieving to incorporate the local maximality conditions. The overall result is the following:

Theorem 1.15. *(Bhargava-Shankar-Tsimerman) The number of cubic fields, up to isomorphism, is*

$$N_{\mathbb{Q},3}(X; S_3) = \frac{1}{3\zeta(3)}X + \frac{4(1+\sqrt{3})\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O_\epsilon(X^{5/6-1/48+\epsilon}). \tag{1.6.2}$$

We also note here that the result 1.6.2, though with a different error bound, was obtained independently by Taniguchi-Thorne [36] using quite different methods involving Shintani zeta functions.

For degree-3 extensions of a general number field, the computation of the growth rate and asymptotic constant is due to Datskovsky-Wright [12], and also relies on the theory of Shintani zeta functions:

Theorem 1.16. *(Datskovsky-Wright) For any number field* K *having* r *real embeddings and* $2s$ *complex embeddings,*

$$N_{K,3}(X; S_3) \sim \frac{2^{r-s-1}}{3^{r+s-1}} \cdot \frac{\zeta_K(1)}{\zeta_K(3)} \cdot X,$$

where the notation $\zeta_K(1)$ *means the residue at* 1*.*

Bhargava's work giving the asymptotics of the counting functions for degree-4 [3] and degree-5 [5] extensions of $\mathbb{Q}$ proceeds in the same general vein as the $n = 3$ case above, except with a number of additional technical difficulties. The fundamental starting point for quartic extensions is the elegant parametrization of quartic orders by the 12-dimensional space of pairs of ternary quadratic forms modulo the action of $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ as detailed in [2]: then similar methods to those detailed above for obtaining the second main term in the cubic case are needed to obtain the ultimate asymptotic results. (Of course, this was not easily done!) The result is as follows:

Theorem 1.17. *(Bhargava) The number of* S_4*-quartic extensions satisfies*

$$N_{\mathbb{Q},4}(X; S_4) \sim \frac{5}{24} \prod_p (1 + p^{-2} - p^{-3} - p^{-4}) \cdot X.$$

For quintic extensions, the starting point is the parametrization of isomorphism classes of quintic orders by the 40-dimensional space of 4 alternating bilinear forms in

5 variables, modulo the action of $\mathsf{GL}_4(\mathbb{Z}) \times \mathsf{SL}_5(\mathbb{Z})$, as detailed in [4]. As would be expected, the cusps of this region are even more complicated than in the quartic case!

Theorem 1.18. *(Bhargava) The number of S_5-quintic extensions satisfies*

$$N_{\mathbb{Q},4}(X; S_5) \sim \frac{13}{120} \prod_p (1 + p^{-2} - p^{-4} - p^{-5}) \cdot X.$$

Bhargava's proof also implies that when ordered by discriminant, a density of 100% of quintic extensions have Galois closure S_5. (In particular, this means the criterion in [16] is, unfortunately, applicable to asymptotically 0% of all quintics ordered by discriminant.)

The space of binary cubic forms analyzed in the cubic case, along with the spaces analyzed by Bhargava for the quartic and quintic cases, are all examples of prehomogeneous vector spaces. (A prehomogeneous vector space is a pair (G, V) where G is a reductive group and V is a linear representation of G such that $G_{\mathbb{C}}$ has a Zariski-open orbit on $V_{\mathbb{C}}$.) The collection of prehomogeneous vector spaces has been completely classified by Sato-Kimura [32], and a program to use prehomogeneous vector spaces to study field-counting by analyzing (variants of) Shintani zeta functions was laid out by Wright-Yukie [40]. As explained in the introduction to [3], although this program has met with some success in establishing Malle's weak conjecture in degrees 4 and 5 [21, 41], it must overcome the obstacle that arises because the corresponding Shintani zeta function also includes terms from imprimitive extensions (which in degree 4 are quadratic extensions of quadratic extensions). Such extensions far outnumber primitive extensions, and they cause the zeta function to have higher-order poles which are difficult to remove. The approach of Bhargava avoids this problem by working with integral orbits rather than rational orbits, which allows for discarding the undesirable points at the beginning rather

than at the end.

We will note also that the fundamental use of prehomogeneous vector spaces suggests that these methods will not extend to higher-degree extensions in general, since the classification of the prehomogeneous vector spaces does not appear to be compatible with the structure of the ring of integers of a degree-n extension for $n \geq 6$. (However, it is possible that for particular Galois groups, these techniques may apply in higher degrees.)

1.6.4. General-Degree Extensions

Our starting point for counting general extensions is the following theorem of Schmidt [33]:

Theorem 1.19. *(Schmidt) For all n and all base fields K,*

$$N_{K,n}(X) \ll X^{(n+2)/4}. \tag{1.6.3}$$

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 $\alpha \in \mathscr{O}_L$ 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. Some care is necessary in the above argument: in fact, Schmidt actually counts chains of primitive extensions $K \subset L_1 \subset \cdots \subset L_{t-1} \subset L$ where there are no additional intermediate subfields beyond those listed.

Rather than giving a lengthier discussion of Schmidt's theorem here, we will defer to the discussion in Chapter 2, because Proposition 2.1 contains a significant portion of

Schmidt's result, and Theorem 2.4 yields Schmidt's result as a corollary.

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

Theorem 1.20. *(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 $n = 20$), the result becomes stronger than Schmidt's bound 1.6.3.

By taking logarithms, one may recast Theorem 1.20 as showing that

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

For comparison, Schmidt's result 1.6.3 is that this limit is at most $\frac{n+2}{4}$, while Linnik's conjecture 1.2.1 is that this limit is 1.

The approach of Ellenberg-Venkatesh, in brief, modifies the technique of Schmidt so that instead of counting the number of possibilities for a single element of $\mathscr{O}_L$, they instead count linearly-independent r-tuples of elements of $\mathscr{O}_L$, 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.

On the invariant theory side, this corresponds to finding the invariants of a direct product of copies of the group $G = S_n$, instead of merely the invariants of G itself (which are simply the symmetric polynomials). Furthermore, Ellenberg-Venkatesh do not take

the full set of invariants; rather, they take a sufficiently large number of low-degree invariants so as to ensure that an appropriate scheme map is generically finite – the main portion of their proof is a geometric lemma ensuring generic finiteness.

In more detail: Let L/K be an extension of degree n and whose relative discriminant norm is less than X. Fix an algebraic closure $\bar{K}$ of K and let $\sigma_1, \cdots, \sigma_n$ be the embeddings of L into $\bar{K}$. Consider $\mathbb{A}^{nr} = (\mathbb{A}^n)^r$ with coordinate functions $x_{j,k}$, $1 \leq j \leq n$, $1 \leq k \leq r$, and let S_n act on $(\mathbb{A}^n)^r$ by index permutation in the first coordinate. The S_n-invariants of this action are called the multisymmetric functions.

Example 1.21. If we take $(\mathbb{A}^3)^2$ with coordinate functions x_1, x_2, x_3 and y_1, y_2, y_3, then the action simply permutes the subscripts: thus $(1\,2)$ applied to $x_2+y_1+y_3$ yields $x_1+y_2+y_3$. Some multisymmetric functions for this action are $x_1x_2x_3$, $(x_1 + x_2 + x_3)(y_1y_2y_3)$, and $x_1y_1 + x_2y_2 + x_3y_3$.

Define the map $\varphi_L : \mathscr{O}_L^r \to \bar{K}^{nr} = \mathbb{A}^{nr}(\bar{K})$ via the r-fold direct sum $\varphi_L = (\sigma_1 \oplus \cdots \oplus \sigma_n)^{\oplus r}$. By obvious properties of algebraic integers, if f is a multisymmetric function with integral coefficients, then the image of anything in $\mathscr{O}_L^r$ under the composition $f \circ \varphi_L : \mathscr{O}_L^r \to \bar{K}$ is actually an algebraic integer, hence it lies in $\mathscr{O}_K$. Therefore, if $R = \mathbb{Z}[f_1, \cdots, f_s]$ is a subring of the ring of multisymmetric functions, for some generators $f_1, \cdots, f_s$, and $A = \mathrm{Spec}(R)$, and L is any number field with $[L : K] = n$, then we get a map from $\mathscr{O}_L^r \to A(\mathscr{O}_K)$.

The strategy is to examine this map carefully and to use its properties to establish a bound on the number of L with $[L : K] = n$ and $\mathrm{Nm}_{K/\mathbb{Q}}(\mathscr{D}_{L/K}) < X$. Explicitly: let $\|x\|$ be the maximum of the archimedean absolute values of x, fix a positive real number Y, and let $B(Y)$ be the set of algebraic integers x in $\bar{K}$ of degree n over K and with $\|x\| < Y$. Then there is a constant c such that $\|f_i(\varphi_L(\alpha_1, \cdots, \alpha_r))\| < c\, Y^{\deg(f_i)}$ provided

that $\alpha_i \in B(Y)$. (That such a c exists is clear: by the triangle inequality, it is bounded above by the sum of the coefficients of f_i.)

Let $A(\mathscr{O}_K)_Y$ be the points P in $A(\mathscr{O}_K)$ such that $\|f_i(P)\| < c\, Y^{\deg(f_i)}$ for each i. For any subset S_Y of $B(Y)^r$ we have set maps

$$\begin{array}{ccc} \left\{(L, \alpha_1, \cdots, \alpha_r) : [L:K] = n,\, \mathrm{Nm}_{K/\mathbb{Q}}(\mathscr{D}_{L/K}) < X,\, (\alpha_1, \cdots, \alpha_r) \in (\mathscr{O}_L)^r \cap S_Y\right\} & \to & A(\mathscr{O}_K)_Y \\ \downarrow & & \\ \left\{L : [L:K] = n,\, d_{L/K} < X\right\} & & \end{array}$$

The goal is to bound the number of elements in the bottom set. The approach now is to choose the polynomial generators of R, the bound Y, and the set S_Y to make the vertical map surjective, and to make the horizontal map have finite fibers whose cardinality is bounded above by a computable constant. Then the cardinality of the bottom set is at most the number of $\mathscr{O}_K$-points on A all of whose valuations are bounded above by Y, times the size of the fibers of the horizontal map.

Chapter 2

The Classical Discriminant

2.1. Overview

Recall that we have defined $N_{K,n}(X;G)$ 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 $\mathrm{Nm}_{K/\mathbb{Q}}(\mathscr{D}_{L/K}) < X$, 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.

and that we refer to such extensions as G-extensions, and to G as the "Galois group" of the extension L/K, despite the fact that this extension is not typically Galois.

The goal of this chapter is to prove the following theorem:

Theorem 2.4. Let $n \geq 2$, let K be any number field, and let G be a proper transitive subgroup of S_n. Then for any $\epsilon > 0$,

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

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

The proof appears in Section 2.2, and the remaining sections are devoted to tabulating and discussing a number of corollaries.

We believe it worthwhile to note here that for every primitive group covered by the Theorem, the result is always strictly better than Schmidt's bound $N_{K,n}(X) \ll X^{(n+2)/4}$ [33], and the savings (see section 2.3) 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 2.1 is to accomplish (1). We modify the basic argument in (2) by rephrasing the counting argument in scheme-theoretic language, and then invoke the theory of polynomial invariants and the large sieve (see Lemma 2.2) to save in the counting part.

2.2. Proof of Counting Theorem

Proposition 2.1. *Let K be a number field of degree l over $\mathbb{Q}$, and L/K an extension of degree n such that $\mathrm{Nm}_{K/\mathbb{Q}}(\mathscr{D}_{L/K}) < X$, and such that any proper subfield K' of L containing K has $[K' : K] \leq t$. Then there exists an $\alpha \in \mathscr{O}_L$ 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. Recall that 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

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

Also recall that the image $\Lambda_L = \varphi_L(\mathscr{O}_L)$ is the Minkowski lattice of rank nl in $\mathbb{R}^{nl}$. (See Section 1.3 for additional background and terminology.)

Let $\beta_1, \cdots, \beta_{nl}$ be the successive minima of the gauge function $f(x_1, \cdots, x_{nl}) = \max(x_1, \ldots, x_{nl})$ 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.) Minkowski's Second Theorem says

$$\prod_{i=1}^{nl} \|\beta_i\| \ll |D_L|^{1/2}, \tag{2.2.1}$$

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 2.2.1 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

$$\|\beta_k\| \ll D_L^{1/2(nl+1-k)}. \tag{2.2.2}$$

For all k with $1 \leq k \leq t + 1$, 2.2.2 implies

$$\|\beta_k\| \ll D_L^{1/2l(n-t)} \ll X^{1/2l(n-t)}. \tag{2.2.3}$$

Now, by our assumption about intermediate subfields, we know that $S = \{\beta_1, \cdots, \beta_{t+1}\}$ 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 sub(L/K) that generates L/K.

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

$$\|\alpha\| \ll X^{1/2l(n-t)}. \tag{2.2.4}$$

□

We also require a sieving lemma:

Lemma 2.2. *Suppose $\Pi : Z \mapsto \mathbb{A}^d(\mathbb{Q})$ 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 $(X^{a_1}, X^{a_2}, \cdots, X^{a_d})$ 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 [10]: 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 $X(\mathbb{Q})$ 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 $(X^{a_1}, X^{a_2}, \cdots, X^{a_d})$ with square boxes each of which has size $(X^{a_1}, X^{a_1}, \cdots, X^{a_1})$: 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 is immediate. □

Remark 2.3. Following page 6 of [34], the principle of Cohen's proof can be seen from an example: consider the case $z^2 = f(x_1, \cdots, x_n)$ where $f \in \mathbb{Z}[x_1, \cdots, x_n]$ is squarefree. The goal is to bound the number of points S_N of $x_i \in \mathbb{Z}^n$ such that $|x_i| \leq N$ and $f(x)$ is a square. Since $z^2 - f$ is absolutely irreducible mod p for almost all p, a theorem of Lang-Weil says that the number of points on the variety mod p is $p^n + O(p^{n-1/2})$ as $p \to \infty$. Since z and $-z$ give the same point, the reduction of S_N modulo p has $\ll (\frac{1}{2} + \epsilon)p^n$ points. This excludes about half of the residue classes modulo p, and allows for an application of the large sieve, yielding the result.

We can now prove our main theorem:

Theorem 2.4. *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 least t. Then for any $\epsilon > 0$,*

$$N_{K,n}(X; G) \ll X^{\frac{1}{2(n-t)}\left[\sum_{i=1}^{n-1} \deg(f_{i+1}) - \frac{1}{[K:\mathbb{Q}]}\right] + \epsilon}, \tag{2.2.5}$$

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 2.5. The condition about the point stabilizer is (by the Galois correspondence) equivalent to the following: if L/K is a G-extension, then any field K' intermediate

between K and L 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 we can take $t = 1$.

Proof. Let G act on the polynomial ring $\mathbb{C}[x_1, \cdots, x_n]$ by index permutation, and let $f_1, \cdots, f_n$ be primary invariants (cf. Section 1.4) of G with associated secondary invariants $1 = g_1, g_2, \cdots, g_k$, 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 $A = \mathbb{C}[f_1, \cdots, f_n]$ and $R = \mathbb{C}[x_1, \cdots, x_n]^G$, and observe that $\bar{R} = R/f_1R$ is an integral domain. Let S be the subring of $\bar{R}$ generated by $\bar{f_2}, \cdots, \bar{f_n}$ and $\bar{g}_2$, and let $Z = \mathrm{Spec}(S)$. S is a domain (since $\bar{R}$ is) so Z is irreducible.

The natural map $\mathbb{C}[f_2, \cdots, f_n] \to S$ induces a projection $\Pi : Z \to \mathbb{A}^{n-1}$, and the map Π is finite because R is a finitely-generated A-module (whence $\bar{R}$ is finite over $\mathbb{C}[f_2, \cdots, f_n]$). Finally, observe that $\bar{g}_2 \notin \mathbb{C}[\bar{f_2}, \cdots, \bar{f_n}]$ (by definition, since R is not A), 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 $\mathrm{Nm}_{K/\mathbb{Q}}(\mathscr{D}_{L/K}) < X$. As noted in Remark 2.5, the condition on the group G implies that any field K' intermediate between K and L has $[K' : K] \leq t$. By Proposition 2.1, there exists a nonzero element $\alpha \in \mathscr{O}_L$ 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 x 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, 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 $\Pi(\mathbf{x}) = (y_2, \cdots, y_n)$ 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 $\mathscr{O}_K$, this box becomes a box in $\mathbb{A}^{nl}(\mathbb{Q})$ with the same bounds (up to fixed constants), each occurring l times, and the image of $\Pi(\mathbf{x})$ is integral. We now apply Lemma 2.2 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

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

which is precisely the desired result. □

Remark 2.6. Note that we require the existence of a secondary invariant in order to apply Lemma 2.2. Without a secondary invariant, we lose the power savings and instead obtain the upper bound $\ll X^{\frac{1}{2(n-t)}\left[\sum_{i=1}^{n-1}\deg(f_{i+1})\right]}$. This will only occur when $G = S_n$, whose primary invariants are the usual symmetric polynomials (with degrees $2, 3, \cdots, n$): it is then easy to see that our upper bound is

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

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.

We would naturally expect the actual number of integral points to be lower than the bound 2.2.5, per Malle's heuristics (cf. section 1.6.1). There are three ways in which we lose accuracy:

1. The map associating an element 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, but we do not expect that the sieving lemma 2.2 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 2.1 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 2.4 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 x of trace zero and whose archimedean valuations are small, we could instead count the number of possibilities for an r-tuple of elements $(x_1, \cdots, x_r)$, 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, we would need to understand 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 – for an example, see the discussion in Section 2.4. However, for large n (certainly, $n > 15$) this seems very unlikely to succeed, since the invariant theory becomes extremely computationally demanding at roughly $n = 10$.

To deal with the deficiencies of (3), it seems likely that a more direct analysis of the possible extension towers using the techniques described in Section 1.6 for extensions of small degree over general base fields would yield significant savings.

2.3. 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 2.4

is significantly better than Schmidt, although the results generally do not get close to X^1, let alone to the bounds in Malle's Conjecture 1.3. 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 [11]. Subfield information was obtained from John Jones' page on transitive group data [20], which also contains additional detailed information about the transitive subgroups.

For brevity in the tables below, we quote the results of Theorem 2.4 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 dihedral groups, there are easy bounds available 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
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							
#	Order	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							
#	Ord	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 1-10 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}	$X^{1/3}$	$X^{5/2}$
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	$X^{9/4}$	$X^{1/2}$	$X^{5/2}$

Proper transitive subgroups 11-30 of S_8							
#	Order	Isom. to	Subfield?	Invariant Degrees	Result	Malle	Schmidt
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	$X^{1/2}$	$X^{5/2}$

Proper transitive subgroups 31-49 of S_8							
#	Order	Isom. to	Subfield?	Invariant Degrees	Result	Malle	Schmidt
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	$2^6 3^1 7$	$AL(8)$	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	$X^{1/3}$	$X^{11/4}$

2.4. A Prototypical Example: $\mathsf{PSL}_2(\mathbb{F}_7)$ in S_7

In this section we give an explicit example of a primary invariant computation, for the group $G = \mathsf{PSL}_2(\mathbb{F}_7) \cong \mathsf{GL}_3(\mathbb{F}_2)$, which is the simple group of order 168, and appears as 7T5 in the table above.

Corollary 2.7. *For any* $\epsilon > 0$,

$$N_{\mathbb{Q},7}(X; G) \ll X^{11/6+\epsilon}.$$

For comparison, Schmidt's bound (for general septic 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 $\mathsf{PSL}_2(\mathbb{F}_7)$ on $\mathbb{P}^1(\mathbb{F}_7)$. A computation with MAGMA shows that primary invariants can be chosen as

$$
\begin{aligned}
f_1 &= x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 \\
f_2 &= x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 \\
f_3 &= x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 + x_6^3 + x_7^3 \\
f_4 &= x_1x_2x_3 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_4 + x_1x_3x_6 + x_1x_3x_7 + x_1x_4x_5 \\
&\quad + x_1x_4x_6 + x_1x_4x_7 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_4 + x_2x_3x_5 + x_2x_3x_7 + x_2x_4x_5 \\
&\quad + x_2x_4x_6 + x_2x_4x_7 + x_2x_5x_6 + x_2x_6x_7 + x_3x_4x_5 + x_3x_4x_6 + x_3x_5x_6 + x_3x_5x_7 \\
&\quad + x_3x_6x_7 + x_4x_5x_7 + x_4x_6x_7 + x_5x_6x_7 \\
f_5 &= x_1^4 + x_2^4 + x_3^4 + x_4^4 + x_5^4 + x_6^4 + x_7^4 \\
f_6 &= x_1^2x_2x_3 + x_1^2x_2x_5 + x_1^2x_2x_6 + x_1^2x_2x_7 + x_1^2x_3x_4 + x_1^2x_3x_6 + x_1^2x_3x_7 + x_1^2x_4x_5 \\
&\quad + x_1^2x_4x_6 + x_1^2x_4x_7 + x_1^2x_5x_6 + x_1^2x_5x_7 + x_1x_2^2x_3 + x_1x_2^2x_5 + x_1x_2^2x_6 + x_1x_2^2x_7 \\
&\quad + x_1x_2x_3^2 + x_1x_2x_5^2 + x_1x_2x_6^2 + x_1x_2x_7^2 + x_1x_3^2x_4 + x_1x_3^2x_6 + x_1x_3^2x_7 + x_1x_3x_4^2 \\
&\quad + x_1x_3x_6^2 + x_1x_3x_7^2 + x_1x_4^2x_5 + x_1x_4^2x_6 + x_1x_4^2x_7 + x_1x_4x_5^2 + x_1x_4x_6^2 + x_1x_4x_7^2 \\
&\quad + x_1x_5^2x_6 + x_1x_5^2x_7 + x_1x_5x_6^2 + x_1x_5x_7^2 + x_2^2x_3x_4 + x_2^2x_3x_5 + x_2^2x_3x_7 + x_2^2x_4x_5 \\
&\quad + x_2^2x_4x_6 + x_2^2x_4x_7 + x_2^2x_5x_6 + x_2^2x_6x_7 + x_2x_3^2x_4 + x_2x_3^2x_5 + x_2x_3^2x_7 + x_2x_3x_4^2 \\
&\quad + x_2x_3x_5^2 + x_2x_3x_7^2 + x_2x_4^2x_5 + x_2x_4^2x_6 + x_2x_4^2x_7 + x_2x_4x_5^2 + x_2x_4x_6^2 + x_2x_4x_7^2 \\
&\quad + x_2x_5^2x_6 + x_2x_5x_6^2 + x_2x_6^2x_7 + x_2x_6x_7^2 + x_3^2x_4x_5 + x_3^2x_4x_6 + x_3^2x_5x_6 + x_3^2x_5x_7 \\
&\quad + x_3^2x_6x_7 + x_3x_4^2x_5 + x_3x_4^2x_6 + x_3x_4x_5^2 + x_3x_4x_6^2 + x_3x_5^2x_6 + x_3x_5^2x_7 + x_3x_5x_6^2 \\
&\quad + x_3x_5x_7^2 + x_3x_6^2x_7 + x_3x_6x_7^2 + x_4^2x_5x_7 + x_4^2x_6x_7 + x_4x_5^2x_7 + x_4x_5x_7^2 + x_4x_6^2x_7 \\
&\quad + x_4x_6x_7^2 + x_5^2x_6x_7 + x_5x_6^2x_7 + x_5x_6x_7^2 \\
f_7 &= x_1^7 + x_2^7 + x_3^7 + x_4^7 + x_5^7 + x_6^7 + x_7^7
\end{aligned}
$$

of degrees $1, 2, 3, 3, 4, 4, 7$ respectively. Invoking Theorem 2.4 yields the stated bound. (Note here that $t = 1$.) □

We will note at this juncture that the group $G = \mathrm{PSL}_2(\mathbb{F}_7)$ also appears as a transitive subgroup of S_8 (it is 8T37 in the tables from Section 2.3), 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: 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, underscoring this difference is the fact that Malle's conjecture gives different predictions for these two different counting problems: the number of extensions in the S_7 case is predicted to grow as $X^{1/2}$ (up to some log terms), while the number of extensions in the S_8 case is predicted to grow as $X^{1/4}$ (up to some log terms).

However, this is not to say that these cases are unrelated: given a septic G-extension, one can construct an octic G-extension with the same Galois closure, and vice versa. Explicitly, given a septic G-extension, the fixed field of the normalizer of a Sylow-7 subgroup in G (which is a maximal subgroup of order 21 and unique up to conjugacy) yields a unique (up to isomorphism) octic G-extension with the same Galois closure. Conversely, given a octic G-extension, there exist two unique (up to isomorphism) septic G-extensions with the same Galois closure (given by fixed fields of the two conjugacy classes of maximal subgroups of G of order 24).

We can, indeed, bound the discriminants Δ_7 and Δ_8 of the septic and octic extensions in terms of powers of one another. For $p \neq 2, 3, 7$, the ramification at p is tame and

the image (in G) of the inertia group at p is cyclic: say, generated by $g \in G$. Then the exponent of p dividing Δ_i for $i = 7, 8$ is then equal to the index (as defined in Section 1.6.1) of the element of S_i to which g is sent under the corresponding permutation representation. It is straightforward to see that the only cyclic subgroups of G are order 7, order 4, order 3, and order 2. If $|g| = 7$, then $\rho_7(g)$ and $\rho_8(g)$ are both 7-cycles (index 6). If $|g| = 4$, then $\rho_7(g)$ is a 2,4-cycle (index 4), and $\rho_8(g)$ is a 4,4-cycle (index 6). If $|g| = 3$, then $\rho_7(g)$ and $\rho_8(g)$ are both 3,3-cycles (index 4). And if $|g| = 2$, then $\rho_7(g)$ is a 2,2-cycle (index 2), and $\rho_8(g)$ is a 2,2,2,2-cycle (index 4). Hence, for each prime $p \neq 2, 3, 7$, it is true that

$$1 \leq \frac{\nu_p(\Delta_8)}{\nu_p(\Delta_7)} \leq 2,$$

meaning that for some absolute positive constants c_1 and c_2 (arising from the potential ramification at 2, 3, and 7, which is bounded), we have

$$c_1\Delta_7 \leq \Delta_8 \leq c_2\Delta_7^2.$$

So we see that in this case, Malle's conjecture is essentially saying that, for tamely ramified primes p, the image of inertia at p in G has order 2, for most primes p in most $\mathrm{PSL}_2(\mathbb{F}_7)$-extensions of $\mathbb{Q}$.

Chapter 3

The ρ-Discriminant and Applications

3.1. Overview

In Chapter 2, we used the theory of polynomial invariants to study counting asymptotics for G-extensions. One way of reinterpreting Theorem 2.4 is to view it as a result about permutation representations of groups. The goal of this chapter is to generalize Theorem 2.4 into a setting with arbitrary representations.

In Section 3.2, we motivate the construction of the global tuning submodule and give the construction along with a few examples. We then introduce a new counting metric, the ρ-discriminant, for counting (Galois) extensions, and a corresponding counting function $N_{K,n}(X;\rho)$ with respect to this metric.

In Section 3.3, we prove the generalization of Theorem 2.4 to our new setting:

Theorem 3.10. Let K be any number field, G be a finite group of order n, and $\rho : G \to GL_d(\mathcal{O}_K)$ be a faithful d-dimensional representation of G on $\mathcal{O}_K$. Also define $t(\rho)$ to be the smallest positive integer such that for any nontrivial subgroup H of G, $(\mathcal{O}_K^d)^{\rho(H)}$ has rank $\leq t(\rho)$ as an $\mathcal{O}_K$-module. Then

$$N_{K,n}(X;\rho) \ll X^{\frac{1}{2(d-t(\rho))}\left[\sum_{i=1}^{d} \deg(f_i)\right]},$$

where the f_i for $1 \leq i \leq d$ are a set of primary invariants for ρ. Furthermore,

if ρ has a nontrivial secondary invariant, then we can replace the upper bound by $X^{\frac{1}{2(d-t(\rho))}\left[\sum_{i=1}^{d}\deg(f_i)-\frac{\deg(f_1)}{2[K:\mathbb{Q}]}\right]+\epsilon}$.

Finally, we give a few examples in Section 3.4.

3.2. The Tuning Submodule and ρ-Discriminant

Let $\hat{L}/K$ be a degree-n Galois extension of number fields with Galois group G, and let the respective rings of integers be $\mathscr{O}_{\hat{L}}$ and $\mathscr{O}_K$. Additionally, let $\rho : G \to GL_d(\mathscr{O}_K)$ be a faithful representation of G.

The proof of Theorem 2.4 can be interpreted as follows: first, we construct a generator α of the extension L/K that has small archimedean valuations relative to the discriminant of the extension. Then we compute the primary invariant polynomials $f_1, \cdots, f_n$ for the permutation representation $\rho : G \to S_n \hookrightarrow GL_n(\mathbb{Z})$, and we observe that $f_i(\boldsymbol{x})$ lies in K, where $\boldsymbol{x}$ is the vector of archimedean embeddings of α (on which G acts through ρ and through the Galois action). Next, we use the finiteness of a scheme map originating from invariant theory to conclude that if we fix the values $f_1(\boldsymbol{x}), \ldots, f_n(\boldsymbol{x})$, then there are only a bounded number of possibilities for $\boldsymbol{x}$. Finally, we count the number of possibilities for these invariant values $f_1(\boldsymbol{x}), \ldots, f_n(\boldsymbol{x})$, yielding an upper bound for the number of possible $\boldsymbol{x}$ and in turn the number of possible α, hence (at last) bounding the number of possible L.

We would like to adapt this technique to a setting with a general representation: so suppose, now, that ρ is an arbitrary degree-d representation. The scheme map originating from invariant theory is still finite, and everything following that point in the argument still holds, provided we can construct some vector $\boldsymbol{x} \in \mathscr{O}_{\hat{L}}^{\oplus d}$ with the property

that $f_i(\mathbf{x}) \in K$ for all of the primary invariants f_i. By Galois theory, $f_i(\mathbf{x}) \in K$ if and only if $g \cdot f_i(\mathbf{x}) = f_i(g \cdot \mathbf{x})$ is in K, where $g \in G$ is acting on $\mathbf{x}$ via the Galois action. If we demand that $g \cdot \mathbf{x} = \rho(g)\mathbf{x}$, where we view $\rho(g)$ as acting on $\mathbf{x}$ via the representation action, then since f_i is an invariant polynomial, we would have $g \cdot f_i(\mathbf{x}) = f_i(g \cdot \mathbf{x}) = f_i(\rho(g)\mathbf{x}) = f_i(\mathbf{x})$, which is precisely the outcome we are seeking. (We also observe that in the case that ρ is a permutation representation, the action of ρ on $\mathbf{x}$ is merely rearrangement of the coordinates, and this is precisely the same action as in the proof of Theorem 2.4.)

We will now formalize this idea: there are two natural actions of G on the space

$$\mathscr{O}_{\hat{L}} \otimes_{\mathscr{O}_K} \mathscr{O}_K^{\oplus d} \cong \mathscr{O}_{\hat{L}}^{\oplus d}.$$

First, there is the action δ stemming from the Galois action of G on $\mathscr{O}_{\hat{L}}$ (which acts on the left side in the tensor product and diagonally on each copy of $\mathscr{O}_{\hat{L}}$ in the direct sum): thus,

$$\delta : G \to \mathrm{Aut}_{\mathscr{O}_K}(\mathscr{O}_{\hat{L}})^{\oplus d}. \tag{3.2.1}$$

There is also the action τ obtained by acting in the right component of the tensor product by ρ (which in the direct sum is equivalent to extending the representation ρ from its action on $\mathscr{O}_K$ to an action on $\mathscr{O}_{\hat{L}}$): thus,

$$\tau : G \to \mathrm{GL}_d(\mathscr{O}_K) \hookrightarrow \mathrm{GL}_d(\mathscr{O}_{\hat{L}}). \tag{3.2.2}$$

The object we are interested in, per the argument above, is the subset of elements where these actions agree:

Definition 3.1. *For a given Galois extension $\hat{L}/K$ with Galois group G and a faithful representation $\rho : G \to \mathrm{GL}_d(\mathscr{O}_K)$, we define the tuning submodule Ξ_ρ to be the subset*

of elements of the space $\mathscr{O}_{\hat{L}}^{\oplus d}$ *on which the two actions* δ *and* τ *from 3.2.1 and 3.2.2 coincide; namely,*

$$\Xi_\rho = \left\{ x \in \mathscr{O}_{\hat{L}}^{\oplus d} : \forall g \in G,\, \delta(g)(x) = \tau(g)(x) \right\}. \tag{3.2.3}$$

Lemma 3.2. *(Wood-Yasuda) The tuning submodule* Ξ_ρ *is a torsion-free* $\mathscr{O}_K$*-module of rank* d*.*

Proof. Clearly, Ξ_ρ is torsion-free. (In fact, it is also locally free.) To compute the rank, consider $\Xi_\rho \otimes_{\mathscr{O}_K} \hat{L} \subset \left(\mathscr{O}_{\hat{L}} \otimes_{\mathscr{O}_K} \hat{L}^{\oplus d} \right)$: the action of each $g \in G$ is an isomorphism in the second component, so $\Xi_\rho \otimes_{\mathscr{O}_K} \hat{L}$ is the subset of elements of $\mathscr{O}_{\hat{L}} \otimes_{\mathscr{O}_K} \hat{L}^{\oplus d}$ for which the two induced actions of G coincide. So $\Xi_\rho \otimes_{\mathscr{O}_K} \hat{L} = \left\{ \tau(g)(x)_{g \in G} : x \in \hat{L}^{\oplus d} \right\} \cong \hat{L}^{\oplus d}$, whence the rank of Ξ_ρ as an $\mathscr{O}_K$-module is d. □

Our goal is to use the tuning submodule to construct a vector $\mathbf{x} = (\alpha_1, \cdots, \alpha_d) \in \mathscr{O}_{\hat{L}}^{\oplus d}$ whose archimedean valuations are small. We can embed $\mathscr{O}_{\hat{L}}^{\oplus d}$ into $\mathbb{R}^{dnl}$ via the direct sum $\varphi_{L,d}$ of d copies of the Minkowski map $\varphi_{\hat{L}} : \mathscr{O}_{\hat{L}} \to \mathbb{R}^{nl}$, and this allows us to view the tuning submodule as a lattice; however, one source of difficulty is that $\varphi(\Xi_\rho)$ only has rank dl as a $\mathbb{Z}$-module. To remedy this, we instead work with the natural embedding ψ of Ξ_ρ into $\mathbb{R}^{dl} \cong \Xi_\rho \otimes_{\mathbb{Z}} \mathbb{R}$, in analogy to the interpretation of the Minkowski map $\varphi'_{\hat{L}}$ as embedding $\mathscr{O}_{\hat{L}}$ as a lattice inside $\mathscr{O}_{\hat{L}} \otimes_{\mathbb{Z}} \mathbb{R}$ (cf. Section 1.3).

Definition 3.3. *If* $\hat{L}/K$ *is a Galois extension with Galois group* G*,* $\rho : G \to GL_d(\mathscr{O}_K)$ *is a faithful representation of* G*,* Ξ_ρ *is the tuning submodule attached to* $(\rho, \hat{L}, K)$*, and* $\psi : \Xi_\rho \to \mathbb{R}^{dl} \cong \Xi_\rho \otimes_{\mathbb{Z}} \mathbb{R}$ *is the natural embedding, we define the* ρ*-discriminant* $D_{L/K}^{(\rho)}$ *to be*

$$D_{\hat{L}/K}^{(\rho)} = \mathrm{covol}(\psi(\Xi_\rho))^2.$$

Let us give a few concrete examples of tuning submodules and ρ-discriminants:

Example 3.4. Let $K = \mathbb{Q}$ and $\hat{L} = \mathbb{Q}(\sqrt{D})$ for a squarefree D. Then $G = \mathbb{Z}/2\mathbb{Z}$, so let ρ be the nontrivial 1-dimensional representation of G: then if g is the nonidentity element of G, we see that for $x = a + b\sqrt{D} \in \mathscr{O}_{\hat{L}}$, we have $\delta(g)(x) = a - b\sqrt{D}$, and $\tau(g)(x) = -x = -a - b\sqrt{D}$, which are equal precisely when $a = 0$. Hence we see $\Xi_\rho = \mathbb{Z}\sqrt{D}$, and it is clear that $\psi(\Xi_\rho)$ has covolume $\sqrt{|D|}$ inside $\mathbb{R}$. For this representation, we then see that $D^{(\rho)}_{\hat{L}/\mathbb{Q}} = |D|$. Since the discriminant $D_{\hat{L}}$ of this extension is D or $4D$, depending on whether D is or is not congruent to 1 modulo 4, respectively, we see that the ρ-discriminant and classical discriminant behave similarly, but not identically, for these extensions.

Example 3.5. Let $K = \mathbb{Q}$ and $\hat{L}$ be an arbitrary Galois extension (of degree n) with Galois group G, and take ρ to be the regular representation of G as a subgroup of S_n. Then Ξ_ρ is the set of n-tuples of elements of $\mathscr{O}_{\hat{L}}$ such that the permutation action of G agrees with the Galois action of G. Since G is transitive on the n coordinates, we see that the tuning submodule Ξ_ρ is precisely the set of n-tuples $(\alpha^{(1)}, \cdots, \alpha^{(n)})$ of Galois orbits of elements $\alpha \in \mathscr{O}_L$. When we apply the embedding ψ, we see that the lattice $\psi(\Xi_\rho)$ is the Minkowski lattice (up to factors of $\sqrt{2}$ in the coordinates arising from the complex embeddings), and has covolume $2^s |D_L|^{1/2}$, where s is the number of complex embeddings of $\hat{L}$.

We note in particular that Example 3.5 shows that, up to a bounded constant, for a regular representation ρ over $\mathbb{Q}$, the ρ-discriminant is precisely the same as the classical discriminant. Indeed, the same argument shows that this statement remains true for general extensions $\hat{L}/K$, provided we replace D_L with the absolute discriminant norm

$\mathrm{Nm}_{K/\mathbb{Q}}(\mathscr{D}_{L/K})$.

We can now form a counting function using the ρ-discriminant:

Definition 3.6. *We define* $N_{K,n}(X;\rho)$ *to be the number of number fields* $\hat{L}$ *(up to* K*-isomorphism) such that*

1. The degree $[\hat{L} : K] = n$,
2. The Galois group $\mathrm{Gal}(\hat{L}/K) = G$, and $\rho : G \to \mathrm{GL}_d(\mathscr{O}_K)$ is a faithful representation of G, and
3. The ρ-discriminant $D^{(\rho)}_{\hat{L}/K}$ is less than X.

It may initially appear that the ordering associated to $N_{K,n}(X;\rho)$ (which at first glance only deals with Galois extensions) is counting a significantly restricted collection of fields relative to the counting function $N_{K,n}(X;G)$ (which counts all G-extensions, not necessarily Galois ones).

In fact, we expect that the result of Example 3.5 should hold for any permutation representation ρ, not just the regular representation: if L/K is a G-extension of degree n with Galois closure $\hat{L}/K$, and ρ is the corresponding permutation representation, then we believe that there exist positive constants c and c', depending only on the extension degrees, such that

$$c' \,\mathrm{Nm}_{K/\mathbb{Q}}(\mathscr{D}_{L/K}) < D^{(\rho)}_{\hat{L}/K} < c\,\mathrm{Nm}_{K/\mathbb{Q}}(\mathscr{D}_{L/K}).$$

In particular, the counting asymptotics $N_{K,n}(X;G)$ and $N_{K,|G|}(X;\rho)$ should have the same growth rate in X. For non-permutation representations, we believe that the ρ-discriminant yields a novel way to order extensions.

In general, we suspect that the ρ-discriminant, possibly up to some local factors at primes dividing $|G|$, can be expressed in terms of the Artin conductor of ρ (composed

with an appropriate map $f : \mathrm{Gal}(\bar{K}/K) \to G$). A local result along these lines was proven by Wood-Yasuda [38]: their Theorem 3.7 shows that for the local analogue of the lattice $\Lambda_\rho = \mathscr{O}_L \Xi_\rho$, the covolume in the appropriate space is a power of the Artin conductor of ρ, for a class of representations ρ including self-dual representations and permutation representations. They also give an example in which their local weights do not agree with the local weights of the Artin conductor, but it is possible that such examples may be intrinsic to the modular representation case (which would not occur in the global case). We would expect that a similar type of result should hold for our lattice $\psi(\Xi_\rho)$.

3.3. Proof of Counting Theorem

Our first goal is to construct an element $\beta \in \Xi_\rho$ such that the coefficients of β generate the extension L/K. In order to do this, we first need to construct the correct analogue of the parameter t that appears in the statement of Theorem 2.4 (which here will account for the possibility that the coefficients of β may generate some intermediate subfield over K, rather than all of L).

Definition 3.7. *Let $\rho : G \to \mathrm{GL}(R)$ be a faithful representation, where R is a torsion-free $\mathscr{O}_K$-module of rank d. Define $t(\rho)$ to be the smallest positive integer such that for any nontrivial subgroup H of G, $R^{\rho(H)}$ has rank $\leq t$ as an $\mathscr{O}_K$-module.*

We collect a few necessary observations about the parameter $t(\rho)$:

Lemma 3.8. *If $\rho : G \to \mathrm{GL}(R)$ is a faithful representation, where R is a torsion-free $\mathscr{O}_K$-module of rank d, then $t(\rho)$ is strictly less than d, and only depends on the rank d and the representation ρ.*

Proof. Without loss of generality, we may extend ρ to $\mathrm{GL}(R \otimes_{\mathscr{O}_K} K) \cong \mathrm{GL}_d(K)$, thereby assuming that $R = K^d$. Then if H is any nontrivial subgroup of G, $\rho(H)$ is nontrivial because ρ is faithful (by assumption), meaning that $R^{\rho(H)}$ is a proper linear subspace of R: thus, its rank must be strictly less than the rank of R, which is d. □

Proposition 3.9. *Let K be a number field of degree l over $\mathbb{Q}$, $\hat{L}/K$ be a Galois extension of degree n with Galois group G, and $\rho : G \to \mathrm{GL}_d(\mathscr{O}_K)$ be a faithful representation with $t(\rho)$ as defined in 3.7. Let Ξ_ρ be the associated tuning submodule, and assume that $D^{(\rho)}_{\hat{L}/K} < X$. Then there exists a nonzero d-tuple $(\alpha_1, \ldots, \alpha_d) \in \Xi_\rho$, such that all archimedean valuations of each of the α_i for $1 \le i \le d$ are $\ll X^{\frac{1}{2l(d-t(\rho))}}$, and such that $L = K(\alpha_1, \ldots, \alpha_d)$.*

The idea of the proof is the same as in Proposition 2.1, except with the lattice $\psi(\Xi_\rho)$ in place of the Minkowski lattice. We also note again (for emphasis) that by Lemma 3.8, $t(\rho)$ is strictly less than d, so everything is well-defined.

Proof. Let $\Lambda = \psi(\Xi_\rho)$ be the image of the tuning submodule Ξ_ρ in $\Xi_\rho \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^{dl}$, and let $\beta_1, \cdots, \beta_{dl}$ be the successive minima of the gauge function $f(x_1, \cdots, x_{dl}) = \max(x_1, \ldots, x_{dl})$ on Λ. Set $f(\psi(\beta_i)) = \|\beta_i\|$ for shorthand. Note that the elements β_i lie in $\mathscr{O}_{\hat{L}}^{\oplus d}$ and thus we can write $\beta_i = (\alpha_{i,1}, \ldots, \alpha_{i,d})$ for some $\alpha_{i,j} \in \mathscr{O}_{\hat{L}}$. We also observe that $\|\beta_i\|$ is (up to an absolute constant) equal to the maximum archimedean valuation of $\alpha_{i,1}, \ldots, \alpha_{i,d}$.

By the definition of the ρ-discriminant and Minkowski's Second Theorem, we have

$$\prod_{i=1}^{dl} \|\beta_i\| \ll \left[D^{(\rho)}_{\hat{L}/K}\right]^{1/2}, \tag{3.3.1}$$

where the implied constant depends only on d, n, l.

Now since the β_i are nondecreasing, for any k we may use the bound given by 3.3.1 to write

$$\|\beta_k\|^{dl+1-k} \leq \prod_{i=k}^{dl} \|\beta_i\| \leq \prod_{i=1}^{dl} \|\beta_i\| \ll \left[D^{(\rho)}_{\hat{L}/K}\right]^{1/2}$$

whence

$$\|\beta_k\| \ll \left[D^{(\rho)}_{\hat{L}/K}\right]^{1/2(dl+1-k)}. \tag{3.3.2}$$

For all k with $1 \leq k \leq lt(\rho)+1$ and all j with $1 \leq j \leq d$, 3.3.2 implies

$$\|\alpha_{k,j}\| \ll \|\beta_k\| \ll \left[D^{(\rho)}_{\hat{L}/K}\right]^{1/2l(d-t(\rho))} < X^{1/2l(d-t(\rho))}. \tag{3.3.3}$$

Now, by the definition of $t(\rho)$, for any nontrivial subgroup H of G, $\Xi_\rho^{\rho(H)}$ has rank $\leq t(\rho)$ as an $\mathscr{O}_K$-module, hence has rank $\leq lt(\rho)$ as a $\mathbb{Z}$-module. Therefore, under the ρ-action, there exists some linear combination $\alpha = \sum c_i\beta_i$ (with coefficients that can be bounded above in terms of n, l, d only) which is only fixed by the trivial subgroup of $\rho(G)$. But by the construction of Ξ_ρ, the ρ-action is the same as the Galois action: thus α is not fixed by any element of $\mathrm{Gal}(\hat{L}/K)$, meaning that its coefficients generate $\hat{L}/K$.

Finally, for this element α, 3.3.3 and the boundedness of the c_i implies that

$$\|\alpha\| \ll X^{1/2l(d-t(\rho))}.$$

□

We can now prove our main theorem:

Theorem 3.10. *Let K be any number field, G be a finite group of order n, and $\rho : G \to GL_d(\mathscr{O}_K)$ be a faithful d-dimensional representation of G on $\mathscr{O}_K$. Also define $t(\rho)$ to be the smallest positive integer such that for any nontrivial subgroup H of G, $(\mathscr{O}_K^d)^{\rho(H)}$ has rank $\leq t(\rho)$ as an $\mathscr{O}_K$-module. Then*

$$N_{K,n}(X;\rho) \ll X^{\frac{1}{2(d-t(\rho))}\left[\sum_{i=1}^{d} \deg(f_i)\right]},$$

where the f_i *for* $1 \leq i \leq d$ *are a set of primary invariants for* ρ. *Furthermore, if* ρ *has a nontrivial secondary invariant, then we can replace the upper bound by* $X^{\frac{1}{2(d-t(\rho))}\left[\sum_{i=1}^{d} \deg(f_i) - \frac{\deg(f_1)}{2[K:\mathbb{Q}]}\right]+\epsilon}$.

Remark 3.11. As noted in Section 1.4, for a fixed representation ρ, a given set of primary invariants has a nontrivial secondary invariant if and only if the product of the primary-invariant degrees is strictly greater than $|G|$. The Chevalley-Shephard-Todd Theorem states that such a set of primary invariants will exist precisely when G is generated by pseudoreflections (although in practice, in order to apply the Theorem one must compute a set of primary invariants, so this yields no additional information).

Proof. Let G act on the polynomial ring $\mathbb{C}[x_1, \cdots, x_d]$ via ρ, and let $f_1, \cdots, f_d$ be primary invariants (cf. Section 1.4) of G with associated secondary invariants $1 = g_1, g_2, \cdots, g_k$, each set arranged in order of nondecreasing degree. In the event that there is only one secondary invariant, which happens precisely when $\prod \deg(f_i) = |G|$, instead set $g_2 = 1$ in what follows.

Let $R = \mathbb{C}[x_1, \cdots, x_d]^{\rho(G)}$, let S be the subring of R generated by $f_1, \cdots, f_d$ and g_2, and let $Z = \mathrm{Spec}(S)$. The ring S is a domain (since R is) so Z is irreducible. The natural map $\mathbb{C}[f_1, \cdots, f_d] \to S$ induces a projection $\Pi : Z \to \mathbb{A}^d$, and the map Π is finite because R is finite over $A = \mathbb{C}[f_1, \cdots, f_d]$. Finally, if $g_2 \neq 1$, then $g_2 \notin \mathbb{C}[f_1, \cdots, f_d]$ (by definition, since R is not A), and so in this case, Π has degree at least 2.

Now suppose we have a Galois extension $\hat{L}/K$ with Galois group G, such that $[K : \mathbb{Q}] = l$, $[\hat{L} : K] = n$, and such that $D^{(\rho)}_{L/K} < X$, and set Ξ_ρ to be the associated tuning submodule. By Proposition 3.9, there exists a nonzero element $\alpha \in \Xi_\rho$ such that all archimedean valuations of each component of α are $\ll X^{\frac{1}{2l(d-t(\rho))}}$.

For any $g \in G$, if $g \cdot x$ denotes the Galois action on $x \in \mathscr{O}_L$, then since f_i is an invariant polynomial under the action of $\rho(g)$, we have

$$g \cdot f_i(\alpha) = f_i(g \cdot \alpha) = f_i(\rho(g)\alpha) = f_i(\alpha),$$

where the middle equality follows from the fact that $\alpha \in \Xi_\rho$. Hence $f_i(\alpha)$ is fixed by every element of $\mathrm{Gal}(\hat{L}/K)$, so it lies in K. Furthermore, the components of α are algebraic integers and $f_i \in \mathscr{O}_K[x_1, \ldots, x_d]$, so $f_i(\alpha)$ is also an algebraic integer.

We may then obtain an upper bound on the total possible number of fields L by bounding the number of possible α. But since Π is finite, we may equivalently bound the number of possibilities for $\Pi(\alpha)$.

The coordinates of $\Pi(\alpha) = (y_1, \cdots, y_d)$ obey the bounds

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

for $1 \leq i \leq d$, which forms a "box" B in $\mathbb{A}^d(K)$. By choosing an integral basis of $\mathscr{O}_K$, this box becomes a box in $\mathbb{A}^{dl}(\mathbb{Q})$ with the same bounds, each occurring l times, and the image of $\Pi(\alpha)$ in $\mathbb{A}^{dl}(\mathbb{Q})$ is integral. But the number of integral points in this box is

$$\ll X^{\frac{1}{2(d-t(\rho))}\left[\sum_{i=1}^{d} \deg(f_i)\right]},$$

which is precisely the desired bound. In the event that ρ has a nontrivial secondary invariant, we may also apply the sieving lemma 2.2 to yield the stated improvement. $\square$

We make a few remarks regarding the bounds obtained by Theorem 3.10: for any given group, it may initially appear that using a small-dimensional representation is superior since a smaller representation will contain the same information as a larger one, but the smaller representation will have fewer invariants to deal with. However,

the counting technique employed here dictates that very small representations will give poor bounds, because the strength of the bound (for fixed K and G) is roughly given by $\frac{1}{d}\sum \deg(f_i)$: thus the arithmetic-geometric mean inequality, combined with the fact that $\prod \deg(f_i)$ is an integral multiple of $|G|$ (cf. Section 1.4), dictates that the exponent obtained from a d-dimensional representation in Theorem 3.10 will tend to be very large for small d. Of course, the ρ-discriminant is different for different representations, but the heuristics of Malle's conjecture combined with our expectations for the permutation-representation case suggest that a lower exponent is generally better.

We also observe that the technique of Ellenberg-Venkatesh can be interpreted (in our setting) as using the rth power of the standard representation of S_n (as opposed to the representation by itself) and they obtain better bounds by taking r to be large. We should note that they obtain additional savings by using only a small number of the invariant polynomials, rather than the full collection; it seems likely that a similar approach is feasible for general representations.

On the other hand, if the representation has very low dimension, the geometry of the scheme Z becomes vastly more tractable, and may in some cases allow much stronger point-counting techniques to improve the result beyond the basic "points in a box" method. And, in contrast with the situation for permutation representations where the invariants for transitive subgroups of S_n for $n \geq 5$ are generally quite complicated, there exist a number of interesting groups G with low-degree representations that nonetheless correspond to extensions of large degree; we give some examples in Section 3.4.

3.4. Sample Calculations for Particular Groups

Rather than attempting to tabulate all low-degree representations of all groups for which it would be computationally feasible to compute the invariant degrees, we will content ourselves to give merely a few examples illustrating the results of Theorem 3.10.

3.4.1. $\mathsf{PSL}_2(\mathbb{F}_7)$

The group $\mathsf{PSL}_2(\mathbb{F}_7)$ has six irreducible representations, of degrees 1, 3, 3, 6, 7, and 8; all of the nontrivial ones are faithful since G is simple.

The two representations of degree 3 are both defined over $\mathbb{Q}(\zeta_7)$ and have $t = 2$ – indeed, they are even defined over the quadratic subfield $\mathbb{Q}(\theta)$ for $\theta = \frac{1}{2}(\zeta_7 + \zeta_7^2 + \zeta_7^4)$. One can verify (for example) that for one of these representations, $\rho(G)$ is generated explicitly by the matrices

$$\begin{bmatrix} -1-2\theta & -\theta & -\theta \\ 2\theta & \theta & -1-\theta \\ 1 & 1+\theta & 1+\theta \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 \\ -1-2\theta & -1-\theta & 1-\theta \\ 1+2\theta & \theta & \theta \end{bmatrix}$$

and that the degrees of the primary invariant polynomials of ρ are 4, 6, and 14. (We do not reproduce the primary invariants here since they have very many coefficients, the largest of which are on the order of 10^8.) Theorem 3.10 then yields (for example) the bound $N_{\mathbb{Q}(\theta),168}(X;\rho) \ll X^{47/4+\epsilon}$. The direct sum of these two representations is defined over $\mathbb{Q}$; however, the primary-invariant computation did not return a result after 3 days of computation on a standard desktop computer.

The irreducible representation of degree 6 is defined over $\mathbb{Q}$, its invariant degrees are 2,3,3,4,4,7, and has $t = 1$. Theorem 3.10 yields the bound $N_{\mathbb{Q},7}(X;\rho) \ll X^{11/6+\epsilon}$.

Note that this representation is the same as the reduced permutation representation corresponding to the transitive subgroup 7T5 that was analyzed in Section 2.4, and (as should be expected) we obtain the same invariant degrees (aside from the missing one in degree 1), and the same exponent in the bound.

3.4.2. The Dihedral Groups D_n

There is a family of $\lfloor n/2 \rfloor$ 2-dimensional irreducible representations ρ of the dihedral group D_n, each of which is defined over $\mathbb{Q}(\zeta_n)$, given by the standard action of G on the vertices of a regular n-gon lying on the unit circle. (In fact, ρ can be defined over a subfield of $\mathbb{Q}(\zeta_n)$, but this merely complicates the exposition.) One such representation has $\rho(G)$ generated by the matrices

$$\begin{bmatrix} \zeta_n & 0 \\ 0 & \bar{\zeta}_n \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

It is then nearly immediate that the two polynomials

$$\begin{aligned} f_1 &= x_1 x_2 \\ f_2 &= x_1^n + x_n^n \end{aligned}$$

form a set of primary invariants for this representation. Since the product of the primary invariant degrees equals the order of the group, there are no nontrivial secondary invariants. A direct application of Theorem 3.10 with $t = 1$ then yields the bound $N_{K,n}(X;\rho) \ll X^{(n+2)/2}$, for any field K containing ζ_n. However, because the invariants of this representation are so simple, it seems exceedingly likely that a better point-counting method would yield a very substantial improvement over the bound arising directly from Theorem 3.10.

For the dihedral group D_7 in particular, there are three irreducible representations of degree 2 that are defined over $\mathbb{Q}(\zeta_7)$ and arise from the construction above. The direct sum of any two of them has primary invariant degrees of 2, 2, 5, and 7, and $t = 2$, yielding the bound $N_{K,n}(X;\rho) \ll X^4$ for any field K containing a seventh root of unity. The direct sum of all three representations has degree 6 and is equivalent to the reduced permutation representation 7T2; as we should expect, the resulting invariant degrees 2, 2, 2, 3, 4, and 7 are the same as those obtained in Section 2.3, and the bound $N_{\mathbb{Q},7}(X;G) \ll X^{19/12+\epsilon}$ obtained via Theorem 3.10 is the same as that obtained via Theorem 2.4 .

We should also note that when G is a dihedral group, good bounds on $N_{K,n}(\mathbb{Q};G)$ are available from class field theory, and show that the problem of counting dihedral extensions is intimately related to the Cohen-Lenstra heuristics; see [23] for more detail.

3.4.3. The Alternating Group A_5

The alternating group A_5 has five irreducible representations, of degrees 1,3,3,4,5 respectively. The nontrivial ones are faithful since A_5 is simple.

The two 3-dimensional representations are defined over $\mathbb{Q}(\zeta_5)$ and have $t = 2$. They each have a set of primary invariants of degrees 2, 6, and 10, and there is one nontrivial secondary invariant. Theorem 3.10 then yields the bound $N_{K,n}(X;\rho) \ll X^{71/4+\epsilon}$, for any field K containing a primitive fifth root of unity. (The computation for the primary invariants of the representation corresponding to the direct sum of these degree-3 representations, unfortunately, did not terminate after 2 days on a 4GHz desktop computer with 1GB of memory.)

The other irreducible representations are equivalent to reduced permutation representations, and the corresponding bounds obtained in the tables in Section 2.3 are the same.

Chapter 4

Related Open Problems

Our work in the previous chapters is related to a number of open questions, which we will briefly mention.

First, as discussed more extensively in Section 2.2, we believe there should be a number of ways to strengthen the result of Theorem 2.4 (and many of these techniques should also apply to Theorem 3.10). One method that could improve the result is to incorporate the technique of Ellenberg-Venkatesh [18], by counting ordered $\mathfrak{r}$-tuples of elements rather than single elements: this can be achieved by applying Theorem 3.10 to the $\mathfrak{r}$-fold direct sum of the underlying representation, although we would expect in this scenario that improvements can be made by throwing away some of the invariants (in the same way as Ellenberg-Venkatesh).

Another possibility is to study more carefully the geometry of the scheme Z for a particular group G, and to apply stronger point-counting techniques than the naive estimate obtained from the points-in-a-box method. Such an approach seems especially fruitful, and likely to result in good bounds, for the 2-dimensional representations of dihedral groups, whose invariants (as discussed in Section 3.4) are particularly simple.

It is also likely that for groups G with the property that a G-extension L/K has an intermediate subfield K' of small index, that a more direct approach (counting the possibilities for the intermediate extension K' and then the number of possible extensions

of K' of the proper degree) would yield better bounds than those arising directly from Theorems 2.4 and 3.10.

Second, we believe it should be possible to give a more explicit description of the ρ-discriminant for most representations ρ. For example, we expect that for permutation representations arising from a subfield, the ρ-discriminant should essentially be the discriminant of that subfield. We believe, indeed, that based on the local results proven by Wood-Yasuda [38], that aside from some local factors at primes dividing $|G|$, the ρ-discriminant should be essentially the same as the Artin conductor of ρ, for sufficiently well-behaved ρ.

Third, of significant interest is the opposite question for giving estimates on *lower* bounds for $N_{K,n}(X)$, on which there are also a number of results [18]. For certain n one can use known results to get easy lower bounds of the correct exponent in X; e.g., if n is even we can simply take the collection of quadratic extensions of any field E with $[E : K] = n/2$. In order to avoid such trivial cases we would likely want to impose conditions on the Galois group and thus convert the question into asking about lower bounds for $N_{K,n}(X; G)$ for any given group G. However, if one could merely show a positive lower bound for $N_{\mathbb{Q},n}(X; G)$ for all G, one would have solved the inverse Galois problem! Thus it seems more likely that this question is only approachable for particular groups or families of groups G (e.g., $G = D_n$, A_n, S_n, $PSL_d(\mathbb{F}_q)$, etc.). We can likewise pose the question of finding good lower bounds for the counting function $N_{K,n}(X; \rho)$.

Another counting question, which is partially related to a number of other heuristics such as Cohen-Lenstra-Martinet, is how the imposition of local conditions alters the asymptotics of $N_{K,n}(X; G)$, for a given group G. The famous counterexample of Wang to Grunwald's Theorem demonstrates that the effect of imposing even a single local

condition can be quite significant!

Fourth, there is also significant interest not only in giving asymptotic counts for the number of G-extensions, but also in computing them explicitly. We suspect that some or all of the invariant theory techniques would be useful in developing computational methods for characterizing G-extensions for larger G.

Bibliography

[1] Andrew Marc Baily, *On the density of discriminants of quartic fields*, J. reine angew. Math. 315:190–210, 1980.

[2] Manjul Bhargava, *Higher composition laws III: The parametrization of quartic rings*, Annals of Mathematics, 159.3: 1329–1360, 2004.

[3] Manjul Bhargava, *The density of discriminants of quartic rings and fields*, Annals of Mathematics pp. 1031–1063, 2005.

[4] Manjul Bhargava, *Higher composition laws IV: The parametrization of quintic rings*, Annals of Mathematics, 167:1–53, 2008.

[5] Manjul Bhargava, *The density of discriminants of quintic rings and fields* (preprint), arXiv:1005.5578, 2010.

[6] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman, *On the Davenport-Heilbronn theorems and second order terms*, Inventiones Mathematicae 193.2:439–499, 2013.

[7] Manjul Bhargava and Melanie Wood, *The density of discriminants of* S_3*-sextic number fields*, Proceedings of the American Mathematical Society 136.5:1581–1587, 2008.

[8] Henri Cohen, *Constructing and Counting Number Fields*, Proceedings of the ICM 2:129–138, 2002.

[9] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. *A survey of discriminant counting*, Algorithmic Number Theory pp. 80–94, 2002.

[10] Stephen D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proceedings of the London Mathematical Society 3.2:227–250, 1981.

[11] John H. Conway, Alexander Hulpke, and John McKay, *On transitive permutation groups*, LMS Journal of Computation and Mathematics 1:1–9, 1998.

[12] Boris Datskovsky and David J. Wright, *Density of discriminants of cubic extensions*, J. reine angew. Math. 386:116–138, 1988.

[13] Harold Davenport and Hans Heilbronn, *On the density of discriminants of cubic fields II*, Proceedings of the Royal Society of London Series A 322(1551):405–420, 1971.

[14] Boris Nikolaevich Delone and Dmitrii Konstantinovich Faddeev, *The theory of irrationalities of the third degree*. American Mathematical Society (vol. 10), 1964.

[15] Harm Derksen and Gregor Kemper, *Computational invariant theory*. Springer (vol. 131), 2002.

[16] David S. Dummit, *Solving solvable quintics*, Mathematics of Computation 57.195:387–401, 1991.

[17] Jordan S. Ellenberg and Akshay Venkatesh, *Counting extensions of function fields with bounded discriminant and specified Galois group*, Geometric Methods in Algebra and Number Theory pp. 151–168, 2005.

[18] Jordan S. Ellenberg and Akshay Venkatesh, *The number of extensions of a number field with fixed degree and bounded discriminant*, Annals of Mathematics pp. 723–741, 2006.

[19] Charles Hermite, *Sur le nombre limité d'irrationalités auxquelle se réduisent les racines des équations à coefficients entiers complex d'un degré et d'un discriminant donnés* (Extrait d'une lettre à M. Borchardt), J. reine angew. Math 53:182–192, 1857.

[20] John Jones, *Transitive Group Data*. Webpage: http://hobbes.la.asu.edu/Groups/. Accessed July 2014.

[21] Anthony C. Kable and Akihiko Yukie, *On the number of quintic fields*, Inventiones Mathematicae 160.2:217–259, 2005.

[22] Jürgen Klüners, *A counter example to Malle's conjecture on the asymptotics of discriminants*, Comptes Rendus Mathematique 340.6:411–414, 2005.

[23] Jürgen Klüners, *Asymptotics of number fields and the Cohen-Lenstra heuristics*, Journal de Théorie des Nombres de Bordeaux 18:607–615, 2006.

[24] Jürgen Klüners, *The distribution of number fields with wreath products as Galois groups*, International Journal of Number Theory 8.03:845–858, 2012.

[25] Jürgen Klüners and Gunter Malle, *Counting nilpotent Galois extensions*, J. reine angew. Math. 572:1–26, 2004.

[26] Gunter Malle, *On the distribution of Galois groups*, Journal of Number Theory 92:315–322, 2002.

[27] Gunter Malle, *On the distribution of Galois groups II*, Experimental Mathematics 13:129–135, 2004.

[28] Hermann Minkowski, *Ueber die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen*, J. reine angew. Math. 107:278–297, 1891.

[29] Wladyslaw Narkiewicz, *Elementary and analytic theory of algebraic numbers*. Springer, 2004.

[30] Jürgen Neukirch, *Algebraic number theory*. Springer, 1999.

[31] David Roberts, *Density of cubic field discriminants*, Mathematics of Computation 70.236:1699–1705, 2001.

[32] Mikio Sato and Tatsuo Kimura, *A classification of irreducible prehomogeneous vector spaces and their relative invariants*, Nagoya Mathematical Journal 65:1–155, 1977.

[33] Wolfgang M. Schmidt, *Number fields of given degree and bounded discriminant*, Astérisque 228.4:189–195, 1995.

[34] Jean-Pierre Serre, Martin Brown, and Michel Waldschmidt, *Lectures on the Mordell-Weil theorem*. Braunschweid: Vieweg, 1990.

[35] Carl L. Siegel, *Lectures on the geometry of numbers*. Springer, 1989.

[36] Takashi Taniguchi and Frank Thorne, *Secondary terms in counting functions for cubic fields*, Duke Mathematical Journal 162.13:2451–2508, 2013.

[37] Seyfi Turkelli, *Connected components of Hurwitz schemes and Malle's conjecture* (preprint), arXiv:0809.0951, 2008.

[38] Melanie Matchett Wood and Takehiko Yasuda, *Mass formulas for local Galois representations and quotient singularities I: a comparison of counting functions* (preprint), arXiv:1309.2879, 2013.

[39] David J. Wright, *Distribution of discriminants of abelian extensions*, Proceedings of the London Mathematical Society 3.1:17–50, 1989.

[40] David J. Wright and Akihiko Yukie, *Prehomogeneous vector spaces and field extensions*, Inventiones Mathematicae 110.1:283–314, 1992.

[41] Akihiko Yukie, *Shintani zeta functions*. Cambridge University Press (no. 183), 1993.