Proceedings of the International Congress of Mathematicians
Hyderabad, India, 2010

Statistics of Number Fields and Function Fields

Akshay Venkatesh[*] and Jordan S. Ellenberg[†]

Abstract

We discuss some problems of arithmetic distribution, including conjectures of Cohen-Lenstra, Malle, and Bhargava; we explain how such conjectures can be heuristically understood for function fields over finite fields, and discuss a general approach to their proof in the function field context based on the topology of Hurwitz spaces. This approach also suggests that the Schur multiplier plays a role in such questions over number fields.

1. Arithmetic Counting Problems

We begin with a concrete example, which has been well-understood for many years.

Let $\mathcal{S}_X$ denote the set of squarefree integers in $[0, X]$ that are congruent to 1 modulo 4; let $\mathcal{C}_X$ denote the set of isomorphism classes of cubic field extensions $K/\mathbf{Q}$ whose discriminant belongs to $\mathcal{S}_X$. Davenport and Heilbronn proved [6] that

$$\frac{|\mathcal{C}_X|}{|\mathcal{S}_X|} \longrightarrow \frac{1}{6}, \quad \text{as } X \to \infty. \tag{1}$$

Our goal is to understand *why limits like that of* (1) *should exist, why they should be rational numbers, and what the rational numbers represent.*

More precisely, we will study several variants on (1) – replacing cubic fields by extensions with prescribed Galois group, and "squarefree discriminant" by other forms of prescribed ramification. We make a heuristic argument as to what the corresponding limits should be when $\mathbf{Q}$ is replaced by the function field of a curve over a finite field, and lay out a program for a proof in certain cases. This program has been partially implemented by us in certain settings, leading to a weak form of the Cohen–Lenstra heuristics (see §4.2) over a rational function field. In the number field case we have no new theorems; however, the study

[*] Akshay Venkatesh, Stanford University. E-mail: akshay@math.stanford.edu.
[†] Jordan Ellenberg, University of Wisconsin. E-mail: ellenber@math.wisc.edu.

of the function field case suggests interesting refinements of known heuristics, related to the size of Schur multipliers.

Let us describe – briefly and approximately – how the $\frac{1}{6}$ makes an appearance over a function field. Let k be a finite field, and $\bar{k}$ an algebraic closure of k; we consider cubic extensions L of $k(t)$ with squarefree discriminant and totally split at ∞. By a *marking* of L we shall mean an ordering of the three places above ∞. "Marked" cubic extensions can be descended: they are identified with fixed points of a Frobenius acting on marked cubic extensions of $\bar{k}(t)$. Recall that *the average number of fixed points of a random permutation on a finite set is* 1; thus, if the Frobenius behaves like a random permutation, we expect there to be on average *one* marked cover per squarefree discriminant. Since there are six markings for each cubic field that is totally split at ∞, we recover $\frac{1}{6}$.

The rest of this paper will discuss methods for trying to make this heuristic into a proof, and how it suggests corrections to our view of number fields. In the function field case, results such as (1) are related to the group-theoretic structure of étale π_1; we may speculate that results such as (1) are reflections of some (as yet, not understood) group-theoretic features of the absolute Galois group of $\mathbf{Q}$.

1.1. Context.

There has been a great deal of work on the topics discussed here. We note in particular that related topics have been discussed [1, 3, 7] in the last three ICMs. Indeed, [1] contains an overview of Bhargava's results for quartic and quintic fields, and [3] discusses both theoretical and numerical evidence for conjectures of the type described in the present paper.

Our point of view is influenced very much by the study of the function field case; in turn, our study of that case was influenced by both Cohen and Lenstra's work and the more recent paper [8] of Dunfield and Thurston on finite covers of hyperbolic 3-manifolds.

The present paper has three sections; although related, they are also to a large extent independent, and can be considered as "variations on the theme of (1)."

- §2 discusses the conjectures of Bhargava-Malle about distribution of number fields, generalizing (1). We also discuss the role that Schur multipliers may play in formulating sharp versions of such conjectures (§2.4). The reader may wish to first look at Section 3.4, which provides the geometric motivation guiding the computations in Sections 2.4 and 2.5.

- §3 discusses the function field setting and its connection with the geometry of Hurwitz spaces; in particular, how purely topological results on the stable homology of Hurwitz spaces would imply function field versions of Bhargava-Malle conjectures.

- §4 discusses the special case of the Cohen–Lenstra heuristics, and our proof (with Westerland) of a weak version in the function field setting.

This proof suggests more general connections between analytic number theory and stable topology.

1.2. Notation.

By a G-extension algebra (resp. field) of a number field K, we shall mean a conjugacy class of homomorphisms (resp. surjective homomorphisms) from the Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ to G. In other words, G-extension fields are in correspondence with isomorphism classes of pairs $(L \supset K, G \overset{\sim}{\to} \mathrm{Gal}(L/K))$, where an isomorphism of pairs (L, f) and (L', f') is simply a K-isomorphism $\phi : L \to L'$ which commutes with the induced G-actions.

A pair (G, c) of a group G and a conjugacy class $c \subset G$ will be called *admissible* – for short, we say that c is an admissible conjugacy class – if

1. c is a rational conjugacy class, i.e., $g \in c \implies g^n \in c$ whenever n is prime to the order of g;
2. c generates the group G.

Given a tamely ramified G-extension and an admissible conjugacy class, we say that *all ramification is of type* c if the image of every inertia group is either trivial or a cyclic subgroup generated by some $g \in c$.

Acknowledgements. We thank Craig Westerland, our collaborator on the work described here, for many years of advice and ideas about the topological side of the subject. We have also greatly benefited from conversations with Manjul Bhargava, Nigel Boston, Ralph Cohen, Henri Cohen, David Roberts, and Melanie Wood.

2. Number Fields

In this section, we discuss Bhargava's heuristics for discriminants of S_n-extensions of $\mathbf{Q}$, and propose that for extensions with certain Galois groups G these heuristics should be modified by a term related to the Schur multiplier of G.

Before proceeding, however, we warn the reader of the alarming gap between theory and experiment. For example, the statement "there are $\frac{1}{6}$ totally real cubic fields per odd squarefree discriminant" is indeed only asymptotically valid; for instance, the smallest squarefree discriminants of real cubic fields are $229, 257$ and 321, and in fact (1) looks quite inaccurate for small X. However, there is convincing numerical evidence [22] that the ratio of (1) converges from below, with a secondary term decreasing proportionally to $D^{-1/6}$. This unpleasant situation – very slow numerical convergence to the expected limit – persists in all the examples we shall discuss in this paper, making it very difficult to test ideas except in somewhat indirect ways. For more discussion of this point, see §2.6.

2.1. Malle's conjecture.

For definiteness, we work over the base field $\mathbf{Q}$ for the moment; the ideas generalize in a straightforward fashion, and we will anyway pass to the case of a general number field in §2.4.

Suppose G is provided with an embedding into S_n. In that case, there is a well-defined "discriminant" of any G-extension algebra or field L, since the map $G \hookrightarrow S_n$ associates to L an étale $\mathbf{Q}$-algebra of degree n which has a discriminant in the usual sense. (In what follows, then, the "discriminant" of an S_n extension field refers to the discriminant of the associated degree n field, and not to the discriminant of its Galois closure.)

In this case, Malle has conjectured [18, 19] that

$$\lim_{X \to \infty} \frac{\#\ G\text{-extension fields of discriminant less than } X}{X^{1/a}(\log X)^b} \tag{2}$$

exists and is nonzero, for certain integers a and b depending on G. For instance, $n - a$ is the maximal number of orbits of any nontrivial $g \in G \subset S_n$.[1] This statement has some consequences which are surprising at first glance: for instance, a positive fraction of quartic fields (ordered by discriminant) contain $\mathbf{Q}(\sqrt{-1})$.

Malle's conjecture has been proved by Davenport–Heilbronn in the case $G = S_3$ (prior to Malle's general formulation!) and by Bhargava in the case S_4, S_5, in each instance with a precise description of the limit in (2) as an Euler product.

2.2. The asymptotic constant.

As originally stated, Malle's conjecture gives no information about the asymptotic constant, i.e. the limit of (2) as $X \to \infty$.

In fact, we do not regard the limiting value of (2) as the object of primary interest. This is because it conflates several independent issues; in particular, it mingles together fields with many different types of ramification, and it is also strongly influenced by the notion of "discriminant" (if we change the embedding $G \hookrightarrow S_n$, the limit will change).

Instead, we shall study the asymptotic constant only after "controlling" for these effects. For example: if we prescribe a set of primes and the ramification type at each prime, what is the expected number of global extensions realizing this "ramification data"? The word "expected" implies a suitable average; we usually mean to average over all sets S of primes with $\prod_{p \in S} p \leq X$, and then let $X \to \infty$.

In the rest of this paper, we shall discuss the case where we *fix a conjugacy class* $c \subset G$ and study G-extensions where *all ramification is of type* c. (See §1.2 for the notation.) For instance, (1) corresponds to the case of $G = S_3$ and c the class of transpositions; in the next section, we shall discuss totally real

[1] The value of b in Malle's original conjecture is now known to be incorrect in some cases when the extension fields being counted can contain extra roots of unity: see [17],[25].

S_n-extensions of odd squarefree discriminant, which corresponds to the case where $G = S_n$ and c is the class of transpositions.

The ideas that we describe can be generalized to multiple ramification types, and one can eventually return to the setting of (2) by putting this information together.

2.3. The asymptotic constant: Bhargava's heuristic.

On the basis of his results for $G = S_4$ and $G = S_5$, Bhargava has formulated a general and very beautiful conjecture [2, Conjecture 1.2] for the constant in the case $G = S_n$. We quote from his paper [2, page 10] and then explain by example:

> *The expected (weighted) number of global S_n-number fields of discriminant D is simply the product of the (weighted) number of local extensions of $\mathbf{Q}_v$ that are discriminant-compatible with D, where v ranges over all places of $\mathbf{Q}$ (finite and infinite).*

By a local extension of $\mathbf{Q}_v$, we mean simply a degree n étale algebra E over $\mathbf{Q}_v$; by discriminant–compatible, we mean (in the non-archimedean case) that the valuation of the discriminant of E coincides with the valuation of D and (in the archimedean case) that the signs match. Bhargava conjectures further that the expected number of S_n-extensions of discriminant D with a specified local behavior at v is obtained by the appropriate modification of the local factor at v in the above product.

Let us consider, for instance, what this means for *totally real fields* of odd squarefree discriminant D, i.e. totally real S_n-extensions all of whose ramification is of "transposition" type. To compute the expected number, one takes the product of local factors weight(v), where

$$\mathrm{weight}(v) = \sum \frac{1}{|\mathrm{Aut}(E/\mathbf{Q}_v)|},$$

the sum being taken over all degree n étale algebras $E/\mathbf{Q}_v$ that are:

- unramified, if v is a place not dividing D;
- have discriminant of valuation 1, if $v(D) = 1$;
- totally real, if v is infinite.

The weights in these cases are computed to be $1, 1$ and $\frac{1}{n!}$ respectively; so Bhargava's heuristic suggests that

> There are, on average, $\frac{1}{n!}$ totally real S_n-extensions of $\mathbf{Q}$ per odd squarefree discriminant,

where this is to be interpreted in a fashion analogous to (1) – in particular, we again restrict to discriminants that are congruent to 1 modulo 4, a necessary condition by Stickelberger's theorem. This statement is compatible with the limit $\frac{1}{6}$ that appears in (1).

One of the remarkable features of Bhargava's heuristic, as well as of the known results in degree ≤ 5, is that there is no restriction to tamely ramified extensions. Our knowledge in more general situations is sadly limited, and we shall unfortunately have to restrict to tame ramification.

2.4. General groups; the role of the Schur multiplier.

Let us now consider the case of a general group G. In this case, we shall propose that in many cases a version of Bhargava's heuristic applies: but that the heuristic as stated above often gives too few extensions, and must be modified by a term related to the size of the Schur multiplier of G. The reader will find motivation for this modification in Section 3.4.

Particularly in the number field case, what follows is speculative: We have, in the function field case, theoretical evidence for this modification, described in §3. But in the number field case we do not yet have serious numerical or theoretical evidence.

Let K, then, be a global field – either a number field, or a function field of a curve over a finite field; allowing this generality now allows ease of comparison later. To isolate as far as possible the particular phenomenon we wish to describe, we consider G-extensions L/K with the following properties:

1. G is center-free and has trivial abelianization;

2. $c \subset G$ is an admissible conjugacy class;

3. If K is a function field, we suppose that the characteristic of K does not divide $|G|$;

4. All ramification in L/K is tame of type c;

5. Fixing a set of places S_∞ of K containing all archimedean places, we consider only extensions L/K that are totally split at S_∞.

In what follows, we regard G, c, S_∞, K as fixed, subject to restrictions 1, 2, 3, and will count extensions L satisfying 4, 5.

The direct analogue of Bhargava's S_n heuristic would suggest that the average number of G-extensions L, for each set of ramified primes compatible with conditions 4 and 5, is $|G|^{-|S_\infty|}$. More precisely, let V be S_∞ together with all places whose residue characteristic divides the order of an element of c; if we denote by $\mathcal{S}_X$ the collection $\{S$ a subset of finite places of $K : S \cap V = \emptyset, \prod_{v \in S} q_v \leq X\}$, and by $\mathcal{F}_X$ the set of G-extensions L satisfying conditions 4,5 and which are ramified precisely at some $S \in \mathcal{S}_X$, then

$$\frac{|\mathcal{F}_X|}{|\mathcal{S}_X|} \longrightarrow |G|^{-|S_\infty|}, \text{ as } X \to \infty.$$

Based on our results in the function field case, we do not think this is right in general, and we speculate instead that

$$\frac{|\mathcal{F}_X|}{|\mathcal{S}_X|} \longrightarrow \frac{h(G,c,K)}{|G|^{|S_\infty|}}, \text{ as } X \to \infty, \tag{3}$$

for some rational number $h(G,c,K)$ related to the order of the Schur multiplier of G. We make precise predictions for the value of $h(G,c,K)$ in some special cases below.

Let $Q = Q_c \subset H_2(G,\mathbf{Z})$ be the subgroup generated by $\phi_*(H_2(\mathbf{Z}\times\mathbf{Z},\mathbf{Z}))$, as ϕ ranges over homomorphisms $\mathbf{Z}\times\mathbf{Z} \longrightarrow G$ taking $(0,1)$ to an element of c. We put

$$H_2(G,c;\mathbf{Z}) := H_2(G,\mathbf{Z})/Q_c. \tag{4}$$

The following interpretation in terms of covering groups will be useful: Fix a universal central covering $H_2(G,\mathbf{Z}) \to \tilde{G} \to G$ (such exists because G is assumed perfect). Fix $g \in c$ and a lift $\tilde{g} \in \tilde{G}$. Then any element $h \in G$ centralizing g has the property that $\tilde{h}\tilde{g}\tilde{h}^{-1} \in \tilde{g}Q_c$. Consequently, the natural projection induces a bijection from the conjugacy class of $\tilde{g}Q_c$ in $\tilde{G}/Q_c$ to the conjugacy class c. Write $\tilde{G}_c$ for the quotient of $\tilde{G}$ by Q_c; it is the "largest covering to which the conjugacy class of c lifts bijectively." Then $H_2(G,c;\mathbf{Z})$ is precisely the kernel of $\tilde{G}_c \to G$.

If the ground field K contains sufficiently many roots of unity (i.e., if $\mu_N \subset K$ where N depends only on (G,c)) and S_∞ is large enough, we believe that

$$h(G,c,K) = \#H_2(G,c;\mathbf{Z}). \tag{5}$$

In the general case, we anticipate $h(G,c,K)$ will be a rational number between 0 and $\#H_2(G,c;\mathbf{Z})$ that depends on the number of roots of unity in K.

For instance, if the order of elements of c are relatively prime to $\#H_2(G,c;\mathbf{Z})$, then we believe that $h(G,c,K) = \#H_2(G,c;\mathbf{Z})$ as soon as the number m of roots of unity in K annihilates $H_2(G,c;\mathbf{Z})$ and S_∞ contains all the primes dividing m.

In fact, in the next section, we shall associate (under these conditions) a fundamental class $\mathfrak{z}(\rho) \in H_2(G,c;\mathbf{Z})$ to any G-extension ρ, and we suggest even the following refinement of (3): for any $\alpha \in H_2(G,c;\mathbf{Z})$,

$$\frac{|\mathcal{F}_X^\alpha|}{|\mathcal{S}_X|} \longrightarrow |G|^{-|S_\infty|}, \text{ as } X \to \infty, \tag{6}$$

where $\mathcal{F}_X^\alpha$ is now restricted to those G-extensions with fundamental class α.

Remark. Heuristic (3) is definitely not valid as stated for general (G,c) with no hypotheses on the extension. The case $G = D_4$ is one whose difficulties have been much studied. There are *no* quartic extensions of $\mathbf{Q}$ with Galois group D_4 and squarefree discriminant, although there are no local obstructions to this; indeed, squarefree discriminant implies that the Galois group is S_n. When one counts quartic dihedral extensions with $|\mathrm{disc}| \le X$, one gets a positive multiple of X, by a result of Cohen, Diaz y Diaz, and Olivier [5]; however, the constant is not equal to that predicted by the heuristics discussed here. The point is that the conjugacy class of "transpositions" in D_4 is not admissible – it fails to generate D_4.

2.5. Lifting invariants over global fields. Motivated by the considerations of the prior section, we shall now associate to a homomorphism $\rho : G_K \to G$, satisfying certain local conditions, a "fundamental class" $\mathfrak{z}(\rho)$ in $H_2(G, c; \mathbf{Z})$. (This association depends on the choice of a generator for the roots of unity in K.) This fundamental class is an invariant of the conjugacy class of ρ, meant to analogize the Fried-Serre "lifting invariant" of branched G-covers of the projective line [11, 24].

In addition to the group-theoretic conditions from §2.4 (namely, G center-free with trivial abelianization, $c \subset G$ admissible) we impose the following restrictions:

1. Let μ_n be the group of roots of unity in K. Then n annihilates $H_2(G, c; \mathbf{Z})$.
2. The order e of any element of c is relatively prime to $\#H_2(G, c; \mathbf{Z})$.

These conditions are satisfied, for instance, when $G = A_5$ and c is the class of 3-cycles. If these conditions fail, one may still obtain an invariant by passing to a sufficiently large cyclotomic extension, but we have not yet studied the resulting construction in sufficient detail to be confident about its properties.

Let $\tilde{G}_c$ be the covering of G constructed after (4). Condition (2) of the prior paragraph implies that there is a *unique* conjugacy class $\tilde{c}$ of $\tilde{G}_c$ which projects bijectively onto c, and whose elements have order e. Moreover, if x is an element of c, there exists a unique lifting of the cyclic subgroup $\langle x \rangle \subset G$ to a cyclic subgroup of $\tilde{G}_c$ of order e.

For brevity, we denote $H_2(G, c; \mathbf{Z})$ by A. We fix an algebraic closure $\bar{K}$ of K and let $G_K = \mathrm{Gal}(\bar{K}/K)$ be the absolute Galois group; for each place v of K, we let $G_v \subset G_K$ be a decomposition group and (for v finite) $I_v \subset G_v$ an inertia group.

Lemma. *Let S_∞ be a finite set of places of K, containing archimedean places. Let $\rho : G_K \to G$ be a homomorphism satisfying the following local properties:*

a. ρ is trivial on G_v for $v \in S_\infty$.

b. ρ is tamely ramified;

c. If v is a ramified place, $\rho(I_v)$ is a cyclic subgroup of G generated by an element of c.

Then ρ lifts to a representation $\tilde{\rho} : G_K \to \tilde{G}_c$. Moreover $\tilde{\rho}$ can be chosen so that it has properties (a), (b), i.e. it is everywhere tame, and trivial on G_v for $v \in S_\infty$.

Proof. The obstruction to such a lift lies in $H^2(G_K, A)$; it suffices to compute the obstruction locally, since the map

$$H^2(G_K, A) \longrightarrow \bigoplus_v H^2(G_v, A)$$

is injective, by virtue of the assumption that $\mu_n \subset K$.

For v infinite it is clear that $\rho|G_v$ can be lifted to a homomorphism $G_v \to \tilde{G}_c$. For v finite, $\rho|G_v$ factors through the maximal tame quotient of G_v. Fixing a generator τ_v for tame inertia as well as a Frobenius element Fr_v, we can specify $\rho|G_v$ by means of a pair $(t = \rho(\tau_v), F = \rho(\mathrm{Fr}_v)) \in G \times G$ satisfying

$$FtF^{-1} = t^q. \tag{7}$$

where $q = q_v$ is the cardinality of the residue field at v.

Let $\tilde{t}$ be the unique preimage of t with exact order e, and $\tilde{F}$ an arbitrary lift of F. By (7), t^q has order e, and so q is relatively prime to e; thus

$$\tilde{F}\tilde{t}\tilde{F}^{-1} = \tilde{t}^q, \tag{8}$$

since both sides are lifts of t^q with order e.

Thus $\rho|G_v$ lifts to $\tilde{G}_c$ for all v; thus ρ also lifts to a representation $\tilde{\rho} : G_K \to \tilde{G}_c$.

It remains to check that $\tilde{\rho}$ can be chosen to be tame at all finite places and trivial at $v \in S_\infty$. We have already constructed a tamely ramified lift of $\rho|G_v$ for each finite v. It follows that there exists, for every $v \notin S_\infty$ for which $\tilde{\rho}|G_v$ is wild, a character $\chi : G_v \to A$ so that $\chi_v\tilde{\rho}$ is tame at v. Similarly, for $v \in S_\infty$, there exists a character $\chi : G_v \to A$ so that $\chi_v\tilde{\rho}$ is trivial on G_v.

We now twist $\tilde{\rho}$ by any character $\chi : G_K \to A$ which extends χ_v at S_∞ and all other places wildly ramified in $\tilde{\rho}$, and which is tame at all other places; one checks that such a χ exists by using weak approximation. □

We now take S_∞ to be the set of archimedean places, together with all places dividing n. We shall associate an invariant $\mathfrak{z}(\rho) \in H_2(G, c; \mathbf{Z})$ to any $\rho : G_K \to G$ that satisfies the condition of the Lemma. Fix a lifting $\tilde{\rho}$ as in the Lemma.

For each place $v \notin S_\infty$ consider the sequence

$$I_v \to W_v^{\mathrm{ab}} \xrightarrow{\sim} K_v^\times,$$

where W_v is the local Weil group and the latter isomorphism is class field theory. This induces a map $I_v^{\mathrm{tame}} \to k_v^\times$, where k_v is the residue field at v.

Fix a generator g for $\mu_n \subset K$; regarding it as an element of $k_v^\times$, let g_v be any preimage of g inside I_v^{tame} with the property that the image of g_v inside the tame quotient I_v^{tame} generates a subgroup of index $\frac{q_v-1}{n}$.

Such g_v exist and any two choices g_v, g_v' satisfy $g_v' = g_v^\lambda, g_v = {g_v'}^{\lambda^{-1}}$ where λ lies in the kernel of the reduction $\widehat{\mathbf{Z}}^\times \twoheadrightarrow (\mathbf{Z}/n\mathbf{Z})^\times$.

Recall that the image $\rho(I_v)$ is either trivial or a cyclic subgroup generated by some element of c and, in either case, admits a unique lift $x \mapsto x^*$ to a cyclic subgroup of the same order in $\tilde{G}_c$. We define the lifting invariant of the homomorphism $\rho : G_K \to G$ as

$$\mathfrak{z}(\rho) = \prod_{v \notin S_\infty} z_v, \quad z_v = \tilde{\rho}(g_v)\left(\rho(g_v)^*\right)^{-1} \in A.$$

1. Independence of $\tilde{\rho}$: Any other lift of ρ as in the Lemma is necessarily of the form $\tilde{\rho}\psi$, for some character $\psi : G_K \to A$ that is everywhere tame, and trivial on all G_v ($v \in S_\infty$). Independence now follows from the reciprocity law of class field theory.

2. Independence of g_v (while fixing g): let $g_v' = g_v^\lambda$, with $\lambda \in \ker(\widehat{\mathbf{Z}}^\times \to (\mathbf{Z}/n\mathbf{Z})^\times)$. Then

$$\begin{aligned}\tilde{\rho}(g_v') = (\tilde{\rho}(g_v))^\lambda &= (z_v \rho(g_v)^*)^\lambda \\ &= z_v(\rho(g_v)^*)^\lambda = z_v\rho(g_v^\lambda)^* = z_v\rho(g_v')^*.\end{aligned}$$

3. Independence on the choice of I_v: the inertia subgroups of G_K are defined up to conjugacy, and it is clear that replacing each g_v by a conjugate does not affect z_v, and thus leaves $\mathfrak{z}(\rho)$ unchanged.

The invariant *does* depend on g; replacing g with g^α for $\alpha \in (\mathbf{Z}/n\mathbf{Z})^*$ has the effect of replacing $\mathfrak{z}$ with $\mathfrak{z}^\alpha$.

Example. Take $G = A_5$ and $K = \mathbf{Q}$. For the conjugacy class c of 3-cycles, we have $\#H_2(G, c; \mathbf{Z}) = 2$; on the other hand, for the conjugacy class c' of products of two commuting transpositions we have $\#H_2(G, c; \mathbf{Z}) = 1$. Thus, we expect there to be *twice as many* tamely ramified totally real A_5-extensions, all of whose ramification is of type c, than those all of whose ramification is of type c'.

In this case, the lifting invariant is defined as follows: The universal cover of A_5 is just $\mathrm{SL}_2(\mathbf{F}_5) \to \mathrm{PSL}_2(\mathbf{F}_5) \cong A_5$. Using the lemma, lift the given homomorphism $\rho : G_\mathbf{Q} \to A_5$ to $\tilde{\rho} : G_\mathbf{Q} \to \mathrm{SL}_2(\mathbf{F}_5)$. Let S be the set of primes p congruent to 3 mod 4 for which $\tilde{\rho}(I_p)$ has even order (cf. [24]).

Then the invariant $\mathfrak{z}(\rho)$ is determined by the parity of $|S|$. This is independent of our choice of $\tilde{\rho}$, since, for any homomorphism $\chi : G_\mathbf{Q} \to \{\pm 1\}$ that is tame and trivial at ∞ – i.e., the character associated to a quadratic field of positive odd discriminant – the set of $p \equiv 3$ mod 4 for which $\chi(I_p) \neq \{1\}$ has even cardinality.

Numerical inspection of John Jones' number field tables [16] indeed shows, amongst totally real, tame A_5-fields of small discriminant, a preponderance of inertial types of order 3, although, as we discuss in the next section, the data is very scarce and one should be very cautious about treating it as evidence.

Remark. Relaxing the condition that $|A|$ and e are coprime leads to more subtle behavior than that discussed here. For instance, take $G = \mathrm{PSL}_2(\mathbf{F}_7)$ and c the unique conjugacy class of order 4, so that $\tilde{G}_c = \mathrm{SL}_2(\mathbf{F}_7)$ and $A = \mathbf{Z}/2\mathbf{Z}$. One can check that c does *not* lift to any conjugacy class of order-4 elements of $\tilde{G}_c$, and $\rho : G_K \to G$ need not lift locally to $\tilde{G}_c$ even though $\mu_2 \subset K$. In this case different modifications to Bhargava's heuristics are needed.

2.6. Numerics. The difficulty of investigating conjectures of this kind increases very rapidly with the degree, not only because of slow convergence but because of the scarcity of examples. For instance, Jones's database of number fields shows that there are just eight totally real quintics with Galois group S_5 and discriminant less than 10^5, while Bhargava's asymptotic (which is provably correct as the discriminant goes to infinity!) would predict around 600.

One can think of this scarcity as following, in part, from analytic lower bounds for the discriminant [21]. Alternatively, one might imagine that the number of S_n-extensions of discriminant in $[0..X]$ has a secondary main term with negative coefficient. In the S_3 case, Roberts has given convincing evidence [22] that the number of totally real cubics of discriminant $\leq X$ admits an asymptotic formula

$$aX - bX^{5/6} + O(X^{1/2+\varepsilon}),$$

for certain explicit constants $a, b > 0$. This modified heuristic, which arises naturally from the pole structure of the pertinent Shintani zeta function, fits numerical data *far better* than does the Davenport-Heilbronn asymptotic aX.

Question. *Describe the lower order terms in the counting function for S_n-discriminants, the main term of which is provided by the conjectures of Malle and Bhargava.*

It seems quite likely that the phenomenon of lower-order terms only slightly smaller than the main term is rather general; thus (barring a sudden increase in the range where number fields can be counted exhaustively) a principled answer to the Question above is likely necessary for any serious numerical investigation of the conjectures, even insofar as the main term is concerned.

3. Function Fields and Hurwitz Spaces

We now discuss features of the topology of Hurwitz spaces that are responsible for the truth of theorems such as (1) over the function fields of finite fields.

We begin by discussing Hurwitz spaces in a purely topological setting (§3.1, §3.2); then, in §3.3, we discuss Hurwitz *schemes* over finite fields and their relevance to function field analogues of Bhargava-type heuristics; finally in §3.4 we discuss motivation for the "Schur correction" from §2.4.

We fix throughout an admissible pair (G, c) of a finite group G and a conjugacy class $c \subset G$; for simplicity we suppose that G is center-free.

3.1. Hurwitz spaces.

In this section, $\mathbf{P}^1_{\mathbf{C}}$ denotes the complex points of the projective line; however, in §3.1 and §3.2 we are only interested in its topology, and the reader could replace it by a two-sphere without changing the meaning.

We will consider the Hurwitz space $\mathsf{Hur}_{G,c}(n)$ that, informally speaking, parameterizes G-covers of $\mathbf{P}^1_{\mathbf{C}}$, branched at n points distinct from ∞, with the monodromy around each branch point lying in c, and with a "marking" of the fiber above ∞, i.e. a G-equivariant identification of this fiber with G. For brevity, we shall regard (G, c) as fixed and write simply $\mathsf{Hur}(n)$ in place of $\mathsf{Hur}_{G,c}(n)$.

Here is the precise definition of $\mathsf{Hur}(n)$: Let $\mathsf{Conf}(n)$ be the configuration space of n points in the complex plane $\mathbf{C}$. It is a $K(\pi, 1)$ whose fundamental group, the *Artin braid group*, is generated by elements $\{\sigma_i : \quad 1 \leq i \leq n-1\}$ which pull one point in front of the next. The generators σ_i and σ_j commute when $|i - j| \neq 1$, and σ_i and σ_{i+1} satisfy the braiding relation $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$; these relations give a presentation of the braid group. Let $\mathsf{Hur}(n)$ be the covering space of $\mathsf{Conf}(n)$ whose fiber above a configuration $D \in \mathsf{Conf}(n)$ is the set of homomorphisms

$$\pi_1(\mathbf{P}^1_{\mathbf{C}} - D, \infty) \longrightarrow G,$$

sending a loop around each puncture to an element of c.

Equivalently, the action of the fundamental group of Conf_n on the fiber of $\mathsf{Hur}(n) \to \mathsf{Conf}(n)$ is equivalent to the standard action of the braid group on $\{(g_1, \ldots, g_n) \in c^n : g_1 g_2 \ldots g_n = 1\}$, given by the rule

$$\sigma_i : (g_1, \ldots, g_i, g_{i+1}, \ldots, g_n) \longrightarrow (g_1, \ldots, g_{i+1}, g_{i+1}^{-1} g_i g_{i+1}, \ldots, g_n). \qquad (9)$$

3.2. Stable homology.

The first thing to note is that the Hurwitz space $\mathsf{Hur}(n)$ need not be connected: Let $\mathsf{CHur}(n) \subset \mathsf{Hur}(n)$ be the subspace of $\mathsf{Hur}(n)$ corresponding to *surjective* homomorphisms $\pi_1(\mathbf{P}^1_{\mathbf{C}} - D, \infty) \longrightarrow G$; then $\mathsf{CHur}(n)$ parametrizes *connected* covers of $\mathbf{P}^1_{\mathbf{C}}$. Then $\mathsf{CHur}(n)$ is open and closed in $\mathsf{Hur}(n)$.

It was proved in the nineteenth century by Clebsch, Lüroth, and Hurwitz that $\mathsf{CHur}(n)$ has only *one* component when G is the symmetric group and c is the conjugacy class of transpositions. However, in general, even $\mathsf{CHur}(n)$ may not be connected, an issue we study further in §3.4. These questions can be reduced to problems in combinatorial group theory: by (9), the components of $\mathsf{Hur}(n)$ are in bijection with the orbits of the braid group on $\{(g_1, \ldots, g_n) \in c^n : g_1 g_2 \ldots g_n = 1\}$; the components of $\mathsf{CHur}(n)$ are the orbits consisting of n-tuples which generate G.

More generally (that is, for arbitrary G, c) it is a pleasant exercise to check that the connected components *stabilize*: that is, there exists an integer E so that $\mathsf{CHur}(n)$ and $\mathsf{CHur}(n+E)$ have the same number of connected components whenever n is large enough relative to G, c.

One can think of this as a stabilization statement for the degree-zero homology group $H_0(\mathsf{CHur}(n))$. What about the higher homology?

We say that (G, c) satisfies the stability (resp. vanishing) condition if:

1. Stability condition: There exists $A > 0, E \in \mathbf{Z}$ so that

$$\dim H_j(\mathsf{CHur}(n), \mathbf{Q}) = \dim H_j(\mathsf{CHur}(n+E), \mathbf{Q}), \quad j < An - 1.$$

2. Vanishing condition: There exists $A > 0$ so that the map $\mathsf{CHur}(n) \longrightarrow \mathsf{Conf}(n)$ induces an isomorphism on rational homology

$$H_j(X, \mathbf{Q}) \xrightarrow{\sim} H_j(\mathsf{Conf}(n), \mathbf{Q})$$

in degrees $j < An$, for each connected component X (if any) of $\mathsf{CHur}(n)$.

Note that $H_j(\mathsf{Conf}(n), \mathbf{Q})$ is vanishing for $j > 1$ and one-dimensional for $j = 1$, thus the name "vanishing condition." It is very interesting to ask to what extent the regularities above might be satisfied with integral coefficients, or $\mathbf{Z}[\frac{1}{|G|}]$-coefficients. In these settings, $\mathsf{Conf}(n)$ has nontrivial cohomology in many degrees.

In [9], we prove a first theorem in this direction.

Theorem. *(E., V., Westerland). Let A be an abelian group of odd order, and $D(A)$ the generalized dihedral group $A \rtimes \mathbf{Z}/2\mathbf{Z}$, where the $\mathbf{Z}/2\mathbf{Z}$ acts on A by $a \mapsto -a$. Then the pair $(D(A), \text{involutions})$ satisfies the stability condition.*

The proof follows, in the large, the same lines as Harer's proof [14] of homological stability for $\mathcal{M}_g$. As in his argument, an essential element is the high connectivity of a combinatorially defined complex – in this case, the "arc complex" studied by Hatcher and Wahl [15] – on which the braid group acts. In the Hurwitz space case, a key role is played by the stable H_0 discussed above:

$$R = \oplus_{n \geq 0} H_0(\mathsf{Hur}(n), \mathbf{Q}) \tag{10}$$

As the notation suggests, R is a *ring*, with product given by concatenation of n-tuples. The animating principle of our argument is that, under the conditions of the theorem, the homological algebra of the category of R-modules is "approximately" the same as that of the category of $\mathbf{Q}[t]$-modules. (Warning: this ring R is not exactly the same as that used in [9], where we consider covers of $\mathbf{A}^1_{\mathbf{C}}$ rather than $\mathbf{P}^1_{\mathbf{C}}$.)

We believe that far more than the Theorem above is true: not only the stability but also the vanishing condition will hold for a wide range – perhaps all – admissible pairs (G, c). For safety, we formulate this as a conjecture only in the case where we feel most secure:

Conjecture. $(S_n, \text{transpositions})$ *satisfies the vanishing condition.*

The significance for arithmetic lies in the fact that the vanishing condition essentially implies the function field version of Malle-Bhargava heuristics (including Schur corrections as in §2.4). For instance, the stated conjecture implies

> There are, on average, $\frac{1}{n!}$ totally real S_n-extensions of $\mathbf{F}_q(T)$ per squarefree discriminant,

where in this context "totally real" means that the extension is totally split at ∞; also – analogous to restricting to discriminants congruent to 1 mod 4 in (1) – we restrict to discriminants of even degree, since there are no such extensions if the discriminant degree is odd.

Similarly, the Theorem implies a (somewhat weaker) form of Malle's conjecture in the case of dihedral groups; since this particular case is usually formulated in terms of the "Cohen–Lenstra heuristics," we return to it separately in §4.

More generally, it seems that many questions of analytic number theory, when considered over a function field, are related to topological phenomena of homology stabilization, a topic that is discussed in [9, §1.7], and which we intend to take up elsewhere.

We now turn to explaining the relation between homological stability conditions, as discussed above, and counting extensions of function fields. The crucial tool that allows us to pass from topology of complex moduli spaces to enumerative questions over finite fields is, as might be expected, the Grothendieck-Lefschetz trace formula.

3.3. Hurwitz schemes.

We now explain how the homology of the Hurwitz space is related to function-field analogues of Malle's conjecture. In what follows, all schemes are over Spec $\mathbf{Z}[\frac{1}{|G|}]$.

Let $\mathscr{C}(n)$ be the scheme parameterizing configurations of n unordered distinct points on $\mathbf{A}^1$. This can be identified with the complement of the discriminant divisor inside the affine space $\mathrm{Sym}^n\mathbf{A}^1$ of degree n monic polynomials; it is an algebraic version of $\mathsf{Conf}(n)$.

It is also possible to define an algebraic version of the space $\mathsf{CHur}(n)$, i.e., a Hurwitz *scheme* $\mathscr{CH}(n)$ over $\mathbf{Z}[\frac{1}{|G|}]$; it is an étale cover of $\mathscr{C}(n)$ parameterizing branched G-covers of $\mathbf{P}^1$ with n branch points, all of whose ramification is tame of type c, and which are endowed with an extra structure called "marking at ∞." The complex points of $\mathscr{C}\mathscr{H}(n)$ are naturally identified with the topological space $\mathsf{CHur}(n)$ of the previous section. For an exposition of the construction of $\mathscr{C}\mathscr{H}(n)$ we refer to [23].

In particular, if k is a finite field, the size of $\mathscr{C}\mathscr{H}_n(k)$ is equal to the number of isomorphism classes of G-extensions of $k(t)$, totally split at ∞ and all ramification of type c, together with a "marking at ∞."

The Grothendieck–Lefschetz fixed point formula gives a relation between the number of $\mathbf{F}_q$-points of an algebraic variety and its étale cohomology. It is possible (cf. [9, §7]) to compare the singular homology of the Hurwitz space $\mathsf{CHur}(n)$, and the étale cohomology of the Hurwitz scheme $\mathscr{C}\mathscr{H}(n)$ over $\overline{\mathbf{F}_q}$. In this way, we obtain a relation between the singular homology of the Hurwitz space and Malle's conjecture.

The stability condition for (G, c) alone, together with relatively elementary bounds, shows that the étale cohomology of the Hurwitz scheme is "not too large;" although the only *a priori* control on the Frobenius action comes from the Weil conjectures, this already suffices for interesting upper and lower bounds for $|\mathscr{C}\mathscr{H}(\mathbf{F}_q)|$. An example of a result thus obtained is the theorem given in §4.2; see also [9, pp. 5–6] for further discussion of this technique.

However, if the Hurwitz scheme and the configuration scheme have *the same* rational homology in some range – as the vanishing conjecture predicts, in cases where $\mathsf{CHur}(n)$ is connected – then $|\mathscr{C}\mathscr{H}(n)(\mathbf{F}_q)|$ and $|\mathscr{C}(n)(\mathbf{F}_q)|$ will be approximately equal, as long as q is sufficiently large relative to (G, c). Equivalently, as $n \to \infty$ with q fixed there will be an average of *one* marked G-extension per discriminant. (The $1/n!$ term in the conjecture stated in the previous section comes from the existence of $n!$ different markings on each extension that is totally split at ∞.)

3.4. Stable components and the Schur correction.

The vanishing condition of §3.2 gives very strong control of the homology of each component of $\mathsf{CHur}(n)$; but $\mathsf{CHur}(n)$ is not connected in general, and indeed, the description of the set of connected components is somewhat subtle, especially when the Galois action is taken into account.

Remarkably, it is possible to completely understand the connected components in the large n limit, owing to a beautiful theorem of Conway–Parker and Fried-Völklein. Only a proof of a special case is available in print: [12, Appendix], but it contains all the necessary ideas. We also do not attempt to formulate it in the most general case, restricting to G perfect. For the definition and basic properties of $\tilde{G}_c$ used in the definition below, we refer the reader to the discussion after (4).

Theorem. *(Conway-Parker-Fried-Völklein). Suppose G is perfect; let $g \mapsto g^*$ be a conjugacy-equivariant bijection from $c \subset G$ to a conjugacy class of $\tilde{G}_c$*

lifting c. Then, for sufficiently large n, the map

$$(g_1, \ldots, g_n) \in c^n \longrightarrow g_1^* \ldots g_n^* \in \tilde{G}_c$$

induces a bijection from the stable component group to $H_2(G, c; \mathbf{Z})$, as defined in (4)*. In particular, the number of components of* $\mathsf{CHur}(n)$ *equals* $\#H_2(G, c; \mathbf{Z})$ *for n sufficiently large.*

The source of the "Schur correction" in the function field case is now apparent: it arises from the fact that the Hurwitz scheme $\mathscr{C}\mathscr{H}_n$ may have multiple components, and therefore more points than expected; the number of components is related to the size of a Schur multiplier. More precisely, the group $H_2(G, c; \mathbf{Z})$ bijects onto the set of *geometric* components of $\mathscr{C}\mathscr{H}_n/\mathbf{F}_q$; if some of these components are not defined over $\mathbf{F}_q$, there may be *fewer* G-covers than expected. This is what happens in the situation of the Remark, page 11; and this is the reason why we have postulated "enough roots of unity" in (5).

Let us make precise the relation to §2.4. Let k be a finite field of order q and $K = k(t)$. We maintain the hypotheses that (G, c) is admissible, that q is relatively prime to $|G|$, that G is center-free and that G^{ab} is trivial; we take the set S_∞ of §2.4 to consist of the place corresponding to the point at ∞.

The methods of [9] establish the following: if k contains sufficiently many roots of unity (that is, if $q-1$ is sufficiently divisible), and q is sufficiently large – both notions depending on (G, c) – then, with $h = \#H_2(G, c; \mathbf{Z})$ the number of connected components of $\mathsf{CHur}(n)$,

> The vanishing condition for (G, c) implies the function field case of (3): $\frac{|\mathcal{F}_{q^m}|}{|\mathcal{S}_{q^m}|} \sim \frac{h}{|G|}$, as $m \to \infty$.

and the weakened version:

> The stability condition for (G, c) implies that $\left|\frac{|\mathcal{F}_{q^m}|}{|\mathcal{S}_{q^m}|} - \frac{h}{|G|}\right| \leq Aq^{-1/2}$, where the constant $A = A(G, c)$ is independent of q, m.

Concerning the notion of "enough" roots of unity: It is very likely[2] that the assumptions of §2.5 – i.e. $\mu_m \subset K$ and $(e, m) = 1$ where e is the order of an element of c and m annihilates $\#H_2(G, c; \mathbf{Z})$ – are sufficient to ensure the validity of the above results, and moreover that, in this case, the refined statement (6) is valid.

Remark. It is particularly interesting to examine from this point of view the phenomenon of "lower order terms" discussed in §2.6. It is natural to suppose that such lower order terms correspond to natural families of cohomology classes on the Hurwitz schemes (albeit classes in degrees which increase with

[2] To verify this amounts to checking compatibility between certain definitions in characteristic zero and positive characteristic; we have not done so carefully.

the dimension of the scheme). Is there any explicit description of these unstable cohomology classes?

4. Special Case: The Cohen–Lenstra Heuristics

The Cohen-Lenstra heuristics – as originally formulated in [4] – are concerned with the average behavior of class groups of quadratic fields; in particular, they try to explain numerical observations such as

$$\mathbf{Z}/9\mathbf{Z} \text{ occurs in class groups more often than } \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}. \tag{11}$$

As we explain, they can be considered a special case of the Bhargava–Malle type conjectures formulated earlier, in the case of dihedral groups. Indeed, (1) establishes one of the few known cases of the Cohen-Lenstra heuristics.

These heuristics are of particular importance because they are readily formulated and relatively easy to investigate numerically.

4.1. Number fields.

For any global field L, denote by C_L the class group. Let $\mathcal{Q}_X$ be the set of imaginary quadratic extensions of $\mathbf{Q}$ with discriminant in $[-X, 0]$. Let ℓ be an odd prime. The Cohen-Lenstra conjecture asserts that, for any finite abelian ℓ-group A,

$$\lim_{X\to\infty} \frac{\sum_{L\in\mathcal{Q}_X} |\mathrm{Epi}(C_L, A)|}{|\mathcal{Q}_X|} = 1. \tag{12}$$

where $\mathrm{Epi}(C_L, A)$ denotes the set of surjective homomorphisms from C_L to A. This implies that[3], for any ℓ-group B, the fraction of $L \in \mathcal{Q}_X$ with $C_L[\ell^\infty] \cong B$ is asymptotically $\frac{\prod_{i=1}^{\infty}(1-\ell^{-i})}{|\mathrm{Aut}(B)|}$. This makes manifest why (11) should be true. But the formulation (12) emphasizes the "rationality" feature of the answer.

Before returning to function fields, let us describe a heuristic for (12) in the spirit of Cohen and Lenstra's original work. The class group of C_L is the quotient of all ideals by principal ideals. If we fix a sufficiently large set of finite places V, C_L will be isomorphic to the quotient of the free group $\mathbf{Z}[V]$ by the image U of the $V \cup \{\infty\}$-units. There are $A^{|V|}$ homomorphisms from $\mathbf{Z}[V]$ to A; the chance that a homomorphism is trivial on U is $|A|^{-\mathrm{rank}\ U}$; since $\mathrm{rank}(U) = |V|$, this suggests (12).

The Cohen-Lenstra heuristics can be viewed as a special case of Malle's conjecture: let $D(A)$ be the group $A \rtimes \mathbf{Z}/2\mathbf{Z}$, where $\mathbf{Z}/2\mathbf{Z}$ acts on A via $a \mapsto -a$, and let c be the set of elements which project to the nontrivial element of $\mathbf{Z}/2\mathbf{Z}$. Then there is a bijection between $D(A)$-extensions of $\mathbf{Q}$, all of whose ramification is of type c, and pairs $(L, f : C_L \twoheadrightarrow A)$, where f is defined only up to ± 1. Thus (12) becomes equivalent to a question of the type considered in §2.

[3] For the implication, see [10] for the case of ℓ-torsion, [9, Corollary 8.2] in general.

4.2. Function fields. Now let k be a finite field of odd cardinality q and let $\mathcal{Q}'_X$ be the set of imaginary[4] quadratic extensions of $k(t)$ with discriminant less than X. The following counting result then follows from the homological stability proved in [9]:

Theorem. *(E. , V., Westerland). Suppose $q \not\equiv 0, 1$ modulo ℓ.*

$$\limsup_{X\to\infty} \frac{\sum_{L\in\mathcal{Q}'_X} |\mathrm{Epi}(C_L, A)|}{|\mathcal{Q}'_X|} = 1 + O(q^{-1/2}), \tag{13}$$

for all q sufficiently large (this notion depending only on A). The same is true for $\liminf$*.*

There is a similar statement [9, Theorem 1.2] concerning the fraction of L for which $C_L[\ell^\infty]$ lies in a specific isomorphism class.

The proof of this theorem is based on the “program” outlined in §3.3 and in particular is a corollary to Theorem of §3.2. As discussed in §3.3, a proof of the *vanishing* conjecture would remove the factor $O(q^{-1/2})$ and show the existence of the limit, as long as q is sufficiently large relative to A.

Remark. The restriction $q \not\equiv 1$ modulo ℓ ensures that k does not contain μ_ℓ. If k contains μ_ℓ, the methods of [9] give a corresponding theorem, but the limit changes, because the pertinent Hurwitz scheme acquires more $\mathbf{F}_q$-rational connected components. A corresponding phenomenon in the number field case has been predicted by Malle [20]. We regard this as an *example* of a Schur correction phenomenon, even though we did not formulate §2.4 in sufficient generality to include dihedral groups. Forthcoming work of Garton [13] will provide an explanation of the phenomena discovered by Malle from the viewpoint of function-field analogies.

References

[1] Manjul Bhargava. Higher composition laws and applications. In *International Congress of Mathematicians. Vol. II*, pages 271–294. Eur. Math. Soc., Zürich, 2006.

[2] Manjul Bhargava. Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants. *Int. Math. Res. Not. IMRN*, (17):Art. ID rnm052, 20, 2007.

[3] H. Cohen. Constructing and counting number fields. In *Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002)*, pages 129–138, Beijing, 2002. Higher Ed. Press.

[4] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups. In *Number theory (New York, 1982)*, volume 1052 of *Lecture Notes in Math.*, pages 26–36. Springer, Berlin, 1984.

[4] That is to say: ramified at ∞.

[5] H. Cohen, F.D. Y Diaz, and M. Olivier. Enumerating Quartic Dihedral Extensions of $\mathbb{Q}$. *Compositio Mathematica*, 133(01):65–93, 2002.

[6] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[7] W. Duke. Bounds for arithmetic multiplicities. In *Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998)*, number Extra Vol. II, pages 163–172 (electronic), 1998.

[8] Nathan M. Dunfield and William P. Thurston. Finite covers of random 3-manifolds. *Invent. Math.*, 166(3):457–521, 2006.

[9] Jordan Ellenberg, Akshay Venkatesh, and Craig Westerland. Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields. `http://arxiv.org/abs/0912.0325`.

[10] Étienne Fouvry and Jürgen Klüners. On the 4-rank of class groups of quadratic number fields. *Invent. Math.*, 167(3):455–513, 2007.

[11] M. Fried. Enhanced review: Serre's Topics in Galois theory. *Proceedings of the Recent developments in the Inverse Galois Problem conference, AMS Cont. Math*, 186:15–32, 1995.

[12] Michael D. Fried and Helmut Völklein. The inverse Galois problem and rational points on moduli spaces. *Math. Ann.*, 290(4):771–800, 1991.

[13] Derek Garton. Random matrices and the Cohen-Lenstra statistics for global fields with roots of unity. UW-Madison Ph.D. thesis, in progress, 2010.

[14] John L. Harer. Stability of the homology of the mapping class groups of orientable surfaces. *Ann. of Math. (2)*, 121(2):215–249, 1985.

[15] Allen Hatcher and Nathalie Wahl. Stabilization for mapping class groups of 3-manifolds. *preprint;* `arXiv:math/0601310`.

[16] John Jones. Table of number fields. `http://hobbes.la.asu.edu/NFDB/`.

[17] Jürgen Klüners. A counterexample to Malle's conjecture on the asymptotics of discriminants. *C. R. Math. Acad. Sci. Paris*, 340(6):411–414, 2005.

[18] Gunter Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002.

[19] Gunter Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004.

[20] Gunter Malle. Cohen-Lenstra heuristic and roots of unity. *J. Number Theory*, 128(10):2823–2835, 2008.

[21] A. M. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. *Sém. Théor. Nombres Bordeaux (2)*, 2(1):119–141, 1990.

[22] David P. Roberts. Density of cubic field discriminants. *Math. Comp.*, 70(236):1699–1705 (electronic), 2001.

[23] Matthieu Romagny and Stefan Wewers. Hurwitz spaces. In *Groupes de Galois arithmétiques et différentiels*, volume 13 of *Sémin. Congr.*, pages 313–341. Soc. Math. France, Paris, 2006.

[24] Jean-Pierre Serre. Revêtements à ramification impaire et thêta-caractéristiques. *C. R. Acad. Sci. Paris Sér. I Math.*, 311(9):547–552, 1990.

[25] Seyfi Türkelli. Connected components of Hurwitz schemes and Malle's conjecture. `http://arxiv.org/abs/0809.0951`, 2008.