ASYMPTOTICS FOR NUMBER FIELDS AND CLASS GROUPS

MELANIE MATCHETT WOOD

Abstract. This article is a exposition of some of the basic questions of arithmetic statistics (counting number fields and distribution of class groups) aimed at readers new to the area. Instead of a thorough treatment of the most general cases, it treats the simplest cases in detailed way, with an emphasis on connections and perspectives that are well-known to experts but absent from the literature.

1. Counting Number Fields

We start by giving an introduction to some of the most basic questions of arithmetic statistics. A number field K is a finite extension of fields $K/\mathbb{Q}$. Associated to a number field is an integer $\operatorname{Disc} X$, its discriminant. (See your favorite algebraic number theory text, or e.g. [Neu99, p. 15].) We have the following classical result

Theorem 1.1 (Hermite's Theorem, see e.g. III.2.16 in [**?**])**.** *Given a positive real number X, there are finitely many number fields K (up to isomorphism, or in a fixed algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$) with $|\operatorname{Disc} K| < X$.*

So the most basic question we can ask is how many are there? Let $D(X)$ be the set of isomorphism classes of number fields K such that $|\operatorname{Disc} K| < X$.

Question 1.2. *What are the asymptotics in X of*

$$N(X) := \#D(X)?$$

Remark 1.3. One can ask a version of this question in which $\mathbb{Q}$ is replaced by any global field, as well, and $\operatorname{Disc} K$ is replaced by the norm of the discriminant ideal.

It turns out that after seeing the heuristics in these talks and perhaps also looking at data, one might conjecture

$$N(X) = cX + o(X)$$

for some constant $c > 0$, but we are a long way from a proof of such a statement.

Notation. Given real-valued functions $f(X)$, $g(X)$, and $h(X)$ on some subset of $\mathbb{R}$ when we write

$$f(X) = g(X) + O(h(X)),$$

we mean that there exists a C such that for every $X \geq 1$ we have

$$|f(x) - g(x)| \leq CX.$$

Given such functions $f(X)$, $g(X)$, and $h(X)$ when we write

$$f(X) = g(X) + o(h(X)),$$

we mean that for every real number $\epsilon > 0$, there exists an N such that for $X > N$, we have

$$|f(X) - g(X)| < \epsilon h(X).$$

When we have $f(X) = g(X) + o(h(X))$ and also $\frac{h(X)}{g(X)} = O(1)$, i.e. $\lim_{X\to\infty} \frac{f(X)}{g(X)} = 1$, then we write

$$f(X) \sim g(X)$$

to denote that $f(X)$ and $g(X)$ are asymptotically equivalent.

One can approach Question 1.2 by filtering the number fields by other invariants.

1.1. **Galois group.** Given a number field K of degree n–not necessarily Galois, with Galois closure $\tilde{K}$ over $\mathbb{Q}$, we define (by a standard abuse of language) the *Galois group of* K, or $\mathrm{Gal}(K)$, to be the permutation group given as the image of

$$\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \to S_n$$

given by the action of the Galois group on the n homomorphisms of K into $\bar{\mathbb{Q}}$. For example if $K = \mathbb{Q}(\theta)$, these n homomorphisms are given by mapping θ to each of its n Galois conjugates in $\bar{\mathbb{Q}}$. The Galois group is well-defined as a permutation group, i.e. up to relabeling the n homomorphisms, or equivalently, conjugation in S_n. Two permutation groups in S_n are isomorphic if they are S_n-conjugate.

Exercise 1.4. Show that the Galois group of a number field is a transitive permutation group, i.e. it has a single orbit on $\{1, 2, \ldots, n\}$.

Exercise 1.5. Show that if K is Galois, then its Galois group as defined above is isomorphic, as a group, to the usual notation of Galois group.

So given a transitive permutation group $\Gamma \subset S_n$, (i.e. a conjugacy class of subgroups of S_n, each with a single orbit), we can ask the following.

Question 1.6. *What are the asymptotics in X of*

$$N_\Gamma(X) := \#\{K \in D(X) \mid \mathrm{Gal}(K) \simeq \Gamma\}?$$

(where $\mathrm{Gal}(K) \simeq \Gamma$ *denotes an isomorphism of permutation groups).*

Note that since Γ determines n, any K with $\mathrm{Gal}(K) \simeq \Gamma$ is necessarily of degree n. Note also that we count fields up to isomorphism, not as subfields of $\bar{\mathbb{Q}}$, so e.g. each isomorphism class of non-Galois cubic field is counted once, not three times.

Remark 1.7. One can of course *ask* these questions, but it should be clear that in general these questions are very hard (for example they contain the inverse Galois problem). In this article we will discuss what one can do towards solving them in some cases.

Exercise 1.8. For each permutation group Γ, determine how $N_\Gamma(X)$ differs from the similar function that counts subfields of $\bar{\mathbb{Q}}$ with Galois group Γ.

Exercise 1.9. For each permutation group Γ, determine how $N_\Gamma(X)$ differs from the similar function that counts elements K of $D(X)$ *with* a choice of isomorphism of $\mathrm{Gal}(K)$ to Γ.

1.2. **Local Behavior.** Given a place p of $\mathbb{Q}$ and a number field K, we can form $K_p := K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ (where $\mathbb{Q}_\infty = \mathbb{R}$).

Exercise 1.10. Prove that K_p is an étale $\mathbb{Q}_p$ algebra, equivalently a direct sum of field extensions of $\mathbb{Q}_p$.

In particular, if $\wp_i$ are the places of K dividing p, then $K_p = \bigoplus_i K_{\wp_i}$. So in particular, we see that the algebra K_p contains the information of the splitting/ramification type of p. The n homomorphisms $K \to \bar{\mathbb{Q}}$ extend to n homomorphisms $K_p \to \bar{\mathbb{Q}}_p$, and we have a map then from the decomposition group $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \subset \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to Γ given by its actions on the n homomorphisms. Let the image of this map be H, as a permutation group, we can define it as $\mathrm{Gal}(K_p)$, the Galois group of the étale algebra (by yet another abuse of language). Note that H is the decomposition subgroup of $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq \Gamma$.

We can also count number fields with a fixed local behavior.

Question 1.11. *Let Γ be a permutation group with sub-permutation group H and let M be an étale K_p algebra with* $\mathrm{Gal}(M) \simeq H$. *What are the asymptotics in X of*

$$N_{\Gamma,M}(X) := \#\{K \in D(X) \mid \mathrm{Gal}(K) \simeq \Gamma, K_p \simeq M, \mathrm{Gal}(K_p) = H\}?$$

Exercise 1.12. I wrote $\mathrm{Gal}(K_p) = H$ to denote that the isomorphism $\mathrm{Gal}(K) \simeq \Gamma$ should induce an isomorphism of $\mathrm{Gal}(K_p)$ onto the precise subgroup H of Γ, not just some other subgroup isomorphic to H. Find a case where this would make a difference.

Question 1.11 then contains for example, the question of counting quadratic number fields that are split completely at 7.

Exercise 1.13. Answer Question 1.11 for the question of counting quadratic number fields that are split completely at 7. Can you extend your method to count non-Galois cubic ($\Gamma = S_3$) fields split completely at 7? What makes this problem harder?

We can further refine Question 1.11 to ask for local conditions at a set of primes (either a finite set of an infinite set).

Exercise 1.14. Answer this refinement for real quadratic fields split completely at 7. Answer this refinement for real quadratic fields split completely at 7 and ramified at 3.

1.3. **Independence.** By dividing the answers to the above questions, we can ask what proportion of number fields (with some Galois structure) have a certain local behavior. It is natural to phrase this proportion as a probability and define

$$\begin{aligned}&\mathbb{P}_{\mathrm{Disc}}(K \text{ with } \mathrm{Gal}(K) \simeq \Gamma \text{ has some local behavior})\\ &= \lim_{X\to\infty} \frac{\#\{K \in D(X) \mid \mathrm{Gal}(K) \simeq \Gamma, K \text{ has that local behavior}\}}{\#\{K \in D(X) \mid \mathrm{Gal}(K) \simeq \Gamma\}}.\end{aligned}$$

This might now remind us of the Chebotarev Density Theorem, which is of similar flavor. That theorem tells us, for example, that if we fix a quadratic field K, then half of the primes of $\mathbb{Q}$ split completely in K and half are inert. We could phrase that as above as a question about a fixed field and a random prime. Note that the probability above is for a *fixed prime* and a *random field*. One thing that makes this version much harder is that it is much harder to enumerate the fields than the primes–with quadratic fields being an exception.

Imagine we make a big chart, listing all the quadratic fields by (absolute value of their) discriminant and all the primes, and marking which split (S), ramify (R), or are inert (I).

⋮	⋮	⋮	⋮	⋮	⋰
$\mathbb{Q}(\sqrt{-7})$	S	I	I	R	⋯
$\mathbb{Q}(\sqrt{5})$	I	I	R	I	⋯
$\mathbb{Q}(i)$	R	I	S	I	⋯
$\mathbb{Q}(\sqrt{-3})$	I	R	I	S	⋯
quad. fields / primes	2	3	5	7	⋯

Above we defined a notion of probability for a random field. Now we do the same for a random prime. For a subset $\mathcal{S}$ of the primes, let

$$\mathbb{P}_p(p \in \mathcal{S}) := \lim_{P\to\infty} \frac{\#\{p \in \mathcal{S} \mid p < P\}}{\#\{p \text{ prime } \mid p < P\}}.$$

The Chebotarev density theorem (or simply Dirchlet's theorem on primes in arithmetic progressions plus quadratic reciprocity) tells us that for each quadratic field K

$$\mathbb{P}_p(p \text{ prime, splits in } K) = 1/2$$
$$\mathbb{P}_p(p \text{ prime, inert in } K) = 1/2$$
$$\mathbb{P}_p(p \text{ prime, ramifies in } K) = 0.$$

This says, in each row of the chart, if we go out far enough to the right, about half the entries are S and have are I. If we ask for $\mathbb{P}_{\text{Disc}}(7 \text{ splits})$, that is asking in the 7th column of the chart, as we look far enough up, what proportion of S's do we get. We can do a simple calculation to see that in $\mathbb{P}_{\text{Disc}}$ there is a *positive* probability of ramification, in contrast to the Chebotarev Density Theorem. So for example we have (as the result of a slightly more complicated but classical calculation, like the exercise above)

$$\begin{aligned}
&\mathbb{P}_{\text{Disc}}(K \text{ with } \operatorname{Gal}(K) \simeq S_2 \text{ splits completely at } 7) && = 7/16\\
&\mathbb{P}_{\text{Disc}}(K \text{ with } \operatorname{Gal}(K) \simeq S_2 \text{ inert at } 7) && = 7/16\\
&\mathbb{P}_{\text{Disc}}(K \text{ with } \operatorname{Gal}(K) \simeq S_2 \text{ ramified at } 7) && = 1/8.
\end{aligned}$$

If we condition on K being unramified, in this case we do obtain the "same probabilities" as in the Chebotarev Density Theorem. We will see this in other cases below, and in generality for abelian extensions in Theorem 9.1.

Note that $\mathbb{P}_{\text{Disc}}$ and $\mathbb{P}_p$ are not probability measures in the usual sense (perhaps more precisely they are "asymptotic probabilities") because they are not always countably additive. However, it is a useful piece of language here, because it lets us phrase the following important question.

Question 1.15. *For a finite set of distinct places, are probabilities of local behaviors independent at those places?*

It is interesting to compare this to the Chebotarev version. Suppose we look in two rows of the above chart. How often do we see

$$\begin{array}{cccc} S & \text{vs. } S & \text{vs. } I & \text{vs. } I \\ S & I & S & I? \end{array}$$

If the two rows were independent, then we would see each of these possibilities 1/4 of the time, asymptotically. Indeed, we can see that is the case by applying the Chebotarev density theorem to the composite of the two quadratic fields.

Exercise 1.16. Do that application of the Chebotarev density theorem.

More generally, the Chebotarev density theorem tells us that even if we included all Galois number fields in our list on the left of our chart, two rows are independent if they correspond to number fields K, L that do not contain a common subfield larger than $\mathbb{Q}$. For example, we have the following.

Proposition 1.17. *Let $K, L \subset \bar{\mathbb{Q}}$ be Galois number fields. Then for a random rational prime p the events "p splits completely in K" and "p splits completely in L" are independent, i.e.*

$$\mathbb{P}_p(p \textit{ splits completely in } K)\mathbb{P}_p(p \textit{ splits completely in } L) = \mathbb{P}_p(p \textit{ splits completely in } K \textit{ and } L),$$

if and only if $K \cap L = \mathbb{Q}$.

Proof. By the Chebotarev Density Theorem, for a Galois number field F we have

$$\mathbb{P}_p(p \text{ splits completely in } F) = [F : \mathbb{Q}]^{-1}.$$

We have, since K is Galois, $[K : \mathbb{Q}][L : \mathbb{Q}] = [KL : \mathbb{Q}]$ if and only if $K \cap L = \mathbb{Q}$. □

Exercise 1.18. Prove the analog of Proposition 1.17 for other local behaviors besides "splits completely."

If K and L are not Galois, the question of independence is more subtle (see, e.g. the notion of Kronecker equivalence in [Kli98, Chapter 2]). If K, L do contain a common subfield F larger than $\mathbb{Q}$, then it is easy to understand heuristically that the rows should not be independent because they both have a dependence on local behaviors in F. One can moreover see that the common subfield exactly accounts for the dependence as in the following.

Proposition 1.19. *Let $K, L \subset \bar{\mathbb{Q}}$ be Galois number fields. Then for a random rational prime p, conditional on p's splitting type in $K \cap L$, the events "p splits completely in K" and "p splits completely in L" are independent, i.e.*

$$\begin{aligned} &\mathbb{P}_p(p \textit{ splits completely in } K | p \textit{ splits completely in } K \cap L) \\ &\cdot\mathbb{P}_p(p \textit{ splits completely in } L | p \textit{ splits completely in } K \cap L) \\ = &\mathbb{P}_p(p \textit{ splits completely in } K \textit{ and } L | p \textit{ splits completely in } K \cap L). \end{aligned}$$

Proof. We have

$$\mathbb{P}_p(p \text{ splits completely in } K | p \text{ splits completely in } K \cap L) = [K : \mathbb{Q}]^{-1}[K \cap L : \mathbb{Q}],$$

and similarly for the other two conditional probabilities. Since K is Galois, $[K : \mathbb{Q}]^{-1}[K \cap L : \mathbb{Q}][L : \mathbb{Q}]^{-1}[K \cap L : \mathbb{Q}] = [KL : \mathbb{Q}]^{-1}[K \cap L : \mathbb{Q}]$. □

We can prove the analogous fact for any local behaviors. So the dependence of two rows for K and L is determined by whether K and L have a subfield in common. You can try to imagine what the analog should be for primes. What should be analogous for primes, to two fields containing a common subfield?

Exercise 1.20. What is the probability that a quadratic field is split completely at 3? at 5? at 3 and 5? is there independence? What more general statement along these lines can you prove for quadratic fields?

2. Counting class groups

Similarly, we can ask what proportion of number fields have a certain class group behavior. Here, even phrasing the right question in the most general case is complicated, so we will start with the simplest case.

Question 2.1. *Given an odd prime p and a finite abelian p-group G, what proportion of imaginary quadratic number fields K, ordered by discriminant, have $Cl(K)_p$ (denoting the Sylow p-subgroup of the class group) isomorphic to G, i.e. what is the limit*

$$\lim_{X\to\infty} \frac{\#\{K \in D(X) \mid K imag\ quad, Cl(K)_p \simeq G\}}{\#\{K \in D(X) \mid K imag\ quad\}}$$

if it exists?

The answer to this question is not known for any G.

Exercise 2.2. Let G be a finite abelian group. What are the asymptotics of the number of imaginary quadratic number fields up to discriminant X with class group isomorphic to G? Can you see why we restrict to the Sylow p-subgroup in Question 2.1?

We can also ask for various averages of the class groups of number fields.

Question 2.3. *Given an odd prime p, what are the limits, if they exist:*

$$\lim_{X\to\infty} \frac{\sum_{K\in D(X) K imag\ quad} |Cl(K)/pCl(K)|}{\#\{K \in D(X) \mid K imag\ quad\}}? \qquad \textit{(average size of } p\textit{-torsion)} \tag{1}$$

$$\lim_{X\to\infty} \frac{\sum_{K\in D(X) K imag\ quad} |Cl(K)/pCl(K)|^k}{\#\{K \in D(X) \mid K imag\ quad\}}? \qquad \textit{(} k\textit{-th moment of } p\textit{-torsion)} \tag{2}$$

$$\lim_{X\to\infty} \frac{\sum_{K\in D(X) K imag\ quad} |\operatorname{Sur}(Cl(K), A)|}{\#\{K \in D(X) \mid K imag\ quad\}}? \qquad \textit{(} A\textit{-th moment),} \tag{3}$$

where A is a finite odd abelian group and Sur *denotes surjections.*

Note that the denominators here are examples of the kind of counting number field functions we considered above (but in an example we can answer!).

Exercise 2.4. If $p = 2$, what is the answer to Equation 1? (Hint: learn about genus theory if you haven't already.)

Exercise 2.5. Can you relate the case $A = (\mathbb{Z}/p\mathbb{Z})^m$ of Equation 3 to Equation 2? (Hint: first try the analog of Equation 3 for homomorphisms instead of surjections. Can you say how many homomorphisms a finite abelian group G has to $(\mathbb{Z}/p\mathbb{Z})^m$ in terms of the size of the p-torsion of G? Then use the fact that homomorphisms are all surjections on to their image.)

One might hope that if you knew the answer to Question 2.1 for every G, then you could average over G to obtain the answers to Question 2.3. However, one cannot switch the sum over G with the limit in X without an argument, of which none has been suggested (if you know one, let me know!).

Questions of the form (3) are the most natural to approach from a certain angle, and in fact the $A = \mathbb{Z}/3\mathbb{Z}$ case (which is also the $p = 3$ case of (1)) is a theorem of Davenport and Heilbronn that we will discuss.

3. Relation between counting number fields and class groups statistics

The questions discussed above, of counting number fields and averages for class groups, are in fact deeply intertwined. We give the first example of their relationship. Let K be an imaginary quadratic field. Then surjections from $Cl(K)$ to $\mathbb{Z}/3\mathbb{Z}$, by class field theory, correspond to unramified $\mathbb{Z}/3\mathbb{Z}$-extensions L of K with an isomorphism $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z}$. Also by class field theory, we can show that such an L is necessarily Galois over $\mathbb{Q}$, with Galois group S_3. So for each imaginary quadratic K, we have a bijection

$$\mathrm{Sur}(Cl(K), \mathbb{Z}/3\mathbb{Z}) \leftrightarrow \{L/K \text{ unramified}, \phi : \mathrm{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z}\}$$

and all L appearing on the right are Galois over $\mathbb{Q}$ with Galois group S_3.

Exercise 3.1. Show it.

Conversely, let $L/\mathbb{Q}$ be a S_3 Galois sextic field (so with Galois group $S_3 \subset S_6$ via the regular representation) with quadratic subfield K, such that K is imaginary, and L/K is unramified. Then we have two corresponding surjections from $Cl(K)$ to $\mathbb{Z}/3\mathbb{Z}$. So, counting surjections from $Cl(K)$ to $\mathbb{Z}/3\mathbb{Z}$ for imaginary quadratic fields K, is the same (up to a multiple of 2) as counting S_3 cubic fields that are unramified over their quadratic subfields (that are also imaginary). And since L/K is unramified $|\operatorname{Disc} L| = |\operatorname{Disc} K|^3$. The condition that the quadratic subfield of L is imaginary is a condition on L_∞, and the condition that L is unramified over its quadratic subfield is a condition on L_p for every p.

So we see here how the class group average of (3) is related to a question of counting S_3 Galois sextic number fields with local conditions (at all primes). This was first explained by Hasse [Has30]. (In particular, we now see the numerator is a question of this flavor. We already noted the denominator was a question of counting number fields.) We can further translate the class group average to an even simpler question of counting number fields. A Galois sextic S_3-field corresponds to exactly one non-Galois cubic field, up to isomorphism (of which it is the Galois closure). So the question of counting $S_3 \subset S_6$ sextic extensions is equivalent to counting S_3 cubic extensions. In general, it is delicate to relate the discriminant of the non-Galois cubics and the discriminant of their Galois closure (we will discuss this further below), but in this case, the local conditions we are imposing make the relationship simple.

Exercise 3.2. What are the different possible ramification types of a prime p in a non-Galois cubic field K_3? Can you tell from the ramification type whether the Galois closure $\tilde{K_3}$ is ramified over its quadratic subfield? How? If $\tilde{K_3}$ is unramified over its quadratic subfield, how are $\operatorname{Disc}\tilde{K_3}$ and $\operatorname{Disc} K_3$ related?

Exercise 3.3. Can you tell from $K_3 \otimes_{\mathbb{Q}} \mathbb{R}$ if the quadratic subfield of $\tilde{K_3}$ is imaginary? How?

Exercise 3.4. Do the same translation of the class group average question (3) to a question of counting number fields with local conditions for an arbitrary finite abelian group A.

This relationship to counting number fields is one reason that the A-moments of (3) are a particularly nice class group statistic. (We will see another reason later.) See [Klü06] for a more indepth discussion and results explaining the connections between asymptotics of number fields and averages of class groups.

4. Different counting invariants

So far in this entire discussion we have *ordered by discriminant*, i.e. counted number fields of discriminant up to X asymptotically in X. We could replace discriminant by other real valued invariants and ask the same questions. We will see below how this can change the answers, both quantitatively and qualitatively.

In fact, some of the questions we have already asked about counting number fields ordered by discriminant can be seen as a question of counting other number fields ordered by a different counting invariant. For example, the question of counting all $S_3 \subset S_6$ sextic extensions by discriminant is equivalent to counting S_3 cubic extensions by the discriminant of their Galois closure, which without the local conditions imposed in the last chapter, is truly a different counting invariant.

5. Cohen-Lenstra heuristics

We will discuss heuristics (conjectural answers) for the questions we have considered so far, starting with the class group question. The Cohen-Lenstra heuristics start from the observation that structures often occur in nature with frequency inversely proportional to their number of automorphisms.

Exercise 5.1. Consider a graph G on n vertices. Of the 2^n graphs on n labeled vertices ("nature"–you might imagine the vertices are n computers actually out there in the world, and we are considering all possible network structures between them) how many are isomorphic to G?

Exercise 5.2. Consider all multiplication tables on n elements $a_1, ..., a_n$ that satisfy the group axioms. How many are isomorphic to a given group G of order n?

Exercise 5.3. Fix a degree n number field K. Consider all subfields of $\bar{\mathbb{Q}}$ with degree n over $\mathbb{Q}$–how many of these are isomorphic to K?

Now that you are convinced of this principle, the idea of the Cohen-Lenstra heuristics is that for odd p, the group $Cl(K)_p$ is a finite abelian p-group occurring in nature, that we know nothing else about, so we will guess it is distributed in this same way. (For $p = 2$, when K is imaginary quadratic, genus theory tells us something about the form of $Cl(K)_2$, or more precisely about $Cl(K)_2/2Cl(K)_2$, but nothing about $2Cl(K)_2$, so as suggested by

Gerth we can make the same guess for $2Cl(K)_2$.) Let $G(n)$ be the set of all finite abelian groups of order n.

Conjecture 5.4 ([CL84], $p = 2$ part from [Ger87a, Ger87b])**.** *For any "reasonable" function f on finite abelian groups we have*

$$\lim_{X\to\infty} \frac{\sum_{K\in D(X) K imag\ quad} |f(2Cl(K))|}{\#\{K \in D(X) \mid K imag\ quad\}} = \lim_{n\to\infty} \frac{\sum_{i=1}^{n} \sum_{G\in G(i)} \frac{f(G)}{\#\operatorname{Aut}(G)}}{\sum_{i=1}^{n} \sum_{G\in G(i)} \frac{1}{\#\operatorname{Aut}(G)}}.$$

I expect that we should interpret this as saying not that both limits exist, but that either both limits do not exist, or they both exist and are equal. Of course, everything hangs on what "reasonable" means. Cohen and Lenstra [CL84] said that "reasonable" should probably include all non-negative functions, but Poonen pointed out to me that it may not make sense to include all non-negative functions as "reasonable". See page 22 of [BKLj$^+$13] for one idea of what one might include as "reasonable". The main examples that Cohen and Lenstra in [CL84] apply their conjecture to are f that only depend on the Sylow p-subgroups of G for finitely many p (which most people think should be "reasonable", [BKLj$^+$13] agrees), and f the characteristic function of cyclic groups (which is not in the class of "reasonable" functions considered in [BKLj$^+$13]).

Notably, Conjecture 5.4 is known for almost no non-trivial f. One exception is when $f = \#\operatorname{Sur}(-, \mathbb{Z}/3\mathbb{Z})$, in which case Conjecture 5.4 is known by Davenport and Heilbronn's work [DH71] (discussed in depth below) on counting cubic fields (see Section 3 for the connection to counting cubic fields). This result, of course, predates the conjecture. The other exception is Fouvry and Klüners results [FK06a, FK06b] that show Conjecture 5.4 when $f = \#\operatorname{Sur}(-, (\mathbb{Z}/2\mathbb{Z})^k)$ or f is the indicator function of having a particular 2-rank, confirming conjectures of Gerth [Ger87a, Ger87b].

In order words, the class group average equals the Aut^{-1} weighted group average. We define, if it exists,

$$M(f) := \lim_{n\to\infty} \frac{\sum_{i=1}^{n} \sum_{G\in G(n)} \frac{f(G)}{\#\operatorname{Aut}(G)}}{\sum_{i=1}^{n} \sum_{G\in G(i)} \frac{1}{\#\operatorname{Aut}(G)}}$$

(the right-hand side of Conjecture 5.4).

It is useful to know (see exercises above or Section 8) that the denominator on the left hand side of Conjecture 5.4 is $\sim \frac{6}{\pi^2}X$.

Exercise 5.5. Show that

$$\lim_{n\to\infty} \sum_{i=1}^{n} \sum_{G\in G(n)} \frac{1}{\#\operatorname{Aut}(G)} = \infty.$$

In particular, then, Conjecture 5.4 implies that each group G appears as a class group of imaginary quadratic fields asymptotically 0% of the time. In fact, it was first shown by Heilbronn [Hei34] that each group G appears as a class group of an imaginary quadratic field only finitely many times.

Cohen and Lenstra in [CL84] compute the right-hand side of Conjecture 5.4 for many interesting functions f (which is purely a problem in "finite group theory statistics" instead of "arithmetic statistics"). If f is the indicator function of cyclic groups they show

$$M(f) \approx .977575.$$

Given an odd prime p, if f is the indicator function for when $p \mid \#G$, then

$$M(f) = 1 - \prod_{i \geq 1}(1 - p^{-i}),$$

and for $p = 3$ this is $\approx .43987$. Perhaps most striking is the following, which follows from combining lemmas of [CL84] but is not highlighted by them.

Proposition 5.6. *If A is a finite abelian group and $f(G) = \# \operatorname{Sur}(G, A)$, then*

$$M(f) = 1.$$

So the Cohen-Lenstra heuristics suggest that the expected number of surjections from an imaginary quadratic class group to A is 1, regardless of the group A. We saw above, these A-moments were related to questions of counting number fields, and now we see they have particularly nice predicted values. (See also Ellenberg's 2014 Arizona Winter School lectures for more on the interpretation of these moments in the function field analog.)

Note that $f(G) = \# \operatorname{Sur}(G, A)$ only depends on finitely many Sylow-p subgroups of G. Let P be a finite set of primes, and let G_P be the sum of the Sylow p-subgroups of G for $p \in P$. Let $G_P(n)$ be the set of finite abelian groups G of order n such that $G = G_P$.

Proposition 5.7 ([CL84])**.** *Let P be a finite set of primes. Let f be a function depending on only the Sylow-p subgroups of G for $p \in P$. Then*

$$\lim_{n \to \infty} \sum_{i=1}^{n} \sum_{G \in G_P(i)} \frac{1}{\# \operatorname{Aut}(G)} = \prod_{p \in P} \prod_{i \geq 1} (1 - p^{-i})^{-1} =: c_P,$$

and

$$M(f) = \frac{\sum_{i=1}^{\infty} \sum_{G \in G_P(i)} \frac{f(G)}{\# \operatorname{Aut}(G)}}{c_P}.$$

Exercise 5.8. If F is the indicator function for groups that have cyclic Sylow 3-subgroup and cyclic Sylow 5-subgroup, compute $M(f)$.

5.1. **Further class group heuristics.** We have only discussed conjectures for class groups of imaginary quadratic fields. There are conjectures for much more general situations. Cohen and Lenstra [CL84] also formulate precise conjectures for real quadratic class groups, and more generally for class groups of totally real number fields with some fixed abelian Galois group. Cohen and Martinet [CM90] further extended these conjectures to arbitrary extensions of an arbitrary global field. It is in general a subtle question for which primes p the general form of the conjecture can be made for $Cl(K)_p$ (e.g. all odd primes in the imaginary quadratic case). See [CM94, Mal08, Mal10, Gar14, AM15] for work on this question, and further modifications of the conjecture for p where the base field contains pth roots of unity. In all of these cases, the conjectures are based on the same sort of principles as those above, but are modified to take into account further information about the fields.

6. Galois permutation representations

In order to formulate the conjectures for counting number fields, it is useful to translate from the language of number fields to Galois (permutation) representations. For a field F, let $G_F := \operatorname{Gal}(\bar{F}/F)$, the Galois group of a separable closure of F (if $charF = 0$ then $\bar{F}$ is equivalently an algebraic closure of F). An étale F-algebra is a direct sum of finitely many finite separable field extensions of F. Two étale F-algebras are isomorphic if they are isomorphic as algebras. The degree of an étale algebra is its dimension as an F-vector space, or equivalently the sum of the degrees of the field extensions. Then given a permutation representation, i.e. a continuous homomorphism

$$G_F \to S_n,$$

we can pick representatives $a_i \in \{1, \dots, n\}$ of the orbits, and let $H_i = \mathrm{Stab}(a_i) \subset G_F$. If K_i is the fixed field of H_i, then we can form an étale F-algebra $\bigoplus_i K_i$. Conversely, given an étale F-algebra $M = \bigoplus_i K_i$, where K_i/F are finite, separable field extensions whose degrees sum to n, we have an action of G_F on the n homomorphisms $M \to \bar{F}$, which gives a permutation representation of G_F. We say two permutation representations are isomorphic if they differ by relabeling the n elements, i.e. by conjugacy in S_n.

Proposition 6.1. *The above constructions gives a bijection between isomorphism classes of permutation representations $G_F \to S_n$ and isomorphism classes of degree n étale F-algebras. In this bijection, transitive permutation representations correspond to field extensions of F.*

Exercise 6.2. Proof the above proposition.

Exercise 6.3. If we restrict $G_{\mathbb{Q}} \to S_n$ (corresponding to a field extension $K/\mathbb{Q}$) to a decomposition group $G_{\mathbb{Q}_p} \to S_n$, show that K_p is the étale algebra corresponding to $G_{\mathbb{Q}_p} \to S_n$.

We will now consider the case when $F = \mathbb{Q}$. Fix a transitive permutation group $\Gamma \subset S_n$. We will be interested in counting $\rho : G_{\mathbb{Q}} \to \Gamma$, whose corresponding field extension K has $|\operatorname{Disc} K| < X$. We define $\operatorname{Disc} \rho := |\operatorname{Disc} K|$. If we factor $|\operatorname{Disc} K| = \prod_i p_i^{e_i}$ with p_i distinct primes, then recall that the ideal $(\operatorname{Disc} K_{p_i}/\mathbb{Q}_{p_i}) = (p_i)^{e_i}$. Further, it we write K_{p_i} as a direct sum of field extensions K_j then $(\prod_j \operatorname{Disc} K_j/\mathbb{Q}_{p_i}) = (\operatorname{Disc} K_{p_i}/\mathbb{Q}_{p_i})$. For an étale $\mathbb{Q}_p$-algebra M, we define $d(M)$ to be the discriminant exponent so that $(\operatorname{Disc} M) = (p)^{d(M)}$. If M corresponds to $\rho_p : \mathbb{G}_{\bar{\mathbb{Q}}_p} \to S_n$, we define $\operatorname{Disc} \rho_p = p^{d(M)}$.

For an étale $\mathbb{Q}_p$-algebra M associated to $\rho : G_{\bar{\mathbb{Q}}_p} \to S_n$, recall that $d(M)$ is the Artin conductor of the composition of ρ with the permutation representation $S_n \to \mathrm{GL}_n(\mathbb{C})$. This allows us to compute $d(M)$. For example, we have the following.

Lemma 6.4. *If $M/\mathbb{Q}_p$ is a tame étale extension corresponding to $\rho : G_{\bar{\mathbb{Q}}_p} \to S_n$, and y is a generator of tame inertia (i.e. a generator of the quotient of the inertia subgroup by its unique pro-p-Sylow subgroup) in $G_{\bar{\mathbb{Q}}_p}$, and c is the number of cycles in $\rho(y)$, then*

$$d(M) = n - c.$$

Exercise 6.5. Prove this lemma.

7. Tauberian theorem

Before we get to the conjectures about counting number fields, we will review an important tool in asymptotic counting. We give an example of a Tauberian theorem, which can be found as Corollary p. 121 of [Nar83].

Theorem 7.1. *Let $f(s) = \sum_{n \geq 1} a_n n^{-s}$ with $a_n \geq 0$ be convergent for $\Re s > a > 0$. Assume that in the domain of convergence $f(s) = g(s)(s-a)^{-w} + h(s)$ holds, where $g(s), h(s)$ are* *holomorphic functions in the closed half plane $\Re s \geq a$, and $g(a) \neq 0$, and $w > 0$. Then*

$$\sum_{1 \leq n \leq X} a_n = \frac{g(a)}{a\Gamma(w)} x^a (\log x)^{w-1} + o(x^a (\log x)^{w-1}).$$

For example, if $f(s)$ converges for $\Re(s) > 1$ and has a meromorphic continuation to $\Re(s) \geq 1$ with a simple pole at $s = 1$ with residue r, then

$$\sum_{1 \leq n \leq X} a_n = rX + o(X).$$

Upon seeing Theorem 7.1, you might think whenever you are counting something asymptotically, you should just make it into a Dirichlet series and study the pole behavior of the function. However, it should be emphasized that in order to gain any traction with this method one must *produce an analytic continuation* of $f(s)$ beyond where the Dirichlet series converges. In general, producing such an analytic continuation can be as hard as any question in mathematics (e.g. one defines the L function of an elliptic curve as a Dirichlet series, and the analytic continuation is a consequence of the modularity theorem, used, for example, in the proof of Fermat's Last Theorem–and that's a case where you have the benefit of the Langlands program telling you where the analytic continuation should come from!). Even if you produce an analytic continuation it may be very non-trivial to understand its rightmost poles (e.g. this is the case when counting quintic number fields by discriminant). Nonetheless, this is a tool that can help us understand some asymptotic counting questions, and it gives us a framework for thinking about the questions that we can't answer.

8. Counting abelian number fields

We will next apply our Tauberian theorem to count some abelian number fields. The results in this section will be special cases of more general results which we will cite more properly in the next section.

Let $J_{\mathbb{Q}}$ be the idèle class group of $\mathbb{Q}$, so

$$J_{\mathbb{Q}} = \left({\prod_p}' \mathbb{Q}_p^* \right) / \mathbb{Q}^*$$

where the product is over places p of $\mathbb{Q}$, and the product is restricted so that an element of $J_{\mathbb{Q}}$ must have all but finitely many terms as units $\mathbb{Z}_p^*$ in the local ring of integers.

We will first consider quadratic extensions. Though these can be approached more directly, the advantage of our method is that it, with enough work, will generalize to any abelian group. Class field theory tells us that the abelianization $G_{\mathbb{Q}}^{ab}$ is isomorphic, as a topological group to the profinite completition $\widehat{J_{\mathbb{Q}}}$, and in particular that continuous homomorphisms

$$G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$$

correspond exactly to continuous homomorphisms

$$J_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}.$$

So, we will focus on maps $\phi : J_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$. Note that ϕ restricts to a map

$$\phi_0 : \prod_p \mathbb{Z}_p^* \to \mathbb{Z}/2\mathbb{Z},$$

where we use $\mathbb{Z}_\infty$ to denote the positive real numbers. Moreover, we will see that any such ϕ_0 extends to a unique $\phi : J_\mathbb{Q} \to \mathbb{Z}/2\mathbb{Z}$. Given ϕ_0, to define an extension we must define $\phi(1, \dots, 1, p, 1, \dots)$ (where the p is in the p place), and we see that the quotient by $\mathbb{Q}^*$ forces

$$\phi(1, \dots, 1, p, 1, \dots) = \phi(p^{-1}, \dots, p^{-1}, 1, p^{-1}, \dots) = \phi_0(p^{-1}, \dots, p^{-1}, 1, p^{-1}, \dots).$$

Similarly, for $\phi(1, \dots, -1)$ (with a 1 in every finite place),

$$\phi(1, \dots, -1) = \phi(-1, \dots, 1) = \phi_0(-1, \dots, 1).$$

So we conclude that ϕ is determined by ϕ_0. Moreover, for any ϕ_0, we can check that the above construction gives a well-defined ϕ.

Moreover, we can compute $\operatorname{Disc} \phi$ (defined to be the discriminant of the corresponding Galois representation to S_2) in terms of ϕ_0. In our map $\phi : J_\mathbb{Q} \to \mathbb{Z}/2\mathbb{Z}$, the image of the decomposition group at p is the image of $\mathbb{Q}_p^*$ and the inertia group is the image of $\mathbb{Z}_p^*$. In particular, since the discriminant (viewed as an Artin conductor) only depends on the inertia group, we see that we can recover $\operatorname{Disc} \phi$ from ϕ_0.

What are the maps $\mathbb{Z}_p^* \to \mathbb{Z}/2\mathbb{Z}$? Since the kernel of the map $\mathbb{Z}_p^* \to (\mathbb{Z}/p\mathbb{Z})^*$ is pro-p, for p odd, a map $\mathbb{Z}_p^* \to \mathbb{Z}/2\mathbb{Z}$ must factor through $(\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Z}/2\mathbb{Z}$. There are of course 2 such maps, depending on whether a generator is sent to 1 or 0. When $p = 2$, a map $\mathbb{Z}_p^* \to \mathbb{Z}/2\mathbb{Z}$ factors through

$$\mathbb{Z}_2^* \to (\mathbb{Z}/8\mathbb{Z})^* \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$$

(to conclude this, one must understand the structure of $\mathbb{Z}_2^*$ as a profinite group). In particular, there are four maps $\mathbb{Z}_2^* \to \mathbb{Z}/2\mathbb{Z}$.

Given a map $\mathbb{Z}_p^* \to \mathbb{Z}/2\mathbb{Z}$, how do we compute the discriminant? One approach is to use the conductor-discriminant formula. This requires knowing the conductor of the map $\mathbb{Z}_p^* \to \mathbb{Z}/2\mathbb{Z}$, which is k where p^k is minimal such that the map factors through $(\mathbb{Z}/p^k\mathbb{Z})^*$.

Exercise 8.1. Show that $\operatorname{Disc} \rho$ for the $\rho : \mathbb{Q}_p^* \to \mathbb{Z}/2\mathbb{Z}$ restricting to the $\mathbb{Z}_p^* \to \mathbb{Z}/2\mathbb{Z}$ discussed above are $1, p$ for odd p, and $1, 2^2, 2^3, 2^3$ for $p = 2$.

So, if a_n is the number of continuous homomorphisms $\rho : G_\mathbb{Q} \to \mathbb{Z}/2\mathbb{Z}$ with $\operatorname{Disc} \rho = n$, we have

$$f(s) = \sum_{n \geq 1} a_n n^{-s} = (1 + 2^{-2s} + 2 \cdot 2^{-3s}) \prod_{p \text{ odd prime}} (1 + p^{-s}).$$

We note that

$$f(s) = h(s) \frac{\zeta(s)}{\zeta(2s)},$$

where $h(s) = (1 + 2^{-2s} + 2 \cdot 2^{-3s})/(1 + 2^{-s})$ and $\zeta(s) = \sum_{n \geq 1} n^{-s}$. In particular, we can apply Theorem 7.1. Since the residue of $f(s)$ at $s = 1$ is $\zeta(2)^{-1} = 6/\pi^2$, we have that

$$N_{S_2}(X) \sim \frac{6}{\pi^2} X.$$

(There is a single non-surjective $\rho : G_\mathbb{Q} \to \mathbb{Z}/2\mathbb{Z}$ so this doesn't affect the asymptotics.) So we have counted, you might say the long way around, quadratic extensions by discriminant. (Such a result is of course classical.)

An important feature of our approach is that it works more generally. Suppose we want to count cyclic cubic fields (as was done by Cohn [Coh54] in the same way as we will do). Each field corresponds to 2 surjective maps $\mathbb{G}_\mathbb{Q} \to \mathbb{Z}/3\mathbb{Z} \subset S_3$. Let a_n be the number of continuous homomorphisms $\rho : G_{\mathbb{Q}} \to \mathbb{Z}/3\mathbb{Z}$ with $\operatorname{Disc}\rho = n$, then by a similar analysis to the above we have

$$f(s) = \sum_{n\geq 1} a_n n^{-s} = (1 + 2 \cdot 3^{-4s}) \prod_{p\equiv 1 \pmod 3 \text{ prime}} (1 + 2p^{-2s}).$$

We can show that the function $f(s)$ has rightmost pole at $s = 1/2$, where it has a simple pole. Let χ be a Dirichlet character modulo 3 such that $\chi(1) = 1$ and $\chi(2) = -1$. Then note that

$$\prod_{p \text{ prime, not } 3} (1 + p^{-2s}) \prod_{p \text{ prime, not } 3} (1 + \chi(p)p^{-2s})$$
$$= \prod_{p\equiv 1 \pmod 3 \text{ prime}} (1 + 2p^{-2s} + p^{-4s}) \prod_{p\equiv 2 \pmod 3 \text{ prime}} (1 - p^{-4s}).$$

By comparison to $\zeta(2s)$ and $L(2s, \chi)$, the top has rightmost pole a simple pole at $s = 1/2$. We can see that the bottom has the same pole behavior as $f(s)$ to $s = 1/2$. We conclude the result of Cohn [Coh54]

$$N_{\mathbb{Z}/3\subset S_3}(X) \sim \frac{1}{2} \lim_{s\mapsto^+ 1/2} (1 + 2 \cdot 3^{-4s}) \prod_{p\equiv 1 \pmod 3 \text{ prime}} (1 + 2p^{-2s})\zeta(2s)^{-1}X^{1/2}, \tag{4}$$

where the limit in s is a constant.

Note here, the main input, after we have applied class field theory in the set-up above, is to find appropriate L functions to compare our Dirichlet series with so that we can analyze the pole behavior and get analytic continuation so as to apply Theorem 7.1. However, so far we are counting all maps $\mathbb{G}_{\mathbb{Q}} \to G$, and when G is not $\mathbb{Z}/\ell$ for some prime ℓ, there will be more than 1 non-surjective map to subtract. We will come back to this issue.

8.1. **Local conditions.** Let's go back to considering $\rho : \mathbb{G}_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$. What if we wanted to impose local conditions Σ such that 3 was split completely? Taylor [Tay84] attributes the question of the distribution of splitting types of a given prime in random G-extensions to Fröhlich, who was motivated by the work of Davenport and Heilbronn [DH71]. We discuss work of Taylor [Tay84] and the author [Woo10] on this question below.

Since in the isomorphism $\mathbb{G}_{\mathbb{Q}_p}^{ab} \simeq \widehat{\mathbb{Q}_p^*}$ of class field theory, we have that $\mathrm{Frob}_p \mapsto p$, this is equivalent to counting $\rho : J_{\mathbb{Q}} \to \mathbb{Z}/2$ such that $\rho(1, 3, 1, \dots) = 0$ (where the 3 is in the $\mathbb{Q}_3$ place). Since we have that $\rho(1, 3, 1, \dots) = \rho(3, 1, 3, \dots)$, we can check this just from the maps from $\mathbb{Z}_p^*$. Where does a local map $\chi : \mathbb{Q}_p^* \to \mathbb{Z}/2$ send 3 when p is not 3? If χ is trivial, then $\chi(3) = 1$. If p is odd and χ is not trivial, then $\chi(p) = 0$ if 3 is a square mod p and $\chi(p) = 1$ if 3 is not a square mod p. Let Ψ be the Dirichlet character that is 1 on odd primes p such that 3 is a square mod p and -1 on odd primes p such that 3 is not a square (which exists and is of modulus 12 by quadratic reciprocity).

Let b_n be the number of continuous homomorphisms $\rho : G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$ with $\operatorname{Disc} \rho = n$ and sending $(1, 3, 1, \dots)$ to 0. Then

$$g(s) = \sum_{n \geq 1} b_n n^{-s}$$
$$= \frac{1}{2}\left((1 + 2^{-2s} + 2 \cdot 2^{-3s}) \prod_{p \text{ odd prime}} (1 + p^{-s}) + (1 - 2^{-2s})(1 + 3^{-s}) \prod_{p \text{ prime}>5} (1 + \Psi(p)p^{-s})\right).$$

The first term counts all $\rho : G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$ with coefficient 1. The second counts $\rho : G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$ that send $(3, 1, 3, \dots) \mapsto 0$ with coefficient 1 and those that send $(3, 1, 3, \dots) \mapsto 1$ with coefficient -1. (We have checked at $p = 2$ that the discriminant 2^2 map sends $3 \mapsto 1$ and of the two discriminant 2^3 maps, one sends $3 \mapsto 1$ and one $3 \mapsto 0$.) We will compare g to the L-function

$$L(s, \Psi) = \prod_{p \text{ prime}} (1 - \Psi(p)p^{-s})^{-1}.$$

We have that

$$g(s) = \frac{1}{2}h(s)\frac{\zeta(s)}{\zeta(2s)} + \frac{1}{2}k(s)\frac{L(s, \Psi)}{L(2s, \Psi)},$$

where $k(s)$ is analytic on $\Re s \geq 1$. Since $\frac{L(s,\Psi)}{L(2s,\Psi)}$ is holomorphic on $\Re s \geq 1$, we have

$$N_{S_2,\Sigma}(X) \sim \frac{1}{2}\frac{6}{\pi^2}X.$$

We can go about this more systematically. Above, we essentially argued that

$$(\prod_{p \text{ finite}} \mathbb{Z}_p^*) \times \mathbb{R}_+ \simeq J_{\mathbb{Q}}.$$

However, let S be a finite set of places, then we also have

$$\left(\prod_{p \in S} \mathbb{Q}_p^* \times \prod_{p \notin S} \mathbb{Z}_p^*\right) / \mathbb{Z}_S^* \simeq J_{\mathbb{Q}}$$

where $\mathbb{Z}_S^*$ denotes S-units, i.e. integers in $\mathbb{Z}_p^*$ at all primes $p \notin S$. (We let $\mathbb{Z}_\infty^* = 1$.) So we will let S be a finite set of places on which we want to make local specifications. We will make a Dirichlet series counting maps $\prod_{p \in S} \mathbb{Q}_p^* \times \prod_{p \notin S} \mathbb{Z}_p^* \to G$ for abelian G, and then we will use multisection (i.e. use the above trick with 1 and -1) to pull out the maps that are trivial on $\mathbb{Z}_S^*$. First we have

$$F_G(s) = \prod_{p \in S} \left(\sum_{\rho_p : \mathbb{Q}_p^* \to G} p^{-d(\rho_p)s} \right) \prod_{p \notin S} \left(\sum_{\rho_p : \mathbb{Z}_p^* \to G} p^{-d(\rho_p)s} \right),$$

which counts all maps $\prod_{p \in S} \mathbb{Q}_p^* \times \prod_{p \notin S} \mathbb{Z}_p^* \to G$. Now, for simplicity, we will let $G = \mathbb{Z}/n\mathbb{Z}$. Let A be a set of representatives for $\mathbb{Z}_S^*/(\mathbb{Z}_S^*)^n$. Let ζ be a primitive nth root of unity. Note that if $\rho : \prod_{p \in S} \mathbb{Q}_p^* \times \prod_{p \notin S} \mathbb{Z}_p^* \to G$, then

$$\frac{1}{\#A} \sum_{a \in A} \zeta^{\rho(a)}$$

is 1 if $\rho(\mathbb{Z}_S^*) = 0$ and is 0 otherwise. So, we have

$$H_G(s) = \frac{1}{\#A}\sum_{a\in A}\left(\prod_{p\in S}\left(\sum_{\rho_p:\mathbb{Q}_p^*\to G}\zeta^{\rho_p(a)}p^{-d(\rho_p)s}\right)\prod_{p\notin S}\left(\sum_{\rho_p:\mathbb{Z}_p^*\to G}\zeta^{\rho_p(a)}p^{-d(\rho_p)s}\right)\right),$$

which counts all maps $\prod_{p\in S}\mathbb{Q}_p^* \times \prod_{p\notin S}\mathbb{Z}_p^* \to G = \mathbb{Z}/n\mathbb{Z}$ that are trivial on $\mathbb{Z}_S^*$, or equivalently, maps $J_{\mathbb{Q}} \to G = \mathbb{Z}/n\mathbb{Z}$ with this property. Now, if we have a local specific Σ at places $p \in S$, we can form

$$(5) \qquad H_{G,\Sigma}(s) = \frac{1}{\#A}\sum_{a\in A}\left(\prod_{p\in S}\left(\sum_{\substack{\rho_p:\mathbb{Q}_p^*\to G\\ \rho_p\in\Sigma_p}}\zeta^{\rho_p(a)}p^{-d(\rho_p)s}\right)\prod_{p\notin S}\left(\sum_{\rho_p:\mathbb{Z}_p^*\to G}\zeta^{\rho_p(a)}p^{-d(\rho_p)s}\right)\right),$$

which counts all maps $J_{\mathbb{Q}} \to G = \mathbb{Z}/n\mathbb{Z}$ satisfying the local conditions Σ. We see now the advantage of taking the full map from $\mathbb{Q}_p^*$ at the places where we want to specify. *Now imposing local conditions is just a matter of taking the terms we want from those factors.*

Exercise 8.2. See that the above gives the same analytic functions for the question of counting quadratic extensions split completely at 3.

Above we see that $H_{G,\Sigma}(s)$ is a sum of $\#A$ Euler products. In an ideal world, (*) the rightmost pole would occur in exactly 1 of those Euler products (presumably the $a = 1$ term, since we could hope the roots of unity help the other terms be smaller), and we would have an analytic continuation beyond the line of that rightmost pole so we could apply Theorem 7.1. If this were true, then the discriminant probability *among all maps, not necessarily surjective,* $J_{\mathbb{Q}} \to G$ of any Σ with specifications on a finite set of primes s would be

$$\frac{\prod_{p\in S}\sum_{\substack{\rho_p:\mathbb{Q}_p^*\to G\\ \rho_p\in\Sigma_p}} p^{-d(\rho_p)s}}{\prod_{p\in S}\sum_{\rho_p:\mathbb{Q}_p^*\to G} p^{-d(\rho_p)s}},$$

and in particular, because only one Euler product contributed to the asymptotic count we would certainly have independence of probabilities of local behaviors at a finite set of places.

However, the world is not always ideal. It turns out (*) is true when G is abelian of prime exponent, but is not true in general. Also, there is a distinction between the question above and the question of counting number fields, which would correspond to surjective ρ. One can use inclusion-exclusion to subtract out ρ with smaller image. In an ideal world, (**) the Dirichlet series coming from the maps with smaller images would be holomorphic past the rightmost pole of H_G. However, (**) is only true when G is abelian of prime exponent as well. (See [Woo10] for the proofs of all of these claims.)

We always consider abelian groups in their regular permutation representation. When $G = (\mathbb{Z}/\ell)^k$ for some prime ℓ, then as we have said (but certainly not proven!) above, one obtains an asymptotic for N_G and for $N_{G,\Sigma}$ for each set Σ of local specifications with restrictions only at finitely many primes. In particular, the probabilities of local conditions at distinct primes are independent. The probabilities are simple values we can read off from above.

Now we consider again an abelian G. If we impose local conditions that only depend on the restriction $\rho_p : \mathbb{Z}_p^* \to G$ (for example whether the map is ramified or unramified at p), then we can pick out the appropriate terms in the Dirichlet series

$$\prod_p \left(\sum_{\rho_p : \mathbb{Z}_p^* \to G} p^{-d(\rho_p)s} \right),$$

and again in this case show independence of such local conditions among all (not necessarily surjective) $\rho_p : \mathbb{Z}_p^* \to G$. (Note we have not shown this here, one still has to do the analysis of the Dirichlet series by comparison to appropriate L functions.)

Exercise 8.3. Let A be an event with positive probability not equal to 1. If E and F are independent, independent given A and we have that $\mathbb{P}(E|A) \neq \mathbb{P}(E)$ and $\mathbb{P}(F|A) \neq \mathbb{P}(F)$, then, given not-$A$, the events E and F are not independent.

Using the exercise above, it is shown in [Woo10] that since ramification is independent, e.g. in $\mathbb{Z}/\ell$ extensions (for ℓ prime), and for maps $\rho : G_{\mathbb{Q}} \to \mathbb{Z}_\ell^2$, then it cannot be independent in $\mathbb{Z}/\ell^2$ extensions. (This requires, among other things, knowing that non-surjective $\rho : G_{\mathbb{Q}} \to \mathbb{Z}/\ell^2\mathbb{Z}$ occur with positive probability.) For example we have the following.

Proposition 8.4 (Proposition 1.4 of [Woo10])**.** *Let $p, q_1,$ and q_2 be primes with $q_i \equiv 1 \pmod{p}$ for $i = 1, 2$. Then q_1 ramifying and q_2 ramifying in a random $\mathbb{Z}/p^2\mathbb{Z}$-extension are not (discriminant) independent.*

One might hope to then simplify things by not considering G-extensions but rather all maps $\mathbb{G}_{\mathbb{Q}} \to G$. Then, we wouldn't have to subtract out non-surjective maps. In this situation, for local conditions only depending on the map of the inertia subgroups, we do indeed get independence of local behaviors and easy to read off probabilities. However, if we consider all local conditions, then the other terms in the Equation (5) sum over $a \in A$ with the same rightmost pole as the $a = 1$ term necessarily have an effect on the answer.

8.2. **Grunwald-Wang.** It follows from Wang's [Wan50] counterexample to Grunwald's "Theorem" [Gru33] (this is a great story to read about if you don't know it already), that there is no $\mathbb{Z}/8$ extension K of $\mathbb{Q}$ for which K_2 is an unramified extension of $\mathbb{Q}_2$ of degree 8. However, there is certainly a local Galois representation $\rho_2 : \mathbb{Q}_2^* \to \mathbb{Z}/8$ that is unramified and sends $2 \mapsto 1$. This local Galois representation does not come from a global $\mathbb{G}_{\mathbb{Q}} \to \mathbb{Z}/8$, and considering all $\mathbb{G}_{\mathbb{Q}} \to \mathbb{Z}/8$ or just surjective $\mathbb{G}_{\mathbb{Q}} \to \mathbb{Z}/8$ does not change a thing about this fact. So, we realize that some term in the Equation (5) sum over $a \in A$ with the same pole as the $a = 1$ term must in fact cancel that pole entirely.

Exercise 8.5. Show there is no $\mathbb{Z}/8$ extension K of $\mathbb{Q}$ for which K_2 is an unramified extension of $\mathbb{Q}_2$ of degree 8.

Exercise 8.6. When $G = \mathbb{Z}/8\mathbb{Z}$ and Σ is the restriction at 2 that $\mathbb{Q}_2^* \to G$ be unramified and surjective, write out the sum of Euler products for $H_{G,\Sigma}$ and see the cancellation explicitly.

It can be completely classified when local Galois representations to abelian groups do not occur as restrictions of global Galois representations (a convenient reference is [AT68, Chapter 10]). Over $\mathbb{Q}$, problems only occur at 2. However, the Wang counterexamples are in fact the nicest possible behavior that occurs when the Equation (5) sum over $a \in A$ has multiple terms with the same pole. In general, say for restrictions only at odd places, there are still multiple terms that contribute to the sum, and the result is terrible looking probabilities, and lack of independence, whether one considers all $\mathbb{G}_{\mathbb{Q}} \to G$ or just surjective ones.

8.3. **Counting by conductor.** One can ask all the same questions for counting abelian extensions, but instead of counting by discriminant, can count by conductor. The answers to the questions above are much nicer in this situation. (In fact, in [Woo10] a notion of *fair* counting function is introduced which includes conductor, and e.g. the product of ramified primes, for which all the same qualitative results hold as for conductor.) When counting by conductor, as in [Woo10], the terms from subtracting non-surjective maps do not have any poles in the relevant region, so (**) is not a problem.

However, we know that some of the other terms in the Equation (5) sum $a \in A$ must have the same rightmost pole as the $a = 1$ term, because counting by a different invariant is never going to eliminate Wang's counterexample. Amazingly, when counting by conductor, while there are indeed multiple terms with the same rightmost pole, they all differ by simple rational constants and can be combined simply. In a precise sense (described in [Woo10, Section 1]), there are no obstructions to simple probabilities and independence other than the completely classified Wang counterexamples. All of the local behaviors that do occur from global extensions still occur with the same relative probabilities that one would expect from their contribution to the $a = 1$ term of the Dirichlet series–just the ones that are impossible occur with probability 0. When counting abelian extensions of $\mathbb{Q}$, since 2 is the only place that has Wang counterexamples, there is independence of local behaviors when counting by conductor.

Over other fields with multiple places dividing 2, there are sometimes local behaviors at two different places that are both possible, but not possible together. (Again, these belong to the completely classified Wang counterexamples.) So when $\mathbb{Q}$ is replaced one of these fields, using any counting function for that field, independence has to fail. However, as described explicitly below, when counting by conductor the simplest possible thing happens given this. We can build a model from the Dirichlet series, and then restrict to what is possible, and that gives the answer.

9. Abelian results

These asymptotics of $N_G(X)$ for G abelian ($G \subset S_{|G|}$ in its regular representation) were determined completely for abelian Galois groups by Mäki [Mäk85]. Mäki [Mäk93] also determined the asymptotics of the number of extensions of $\mathbb{Q}$ with fixed abelian Galois group and bounded conductor. Wright [Wri89] proved the analogous asymptotics for counting G-extensions for a fixed abelian G by discriminant over any number field or function field (in tame characteristic). Wright also showed that any local restrictions that occur at all (i.e. are not Wang counter examples) occur with positive asymptotic probability. Wright, however, noted that the probabilities seem quite complicated. Before the work of Mäki and Wright, there were many papers that worked on these questions for specific abelian groups. See [Wri89] for an overview of this literature.

In [Woo10], we give the asymptotics of the number of G-extensions with bounded conductor (or any fair counting function) for a finite abelian group G over any number field. We also give the constant in the asymptotic more explicitly than it appears in [Mäk93]. In [Woo10], we also completely determine the probabilities of local conditions when counting G-extensions by conductor for some fixed abelian G. We also more carefully analyze the probabilities when counting by discriminant to prove that indeed they are as bad as Wright suspected.

9.1. **Some explicit results.** If we count abelian number fields by their conductor (in the sense of class field theory [Neu99, Chapter VI, 6.4]), we can define $\mathbb{P}_{cond}$ analogously to our definition of $\mathbb{P}_{\mathrm{Disc}}$ in Section 1 above.

Theorem 9.1 ([Woo10]). *Let G be a finite abelian group in its regular permutation representation, and q be a fixed rational prime (not 2 if $|G|$ is even). Then for a random L with Galois group G, a fixed K with Galois group G, and a random rational prime p*

$$\mathbb{P}_{cond}(q \textit{ splits into } r \textit{ primes in } L \mid q \textit{ unramified in } L) = \mathbb{P}_p(p \textit{ splits into } r \textit{ primes in } K).$$

Taylor [Tay84] first proved the result of Theorem 9.1 in the special case that $G = \mathbb{Z}/n\mathbb{Z}$, and assuming that $4 \nmid n$. Wright [Wri89] proves an analog of Theorem 9.1 for discriminant probability in the case that $G = (\mathbb{Z}/p\mathbb{Z})^b$ for p prime, and for these G the discriminant is a fixed power of the conductor, and thus discriminant probability is the same as conductor probability. Theorem 9.1 relates the row probabilities to the column probabilities of the sort of big chart we made in Section 1. In fact in [Woo10], the probabilities of all (ramified or unramified) local behaviors are determined. Further it is shown $|G|$ is even and $p = 2$ the probabilities of splitting types that ever occur in a random G-extension that occur in the same proportions as they occur in the Chebotarev density theorem for a fixed extension and random prime. Of course, there will always be the contrast, seen already for quadratic extensions in Section 1, that for a fixed p and a random G-extension L, the prime p will be ramified with positive probability, while for a fixed number field K a random prime q is ramified with probability 0.

Further, in [Woo10] it is shown that these local probabilities for splitting in a random G extension are independent for different primes.

Theorem 9.2 ([Woo10]). *Let G be a finite abelian group in its regular permutation representation. For any finite set S of places of $\mathbb{Q}$ and any choice of local $\mathbb{Q}_v$-algebras T_v for $v \in S$, for a random L with Galois group G (counted by conductor), the events $L \otimes_{\mathbb{Q}} \mathbb{Q}_v \simeq T_v$ are independent.*

Wright [Wri89] showed that all $\mathbb{Q}_v$-algebras that ever occur as $L \otimes_{\mathbb{Q}} \mathbb{Q}_v$ for a number field L with Galois group G occur with positive discriminant probability, but noted that the probabilities are apparently very complicated. The discriminant probability analog of Theorem 9.1 does not hold. If K is a fixed number field with Galois group $\mathbb{Z}/9\mathbb{Z}$ and p a random rational prime, then

$$\mathbb{P}_p(p \text{ splits completely in } K) = \frac{1}{9}.$$

However, we have the following.

Proposition 9.3 ([Woo10]). *Let $q = 2$, 3, 5, 7, 11, or 13. Then for a random L with Galois group $\mathbb{Z}/9\mathbb{Z}$,*

$$\mathbb{P}_{\mathrm{Disc}}(q \textit{ splits completely in } L \mid q \textit{ unramified in } L) < \frac{1}{9}.$$

The situation for abelian extensions and their local behaviors is quite interesting over a base number field K other than $\mathbb{Q}$. Wang counterexamples occur only at primes dividing 2, but now there can be more than one such prime, and so these examples affect even independence. Given an abelian G, it is possible that the K_v-algebra T_v and the $K_{v'}$-algebra $T'_{v'}$ both occur from global G-extensions, but never occur simultaneously. This suggests that we should not expect T_v and $T'_{v'}$ to be independent events. However, given obstructions of this sort, which were completely determined in [Wan50] (or see [AT68, Chapter 10]), we have the best possible behavior of the local probabilities. This is described in detail in [Woo10, Section 1], but roughly if you build a model where are local behaviors are predicted to have their heuristic probabilities (see Section 10), and then restrict to the combinations of local behaviors that ever occur, the model gives the correct predictions.

10. The Malle-Bhargava principle

Malle [Mal02, Mal04] has given a conjecture for Question 1.6 and Bhargava [Bha10b] has given some heuristics (stated as a question–when do these heuristics apply?) for the more refined Questions 1.11 that extend Malle's original conjecture. However, there are counterexamples to both the original conjecture (see Klüners [Klü05]), and to Bhargava's more refined heuristics (e.g. some of the abelian counting results of [Woo08] above), so we will refer to these conjectures/heuristics as a principle. (Though notably, there are not any known counterexamples to the weaker form of Malle's conjecture given in [Mal02] that says $K_\Gamma X^{1/a(\Gamma)} \leq N_\Gamma(X) \leq K_{\Gamma,\epsilon} X^{1/a(\Gamma)+\epsilon}$ for a specified constant $a(\Gamma)$ and unspecified constants $K_\Gamma, K_{\Gamma,\epsilon}$.) An important open question is to even make a good conjecture about when exactly the principle should apply.

We now explain the principle, following [Bha10b] (similar, but not identical, heuristic reasoning is given by [Mal04]). Let $\Gamma \subset S_n$ be a permutation group. For each place p of $\mathbb{Q}$, let Σ_p be a set of continuous homomorphisms $G_{\mathbb{Q}_p} \to \Gamma$. Let Σ be the collection of these Σ_p. If Σ_p is all the maps $G_{\mathbb{Q}_p} \to \Gamma$ for all but finitely many p we say Σ is nice. (We may want to call other Σ nice as well.) We define a Dirchlet series as an Euler product over places p

$$D_{\Gamma,\Sigma}(s) := C_\Gamma \prod_p \left(\frac{1}{\#\Gamma} \sum_{\rho_p \in \Sigma_p} (\operatorname{Disc} \rho_p)^{-s} \right)$$

for some as yet unspecified constant C_Γ, where the product is over all places p of $\mathbb{Q}$. Let $D_{\Gamma,\Sigma}(s) = \sum_{n\geq 1} d_n n^{-s}$.

For nice Σ, the principle predicts that the asymptotics of

$$\#\{\rho : G_{\mathbb{Q}} \to \Gamma \mid \Gamma \text{ surjective},\ \operatorname{Disc} \rho < X, \rho_p \in \Sigma_p \text{ for all } p\}$$

in X are the same as the asymptotics of

$$\sum_{n=1}^{X} d_n$$

in X. (Equivalently, it predicts that the limit of their ratios is 1.) Perhaps stated another way, the principle would suggest that $D_{\Gamma,\Sigma}(s)$ and a Dirichlet series counting surjective $G_{\mathbb{Q}} \to \Gamma$ by discriminant would have the same rightmost pole and residue at that pole and analytic continuation just beyond the pole, so that the previous version of the principle would follow from Theorem 7.1.

10.1. **Local factors.** To begin to digest this principle, we will consider a single local factor

$$\frac{1}{\#\Gamma}\sum_{\rho_p\in\Sigma_p}(\operatorname{Disc}\rho_p)^{-s}.$$

Finitely many factors have $p|\#\Gamma$ (these are the terms where the local extension might be wild), but we see that these finitely many factors cannot introduce any poles to $D_{\Gamma,\Sigma}(s)$. So we expect the important analytic behavior of $D_{\Gamma,\Sigma}(s)$ to be present in just the tame factors, and for the rest of this subsection we assume $p\nmid\#\Gamma$.

Let $\mathbb{Q}_p^t$ be the maximal tame extension of $\mathbb{Q}_p$, and $G^t_{\mathbb{Q}_p}:=\operatorname{Gal}(\mathbb{Q}_p^t/\mathbb{Q}_p)$ be the tame quotient of the absolute Galois group of $\mathbb{Q}_p$. Let F be the free group on x and y with the relation

$$xyx^{-1}=y^p.$$

Let $\hat{F}$ be the profinite completion of F. Then we have an isomorphism

$$\hat{F}\simeq G^t_{\mathbb{Q}_p},$$

where y goes to a topological generator of the inertia subgroup, and x goes to Frob (see, e.g. [NSW00, Theorem 7.5.2]). Given a $y\in\Gamma$, let $c(y)$ be the number of orbits of y on $\{1,\dots,n\}$, and let $d(y)=n-c(y)$. So

$$\sum_{\rho_p\in\Sigma_p}(\operatorname{Disc}\rho_p)^{-s}=\sum_{\substack{x,y\in\Gamma\\ xyx^{-1}=y^p}}p^{-d(y)s}.$$

Given $y\in\Gamma$, how many x are there in Γ such that $xyx^{-1}=y^p$? If y and y^p are conjugate then there are $\#\Gamma/\#\{\text{conj. class of } y\}$. If y and y^p are not conjugate, then there are no such x. Let $\sim$ denote "is conjugate to." Then we have

$$\sum_{\rho_p\in\Sigma_p}(\operatorname{Disc}\rho_p)^{-s}=\sum_{\substack{y\in\Gamma\\ y\sim y^p}}\frac{\#\Gamma}{\#\{\text{conj. class of } y\}}p^{-d(y)s}.$$

We can see why we must include the factor $1/\#\Gamma$ to get a reasonable principle. From the $y=1$ term, the above sum has constant term $\#\Gamma$, and so the $1/\#\Gamma$ factor is necessary so that we could even have a chance of the product over p converging in some right half-plane. Let Γ_p be the set of conjugacy classes of Γ of the form $[y]$ such that $y\sim y^p$. So

$$\frac{1}{\#\Gamma}\sum_{\rho_p\in\Sigma_p}(\operatorname{Disc}\rho_p)^{-s}=\sum_{[y]\in\Gamma_p}p^{-d(y)s}.$$

Note that we always have plenty of primes $p\equiv 1\pmod{\#\Gamma}$, so that every $y\sim y^p$, and Γ_p is simply the set of conjugacy classes of Γ. A nice special case is when $\Gamma=S_n$. For $p>n$, we have $y\sim y^p$ for every $y\in S_n$, so for every tame prime p in this case Γ_p is simply the set of conjugacy classes of Γ.

Computing these locals factors in the wild cases is much more complicated, and some interesting phenomena arise (see [Bha10b, Ked07, Woo08, WY15]).

10.2. **Malle's conjecture.** This computation of the local factors leads to Malle's conjecture [Mal04, Mal02] that

$$N_\Gamma(X) \sim K_\Gamma X^{1/a(\Gamma)}(\log X)^{b(\Gamma)}$$

for some constant K_Γ and $a = \min_{y \in \Gamma \setminus \{1\}} d(y)$ and where $b(\Gamma)$ can also be given explicitly. Klüners [Klü05] has given a counterexample when $\Gamma = C_3 \wr C_2$, where the value of $b(\Gamma)$ is too small, or said another way, there are more extensions than the conjecture predicts by a $\log X$ factor. Turkelli, by analogy with heuristics on the function field side, has given a "corrected" version of Malle's conjecture that takes into account Klüners counterexample [Tur08] to give a different prediction for the log factor.

The weak conjecture of Malle [Mal02] says $K_\Gamma X^{1/a(\Gamma)} \leq N_\Gamma(X) \leq K_{\Gamma,\epsilon} X^{1/a(\Gamma)+\epsilon}$ for some constants $K_\Gamma, K_{\Gamma,\epsilon}$. There are no known counterexamples to this conjecture, and it is known in a wide variety of cases (see below).

10.3. **Independence and local behaviors.** The principle suggests that when counting extensions with Galois group Γ, for any finite set of places, local conditions at those places should be independent. We can see this from the mechanics of how the Tauberian Theorem applies. Changing a finite number of the factors in the Euler product for $D_{\Gamma,\Sigma}$ just changes the constant in the asymptotic by the product of the ratios of the new factors over the old factors, all evaluated at the rightmost pole.

More precisely, let $a(\Gamma)$ be as above. Recall, the definition of $D_{\Gamma,\Sigma}(s)$ above as an Euler product built as a heuristic model for the Dirichlet series counting extensions with Galois group Γ and local behaviors Σ.

Exercise 10.1. Show that $D_{\Gamma,\Sigma}(s)$ converges in $\Re(s) > 1/a(\Gamma)$.

Exercise 10.2. Show that $D_{\Gamma,\Sigma}(1/a(\Gamma))$ does not converge.

So, if there is a meromorphic continuation past $\Re(s) > 1/a(\Gamma)$, we expect a pole at $1/a(\Gamma)$. (To show more precisely that such a pole had to exist, we could find $\lim_{s \to ^+ 1/a(\Gamma)} D_{\Gamma,\Sigma}(s)$.) So, supposing that $D_{\Gamma,\Sigma}$ has a meromorphic continuation to $\Re(s) \geq 1/a(\Gamma)$ (which one can actually show for every Γ), if D_Γ is the Dirichlet series where all local behaviors are allowed with coefficients d_n, and Σ makes specifications at a finite set S of places, and $D_{\Gamma,\Sigma}$ has coefficients $d(\Sigma)_n$, then we have

$$\lim_{X \to \infty} \frac{\sum_{n=1}^{X} d(\Sigma)_n}{\sum_{n=1}^{X} d_n} = \prod_{p \in S} \frac{\frac{1}{\#\Gamma} \sum_{\rho_p \in \Sigma_p} (\mathrm{Disc}\, \rho_p)^{-1/a(\Gamma)}}{\frac{1}{\#\Gamma} \sum_{\rho_p : G_{\mathbb{Q}_p} \to \Gamma} (\mathrm{Disc}\, \rho_p)^{-1/a(\Gamma)}}.$$

Exercise 10.3. Show this (assuming a continuation to $\Re(s) \geq 1/a(\Gamma)$ with no other poles except at $1/a(\Gamma)$).

So we see the probabilities of local behaviors at different places would be independent and given by relatively simple fractions (with all the principles/assumptions above).

10.4. **When the principle holds.** It is an important open question to even make a good guess as to when the above principle holds. The work of Mäki [Mäk85] (and also Wright [Wri89]) shows that Malle's conjecture holds when Γ is abelian in its regular representation, i.e. the order of magnitude is right when counting all Γ extensions. Moreover, Wright shows that the order of magnitude is right for any local condition that is not a Wang counterexample (in which case the principle's prediction must be wrong since the actual count is 0). However, we saw above that [Woo10] shows that the general principle fails when Γ is not abelian with prime exponent because the independence of local conditions fails. (But all can be recovered if one counts by conductor instead of discriminant!) Somewhat orthogonal to the focus of the principle above, but also interesting, is work of Cohen, Diaz y Diaz, and Oliver [CDyDO02b] that finds the constant K_Γ very explicitly when Γ is cyclic of prime degree.

For $\Gamma = S_3$, it is a theorem of Davenport and Heilbronn [DH71], that we will discuss below, that the entire principle holds. Moreover, when $\Gamma = S_3 \subset S_6$ via the regular representation (i.e. counting Galois sextic S_3 fields) Bhargava and the author [BW08] have shown that the entire principle holds.

For $\Gamma = S_4, S_5$, theorems of Bhargava [Bha05, Bha10b] show that the entire principle holds. For $\Gamma = D_4 \subset S_4$, Cohen, Diaz y Diaz, and Oliver [CDyDO02a] have shown that Malle's conjecture holds, but the evidence suggests that the entire principle does not hold. (In fact, Cohen [Coh03] counts D_4 extensions with local conditions at infinity, from which it could probably be seen explicitly that the entire principle does not hold.) Given the above story with abelian Γ, perhaps the right question is how can we count extensions so that the principle holds, and in [Woo08] a different way of counting D_4 extensions is suggested for which the principle might hold. Klüners [Klü12] has shown that Malle's conjecture holds for groups $C_2 \wr H$, under mild assumptions on the count of H-extensions.

As mentioned above, for some groups even Malle's conjecture fails. (See [Klü05] and [Tur08].) However, the weak conjecture of Malle is proven in many cases and has no known counterexamples. Besides those mentioned above it is also known for nilpotent groups in their regular representation by Klüners and Malle [KM04].

10.5. **Other base fields.** Of course, in these questions we could replace $\mathbb{Q}$ with any number field or function field. As suggested by Bhargava [Bha10b], the principle above could be formulated over any global field, and in particular it refines Malle's conjecture [Mal04, Mal02] which is stated over an arbitrary number field. Of the work above, [Wri89] is over any number field or function field of tame characteristic and [Woo10, CDyDO02b, Klü12, KM04] are over any number field. Also when $\Gamma = \mathbb{Z}/\ell\mathbb{Z}$ and the base field is a rational function field, the counting has been done in [BDF$^+$15], and in particular cases relevant to the application at hand there it is shown that the full principle with local conditions also holds. The work [DH71] has been generalized to any number field or function field of tame characteristic by Datskovsky and Wright in [DW86], and the result of [BW08] is given over any number field. As far as the current author is aware, the results [Bha05, Bha10b, CDyDO02a] are known only over $\mathbb{Q}$.

11. Davenport-Heilbronn

In this section, we will discuss how to answer Question 1.6 for $\Gamma = S_3$, i.e. to count non-Galois cubic number fields. This is originally a result of Davenport and Heilbronn [DH71]. Since we know from Cohn [Coh54] (see Equation (4)) that

$$N_{\mathbb{Z}/3}(X) \sim cX^{1/2}$$

and the results of Davenport and Heilbronn [DH71] will say that

$$N_{S_3}(X) \sim c'X,$$

we may equally well consider counting all cubic number fields. We will outline a modern proof (largely following [BST13]) of this statement, which has the same main ideas as the original proof, but with improvements and simplifications. There is an excellent exposition of such a modern proof in Section 2-5 and 8 of the paper of Bhargava, Shankar, and Tsimerman [BST13] (which, in the other sections, proves a *secondary* term for this asymptotic count– see also [TT13] where the secondary term is proven with very different methods). So in these notes we will mostly emphasize aspects that are complementary to what is given in that exposition, and might be best read along with [BST13]. There is also a do-it-yourself exposition of the proof in the Arizona Winter School 2014 problem set, as a series of problems that should complement this article nicely.

11.1. **The parametrization.** We begin by considering *cubic rings*, which are commutative rings whose underlying additive groups structure is isomorphic to $\mathbb{Z}^3$ (equivalently, locally free rank 3 $\mathbb{Z}$-algebras, or a finite, flat degree 3 cover of $\operatorname{Spec}\mathbb{Z}$). We will be able to count cubic rings, and then we will specialize to cubic rings that are domains and maximal. The maximal cubic domains correspond exactly to the rings of integers in cubic number fields. We give a parametrization of cubic rings originally due to Delone and Faddeev [DF64] (and refined by Gan, Gross, and Savin [GGS02]).

Let R be a cubic ring.

Exercise 11.1. Show that 1 generates a direct summand of R.

Let $1, W, T$ be a $\mathbb{Z}$ basis of R. Since

$$WT = q + rW + sT,$$

for some $q, r, s \in \mathbb{Z}$, we can take $\omega = W - s$ and $\theta = T - r$ and have $1, \omega, \theta$ a $\mathbb{Z}$ basis of R with $\omega\theta \in \mathbb{Z}$. We call such a basis a *normalized* basis. Next, we write down a multiplication table for a normalized basis:

$$\begin{aligned} \omega\theta &= n \\ \omega^2 &= m - b\omega + a\theta \\ \theta^2 &= \ell - d\omega + c\theta, \end{aligned} \tag{6}$$

where $n, m, \ell, a, b, c, d \in \mathbb{Z}$. However, not all values of n, m, ℓ, a, b, c, d are possible.

Exercise 11.2. Show that the associative law exactly corresponds to the equations

$$n = -ad \quad m = ac \quad \ell = -bd. \tag{7}$$

That means that not only is Equation 7 necessarily true for any cubic ring R with normalized basis $1, \omega, \theta$, but also if we have a free rank 3 $\mathbb{Z}$-module with generators $1, \omega, \theta$, we can put a commutative, associative multiplication structure on the module using Equations (6) and (7). So rank 3 rings with a choice of normalized basis are parametrized by $\mathbb{Z}^4$ using (a, b, c, d). We can package an element $(a, b, c, d) \in \mathbb{Z}^4$ as a binary cubic form $ax^3 + bx^2y + cxy^2 + dy^3$, and thereby such forms parametrize rank 3 rings with a choice of normalized basis. Given a form f, let R_f be the associated cubic ring with a choice of normalized basis. One important fact is that the construction above preserves discriminants (see [GGS02] or any of the other references on this parametrization).

Exercise 11.3. Find a binary cubic form associated to $\mathbb{Z}[\sqrt[3]{2}]$. Find another one (using a different choice of basis). Find a binary cubic form associated to $\mathbb{Z}[i] \oplus \mathbb{Z}$ (with componentwise multiplication). Find a binary cubic form associated to $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$. What cubic ring is associated to the zero form?

A choice of normalized basis of R is equivalent to a choice of $\mathbb{Z}$ basis of $R/\mathbb{Z}$. The action of $\mathrm{GL}_2(\mathbb{Z})$ on bases of $R/\mathbb{Z}$ gives a $\mathrm{GL}_2(\mathbb{Z})$ action on $\mathbb{Z}^4$, such that the orbits are in bijection with cubic rings as given above. Because of the normalization, this action is slightly annoying to work out by hand, though perhaps not so bad to at least see it is linear. The action turns out to be (almost) the 4 dimensional representation of $\mathrm{GL}_2(\mathbb{Z})$ on binary cubic forms. Let $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$. Let $g \in \mathrm{GL}_2(\mathbb{Z})$. Then we can let $\mathrm{GL}_2(\mathbb{Z})$ act on binary cubic forms via

$$(gf)(x, y) = \frac{1}{\det(g)} f((x, y)g), \tag{8}$$

where $(x, y)g$ is the multiplication of a row vector by a matrix on the right. This action exactly translates into the action on the parameters (a, b, c, d) of cubic rings given by action on the choice of basis of $R/\mathbb{Z}$. There are several ways to see this more intuitively, we will see one later. So, we will face the problem of counting $\mathrm{GL}_2(\mathbb{Z})$ classes of binary cubic forms, with the action given in Equation (8).

An important feature of the parametrization is that in fact many important properties of the cubic ring can be read off from the associated binary cubic form. One way to see this is to understand that the parametrization is more general than what is written above over $\mathbb{Z}$. We will in fact see that it is far more general.

Let B be a commutative ring (which will replace $\mathbb{Z}$). A cubic B-algebra is a commutative B-algebra which is locally free rank 3 as a B-module. (There are two common notions of locally free, an algebraic one where "locally" means at localizations at prime ideals, and a geometric one where "locally" means in Zariski opens of $\operatorname{Spec} B$, but the rank 3 condition ensures that these two notions are the same in this case.) If R is a cubic B-algebra, then $\operatorname{Spec} R$ is a finite, flat, degree 3 cover of $\operatorname{Spec} B$, and conversely, every finite, flat degree 3 cover is $\operatorname{Spec} R$ for a cubic algebra R. Similarly, for any scheme S, we can define a *cubic cover* of S to be a finite, flat, degree 3 cover of S, or equivalently a locally free rank 3 $\mathcal{O}_S$-algebra (which we call a *cubic $\mathcal{O}_S$-algebra*).

Over a scheme S, we define a *binary cubic form* to be a locally free rank 2 $\mathcal{O}_S$-module V (i.e. a rank 2 vector bundle on S) and a global section $f \in H^0(S, \operatorname{Sym}^3 V \otimes \wedge^2 V^*)$, where all tensors and exterior powers are over $\mathcal{O}_S$ and for an $\mathcal{O}_S$-module W, we write W^* for the dual $\mathcal{O}_S$ module $\mathcal{H}om(W, \mathcal{O}_S)$. (These might be more properly called "twisted" binary cubic forms because of the twist by the locally free rank 1 $\wedge^2 V^*$, but they are the only ones we will talk about, so we will leave out the "twisted.") Over a ring B then (applying the above definition in the case $S = \operatorname{Spec} B$), we see that a binary cubic form is a locally-free rank 2 B-module V, and an element $f \in \operatorname{Sym}^3 V \otimes \wedge^2 V^*$. An isomorphism of binary cubic forms is given by an isomorphism $V \to V'$ that takes $f \to f'$.

Given a binary cubic form (V, f) over S, we can construct a cubic cover of S as follows. This construction is due to Deligne [Del] (see [Woo11c, Sections 2.3,2.4,3] for a generalization of this construction from binary cubic forms to binary n-ic forms for any n). Let $\mathbb{P}(V) = \operatorname{Proj} \operatorname{Sym} V$, so $\pi : \mathbb{P}(V) \to S$ is a $\mathbb{P}^1$ bundle over S. If f is not a zero divisor, then f cuts out a codimension 1 subscheme $S_f \subset \mathbb{P}(V)$. Then $\pi_*(\mathcal{O}_{S_f})$ is a locally-free rank 3 $\mathcal{O}_s$-algebra. This construction does not work when f is identically the 0 form.

Let $\mathcal{O}(k)$ denote the usual sheaf of $\mathbb{P}(V)$. We then have a complex of sheaves

$$C_f : \mathcal{O}(-3) \otimes \pi^* \wedge^2 V \xrightarrow{f} \mathcal{O},$$

(in degrees -1 and 0). If f is not a zero-divisor, then the map above is injective, so this complex is quasi-isomorphic to

$$0 \rightarrow \mathcal{O}/f(\mathcal{O}(-3) \otimes \pi^* \wedge^2 V),$$

and the term on the right is just $\mathcal{O}_{S_f}$. The hypercohomology

$$H^0 R\pi_*(C_f)$$

has a product given by the product on the complex (which is a Koszul complex so has that natural product) and inherits the structure of a cubic $\mathcal{O}_s$-algebra (see [Woo11c, Sections 2.4,3] for more details on this structure, and this entire construction). When f is not a zero-divisor, by the quasi-isomorphism above, we see that this agrees with $\pi_*(\mathcal{O}_{S_f})$.

Theorem 11.4 (Theorem 2.4 of [Woo11c]). *When V is a free $\mathcal{O}_S$-module (e.g. this is always the case when B is a P.I.D. and $S = \operatorname{Spec} B$), this geometric/hypercohomological construction of a cubic $\mathcal{O}_S$-algebra from a binary cubic form $(\mathcal{O}_S^{\oplus 2}, f)$ agrees with R_f constructed from Equations* (6) *and* (7) *above.*

We restrict to V a free $\mathcal{O}_S$-module only because that is the case for which the first construction is defined.

Theorem 11.5 (Corollary 4.7 of [Woo11c]). *Given a scheme S, the geometric/hypercohomological construction above gives an isomorphism of categories between the category of binary cubic forms over S (where the morphisms are isomorphisms) and the category of cubic $\mathcal{O}_S$-algebras (where the morphisms are isomorphisms). Thus, over a scheme S, the construction gives a bijection between isomorphism classes of cubic algebras and isomorphism classes of binary cubic forms. If a cubic algebra R corresponds to a binary cubic form (V, f), then as $\mathcal{O}_S$-modules, we have $R/\mathcal{O}_S \simeq V^*$. The functor described above from binary cubic forms to cubic $\mathcal{O}_s$-algebras commutes with base change in S.*

(See also [Poo08] which proves an isomorphism of categories using a rigidification by a choice of basis and the construction from Equations (6) and (7) above.)

We will now unpack some of the features of this result. Let B be a principal ideal domain. Then the only choice of a locally free rank 2 B-module V is $V = B^2$, and we will take generators x and y. Let x^*, y^* be the associated dual basis of $V^* = \operatorname{Hom}(V, B)$. Then $\operatorname{Sym}^3 V$ is a free rank 4 B-module generated by x^3, x^2y, xy^2, y^3. The element $x^* \wedge y^*$ gives an isomorphism $B \simeq \wedge^2 V^*$. So then a binary cubic form over B is a choice $a, b, c, d \in B$ for

$$(ax^3 + bx^2y + cxy^2 + dy^3) \otimes (x^* \wedge y^*).$$

However, since we had to pick a basis x, y of B, the choice of a, b, c, d is only well-defined up to the $\mathrm{GL}_2(B)$ action on x, y.

Exercise 11.6. When B is a PID, show that this notion of isomorphism classes of binary cubic forms over B agrees with the notion of $\mathrm{GL}_2(B)$ classes of binary cubic forms that was given above over $\mathbb{Z}$ (but could be just as well interpreted over B).

Exercise 11.7. Suppose B is the ring of integers of a number field but is not a PID. Show that our notion of isomorphism classes of binary cubic forms over B does not agree with the notion of $\mathrm{GL}_2(B)$ classes of binary cubic forms given that was given above over $\mathbb{Z}$ (but could be just as well interpreted over B).

The twist by $\wedge^2 V^*$ may look somewhat irrelevant, especially if one is working only over $\mathbb{Z}$, where the determinant of an element in $\mathrm{GL}_2(\mathbb{Z})$ can only be ± 1. Even over B, for $\lambda \in B^*$ the matrix λI multiplies each of a, b, c, d by λ. (In particular, this remark shows that the $\mathrm{GL}_2(B)$ classes of binary cubic forms over B would be the same even if we didn't take the twisted action.) However, it is actually quite important. Without the twist, the GL_2 action on the form does not agree with the GL_2 action of the choice of basis of R/B. This agreement is important because we will need to use the fact that the automorphism groups of corresponding objects agree, which comes from the equivalence of categories statement above or can be seen more concretely from the fact that the GL_2 actions agree.

For any integer ℓ, over a general base scheme S, for $f \in H^0(S, \operatorname{Sym}^3 V \otimes (\wedge^2 V)^\ell)$ one can make a cubic algebra via an analog of the above construction [Woo11c, p. 219]. (Note that since $(\wedge^2 V)^{-1} = (\wedge^2 V)^*$ the above construction is the case $\ell = -1$.) This always gives a functor from (ℓ-twisted) binary cubic forms to cubic algebras over S that commutes with base change [Woo11c, p. 219]. However only in the cases $\ell = -1$ and $\ell = -2$ is this functor an isomorphism of categories. For other ℓ, even over $S = \mathbb{P}^1$ one can see that not all cubic algebras arise (see the last paragraph of page 227 of [Woo11c]).

Over a field K, we see that a non-zero binary cubic form f just cuts out a degree 3 subscheme of $\mathbb{P}^1_K$. If $a \neq 0$ (and if the form is non-zero we can always change basis so that this is the case unless $K = \mathbb{F}_2$), then the cubic K-algebra is $K[\alpha]/(a\alpha^3 + b\alpha^2 + c\alpha + d)$.

Exercise 11.8. Show that this agrees with each of the above constructions (the construction originally given over $\mathbb{Z}$ in terms of the multiplication table, and the geometric description involving the global functions on the scheme cut out by the form).

From this, using the base change from $\mathbb{Z}$ to $\mathbb{Q}$, it follows, over $\mathbb{Z}$, that the cubic ring R_f (associated to f) is a domain if and only if f is irreducible (over $\mathbb{Q}$). In this case, we call f *irreducible*, and otherwise we call it *reducible*. We have that f is irreducible if and only if R_f is an order in a cubic number field. The number field then is given by the dehomogenized version of the binary cubic form.

We can use the base change from $\mathbb{Z}$ to $\mathbb{Z}_p$ to understand which forms associated to orders in cubic fields are associated to orders maximal at p (meaning they have index relatively prime to p in the maximal order). In fact, maximality at p is determined by the class of the form modulo p^2. See [BST13, Lemma 13] for more details on this.

One can, in fact, see more explicitly what the geometric construction gives over $\mathbb{Z}$ (base change from $\mathbb{Z}$ to $\mathbb{Z}_p$ also simplifies matters in understanding this, see also [Woo11c, Section2]). If f is non-zero, then it cuts out a 1 dimensional subscheme S_f of $\mathbb{P}^1_{\mathbb{Z}}$. If for some prime p, we have $p|a, b, c, d$, then S_f has a vertical fiber over p, and in particular, S_f is not finite, flat degree 3 over $\mathbb{Z}$. However, the global functions $H^0(S_f, \mathcal{O}_{S_f})$ are still a cubic ring, and this is the associated cubic ring R_f. So $\operatorname{Spec} R_f$ is a finite, flat, degree 3 cover (in particular, we have gotten rid of the vertical fibers). We have a map $S_f \to \operatorname{Spec} R_f$, in which $\operatorname{Spec} R_f$ is the universal affine variety that S_f maps to. Over p, the scheme $\operatorname{Spec} R_f$ has a singularity that cannot be embedded in $\mathbb{P}^1_{\mathbb{Z}}$. If $(a,b,c,d)=1$, we call the form *primitive*, and then in fact S_f is affine and is the cubic cover of $\operatorname{Spec}\mathbb{Z}$ associated to f.

We can use base change from $\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$ to see that R_f/p is the cubic ring given by reducing f modulo p. Over $\mathbb{Z}/p\mathbb{Z}$, there are not so many options for f up to isomorphism. It either is 0, has three distinct roots over $\mathbb{Z}/p\mathbb{Z}$, has 1 single root over $\mathbb{Z}/p\mathbb{Z}$, has 1 double roots and 1 single root over $\mathbb{Z}/p\mathbb{Z}$, or has 1 triple root over $\mathbb{Z}/\mathbb{Z}$, and in each of these cases we can read off the cubic algebra from the analysis for a general field K above. So in the case when R_f is a maximal order, this lets us read off R_f/p and thus the splitting type of p in R_f from the splitting of f modulo p.

The parametrization of cubic rings given above seems so simple, that at first glance one might think that one could parametrize all rank n rings this way. However, things get much more complicated quickly. As mentioned above, the construction of a rank n ring from a binary n-ic form works for all n [Woo11c], but for $n>3$ not all rings are obtained this way. The paper [Woo11c] proves that the rings obtained this way are the ones with certain special kinds of ideal classes. For more reading on parametrizations of rings and ideal classes in rings, see [Bha04b, Bha04a, Bha04c, Bha08, Woo11b, Woo11a, Woo11c, Woo12, Woo14, EW11].

11.2. **Fundamental domain.** Let $V_{\mathbb{Z}}$ be the space of binary cubic forms over $\mathbb{Z}$ (in the first sense, so $V_{\mathbb{Z}}=\mathbb{Z}^4$), and $V_{\mathbb{R}}$ be the space of binary cubic forms over $\mathbb{R}$. Let F be a fundamental domain for the action of $\mathrm{GL}_2(\mathbb{Z})$ on binary cubic forms. Let F_X be the intersection of F with $\{v || \operatorname{Disc}(v)| < X\}$. Given the above parametrization, we would like to count $\mathrm{GL}_2(\mathbb{Z})$ orbits of $V_{\mathbb{Z}}$ of discriminant up to X, with additional conditions we will come back to later. This is the same as counting lattice points of $V_{\mathbb{Z}}$ in F_X, asymptotically in X. To solve this problem, we will use geometry of numbers techniques. From the beginning, we should note that F_X is *not* expanding homogeneously in X. The $|\operatorname{Disc}(v)|<X$ boundaries are homogeneously expanding, but the boundaries of F are not expanding as X grows. So the geometry of numbers is more complicated than the first examples ones sees in number theory.

Davenport [Dav51] writes down explicit equations for a fundamental domain F using Hermite's reduction theory of binary cubic forms. Let

$$A=b^2-3ac, \quad B=bc-9ad, \quad \text{and } C=c^2-3bd. \tag{9}$$

Then the points in F are those satisfying

$$-A<B\le A<C \text{ or } 0\le B\le A=C.$$

These are fairly simple quadratic inequalities defining F. Davenport uses this fundamental domain to (successfully) count binary cubic forms, and eventually, with Heilbronn [DH71], to count cubic fields. However, we are going to use the approach of Bhargava [Bha05] (in his work counting quartic fields) to find a different fundamental domain.

Let $\mathcal{F}$ be Gauss's fundamental domain for $\mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{GL}_2(\mathbb{R})$. We can write

$$\mathcal{F}=\{na'k\lambda \mid n\in N'(a'), a'\in A', k\in K, \lambda\in\Lambda\},$$

where

$$N'(a')=\left\{\begin{pmatrix}1 & \\ n & 1\end{pmatrix} : n\in\nu(a')\right\}, \quad A'=\left\{\begin{pmatrix}t^{-1} & \\ & t\end{pmatrix} : t\ge\sqrt[4]{3}/\sqrt{2}\right\}, \quad \Lambda=\left\{\begin{pmatrix}\lambda & \\ & \lambda\end{pmatrix} : \lambda>0\right\},$$

and K is as usual the (compact) real special orthogonal group $\mathrm{SO}_2(\mathbb{R})$; here $\nu(a')$ is the union of either one or two subintervals of $[-\frac{1}{2},\frac{1}{2}]$ depending only on the value of $a'\in A'$.

Furthermore, if a' is such that $t \geq 1$, then $\nu(a') = [-\frac{1}{2}, \frac{1}{2}]$. (There is an unfortunate coincidence that a is the first coefficient of our binary cubic form and a' a diagonal matrix. This however is consistent with the literature, except for when the literature calls them both a.)

To recognize this fundamental domain as something we all know and love (the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane), consider the action on shapes of lattices in $\mathbb{C}$, realized as elements of the upper half-plane $\mathbb{H}$. (So τ in the upper half-plane corresponds to the shape of the lattice $\mathbb{Z} \oplus \tau\mathbb{Z}$.) Let $\mathrm{GL}_2^+(\mathbb{R})$ be the elements of positive discriminant.

Exercise 11.9. Show that a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})\backslash \mathrm{GL}_2^+(\mathbb{R})$ gives a fundamental domain for $\mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{GL}_2(\mathbb{R})$. Conversely, show that a fundamental domain for $\mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{GL}_2(\mathbb{R})$ that is contained in $\mathrm{GL}_2^+(\mathbb{R})$ gives a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})\backslash \mathrm{GL}_2^+(\mathbb{R})$.

So we consider the action of $\mathrm{GL}_2^+(\mathbb{R})$ on the upper half-plane $\mathbb{H}$ given by

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \circ \tau = \frac{D\tau + C}{B + A\tau}$$

for $\tau \in \mathbb{H}$. (This is the conjugate of the usual action by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.) We see that Λ is in the kernel of this action. In the quotient $\mathrm{GL}_2^+(\mathbb{R})/\Lambda$, the group K is the stabilizer of $i \in \mathbb{H}$. (If we consider not just shapes of lattices up to homothety, but actual lattices, then the lattices are equivalent to binary quadratic forms, and the $\mathrm{GL}_2^+(\mathbb{R})$-action can be lifted in the obvious way. The binary quadratic form $x^2 + y^2$ corresponds to the square lattice shape, which is represented by the point $i \in \mathbb{H}$. Then $\mathrm{Stab}_{\mathrm{GL}_2^+(\mathbb{R})}(x^2 + y^2) = \mathrm{SO}_2(\mathbb{R}) = K$.) So, we have that $\mathcal{F} \circ i = \{na \circ i \mid n \in N'(a), a' \in A'\}$. This is the familiar fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$.

The matrix $a' \in A'$ scales points in the upper-half plane by t^2. The group $N'(a')$ translates points in the upper-half plane to the left and right by at most $1/2$ in each direction. So $na \circ i = t^2 i + n$. Now we see that the inequalities defining $N'(a')$ and A' look familiar from our usual fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ on the upper half-plane.

The action of $\mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{Z}}$ has 2 4-dimensional orbits, corresponding to the cubic rings $\mathbb{R}^3$ and $\mathbb{R} \oplus \mathbb{C}$. These cover all the points of $V_{\mathbb{Z}}$ with non-zero discriminant. Let V^+ be the orbit where the points have positive discriminant (corresponding to $\mathbb{R}^3$) and V^- be the orbit where the points have negative discriminant (corresponding to $\mathbb{R} \oplus \mathbb{C}$). Let $v \in V^-$. Then, roughly, the idea is that $\mathcal{F}v$ is a fundamental domain for the action of $\mathrm{GL}_2(\mathbb{Z})$ on V^-. We can do everything similarly for V^+, so for now we will restrict our attention to V^-.

The presence of stabilizers means that $\mathcal{F}v$ is not a fundamental domain, but rather a "multi-fundamental domain." More precisely, we consider $\mathcal{F}v$ as the multiset $\{fv \mid f \in \mathcal{F}\}$.

Exercise 11.10. For $x \in V_{\mathbb{Z}}^-$, show that the number of times an element of $\mathrm{GL}_2(\mathbb{Z})x$ appears in $\mathcal{F}v$ is

$$\frac{\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}\,x}{\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}\,x}.$$

We note that for $x \in V_{\mathbb{Z}}^-$, we have $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}\,x = \mathrm{Aut}_{\mathbb{R}}(\mathbb{R} \oplus \mathbb{C}) = \mathbb{Z}/2\mathbb{Z}$. Also, $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}\,x$ are the automorphisms of the corresponding cubic ring, which will be trivial if the ring is a domain (in V^- there are no cyclic cubic fields), and will be $\mathbb{Z}/2\mathbb{Z}$ if the cubic ring is a subring of $K \oplus \mathbb{Q}$ for an imaginary quadratic field $\mathbb{Q}$. So $\mathcal{F}v$ covers all the points we are interested in twice, which is just as good as a fundamental domain (as long as we divide by 2 in the end).

Let $\mathcal{R}_X(v) = \mathcal{F}v \cap \{w \mid 1 \leq |\operatorname{Disc}(w)| < X\}$.

11.3. **Geometry of numbers.** To count points in this very problem, Davenport [Dav51] proved a general result on counting points in regions defined by polynomial inequalities. Let R be a region in $\mathbb{R}^n$ and let $N(R)$ be the number of lattice points in R. We would like to say

$$N(R) \approx \operatorname{Vol}(R),$$

and the real content of such a statement is an estimate for the error

$$|N(R) - \operatorname{Vol}(R)|.$$

We will now imagine what can contribute to such an error. In 2 dimensions, clearly, the perimeter of R is closely tied to this error. Consider a square that is $N + \epsilon$ by $M + \epsilon$. It may have as many as $(N + 1)(M + 1)$ or as few as NM lattice points, compared to its area which is near NM. Considering a $1/N \times 1/N$ box, which may have 1 or 0 points, we see we need a 1 in the error as well. In fact in two dimensions

$$|N(R) - \operatorname{Vol}(R)| \leq 4(L + 1),$$

where L is the length of the boundary of R.

In $\mathbb{R}^n$, a similar construction with a box shows that the volumes of the projections onto $\mathbb{R}^{n-1}$ by dropping a coordinate are related to the error $|N(R) - \operatorname{Vol}(R)|$. A box which is approximately $N_1 \times \cdots \times N_n$ will have volume $N_1 \ldots N_n$, but could have $N_1 \cdots N_n$ points or could have

$$N_1 \cdots N_n + N_2 \cdots N_n$$

points. However, these $n - 1$ dimensional projections are not enough. Consider a $1/N \times 1/N \times N$ box. This may have as few as 0 points or as many as N. However the 2-dimensional projections have size $1, 1, 1/N^2$, so are not large enough to account for this discrepancy, even allowing for constant factors. However, there is a 1-dimensional projection of size N. Davenport shows that these volumes of projections are indeed enough to bound the error.

Lemma 11.11 ([Dav51])**.** *Let R be a closed, bounded region in $\mathbb{R}^n$ defined by k polynomials of degree at most d, and let $h = kd/2$. Then*

$$|N(R) - \operatorname{Vol}(R)| \leq \sum_{m=0}^{n-1} h^{n-m} R_m,$$

where R_m is the sum of the m-dimensional volumes of the projections of R onto any of the coordinate spaces obtained by forgetting some $n - m$ coordinates, and $R_0 = 1$.

We also write this as

$$|N(R) - \operatorname{Vol}(R)| = O(\operatorname{Vol}(\operatorname{Proj}(R)), 1),$$

where the constant in the big O notation depends on the dimension n of R and the number and maximum degree of the defining inequalities. The notation $\operatorname{Proj}(R)$ is supposed to denote all the projections, and we write the 1 as not to forget the 0-dimensional projection.

11.4. **Averaging.** One advantage of taking a fundamental domain $\mathcal{F}v$ as we have done above (instead of Davenport's explicit F) is that this generalizes more easily to finding fundamental domains in more complicated situations, such as those Bhargava encounters when counting quartic and quintic fields [Bha05, Bha10b]. Another advantage is we can use an averaging technique due to Bhargava (in [Bha05], where he counts quartic fields) which significantly improves the geometry of numbers results. (Yet another advantage is that it will be simpler to compute the volume of our fundamental domain.)

The idea of averaging is that $\mathcal{F}v$ is a fundamental domain for any choice of v, so in fact we have many fundamental domains. Now since they are all fundamental domains, the number of lattice points in $\mathcal{R}_X(v)$ does not depend on v (for $v \in V^-$). So we will average over many such v, and obtain the same count as in one $\mathcal{F}v$.

At first, it might seem counterintuitive that this can help. The key is that the answer is the same, but we have more tools to estimate the averaged number of points. It sometimes helps to first think about a discrete averaging scenario. Image a fundamental domain for the action of $\mathbb{Z}$ on $\mathbb{R}^2$ by addition in the y coordinate, and we would like to count lattice points with $|x| \leq X$, asymptotically in X (and we are ignoring constant factors). This is like counting lattice points in a $1 \times X$ box, so the volume is order X, but there is a projection of size X. We cannot get a useful result from Davenport's geometry of numbers Lemma 11.11 in this case, so we have to use more information. Given the volume of the box and the size of its projections, it could have as many as 0 points or as many as X (up to constants). Suppose instead we take X fundamental domains, all stacked on top of each other to form a $X \times X$ box. Now, the fact that they make a nice box exactly (e.g. each was, say, closed on the bottom and open on the top, and they perfectly fit together) essentially comes from the fact that they are fundamental domains. So we get $X^2 + O(X)$ points in our X fundamental domains, and so $X + O(1)$ in a single fundamental domain. We could not have gotten an error term this small without using the fact that our region was a fundamental domain.

Now continuous averaging can be even more powerful. We will average over v in some bounded compact region B. You should think of B as a ball. So for each $v \in B$, we get some number of lattice points in $\mathcal{R}_X(v) = \mathcal{F}v \cap \{w \mid 1 \leq |\operatorname{Disc}(w)| < X\}$. We could average this over v in B according to any measure we choose on B, and the answer would be the same (the same as the number of lattice points in a single fundamental domain), but the measure we choose will affect whether we can find said answer.

For each $v \in B$, we are counting lattice points in $\mathcal{F}v \cap \{w \mid 1 \leq |\operatorname{Disc}(w)| < X\}$ and then we are adding up (integrating) over v. Intuitively, it is not hard to imagine this is related to counting lattice points in $gB \cap \{w \mid 1 \leq |\operatorname{Disc}(w)| < X\}$ for each $g \in \mathcal{F}$. To actually change variables from an integral over $v \in B$ to an integral over $g \in \mathcal{F}$ is somewhat delicate (see problem 62 in the problem set), and in particular in order to end up with a reasonable measure on $g \in \mathcal{F}$ for integrating with respect to, we need to have carefully chosen our measure on $v \in B$. We will take the measure on $v \in B$ to be the pushforward of the Haar measure on $\mathrm{GL}_2(\mathbb{R})$, and the result is that we need to average the number of points in gB over $g \in \mathcal{F}$ with respect to Haar measure on $\mathcal{F}$.

The question that remains is what the gB look like and if they are easy to count points in. Write $g \in \mathcal{F}$ as $g = na'k\lambda$. We are interested in $na'k\lambda B$. First it is useful to understand what g does to the discriminant, and how X is involved. The matrix λ multiplies each of a, b, c, d by λ, and thus scales the discriminant by λ^4.

Exercise 11.12. Show that the actions of n, a', k do not change the discriminant of a binary cubic form.

We can, for example, pick our B so that all the discriminants of points $v \in B$ are between 1 and 2. Since we would only like to count lattice points with absolute discriminant between 1 and X, that means λ is ranging between $2{-}4$ and $X^{1/4}$, or up to multiplicative constants between 1 and $X^{1/4}$. Once $\lambda \geq X^{1/4}$, there are no points in gB of discriminant $< X$. This is the main place that X comes in to play.

Now λ just scales our ball B, so in particular does not change its shape, so λB is a good shape for geometry of numbers. We have $\mathrm{Vol}(\lambda B)$ is of order λ^4 (up to multiplicative constants, that depend on B) and the largest projection is $O(\lambda^3)$.

Now for k, we can just pick a B that is fixed by K so that $kB = B$ for each $k \in K$. (For this it is important that K is compact. If we had chosen a B that was not fixed by K, we could just average it over K to obtain a choice that was fixed by K.)

The element $a' \in A'$ will stretch our ball B by different amounts in different directions. We have that

$$a' \circ (a, b, c, d) = (t^{-3}a, t^{-1}b, tc, t^3 d).$$

This is exactly the kind of thing that can make a terrible region for geometry of numbers. Suppose t is some large number Y. Then we have that $a'B$ is a region of volume $\mathrm{Vol}(a'B) = \mathrm{Vol}(B)$. However, the projection onto the d coordinate is order of magnitude Y^3, which is much bigger than the volume (as, say, we take Y larger and larger). It turns out that this reflects a reality about the shape of our fundamental domains $\mathcal{F}v$ that we can't get around by averaging. They have a long, skinny cusp around $a = 0$.

What saves us here is that the forms with $a = 0$ correspond to cubic rings that are not domains (as we saw above). So we don't want to count points with $a = 0$ in the end. So, instead of counting points in $\mathcal{R}_X(v) = \mathcal{F}v \cap \{w \mid 1 \leq |\operatorname{Disc}(w)| < X\}$, we will intersect that region with $|a| \geq 1$ and count points there.

Before we keep going with the geometry of numbers, we want to point out an issue. All of our fundamental domains contained the same number of points, because they all correspond to orbits of something (counted with $1/\#\,\mathrm{Stab}$ weight). However, when we add the condition $|a| \geq 1$ this is no longer true. The fundamental domains intersected with $|a| \geq 1$ may now include different numbers of reducible orbits (we only got rid of reducible forms when we eliminated the case $a = 0$). In the end we will be able to deal with this–we were going to have to get rid of reducible forms anyway at some point.

Now, let C be the maximum $|a|$ for any form in B. So we have that in $a'k\lambda B$, the maximum x^3 coefficient is $t^{-3}\lambda C$.

Exercise 11.13. Show that the action of n does not change the a coordinate.

Thus, we only need to consider g with $\lambda \leq X^{1/4}$, and t so that $C\lambda/t^3 \geq 1$. This means that t cannot get too large, and so a' does not make our region too stretched out.

11.5. **Counting lattice points after a lower triangular transformation.** Now we come to n. A method of the author [Woo06] allows one to completely generally ignore lower triangular transformations when applying Davenport's geometry of numbers Lemma 11.11 (even if the lower triangular transformations are not bounded). Let's first consider a simple example. Suppose you have a roughly X by X region H (so it has around X^2 lattice points, with $O(X)$ error). Now we apply a shear mapping s that sends a point with coordinate $(x,y) \mapsto (x, y + X^2 x)$. So the sheared region $s(H)$ has the same volume X^2 as H, but now the projection onto the second coordinate is size X^3, so we can't use Davenport's geometry of numbers lemma to count points in this region.

However, since a slice for each x coordinate was just shifted up in the plane, we can see that each slice of $s(H)$ has almost the same number of lattice points as H (differing by at most 1). In fact, if we merely translate a region R in $\mathbb{R}^n$ to $t(R)$ since we don't change the volume or the size of the projections, we can only change the number of lattice points from R to $t(R)$ by $O(\mathrm{Proj}(R)+1)$.

More generally we have the following. Recall for a region E in $\mathbb{R}^n$, we let $N(E)$ be the number of points in $\mathbb{Z}^n \cap E$.

Theorem 11.14 ([Woo06])**.** *If E is a semi-algebraic region of $\mathbb{R}^n$ and T is an upper (or lower) triangular linear transformation of $\mathbb{R}^n$ with ones along the diagonal, then*

$$|N(E) - N(T(E))| = O(\mathrm{Vol}\,\mathrm{Proj}\,E + 1),$$

where $\mathrm{Vol}\,\mathrm{Proj}\,E$ denotes the volume of the largest (in volume) projection of E onto any proper coordinate hyperplane (of any dimension $< n$). The constant in the O notation depends only on n and the degree of the semi-algebraic region.

Proof. Write $T = t_k \circ \cdots \circ t_2$, where t_i is a linear transformation that fixes the value of x_j for $j \neq i$, and for a point P we have $x_i(T(P)) = x_i + \lambda_{i-1}x_{i-1} + \lambda_{i-2}x_{i-2} + \cdots + \lambda_1 x_1$.

Lemma 11.15. *For any semi-algebraic region E of $\mathbb{R}^n$*

$$|N(E) - N(T(E))| = O(N\,\mathrm{Proj}\,E),$$

where NProj(E) is the number of $\mathbb{Z}^n$ points in the projection of E onto a proper coordinate hyperplane that has the most lattice points. The constant in the O notation depends on n and the degree of E.

Proof. We induct on the number of terms t_i in T. First, we assume $T = t_i$. For a given set of $c_j \in \mathbb{Z}$, we consider the line $L = \{x_j = c_j : j \neq i\}$. The region $R \cap L$ is a union of intervals on the line. Since T only affects the coordinate x_i, we have that T preserves L and $T(E) \cap L = T(E \cap L)$. The transformation T just translates the intervals of $R \cap L$ along L. Since an interval of length ℓ has between $\ell - 1$ and $\ell + 1$ integral points, the difference $|N(E \cap L) - N(T(E) \cap L)|$ is at most twice the number of intervals of $E \cap L$, which is bounded by the degree of E. It remains to estimate the number of choices of c_j (for all $j \neq i$) such that $E \cap L$ is non-empty. This is exactly the number of lattice points in the projection of E onto $x_i = 0$, which is $O(N\,\mathrm{Proj}\,E)$.

Assuming the inductive hypothesis, we write $T = t_k \circ \cdots \circ t_2$ and $T' = t_{k-1} \circ \cdots \circ t_2$. We have

$$N(E) - N(T(E)) = N(E) - N(T'(E)) + N(T'(E)) - N(t_k \circ T'(E)),$$

and by the inductive hypothesis, we have

$$|N(E) - N(T'(E))| \leq O(N\,\mathrm{Proj}\,E). \tag{10}$$

By our work above, for the case $k = 1$ we have

$$|N(T'(E)) - N(t_k \circ T'(E))| \leq O(N(T'(E)_k)),$$

where $T'(E)_k$ is the projection of $T'(E)$ onto the hyperplane cut out by $x_k = 0$. For a point P, the values of $x_i(T'(P))$ for $i \neq k$ do not depend on $x_k(P)$, we have that $T'(E)_k$ is just T' applied to the projection E_k of E onto the hyperplane $x_k = 0$. Thus,

$$|N(T'(E)) - N(t_k \circ T'(E))| \leq O\left(N\left(T'(E_k)\right)\right). \tag{11}$$

By the inductive hypothesis, we have

$$N(T'(E_k)) - N(E_k) \leq O\left(N \operatorname{Proj} E_k\right). \tag{12}$$

Thus combining Equations (10), (11), and (12), we have

$$|N(E) - N\left(T(E)\right)| \leq O\left(N \operatorname{Proj} E + N(E_k) + N \operatorname{Proj} E_k\right),$$

proving the lemma. (Though at each step of the induction, the constants in the O notation might grow, they are bounded in terms of n). Note that if E has infinitely many lattice points, then so does some projection of E onto a coordinate hyperplane. □

The number of points in the projection E' of E onto some proper coordinate plane is $\operatorname{Vol} E' + O(\operatorname{Proj} E' + 1)$. Since every projection of E' onto a proper coordinate hyperplane is also a projection of E, we have that $|N(E) - N\left(T(E)\right)| = O(\operatorname{Proj} E + 1)$, as desired. □

Though this general result is often quoted, in some cases, including our problem at hand (counting binary cubic forms), one can use a simpler argument that involves the specific lower triangular transformation and the shape of the region it is being applied to (see Exercise 46 in the problem set). In any case, we conclude that we only need to estimate the size of the projections of $a'k\lambda B$ in order to bound the error between the number of lattice points in gB and the volume of gB.

11.6. **Estimating the projections.** We have that $a'k\lambda B = a'\lambda k B = a'\lambda B$. We have

$$a'\lambda \circ (a, b, c, d) = (\lambda t^{-3} a, \lambda t^{-1} b, \lambda t c, \lambda t^3 d),$$

and λ, t are bounded below by constants. Also, recall from the end of Section 11.4, we had $\lambda = O(X^{1/4})$ and $t = O(\lambda^{1/3})$. So we can bound the volume of each of the projections of $a'k\lambda B$, using the fact that B is fixed. For example, the projection onto the last three coordinates has size $O(\lambda t^{-1} \cdot \lambda t \cdot \lambda t^3) = O(\lambda^3 t^3)$. The projection onto the last coordinate is size $O(\lambda t^3)$, but this is $O(\lambda^3 t^3)$ since λ is bounded below by a constant. Similarly, we can bound each of the lower dimensional projections and conclude

$$\operatorname{Vol} \operatorname{Proj}(a'k\lambda B) = O(\lambda^3 t^3).$$

We then integrate over the Haar measure dg (see Problem 6.4 on the problem set for the determination of the Haar measure). We have (where the below ignores constant factors in all inequalities)

$$\begin{aligned}\int_{g\in\mathcal{F}, gB\cap\{1\le|\operatorname{Disc}(-)|<X\}\cap\{|a|\ge1\}\neq\emptyset}\operatorname{Vol}\operatorname{Proj}(a'k\lambda B)dg &\le \int_{g\in\mathcal{F},1\le\lambda\le X^{1/4},1\le t\le\lambda^{1/3}} O(\lambda^3t^3)\lambda^{-1}t^{-3}d\lambda dtdndk\\ &= \int_{g\in\mathcal{F},1\le\lambda\le X^{1/4},1\le t\le\lambda^{1/3}} O(\lambda^2)d\lambda dtdndk\\ &= \int_{(n,a',k,\lambda)\in\mathcal{F},1\le\lambda\le X^{1/4}} O(\lambda^{7/3})d\lambda dndk\\ &= \int_{n\in N',k\in K} O(X^{5/6})dndk.\end{aligned}$$

The final integral is $O(X^{5/6})$ because we have that N' and K are compact and fixed (where N' is the union of all the $N'(a')$, i.e. $N' = N'(a')$ for a value of a' with $t \ge 1$).

11.7. **Putting the count together.** To put all the pieces together, we need to also compute the (average over g) volumes of our gB's, which we can do by reversing the change of variables we did above and instead computing volumes of fundamental domains $\mathcal{F}v$. For this, we can use a well-known calculation of the volume of $\mathcal{F}$. The average volume is order of X, and so the error term $O(X^{5/6})$ above is indeed small enough.

Also, our count now includes some reducible binary cubic forms (but not all of them since we cut out the $a = 0$ forms in each fundamental domain). First of all, notice that it we had included all of them, it would have contributed to our main term. For each quadratic field K with $|\operatorname{Disc}(K)| < X$, we have a cubic ring R which is the maximal order in $K \oplus \mathbb{Q}$, and has $|\operatorname{Disc}(R)| < X$. So if we counted all classes of reducible binary cubic forms, we would be seeing the reducible ones contribute to our main term (as $N_{S_2}(X) \sim cX$). (This perhaps would not be so bad, because we have an exact main term for $N_{S_2}(X)$.) However, it turns out that by discarding the $a = 0$ forms, we have thrown out 100% (asymptotically in X) of the reducible forms (though the precise number we have thrown out in $\mathcal{F}v$ can depend a bit on v). See Problems 69 and 70 in the problem set or Lemma 21 of [BST13].

11.8. **Sieving for maximal rings.** So far, we have outlined the proof of counting classes of binary cubic forms that correspond to orders in cubic fields. The final step to count cubic fields is to sieve for maximal orders. We discussed above that maximality at p of the cubic ring can be given by a condition on the form modulo p^2. One can compute [BST13, Lemma 19] the proportion $\mu(\mathcal{U}_p)$ of binary cubic forms modulo p that correspond to cubic rings that are maximal at p. One then can do all the above counting, but instead of using integral binary cubic forms, only using ones with "maximal" reductions modulo p^2. One would get the main term multiplied by $\mu(\mathcal{U}_p)$, and the same error term *with the constant in the error term now depending on p.* For finitely many primes, one can sieve like this, but for infinitely many primes, the constant in the error term could in theory go off to infinity. One needs a uniform error bound to sieve at infinitely many primes.

This is a sieve in the spirit of the sieve for squarefree integers that is discussed in Poonen's Arizona Winter School 2014 lectures and in Problems 53-55 of the problem set, but the error bounds one needs as input are more sophisticated. (The sieve itself is carried out in Problem 78 of the problem set, but assuming the required input bound–see [BST13, Section 8.2] for the required bound.) One can finally obtain the following result of Davenport and Heilbronn.

Theorem 11.16. *We have*

$$N_{S_3}(X) \sim \frac{1}{3\zeta(3)} X.$$

If instead, we sieve for cubic rings that are not only maximal at p but also not totally ramified at p, we are counting 2-torsion in class groups of cubic fields (see Section 3). One final result of Davenport and Heilbronn [DH71] is

$$\lim_{X\to\infty} \frac{\sum_{K\in D(X) K \text{ imag quad}} |Cl(K)/3Cl(K)|}{\#\{K \in D(X) \mid K \text{ imag quad}\}} = 2.$$

We will see a sieve like that is necessary for either of these cases in the next section.

12. Counting Galois S_3 sextics

In this section, we outline a result from [BW08] giving the asymptotics of $N_{S_3\subset S_6}(X)$, where S_3 is acting via its regular representation. As discussed above, this gives another example of counting fields by an invariant other than their discriminant. It will also show the kind of sieve that is necessary to sieve for even maximal cubic rings in Davenport and Heilbronn's result above. We are counting non-Galois cubic fields by the discriminant of their Galois closure. Degree 6 number fields with Galois group $S_3 \subset S_6$ are called S_3-*sextic fields*, and they are Galois over $\mathbb{Q}$. We are able to obtain an exact asymptotic in this case.

Theorem 12.1 ([BW08])**.** *We have* $N_{S_3\subset S_6}(X) \sim \left(\frac{1}{3}\prod_p c_p\right) X^{1/3}$, *where the product is over primes,* $c_p = (1 + p^{-1} + p^{-4/3})(1 - p^{-1})$ *for* $p \neq 3$*, and* $c_3 = (\frac{4}{3} + \frac{1}{3^{5/3}} + \frac{2}{3^{7/3}})(1 - \frac{1}{3})$.

Theorem 12.1 was also obtained (independently) by Belabas-Fouvry [BBP10] as a result of a deeper study of S_3-sextic fields. To compare with Davenport and Heilbronn's theorem

$$N_{S_3}(X) \sim \frac{1}{3\zeta(3)} X,$$

we may write $\frac{1}{\zeta(3)} = \prod_p (1 + p^{-1} + p^{-2})(1 - p^{-1})$.

Any S_3-sextic field K_6 contains a unique (up to conjugation) non-Galois cubic subfield K_3. Conversely, any non-Galois cubic field K_3 has a unique Galois closure K_6, which is an S_3-sextic field. Let K_3 and K_6 be such for the rest of the section. Let $v_p(n)$ denote the exponent of the largest power of p that divides n. If K_3 is nowhere totally or wildly ramified, then $d(K_6) = d(K_3)^3$. If this were always the case, then the asymptotics of $N(X, S_3(6))$ would follow immediately from Theorem 11.16. However, at a tame rational prime p, the possible ramification types in K_3 are $\mathfrak{p}_1^2\mathfrak{p}$ *and* $\mathfrak{p}^3$, and $v_p(d(K_3))$ is 1 and 2 in these cases, respectively. These give, respectively, splitting types $\wp_1^2\wp_2^2\wp_3^2$ and $\wp_1^3\wp_2^3$ in K_6, and hence $v_p(d(K_6))$ is 3 and 4 in these cases, respectively. We call primes p of the second type *overramified* in K_3 (or K_6).

If tamely overramified primes exist, then evidently $d(K_3)^3 \neq d(K_6)$. To prove Theorem 12.1, we define transitional discriminants $d_Y(K_6)$ for K_6 that "correct" $d(K_3)^3$ to $d(K_6)$ at the primes less than Y:

Definition. Let $d_Y(K_6)$ be the positive integer such that

$$v_p(d_Y(K_6)) = \begin{cases} v_p(d(K_6)) & \text{if } p \text{ is a prime} < Y \\ v_p(d(K_3)^3) & \text{if } p \text{ is a prime} \geq Y \end{cases}.$$

In fact, a stronger version of Theorem 11.16 is true, and is proven with essentially the same methods. For an integer m, let ϕ_m be the map that takes binary cubic forms with integer coefficients to binary cubic forms with coefficients in $\mathbb{Z}/m\mathbb{Z}$, via reduction of the coefficients modulo m. For each of *finitely many* rational primes p_i, let us specify a set Σ_i of étale cubic $\mathbb{Q}_{p_i}$-algebras and let Σ_i' be the corresponding set of maximal $\mathbb{Z}_{p_i}$-orders. For some $m = \prod_i p_i^{n_i}$, there are sets U and S of binary cubic forms with coefficients in $\mathbb{Z}/m\mathbb{Z}$ such that $\phi_m^{-1}(U)$ is the set of forms which correspond to rings which are maximal at all p_i and $\phi_m^{-1}(S)$ is the set of forms which correspond to rings which are maximal at all p_i and whose p_i-adic completions are in Σ_i'. We define the *relative density* of $\{\Sigma_i\}_i$ to be $\#S/\#U$. By the Chinese Remainder Theorem, this relative density is simply the product of the *relative p_i-adic densities* of the individual Σ_i, defined as above in the case that $\{p_i\}_i$ has one element. The strengthened version of Theorem 11.16 we require is that

(13)

$$\#\{K \in \mathcal{F}(S_3) \mid d(K) < X \text{ and } K \otimes \mathbb{Q}_{p_i} \in \Sigma_i \text{ for all } i\} \;\sim\; (\text{relative density of } \{\Sigma_i\}_i) \cdot \frac{X}{3\zeta(3)}.$$

(For further details on this strengthened Theorem 11.16, see [DH71, Section 5] or [BST13, Theorem 31].) Since $d_Y(K_6)$ only differs from $d(K_3)^3$ at finitely many primes, we can compute the asymptotics of $N_Y(X) := \#\{K_6 \mid d_Y(K_6) < X\}$ directly from such a strengthened version of Theorem 11.16.

In [BW08] we compute these relative densities and obtain

$$\lim_{X\to\infty} \frac{N_Y(X)}{X^{1/3}} = \frac{c_2c_3}{(1-2^{-3})(1-3^{-3})} \prod_{3<p<Y} \frac{1+p^{-1}+p^{-4/3}}{1+p^{-1}+p^{-2}} \frac{1}{3\zeta(3)}.$$

Taking the limit in Y, we obtain

$$\lim_{Y\to\infty} \lim_{X\to\infty} \frac{N_Y(X)}{X^{1/3}} = \frac{c_2c_3}{3\zeta(3)} \prod_{p>3} \frac{1+p^{-1}+p^{-4/3}}{1+p^{-1}+p^{-2}}. \tag{14}$$

12.1. **Proof of Theorem 12.1.** We now compute the asymptotics of $N(X) := N_{S_3\subset S_6}(X)$. Note that for $Y > 3$, we have $N_Y(X) \leq N(X)$ and thus

$$\lim_{Y\to\infty} \lim_{X\to\infty} \frac{N_Y(X)}{X^{1/3}} \leq \liminf_{X\to\infty} \frac{N(X)}{X^{1/3}}. \tag{15}$$

To obtain an upper bound, let $M(n, X) = \#\{K_3 \text{ overramified at all primes } p|n,\ d(K_3) < X\}$. From [BF10, Lemma 3.3], we know $M(n, X) = O(n^{-2+\epsilon}X)$. If K_6 is an S_3-sextic field with $d(K_6) < X$, and n is the product of the primes where K_6 is overramified, then $d(K_3) < cn^{2/3}X^{1/3}$ for some finite absolute constant c given by the behavior of the finitely many 2-adic and 3-adic cubic algebras (in fact, we may take $c = 36$). Thus,

$$N(X) \leq N_Y(X) + \sum_{n\geq Y} M(n, cn^{2/3}X^{1/3}) \leq N_Y(X) + d\sum_{n\geq Y} \frac{X^{1/3}}{n^{4/3+\epsilon}}$$

for some constant d. Taking limits in X, we obtain

$$\limsup_{X\to\infty} \frac{N(X)}{X^{1/3}} \leq \lim_{X\to\infty} \frac{N_Y(X)}{X^{1/3}} + d\sum_{n\geq Y} \frac{1}{n^{4/3+\epsilon}},$$

and then taking limits in Y, we conclude

$$\limsup_{X\to\infty} \frac{N(X)}{X^{1/3}} \leq \lim_{Y\to\infty} \lim_{X\to\infty} \frac{N_Y(X)}{X^{1/3}}. \tag{16}$$

Equations (15) and (16) combine to prove $\lim_{X\to\infty} \frac{N(X)}{X^{1/3}} = \lim_{Y\to\infty} \lim_{X\to\infty} \frac{N_Y(X)}{X^{1/3}}$, which together with Equation (14) proves Theorem 12.1.

In [BW08, Section 5], we give an interpretation of the constants c_p above, which are exactly as predicted by the Malle-Bhargava principle discussed above. Further the work in [BW08] shows that the Malle-Bhargava principle holds in full generality, with local behaviors, in the case $G = S_3 \subset S_6$.

Acknowledgements. This article was developed from lecture notes for a series of five lectures at the Arizona Winter School on "Arithmetic statistics" held March 15-19, 2014 in Tucson, Arizona. Thank you to Bjorn Poonen, Michiel Kosters, Jonah Leshin, and especially the anonymous referee for helpful comments. This work was done with the support of an American Institute of Mathematics Five-Year Fellowship and National Science Foundation grants DMS-1147782 and DMS-1301690.

References

[AM15] Michael Adam and Gunter Malle. A class group heuristic based on the distribution of 1-eigenspaces in matrix groups. *Journal of Number Theory*, 149:225–235, April 2015.

[AT68] E. Artin and J. Tate. *Class field theory*. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[BBP10] Karim Belabas, Manjul Bhargava, and Carl Pomerance. Error estimates for the Davenport-Heilbronn theorems. *Duke Mathematical Journal*, 153(1):173–210, May 2010.

[BDF$^+$15] Alina Bucur, Chantal David, Brooke Feigon, Nathan Kaplan, Matilde Lalín, Ekin Ozman, and Melanie Matchett Wood. The distribution of $\mathbb{F}_q$-points on cyclic ℓ-covers of genus g. *arXiv:1505.07136 [math]*, May 2015.

[BF10] Karim Belabas and Étienne Fouvry. Discriminants cubiques et progressions arithmétiques. *International Journal of Number Theory*, 6(7):1491–1529, 2010.

[Bha04a] Manjul Bhargava. Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. *Annals of Mathematics. Second Series*, 159(1):217–250, 2004.

[Bha04b] Manjul Bhargava. Higher composition laws. II: On cubic analogues of Gauss composition. *Annals of Mathematics*, 159(2):865–886, March 2004.

[Bha04c] Manjul Bhargava. Higher composition laws III: The parametrization of quartic rings. *Annals of Mathematics*, 159(3):1329–1360, May 2004.

[Bha05] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Annals of Mathematics*, 162(2):1031–1063, September 2005.

[Bha08] Manjul Bhargava. Higher composition laws. IV. The parametrization of quintic rings. *Annals of Mathematics. Second Series*, 167(1):53–94, 2008.

[Bha10a] Manjul Bhargava. The density of discriminants of quintic rings and fields. *Annals of Mathematics*, 172(3):1559–1591, October 2010.

[Bha10b] Manjul Bhargava. Mass Formulae for Extensions of Local Fields, and Conjectures on the Density of Number Field Discriminants. *International Mathematics Research Notices*, July 2010.

[BKLj^{+}13] Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra jr., Bjorn Poonen, and Eric Rains. Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves. *arXiv:1304.3971 [math]*, April 2013.

[BST13] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. On the Davenport–Heilbronn theorems and second order terms. *Inventiones mathematicae*, 193(2):439–499, August 2013.

[BW08] Manjul Bhargava and Melanie Matchett Wood. The density of discriminants of S_3-sextic number fields. *Proceedings of the American Mathematical Society*, 136(5):1581–1587, 2008.

[CDyDO02a] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. Enumerating quartic dihedral extensions of $\mathbb{Q}$. *Compositio Mathematica*, 133(1):65–93, 2002.

[CDyDO02b] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. On the density of discriminants of cyclic extensions of prime degree. *Journal für die Reine und Angewandte Mathematik*, 550:169–209, 2002.

[CL84] Henri Cohen and Hendrik W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[CM90] Henri Cohen and Jacques Martinet. Étude heuristique des groupes de classes des corps de nombres. *Journal für die Reine und Angewandte Mathematik*, 404:39–76, 1990.

[CM94] Henri Cohen and Jacques Martinet. Heuristics on class groups: some good primes are not too good. *Mathematics of Computation*, 63(207):329–334, 1994.

[Coh54] Harvey Cohn. The density of abelian cubic fields. *Proceedings of the American Mathematical Society*, 5:476–477, 1954.

[Coh03] Henri Cohen. Enumerating quartic dihedral extensions of $\mathbb{Q}$ with signatures. *Université de Grenoble. Annales de l'Institut Fourier*, 53(2):339–377, 2003.

[Dav51] H. Davenport. On a principle of Lipschitz. *Journal of the London Mathematical Society. Second Series*, 26:179–183, 1951.

[Del] Pierre Deligne. letter to W. T. Gan, B. Gross and G. Savin. November 13, 2000.

[DF64] B. N. Delone and D. K. Faddeev. *The theory of irrationalities of the third degree.* Translations of Mathematical Monographs, Vol. 10. American Mathematical Society, Providence, R.I., 1964.

[DH71] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proceedings of the Royal Society. London. Series A. Mathematical, Physical and Engineering Sciences*, 322(1551):405–420, 1971.

[DW86] Boris Datskovsky and David J. Wright. The adelic zeta function associated to the space of binary cubic forms. II. Local theory. *Journal für die Reine und Angewandte Mathematik*, 367:27–75, 1986.

[EW11] Daniel Erman and Melanie Matchett Wood. Gauss Composition for Pˆ1, and the universal Jacobian of the Hurwitz space of double covers. *arXiv:1111.0498 [math]*, November 2011.

[FK06a] Étienne Fouvry and Jürgen Klüners. Cohen–Lenstra Heuristics of Quadratic Number Fields. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Algorithmic Number Theory*, number 4076 in Lecture Notes in Computer Science, pages 40–55. Springer Berlin Heidelberg, January 2006.

[FK06b] Étienne Fouvry and Jürgen Klüners. On the 4-rank of class groups of quadratic number fields. *Inventiones mathematicae*, 167(3):455–513, November 2006.

[Gar14] Derek Garton. Random matrices, the Cohen-Lenstra heuristics, and roots of unity. *arXiv:1405.6083 [math]*, May 2014.

[Ger87a] Frank Gerth, III. Densities for ranks of certain parts of p-class groups. *Proceedings of the American Mathematical Society*, 99(1):1–8, 1987.

[Ger87b] Frank Gerth, III. Extension of conjectures of Cohen and Lenstra. *Expositiones Mathematicae. International Journal for Pure and Applied Mathematics*, 5(2):181–184, 1987.

[GGS02] Wee Teck Gan, Benedict Gross, and Gordan Savin. Fourier coefficients of modular forms on G_2. *Duke Mathematical Journal*, 115(1):105–169, 2002.

[Gru33] Wilhelm Grunwald. Ein allgemeines Existenztheorem für algebraische Zahlkörper. *Journal für die reine und angewandte Mathematik (Crelle's Journal)*, 1933(169), 1933.

[Has30] Helmut Hasse. Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. *Mathematische Zeitschrift*, 31(1):565–582, 1930.

[Hei34] Hans Heilbronn. On the class-number in imaginary quadratic fields. *The Quarterly Journal of Mathematics*, os-5(1):150–160, 1934.

[Ked07] Kiran S. Kedlaya. Mass formulas for local Galois representations. *International Mathematics Research Notices. IMRN*, (17):Art. ID rnm021, 26, 2007. With an appendix by Daniel Gulotta.

[Kli98] Norbert Klingen. *Arithmetical similarities*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1998. Prime decomposition and finite group theory, Oxford Science Publications.

[Klü05] Jürgen Klüners. A counterexample to Malle's conjecture on the asymptotics of discriminants. *Comptes Rendus Mathématique. Académie des Sciences. Paris*, 340(6):411–414, 2005.

[Klü06] Jürgen Klüners. Asymptotics of number fields and the Cohen–Lenstra heuristics. *Journal de Théorie des Nombres de Bordeaux*, 18(3):607–615, 2006.

[Klü12] Jürgen Klüners. The distribution of number fields with wreath products as Galois groups. *International Journal of Number Theory*, 8(3):845–858, 2012.

[KM04] Jürgen Klüners and Gunter Malle. Counting nilpotent Galois extensions. *Journal für die Reine und Angewandte Mathematik*, 572:1–26, 2004.

[Mäk85] Sirpa Mäki. On the density of abelian number fields. *Annales Academiae Scientiarum Fennicae. Series A I. Mathematica Dissertationes*, (54):104, 1985.

[Mäk93] Sirpa Mäki. The conductor density of abelian number fields. *Journal of the London Mathematical Society. Second Series*, 47(1):18–30, 1993.

[Mal02] Gunter Malle. On the distribution of Galois groups. *Journal of Number Theory*, 92(2):315–329, 2002.

[Mal04] Gunter Malle. On the distribution of Galois groups. II. *Experimental Mathematics*, 13(2):129–135, 2004.

[Mal08] Gunter Malle. Cohen–Lenstra heuristic and roots of unity. *Journal of Number Theory*, 128(10):2823–2835, October 2008.

[Mal10] Gunter Malle. On the Distribution of Class Groups of Number Fields. *Experimental Mathematics*, 19(4):465–474, 2010.

[Nar83] W. Narkiewicz. *Number theory*. World Scientific Publishing Co., Singapore, 1983. Translated from the Polish by S. Kanemitsu.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[NSW00] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2000.

[Poo08] Bjorn Poonen. The moduli space of commutative algebras of finite rank. *Journal of the European Mathematical Society*, pages 817–836, 2008.

[Tay84] M. J. Taylor. On the equidistribution of Frobenius in cyclic extensions of a number field. *Journal of the London Mathematical Society. Second Series*, 29(2):211–223, 1984.

[TT13] Takashi Taniguchi and Frank Thorne. Secondary terms in counting functions for cubic fields. *Duke Mathematical Journal*, 162(13):2451–2508, October 2013.

[Tur08] Seyfi Turkelli. Connected Components of Hurwitz Schemes and Malle's Conjecture. *arXiv:0809.0951 [math]*, September 2008.

[Wan50] Shianghaw Wang. On Grunwald's theorem. *Annals of Mathematics. Second Series*, 51:471–484, 1950.

[Woo06] Melanie Matchett Wood. Lemma on the number of lattice points after triangular transformation. 2006. preprint.

[Woo08] Melanie Matchett Wood. Mass formulas for local Galois representations to wreath products and cross products. *Algebra & Number Theory*, 2(4):391–405, June 2008.

[Woo10] Melanie Matchett Wood. On the probabilities of local behaviors in abelian field extensions. *Compositio Mathematica*, 146(1):102–128, 2010.

[Woo11a] Melanie Matchett Wood. Gauss composition over an arbitrary base. *Advances in Mathematics*, 226(2):1756–1771, January 2011.

[Woo11b] Melanie Matchett Wood. Parametrizing quartic algebras over an arbitrary base. *Algebra & Number Theory*, 5(8):1069–1094, 2011.

[Woo11c] Melanie Matchett Wood. Rings and ideals parameterized by binary n-ic forms. *Journal of the London Mathematical Society*, 83(1):208–231, February 2011.

[Woo12] Melanie Matchett Wood. Quartic Rings Associated to Binary Quartic Forms. *International Mathematics Research Notices*, 2012(6):1300–1320, January 2012.

[Woo14] Melanie Matchett Wood. Parametrization of ideal classes in rings associated to binary forms. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2014(689):169–199, April 2014.

[Wri89] David J. Wright. Distribution of discriminants of abelian extensions. *Proceedings of the London Mathematical Society. Third Series*, 58(1):17–50, 1989.

[WY15] Melanie Machett Wood and Takehiko Yasuda. Mass Formulas for Local Galois Representations and Quotient Singularities. I: A Comparison of Counting Functions. *International Mathematics Research Notices*, page rnv074, March 2015.

Department of Mathematics, University of Wisconsin-Madison, 480 Lincoln Drive, Madison, WI 53705 USA, and American Institute of Mathematics, 360 Portage Ave, Palo Alto, CA 94306-2244 USA

E-mail address: `mmwood@math.wisc.edu`