IAS/Park City Mathematics Series
Volume 00, Pages 000–000
S 1079-5634(XX)0000-0

Number field counting, class group heuristics, and computation

Melanie Matchett Wood

Abstract. These notes give an introduction to the asymptotic counting of number fields by Galois group and the Cohen-Lenstra heuristics for the distribution of class groups of quadratic fields. We discuss the connection of the class group heuristics to random matrices and discuss the moments of the conjectured distribution and the role they play. We point out places where computation has been crucial in the development of this theory, and suggest some important directions for future computational work. We give many exercises, ranging from quite easy, to quite difficult, including longer term projects.

Any comments, corrections, typos, etc. are very welcome at mmwood@math.harvard.edu

1. Counting number fields

1.1. Questions Number fields, i.e. finite extensions of the rational numbers $\mathbb{Q}$, are the basic objects of algebraic number theory. We can ask how many there are, and there are infinitely many, and so we ask a more refined question. For a number field K, we write D_K for its *absolute discriminant*, that is, the absolute value of its discriminant.

Question 1.1.1. *Given a positive integer* d*, how many isomorphism classes of number fields of degree* d *and absolute discriminant at most* X *are there, asymptotically in* X*?*

"Asymptotically in X" means that if $N_d(X)$ is the number of isomorphism classes of number fields K of degree d over $\mathbb{Q}$ with $D_K \leqslant X$, we are looking for an answer of the form

$$N_d(X) = f(X) + o(f(X)),$$

where $f(X)$ is some simple function, like $X^a(\log X)^b$ for some real numbers a, b. We write $g(X) = f(X) + o(h(X))$ to mean that

$$\lim_{X\to\infty} \frac{|g(X) - f(X)|}{h(X)} = 0.$$

We have asked about isomorphism classes of number fields, though it is also natural to ask about subfields of $\bar{\mathbb{Q}}$ instead. These two questions are closely related (see Exercise 1.1.3). We know classically that $N_d(X)$ is finite.

2010 *Mathematics Subject Classification.* Primary 14Dxx; Secondary 14Dxx.
Key words and phrases. Park City Mathematics Institute.

©0000 (copyright holder)

Theorem 1.1.2 (Hermite's theorem, see, e.g., III.2.16 in [85])**.** *Given a real number* X*, there are finitely many isomorphism classes of number fields* K *with* $|D_K| \leqslant X$*.*

Exercise 1.1.3. *Show that* $N_d(\infty)$ *is infinite for each positive integer* $d \geqslant 2$*. What lower bound does your argument give for* $N_d(X)$*?*

There are many ways one might approach Exercise 1.1.3, and they lead in some of the different directions of work in the area. One might give an infinite list of fields, using polynomials or adjoining dth roots, but then one needs some argument to make sure that the elements of the list are actually degree d fields and distinct. One might use the theorems of class field theory, which handles these issues well but only can access abelian fields.

Given Theorem 1.1.2, one might ask why we even fix a degree d at all. First of all, fixing the degree makes the question have more accessible parts. However, in addition, once we have some of the answers, e.g. for $d = 2, 3, 4$, we can see that the various degrees have natural answers, suggesting the most natural form of the answer for all degrees would simply be the sum over the answers for each d. In fact, from the answers in low degree, we further see that the level at which we have natural answers is if we fix not only a degree but also a Galois group. More precisely, we should fix the Galois group of the Galois closure and its action of the embeddings of the number field in $\bar{\mathbb{Q}}$.

Definition. A *permutation group* G is a group G, a set X, and a faithful action of G on X. We often leave X implicit in the notation. An isomorphism of two permutation groups (G, X) and (G', X') is a group isomorphism $f : G \to G'$ and a bijection $h : X \to X'$ such that for all $g \in G$ and $x \in X$, we have $h(g(x)) = f(g)(h(x))$. The permutation group is *transitive* if the group action is transitive. We say $|X|$ is the *degree* of the permutation group, and that the permutation group is *finite* if it has finite degree.

Exercise 1.1.4. *Show that, for each* n*, isomorphism classes of permutation groups whose underlying set has size* n *are in natural bijection with conjugacy classes of the symmetric group* S_n*.*

Definition. For a number field K, we write $\mathrm{Gal}(K/\mathbb{Q})$ for the permutation group whose underlying group is $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$, where $\tilde{K}$ is the Galois closure of K over $\mathbb{Q}$, acting on the $[K : \mathbb{Q}]$ homomorphisms $K \to \bar{\mathbb{Q}}$. More precisely, $\tau \in \mathrm{Gal}(\tilde{K}/\mathbb{Q})$ sends $i \in \mathrm{Hom}(K, \bar{\mathbb{Q}})$ to τi.

While it might be jarring at first to write $\mathrm{Gal}(K/\mathbb{Q})$ when K is not Galois, this is a very helpful concept and notation. For example, theorems in arithmetic statistics show us that the degree 4 fields whose Galois closure has group D_4 behave quite differently from those whose Galois closure has group S_4.

Exercise 1.1.5. *If K is a number field, show that $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ acts faithfully on the $[K:\mathbb{Q}]$ homomorphisms $K \to \bar{\mathbb{Q}}$.*

Exercise 1.1.6. *If K is a number field, show that $\mathrm{Gal}(K/\mathbb{Q})$ is a transitive permutation group.*

Any group G acts on itself via left multiplication, and we call this permutation group the *regular representation*.

Exercise 1.1.7. *If K is Galois, show that the permutation group $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the usual Galois group with its regular representation.*

Exercise 1.1.8. *Show that if G is a transitive permutation group of finite degree $|G|$ (equivalently a finite simply transitive permutation group), then it is isomorphic to the underlying group in its regular representation.*

Exercise 1.1.9. *Show that if A is a finite abelian group, the only transitive permutation group structure one can put on A is the regular representation.*

Exercise 1.1.10. *Find an example of two non-isomorphic transitive permutation groups of the same degree whose underlying group is isomorphic. [Hint: the GroupNames database online, or similar, might be useful.]*

Exercise 1.1.10 shows why we keep track of the permutation group and not just the group, even though in low degrees we can often refer to *the* transitive degree d action of a particular group, e.g. the transitive degree 4 action of D_4. We can now state the most common version of the counting number fields question in arithmetic statistics.

Given a positive integer d and a transitive permutation group G of degree d, let S_G be the set of isomorphism classes of number fields K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$. We call such number fields G-*extensions* (or if we replace $\mathbb{Q}$ with a base field K_0, we would call them G-extensions of K_0).[1] When a group G has a single transitive permutation group structure (up to isomorphism) of degree d, we often write d-ic (e.g. cubic, quartic,...) G-extensions to mean that G should be endowed with this transitive permutation group structure. Let $N_G(X)$ be the number of $K \in S_G$ with $|D_K| \leqslant X$.

Question 1.1.11. *What is $N_G(X)$, asymptotically in X?*

Note that the question, for a given finite group G, of whether $N_G(X)$ is ever at least 1, is the Inverse Galois Problem, a famously hard and open question. However, there are many G for which we do know there exist many number fields with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$, and for some of these we can answer Question 1.1.11. Note that if we answer Question 1.1.11 for all transitive permutation groups G

[1] It is generally better practice to define a G-extension to be an isomorphism class of pairs (K, ϕ) where ϕ is a choice of isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$. This inflates the number of automorphisms by a predictable amount, but when one needs to use an isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$, it is often more convenient to have one specified. However, we try to avoid needing this in this paper for simplicity.

of a given degree d, since there are only finitely many, we can add the results to get an answer to Question 1.1.1. Indeed, if for one G of degree d we have an asymptotic of $f(X)$, to answer Question 1.1.1, it would suffice to have, for each other G of degree d, either an asymptotic for $N_G(X)$ or an upper bound of $o(f(X))$. This approach is how we know the answer to Question 1.1.1 for $d \leqslant 5$ [16, 18, 38, 45], which in each $d \leqslant 5$ is

$$N_d(X) = c_d X + o(X)$$

for some $c_d > 0$.

Exercise 1.1.12. *If K is a number field with $G = \mathrm{Gal}(K/\mathbb{Q})$ and $S \subset G$ the stabilizer of an element (i.e. one of the embeddings $K \to \tilde{K}$), show that $\mathrm{Aut}(K)$ is isomorphic to quotient of the normalizer of S in G by S.*

Exercise 1.1.13. *Given a positive integer d and a permutation group G of degree d, an a number field K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$, show that there are exactly $\frac{d}{|\mathrm{Aut}(K)|}$ subfields of $\bar{\mathbb{Q}}$ that are isomorphic to K.*

1.2. Approaches and results The answer is Question 1.1.11 is known for many G. For example, we consider the permutation group S_2 in its standard permutation action on 2 elements and $N_{S_2}(X)$ counts quadratic fields. Early in algebraic number theory, we classify all quadratic fields, and show they are determined by their discriminant. A quadratic field K must contain some α satisfying an equation $\alpha^2 + a\alpha - d = 0$ for some $a, d \in \mathbb{Q}$. We can replace α with $\alpha + a/2$ and then have $a = 0$. We can replace α with an integer multiple to have $d \in \mathbb{Z}$, but then we can also divide α by an integer to have that d is square-free. So every quadratic field is $\mathbb{Q}(\sqrt{d})$ for some square-free integer $d \neq 1$. How do we know these fields are all in distinct isomorphism classes? Typically, we compute their rings of integers and their discriminants, and then we can observe they all have unique discriminants. Moreover, the discriminants that arise are exactly the set $\mathcal{F}$ of integers D such that

(1) $D \equiv 1 \pmod 4$ and D is square-free and $D \neq 1$, or
(2) $D = 4d$, where $d \equiv 2$ or $3 \pmod 4$ and d square-free.

We will now discuss how to count these integers. We have $N_{S_2}(X) = \mathcal{F} \cap [-X, X]$. We can rewrite the above conditions defining $\mathcal{F}$ as above as requiring that $D \equiv 1, 5, 8, 9, 12, 13 \pmod{16}$ and that for each odd prime p, we have $D \not\equiv 0 \pmod{p^2}$ (and that D is not 1). The problem is essentially the same in spirit as how one could count square-free integers, but the conditions at 2 require some additional care. For a square-free number n, let $B_n(X)$ be the number of non-zero integers $D \in [-X, X]$ that fail our conditions at each prime dividing n, i.e. if n is even then $D \pmod{16} \notin \{1, 5, 8, 9, 12, 13\}$ and for each odd prime $p \mid n$, we have $D \equiv 0 \pmod{p^2}$.

Exercise 1.2.1. *Show that for all $X \geqslant 2$, we have*

$$N_{S_2}(X) = -1 + \sum_{1 \leqslant n \leqslant 2\sqrt{X}} \mu(n) B_n(X),$$

where μ is the Möbius function. [Hint: consider some non-zero $D \in [-X, X]$ that fails the conditions at primes $2, p_1, \dots, p_k$ or odd primes $p_1, \dots, p_k$. How many times is it counted on the right-hand side?]

If X is a multiple of $4n^2$, then it is easy to count $B_n(X)$ exactly. Otherwise, we can estimate. We write $f(n, X) = g(n, X) + O(h(n, X))$ to mean that there exists a constant C such that for all $n, X \geqslant 1$ we have

$$|f(n, X) - g(n, X)| \leqslant C h(n, X).$$

Exercise 1.2.2. *If n is an odd square-free integer, show $B_n(X) = 2\lfloor \frac{X}{n^2} \rfloor$, and so*

$$B_n(X) = 2\frac{X}{n^2} + O(1).$$

Exercise 1.2.3. *If $n = 2m$, with m odd square-free, show $B_n(X) = 20\lfloor \frac{X}{4n^2} \rfloor + \epsilon$, where $0 \leqslant \epsilon \leqslant 20$, and so*

$$B_n(X) = 2\frac{5/2}{n^2}X + O(1).$$

Let $d_n = n^2$ if n is odd and $d_n = 2n^2/5$ if n is even. So we can conclude

$$N_{S_2}(X) = 2 \sum_{1 \leqslant n \leqslant 2\sqrt{X}} \mu(n) \frac{X}{d_n} + O(\sqrt{X}).$$

Exercise 1.2.4. *Show*

$$2 \sum_{n \geqslant 1} \mu(n) \frac{X}{d_n} = 2X \left(1 - \frac{5}{8}\right) \prod_{\substack{2 < p \\ \text{prime}}} (1 - p^{-2}) = \zeta(2)^{-1} X.$$

Exercise 1.2.5. *Show*

$$2 \sum_{n > 2\sqrt{X}} \mu(n) \frac{X}{d_n} = O(\sqrt{X}).$$

The exercises above combine to show

$$N_{S_2}(X) = \zeta(2)^{-1} X + O(\sqrt{X}) = \zeta(2)^{-1} X + o(X).$$

Exercise 1.2.6. *Plot a graph of $N_{S_2}(X)$ and $\zeta(2)^{-1}X$, and then "zoom in" by plotting*

$$\frac{N_{S_2}(X) - \zeta(2)^{-1} X}{\sqrt{X}}.$$

Does there appear to be a "secondary term," e.g. a function $f(x)$ of the form $cX^a (\log X)^b$ for reals a, b, c such that

$$N_{S_2}(X) = \zeta(2)^{-1} X + f(X) + o(f(X))?$$

Does there appear to be a an improved error term, e.g. a value $a < 1/2$ such that

$$N_{S_2}(X) = \zeta(2)^{-1} X + O(X^a)?$$

If the answer to the above questions is no, we can informally consider $O(\sqrt{X})$ as a "true error term," as opposed to the current state of knowledge. We could use the above questions to make this a precise notion, but it does not seem precision here is warranted, since the second question above ignores $\log X$ terms, and both ignore $\log\log X$ and other terms that might appear.

However, even once we consider number fields of degree 3, the situation becomes vastly more complicated. Still each cubic field can be generated by a degree 3 algebraic number α satisfying some $\alpha^3 + p\alpha + q = 0$, for $p, q \in \mathbb{Z}$, but it becomes much harder to use this to count. For one, the discriminant no longer is quite as discriminating.

Exercise 1.2.7. *Use a database (e.g. the LMFDB* [77]*) to find the smallest* D *such that there are two non-isomorphic cubic fields of discriminant* D*.*

However, even to get the discriminant from p, q is not something we can write down a simple formula for because we cannot write a formula for the ring of integers. (We can of course, give a formula for the discriminant of the ring $\mathbb{Z}[\alpha]$, but we do not know its index in the maximal order of K.) So we cannot say either what the discriminant of the field given by (p, q) is or when (p, q) and (p', q') give the same field. Remarkably, Shankar and Tsimerman [95] give a heuristic argument following this line of reasoning that gives a predicted asymptotic for S_d-extensions for each d by quantifying how much overcounting of fields is done and understanding the discriminant of the maximal order in terms of local conditions. Their approach even gives a proof when $d = 3$, though we will give an older proof below.

Even though all number fields of degree d come from degree d polynomials, this highlights the difference between understanding the (finite) set of isomorphism classes of number fields of bounded discriminant and understanding the (infinite) set of polynomials of bounded discriminant (or even further contrast with understanding the natural finite set of polynomials with bounded coefficients). This contrast plays out in many places, from theoretical results (such as what we will see about counts of quartic D_4 and S_4 fields below), to computational challenges in making tables of number fields (see [36, 64, 107]).

However, another approach of parametrizing cubic fields was used by Davenport and Heilbronn in 1971 [45] to give the asymptotics of $N_3(X)$ as

$$N_3(X) = \frac{1}{3\zeta(3)}X + o(X).$$

Class field theory allows one to count Galois cubic fields, and Cohn in 1954 [42] had shown

$$N_{C_3}(X) = c_{C_3}X^{1/2} + o(X^{1/2}),$$

where we write C_3 for the cyclic group of order 3 in its regular representation and c_{C_3} is some explicit constant given by Cohn. From these results, if we write S_3 for the permutation group in its standard representation on a set of 3 elements, it

follows that

$$N_{S_3}(X) = \frac{1}{3\zeta(3)}X + o(X).$$

Let D_4 be the dihedral group of 8 elements with its action on as automorphisms of a square on its vertices. In 2002, Cohen, Diaz y Diaz, and Olivier [38] showed

$$N_{D_4}(X) = c_{D_4}X + o(X),$$

where c_{D_4} is an explicitly given constant. Their approach was to count quadratic extensions of quadratic fields, of which all quartic fields K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq D_4$ are. Bhargava [16] showed

$$N_{S_4}(X) = c_{S_4}X + o(X),$$

where c_{S_4} is an explicitly given constant.

It is also known that for G a transitive permutation group other than D_4, we have $N_G(X) = o(X)$. Thus the above two results show that asymptotically, a positive proportion (around 17%) of quartic fields, ordered by discriminant, are D_4-extensions, and a positive proportion (around 83%) of quartic fields, ordered by discriminant are S_4-extensions. If we instead consider degree n polynomials with bounded integral coefficients, asymptotically 100% have Galois group S_n. This is suggested by Hilbert's Irreducibility Theorem and was shown by van der Waerden [104] (see also [19]).

Today we know the answer to Question 1.1.11 for many more G, but many of the high-level strategies are descendants of one of these 3 approaches.

Class Field Theory Class field theory is a powerful tool for understanding abelian extensions. In 1985, Mäki [78] gave asymptotics for $N_G(X)$ for each finite abelian group G in its regular representation, using the Kronecker-Weber theorem. One can also see work of Frei, Loughran, and Newton [53] for a more modern, class field theoretic approach to these asymptotics for abelian G. We briefly outline Cohn's proof [42] for C_3 extensions to give the flavor.

Let K be a number field. Let C_K be the idéle class group of K, i.e. $(\prod_\nu' K_\nu^*)/K$, where the product is over places ν of K, and is restricted to elements that are units in all but finitely many places (with the restricted product topology). Let G_K be the absolute Galois group of K. Class field theory tells us that for a finite abelian group A, the Artin map $C_K \to G_K^{ab}$ induces a bijection

$$\mathrm{Sur}(G_K, A) \to \mathrm{Sur}(C_K, A)$$

(where Sur denotes continuous surjective group homomorphisms). For a finite place ν the image of the local units $\mathcal{O}_\nu^*$ is the image of the inertia group at ν of the corresponding map, and for a real place ν the image of K_ν^* is the image of the inertia group.

Exercise 1.2.8. *Let $\mathbb{R}^*_{>0}$ denote the positive reals (under multiplication). Show that the natural map*

$$\prod_p \mathbb{Z}_p^* \times \mathbb{R}^*_{>0} \to C_Q$$

is an isomorphism. Conclude that for a finite abelian group A, we have a bijection

$$\mathrm{Hom}(G_Q, A) \to \mathrm{Hom}(\prod_p \mathbb{Z}_p^*, A),$$

(where Hom *denotes continuous homomorphisms) where the image of the inertia group at p corresponds to the image of $\mathbb{Z}_p^*$.*

Exercise 1.2.9. *Show that $\mathbb{Z}_p^*$ has a continuous surjective homomorphism to C_3 if and only if p is 0 or 1 mod 3, in which case it has exactly two such homomorphisms.*

Exercise 1.2.10. *Show that a cyclic cubic field K has a square discriminant D, and if P is the product of the rational primes ramified in K, then if $3 \nmid P$ then $D = P^2$ and if $3 \mid P$, then $D = 9P^2$. [Hint: there are many ways to do the last part, e.g. using* [85, III.2.6]*, the relationship between the class field theory conductor and the discriminant, or tables of local fields.]*

For a $\phi \in \mathrm{Hom}(G_Q, C_3)$, we write D_ϕ for the absolute discriminant of the corresponding extension of $\mathbb{Q}$. Thus we can explicitly write the Dirichlet series of C_3 extensions

$$D(s) = \sum_{\phi \in \mathrm{Hom}(G_Q, C_3)} \frac{1}{D_\phi^s} = (1 + 2 \cdot 9^{-2s}) \prod_{\substack{p \equiv 1 \pmod 3 \\ \text{prime}}} (1 + 2p^{-2s}).$$

This tells us what all cyclic cubic extensions of $\mathbb{Q}$, with their discriminants, are, and it remains a question of analytic number theory of the integers to do the asymptotic counting. This can be done by analysis of the right-most pole of $D(s)$ and an application of a Tauberian theorem such as the following.

Theorem 1.2.11 ([84, Corollary p. 121])**.** *Let $f(s) = \sum_{n \geqslant 1} a_n n^{-s}$ with $a_n \geqslant 0$ 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 $\Re s \geqslant a$, and $g(a) \neq 0$, and $w > 0$. Then*

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

Exercise 1.2.12. *Let χ be a non-trivial Dirichlet character of modulus 3. Show that*

$$\frac{D(s)}{L(2s, \chi)\zeta(2s)}$$

is analytic for $\Re(s) > 1/4$. Use this and Theorem 1.2.11 to conclude Cohn's asymptotic for $N_{C_3}(X)$.

Exercise 1.2.13. *Use Theorem 1.2.11 to give another proof that $N_{S_2}(X) = \frac{1}{\zeta(2)} X + o(X)$.*

Exercise 1.2.14. *Use Perron's formula (which can be used to prove Theorem 1.2.11) to analyze the size of* $N_{S_2}(X) - \frac{1}{\zeta(2)}X$*. How does what you find relate to what you found in Exercise 1.2.6?*

See [113, Section 8] for more examples and more detailed exposition of this approach.

Parametrization and geometry of numbers For many years, the approach of parametrization and geometry of number had only been applied to count cubic fields. However, Bhargava made significant breakthroughs in parametrizations (including the realization that resolvent rings needed to be parametrized and the construction of integral models of these) [15, 17] and geometry of numbers (including introducing averaging methods and methods for dealing with cusps) [16, 18] that allowed him to extend this approach to count quartic fields K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_4$ and quintic fields K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_5$. The work of Davenport-Heilbronn was also the starting place for Belabas and Fouvry [14] and for Bhargava and the author [29] to count Galois sextic S_3 extensions.

Now we briefly outline the approach of Davenport-Heilbronn. We give a parametrization originally due to Delone and Faddeev [46] (and refined by Gan, Gross, and Savin [56]), that is a cleaner version of what Davenport and Heilbronn used.

Let $\mathcal{O}_K$ be the ring of integers in a cubic number field.

Exercise 1.2.15. *Show that* 1 *generates a direct summand of* $\mathcal{O}_K$ *as a* $\mathbb{Z}$*-module.*

Let $1, W, T$ be a $\mathbb{Z}$ basis of $\mathcal{O}_K$. 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:

$$\begin{aligned} \omega\theta &= n \\ \omega^2 &= m - b\omega + a\theta \\ \theta^2 &= \ell - d\omega + c\theta, \end{aligned} \tag{1.2.16}$$

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 1.2.17. *Show that the associativity of multiplication in* $\mathcal{O}_K$ *exactly corresponds to the equations*

$$n = -ad \quad m = -ac \quad \ell = -bd. \tag{1.2.18}$$

We package these a, b, c, d into a binary cubic form $ax^3 + bx^2y + cxy^2 + dy^3$.

Exercise 1.2.19. *Find a binary cubic form associated to* $\mathbb{Z}[\sqrt[3]{2}]$ *and some normalized basis. Find another one (using a different choice of normalized basis). What is the discriminant of the binary cubic forms you found? What is the discriminant of* $\mathbb{Z}[\sqrt[3]{2}]$*?*

A choice of normalized basis of $\mathcal{O}_K$ is equivalent to a choice of $\mathbb{Z}$ basis of the $\mathbb{Z}$-module $\mathcal{O}_K/\mathbb{Z}$. The action of $GL_2(\mathbb{Z})$ on bases of $\mathcal{O}_K/\mathbb{Z}$ gives a $GL_2(\mathbb{Z})$ action on the tuples $(a,b,c,d) \in \mathbb{Z}^4$, arising above, such that the orbits are in bijection with isomorphism classes of $\mathcal{O}_K$. The action is (almost) the 4 dimensional representation of $GL_2(\mathbb{Z})$ on binary cubic forms. Let $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$. Let $g \in GL_2(\mathbb{Z})$. Then we can let $GL_2(\mathbb{Z})$ act on binary cubic forms via

$$(gf)(x,y) = \frac{1}{\det(g)} f((x,y)g), \tag{1.2.20}$$

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) given by action on the choice of basis of $\mathcal{O}_K/\mathbb{Z}$.

Exercise 1.2.21. *Check that for* $g = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ *the action on the set of* (a,b,c,d) *is as claimed. Check it for* $g = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *and* $g = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ *as well, and conclude the action is as claimed for all of* $GL_2(\mathbb{Z})$.

It turns out the discriminant of $\mathcal{O}_K$ is equal to the discriminant of the associated binary cubic forms. (These are both polynomials in a,b,c,d and it is computationally straightforward to check they are the same.) Thus it remains to understand (1)which tuples (a,b,c,d) arise, and (2) to count their $GL_2(\mathbb{Z})$ orbits, asymptotically by discriminant. For (1), it turns out that this can be understood by some relatively simply criteria (the form should be irreducible over $\mathbb{Q}$, along with a condition mod p^2 for every prime p). For (2), one can count orbits by counting the (relevant) lattice points in a fundamental domain for the action, which can be done with methods from the geometry of numbers.

See also [113, Section 11], and [22] for further exposition of this approach from a modern point of view, as well as [62, p.12-18] for a series of exercises that provides a do-it-yourself proof of Davenport-Heilbronn's result.

Counting fields up to discriminant X is closely related to producing complete, non-redundant lists or tables of such fields, sometimes called *tabulating* fields. See [36, Section 9] for an exposition of algorithms for such tabulation. For general degree, they are required to essentially consider polynomials or algebraic numbers, which as we have seen above do not line up perfectly with fields, and thus require considering and computing with many more polynomials than actually produce unique fields. However, for cubic fields, this parametrization relating isomorphism classes of cubic fields to certain lattice points in a fundamental domain also is the basis of Belabas's [11] approach to tabulating cubic fields, which is far more efficient than is available for general degree. It would be very interesting to see if Bhargava's parametrizations of quartic and quintic fields [15, 17] could be used to give an efficient approach to tabulating quartic and quintic fields (see also [37] for other approaches for quartic fields).

Extensions of extensions The general approach to counting number fields which are composite extensions by counting extensions of extensions has been used by

many authors. Klüners [68] was able to asymptotically count G extensions for many G of the form $C_2 \wr H$. Wang [109] and Masri, Thorne, Tsai, and Wang were able to asymptotically count G extensions for $G = S_n \times A$ where $n = 3, 4$, or 5 and A is an abelian group. There is forthcoming work of Alberts, Lemke Oliver, Wang, and the author that counts composite extensions for many more G.

Cohen, Diaz y Diaz, and Oliver were able to count quartic fields K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq D_4$ fields by using the fact that these fields were all quadratic extensions of quadratic extensions, and we can enumerate quadratic extensions of any field in a relatively concrete way. We outline such an approach here.

Exercise 1.2.22. *Show that each quartic field K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq D_4$ contains a unique quadratic field as a subfield.*

Exercise 1.2.23. *Show that any quadratic extension K of a quadratic field has $\mathrm{Gal}(K/\mathbb{Q}) \simeq D_4, \mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

We can use the class field theory approach, outlined above, to show the following:

(1) For each quadratic field F, the number $N_{F,S_2}(X)$ of quadratic extensions K of F with $\mathrm{Nm}_{F/\mathbb{Q}}(\mathrm{Disc}(K/F)) \leqslant X$ satisfies
$$N_{F,S_2}(X) = c_F X + o(X),$$
for some $c_F > 0$.

(2) There exists a number C such that for each quadratic field F, for all X
$$N_{F,S_2}(X) \leqslant C D_F^{2/3} X.$$

Exercise 1.2.24. *Use class field theory and the Tauberian theorem above to show statement (1) above.*

We can combine the two statements above, along with our knowledge of the quadratic extensions of $\mathbb{Q}$, to count quadratic extensions K of quadratic fields F. Recall $|\mathrm{Disc}(K/\mathbb{Q})| = \mathrm{Nm}_{F/\mathbb{Q}}(\mathrm{Disc}(K/F)) D_F^2$. If $N(X)$ is the number of quadratic extensions of quadratic fields (more precisely we count pairs (F, K), where $F/\mathbb{Q}$ is an isomorphism class of quadratic fields, and K/F is an isomorphism class of quadratic extensions), we have

$$\begin{aligned} N(X) &= \sum_{[F:\mathbb{Q}]=2} N_{F,S_2}\left(\frac{X}{D_F^2}\right) \\ &= \sum_{[F:\mathbb{Q}]=2} \left(\left(\frac{c_F}{D_F^2}\right) X + o(X)\right). \end{aligned}$$

Unfortunately, we cannot exchange the $o(X)$ (and its implicit limit statement) with an infinite sum in F. However, if we fix some Y, and only consider F with $D_F \leqslant Y$,

then we have

$$\begin{aligned} N_Y(X) &:= \sum_{\substack{[F:\mathbb{Q}]=2 \\ D_F \leqslant Y}} N_{F,S_2}\left(\frac{X}{D_F^2}\right) \\ &= \sum_{\substack{[F:\mathbb{Q}]=2 \\ D_F \leqslant Y}} \left(\left(\frac{c_F}{D_F^2}\right) X + o(X)\right) \\ &= \left(\sum_{\substack{[F:\mathbb{Q}]=2 \\ D_F \leqslant Y}} \frac{c_F}{D_F^2}\right) X + o(X). \end{aligned}$$

Exercise 1.2.25. *Using statements (1) and (2) above, show that* $\sum_{[F:\mathbb{Q}]=2} \frac{c_F}{D_F^2}$ *converges.*

This gives a lower bound

$$\liminf_{X\to\infty} \frac{N(X)}{X} \geqslant \sum_{[F:\mathbb{Q}]=2} \frac{c_F}{D_F^2}.$$

However, we also have

$$\begin{aligned} N(X) \leqslant & N_Y(X) + \sum_{\substack{[F:\mathbb{Q}]=2 \\ D_F > Y}} N_{F,S_2}\left(\frac{X}{D_F^2}\right) \\ \leqslant & N_Y(X) + \sum_{\substack{[F:\mathbb{Q}]=2 \\ D_F > Y}} C D_F^{-4/3} X. \end{aligned}$$

Exercise 1.2.26. *Show* $\sum_{[F:\mathbb{Q}]=2} D_F^{-4/3}$ *converges.*

So we have

$$\limsup_{X\to\infty} \frac{N(X)}{X} \leqslant \sum_{\substack{[F:\mathbb{Q}]=2 \\ D_F \leqslant Y}} \frac{c_F}{D_F^2} + \sum_{\substack{[F:\mathbb{Q}]=2 \\ D_F > Y}} C D_F^{-4/3},$$

and taking the limit as $Y \to \infty$ we obtain

$$\limsup_{X\to\infty} \frac{N(X)}{X} \leqslant \sum_{\substack{[F:\mathbb{Q}]=2 \\ D_F \leqslant Y}} \frac{c_F}{D_F^2}.$$

Combined with the lim inf statement above, we have

$$N(X) = \left(\sum_{[F:\mathbb{Q}]=2} \frac{c_F}{D_F^2}\right) X + o(X).$$

To obtain an asymptotic on $N_{D_4}(X)$, we can use the fact that the asymptotics for $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ quartic fields (which can be obtained by class field theory) are of smaller order, i.e.

$$N_{\mathbb{Z}/4\mathbb{Z}}(X) + N_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}}(X) = o(X).$$

To be quite precise, we should account for how many times each D_4 quartic appears in $N(X)$.

Exercise 1.2.27. *Show that the map from pairs* (F, K)*, where* F *is an isomorphism class of quadratic field, and* K/F *is an isomorphism class of a quadratic extension of* F *such that* $\mathrm{Gal}(K/\mathbb{Q}) \simeq D_4$*, to isomorphism classes of* D_4*-quartic extensions of* $\mathbb{Q}$ *is* $2-1$*.*

1.3. Conjectures and more results For each transitive finite permutation group G, Malle [80] defined integers a_G, b_G such that he conjectured that there was some $c_G > 0$ (not predicted) such that

$$N_G(X) = c_G X^{1/a_G} (\log X)^{b_G}. \tag{1.3.1}$$

Though the examples mentioned above all confirm cases of Malle's conjecture, Klüners [66] found a counterexample in $G = C_3 \wr C_2$, for which there were more extensions than conjectured. One still has "Weak Malle," an earlier conjecture of Malle [79] that there is a $c_G > 0$, and for every $\epsilon > 0$ and $c'_{G,\epsilon}$ such that for all X we have

$$c_G X^{1/a_G} \leqslant N_G(X) \leqslant c'_{G,\epsilon} X^{1/a_G+\epsilon}. \tag{1.3.2}$$

Conjecture (1.3.2) has no known counterexamples and is generally expected to be true. We expect that one could add the $(\log X)^{b_G}$ term to the lower bound in (1.3.2) and the inequality still hold. Türkelli [103, Conjecture 6.7] has given a revised definition of b_G for which he conjectures (1.3.1) holds. See [113, Section 10] for further exposition of Malle's conjecture, as well as the general heuristic principle that implies the conjecture as well as related conjectures (called the Malle-Bhargava Principle).

New approaches have asymptotically counted G-extensions for other G, including work of Fouvry and Koymans [52] that counts nonic Heisenberg extensions, work of Klüners [65] for generalized quaternion groups G, and work of Koymans and Pagano [71] that counts G extensions for many nilpotent G.

1.4. Variations and directions There are of course many variations one can put on Question 1.1.11. We will not give a complete literature review but try to point the reader to some recent papers from which they can learn about various directions. In the cases for which we know the answer, it is common that the answer is also given when the fields counted have a restricted signature. It is common to also be able to give asymptotics only counting fields satisfying local conditions at some finite (or even infinite) set of primes [23, 53, 111]. See [113] for an introduction to counting with local conditions, including results and conjectures in this direction.

When asymptotics are known, one can ask for improved error bounds [13, 94] or secondary terms. While Davenport and Heilbronn's result on counting cubic fields is a theorem, tables such as those produced by Belabas [11] show various slow convergence to the known asymptotic. Supported by significant numerical evidence from such tables, Roberts [92] was able to conjecture a precise secondary

term for the counting of cubic fields (beyond the main term of Davenport and Heilbronn). Taniguchi and Thorne [101] and Bhargava, Shankar, and Tsimerman [22] independently proved Roberts conjectured secondary term. The best current result is of Bhargava, Taniguchi, and Thorne [26] and gives

$$N_{S_3}(X) = \frac{1}{3\zeta(3)}X + c'_{S_3}X^{5/6} + O(X^{2/3}(\log X)^{2.09}),$$

where c'_{S_3} is an explicitly given, non-zero constant.

Wang [108] proves the first secondary terms beyond cubic fields, in counting $S_3 \times A$ extensions, where A is an abelian odd order group. In general there are no conjectures for secondary terms, and it would be a useful computational project to make numerical computations tabulating fields that were strong enough to suggest more secondary terms, true error terms, or speed of convergence for counting G-extensions for other G. It is possible some such computations could be done with pre-existing tables of fields, at least as a starting place.

When asymptotics are not known, one can ask for lower or upper bounds [4, 25, 72], or to prove Weak Malle [4, 69]. In light of recent progress on the upper bound for degree d extensions [9, 24, 43, 87], as well as for G-extensions [48], it is very natural to ask if these ideas can be used to develop more efficient algorithm for tabulating number fields of a fixed degree or Galois group. Such improved algorithms could be very helpful to produce more exhaustive tables, and in particular to help with the questions of predicting secondary and error terms discussed above.

It would be very interesting to develop a "sampling" algorithm that might be able to numerically estimate $N_G(X)$ for some X large enough that we are not able to produce tables listing all G-extensions up to absolute discriminant X. Current tabulation algorithms consider various polynomials and some fraction of them end up producing new fields for the table. Is there a way to do some computations with random polynomials that could provide good enough estimates for use in predicting secondary or error terms?

One can replace $\mathbb{Q}$ with another number field K_0, or more generally a global field [23, 53, 71, 106, 119]. One can count extensions L/K that also have a specified Galois group over some subfield K_0 of K [5, 6]. One can also count extensions by invariants other than the discriminant, such class the class field theory conductor for abelian extensions [111] , Artin conductors [7], or more general invariants [93].

2. Distribution of class groups

2.1. Motivating Questions For a finite transitive permutation group G, one can ask as we consider the number fields in S_G, what is the distribution of class groups that arise? In particular for a finite abelian group A, we could ask what is

$$\lim_{X\to\infty} \frac{|\{K \in S_G \mid Cl_K \simeq A, D_K \leqslant X\}|}{N_G(X)}? \tag{2.1.1}$$

More generally, for a set S of number fields, and a function f taking finite abelian groups to real numbers, we ask what are the asymptotics of

$$\frac{\sum_{\substack{K\in S\\ D_K\leqslant X}} f(\mathrm{Cl}_K)}{\sum_{\substack{K\in S\\ D_K\leqslant X}} 1}? \tag{2.1.2}$$

Note that the denominator of these questions are the number field counting questions above (or similar).

Class groups, in some sense, provide the first example of the strategy of parametrization mentioned above that Davenport and Heilbronn used to count cubic fields. Gauss studied $\mathrm{SL}_2(\mathbb{Z})$ orbits of integral binary cubic forms $ax^2 + bxy + cy^2$ (with $a, b, c \in \mathbb{Z}$), working with Lagrange's reduction theory that relates orbits to triples (a, b, c) in a certain region of $\mathbb{Z}^3$. This allowed Gauss to, for example, tabulate and enumerate those orbits. Remarkably, Gauss found a group law on these orbits. Dedekind later realized that these orbits were related to class group of quadratic fields (and we now recognize Gauss's group law as the usual group law on class groups). This relationship is what allows us to compute class groups of quadratic fields much faster than class groups of higher degree fields. See [83] and the extensive tables of class groups of quadratic fields available at the LMFDB [77].

In tables of class group of quadratic fields, one can observe that the group $\mathbb{Z}/9\mathbb{Z}$ occurs much more often than the group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ even though both groups have order 9. Cohen and Lenstra [39] sought to explain this and other patterns available in the empircal data on the class groups of quadratic fields, and developed heuristics that gave conjectures for the distribution of class groups of quadratic fields and real abelian fields.

Before we can describe some of Cohen and Lenstra's conjectures, we have the explain a bit more context on class groups. Almost any empirical or theoretical study of class groups of quadratic fields will show you that those of real quadratic fields behave quite differently than those of imaginary quadratic fields.

Exercise 2.1.3. *Using a database such as the LMFDB, look at class groups of several hundred real and imaginary quadratic fields. What is the major difference you notice?*

This difference is already apparent in Gauss's study, and Gauss conjectured (in modern terms) (1)that there are only finitely many imaginary quadratic fields with a given class group, and (2) that there are infinitely many real quadratic fields with trivial class group. The conejcture (1) was proven by Heilbronn [61], but (2) is still open.

Exercise 2.1.4. *Recall the Brauer-Siegel theorem, and see why it implies (1) above. Why doesn't it give the same conclusion for real quadratic fields?*

2.2. Genus theory of quadratic fields Secondly, Gauss found that the 2-torsion in class groups of quadratic fields (in his binary forms language) was relatively easy to describe.

Theorem 2.2.1. *If K is a quadratic field and N_K is its narrow class group, then $N_K[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$, where t is the number of ramified primes of $K/\mathbb{Q}$.*

When $K/\mathbb{Q}$ is imaginary quadratic, then $N_K = Cl_K$ by definition.

Exercise 2.2.2. *When $K/\mathbb{Q}$ is real quadratic, show that $N_K \to Cl_K$ is either an isomorphic or has kernel isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (depending on whether the fundamental unit has negative or positive norm). Conclude that $Cl_K[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1-\epsilon}$, where ϵ is either 1 or 0.*

While Gauss proved Theorem 2.2.1 very explicitly with binary quadratic forms, we will give a proof here using class field theory. This both gives good practice using the statements of class field theory, but also puts this phenomenon in a larger context. However, first we will not that one can see quite explicitly some potential 2-torsion. If p is a prime ramified in a quadratic field K, where $(p) = \mathfrak{p}^2$, then $\mathfrak{p}$ is either trivial or order 2 in Cl_K . There is no known simple way to produce such possible p-torsion for any primes $p > 2$.

To understand $Cl_K/2Cl_K$ (which is abstractly isomorphic to $Cl_K[2]$ by the theory of finite abelian groups), we can then try to understand $\mathrm{Sur}(Cl_K, \mathbb{Z}/2\mathbb{Z})$, which via class field theory, corresponds to the set of everywhere unramified quadratic extensions of K. Similarly to understand the narrow class group, we need to understand quadratic extensions of K unramified at all finite places.

Exercise 2.2.3. *Let K be a number field. For a real place v let $K_v^{>0}$ be the subgroup of positive elements of K_v^*. Show that there is a unique continuous homomorphism*

$$C_K/\left(\prod_{v \text{ finite}} \mathcal{O}_v^* \times \prod_{v \text{ real}} K_v^{>0} \times \prod_{v \text{ complex}} K_v^*\right) \to N_K$$

sending, for each finite place v of K, a uniformizer $\pi_v \in K_v^*$ to the image of the corresponding prime ideal of v in N_K, and that the homomorphism is an isomorphism. Show this implies that N_K is isomorphic to the Galois group of the maximal abelian extension of K unramified at all finite places.

Exercise 2.2.4. *Let K be a number field. Show that there is a unique continuous homomorphism*

$$C_K/\left(\prod_{v \text{ finite}} \mathcal{O}_v^* \times \prod_{v \text{ real}} K_v^* \times \prod_{v \text{ complex}} K_v^*\right) \to Cl_K$$

sending, for each finite place v of K, a uniformizer $\pi_v \in K_v^*$ to the image of the corresponding prime ideal of v in N, and that the homomorphism is an isomorphism. Show this implies that Cl_K is isomorphic to the Galois group of the maximal abelian extension of K unramified at all places.

Exercise 2.2.5. *If $K/\mathbb{Q}$ is quadratic, show that the action of the generator of $\mathrm{Gal}(K/\mathbb{Q})$ on N_K is by multiplication by -1.*

Exercise 2.2.6. *Show if* K *is a quadratic field and* L/K *is everywhere unramified, that* $L/\mathbb{Q}$ *is Galois, and* $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *[Hint: this may require reviewing the statements of class field theory to recall that, for* K *Galois, the map* $G_K \to G_K$ *given by conjugating by* $\sigma \in \mathbb{G}_{\mathbb{Q}}$ *corresponds, via the Artin map, to the natural action of* σ*, through* $\mathrm{Gal}(K/\mathbb{Q})$*, on* C_K*.]*

Proof of Theorem 2.2.1. Let $N = N_K$. We have, from the theory of finite abelian groups that $|N/2N| = |\mathrm{Hom}(N, \mathbb{Z}/2\mathbb{Z})$. If we consider the homomorphisms $N \to \mathbb{Z}/2\mathbb{Z}$, there is one trivial homomorphism, and the rest correspond, via the class field theory above, exactly to the unramified at finite places quadratic extensions L of K. We have seen that each such L is a Galois $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ extension of $\mathbb{Q}$.

So now we can ask, what are the $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ extensions L of $\mathbb{Q}$ containing K? By Galois theory, these correspond to normal subgroups S of $G_{\mathbb{Q}}$, contained in G_K and with quotient isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then these almost correspond to surjections $G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, whose projection onto the second coordinate gives the map $G_{\mathbb{Q}}/G_K \simeq \mathbb{Z}/2\mathbb{Z}$, except two surjections with the same kernel correspond to the same field. So two surjections correspond to the same field if and only if they differ by an automorphism of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and since we have fixed the projection onto the second coordinate, it must be an automorphism that preserves that projection. There are two such automorphisms, so each field L corresponds to two surjections $G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ whose projection onto the second coordinate gives the map $G_{\mathbb{Q}}/G_K \simeq \mathbb{Z}/2\mathbb{Z}$.

Given $L/\mathbb{Q}$ Galois with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and K the fixed field of $\langle (1,0) \rangle$ (as arranged above), we have L/K is unramified at all finite places if and only if the inertia groups of all finite places in $\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ have trivial intersection with $\langle (1,0) \rangle$. The only subgroups of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with this property are the trivial subgroup, $\langle (1,1) \rangle$, and $\langle (0,1) \rangle$. If a finite place ν of $\mathbb{Q}$ is unramified in K, then it follows that for L/K unramified at all finite places we must have the inertia group of ν in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ trivial.

From the above exercise, we have that

$$\prod_{\nu \text{ finite of } \mathbb{Q}} \mathcal{O}_\nu^* \times \mathbb{R}^* \simeq C_{\mathbb{Q}},$$

and so a continuous surjection $C_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ unramified outside of a set S of places of $\mathbb{Q}$ (those ramified in K) corresponds exactly to a continuous surjection

$$\phi : \prod_{\nu \in S} \mathcal{O}_\nu^* \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

In K, we are given, for each $\nu \in S$, a continuous surjection $\mathcal{O}_\nu^* \to \mathbb{Z}/2\mathbb{Z}$, and we see that to construct a ϕ corresponding to L as above we may lift this map to $\mathcal{O}_\nu^* \to \langle (1,1) \rangle$ or $\mathcal{O}_\nu^* \to \langle (0,1) \rangle$. If we lift all of the maps from $\mathcal{O}_\nu^*$ to the same subgroup, then ϕ won't be surjective, but otherwise it will be surjective. Any such surjective ϕ gives an L/K quadratic and unramified at finite places, and any L/K quadratic and unramified at finite places comes from two such

surjective ϕ. Thus we have that the number of L is $\frac{2^{|S|-2}}{2} = 2^{|S|-1}-1$, and thus $|N/2N| = |\operatorname{Hom}(N, \mathbb{Z}/2\mathbb{Z}) = 2^{t-1}$, as desired. □

So from the point of view of class field theory, these unramified abelian extensions L/K are "predictable" because they come from abelian extensions of $\mathbb{Q}$. We might wonder if there are are other such unramified abelian extensions that we can produce from abelian extensions of $\mathbb{Q}$.

Exercise 2.2.7. *Let K be a quadratic extension. Let $E/\mathbb{Q}$ be the maximal abelian extension of $\mathbb{Q}$ such that EK/K is unramified. So EK/K is an unramified abelian extension. Show that it corresponds to $2\operatorname{Cl}_K$ via class field theory (and Galois theory). So $\operatorname{Cl}_K/2\operatorname{Cl}_K$ is the part of Cl_K that abelian extensions of $\mathbb{Q}$ tell us about. Show the analogous statement for "unramified at finite places" and the narrow class group.*

This gives us a precise sense in which $\operatorname{Cl}_K/2\operatorname{Cl}_K$ is well-understood that provably does not apply to the rest of Cl_K. In any case, as there is this "predictable" piece of the class group Cl_K of a quadratic field in the 2-Sylow subgroup, Cohen and Lenstra, in their heuristics for the distribution of class groups, only considered the odd part $\operatorname{Cl}_K^{odd}$ (the quotient of Cl_K by its 2-Sylow subgroup).

2.3. The Cohen-Lenstra heuristics For simplicity, we will fix an odd p, and only consider $\operatorname{Cl}_{K,p}$, the Sylow p-subgroup of Cl_K. Let IQ, RQ be the sets of isomorphism classes of imaginary and real quadratic fields, respectively. Cohen and Lenstra's heuristics imply that for any "reasonable" [2] function f from the set of isomorphism classes of finite abelian p-groups to $\mathbb{R}$, that

$$\lim_{X\to\infty} \frac{\sum_{\substack{K\in IQ \\ D_K\leqslant X}} f(\operatorname{Cl}_K)}{\sum_{\substack{K\in IQ \\ D_K\leqslant X}} 1} = \frac{\sum_{A \text{ fin. ab. } p\text{-group}} \frac{f(A)}{|\operatorname{Aut}(A)|}}{\sum_{A \text{ fin. ab. } p\text{-group}} \frac{1}{|\operatorname{Aut}(A)|}} \tag{2.3.1}$$

and

$$\lim_{X\to\infty} \frac{\sum_{\substack{K\in RQ \\ D_K\leqslant X}} f(\operatorname{Cl}_K)}{\sum_{\substack{K\in RQ \\ D_K\leqslant X}} 1} = \frac{\sum_{A \text{ fin. ab. } p\text{-group}} \frac{f(A)}{|A||\operatorname{Aut}(A)|}}{\sum_{A \text{ fin. ab. } p\text{-group}} \frac{1}{|A||\operatorname{Aut}(A)|}}. \tag{2.3.2}$$

Note the denominators in (2.3.1) and (2.3.2) do not depend on f. They are simply some constant coming from the theory of finite abelian p-groups. Indeed, we have

$$\sum_{A \text{ fin. ab. } p\text{-group}} \frac{1}{|\operatorname{Aut}(A)|} = \prod_{i\geqslant 1}(1-p^{-i})^{-1} \quad \text{and} \quad \sum_{A \text{ fin. ab. } p\text{-group}} \frac{1}{|A||\operatorname{Aut}(A)|} = \prod_{i\geqslant 2}(1-p^{-i})^{-1}.$$

If we take f to be the characteristic function of a particular group, we see that the conjectures imply a particular p-group appears with a frequency inversely proportional to $|\operatorname{Aut}(A)|$ in the imaginary case and inversely proportional to $|A||\operatorname{Aut}(A)|$

[2] No particular definition of reasonable is given, but see [21, Section 5.6] and [10, Section 7].

in the real case. So in particular, this conjecture explains, in a precise way, the different frequencies with which different groups were empirically appearing in the tables. See [113, Section 5] and [110] for further exposition on these conjectures.

Exercise 2.3.3. *How often do the conjectures above predict that imaginary, respectively real, quadratic fields have cyclic Sylow* p*-subgroup?*

The heuristics of Cohen and Lenstra greatly benefited from the existence of tables of class groups of quadratic fields that could be used as evidence for the precise conjectures being made.

Exercise 2.3.4. *Using existing databases, make some tables of the frequency of* 3*-Sylow subgroups in class groups of imaginary (and/or real) quadratic fields up to some large discriminant. How do they compare to the conjectured values?*

There are no general conjectures about how quickly the limits in (2.3.1) and (2.3.2) approach their conjectured values. One could imagine conjectural secondary terms as well as conjectural error terms. Using the same approach as for counting cubic fields, we have secondary terms in one case [22, 26, 101] (we will discuss further below why the "same approach" applies). Not only would such a conjecture be interesting in its own right, but also if believable (say, based on evidence is certain cases and general heuristic reasoning), it might help us evaluate in other cases whether given data on class groups gives good evidence for a particular conjecture.

Project 2.3.5. *Using existing databases, make some graphs of how the proportion of imaginary (and/or) real quadratic fields of absolute discriminant in* $(X, 2X]$ *with a given class group changes with* X*. Do any of your graphs (or the underlying numbers) suggest a rate at which the limit is approached? Do they suggest precise secondary terms?*

Note that in the above exercise if you can uniformly randomly select a sample of fields in each range, you can ensure you get values close to the actual proportions via probability (e.g. Chebyshev's inequality). For quadratic fields, since you are likely getting class groups from a table as opposed to computing them, this doesn't seem worthwhile. However, if you are in a setting where you have to *compute* each class group, then sampling will vastly increase how large of an X you may consider.

Based on computations of the sort suggested in Project 2.3.5, Lewis and Williams conjecture approximate secondary terms for the proportion of real quadratic fields having class group with non-trivial Sylow p-subgroup. It would be interesting for these conjectures to be made more precise as in [92] and also to have conjectural secondary terms in other cases. Such conjectures, or a more general theory of how large we expect secondary or true error terms to be, can be very important in understanding if numerical data is supporting a conjecture, contradicting a conjecture, or not powerful enough to do either.

Two important motivations for Cohen-Lenstra heuristics originally were the agreement with tables and the general philosophy that objects occur in nature with frequency inversely proportional to the size of their automorphism group. See, e.g. Exercise 1.1.13 as well as the following exercise for some examples of this ubiquitous phenomenon.

Exercise 2.3.6. *Consider all* multiplication tables on n elements, *i.e. functions* $\{1,\dots,n\}\times\{1,\dots,n\}\to\{1,\dots,n\}$ *that are associative and have inverses and an identity. Show that a finite group* G *or order* n *is isomorphic to* $n!/|\operatorname{Aut}(G)|$ *of the groups given by these tables.*

3. A matrix model for class groups

3.1. The model Venkatesh and Ellenberg [106, Section 4.1] introduced an interesting perspective on class groups of quadratic fields as follows. Let K be a quadratic field and let S be a set of primes of K that generate Cl_K. We write $\mathcal{O}_S^*$ for the S-units in the integers $\mathcal{O}_K$, and I_K^S for the abelian group of fractional ideals generated by the elements of S. Let μ_K be the group of roots of unity in K. Then

$$\mathrm{Cl}(K)=\operatorname{cok}(\mathcal{O}_S^*/\mu_K\to I_K^S), \tag{3.1.1}$$

where the map takes α to the ideal (α).

Exercise 3.1.2. *If* A *is a finite abelian group given as* $\operatorname{cok}(U\to V)$ *for* U,V *finitely generated abelian groups, then the Sylow* p*-subgroup* A_p *is* $\operatorname{cok}(U\otimes\mathbb{Z}_p\to V\otimes\mathbb{Z}_p)$.

So

$$\mathrm{Cl}(K)_p=\operatorname{cok}(\mathcal{O}_S^*/\mu_K\otimes\mathbb{Z}_p\to I_K^S\otimes\mathbb{Z}_p).$$

We have that I_K^S is a free abelian group of rank $|S|$, so $I_K^S\otimes\mathbb{Z}_p\simeq\mathbb{Z}_p^{|S|}$. Dirichlet's unit theorem gives that $\mathcal{O}_S^*/\mu_K$ is a free abelian group of rank $|S|+u$, where $U=0$ if K is imaginary and $u=1$ if K is quadratic. So $\mathcal{O}_S^*/\mu_K\otimes\mathbb{Z}_p\simeq\mathbb{Z}_p^{|S|+u}$. If we choose bases for I_K^S and $\mathcal{O}_S^*/\mu_K$ as $\mathbb{Z}$-modules (which would give specific isomorphisms as above), then the map $\mathcal{O}_S^*/\mu_K\otimes\mathbb{Z}_p\to I_K^S\otimes\mathbb{Z}_p$ can be written as a matrix $M\in\mathrm{Mat}_{|S|\times|S|+u}(\mathbb{Z}_p)$. (Though M has integral entries, since we are interested in $\mathrm{Cl}_{K,p}$ we take the cokernel as a $\mathbb{Z}_p$-matrix.)

Exercise 3.1.3. *If* A *is a finite abelian* p*-group, the isomorphism type of* A *can be determined from* $A\otimes\mathbb{Z}/p\mathbb{Z}, A\otimes\mathbb{Z}/p^2\mathbb{Z}, A\otimes\mathbb{Z}/p^3\mathbb{Z},\dots$.

It is then natural to consider the distribution of $\mathrm{Cl}_K\otimes\mathbb{Z}/p^k\mathbb{Z}$.

Exercise 3.1.4. *Let* $N\in\mathrm{Mat}_{n\times m}(\mathbb{Z}_p)$ *and let* $\bar N\in\mathrm{Mat}_{n\times m}(\mathbb{Z}/p^k\mathbb{Z})$ *be obtained from* N *by reducing each coefficient mod* p^k*. Show*

$$\operatorname{cok}(N:\mathbb{Z}_p^m\to\mathbb{Z}_p^n)\otimes\mathbb{Z}/p^k\mathbb{Z}\simeq\operatorname{cok}(\bar N:(\mathbb{Z}/p^k\mathbb{Z})^m\to(\mathbb{Z}/p^k\mathbb{Z})^n).$$

So if we let $\bar M$ be the reduction of M mod p^k, we are interested in the distribution of the cokernels of these $\bar M\in\mathrm{Mat}_{|S|\times|S|+u}(\mathbb{Z}/p^k\mathbb{Z})$, where u is either 0 or 1. Now a priori we have no idea what the distribution of these $\bar M$ is,

but a baseline heuristic might be to guess they are approximately uniform in $\mathrm{Mat}_{n\times n+u}(\mathbb{Z}/p^k\mathbb{Z})$. Putting this together over different k, one might guess that the M are approximately distributed according to Haar measure on $\mathrm{Mat}_{n\times n+u}(\mathbb{Z}_p)$. This doesn't make perfect sense, because the n involved is not fixed, but as a heuristic we just imagine that n is large.

In any case, this leads to a natural question. What is the distribution of the cokernel of a random matrix from $\mathrm{Mat}_{n\times n+u}(\mathbb{Z}_p)$ taken with respect to Haar measure? Friedman and Washington [55] answered this question in the case $u = 0$. They were also motivated by the Cohen-Lenstra heuristics, but particularly the analog in which $\mathbb{Q}$ is replaced by $\mathbb{F}_q(t)$, in which one can write the class group as a cokernel of a different matrix involving the Frobenius.

Let N be a random matrix from $\mathrm{Mat}_{n\times n+u}(\mathbb{Z}_p)$ taken with respect to Haar measure. We wish to determine $\mathrm{Prob}(\mathrm{cok}(N) \simeq A)$ for each finite abelian p-group A, and we will follow the approach of [75] which does the analog for non-abelian profinite groups.

Exercise 3.1.5. *Show that if* $u \geqslant 0$, *then* $\mathrm{Prob}(\mathrm{cok}(N)$ *finite*$) = 1$.

Note that $\mathrm{Prob}(\mathrm{cok}(N) \simeq A) = |\mathrm{Aut}(A)|^{-1}\mathbb{E}(\#\mathrm{Isom}(\mathrm{cok}(N), A))$. (We use $\mathbb{E}$ to denote the expectation, or average, of a random real number.) Since $\mathrm{cok}\, N = \mathbb{Z}_p^n/N(\mathbb{Z}_p^{n+u})$, any isomorphism $\mathrm{cok}(N) \to A$ gives a distinct surjection of $\mathbb{Z}_p$-modules $\mathbb{Z}_p^n \to A$. So we consider a surjection $F : \mathbb{Z}_p^n \to A$, and ask, what is the probability that F descends to an isomorphism $\mathrm{cok}(N) \to A$? First, each column of N has to land in $\ker(F)$, and since each column is chosen independently from Haar measure on $\mathbb{Z}_p^n$, this happens with probability $[\mathbb{Z}_p^n : \ker F]^{n+u} = |A|^{n+u}$. The Haar measure on $\mathbb{Z}_p^n$ restricted to $\ker F$ is the Haar measure on $\ker F$. So the probability that F descends to an isomorphism $\mathrm{cok}(N) \to A$, conditioned on $FN = 0$ (i.e. each column of N is in $\ker F$), is the probability that $n + u$ independent elements from $\ker F \simeq \mathbb{Z}_p^n$ taken from Haar measure generate $\mathbb{Z}_p^n$. By Nakayma's lemma, this generation is equivalent to generation mod p, where the Haar measure becomes the uniform measure.

Exercise 3.1.6. *Show that the probability that* $n+u$ *uniform random elements of* $(\mathbb{Z}/p\mathbb{Z})^n$ *generate the group is*

$$\prod_{i=u+1}^{n+u}(1-p^{-i}).$$

Exercise 3.1.7. *If* A *is a finite abelian* p*-group of rank* r *(i.e.* $A \otimes \mathbb{Z}/p\mathbb{Z} \simeq (\mathbb{Z}/p\mathbb{Z})^r$*), show*

$$\#\mathrm{Sur}_{\mathbb{Z}_p}(\mathbb{Z}_p^n, A) = |A|^n \prod_{i=n-r+1}^{n}(1-p^{-i})$$

(where $\mathrm{Sur}_{\mathbb{Z}_p}$ *denotes* $\mathbb{Z}_p$*-module surjections).*

We conclude, that for A a finite abelian group, we have

(3.1.8)

$$\begin{aligned}\mathrm{Prob}(\mathrm{cok}(N) \simeq A) &= |\operatorname{Aut}(A)|^{-1}\mathbb{E}(\#\operatorname{Isom}(\mathrm{cok}(N), A)) \\ &= |\operatorname{Aut}(A)|^{-1}\#\operatorname{Sur}_{\mathbb{Z}_p}(\mathbb{Z}_p^n, A)|A|^{-(n+u)}\prod_{i=u+1}^{n+u}(1-p^{-i}) \\ &= |\operatorname{Aut}(A)|^{-1}|A|^n\prod_{i=n-r+1}^{n}(1-p^{-i})|A|^{-(n+u)}\prod_{i=u+1}^{n+u}(1-p^{-i}) \\ &= |\operatorname{Aut}(A)|^{-1}|A|^{-u}\prod_{i=u+1}^{n+u}(1-p^{-i})\prod_{i=n-r+1}^{n}(1-p^{-i}).\end{aligned}$$

We are interested in this value for a fixed A (and hence r), when n is large. So it is interesting to note that the above probabilities approach a limit as $n \to \infty$, and in particular approach

$$|\operatorname{Aut}(A)|^{-1}|A|^{-u}\prod_{i\geqslant u+1}(1-p^{-i}),$$

which are precisely the probabilities prediction by the Cohen-Lenstra heuristics for class groups of imaginary and real quadratic fields.

Exercise 3.1.9. *Find a formula for* $|\operatorname{Aut}(G)|$ *when* G *is an abelian* p*-group. [Hint: it is useful to choose* $\lambda_1 \geqslant \lambda_2 \geqslant \cdots$ *to denote the isomorphism type of the group, where* $p^{i-1}G/p^iG \simeq (\mathbb{Z}/p\mathbb{Z})^{\lambda_i}$*. As in the proof above, first count homomorphisms, and then restrict to counting those that are surjective.]*

3.2. Class group matrices From the above analysis, it is tempting to make a conjecture about the distribution of the matrices M described in the last section as K varies over quadratic fields. In particular one imagines a conjecture that the M are approximately or asymptotically distributed with respect to Haar measure on p-adic matrices which would imply the Cohen-Lenstra conjecture for the distribution of class groups. There are several subtleties. One needs, for each K, to pick a set S of primes. One could take, for example, all primes of K up to norm B, where B is the Minkowski bound so that S necessarily generates Cl_K. One needs to pick bases for I^S and $\mathcal{O}_S^*/\mu_K$. Of course, there is a natural basis for I^S given by the elements of S.

Question 3.2.1. *Is there a "natural" basis of* $\mathcal{O}_S^*$*?*

Then, one needs an equidistribution conjecture for elements in groups, where the groups themselves are changing (since $|S|$ will not be constant). Friedman and Washington [55, Section 2] suggest one way to do this.

Preliminary computations however, using choices as suggested above, with a basis of $\mathcal{O}_S^*$ given by the output of computer algebra computations of $\mathcal{O}_S^*$, suggest these matrices are quite far from equidistributed for Haar measure.

Project 3.2.2. *Do such computations and see what the distribution of matrices arising looks like. Do they look like they are coming from Haar measure? Try other choices of setup e.g. fixing an* n *and then taking all* K *such that known bounds guarantee that the first* n *primes of* K *are sufficient to generate the class group, so one has many matrices of the same dimension.*

3.3. Universality If the actual matrices defining Sylow p-subgroups of class groups as above are not distributed as in they are coming from Haar measure, does that mean that the Cohen-Lenstra conjectures are wrong? The answer is very much no. In fact, there is a *universality* phenomenon that says a very wide range of distributions of random matrices, asymptotically as the size of the matrices goes to infinity, have cokernel distribution approach the Cohen-Lenstra distribution. This universality is in the sense of the Central Limit Theorem.

Theorem 3.3.1 (Central Limit Theorem)**.** *Let* $X_1, X_2, \dots$ *be independent, identically distributed random real numbers with finite mean* $\mu = \mathbb{E}(X_i)$ *and finite variance* σ^2*. Then as* $n \to \infty$*,*

$$\sqrt{n}\left(\frac{X_1 + \cdots + X_n}{n} - \mu\right)$$

converge in distribution to the normal distribution with mean 0 *and variance* σ^2*.*

The universality aspect of the Central Limit Theorem is that X_i can have almost any distribution. That includes the case when the X_i are normal, which is a highly symmetric distribution that we think of as analogous to Haar measure. However, the Central Limit Theorem also applies for X_i that are quite irregular. No matter what X_i you put in, the asymptotic output of this weighted averaging process is a normal distribution.

There is a morally similar result of the author for cokernels of random matrices.

Theorem 3.3.2 ([117, Theorem 1.3])**.** *Let* p *be a prime,* u *be a non-negative integer and* $\epsilon > 0$ *be a real number. For each positive integer* n*, let* $M(n)$ *be a random matrix valued in* $\mathrm{Mat}_{n \times n+u}(\mathbb{Z}_p)$ *with independent entries. Further, for any entry* $M(n)_{i,j}$ *of any* $M(n)$ *and any* $r \in \mathbb{Z}/p\mathbb{Z}$*, we require that*

$$\mathbb{P}(M(n)_{i,j} \equiv r \pmod{p}) \leqslant 1 - \epsilon. \tag{3.3.3}$$

Then for any finite abelian p*-group* A*,*

$$\lim_{n \to \infty} \mathbb{P}(\mathrm{cok}(M(n)) \simeq A) = \frac{\prod_{i \geqslant 1}^{\infty}(1 - p^{-i})}{|A|^u \,\mathrm{Aut}(A)|}. \tag{3.3.4}$$

Theorem 3.3.2 allows great flexibility in the random matrices, in particular the matrix entries do not have to be identically distributed. The matrix entries are certainly not required to take every value mod p (and hence are not required to take every value mod p^k), but have a much weaker requirement that they not be entirely concentrated on one value mod p. It is easy to see some such condition is required, as the all 0's matrix is technically a random matrix with independent entries. The given hypothesis (3.3.3) can certainly be weakened, see [86, Theorem

4.1]). The independence of the entries is indeed a strong requirement, and something along those lines is of course necessary, but one could imagine weakening the hypothesis to some kind of asymptotic or approximate independence. See also [118, Section 3] for further exposition of this kind of universality phenomenon.

Project 3.3.5. *Based on computations from* (3.2.2)*, make an empirically supported conjecture about the distribution of the matrices* M *from imaginary and/or real quadratic fields. Can the methods of* [117] *be extended to show that prove matrices from with a distribution as conjectured satisfy* (3.3.4)*?*

4. Moments of class group distributions

So far, the main function f we have been considering averaging in (2.1.2) (i.e. over class groups of number fields) has been the characteristic function of having a specified Sylow p-subgroup.

4.1. Definition of moments of a random finite abelian group In fact, there is another class of important f, which are indexed by finite abelian groups B, where

$$f_B(X) := \#\mathrm{Sur}(X, B).$$

Let

$$E(f, S) := \lim_{X\to\infty} \frac{\sum_{K\in S,\ D_K\leqslant X} f(\mathrm{Cl}_K)}{\sum_{K\in S,\ D_K\leqslant X} 1}$$

be the empirical average of f over a family S of number fields, assuming the limit exists. (Showing that such a limit exists is quite difficult, and indeed is only known in the few cases where we know what the limit is.)

Exercise 4.1.1. *If* B *is a finite abelian group, show that the values of* $E(\#\mathrm{Sur}(-, B'), S)$ *over subgroups* B' *of* B *determine the value of* $E(\#\mathrm{Hom}(-, B), S)$*, and that the values of* $E(\#\mathrm{Hom}(-, B'), S)$ *over subgroups* B' *of* B *determine the value of* $E(\#\mathrm{Sur}(-, B), S)$*.*

Exercise 4.1.2. *If* X *is a finite abelian group of exponent* p*, show that* $\#\mathrm{Hom}(X, (\mathbb{Z}/p\mathbb{Z})^k) = |X|^k$*.*

This is reminiscent of certain functions $f_k(X) = X^k$, whose averages are important statistics of distributions of real numbers. If X is a random number, then $\mathbb{E}(X^k)$ is called the k-th moment of X or the distribution of X. These moments are often more accessible than direct information about a distribution. Yet wonderfully, knowledge of all of the moments often determines a distribution uniquely. For example, we have the following classical theorem on the moment problem.

Theorem 4.1.3 (Carleman's condition)**.** *Let* X *be a random real number such that* $M_k = \mathbb{E}(X^k)$ *is finite for all integers* $k \geqslant 0$*. Then if*

$$\sum_{k\geqslant 1} M_{2k}^{-\frac{1}{2k}} = \infty, \tag{4.1.4}$$

then there is a unique distribution for a random real number Y *such that* $\mathbb{E}(Y^k) = M_k$ *for all* $k \geqslant 0$.

Exercise 4.1.5. *Can you apply Theorem 4.1.3 for* $M_k = e^k$*? What about* $M_k = e^{k^2}$*?*

The averages of $\#\mathrm{Sur}(-, B)$ are important enough that they are called the *moments* of a distribution of finite abelian groups. The moments are indexed by finite abelian groups. If X is a random finite abelian group, then the average $\mathbb{E}(\#\mathrm{Sur}(X, B))$ is the B-moment of X, or of the distribution of X. As in Exercise 4.1.2, if we reduce a finite abelian group to a certain list of integer invariants, then the averages of $\#\mathrm{Hom}(-, B)$ are precisely the mixed moments of those integer invariants (in the classical sense of mixed moments) [35, Section 3.3]. Exercise 4.1.1 shows that as far as knowledge of the moments of a random variable (or even the limit of moments of a sequence of random variables) is concerned, it doesn't matter if we count homomorphisms or surjective homomorphisms. This is analogous to the relationship between the moments $\mathbb{E}(X^k)$ and the factorial moments $\mathbb{E}(X(X-1)\cdots(X-k+1))$ of a random number. One uses one version of the moments as opposed to the other generally when they make the computations and formulas simpler.

One important feature of these moments of finite abelian groups is that they determine a distribution uniquely (when they are not too large), analogously to Theorem 4.1.3.

Theorem 4.1.6 ([118, Corollary 2.6])**.** *Let* $M_A \in \mathbb{R}$ *for each finite abelian group* A *such that there is a constant* C *such that* $M_A \leqslant C|\wedge^2 A|$ *for every* A*. Let* X, Y *be random finite abelian groups, If for every finite abelian group* A*, we have*

$$\mathbb{E}(\#\mathrm{Sur}(X, A)) = \mathbb{E}(\#\mathrm{Sur}(Y, A)) = M_A,$$

then X *and* Y *have the same distribution, i.e. for every finite abelian group* B*,*

$$\mathrm{Prob}(X \simeq B) = \mathrm{Prob}(Y \simeq B).$$

For our questions of distribution of class groups, we are never considering a single random group, but rather a sequence of random groups (indexed by X, where for each X we take a uniform random field with $D_K \leqslant X$). The averages $\mathbb{E}(f, S)$ we consider are limits of averages. So we naturally ask when the limit moments of a sequence of random variables implies the sequence has a given limit distribution. This works well for finite abelian p-groups, but breaks down when we consider all finite abelian groups, at least for the most naive sense of limit distribution.

Theorem 4.1.7 (see [114, Thm 8.3, proof of Cor 9.2])**.** *Let* p *be prime, and let* $\mathcal{A}$ *be the set of finite abelian* p*-groups. Let* $M_A \in \mathbb{R}$ *for each* $A \in \mathcal{A}$ *such that there is a constant* C *such that* $M_A \leqslant C|\wedge^2 A|$ *for all* $A \in \mathcal{A}$*. Let* $Y, X_1, X_2, \ldots$ *be random groups in* $\mathcal{A}$*. If for every* $A \in \mathcal{A}$*, we have*

$$\lim_{n\to\infty} \mathbb{E}(\#\mathrm{Sur}(X_n, A)) = \mathbb{E}(\#\mathrm{Sur}(Y, A)) = M_A,$$

then for every $B \in \mathcal{A}$,

$$\lim_{n\to\infty} \mathrm{Prob}(X_n \simeq B) = \mathrm{Prob}(Y \simeq B).$$

As in [110, Example 6.14], we can consider a random finite abelian group X, e.g. such that

$$\mathrm{Prob}(X \simeq A) = \frac{\zeta(2)^{-1}\zeta(3)^{-1}\zeta(4)^{-1}\cdots}{|A||\operatorname{Aut} A|}.$$

(There is a random group with this distribution–see e.g. [115, Proposition 2.1].) Then consider the random groups $X_p := X \times \mathbb{Z}/p\mathbb{Z}$ for each prime p.

Exercise 4.1.8. *For any finite abelian group* A*, show that*

$$\lim_{p\to\infty} \mathbb{E}(\#\mathrm{Sur}(X \times \mathbb{Z}/p\mathbb{Z}, A)) = \mathbb{E}(\#\mathrm{Sur}(X, A)).$$

What is $\lim_{n\to\infty} \mathrm{Prob}(X_n \simeq A)$*?*

While Theorem 4.1.6 shows that on finite abelian p-groups, limit moments contain enough information to determine a limit distribution, the converse is false.

Exercise 4.1.9. *Construct a sequence* $Y, X_1, X_2, \ldots$ *of random finite abelian* p*-groups such that for every finite abelian* p*-group* B *we have*

$$\lim_{n\to\infty} \mathrm{Prob}(X_n \simeq B) = \mathrm{Prob}(Y \simeq B).$$

but yet for some finite abelian p*-group* A *we have*

$$\lim_{n\to\infty} \mathbb{E}(\#\mathrm{Sur}(X_n, A)) \neq \mathbb{E}(\#\mathrm{Sur}(Y, A)).$$

Show that you can do this for any Y *with finite moments. Show that you can have the limit* $\lim_{n\to\infty} \mathbb{E}(\#\mathrm{Sur}(X_n, A))$ *not exist.*

So, when we are taking limits of distributions of finite abelian p-groups, we see that these limiting moments are even stronger information than the limiting distributions. See [118, Section 2] and [114, Sections 1.5, 8] for further exposition on the moment problem for random groups and its applications to number theory.

Project 4.1.10. *Similar to Project 2.3.5, using existing databases, make some graphs of how various moments of the class groups of imaginary (and/or) real quadratic fields of absolute discriminant converge to the predicted values. (See* [81] *and* [116, Appendix] *for some such computations.) Do any of your graphs (or the underlying numbers) suggest a rate at which the limit is approached? Do they suggest precise secondary terms?*

The importance of having conjectures for the rate of convergence or secondary terms has been discussed above for the average proportion of class groups having a fixed Sylow p-subgroup. In the case of moments, it is perhaps even more important, because convergence to moments is a more desirable target to check given that, as we will see below, the conjectural moment values are generally nice rational numbers (as opposed to the conjectural proportion values).

4.2. Relationship of moments to field counting What about the aspect of moments that they are supposed to be easier to access? This turns out to also be the case for distributions of class groups. The only non-trivial f for which the averages (2.3.1) or (2.3.2) predicted by the Cohen-Lenstra heuristics for quadratic fields is known is $\#\mathrm{Sur}(-, \mathbb{Z}/3\mathbb{Z})$. These averages are results of Davenport and Heilbronn [45], and predate the Cohen-Lenstra Heuristics. They turn out to be closely related to counting cubic fields. (See also [67] and [113, Section 3] for more discussion on the relationship between counting number fields and the Cohen-Lenstra heuristics, and [90] for a discussion of the relationship between both these questions and conjectures on upper bounds on class groups.)

Let A be an odd finite abelian group, and let $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ be the semi-direct product where $\mathbb{Z}/2\mathbb{Z}$ acts on A by multiplication by -1.

Exercise 4.2.1. *Let K be a quadratic field and L/K and unramified abelian extension with $\mathrm{Gal}(L/K) \simeq A$. Show that $L/\mathbb{Q}$ is Galois and $\mathrm{Gal}(L/K) \simeq A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$. (Don't forget that when $|A|$ is even there can be more than one group extension of $\mathbb{Z}/2\mathbb{Z}$ by A where the associated action is by -1.)*

Exercise 4.2.2. *Let A be an odd order finite abelian group. Let $L/\mathbb{Q}$ be Galois with Galois group $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$. Show that L contains a unique quadratic field K_L.*

Thus, for an odd order abelian group A, we have a correspondence between pairs (K, L) where K is an isomorphism class of quadratic fields and L/K is an isomorphism class of unramified abelian extensions of K with Galois group A and isomorphism classes of $L/\mathbb{Q}$ Galois with Galois group $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ such that L is unramified over its unique quadratic subfield.

Exercise 4.2.3. *Show that this correspondence is $2-1$. (See Exercise 1.2.27.)*

Given K, isomorphism classes L/K of unramified abelian extensions of K with Galois group A correspond to $\mathrm{Aut}(A)$ orbits of surjections $\mathrm{Sur}(\mathrm{Cl}_K, A)$, via class field theory. Thus $\mathrm{Sur}(\mathrm{Cl}_K, A)$ has a natural meaning in terms of unramified extensions, which gives another motivation for the definition of moments above– we are averaging a count that is algebraically meaningful.

Let S be a set of quadratic fields K and A a finite abelian group A. Let T be the set of isomorphism classes of Galois $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ extensions, unramified over their quadratic subfields, such that their quadratic subfield is in S. Then

$$\sum_{K \in S} \#\mathrm{Sur}(\mathrm{Cl}_K, A) = 2|\mathrm{Aut}(A)|\#T.$$

Thus the moments of class group distributions are closely related the the number field counting questions in the first section, for groups $G = A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ in their regular representation. The main difference is that we restrict ramification behavior (and since in class group questions we usually fix the signature of the quadratic field, this would also require an additional restriction on the counted G fields at infinity).

We can slightly shift the problem, by recognizing that since $\mathbb{Z}/2\mathbb{Z}$ is a subgroup of $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$, that a Galois $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ extension $L/\mathbb{Q}$ also has a subfield F such that L/F is quadratic.

Exercise 4.2.4. *In the above situation, show that $F/\mathbb{Q}$ is not Galois, and that L is its Galois closure. In fact, there are many such subfields F, but show they are all isomorphic.*

Exercise 4.2.5. *In the above situation, find the Galois group $\mathrm{Gal}(F/\mathbb{Q})$, as a permutation group.*

Exercise 4.2.6. *In the above situation, show that the absolute discriminants have the property $D_F = D_{K_L}^{(|A|-1)/2}$. (Hint: it may be useful to use the fact that for a Galois extension $L/\mathbb{Q}$ with subgroup H, the discriminant $\mathrm{Disc}\, L^H$ of the fixed field is the Artin conductor of the permutation representation of G on H cosets* [85, VII:11.8].*)*

Thus one could also count $F/\mathbb{Q}$ with the Galois group above, with sufficient conditions on ramification and at infinity to ensure that the corresponding L and K_L are as desired. When $A = \mathbb{Z}/3\mathbb{Z}$, the corresponding F are precisely non-Galois cubic extensions such that no prime of $\mathbb{Q}$ ramifies completely in F.

Exercise 4.2.7. *Show that in the case $A = \mathbb{Z}/3\mathbb{Z}$, for a non-Galois cubic field F to have the corresponding L/K_L unramified, it is necessary and sufficient that no prime of $\mathbb{Q}$ ramifies completely in F.*

The approach of Davenport and Heilbronn [45] was sufficiently flexible to impose this ramification condition on cubic fields (it turns out to be a condition on the associated binary cubic form mod p^2 for each prime p, which is already the sort of condition they had to face to consider which forms actually corresponded to fields).

Theorem 4.2.8 ([45, Theorem 3])**.** *We have*

$$\lim_{X\to\infty} \frac{\sum_{\substack{K\in IQ \\ D_K\leqslant X}} \#\mathrm{Sur}(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z}))}{\sum_{\substack{K\in IQ \\ D_K\leqslant X}} 1} = 1 \tag{4.2.9}$$

and

$$\lim_{X\to\infty} \frac{\sum_{\substack{K\in RQ \\ D_K\leqslant X}} \#\mathrm{Sur}(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z})}{\sum_{\substack{K\in RQ \\ D_K\leqslant X}} 1} = \frac{1}{3}. \tag{4.2.10}$$

Given the Cohen-Lenstra conjectures (2.3.1) and (2.3.2), this begs the question whether

$$\sum_{\substack{A \text{ fin. ab.} \\ 3\text{-group}}} \frac{\#\mathrm{Sur}(A, \mathbb{Z}/3\mathbb{Z})}{|\mathrm{Aut}(A)|} \prod_{i\geqslant 1}(1-3^{-i}) = 1 \quad \text{and} \quad \sum_{\substack{A \text{ fin. ab.} \\ 3\text{-group}}} \frac{\#\mathrm{Sur}(A, \mathbb{Z}/3\mathbb{Z})}{|A||\mathrm{Aut}(A)|} \prod_{i\geqslant 2}(1-3^{-i}) = \frac{1}{3}? \tag{4.2.11}$$

These two equalities are indeed true (recall the the work of Davenport and Heilbronn predated the work of Cohen and Lenstra). In fact, more generally we

have for a prime p and finite abelian p-group B

$$\sum_{\substack{A \text{fin. ab.}\\ p\text{-group}}} \frac{\#\mathrm{Sur}(A,B)}{|\mathrm{Aut}(A)|}\prod_{i\geqslant 1}(1-p^{-i}) = 1 \quad \text{and} \quad \sum_{\substack{A \text{fin. ab.}\\ p\text{-group}}} \frac{\#\mathrm{Sur}(A,B)}{|A||\mathrm{Aut}(A)|}\prod_{i\geqslant 2}(1-p^{-i}) = \frac{1}{|B|},$$

and the Cohen-Lenstra heuristics predict the corresponding averages for the class groups of imaginary and real quadratic fields, respectively. Since we know all finite abelian p-groups, we can express the left-hand sides above as a formal expression in p. Cohen and Lenstra developed a generating function machinery that allows one to compute such group theoretic averages (see [39, Section 9 (C6),(C9)] and [117, Lemma 3.2]). However, perhaps the most direct path to the computations above is to consider the random matrix models of Section 3.

Exercise 4.2.12. *Let N be a random matrix from $\mathrm{Mat}_{n\times n+u}(\mathbb{Z}_p)$ (for $u \geqslant 0$) taken with respect to Haar measure. For a finite abelian p-group B, find $\mathbb{E}(\#\mathrm{Sur}(\mathrm{cok}(N),B)$ and show*

$$\lim_{n\to\infty} \mathbb{E}(\#\mathrm{Sur}(\mathrm{cok}(N),B) = |B|^{-u}.$$

[Hint: this is an easier version of the computation of $\mathbb{E}(\#\mathrm{Isom}(\mathrm{cok}(N),B)$ we did in Section 3.]

Thus we have

$$\lim_{n\to\infty} \sum_{\substack{A \text{ fin. ab.}\\ p\text{-group}}} \mathrm{Prob}(\mathrm{cok}(N)\simeq A)\#\mathrm{Sur}(A,B) = |B|^{-u}. \tag{4.2.13}$$

Since we know

$$\lim_{n\to\infty} \mathrm{Prob}(\mathrm{cok}(N)\simeq A) = \frac{\prod_{i\geqslant u+1}(1-p^{-i})}{|A|^u|\mathrm{Aut}\,A|}, \tag{4.2.14}$$

if we can exchange the limit in n with the sum over A, we would conclude

$$\sum_{\substack{A \text{ fin. ab.}\\ p\text{-group}}} \frac{\#\mathrm{Sur}(A,B)}{|A|^u|\mathrm{Aut}\,A|}\prod_{i\geqslant u+1}(1-p^{-i}) = |B|^{-u}. \tag{4.2.15}$$

While such an exchange is not always possible, here it can be justified. From (3.1.8), we have

(4.2.16)

$$\frac{\mathrm{Prob}(\mathrm{cok}(N)\simeq A)}{\prod_{i=u+1}^{n+u}(1-p^{-i})}\#\mathrm{Sur}(A,B) = |\mathrm{Aut}(A)|^{-1}|A|^{-u}\prod_{i=n-r+1}^{n}(1-p^{-i})\#\mathrm{Sur}(A,B).$$

Observe that the expression on the right is increasing in n. Thus by the monotone convergence theorem, we have

$$\lim_{n\to\infty}\sum_{\substack{A \text{ fin. ab.}\\ p\text{-group}}} \frac{\mathrm{Prob}(\mathrm{cok}(N)\simeq A)}{\prod_{i=u+1}^{n+u}(1-p^{-i})}\#\mathrm{Sur}(A,B) = \sum_{\substack{A \text{ fin. ab.}\\ p\text{-group}}} \lim_{n\to\infty}\frac{\mathrm{Prob}(\mathrm{cok}(N)\simeq A)}{\prod_{i=u+1}^{n+u}(1-p^{-i})}\#\mathrm{Sur}(A,B).$$

Since $\prod_{i=u+1}^{n+u}(1-p^{-i})$ doesn't depend on A, it (along with its limit) can pull out of the sum and we have

$$\lim_{n\to\infty}\sum_{\substack{A \text{ fin. ab.}\\ p\text{-group}}} \mathrm{Prob}(\mathrm{cok}(N)\simeq A)\#\mathrm{Sur}(A,B) = \sum_{\substack{A \text{ fin. ab.}\\ p\text{-group}}} \lim_{n\to\infty}\mathrm{Prob}(\mathrm{cok}(N)\simeq A)\#\mathrm{Sur}(A,B),$$

which, with (4.2.13) and (4.2.14), implies (4.2.15).

Theorem 4.1.7 then implies that Cohen and Lenstra's conjectural distribution for Sylow p-subgroups of class groups of imaginary, respectively real, quadratic fields is the unique distribution on finite abelian p-groups with moments all 1, respectively with B-moment $|B|^{-1}$.

Exercise 4.2.17. *Using genus theory (and some results from analytic number theory of the integers that you might have to look up), show that*

$$\lim_{X\to\infty}\frac{\sum_{\substack{K\in RQ\\ D_K\leqslant X}}\#\mathrm{Sur}(\mathrm{Cl}_K,\mathbb{Z}/2\mathbb{Z})}{\sum_{\substack{K\in RQ\\ D_K\leqslant X}}1} = \lim_{X\to\infty}\frac{\sum_{\substack{K\in RQ\\ D_K\leqslant X}}\#\mathrm{Sur}(\mathrm{Cl}_K,\mathbb{Z}/2\mathbb{Z})}{\sum_{\substack{K\in RQ\\ D_K\leqslant X}}1} = \infty$$

This shows another, quantitative, way in which the 2-Sylow subgroups of class groups of quadratic fields behave differently than the (conjectural) behavior of the odd part of the class groups.

5. Cohen-Lenstra-Martinet heuristics

What about the distribution of class groups of number fields of higher degree than 2? Cohen and Lenstra [39] actually gave conjectures on class groups distributions for totally real G-extensions for any abelian group G, and Cohen and Martinet [40] gave conjectures on class groups distributions for G-extensions for any transitive permutation group G and any signature. See also [110] for an exposition of these conjectures as well as more direct, equivalent forms of the conjectures.

5.1. Class groups of Galois extensions Let G be a finite simply transitive permutation group, so in particular G-extensions are Galois over $\mathbb{Q}$. We will consider class groups of G-extensions that come with an isomorphism $\mathrm{Gal}(K/\mathbb{Q})\simeq G$, and call these pairs of a field and an isomorphism *G-Extensions*. If K is a G-Extension, then Cl_K is a G-module (i.e. a module for the group ring $\mathbb{Z}[G]$). Note that for Cl_K to be a G-module, and not just a $\mathrm{Gal}(K/\mathbb{Q})$-module, we do require the data of the isomorphism $\mathrm{Gal}(K/\mathbb{Q})\simeq G$.

The conjectural probabilities in (2.3.1) and (2.3.2) involve $|\mathrm{Aut}(A)|$. Part of the philosophy of Cohen-Lenstra-Martinet is what we should always consider objects with all available structure. After all, we consider the automorphisms of A as a group, not a set. So the probabilities for class groups of G-Extensions should involve $|\mathrm{Aut}_G(A)|$, the number of automorphisms of A as a G-module.

Which finite G-modules can arise?

Exercise 5.1.1. *Show that* $N := \sum_{g \in G} G$ *acts as zero on* Cl_K*, i.e.* $N \mathrm{Cl}_K = 0$*.*

So we let $R = \mathbb{Z}[G]/N\mathbb{Z}[G]$, and have that Cl_K is a finite R-module.

Exercise 5.1.2. *For* $G = \mathbb{Z}/3\mathbb{Z}$*, find an example of finite abelian group that can't be the class group of a* G*-extension, because it doesn't have the structure of an* R*-module.*

Exercise 5.1.3. *For a finite* R*-module* A*, show that* $|\mathrm{Aut}_G(A)| = |\mathrm{Aut}_R(A)|$*, where* $\mathrm{Aut}_R(A)$ *is the group of automorphisms of* A *as an* R*-module.*

What then is the analog of the $|A|^u$ factor? In the case of quadratic fields, we saw that the actual value of this factor (i.e. the value of u), was different in the different families of fields depending on their behavior at infinity. Fix a subgroup G_∞ of G. Let S_{G,G_∞} be the set of isomorphism classes of G-Extensions of $\mathbb{Q}$ (where isomorphisms are given by isomorphisms of the field that respect the identification of the Galois group with G) whose decomposition group at infinity is conjugate to G_∞ (i.e. so that complex conjugation generates a subgroup conjugate to G_∞).

Exercise 5.1.4. *Find the signature and the unit rank of a* $K \in S_{G,G_\infty}$*.*

Let p be a prime such that $p \nmid |G|$. We will restrict to Sylow p-subgroups of class groups for simplicity. Cohen and Martinet's heuristics [40, Hypothesis 6.6] give a conjecture on the distribution of Sylow p-subgroups class groups of G-extensions that takes quite a bit of notation to write down. However, Wang and the author [110, Theorems 1.1 and 4.1, Proposition 6.6] prove that it is equivalent to conjecturing that for "reasonable" functions f from the set of finite p-group R-modules to $\mathbb{R}$ that we have

$$\lim_{X\to\infty} \frac{\sum_{\substack{K\in S_{G,G_\infty}\\ D_K\leqslant X}} f(\mathrm{Cl}_K)}{\sum_{\substack{K\in S_{G,G_\infty}\\ D_K\leqslant X}} 1} = \frac{\sum_{A \text{ fin. } p\text{-group}\atop R\text{-module}} \frac{f(A)}{|A^{G_\infty}||\mathrm{Aut}_R(A)|}}{\sum_{A \text{ fin. } p\text{-group}\atop R\text{-module}} \frac{1}{|A^{G_\infty}||\mathrm{Aut}_R(A)|}}. \tag{5.1.5}$$

Here A^{G_∞} is the subgroup of elements of A that are fixed by every element of G_∞.

As before, the denominator of the right-hand side of (5.1.5) is a convergent sum and can be given explicitly (see [110, Remark 3.4], [40, Theorem 3.6]).

Of course, these conjectures should specialize to the conjectures of Cohen and Lenstra (2.3.1) and (2.3.2) for quadratic extensions.

Exercise 5.1.6. *Check* $|A^{G_\infty}|$ *is consistent with the* $|A|^u$ *terms in the quadratic conjectures* (2.3.1) *and* (2.3.2)*.*

When $G = S_2$, then $R = \mathbb{Z}[\sigma]/(1+\sigma) = \mathbb{Z}$. So $\mathrm{Aut}(A) = \mathrm{Aut}_R(A)$. This echoes the fact, that we saw in Exercise 2.2.5, that the Galois group acts at -1 on the class group in this case, which is not really any "additional structure" on an abelian group.

Exercise 5.1.7. *Let* $G = \mathbb{Z}/\ell\mathbb{Z}$ *for a prime* ℓ*. What is* R *in this case? What are all the* p*-group* R*-modules?*

Exercise 5.1.8. *Let* $G = \mathbb{Z}/\ell\mathbb{Z}$ *for a prime* ℓ*. Find a formula for* $|\operatorname{Aut}_R(A)|$ *when* A *is a* p*-group* R*-module. [Hint: As in Exercise 3.1.9 it is useful denote the isomorphism type of the* R*-module by a set of partitions indexed by the primes* $\wp$ *of* R *dividing* p*, where if* λ *is the partition corresponding to* $\wp$*, then* $\wp^{i-1}A/\wp^i A \simeq (R/\wp)^{\lambda_i}$*.]*

There were some class group tables available for Cohen and Martinet to check their conjectures against, but not nearly as many as in the case of quadratic fields. Also, it is often difficult to distinguish between slow convergence to the conjectured values and convergence that is contradicting the conjectures. Malle [81, 82] later was able to compute significantly more data on class groups, and was able discover compelling evidence from his tables that for $|G|$ odd and $p = 2$ the conjecture (5.1.5) is likely incorrect. These conjectures are expected to come from roots of unity in the base field—in this case $\{\pm 1\} \subset \mathbb{Q}$. (This expected relationship to roots of unity comes also from further computations, including computations of Malle over other base fields, theoretical considerations, as well as function field results including [1, 50]). The fact that $|\{\pm 1\}| = 2$ is why $p = 2$ is a problem, and when $|G|$ is even, $p = 2$ was already excluded for other reasons. Several works have addressed the question of how to modify (5.1.5) when $p = 2$ and $|G|$ is odd or analogous situations over base fields other than $\mathbb{Q}$ [3, 57, 73, 74].

As in the case of quadratic extensions, there are certain functions f whose averages are particularly useful and more accessible. For a finite R-module B, the average of $\#\operatorname{Sur}_R(-, B)$ over a distribution is the B-moment of a distribution of R-modules, or for a random R-module X, we say that

$$\mathbb{E}(\#\operatorname{Sur}_R(X, B))$$

is its B-moment. As in the case of conjectures for quadratic extensions, these moments have nice values over the distribution from the right-hand side of (5.1.5).

Theorem 5.1.9 ([110, Theorem 6.2])**.** *For any finite group* G*, prime* $p \nmid |G|$*, subgroup* G_∞ *of* G*, and* p*-group* R*-module* B*, we have*

$$\frac{\sum_{\substack{A \text{ fin. } p\text{-group} \\ R\text{-module}}} \frac{\#\operatorname{Sur}_R(A,B))}{|A^{G_\infty}||\operatorname{Aut}_R(A)|}}{\sum_{\substack{A \text{ fin. } p\text{-group} \\ R\text{-module}}} \frac{1}{|A^{G_\infty}||\operatorname{Aut}_R(A)|}} = \frac{1}{|B^{G_\infty}|}$$

Exercise 5.1.10. *For* $G = \mathbb{Z}/\ell\mathbb{Z}$ *for a prime* ℓ*, prove Theorem 5.1.9 using a strategy similar to what we used to prove* (4.2.15)*.*

Moreover, as in Theorem 4.1.7, these moments determine a unique distribution on p-group R-modules, even through a limit [110, Theorem 6.12].

Project 5.1.11. *Replicate and extend Malle's empirical class group distribution computations for* $G = \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$*, and/or* $\mathbb{Z}/7\mathbb{Z}$ [81, Sections 2,3] *and* [82, Section 6.1]*, i.e. over a large number of appropriate fields compute the class group distribution and*

first few moments (see the subsection below on different notions of moments). Can you see the bad behavior at $p = 2$*? At other* p*, do you see convergence towards the predicted value? Can you make a conjecture about a rate of convergence, second term, or error term? Can you implement a sampling technique to randomly sample fields up to a given discriminant instead of considering all fields? What is the trade-off in computation time and accuracy?*

Project 5.1.12. *The same as Project 5.1.11 except for* $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *(and ignore* $p = 2$*, but don't forget to consider different* G_∞*).*

Project 5.1.13. *For* $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*, and an odd prime* p*, use Exercise 5.2.2 to show that for a* G*-Extension* K*, that* $\mathrm{Cl}_{K,p}$ *is determined by the Sylow* p*-subgroups of the class groups of the three quadratic subextensions (indeed, it is their product). Can this be used to show that* (5.1.5) *for* $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *follows from* (2.3.1) *and* (2.3.2)*? Or how could you strengthen the latter so that it would?*

For many G, the conjecture (5.1.5) is probably false even at odd p, for a different reason. When asymptotically counting fields by discriminant, for many G, a positive proportion of the fields contain some fixed subfield. (See [111, 119] for thorough discussion of when this happens for abelian G.) When this is the case, the class group of that fixed subfield has an outsize contribution to the entire class group average, which tends to violate the conjectures.

Exercise 5.1.14. *Let* K *be a quadratic field in which every ramified prime is* 1 *mod* 4*. Use the class field theory methods above to show that a positive proportion of* $\mathbb{Z}/4\mathbb{Z}$*-extensions, asymptotically by discriminant, contain* K*.*

Bartel and Lenstra [10] use this to show a concrete counterexample to (5.1.5) for $G = \mathbb{Z}/4\mathbb{Z}$ and f the characteristic function of having 3 divide the order of the group. Based on work in [111] and [10, Proposition 6.6], they propose replacing the absolute discriminant D_K in (5.1.5) with P_K, the product of the ramified primes in K.

Exercise 5.1.15. *Find the asymptotics of* $G = \mathbb{Z}/2\mathbb{Z}$ *and* $G = \mathbb{Z}/3\mathbb{Z}$ *fields by* P_K *instead of* D_K*.*

Exercise 5.1.16. *When* $G = \mathbb{Z}/4\mathbb{Z}$*-extensions are counted asymptotically by* P_K*, show that there does not exist a quadratic field that is a subfield of a positive proportion of the* $\mathbb{Z}/4\mathbb{Z}$*-extensions.*

Project 5.1.17. *Do computations as in Project 5.1.11 except for* $G = \mathbb{Z}/4\mathbb{Z}$*. Do some tables by* D_K *and some by* P_K*. Can you see the difference? Also try ordering fields by* P^2Q*, where* P *is the product of partially ramified primes and* Q *is the product of totally ramified primes. (For this ordering, show the analog of Exercise 5.1.16.)*

Different notions of moments

Exercise 5.1.18. *Malle* [81, 82] *computes the classical moments of the size of the* p*-torsion of a random group* X*, i.e. the average of* $|X[p]|^k$*. How is this related to our* $(\mathbb{Z}/p\mathbb{Z})^j$*-moments for a random finite abelian group? [Hint: first consider the average of* $\mathrm{Hom}(-, (\mathbb{Z}/p\mathbb{Z})^k)$*]*

A p-group R-module has an underlying abelian p-group. So when p-group R-module moments (averages of $\#\mathrm{Sur}_R(-, B)$) determine a unique distribution of p-group R-modules, they necessarily determine a unique distribution of abelian p-groups. Then (without any limits), that must uniquely determine the abelian p-group moments (averages of $\#\mathrm{Sur}(-, B)$). However, we can go more directly from p-group R-module moments to p-group moments.

Exercise 5.1.19. *If* M *is a* p*-group* R*-module, and* B *is a finite abelian* p *group, express* $\#\mathrm{Sur}(M, B)$ *in terms of* $\#\mathrm{Sur}_R(M, B_i)$ *for various* R*-modules* B_i *that only depend on* B*. Use this to relate the two kind of moments as suggested above.*

Exercise 5.1.20. *When* $G = \mathbb{Z}/\ell\mathbb{Z}$*, use the two exercises above and Theorem 5.1.9 to find the predicted (from* (5.1.5)*) average of* $|\mathrm{Cl}_K[p]|^k$ *over* G*-Extensions* K*.*

5.2. Class groups of non-Galois extensions Now we consider G a finite transitive permutation group that is not necessary simply transitive, with $H \subset G$ the stabilizer of an element. We will be considering G-Extensions, which are not necessarily Galois. We can still define S_{G,G_∞} as above.

Exercise 5.2.1. *Let* K *be a* G*-Extension, and* L *its Galois closure over* $\mathbb{Q}$*. Let* $H \subset G$ *be the stabilizer of an element. Show* $\mathrm{Gal}(L/K) \simeq H$*, as groups.*

Exercise 5.2.2. *Let* $L/\mathbb{Q}$ *be a Galois extension with Galois group* G*. Let* H *be a subgroup of* G *and* K *be the fixed field* L^H*. Show that the inclusion map*

$$\mathrm{Cl}_K \to \mathrm{Cl}_L^H$$

is an isomorphism on Sylow p*-subgroups for any* $p \nmid |H|$*. [Hint: consider to norm map* $\mathrm{Cl}_L \to \mathrm{Cl}_K$ *as well.]*

Even though Cohen and Martinet do not make a general conjecture for non-Galois extensions, for $p \nmid |G|$, (5.1.5) implies a conjecture on the distribution of $\mathrm{Cl}_{K,p}$ by pushing forward the distribution from (5.1.5) along taking H-invariants. Said another way, one can consider functions $f(A)$ that only depend on A^H in (5.1.5) and have a conjecture of the distribution of $\mathrm{Cl}_{K,p}$ for G-Extensions, with the minor caveat that (5.1.5) orders fields by the discriminant of the Galois closure and not the discriminant of the G-Extensions. (We say this is minor not because there is any clear way to go from one such average to the other, but rather because it seems there is no strong a priori reason to prefer one ordering of the fields over the other.) Explicit formulas for this pushforward are given in [110, Theorem 8.14], and they are indeed quite similar to (2.3.1), (2.3.2), (5.1.5). We will now describe some aspects of those formulas.

Absolutely irreducible permutation groups A finite permutation group G on X naturally gives an $|X|$-dimensional representation of G over $\mathbb{C}$, where G acts on the basis vectors via its action on X. The associated representation always contains one copy of the trivial representation (spanned by the sum of the basis vectors), and let V_G be the quotient of this representation by that 1-dimensional trivial representation. We say G is *absolutely irreducible* if V_G is. (The *absolutely* emphasizes that we considered the representation over $\mathbb{C}$ and not $\mathbb{Q}$).

For example, if $G = S_n$ in its usual degree n permutation representation, then G is absolutely irreducible.

Let G be an absolutely irreducible finite permutation group, p a prime not diving $|G|$, and G_∞ a subgroup of G. Let $u+1$ be the number of cycles in the action of G_∞ on the underlying set. Then we have that Cohen and Martinet's conjecture (5.1.5) implies that for "reasonable" f on the set of finite abelian p-groups, we have

$$\lim_{X\to\infty} \frac{\sum_{\substack{K\in S_{G,G_\infty}\\ D_{\tilde{K}}\leqslant X}} f(\mathrm{Cl}_K)}{\sum_{\substack{K\in S_{G,G_\infty}\\ D_{\tilde{K}}\leqslant X}} 1} = \frac{\sum_{\substack{A \text{ fin. ab.}\\ p\text{-group}}} \frac{f(A)}{|A|^u |\mathrm{Aut}(A)|}}{\sum_{\substack{A \text{ fin. ab.}\\ p\text{-group}}} \frac{1}{|A|^u |\mathrm{Aut}(A)|}}. \tag{5.2.3}$$

This implication follows from [110, Theorem 8.14, Proposition 8.16]. (In this deduction, the absolute irreducibility implies $k = 2$ and $a_{\Gamma/\Gamma'} = \phi_2$; so, $\langle \phi_2, a_\Gamma\rangle = \dim \phi_2 = \dim a_{\Gamma/\Gamma'}$ and $\langle \phi_2, a_{\Gamma/\Gamma'}\rangle = 1$ and $\langle \chi_K, \phi_2\rangle = \langle \mathrm{Ind}_{\Gamma_\infty}^{\Gamma} \mathbb{C}, \phi_2\rangle = \langle \mathbb{C}, \mathrm{Res}_{\Gamma_\infty}^{\Gamma} \phi_2\rangle = \langle \mathbb{C}, V_G\rangle_{\Gamma\infty} = u$ and $h_i = \dim a_{\Gamma/\Gamma'}$.)

We have already seen in (4.2.15) the moments of the distributions above, and we know from Theorem 4.1.7, that they determine a unique distribution.

The same caveats about avoiding $p = 2$ (because of the roots of unity in $\mathbb{Q}$) and counting by P_K instead of D_k apply to (5.2.3) as they did to (5.1.5).

Exercise 5.2.4. *Show that for $K \in S_{G,G_\infty}$ that u (the number of cycles in the action of G_∞ on the underlying set, minus 1) is the rank of the group of units of K.*

Project 5.2.5. *Do computations as in* (5.1.11) *for $G = S_3, S_4$, and/or S_5 in their standard permutation representations, for $p \nmid |G|$. Malle has done some computations for $G = S_3$ in* [81, Section 5] *and* [82, Section 5]*, and you will likely want to use Belabas's CUBIC program* [12] *for S_3. For quartic and quintic fields, you could do some computations with existing databases, or build on the suggested direction above to find new field enumeration algorithms for S_4 and S_5 fields based on Bhargava's parametrizations.*

Beyond absolutely irreducible permutation groups A takeaway from the above conjecture is that we conjecture when G is absolutely irreducible, then there is no "additional structure" on the class groups of G-Extensions (at least for Sylow p-subgroups for $p \nmid 2|G|$). However, other non-Galois G-extensions do have extra structure on their class groups.

Consider the case when $G = D_4$ in its transitive permutation representation on the four vertices of a square. If K is a G-Extension, then $\mathrm{Aut}(K) = \mathbb{Z}/2\mathbb{Z}$. Of

course, $\mathrm{Aut}(K)$ acts on Cl_K, so even though K is not Galois, Cl_K has additional structure.

However, also consider the following example from [110, Example 8.20]. Let $G = A_5$ in the transitive degree 10 action with $H = \langle (123), (12)(45) \rangle$ (as abstract groups $H \simeq S_3$).

Exercise 5.2.6. *For the G above, show that a G-extension K has no non-trivial automorphisms (e.g. by using Exercise 1.1.12).*

Yet, if K is a G-Extension, for this $G = A_5$, and p a prime > 5, then $\mathrm{Cl}_{K,p}$ is naturally a module for a ring larger than $\mathbb{Z}$. Indeed, this happens when G is not absolutely irreducible [110, Lemma 8.4,Proposition 8.16].

Let H be a subgroup of a finite group G. Let $e = \frac{1}{|H|} \sum_{h \in H} h$ be an element of the group algebra $\mathbb{Q}[G]$. We can consider the $\mathbb{Z}$-algebra $e\mathbb{Z}[G]e$. (Note $e\mathbb{Z}[G]e$ is additively and multiplicatively closed in $\mathbb{Q}[G]$ though we usually would not call it a subalgebra because it does not have the same unit.)

Exercise 5.2.7. *Show that*

$$e\mathbb{Z}[G]e \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}[H\backslash G/H],$$

where $\mathbb{Q}[H\backslash G/H]$ is the Hecke algebra of a finite group.

Exercise 5.2.8. *Let A be a finite abelian G-module of order prime to $|G|$. Show that $e\mathbb{Z}[G]e$ acts on the invariants A^H making A^H into a module for $e\mathbb{Z}[G]e$. [Hint:for $g \in G$ and $a \in A^H$, let $ege = ega$, where the action all happens in A and the $|H|^{-1}$ acts by an integer equivalent to it mod $|A|$.]*

Exercise 5.2.9. *Let L be a Galois field with Galois group G. Let K be the fixed field of H. Let p be a prime not dividing $|G|$. Where N is defined as in Section 5.1, show that $e\mathbb{Z}[G]e/Ne\mathbb{Z}[G]e$ acts on the Sylow p-subgroup of Cl_K.*

See [110, Section 8] for a more complete explanation of this $o := e\mathbb{Z}[G]e/Ne\mathbb{Z}[G]e$ action on $\mathrm{Cl}_{K,p}$, and in particular the proof that o is not $\mathbb{Z}$ when G is not absolutely irreducible [110, Proposition 8.16], and the precise formula for the push-forward of the conjectural Galois distribution on class groups from (5.1.5) along $A \mapsto A^H$, which can be given in terms of $|\mathrm{Aut}_o(B)|$ [110, Theorem 8.14].

Project 5.2.10. *Do computations for $G = D_4$ in its transitive degree 4 permutation representation, i.e. on quartic D_4 fields, as in Project 5.1.11. Order fields by discriminant, product of ramified primes, and also the Artin conductor of the 2-dimensional irreducible representation of D_4 (see [7] for asymptotic counting of D_4-extensions by this invariant). How do these different orders change the invariants? Note that a positive proportion of D_4-extensions, when counted by discriminant, include a given quadratic field (which we can see from our asymptotic count above).*

There is one further interesting feature in the non-Galois case, which is that predictions can be made for some $p \mid |G|$. See [110, Section 7-8] for further discussion of how this works, which is beyond the scope of these notes.

Previous computations [41] suggested that conjectures on the 2-Sylow subgroup of class groups of non-Galois cubic fields might be wrong, which may have been because these computations were just seeing a large secondary or true error term, or may have been an indication that the conjectures were wrong, which might be coming from the roots of unity in $\mathbb{Q}$. While Bhargava has proved one average [16] on the 2-Sylow subgroup of class groups of cubic fields, it is still quite open what the general distribution is.

Project 5.2.11. *Do computations for* $G = S_3$ *in its standard representation and* $p = 2$*, as in Project 5.1.11. Do the same for* $G = A_4$ *and/or* S_4 *and* $p = 3$*. Do the values look like they approach the values in* (5.2.3) *and moments as in* (4.2.15) *(which are the values predicted by Cohen and Martinet, even for these particular cases where* $p \mid |G|$*)?*

Project 5.2.12. *Do computations for* $G = A_5$ *and/or* S_5 *in its standard representation and* $p = 3$*, as in Project 5.1.11. Do the same for* $G = A_4$ *and/or* S_4 *and* $p = 3$*. In these cases, the conjectures of Cohen and Martinet make no prediction. Can you guess a pattern from the empirical values?*

5.3. Generalizations and known results There are of course more generalizations of the questions of class group distribution. We do not attempt to give a complete literature review, but give pointers to examples of recent work if various directions. One can replace the base field $\mathbb{Q}$ with another number field K_0, or even a global field such as a finite extension of $\mathbb{F}_q(t)$. For $G = \mathbb{Z}/p\mathbb{Z}$ for a prime p, Gerth [58,59] has extended the conjectures to include conjectures on the Sylow p-subgroup.

Even within the scope of all these generalizations, there are few known class group averages. Datskovsky and Wright [44] found the average of $\mathrm{Sur}(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z})$ over quadratic extensions of a general global field of characteristic not 2 or 3. Bhargava [16] found the average of $\mathrm{Sur}(\mathrm{Cl}_K, \mathbb{Z}/2\mathbb{Z})$ over imaginary, respectively real, non-Galois cubic fields K. The work of Bhargava, Shankar, and Wang [23] address the analog of this average over general global fields. For G any transitive permutation 2-group containing a transposition, Lemke Oliver, Wang, and the author [89] found the average of $\mathrm{Sur}(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z})$ over G-extensions K/K_0 for any base number field K_0. We also find the $\mathbb{Z}/3\mathbb{Z}$-moments of certain relative class groups of these G-extensions. The method in [89] can be used to give these averages for many other G of the form $\mathbb{Z}/2\mathbb{Z} \wr H$, see [89, Section 8]. When $G = \mathbb{Z}/4\mathbb{Z}$ and f is bounded and only depends on the class group of the quadratic subfield of the cyclic quartic of a quartic G-extension K, Bartel and Lenstra [10] showed that the average of $f(\mathrm{Cl}_K)$ over G-extensions K is computable in finite time to arbitrary precision. These are the known averages on the part of the class group of order prime to the degree of the extensions being averaged over. However, Alex Smith [98,99] has groundbreaking work that has proven the entirety of Gerth's conjecture on the distribution of $2\,\mathrm{Cl}_{K,2} = \mathrm{Cl}_{K,2} / \mathrm{Cl}_K[2]$ for quadratic fields, as well as

Gerth's analogous conjecture on $\mathrm{Cl}_{K,p}$ over cyclic p-extension K, improving earlier results [51,70]. When the base field is $\mathbb{F}_q(t)$ and one introduces an additional limit $q \to \infty$ into the question, there are many results [1,2,50,76,115] and recently these function field theorems have played a large role in guiding conjectures in the area.

One can also ask about refinements of class groups, such as ray class groups [34, 47, 105] or Arakelov class groups [10], or pointed groups that specify the element in the class group corresponding to certain ideals [115]. One can restrict the fields averaged over by imposing local conditions at finite primes [27,28,105, 115], or enlarge to consider class groups of non-maximal orders [27, 28]. One can also impose global conditions on the fields [20, 63, 96, 97, 100, 112], such as requiring their ring of integers be be generated by a single element (as an $\mathbb{Z}$-algebra). When one cannot obtain exact asymptotics for moments of class group distributions, one may ask for upper bounds [8,49,54,60,88,91,102].

5.4. Unramified extensions Most of the above mentioned results access Cl_K through class field theory as $\mathrm{Gal}(K^{un,ab}/K)$, the Galois group of the maximal unramified, abelian extension of K. The averages are proven by counting unramified extensions. From this point of view, it is natural to ask more generally about the distribution of the non-abelian (profinite) groups $\mathrm{Gal}(K^{un}/K)$, where K^{un} is the maximal unramified extension of K. As in the abelian case, we have moments, now indexed by finite groups G, and the Gth moment is the average of $\#\mathrm{Sur}(-, G)$, where Sur denotes continuous surjections. The Gth moment of $\mathrm{Gal}(K^{un}/K)$, as K ranges uniformly over a family of number fields, is then $|\mathrm{Aut}(G)|$ times the average number of unramified G-extensions of K (by Galois theory).

Liu, Zureick-Brown, and the author [76, Conjecture 1.3] have given conjectures on the distribution of the part of $\mathrm{Gal}(K^{un}/K)$ prime to $2|\Gamma|$ (as K ranges over totally real Γ-extensions), and in particular on the Gth moment for any finite group G of order relatively prime to $2|\Gamma|$. These conjectures generalize the conjecture of Boston, Bush, and Hajir [31–33] on the maximal pro-p quotient of $\mathrm{Gal}(K^{un}/K)$ (the p-class tower group) as K ranges over quadratic fields. The conjectures of Boston, Bush, and Hajir were based on extensive computation and numerical evidence in the number field case. The general conjectures of [76] are based on theoretical reasoning about the presentation of $\mathrm{Gal}(K^{un}/K)$ and on $q \to \infty$ theorems in the function field case. It would be very interesting the have more empirical evidence in the number field case, in particular on whether the moments are approaching their predicted values. See [76, Section 1.5] for a detailed discussion of the most interesting and accessible moments that would make useful computational projects to explore experimentally. See also [116] for conjectures on G-moments of $\mathrm{Gal}(K^{un}/K)$ as K ranges over quadratic fields and $|G|$ has *even* order. These conjectures are based on function field $q \to \infty$ theorems, but the paper includes an appendix in which computations are done to give empirical number field evidence. Boston and Bush [30] also have significant computations

on the maximal pro-2 quotient of $\mathrm{Gal}(K^{un}/K)$ as K ranges over cyclic cubic fields, which is beyond the scope of the conjectures of [76].

References

[1] J. D. Achter, *The distribution of class groups of function fields*, Journal of Pure and Applied Algebra **204** (February 2006), no. 2, 316–333. ←32, 38

[2] J. D. Achter, *Results of Cohen-Lenstra type for quadratic function fields*, Computational arithmetic geometry, 2008, pp. 1–7. MR2459984 ←38

[3] M. Adam and G. Malle, *A class group heuristic based on the distribution of 1-eigenspaces in matrix groups*, Journal of Number Theory **149** (April 2015), 225–235. ←32

[4] B. Alberts, *The weak form of Malle's conjecture and solvable groups*, Research in Number Theory **6** (January 2020), no. 1, 10. ←14

[5] B. Alberts, *Statistics of the First Galois Cohomology Group: A Refinement of Malle's Conjecture*, Algebra & Number Theory **15** (December 2021), no. 10, 2513–2569, available at 1907.06289. ←14

[6] B. Alberts and E. O'Dorney, *Harmonic analysis and statistics of the first Galois cohomology group*, Research in the Mathematical Sciences **8** (August 2021), no. 3, 50. ←14

[7] S. A. Altug, A. Shankar, I. Varma, and K. H. Wilson, *The number of D_4-fields ordered by conductor*, Journal of the European Mathematical Society **23** (May 2021), no. 8, 2733–2785. ←14, 36

[8] C. An, *$\ell $-torsion in class groups of certain families of D_4-quartic fields*, Journal de Théorie des Nombres de Bordeaux **32** (2020), no. 1, 1–23. ←38

[9] T. C. Anderson, A. Gafni, K. Hughes, R. J. L. Oliver, D. Lowry-Duda, F. Thorne, J. Wang, and R. Zhang, *Improved bounds on number fields of small degree*, arXiv, 2022. ←14

[10] A. Bartel and H. W. Lenstra, *On class groups of random number fields*, Proceedings of the London Mathematical Society **121** (2020), no. 4, 927–953, available at 1803.06903. ←18, 33, 37, 38

[11] K. Belabas, *A fast algorithm to compute cubic fields*, Mathematics of Computation of the American Mathematical Society **66** (1997), no. 219, 1213–1237. ←10, 13

[12] K. Belabas, *Cubic*, Accessed July 24, 2022. ←35

[13] K. Belabas, M. Bhargava, and C. Pomerance, *Error estimates for the Davenport-Heilbronn theorems*, Duke Mathematical Journal **153** (May 2010), no. 1, 173–210. ←13

[14] K. Belabas and É. Fouvry, *Discriminants cubiques et progressions arithmétiques*, International Journal of Number Theory **6** (2010), no. 7, 1491–1529. ←9

[15] M. Bhargava, *Higher composition laws III: The parametrization of quartic rings*, Annals of Mathematics **159** (May 2004), no. 3, 1329–1360. ←9, 10

[16] M. Bhargava, *The density of discriminants of quartic rings and fields*, Annals of Mathematics **162** (September 2005), no. 2, 1031–1063. ←4, 7, 9, 37

[17] M. Bhargava, *Higher composition laws IV: The parametrization of quintic rings*, Annals of Mathematics **167** (January 2008), no. 1, 53–94. ←9, 10

[18] M. Bhargava, *The density of discriminants of quintic rings and fields*, Annals of Mathematics **172** (October 2010), no. 3, 1559–1591. ←4, 9

[19] M. Bhargava, *Galois groups of random integer polynomials and van der Waerden's Conjecture*, arXiv, 2021. ←7

[20] M. Bhargava, J. Hanke, and A. Shankar, *The mean number of 2-torsion elements in the class groups of n-monogenized cubic fields* (October 2020). ←38

[21] M. Bhargava, D. M. Kane, H. W. Lenstra Jr., B. Poonen, and E. Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, Cambridge Journal of Mathematics **3** (2015), no. 3, 275–321. MR3393023 ←18

[22] M. Bhargava, A. Shankar, and J. Tsimerman, *On the Davenport–Heilbronn theorems and second order terms*, Inventiones mathematicae **193** (August 2013), no. 2, 439–499. ←10, 14, 19

[23] M. Bhargava, A. Shankar, and X. Wang, *Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces*, arXiv:1512.03035 [math] (December 2015), available at 1512.03035. ←13, 14, 37

[24] M. Bhargava, A. Shankar, and X. Wang, *An improvement on Schmidt's bound on the number of number fields of bounded discriminant and small degree* (April 2022). ←14

[25] M. Bhargava, A. Shankar, and X. Wang, *Squarefree values of polynomial discriminants II* (July 2022). ←14

[26] M. Bhargava, T. Taniguchi, and F. Thorne, *Improved error estimates for the Davenport-Heilbronn theorems*, arXiv:2107.12819 [math] (July 2021), available at 2107.12819. ←14, 19

[27] M. Bhargava and I. Varma, *On the mean number of 2-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields*, Duke Mathematical Journal **164** (2015), no. 10, 1911–1933. MR3369305 ←38

[28] M. Bhargava and I. Varma, *The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders*, Proceedings of the London Mathematical Society **112** (March 2016), no. 2, 235–266. ←38

[29] M. Bhargava and M. M. Wood, *The density of discriminants of S_3-sextic number fields*, Proceedings of the American Mathematical Society **136** (2008), no. 5, 1581–1587. ←9

[30] N. Boston and M. R. Bush, *Heuristics for 2-class Towers of Cyclic Cubic Fields*, Experimental Mathematics **0** (December 2021), no. 0, 1–12. ←38

[31] N. Boston, M. R. Bush, and F. Hajir, *Heuristics for p-class towers of imaginary quadratic fields*, Mathematische Annalen **368** (2017), no. 1-2, 633–669. MR3651585 ←38

[32] N. Boston, M. R. Bush, and F. Hajir, *Heuristics for p-class towers of real quadratic fields*, Journal of the Institute of Mathematics of Jussieu. JIMJ. Journal de l'Institut de Mathématiques de Jussieu **20** (2021), no. 4, 1429–1452, available at 1803.04047. MR4293801 ←38

[33] N. Boston and M. M. Wood, *Non-abelian Cohen–Lenstra heuristics over function fields*, Compositio Mathematica **153** (July 2017), no. 7, 1372–1390. ←38

[34] B. Breen, I. Varma, J. Voight, and a. w. N. Elkies, *On unit signatures and narrow class groups of odd degree abelian number fields*, arXiv, 2021. ←38

[35] J. Clancy, N. Kaplan, T. Leake, S. Payne, and M. M. Wood, *On a Cohen–Lenstra heuristic for Jacobians of random graphs*, Journal of Algebraic Combinatorics (May 2015), 1–23. ←25

[36] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR1728313 ←6, 10

[37] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Constructing complete tables of quartic fields using Kummer theory*, Mathematics of Computation **72** (June 2002), no. 242, 941–951. ←10

[38] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Enumerating quartic dihedral extensions of $\Bbb Q$*, Compositio Mathematica **133** (2002), no. 1, 65–93. ←4, 7

[39] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), 1984, pp. 33–62. ←15, 29, 30

[40] H. Cohen and J. Martinet, *étude heuristique des groupes de classes des corps de nombres*, Journal für die Reine und Angewandte Mathematik **404** (1990), 39–76. ←30, 31

[41] H. Cohen and J. Martinet, *Heuristics on class groups: Some good primes are not too good*, Mathematics of Computation **63** (1994), no. 207, 329–334. ←37

[42] H. Cohn, *The density of abelian cubic fields*, Proceedings of the American Mathematical Society **5** (1954), 476–477. ←6, 7

[43] J.-M. Couveignes, *Enumerating number fields*, Annals of Mathematics **192** (September 2020), no. 2, 487–497. ←14

[44] B. Datskovsky and D. J. Wright, *Density of discriminants of cubic extensions*, Journal für die Reine und Angewandte Mathematik **386** (1988), 116–138. MR936994 ←37

[45] 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** (1971), no. 1551, 405–420. ←4, 6, 27, 28

[46] 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. ←9

[47] D. S. Dummit and J. Voight, *The 2-Selmer group of a number field and heuristics for narrow class groups and signature ranks of units*, Proceedings of the London Mathematical Society. Third Series **117** (2018), no. 4, 682–726. MR3873132 ←38

[48] E. P. Dummit, *Counting G-extensions by discriminant*, Mathematical Research Letters **25** (July 2018), no. 4, 1151–1172. ←14

[49] J. Ellenberg, L. Pierce, and M. Wood, *On l-torsion in class groups of number fields*, Algebra & Number Theory **11** (October 2017), no. 8, 1739–1778. ←38

[50] J. S. Ellenberg, A. Venkatesh, and C. Westerland, *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields*, Annals of Mathematics. Second Series **183** (2016), no. 3, 729–786. MR3488737 ←32, 38

[51] É. Fouvry and J. Klüners, *On the 4-rank of class groups of quadratic number fields*, Inventiones mathematicae **167** (November 2006), no. 3, 455–513. ←38

[52] É. Fouvry and P. Koymans, *Malle's conjecture for nonic Heisenberg extensions*, arXiv:2102.09465 [math] (February 2021), available at 2102.09465. ←13

[53] C. Frei, D. Loughran, and R. Newton, *The Hasse norm principle for abelian extensions*, arXiv:1508.02518 [math] (August 2015), available at 1508.02518. ←7, 13, 14

[54] C. Frei and M. Widmer, *Averages and higher moments for the $$\ell $$-torsion in class groups*, Mathematische Annalen **379** (April 2021), no. 3, 1205–1229. ←38

[55] E. Friedman and L. C. Washington, *On the distribution of divisor class groups of curves over a finite field*, Théorie des nombres (Quebec, PQ, 1987), 1989, pp. 227–239. MR1024565 ←21, 22

[56] W. T. Gan, B. Gross, and G. Savin, *Fourier coefficients of modular forms on G_2*, Duke Mathematical Journal **115** (2002), no. 1, 105–169. ←9

[57] D. Garton, *Random matrices, the Cohen–Lenstra heuristics, and roots of unity*, Algebra & Number Theory **9** (February 2015), no. 1, 149–171. ←32

[58] F. Gerth III, *Densities for ranks of certain parts of p-class groups*, Proceedings of the American Mathematical Society **99** (1987), no. 1, 1–8. ←37

[59] F. Gerth III, *Extension of conjectures of Cohen and Lenstra*, Expositiones Mathematicae. International Journal for Pure and Applied Mathematics **5** (1987), no. 2, 181–184. ←37

[60] D. R. Heath-Brown and L. B. Pierce, *Averages and moments associated to class numbers of imaginary quadratic fields*, Compositio Mathematica **153** (November 2017), no. 11, 2287–2309, available at 1409.3177. ←38

[61] H. Heilbronn, *On the class-number in imaginary quadratic fields*, The Quarterly Journal of Mathematics **os-5** (1934), no. 1, 150–160. ←15

[62] W. Ho and A. Shankar, *Problem set for 2014 arizona winter school*, 2014. [Online; accessed 21 July 2022]. ←10

[63] W. Ho, A. Shankar, and I. Varma, *Odd degree number fields with odd class number*, Duke Mathematical Journal **167** (April 2018), no. 5, 995–1047, available at 1603.06269. ←38

[64] J. W. Jones and D. P. Roberts, *A database of number fields*, LMS Journal of Computation and Mathematics **17** (2014/ed), no. 1, 595–618. ←6

[65] J. Klüners, *Ueber die Berechnung von Automorphismen und Teilkörpern algebraischer Zahlkörper*, Ph.D. Thesis, Berlin, 1997. ←

[66] J. Klüners, *A counterexample to Malle's conjecture on the asymptotics of discriminants*, Comptes Rendus Mathématique. Académie des Sciences. Paris **340** (2005), no. 6, 411–414. MR2135320 ←13

[67] J. Klüners, *Asymptotics of number fields and the Cohen–Lenstra heuristics*, Journal de Théorie des Nombres de Bordeaux **18** (2006), no. 3, 607–615. ←27

[68] J. Klüners, *The distribution of number fields with wreath products as Galois groups*, International Journal of Number Theory **8** (2012), no. 3, 845–858. MR2904935 ←11

[69] J. Klüners and G. Malle, *Counting nilpotent Galois extensions*, Journal für die Reine und Angewandte Mathematik **572** (2004), 1–26. MR2076117 ←14

[70] J. Klys, *The distribution of p-torsion in degree p cyclic fields*, Algebra & Number Theory **14** (June 2020), no. 4, 815–854, available at 1610.00226. ←38

[71] P. Koymans and C. Pagano, *On Malle's conjecture for nilpotent groups, I*, arXiv:2103.17223 [math] (March 2021), available at 2103.17223. ←13, 14

[72] A. Landesman, R. J. Lemke Oliver, and F. Thorne, *Improved lower bounds for the number of fields with alternating Galois group*, Bulletin of the London Mathematical Society **53** (2021), no. 4, 1159–1173. ←14

[73] M. Lipnowski, W. Sawin, and J. Tsimerman, *Cohen-Lenstra heuristics and bilinear pairings in the presence of roots of unity*, arXiv:2007.12533 [math] (July 2020), available at 2007.12533. ←32

[74] Y. Liu, *Non-abelian Cohen–Lenstra Heuristics in the presence of roots of unity*, arXiv, 2022. ←32

[75] Y. Liu and M. M. Wood, *The free group on n generators modulo n + u random relations as n goes to infinity*, Journal für die reine und angewandte Mathematik **2020** (May 2020), no. 762, 123–166, available at 1708.08509. ←21

[76] Y. Liu, M. M. Wood, and D. Zureick-Brown, *A predicted distribution for Galois groups of maximal unramified extensions*, arXiv:1907.05002 [math] (July 2019), available at 1907.05002. ←38, 39

[77] T. LMFDB Collaboration, *The L-functions and modular forms database*, 2022. [Online; accessed 21 July 2022]. ←6, 15
[78] S. Mäki, *On the density of abelian number fields*, Annales Academiae Scientiarum Fennicae. Series A I. Mathematica Dissertationes **54** (1985), 104. ←7
[79] G. Malle, *On the distribution of Galois groups*, Journal of Number Theory **92** (2002), no. 2, 315–329. ←13
[80] G. Malle, *On the distribution of Galois groups. II*, Experimental Mathematics **13** (2004), no. 2, 129–135. MR2068887 ←13
[81] G. Malle, *Cohen–Lenstra heuristic and roots of unity*, Journal of Number Theory **128** (October 2008), no. 10, 2823–2835. ←26, 32, 34, 35
[82] G. Malle, *On the Distribution of Class Groups of Number Fields*, Experimental Mathematics **19** (2010), no. 4, 465–474. ←32, 34, 35
[83] A. Mosunov and Jacobson, *Unconditional class group tabulation of imaginary quadratic fields to* $|\Delta| < 2^{40}$, Mathematics of Computation **85** (2016), no. 300, 1983–2009. ←15
[84] W. Narkiewicz, *Number theory*, World Scientific Publishing Co., Singapore, 1983. ←8
[85] J. Neukirch, *Algebraic number theory*, Grundlehren Der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. ←2, 8, 28
[86] H. H. Nguyen and M. M. Wood, *Random integral matrices: Universality of surjectivity and the cokernel*, Inventiones mathematicae (October 2021), available at 1806.00596. ←23
[87] R. J. L. Oliver and F. Thorne, *Upper bounds on number fields of given degree and bounded discriminant*, arXiv, 2020. ←14
[88] R. J. L. Oliver, J. Thorner, and A. Zaman, *An approximate form of Artin's holomorphy conjecture and non-vanishing of Artin L-functions*, arXiv:2012.14422 [math] (May 2021), available at 2012.14422. ←38
[89] R. J. L. Oliver, J. Wang, and M. M. Wood, *The average size of 3-torsion in class groups of 2-extensions*, arXiv, 2021. ←37
[90] L. B. Pierce, C. L. Turnage-Butterbaugh, and M. Matchett Wood, *On a conjecture for ℓ-torsion in class groups of number fields: From the perspective of moments*, Mathematical Research Letters **28** (March 2021), no. 2, 575–621, available at 1902.02008. ←27
[91] L. B. Pierce, C. L. Turnage-Butterbaugh, and M. M. Wood, *An effective Chebotarev density theorem for families of number fields, with an application to $$\ell $$-torsion in class groups*, Inventiones mathematicae **219** (February 2020), no. 2, 701–778, available at 1709.09637. ←38
[92] D. Roberts, *Density of cubic field discriminants*, Mathematics of Computation **70** (2001), no. 236, 1699–1705. ←13, 19
[93] A. Shankar and F. Thorne, *On the asymptotics of cubic fields ordered by general invariants*, arXiv, 2022. ←14
[94] A. Shankar and J. Tsimerman, *Counting S5-fields with a power saving error term*, Forum of Mathematics, Sigma **2** (2014), null–null. ←13
[95] A. Shankar and J. Tsimerman, *Heuristics for the asymptotics of the number of S_n-number fields*, arXiv, 2020. ←6
[96] A. Siad, *Monogenic fields with odd class number Part I: Odd degree* (November 2020). ←38
[97] A. Siad, *Monogenic fields with odd class number Part II: Even degree* (November 2020). ←38
[98] A. Smith, *The distribution of fixed point Selmer groups in twist families* (July 2022). ←37
[99] A. Smith, *The distribution of $\ell\^infty$-Selmer groups in degree ℓ twist families* (July 2022). ←37
[100] A. Swaminathan, *Average 2-Torsion in Class Groups of Rings Associated to Binary n-ic Forms*, arXiv, 2021. ←38
[101] T. Taniguchi and F. Thorne, *Secondary terms in counting functions for cubic fields*, Duke Mathematical Journal **162** (October 2013), no. 13, 2451–2508. ←14, 19
[102] J. Thorner and A. Zaman, *A Zero Density Estimate for Dedekind Zeta Functions*, International Mathematics Research Notices (March 2022), rnac015, available at 1909.01338. ←38
[103] S. Türkelli, *Connected components of Hurwitz schemes and Malle's conjecture*, Journal of Number Theory **155** (October 2015), 163–201. ←13
[104] B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatshefte für Mathematik und Physik **43** (December 1936), no. 1, 133–147. ←7

[105] I. Varma, *The mean number of 3-torsion elements in ray class groups of quadratic fields*, arXiv, 2021. ←38

[106] A. Venkatesh and J. S. Ellenberg, *Statistics of number fields and function fields*, Proceedings of the International Congress of Mathematicians. Volume II, 2010, pp. 383–402. MR2827801 ←14, 20

[107] J. Voight, *Enumeration of Totally Real Number Fields of Bounded Root Discriminant*, Algorithmic Number Theory, 2008, pp. 268–281. ←6

[108] J. Wang, *Secondary Term of Asymptotic Distribution of $S_3\times A$ Extensions over $\mathbb{Q}$*, arXiv, 2017. ←14

[109] J. Wang, *Malle's conjecture for Sn x A for n=3,4,5*, Compositio Mathematica **157** (January 2021), no. 1, 83–121. ←11

[110] W. Wang and M. M. Wood, *Moments and interpretations of the Cohen–Lenstra–Martinet heuristics*, Commentarii Mathematici Helvetici **96** (June 2021), no. 2, 339–387, available at 1907.11201. ←19, 26, 30, 31, 32, 34, 35, 36

[111] M. M. Wood, *On the probabilities of local behaviors in abelian field extensions*, Compositio Mathematica **146** (2010), no. 1, 102–128. ←13, 14, 33

[112] M. M. Wood, *Parametrization of ideal classes in rings associated to binary forms*, Journal für die reine und angewandte Mathematik (Crelles Journal) **2014** (April 2014), no. 689, 169–199. ←38

[113] M. M. Wood, *Asymptotics for number fields and class groups*, Directions in Number Theory: Proceedings of the 2014 WIN3 Workshop, July 2016. ←9, 10, 13, 19, 27

[114] M. M. Wood, *The distribution of sandpile groups of random graphs*, Journal of the American Mathematical Society **30** (2017), no. 4, 915–958. ←25, 26

[115] M. M. Wood, *Cohen-Lenstra heuristics and local conditions*, Research in Number Theory **4** (September 2018), no. 4, 41. ←26, 38

[116] M. M. Wood, *Nonabelian Cohen–Lenstra moments*, Duke Mathematical Journal **168** (February 2019), no. 3, 377–427, available at 1702.04644. ←26, 38

[117] M. M. Wood, *Random integral matrices and the Cohen-Lenstra heuristics*, American Journal of Mathematics **141** (2019), no. 2, 383–398, available at 1504.04391. MR3928040 ←23, 24, 29

[118] M. M. Wood, *Probability theory for random groups arising in number theory* (2022). ICM lecture notes, available at https://people.math.harvard.edu/ mmwood/Publications/. ←24, 25, 26

[119] D. J. Wright, *Distribution of discriminants of abelian extensions*, Proceedings of the London Mathematical Society. Third Series **58** (1989), no. 1, 17–50. ←14, 33

Department of Mathematics, Harvard University, Science Center Room 325, 1 Oxford Street, Cambridge, MA 02138 USA

Email address: mmwood@math.harvard.edu