The average size of 3-torsion in class groups of 2-extensions

Robert J. Lemke Oliver, Jiuya Wang, Melanie Matchett Wood

October 15, 2021

Abstract

We determine the average size of the 3-torsion in class groups of G-extensions of a number field when G is any transitive 2-group containing a transposition, for example D_4. It follows from the Cohen–Lenstra–Martinet heuristics that the average size of the p-torsion in class groups of G-extensions of a number field is conjecturally finite for any G and most p (including $p \nmid |G|$). Previously this conjecture had only been proven in the cases of $G = S_2$ with $p = 3$ and $G = S_3$ with $p = 2$. We also show that the average 3-torsion in a certain relative class group for these G-extensions is as predicted by Cohen and Martinet, proving new cases of the Cohen–Lenstra–Martinet heuristics. Our new method also works for many other permutation groups G that are not 2-groups.

1 Introduction

Cohen, Lenstra, and Martinet [CL84, CM90] have given heuristics on the distribution of class groups of number fields that lead to the following conjecture. For a number field k, a transitive permutation group G, and a prime $p \nmid |G|$, there conjecturally exists a constant $c_{k,G,p} > 0$ such that

$$\lim_{X \to \infty} \frac{1}{|E_k(G,X)|} \sum_{K \in E_k(G,X)} |\operatorname{Cl}_K[p]| \overset{\text{Conj.}}{=} c_{k,G,p}, \tag{1.1}$$

where $E_k(G,X)$ is the set of extensions K/k with Galois closure group G (that is, the Galois group of the normal closure; see Section 1.5) and $\operatorname{Disc}(K) \leq X$. The limiting average in (1.1) was previously known for only two cases of G and p: for $G = S_2$ and $p = 3$ by Davenport and Heilbronn [DH71] when $k = \mathbb{Q}$ and Datskovsky and Wright [DW88] for general k, and for $G = S_3$ and $p = 2$ by Bhargava [Bha05] when $k = \mathbb{Q}$ (see also the work of Bhargava, Shankar, and Wang [BSW15] for the case of general k). This conjecture is particularly notable in light of the fact that the best general upper bound on $|\operatorname{Cl}(K)[p]|$ is $\operatorname{Disc}(K)^{1/2+\epsilon}$, and there has been a lot of recent breakthrough work (e.g. [HP17, PTBW20]) even to show that the average in (1.1) is bounded by $X^{1/2-\delta}$ for some $\delta > 0$, for certain G, despite the fact that it is conjectured to have constant limit.

Our first main result is that we find the average and prove the conjecture in (1.1) when G is any transitive 2-group containing a transposition and $p = 3$.

Theorem 1.1. *For any m, let $G \subset S_{2^m}$ be a transitive permutation 2-group containing a transposition. For any number field k, there exists a constant $c_{k,G,3}$ (given explicitly in Section 6) such that*

$$\lim_{X \to \infty} \frac{1}{|E_k(G,X)|} \sum_{K \in E_k(G,X)} |\operatorname{Cl}_K[3]| = c_{k,G,3}.$$

The simplest new example that Theorem 1.1 provides is that the average size of 3-torsion in the class groups of D_4-quartic fields over k tends to a constant; when $k = \mathbb{Q}$, this constant works out to be around 1.42. It applies also to three permutation groups G of degree 8, to 26 groups of degree 16, and to at least as many groups in degree 2^m as in degree 2^{m-1}.

The restriction that G has a transposition is necessary for our proof, and is a natural condition in this setting. In particular, it is expected (for example, according to Malle's conjecture [Mal04]) that the groups G

1

arising with positive density as Galois groups when fields of degree n are ordered by discriminant are precisely those with a transposition in their degree n permutation representation. This is known for $n = 4$ where there are $\sim c_1 X$ quartic D_4 fields [CyDO02] and $\sim c_2 X$ quartic S_4 fields [Bha05] of absolute discriminant bounded by X for certain constants $c_1, c_2 > 0$, and $O_\epsilon(X^{1/2+\epsilon})$ quartic fields with any other Galois closure group. Thus, the 2-groups to which Theorem 1.1 applies—or, indeed, the groups susceptible to our method as a whole—are those expected to have positive density within the set of all fields of a given degree, which you might think of as "generic" Galois groups.

When G is a transitive permutation 2-group with a transposition and $K \in E_k(G, X)$, then K has a unique index two subfield F, and we can also ask about the relative class group of K/F. Indeed for $G = D_4$ Cohen and Martinet [CM87] have said this part of Cl_K is of particular interest. Our next main result gives the averages of $|\mathrm{Cl}_{K/F}[3]| = |\mathrm{Cl}_K[3]|/|\mathrm{Cl}_F[3]|$.

Theorem 1.2. *For any m, let $G \subset S_{2^m}$ be a transitive permutation 2-group containing a transposition. Let k be a number field, u be an integer, and $E_k^u(G, X)$ be those extensions $K \in E_k(G, X)$ such that $\mathrm{rk}\, \mathcal{O}_K^* - \mathrm{rk}\, \mathcal{O}_{F_K}^* = u$, where F_K is the unique extension of k such that $[K : F_K] = 2$. Then, if $E_k^u(G, \infty)$ is non-empty,*

$$\lim_{X \to \infty} \frac{1}{|E_k^u(G, X)|} \sum_{K \in E_k^u(G, X)} |\mathrm{Cl}_{K/F_K}[3]| = 1 + 3^{-u},$$

and this particular average value is predicted by the Cohen–Lenstra–Martinet heuristics.

Cohen, Lenstra, and Martinet actually gave heuristics for predicting the average of $f(\mathrm{Cl}_K)$ over G-extensions K/k for any function f not depending on certain "bad" Sylow subgroups of the class group. The only of these non-trivial averages previously known were in the two cases when $f(\mathrm{Cl}_K) = |\mathrm{Cl}_K[p]|$ given above. Theorem 1.2 thus gives the first average of a function other than $|\mathrm{Cl}_K[p]|$ (or trivial variations), and does this for infinitely many groups G. (There have also been some averages proven on the "bad" part of the class group including work of Fouvry and Klüners [FK06] and Klys [Kly20], as well as the recent groundbreaking work of Smith [Smi17] determining the entire distribution of $\mathrm{Cl}_K[2^\infty]$ when $G = S_2$.)

1.1 Methods

The condition that G contains a transposition implies that $G = C_2 \wr H$ for some H. So, for the extensions K/k we consider, K has a unique index two subfield F, and the overarching strategy of the paper is to average and then sum over each F. Accordingly, the work of Datskovsky and Wright on the average of $|\mathrm{Cl}_K[3]|$ over quadratic extensions of a fixed F is a key input into our work. If we could use just the main term of the average in place of the average, the argument would be essentially straightforward. However, summing the error terms over F in a straightforward way leads to error that is larger than the main term.

The major obstacle we overcome in this paper is proving a sufficiently good tail bound so that we can sum over F. In particular, the challenge is to bound the contribution when the average is taken over a relatively small interval, given $\mathrm{Disc}(F)$. Our first tool to do this is a heavily optimized upper bound on the average 3-class number of quadratic extensions of a number field F, and the closely related number of S_3 extensions of F. For very small or very large intervals, compared to $\mathrm{Disc}(F)$, we use class field theory and the theory of the Shintani zeta function counting cubic orders due to Datskovsky and Wright [DW88], respectively. While cubic extensions of a general number field are counted in [DW88], in order to sum over different base fields, we must determine the explicit dependence of the count on the base field, which has not been done in previous work.

For intermediate intervals, however — summing $|\mathrm{Cl}(K)[3]|$ for roughly $\mathrm{Disc}(K) \in [\mathrm{Disc}(F)^{3.1}, \mathrm{Disc}(F)^6]$ — we require a new technique, which we call propagation of orders. In this range, the bound on cubic extensions given by the Shintani zeta function is too large. However, the Shintani zeta function we use counts non-maximal orders as well as maximal orders. Given a maximal order, one can prove a lower bound on the number of non-maximal orders inside it, up to a certain discriminant bound. Then, to count maximal orders of discriminant up to X, we count all orders of discriminant up to Z for some $Z > X$, and then account for the known overcounting. As Z gets larger the total count goes up but the known overcounting also improves, and it turns out in the intermediate range these trade-offs work out to give us an improved and sufficiently good bound.

With these optimized bounds on S_3 extensions of a single F, especially in shorter intervals, we begin to take the sum over F, and we can bound the sum as required except in one problematic range, which we call the critical range. In this range, $\mathrm{Disc}(K) \approx \mathrm{Disc}(F)^3$. If $\mathrm{Disc}(K)$ is a power smaller or larger than this, then the methods above are sufficient. In the critical range, the best individual bounds we can prove on S_3 extensions of F use class field theory and a trivial bound for $|\mathrm{Cl}_{K/F}[3]|$, and are too large when summed. Ellenberg and Venkatesh [EV07] have shown that one can improve the trivial bound when K has enough small split primes. Ellenberg, Pierce, and the third author [EPW17] introduced the idea that in many situations, one can prove that most fields in a family have enough small split primes to apply [EV07]. We use that approach, though there is one significant new aspect. As we sum $|\mathrm{Cl}_K[3]| = |\mathrm{Cl}_F[3]||\mathrm{Cl}_{K/F}[3]|$ over F, we require significant savings over the trivial bound. We structure our proof as an induction, which allows us to assume an optimal (constant average) bound for the $|\mathrm{Cl}_F[3]|$ factor. We then further need a non-trivial bound on the relative class number $|\mathrm{Cl}_{K/F}[3]| = |\mathrm{Cl}_K[3]|/|\mathrm{Cl}_F[3]|$. For this, we develop a relative version of the widely-used lemma of Ellenberg and Venkatesh [EV07], using the relative Arakelov class group to show that one obtains a non-trivial bound on $|\mathrm{Cl}_{K/F}[p]|$ when there are sufficiently many small split primes in K/F. To find that most fields have small split primes, we use a uniform zero density estimate for Hecke L-functions as in [Pas17, Proposition A.2] or [TZ21, Theorem 1.2] to show that most of the Dedekind zeta functions do not have zeros in the relevant region.

Our methods apply more broadly than just to 2-groups. We determine in Section 8 the average size of 3-torsion in the class group of $(C_2 \wr G)$-extensions for many general classes of group G, where $C_2 \wr G$ denotes the wreath product.

1.2 Previous Work

There is a large body of previous work in arithmetic statistics and analytic number theory on the questions that arise in the this paper. There have been many remarkable achievements on counting cubic extensions, and relatedly averaging three torsion in class groups over quadratic extensions, after the work of Davenport and Heilbronn [DH71] and Datskovsky and Wright [DW88] discussed above. Taniguchi and Thorne [TT13] and Bhargava, Shankar, and Tsimerman [BST13] improved the error term in Davenport and Heilbronn's count so far as to uncover a secondary term, and recent work by Bhargava, Taniguchi, and Thorne [BTT21] has improved the error term even further. Bhargava, Shankar, and Wang [BSW15] have given a geometry of numbers proof of the counting results of Datskovsky and Wright, opening the door to further applications. See also Thorne's exposition [Tho11] of the different approaches that have been used to count cubic fields.

The problem of proving non-trivial bounds for $|\mathrm{Cl}_K[p]|$ has also been the topic of many important works. Pierce, Helfgott, and Venkatesh [Pie05, HV06, Pie06] proved the first non-trivial bounds (at a prime p not dividing the order of the Galois group), breaking the trivial bound in the case that K is quadratic field and $p = 3$. This bound was improved by Ellenberg and Venkatesh [EV07] to $|\mathrm{Cl}_K[3]| = O_\epsilon(\mathrm{Disc}\,K^{1/3+\epsilon})$ for quadratic fields K. Bhargava, Shankar, Taniguchi, Thorne, Tsimerman, and Zhao [BST$^+$20] gave a non-trivial bound on $|\mathrm{Cl}_K[2]|$ for all K using geometry of numbers. Ellenberg and Venkatesh [EV07] also proved a non-trivial bound on $|\mathrm{Cl}_K[3]|$ whenever $[K : \mathbb{Q}] \leq 4$. The second author gave a non-trivial bound on $|\mathrm{Cl}_K[p]|$ when K is Galois with the Galois group a non-cyclic and non-quaternion ℓ-group or a nilpotent group where every Sylow-ℓ subgroup is non-cyclic and non-quaternion [Wan21, Wan20]. In the setting when p divides the order of the Galois closure group of K, Klüners and the second author [KW20] proved $|\mathrm{Cl}_K[p]| = O_\epsilon(\mathrm{Disc}\,K^\epsilon)$ when K has Galois closure group a p-group, generalizing the classical result from Gauss's genus theory for K quadratic and $p = 2$.

Soundararajan [Sou00, pg.690] was the first to observe that non-trivial bounds for $|\mathrm{Cl}_K[p]|$ could be proved for almost all imaginary quadratic K, or equivalently, on average over K. Heath-Brown and Pierce [HP17] reinvigorated the study of such average bounds for $|\mathrm{Cl}_K[p]|$, as well as bounds on higher moments, by using the large sieve. As mentioned above, Ellenberg, Pierce, and the third author [EPW17] proved non-trivial bounds for most fields in low degree families using a non-trivial bound of Ellenberg and Venkatesh [EV07] conditional on the existence of small split primes, and precise field counting results with local conditions to prove such existence. Pierce, Turnage-Butterbaugh, and the third author [PTBW20] found ways to prove non-trivial bounds for many more families using zero density estimates for L-functions to prove the required existence of small primes, which is a strategy we use in this paper. This strategy has been improved and extended to further cases by An [An20], Frei and Widmer [FW18, FW21], Widmer [Wid18], Thorner and

Zaman [TZ19b], and the first author, Thorner and Zaman [LOTZ21].

1.3 Further questions

We expect the methods in this paper can be used in other settings. We have forthcoming work with Alberts which uses a similar inductive approach to prove many new cases of Malle's conjecture [Mal04] on the asymptotics of $|E_k(G, X)|$. It would be natural to apply our approach to the 2-part of class groups of fields that can be obtained as cubic extensions of other extensions, using [Bha05] as a base case.

It was noted by Bhargava and Varma [BV16] that the average 3-torsion in class group of quadratic extensions does not change when the fields are subject to finitely many local conditions at finite primes (see also [Woo18]). We expect that the average in Theorem 1.2 behaves similarly and is insensitive to local conditions, while the average in Theorem 1.1 behaves differently and is quite sensitive to local conditions, and it would be interesting to investigate whether this is the case. A subtlety in this question is in defining a notion of local conditions that works well in towers of fields.

The contrast between the constants in Theorems 1.1 and 1.2 naturally leads to the question: when ordering fields by a particular invariant, which averages does one expect to be as predicted by Cohen–Lenstra–Martinet? For example, does the analogue of Theorem 1.2 hold when the fields K are instead ordered by the Artin conductor of the representation of $\mathrm{Gal}(\bar{k}/k)$ induced from the sign representation of $\mathrm{Gal}(K/F_K)$? (This is an irreducible representation, as we show in the proof of Theorem 7.1.) In the case of quartic D_4 extensions of $k = \mathbb{Q}$, the fields themselves were recently counted by this Artin conductor in work of Altuğ, Shankar, Varma, and Wilson [ASVW21].

It would be interesting to extend our methods to as wide a range of groups G as possible (e.g., by incorporating ideas from Sections 2 and 4 into an argument as in Section 8). For example, does an analogue of Theorem 1.1 hold for $(C_2 \wr G)$-extensions for arbitrary abelian groups G? Arbitrary p-groups?

Finally, as noted above, Malle's conjecture predicts asymptotics for $|E_k(G, X)|$. These predicted asymptotics are of the form $|E_k(G, X)| \sim c_{G,k} X^{1/a(G)} (\log X)^{b(k,G)-1}$ for specified integers $a(G)$ and $b(k, G)$, and an unspecified positive constant $c_{G,k}$, as X tends to infinity. Our work raises the question, what is the least exponent $\alpha = \alpha(G)$ such that $|E_k(G, X)| \ll_{[k:\mathbb{Q}], \epsilon} \mathrm{Disc}(k)^{\alpha+\epsilon} X^{1/a(G)} (\log X)^{b(k,G)-1}$ for all k, all $\epsilon > 0$, and all $X \geq 1$? Does such an exponent even exist? When G is abelian, this problem is closely related to bounding torsion subgroups of class groups. Some of the key technical results of this paper (see Section 3) provide the first such result for a non-abelian group G, namely $G = S_3$. What can be said for other non-abelian groups G? This question when $G = S_3$ could naturally be approached by proving a discriminant-aspect subconvexity bound for the relevant Shintani zeta functions, which the methods of Section 3 fall a little short of proving. Can these or other methods be adapted to prove such a subconvexity result? We mention recent work of Hough and Lee [HL21] that establishes a subconvexity bound in t-aspect for the Shintani zeta functions over $\mathbb{Q}$, though we expect these methods do not easily apply to discriminant-aspect.

1.4 Technical remarks

The conjectures of Cohen, Lenstra, and Martinet in fact fix some archimedean data and only consider families of fields with this fixed data. In particular, for Galois Γ-extensions L/k, they fix the Γ-module structure of $\mathcal{O}_L^* \otimes_{\mathbb{Z}} \mathbb{Q}$, which is equivalent [CM90, Théorème 6.7] to fixing the representation $\oplus_v \mathrm{Ind}_{\Gamma_v}^\Gamma \mathbb{Q}$, where the sum is over infinite places v of k and Γ_v is the decomposition group of L/k at v, and we call this the *enriched signature*. The papers of Cohen, Lenstra, and Martinet are agnostic on the relative frequency of the various enriched signatures (and even whether such limiting frequencies exist). So, to be precise, to obtain (1.1) from their conjectures one must also assume such frequencies exist (which is natural to conjecture given all known counting results, e.g. [DH71, Wri89, CyDO02, Bha05], and is conjectured by Malle [Mal04]), and the conjectural value would be given as a weighted average of particular values for each enriched signature as conjectured by Cohen, Lenstra, and Martinet, where the weights are these frequencies. When one fixes an enriched signature, one can use the results of [WW21] to find the average value predicted by Cohen, Lenstra, and Martinet (see Section 7).

We prove a version of Theorem 1.1 with a specified enriched signature (in fact with slightly more specification at infinity) in Theorem 6.1. However, even when we do this, we do not apparently obtain the values conjectured by Cohen and Martinet in [CM90]. We show this computationally is the case in Section 7.2.

This is because in this setting each F appears as the index 2 subfield for a positive proportion of K, and so the 3-ranks of the particular F that appear with significant frequency bias the statistics, as in the work of Bartel and Lenstra [BL20]. When we only average $\mathrm{Cl}_{K/F}$ as in Theorem 1.2, this bias is removed.

1.5 List of notations

k: a number field, for us a subfield of a fixed algebraic closure $\bar{\mathbb{Q}}$
$\mathcal{O}_k$: the ring of algebraic integers in k
$\mathrm{disc}(F/k)$: relative discriminant ideal in $\mathcal{O}_k$, for an extension F/k
$\mathrm{Nm}\, I$: norm $|\mathcal{O}_k/I|$ of an ideal I in $\mathcal{O}_k$ and extend to any fractional ideals in $\mathcal{O}_k$ multiplicatively
$\mathrm{Nm}_{F/k}\, I$: an ideal in $\mathcal{O}_k$ that is $(I \cap \mathcal{O}_k)^{f(I | I \cap \mathcal{O}_k)}$ when I is a prime ideal in $\mathcal{O}_F$ and f is the inertia degree of I over $I \cap \mathcal{O}_k$, and defined for any fractional ideals in $\mathcal{O}_F$ multiplicatively
$\mathrm{Disc}(F/k)$: $\mathrm{Nm}(\mathrm{disc}(F/k))$ (When k omitted, $k = \mathbb{Q}$)
$\mathrm{Gal}(F/k)$: the *Galois closure group* of F/k, defined as the Galois group of $\tilde{F}/k$ as a *permutation group*, where $\tilde{F}$ is the Galois closure of F over k (in $\bar{\mathbb{Q}}$) acting on the embeddings of $F \to \tilde{F}$ that fix k pointwise
G-extension: for a permutation group G, an extension L/k of number fields (in $\bar{\mathbb{Q}}$), *and a choice of isomorphism* $\phi : \mathrm{Gal}(L/k) \simeq G$ *as permutation groups* (see Definition 6.7)
2-extension: a G-extension for some 2-group G
$E_k(G, X)$: the set of G-extensions F/k with $\mathrm{Disc}(F) \leq X$
$N_k(G, X)$: the number of G-extensions F/k with $\mathrm{Disc}(F/k) \leq X$ (note relative discriminant, versus absolute above)
Cl_F: class group of F
$\mathrm{Cl}_{F/k}$: relative class group of F/k, when $k = \mathbb{Q}$ it is the usual class group of F (see Section 2)
$A[\ell]$: $\{[\alpha] \in A \mid \ell[\alpha] = 0 \in A\}$ for an abelian group A
$h(F/k), h(F)$: the size of $\mathrm{Cl}_{F/k}, \mathrm{Cl}_F$
$h_\ell(F/k), h_\ell(F)$: the size of $\mathrm{Cl}_{F/k}[\ell], \mathrm{Cl}_F[\ell]$
$\widetilde{\mathrm{Cl}}_L$: Arakelov class group
$\pi_k(X)$: the number of prime ideals $\mathfrak{p}$ in k with $\mathrm{Nm}(\mathfrak{p}) < X$
$\pi_k(Y; F, \mathcal{C})$: the number of unramified prime ideals $\mathfrak{p}$ in k with $\mathrm{Nm}_{k/\mathbb{Q}}(\mathfrak{p}) < Y$ and with Frobenius at $\mathfrak{p}$ in the conjugacy class of $\mathcal{C}$ in $\mathrm{Gal}(F/k)$
$r_1(k)$: the number of real embeddings of k
$r_2(k)$: the number of pairs of complex embeddings of k
$\mathrm{rk}\, \mathcal{O}_K^*$: the unit rank, i.e. $\dim_{\mathbb{Q}}(\mathcal{O}_k^* \otimes \mathbb{Q})$
$\zeta_k(s)$: Dedekind zeta function of k
κ_k: the residue $\mathrm{Res}_{s=1}\zeta_k(s)$
Rg_k: the regulator of k
$f(X) \sim g(X)$: $\lim_{X \to \infty} f(X)/g(X) = 1$ or $\lim_{X \to \infty} f(X) = \lim_{X \to \infty} g(X) = 0$
$f(X) = O_{p_1,\dots}(g(X))$: there exists a constant C depending only on $p_1,\dots$ such that for all values of all variables $|f(X)| \leq Cg(X)$
$f(X) \ll_{p_1,\dots} g(X)$: $f(X) = O_{p_1,\dots}(g(X))$
$f(X) \gg_{p_1,\dots} g(X)$: only used when both sides non-negative, and then means $g(X) \ll_{p_1,\dots} f(X)$

Acknowledgements

2 Nontrivial Bound for the Relative Class Group

In this section, our main goal is to establish Lemma 2.1, which is a *relative* version of a widely used lemma of Ellenberg–Venkatesh [EV07, Lemma 2.3]. Let L/K be an extension of number fields. The relative class group $\mathrm{Cl}_{L/K} \subset \mathrm{Cl}_L$ is defined to be the kernel of the map $\mathrm{Nm}_{L/K} : \mathrm{Cl}_L \to \mathrm{Cl}_K$ induced from the usual norm on fractional ideals of L.

Lemma 2.1 (Relative Ellenberg–Venkatesh)**.** *Let L/K be an extension of number fields with $[L : K] = d$, let $\ell \geq 1$ be an integer, and let θ be a real number such that $0 < \theta < \frac{1}{4\ell(d-1)}$. Suppose there exist M pairs of distinct primes $(\wp_i, \bar{\wp}_i)$ in $\mathcal{O}_L$ and coprime integers a_i, b_i such that*

1. *For each i, we have $\wp_i \cap \mathcal{O}_K = \bar{\wp}_i \cap \mathcal{O}_K$ and $\mathrm{Nm}_{L/K}(\wp_i)^{a_i} = \mathrm{Nm}_{L/K}(\bar{\wp}_i)^{b_i}$;*

2. *For each i, the norms satisfy $\mathrm{Nm}(\wp_i)^{a_i} = \mathrm{Nm}(\bar{\wp}_i)^{b_i} < \mathrm{Disc}(L/K)^{\theta}$; and*

3. *For each i, there is no intermediate field H with $K \subset H \subsetneq L$ such that $\wp_i$ and $\bar{\wp}_i$ are both extended from H. (A prime $\wp \subset \mathcal{O}_L$ is* extended *from H if there exists a prime $\mathfrak{p} \subset \mathcal{O}_H$ such that $\wp = \mathfrak{p}\,\mathcal{O}_L$.)*

Then

$$|\mathrm{Cl}_{L/K}[\ell]| = O_{[L:\mathbb{Q}],\theta,\epsilon}\Big(\frac{\mathrm{Disc}(L/K)^{1/2+\epsilon}\,\mathrm{Disc}(K)^{(d-1)/2+\epsilon}}{M}\Big). \tag{2.1}$$

Remark 2.2. *In our application, we will only use prime ideals that are split completely in L/K, therefore the first and third conditions will be automatically satisfied, and the second condition will be equivalent to $\mathrm{Nm}(\wp \cap \mathcal{O}_K) < \mathrm{Disc}(L/K)^{\theta}$.*

The original lemma [EV07] gives a non-trivial bound

$$|\mathrm{Cl}_L[\ell]| = O_{[L:\mathbb{Q}],\theta,\epsilon}\Big(\frac{\mathrm{Disc}(L)^{1/2+\epsilon}}{M}\Big), \tag{2.2}$$

for the absolute class group $\mathrm{Cl}_L[\ell]$ under the same assumptions. Our improvement is in proving a savings from the trivial bound on the size of the *relative* class group $\mathrm{Cl}_{L/K}[\ell]$ instead of the *absolute* class group. Such a refinement is crucial for our application since we will treat Cl_K and $\mathrm{Cl}_{L/K}$ separately.

When ℓ is relatively prime to $[L : K]$, there is a short exact sequence

$$0 \longrightarrow \mathrm{Cl}_{L/K}[\ell] \longrightarrow \mathrm{Cl}_L[\ell] \xrightarrow{\mathrm{Nm}_{L/K}} \mathrm{Cl}_K[\ell] \longrightarrow 0.$$

Let ι be the natural map from Cl_K to Cl_L by extension of ideals. The composition $\mathrm{Nm}_{L/K} \circ \iota : \mathrm{Cl}_K[\ell] \to \mathrm{Cl}_K[\ell]$ is equal to multiplication by $[L : K]$ and thus is an isomorphism since $(\ell, [L : K]) = 1$, so ι induces a splitting section of the above sequence. So we have

$$\mathrm{Cl}_L[\ell] \simeq \mathrm{Cl}_{L/K}[\ell] \times \mathrm{Cl}_K[\ell], \qquad h_\ell(L) = h_\ell(K) \cdot h_\ell(L/K).$$

This leads to a strategy we use in this paper to bound $h_\ell(L)$, that is, to bound $h_\ell(K)$ and $h_\ell(L/K)$ separately.

The organization of this section is as follows. In Section 2.1, we give a definition of a *relative Arakelov class group*, compute the volume of it and derive the "trivial" bound for the relative class group in Lemma 2.5. In Section 2.2, we prove Lemma 2.1.

2.1 The relative Arakelov class group

In this section we will define a relative version of the Arakelov class group. First we recall the usual *absolute* notion of the Arakelov class group. A nice reference for the theory of the absolute Arakelov class group is [Sch08].

For any number field L with degree n and $r = r_1 + r_2$ infinite places, we let I_L be the group of fractional ideals and $L_\infty := \prod_{v|\infty} \mathbb{R}_{>0}^{\times}$. We define the degree 0 divisors to be $\mathrm{Div}^0(L) := \{(x, \mathfrak{a}) \in L_\infty^{\times} \times I_L : |x|_\infty = \mathrm{Nm}(\mathfrak{a})\}$ where $\mathrm{Nm}(\mathfrak{a}) := |\mathcal{O}_L/\mathfrak{a}|$ and $|x|_\infty = \prod_{v|\infty} |x_v|$. There is a natural embedding $\pi : L^{\times} \to \mathrm{Div}^0(L)$ by

sending $\alpha \in L^\times$ to $((|\alpha|_v), (\alpha)) \in \mathrm{Div}^0(L)$ from the product formula (here $|\cdot|_v$ is the usual norm in $\mathbb{R}$ at the r_1 real embeddings and the square of the usual norm in $\mathbb{R}$ at the r_2 complex embeddings).

The absolute Arakelov class group $\widetilde{\mathrm{Cl}}_L$ of L is then defined as $\widetilde{\mathrm{Cl}}_L := \mathrm{Div}^0(L)/\pi(L^\times)$, and it fits into the following short exact sequence

$$0 \longrightarrow (\oplus\mathbb{R})^{(0)}/\mathcal{L}(L) \longrightarrow \widetilde{\mathrm{Cl}}_L \longrightarrow \mathrm{Cl}_L \longrightarrow 0,$$

where $(\oplus_v\mathbb{R})^{(0)}$ is isomorphic to $L_\infty^{(1)}$ (the elements of $L_\infty^\times$ of norm 1) via the Minkowski embedding, i.e. the logarithm map $\log = \oplus_v \log$, and $\mathcal{L}(L) = \log(\pi(\mathcal{O}_L^\times))$ is a full rank lattice by Dirichlet's unit theorem.

The Arakelov class group is not only an abelian group but also a Lie group. We fix a left-invariant Riemannian metric on $\widetilde{\mathrm{Cl}}_L$ that on $(\oplus_v\mathbb{R})^{(0)}$ agrees with the restriction of the standard Riemannian metric from $\oplus_v\mathbb{R}$. We will use this Riemannian metric on $\tilde{\mathrm{Cl}}_L$, and the induced metrics on various sub-Lie groups, to compute all volumes in this section. We compute $\mathrm{Vol}(\widetilde{\mathrm{Cl}}_L) = h(L) \cdot \mathrm{Rg}(L) \cdot \sqrt{r}$. Though the language of a Riemannian metric is convenient, we remark that in our case this metric is very concrete (in particular, because unlike [EV07], we are using the *non-oriented Arakelov class group* as in [Sch08, Section 5]). All of our groups are a disjoint union of finitely many copies of quotients of subspaces of $\mathbb{R}^n$, and the volumes we compute are always the ones that come from the usual metric on $\mathbb{R}^n$.

The absolute Arakelov class group associated to L and K can be related by a norm map $\mathrm{Nm}_{L/K} : \widetilde{\mathrm{Cl}}_L \to \widetilde{\mathrm{Cl}}_K$ where we use the relative norm map $\mathrm{Nm}_{L/K} : I_L \to I_K$ for fractional ideals and $\mathrm{Nm}_\infty : (\oplus_v\mathbb{R})^{(0)} \to (\oplus_w\mathbb{R})^{(0)}$ that sends $(x_v)_{v|\infty} \mapsto (\sum_{v|w} x_v)_{w|\infty}$ for archimedean embeddings. This norm map $\mathrm{Nm}_{L/K}$ fits into the following commutative diagram:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & (\oplus_v\mathbb{R})^{(0)}/\mathcal{L}(L) & \longrightarrow & \widetilde{\mathrm{Cl}}_L & \longrightarrow & \mathrm{Cl}_L & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\mathrm{Nm}_\infty} & & \downarrow{\scriptstyle\mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle\mathrm{Nm}_{L/K}} & & \\
0 & \longrightarrow & (\oplus_w\mathbb{R})^{(0)}/\mathcal{L}(K) & \longrightarrow & \widetilde{\mathrm{Cl}}_K & \longrightarrow & \mathrm{Cl}_K & \longrightarrow & 0.
\end{array}
\tag{2.3}
$$

We now can define the relative Arakelov class group in a manner analogous to the relative class group, as a subgroup of the absolute Arakelov class group.

Definition 2.3 (Relative Arakelov Class Group). *Given an extension L/K of number fields, we define the relative Arakelov class group $\widetilde{\mathrm{Cl}}_{L/K}$ to be the kernel of $\mathrm{Nm}_{L/K} : \widetilde{\mathrm{Cl}}_L \to \widetilde{\mathrm{Cl}}_K$.*

We obtain a short exact sequence for the relative Arakelov class group as an abelian group, similar to the sequence 2.1:

$$0 \longrightarrow \mathrm{Ker}(\mathrm{Nm}_\infty) \longrightarrow \widetilde{\mathrm{Cl}}_{L/K} \longrightarrow \mathrm{Cl}_{L/K} \longrightarrow 0, \tag{2.4}$$

from an application of the snake lemma on (2.3), since Nm_∞ is surjective.

Our next goal is to show that $\mathrm{Vol}(\mathrm{Ker}(\mathrm{Nm}_\infty)) = C \, \mathrm{Rg}_L / \mathrm{Rg}_K$ where C is a constant only depending on the signatures of L and K. Let $v_{i,j}$ be the standard coordinates in $\oplus_v\mathbb{R}$ and w_i in $\oplus_w\mathbb{R}$, where Nm_∞ maps $w_i = \sum_{1 \le j \le i_k} v_{i,j}$ and i_k is the number of infinite places above w_i. We then choose a new coordinate system for $\oplus_v\mathbb{R}$ to be $\tilde{v}_{i,j}$ where $\tilde{v}_{i,j} = v_{i,j}$ for $j > 1$ and $\tilde{v}_{i,1} = \sum_j v_{i,j} = w_i$. Then we can compute the covolume of $(\oplus_v\mathbb{R})^{(0)}/\mathcal{L}(L)$ using the coordinate system $v_{i,j}$ or $\tilde{v}_{i,j}$ (without $v_{1,1}$ and $\tilde{v}_{1,1}$ respectively):

$$\mathrm{Rg}_L = \int_{\tilde{v} \in \mathcal{F}_L} \mathrm{d}\tilde{v} = \int_{w \in \mathcal{F}_K} \mathrm{d}w \int_{\tilde{v}' \in \mathrm{Nm}_\infty^{-1}(w)} \mathrm{d}\tilde{v}' = \mathrm{Rg}_K \cdot \int_{\tilde{v}' \in \mathrm{Nm}_\infty^{-1}(0)} \mathrm{d}\tilde{v}'.$$

Here $\mathcal{F}_L$ is the projection of a fundamental domain for $(\oplus_v\mathbb{R})^{(0)}/\mathcal{L}(L)$ onto the $v_{i,j}((i,j) \neq (1,1))$-coordinate plane, and we define $\mathcal{F}_K$ analogously. The first equality comes from the definition of regulator. The second equality is an iterated integral where we use $\tilde{v}'$ to denote the variables in $\tilde{v}$ aside from $\tilde{v}_{i,1}$, and $\mathrm{Nm}_\infty^{-1}(w) = \{v \in \mathcal{F}_L \mid \mathrm{Nm}_\infty(v) \equiv w \mod \mathcal{L}(K)\}$. In the last equality $\int_{\tilde{v}' \in \mathrm{Nm}_\infty^{-1}(0)} \mathrm{d}\tilde{v}' = \int_{\tilde{v}' \in \mathrm{Nm}_\infty^{-1}(w)} \mathrm{d}\tilde{v}'$ for any $w \in \mathcal{F}_K$ since the two domains for $\tilde{v}'$ only differ by a translation. We have $\mathrm{Vol}(\mathrm{Ker}(\mathrm{Nm}_\infty)) = \prod_i \sqrt{i_k} \cdot \int_{\tilde{v}' \in \mathrm{Nm}_\infty^{-1}(0)} \mathrm{d}\tilde{v}' = \prod_i \sqrt{i_k} \frac{\mathrm{Rg}_L}{\mathrm{Rg}_K}$.

In the following lemma we give the description of the cokernel of the map $\mathrm{Nm}_{L/K} : \mathrm{Cl}_L \to \mathrm{Cl}_K$.

Lemma 2.4. *Given an extension L/K of number fields, the cokernel of $\mathrm{Nm}_{L/K} : \mathrm{Cl}_L \to \mathrm{Cl}_K$ is isomorphic to $\mathrm{Gal}(M/K)$, where $M = H_K \cap L$ and H_K is the Hilbert class field of K.*

Proof. By class field theory, the map $\mathrm{Nm}_{L/K} : \mathrm{Cl}_L \to \mathrm{Cl}_K$ agrees with the restriction map on the Galois groups $\mathrm{Gal}(H_L/L) \to \mathrm{Gal}(H_K/K)$ after identifying class groups and Galois groups with the reciprocity map. Since H_K/K is Galois, we have $\mathrm{Gal}(H_L/L) \twoheadrightarrow \mathrm{Gal}(H_K L/L) \simeq \mathrm{Gal}(H_K/M) = \mathrm{Im}(\mathrm{Nm}_{L/K} : \mathrm{Cl}_L \to \mathrm{Cl}_K)$, and the lemma follows. $\square$

As a consequence, we have an upper bound $|\mathrm{Coker}(\mathrm{Nm}_{L/K} : \mathrm{Cl}_L \to \mathrm{Cl}_K)| \leq [L : K]$, and thus we can obtain the following upper bound on $h(L/K)$, which we consider as the "trivial bound" on the ℓ-torsion in the relative class group.

Lemma 2.5. *Given a relative extension L/K with $[L : K] = d$ and an arbitrary integer $\ell > 0$, we have*

$$h_\ell(L/K) \ll_{[L:\mathbb{Q}],\epsilon} \mathrm{Disc}(L/K)^{1/2+\epsilon} \cdot \mathrm{Disc}(K)^{(d-1)/2+\epsilon}.$$

Proof. We have

$$h_\ell(L/K) \leq h(L/K) \leq [L : K] \cdot \frac{h(L)}{h(K)} \ll_{[L:\mathbb{Q}],\epsilon} \mathrm{Disc}(L/K)^{1/2+\epsilon}\mathrm{Disc}(K)^{(d-1)/2+\epsilon}, \tag{2.5}$$

where the first inequality is trivial, and the second inequality follows from Lemma 2.4. The third inequality comes from the theorem of Brauer-Siegel, an absolute lower bound $\frac{\mathrm{Rg}(L)}{\mathrm{Rg}(K)} \gg_{[L:\mathbb{Q}]} 1$ on the ratio of regulator by [FS99], and the expression of the relative discriminant in terms of absolute discriminants. $\square$

Combining the discussion of $\mathrm{Vol}(\mathrm{Ker}(\mathrm{Nm}_\infty))$ and $\mathrm{Cl}_{L/K}$, we obtain an estimate of $\mathrm{Vol}(\widetilde{\mathrm{Cl}}_{L/K})$.

Lemma 2.6. *Given an extension L/K of number fields with $[L : K] = d$, with the measure above, we have*

$$\mathrm{Disc}(L/K)^{1/2-\epsilon} \mathrm{Disc}(K)^{(d-1)/2-\epsilon} \ll_{[L:\mathbb{Q}],\epsilon} \mathrm{Vol}(\widetilde{\mathrm{Cl}}_{L/K}) \ll_{[L:\mathbb{Q}],\epsilon} \mathrm{Disc}(L/K)^{1/2+\epsilon} \mathrm{Disc}(K)^{(d-1)/2+\epsilon}.$$

Remark 2.7. The upper bounds in Lemmas 2.5 and 2.6 are both effective, despite the invocation of Brauer–Siegel to estimate the quotient of residues $\mathrm{Res}_{s=1}\zeta_L(s)/\mathrm{Res}_{s=1}\zeta_K(s)$, and the lower bound of Lemma 2.6 is effective if L does not contain a nontrivial quadratic extension of the form $K(\sqrt{D})$ for $D \in \mathbb{Q}$. In particular, there is always an effective upper bound on the residue $\mathrm{Res}_{s=1}\zeta_L(s)$ due to Landau (see also [Bra47, Lemma 3]), and there is an effective lower bound on $\mathrm{Res}_{s=1}\zeta_K(s)$ whenever $\zeta_K(s)$ does not have an exceptional Landau–Siegel zero due to Stark [Sta74]. Thus, if $\zeta_K(s)$ does not have an exceptional zero, we simply combine these two results to get an effective upper bound. When $\zeta_K(s)$ does have an exceptional zero, the quotient $\zeta_{\widetilde{L}}(s)/\zeta_K(s)$ is entire by the Aramata–Brauer theorem [Bra47, Theorem 1], where $\widetilde{L}$ denotes the normal closure of L over K, and does not have an exceptional zero by Stark [Sta74, Theorem 3]. Moreover, by [Bra47, Lemma on p.244], this quotient may be expressed as a product over all L-functions associated to nontrivial 1-dimensional characters of subextensions of $\widetilde{L}/K$, where each such L-function appears with a strictly positive rational exponent. These L-functions thus also do not have an exceptional zero, and are subject to effective lower bounds [Sta74, Lemma 2] in addition to the effective upper bounds that hold for any entire L-function [IK04, Ch. 5]. The quotient $\zeta_L(s)/\zeta_K(s)$ may be expressed as a product and quotient of these L-functions, and is thus subject to an effective upper bound in the case that $\zeta_K(s)$ has an exceptional zero as well. For the lower bound on $\mathrm{Res}_{s=1}\zeta_L(s)/\mathrm{Res}_{s=1}\zeta_K(s)$, if $\zeta_L(s)$ does not have an exceptional zero, we simply use the effective lower bound on its residue and the effective upper bound on that of $\zeta_K(s)$. If $\zeta_L(s)$ has an exceptional zero, it is inherited either from $\zeta_K(s)$ or from the Dedekind zeta function of a subextension of L/K of the form $K(\sqrt{D})$ with $D \in \mathbb{Q}$ by [Sta74, Theorem 3]. In the former case, we proceed as in the proof of the effective upper bound to also obtain an effective lower bound; in the latter, there does not appear to be a way to make the lower bound effective.

2.2 Relative Ellenberg–Venkatesh Lemma

Now we are ready to prove Lemma 2.1. The idea of the proof is similar to the proof of Lemma 2.3 in [EV07], where the major difference is we use a different set T of ideals that cut out the non-trivial savings in the proof. As a result, we can show a savings that is completely coming from the relative class group.

Proof of Lemma 2.1. We let $\psi : \mathrm{Div}^0(L) \to \widetilde{\mathrm{Cl}}_L$ to be natural quotient map, and denote the following subgroups of $\mathrm{Div}^0(L)$

$$G = \psi^{-1}(\widetilde{\mathrm{Cl}}_{L/K}), \quad P = \pi(L^\times), \quad P_\ell = \ell G + P.$$

We can pull-back the Riemannian metric from $\widetilde{\mathrm{Cl}}_L$ to a left-invariant Riemannian metric on G. The short exact sequence (2.4) induces an isomorphism $\mathrm{Cl}_{L/K}/\ell\,\mathrm{Cl}_{L/K} \simeq \widetilde{\mathrm{Cl}}_{L/K}/\ell\widetilde{\mathrm{Cl}}_{L/K}$. Therefore we obtain an upper bound on $|\mathrm{Cl}_{L/K}[\ell]| = |\mathrm{Cl}_{L/K}/\ell\,\mathrm{Cl}_{L/K}|$ by $\mathrm{Vol}(\widetilde{\mathrm{Cl}}_{L/K})/\mathrm{Vol}(\ell\widetilde{\mathrm{Cl}}_{L/K})$ where $\widetilde{\mathrm{Cl}}_{L/K} = G/P$ and $\ell\widetilde{\mathrm{Cl}}_{L/K} = P_\ell/P$. We will give a lower bound on $\mathrm{Vol}(P_\ell/P)$ and derive an upper bound for $\mathrm{Vol}(G/P_\ell)$ using the trivial upper bound for $\mathrm{Vol}(G/P) = \mathrm{Vol}(\widetilde{\mathrm{Cl}}_{L/K})$ in Lemma 2.6.

Now we let Σ_L be the set of infinite places of L, and for a constant $C > 1$ we define

$$T := \{(x, J) \in G \mid J = \wp_i^{a_i}\bar{\wp}_i^{-b_i} \text{ for some } i, \text{ and } \forall v_1, v_2 \in \Sigma_L, C^{-1/\ell} < |x|_{v_1}/|x|_{v_2} < C^{1/\ell}\} \subseteq \mathrm{Div}^0(L),$$

where $(\wp_i, \bar{\wp}_i)$ for $i = 1, \cdots, M$ are the pairs of prime ideals in $\mathcal{O}_L$ that are given in the statement of the lemma. We will show that

$$\mathrm{Vol}(P_\ell/P) \geq \mathrm{Vol}((\ell T + P)/P) \gg_{[L:\mathbb{Q}], C} M,$$

from which it follows that $|\widetilde{\mathrm{Cl}}_{L/K}[\ell]| \ll_{[L:\mathbb{Q}], C} \frac{\mathrm{Vol}(\widetilde{\mathrm{Cl}}_{L/K})}{M}$. The first inequality is clear since there is a natural embedding $\ell T + P \hookrightarrow P_\ell = \ell G + P$.

It suffices to prove the second inequality. For each i, we let $T_i \subset T$ be the subset of elements with $J = \wp_i^{a_i}\bar{\wp}_i^{-b_i}$ and let D_i be the corresponding disk $D_i := (\ell T_i + P)/P \subseteq \widetilde{\mathrm{Cl}}_{L/K}$. We now show that for each i, the volume of D_i satisfies $\mathrm{Vol}(D_i) \gg_{[L:\mathbb{Q}], C} 1$. We can compute that $\mathrm{Vol}(\ell T_i)$ in G is a constant in terms of C and $[L : \mathbb{Q}]$. If $t_1^\ell, t_2^\ell \in \ell T_i$ correspond to the same point in D_i, then let $u := t_1^\ell/t_2^\ell$. We see that $u \in \mathcal{O}_L^\times$ since u has no non-archimedean valuations, and moreover it satisfies $C^{-2} < |u|_{v_1}/|u|_{v_2} < C^2$ for any archimedean valuations $v_1, v_2 \in \Sigma_L$. Now all archimedean valuations of u are of roughly the same size and their product is 1, therefore the number of such u can be uniformly bounded in terms of $[L : \mathbb{Q}]$ and C, since the defining polynomial of u has bounded integral coefficients and bounded degree. This then implies that the disk $D_i = (\ell T_i + P)/P$ has $\mathrm{Vol}(D_i) \gg_{[L:\mathbb{Q}], C} 1$.

On the other hand, we now show that for any $i \neq j$, the disks D_i and D_j do not overlap. Suppose $t_i \in T_i, t_j \in T_j$ with $i \neq j$ satisfy $u := t_i^\ell t_j^{-\ell} \in L^\times$. Then recall that for $u \in \mathrm{Div}_L^0$, we define the height of u as in [EV07] to be

$$H(u) := \prod_{v|\infty} \max\{u_v, 1\} \prod_\wp \max\{|\wp|^{-\mathrm{val}_\wp(u)}, 1\}.$$

Then for the given u, we have $H(u) \leq C^{2[L:\mathbb{Q}]} \mathrm{Nm}(\wp_j)^{a_j \ell} \mathrm{Nm}(\bar{\wp}_i)^{b_i \ell}$, which is bounded by $C^{2[L:\mathbb{Q}]} \mathrm{Disc}(L/K)^{2\theta\ell}$ from our assumption on $(\wp, \bar{\wp})$. By [EV07, Lemma 2.2], there is a constant $D_0 = D_0(\theta, [L : \mathbb{Q}])$ such that when $\mathrm{Disc}(L/K)$ is larger than D_0, the height of u is not large enough to generate L. Therefore u generates a strict subfield $K(u) \subsetneq L$. This is a contradiction, since the non-archimedean part of u has valuations from $\wp_i$ and $\bar{\wp}_i$, which are not extended from any strict intermediate subfield by assumption. Thus, when $\mathrm{Disc}(L/K)$ is sufficiently large, we have shown that $D_i \cap D_j = \emptyset$ for any $i \neq j$.

Therefore by choosing an arbitrary absolute constant $C > 1$, we get for $\mathrm{Disc}(L/K)$ sufficiently larger $D_0 = D_0(\theta, [L : \mathbb{Q}])$ that

$$\mathrm{Vol}((\ell T + P)/P) \geq \sum_i \mathrm{Vol}(D_i) \gg_{[L:\mathbb{Q}]} M.$$

$\square$

3 Uniform bounds on cubic extensions and the average 3-part of quadratic extensions

In this section we are going to bound the sum of $h_3(F/k)$ for quadratic extensions F/k of a general number field k, and the closely related number of S_3 cubic extensions of k. This proof will employ different techniques and ideas for different regimes of X versus $\mathrm{Disc}(k)$. Let $N_k(G, X)$ be the number of isomorphism classes of G-extensions L/k with $\mathrm{Disc}(L/k) \leq X$. The main theorem is the following, which we expect will be useful for other applications as well.

Theorem 3.1. *Let k be a number field, let $h = h_2(k)$ denote the size of the 2-torsion subgroup of the class group of k, and let $D_k = \mathrm{Disc}(k)$. For any $X \geq 1$ we have*

$$\sum_{\substack{[F:k]=2 \\ \mathrm{Disc}(F/k) \leq X}} h_3(F/k) \ll_{[k:\mathbb{Q}],\epsilon} D_k^\epsilon \cdot \begin{cases} hX^{3/2}D_k^{1/2}, & \text{if } X \leq D_k h^{-2/3}, \\ h^{1/3}X^{1/2}D_k^{3/2}, & \text{if } D_k h^{-2/3} \leq X \leq D_k^2 h^{2/3}, \\ XD_k^{1/2}, & \text{if } D_k^2 h^{2/3} \leq X \leq D_k^{5/2}h^{2/3}, \\ h^{2/3}D_k^3, & \text{if } D_k^{5/2}h^{2/3} \leq X \leq D_k^3 h^{2/3}, \text{ and} \\ X, & \text{if } X \geq D_k^3 h^{2/3}. \end{cases}$$

The same upper bound holds for $N_k(S_3, X)$. (The sum is over $F \subset \bar{\mathbb{Q}}$.)

We obtain the following convenient corollary for general number fields k.

Corollary 3.2. *For any number field k and any $X \geq 1$, we have*

$$\sum_{\substack{[F:k]=2 \\ \mathrm{Disc}(F/k) \leq X}} h_3(F/k) = O_{[k:\mathbb{Q}],\epsilon}(\mathrm{Disc}(k)^{1+\epsilon}h_2(k)^{2/3}X).$$

The same upper bound holds for $N_k(S_3, X)$ under the same hypotheses.

Using the trivial bound on $h_2(k)$ in Corollary 3.2, the right-hand side becomes $O_{[k:\mathbb{Q}],\epsilon}(\mathrm{Disc}(k)^{4/3+\epsilon}X)$ for any k, and when k is a 2-extension, it follows from Lemma 5.6 that the right-hand side is $O_{[k:\mathbb{Q}],\epsilon}(\mathrm{Disc}(k)^{1+\epsilon}X)$.

Remark 3.3. *Theorem 3.1 relies on an application of the Brauer–Siegel theorem to give a lower bound on the residue $\mathrm{Res}_{s=1}\zeta_k(s)$ of the Dedekind zeta function of k. In particular, the implied constant depends on ϵ ineffectively. However, the key results of Sections 3.1–3.3 from which Theorem 3.1 is obtained, namely Propositions 3.4, 3.6, and 3.12, have effective constants and an explicit dependence on the residue, and could be used to prove an effective analogue of Theorem 3.1 with dependence on the residue.*

In order to prove Theorem 3.1, we will use different approaches for three regimes of X compared to $\mathrm{Disc}(k)$: the small range, the large range, and the intermediate range. In Section 3.1, for X in the small range, we will use class field theory to give what we regard as a weak bound on the number of cubic extensions with a fixed discriminant. This will give a correspondingly weak bound on the number of cubic extensions with bounded discriminant. In Section 3.2, for X in the large range, by using the functional equation of the Shintani zeta function for cubic rings, we can use the bound on the coefficients we obtained from class field theory and get improved bounds on the number of cubic fields with discriminants quite large compared to $\mathrm{Disc}(k)$. In Section 3.3, we will take advantage of the fact that the bound from the Shintani zeta function is actually also an upper bound for counting all cubic rings. Since the number of cubic orders associated to each cubic field is large, we show it is impossible to get too many cubic fields with X in the intermediate range. Finally, in Section 3.4, we prove Theorem 3.1 by combining the previous propositions for all ranges of X.

3.1 Small range: class field theory

In this section we will use class field theory to give the following upper bound on the number of small degree extensions of k.

Proposition 3.4. *For any number field k and any $X \geq 1$, we have*

$$N_k(S_3, X) + N_k(C_3, X) + N_k(S_2, X) = O_{[k:\mathbb{Q}],\epsilon}(X^{3/2+\epsilon}\mathrm{Disc}(k)^{1/2+\epsilon}h_2(k)).$$

To prove this proposition, we apply class field theory and the trivial bound on torsion in relative class groups to give the following pointwise bound on the number of relative S_3 cubic extensions.

Lemma 3.5. *For any positive integer n and any number field k, the number of extensions K/k in $\bar{\mathbb{Q}}$ with $\mathrm{Disc}(K/k) = n$ and $[K : k] \leq 3$ is $O_{[k:\mathbb{Q}],\epsilon}(n^{1/2+\epsilon}h_2(k)\mathrm{Disc}(k)^{1/2+\epsilon})$.*

Proof. If K/k is an S_3 cubic extension with $\text{Disc}(K/k) = n$, then its associated quadratic resolvent F/k has $\text{Disc}(F/k) = m$ and $m| \text{Disc}(K/k)$. By class field theory, quadratic extensions of k are in bijection to surjective homomorphisms from the idèle class group $C_k = \mathbb{A}_k^\times / k^\times$ to C_2, where $\mathbb{A}_k^\times$ is the idèle group. We have the following exact sequence of C_k,

$$1 \to O_k^\times \to \prod_v O_v^\times \to C_k \to \text{Cl}_k \to 1.$$

Since $\text{Hom}(\cdot, A)$ is left exact, we get

$$1 \to \text{Hom}(\text{Cl}_k, C_2) \to \text{Hom}(C_k, C_2) \to \text{Hom}(\prod_v O_v^\times, C_2).$$

Here $|\text{Hom}(\text{Cl}_k, C_2)| = h_2(k)$. Given a $\rho \in \text{Hom}(C_k, C_2)$, its image in $\text{Hom}(\prod_v O_v^\times, C_2)$ determines the relative discriminant ideal of the quadratic field corresponding to ρ. Therefore for each fixed m, the number of possible F/k with $\text{Disc}(F/k) = m$ is bounded by $h_2(k)$. For each fixed n, there are at most $O_{[k:\mathbb{Q}],\epsilon}(n^\epsilon)$ possible m, therefore there are at most $O_{[k:\mathbb{Q}],\epsilon}(n^\epsilon h_2(k))$ quadratic extensions F/k with $\text{Disc}(F/k)|n$.

Similarly, for each fixed quadratic extension F/k, any associated S_3 cubic extension K/k has Galois closure $\tilde{K}/k$ such that $\tilde{K}/F$ has $\text{Gal}(\tilde{K}/F) = C_3$. Thus, we can use class field theory again to determine that, for each fixed F/k, the number of associated S_3 cubic extensions with $\text{Disc}(K/k)|n$ is

$$\ll_{[k:\mathbb{Q}],\epsilon} n^\epsilon h_3(F/k) \ll_{[k:\mathbb{Q}],\epsilon} n^\epsilon \text{Disc}(F/k)^{1/2+\epsilon} \text{Disc}(k)^{1/2+\epsilon} \ll_{[k:\mathbb{Q}],\epsilon} n^{1/2+\epsilon} \text{Disc}(k)^{1/2+\epsilon},$$

by the trivial bound on $h_3(F/k)$ in Lemma 2.5. Altogether, the total number of S_3-extensions is now $O_{[k:\mathbb{Q}],\epsilon}(n^{1/2+\epsilon} h_2(k) \text{Disc}(k)^{1/2+\epsilon})$, as claimed. As above, we can bound the number of C_3-extensions F/k by $O_{[k:\mathbb{Q}],\epsilon}(n^\epsilon h_3(k))$ and the lemma follows. $\square$

Summing Lemma 3.5 over integers n immediately yields Proposition 3.4.

3.2 Large range: the Shintani zeta function

In this section, we are going to give a better bound for $N_k(S_3, X)$ when X is very large compared to $\text{Disc}(k)$. The main idea is to use the bound in Lemma 3.5 to get a better estimate on $N_k(S_3, X)$ using *Shintani zeta functions* over a general number field k. Moreover, the upper bound we obtain in this section is also an upper bound on the number of cubic rings over k, not just cubic fields. This will be important in Section 3.3.

Given a number field k, Shintani zeta functions over k count *cubic rings* over k with a specified signature. More specifically, given a cubic ring R over k (that is, a ring that is a locally free rank three $\mathcal{O}_k$-module), let $\text{disc}(R/\mathcal{O}_k)$ denote the relative discriminant ideal of R and $\text{Disc}(R/\mathcal{O}_k) = \text{Nm}_{k/\mathbb{Q}}(\text{disc}(R/\mathcal{O}_k))$. For each archimedean place v of k, let k_v be the completion of k at v, and let $R_v := R \otimes_{\mathcal{O}_k} k_v$. Each R_v is a cubic étale algebra over k_v. If $k_v \simeq \mathbb{C}$, then there is only one such cubic étale algebra $\mathbb{C}^3$, while if $k_v \simeq \mathbb{R}$, then either $R_v \simeq \mathbb{R}^3$ or $R_v \simeq \mathbb{R} \times \mathbb{C}$. The signature of R is the tuple $\text{sgn}(R) = (R_v)_{v|\infty}$ that records the isomorphism class of each R_v.

We will use $N_k^3(X)$ to denote the number of isomorphism classes of cubic rings K/k over a number field k with $0 < \text{Disc}(K/k) \leq X$, and $N_{k,\alpha}^3(X)$ to denote the number of isomorphism classes of cubic rings K/k over a number field k with $0 < \text{Disc}(K/k) \leq X$ with signature α. Then the main proposition we are going to prove for this subsection is as follows.

Proposition 3.6. *For any number field k and $X \geq \text{Disc}(k)^3 h_2(k)^{2/3}$, we have*

$$N_k^3(X) \ll_{[k:\mathbb{Q}],\epsilon} \text{Disc}(k)^\epsilon X.$$

We start by introducing properties of Shintani zeta functions over a general number field, including all useful notations. For a fixed signature α, let

$$\xi_{k,\alpha}(s) := \sum_{\substack{R/\mathcal{O}_k: \\ \text{Disc}(R/\mathcal{O}_k) \neq 0, \\ \text{sgn}(R) = \alpha}} \frac{|\text{Aut}_{\mathcal{O}_k}(R)|^{-1}}{\text{Disc}(R/\mathcal{O}_k)^s},$$

11

where the sum runs over isomorphism classes of cubic rings R over k.

Let $\zeta_k(s)$ be the Dekekind zeta function of k. For convenience in what is to come, we define

$$\mathfrak{A}_k := \frac{\zeta_k(2)\operatorname{Res}_{s=1}\zeta_k(s)}{2^{r_1(k)+r_2(k)+1}} \text{ and } \mathfrak{B}_k := \frac{3^{r_1(k)+r_2(k)/2}\zeta_k(1/3)\operatorname{Res}_{s=1}\zeta_k(s)}{6 \cdot 2^{r_1(k)+r_2(k)}\operatorname{Disc}(k)^{1/2}}\left(\frac{\Gamma(1/3)^3}{2\pi}\right)^{[k:\mathbb{Q}]}.$$

Additionally, for each pair of signatures α, β and each infinite place $v \mid \infty$ of k, we define a factor $c_{v,\alpha\beta}(s)$ as follows. If $k_v \simeq \mathbb{C}$, set $c_{v,\alpha\beta}(s) = \sin^2(\pi s)\sin(\pi s - \pi/6)\sin(\pi s + \pi/6)$. If $k_v \simeq \mathbb{R}$ and $\alpha_v \simeq \beta_v$, set $c_{v,\alpha\beta}(s) = \sin(2\pi s)/2$. In the remaining cases, set

$$c_{v,\alpha\beta}(s) = \frac{1}{2}\begin{cases} 3\sin(\pi s), & \text{if } \alpha_v \simeq \mathbb{R}^3, \beta_v \simeq \mathbb{R} \times \mathbb{C}, \\ \sin(\pi s), & \text{if } \alpha_v \simeq \mathbb{R} \times \mathbb{C}, \beta_v \simeq \mathbb{R}^3, \end{cases} \tag{3.1}$$

and define $c_{\alpha\beta}(s) := \prod_{v\mid\infty} c_{v,\alpha\beta}(s)$.

The basic properties of $\xi_{k,\alpha}(s)$ are recorded in the following proposition that collects results due to Shintani [Shi72], Wright [Wri82, Wri85], and Datskovsky and Wright [DW86]. We also refer the interested reader to the work of Taniguchi [Tan06] for more information.

Proposition 3.7. *We have the following properties for Shintani zeta functions over a general number field k:*

1. *For each number field k and each signature α, the function $\xi_{k,\alpha}(s)$ converges absolutely in the region $\Re(s) > 1$.*

2. *The function $\xi_{k,\alpha}(s)$ has a meromorphic continuation to $\mathbb{C}$ with poles only at $s = 1$ and $s = 5/6$. Each of these poles is simple, with residues*

$$\mathfrak{A}_k \cdot (1 + 3^{-r(\alpha)-r_2(k)}) \text{ and } \mathfrak{B}_k \cdot 3^{-r(\alpha)/2}$$

   respectively, where $r(\alpha) = \#\{v \mid \infty : \alpha_v \simeq \mathbb{R}^3\}$.

3. *The function $\xi_{k,\alpha}(s)$ satisfies a functional equation,*

$$\xi_{k,\alpha}(1-s) = \left(\frac{3^{(6s-2)}}{\pi^{4s}}\Gamma(s)^2\Gamma(s-1/6)\Gamma(s+1/6)\right)^{[k:\mathbb{Q}]}\operatorname{Disc}(k)^{4s-2}\sum_\beta c_{\alpha\beta}(s)\hat{\xi}_{k,\beta}(s),$$

   where the sum runs over possible signatures β and where $\hat{\xi}_{k,\beta}(s)$ is the dual Shintani zeta function defined via the Dirichlet series

$$\hat{\xi}_{k,\beta}(s) = \sum_{\substack{R/\mathcal{O}_k: \\ \operatorname{Disc}(R/\mathcal{O}_k)\neq 0 \\ \operatorname{sgn}(R)=\beta \\ 3\mid\operatorname{tr}(t)\,\forall t\in R}} \frac{|\operatorname{Aut}_{\mathcal{O}_k}(R)|^{-1}}{\operatorname{Disc}(R/\mathcal{O}_k)^s},$$

   where the sum runs over isomorphism classes of cubic rings R over k.

4. *For each α, the function $\hat{\xi}_{k,\alpha}(s)$ has a meromorphic continuation to all of $\mathbb{C}$ with poles at $s = 1$ and $s = 5/6$ (both simple), and satisfies the inequality $\hat{\xi}_{k,\alpha}(s) < \xi_{k,\alpha}(s)$ for real $s > 1$.*

5. *For each α, the functions $(s-1)(s-5/6)\xi_{k,\alpha}(s)$ and $(s-1)(s-5/6)\hat{\xi}_{k,\alpha}(s)$ are entire of order 1.*

Proof. We provide references for these claims without regard to necessarily providing the original reference. The first claim follows from [Wri85, Theorem 4.1]. The second through fourth primarily follow from [DW86, Theorem 6.2], with the claim that $\hat{\xi}_{k,\alpha}(s) < \xi_{k,\alpha}(s)$ for real $s > 1$ following from the absolute convergence of $\xi_{k,\alpha}(s)$ in this region. The fifth follows from a generalization of [Shi72, Theorem 2.1.iii] as is explained on [Wri82, pg. 96]. $\qquad\square$

We next record one more useful property of $\xi_{k,\alpha}(s)$.

Lemma 3.8. *If k has degree at least 2, then $\xi_{k,\alpha}(0) = 0$ for each signature α.*

Proof. From the formulas given, it follows that each $c_{\alpha\beta}(s)$ has a zero of order $[k : \mathbb{Q}]$ at $s = 1$. The claim then follows from the functional equation for $\xi_{k,\alpha}(s)$. $\square$

While Proposition 3.7 establishes that $\xi_{k,\alpha}(s)$ converges absolutely in the region $\Re(s) > 1$, it does not guarantee that this convergence is uniform in k. To control this uniformity, we must control the number of cubic rings over k with small discriminant. This will essentially be afforded to us by Proposition 3.4 on the number of small discriminant cubic algebras over k, except that $\xi_{k,\alpha}(s)$ counts all orders in cubic étale algebras over k, not just the maximal orders. We will later exploit this overcounting in the proof of Proposition 3.15, but for now, we simply record the following result of Datskovsky and Wright [DW86, Theorem 6.1] in order to track the number of orders in a cubic étale algebra A/k.

Lemma 3.9 (Datskovsky–Wright). *Let A be a cubic étale algebra over k with maximal order $\mathcal{O}_A$. Thus, either $A \simeq k^3$, $A \simeq F \times k$ where F/k is a quadratic extension, or $A \simeq K$ where K/k is a relative cubic field extension. For each n, let a_n denote the number of orders $\mathcal{O} \subset A$ for which $[\mathcal{O}_A : \mathcal{O}]^2 = n$, equivalently, the number of orders $\mathcal{O} \subset A$ for which $\mathrm{Disc}(\mathcal{O}/\mathcal{O}_k) = \mathrm{Disc}(\mathcal{O}_A/\mathcal{O}_k) \cdot n$. Then the Dirichlet series $f_A(s) := \sum_n a_n n^{-s}$ satisfies*

$$f_A(s) = \zeta_k(4s)\zeta_k(6s - 1)\frac{\zeta_A(2s)}{\zeta_A(4s)},$$

where

$$\zeta_A(s) = \begin{cases} \zeta_k(s)^3, & \text{if } A \simeq k^3, \\ \zeta_k(s)\zeta_F(s), & \text{if } A \simeq F \times k, \\ \zeta_K(s), & \text{if } A \simeq K, \end{cases}$$

with notation as above, and where for a number field L, $\zeta_L(s)$ denotes the Dedekind zeta function of L.

Combining Lemma 3.9 and Lemma 3.5, we derive the following lemma on the values of Shintani zeta function in a right half-plane.

Lemma 3.10. *For any real $\sigma > 3/2$ and any $t \in \mathbb{R}$, we have $\xi_{k,\alpha}(\sigma + it) \ll_{[k:\mathbb{Q}],\sigma,\epsilon} \mathrm{Disc}(k)^{1/2+\epsilon}h_2(k)$.*

Proof. By the triangle inequality, it suffices to prove the lemma when $t = 0$. Assume $\sigma > 3/2$ is given. With the notation of Lemma 3.9, for any cubic étale algebra A, we have $\zeta_A(\sigma) \leq \zeta_k(\sigma)^3$ whenever $\sigma > 1$. It follows that

$$\begin{aligned} \xi_{k,\alpha}(\sigma) &\leq \sum_{[L:k]\leq 3} \frac{1}{\mathrm{Disc}(L/k)^\sigma} \cdot \zeta_k(4\sigma)\zeta_k(6\sigma - 1)\frac{\zeta_A(2\sigma)}{\zeta_A(4\sigma)} \\ &\leq \zeta_k(2\sigma)^3\zeta_k(4\sigma)\zeta_k(6\sigma - 1) \sum_{[L:k]\leq 3} \frac{1}{\mathrm{Disc}(L/k)^\sigma}, \end{aligned} \tag{3.2}$$

where the sum runs over isomorphism classes of field extensions L/k of degree at most 3. The second inequality comes from $\zeta_A(4\sigma) \geq 1$, valid for $\sigma > 1$. The factors of $\zeta_k(\sigma)$ may be bounded by suitable powers of the Riemann zeta function $\zeta(\sigma)$, depending only on the degree of $k/\mathbb{Q}$. So it suffices to understand the Dirichlet series of field discriminants. By Lemma 3.5, we then find that for any $\epsilon < \sigma - 3/2$,

$$\sum_{L/k} \frac{1}{\mathrm{Disc}(L/k)^\sigma} \ll_{[k:\mathbb{Q}],\epsilon} h_2(k)\mathrm{Disc}(k)^{1/2+\epsilon} \sum_n \frac{n^{1/2+\epsilon}}{n^\sigma} \ll_{[k:\mathbb{Q}],\epsilon} \mathrm{Disc}(k)^{1/2+\epsilon}h_2(k)\zeta(\sigma - 1/2 - \epsilon),$$

yielding the lemma. $\square$

Next, we apply the functional equation to deduce a discriminant-aspect "convexity bound" for the Shintani zeta function.

Lemma 3.11. *For any $-1/2 \leq \sigma \leq 3/2$ and any $t \in \mathbb{R}$, the Shintani zeta function satisfies*

$$\xi_{k,\alpha}(\sigma + it) = O_{[k:\mathbb{Q}],\epsilon}(h_2(k)\mathrm{Disc}(k)^{\frac{7}{2}-2\sigma+\epsilon}(1 + |t|)^{2[k:\mathbb{Q}](\frac{3}{2}-\sigma)+\epsilon}).$$

Proof. Let $\delta > 0$ be small. For $\sigma = 3/2 + \delta$, it follows from Lemma 3.10 that

$$\xi_k(\sigma + it) \ll_{[k:\mathbb{Q}],\delta,\epsilon} \operatorname{Disc}(k)^{1/2+\epsilon} h_2(k).$$

For $s = \sigma + it$ with $\sigma = 3/2 + \delta$, we apply the functional equation and Stirling's formula to extract cancellation between the gamma factors and the $c_{\alpha\beta}(s)$ in order to find also

$$\xi_{k,\alpha}(1-s) = \left(\frac{3^{(6s-2)}}{\pi^{4s}} \Gamma(s)^2 \Gamma(s-1/6)\Gamma(s+1/6) \right)^{[k:\mathbb{Q}]} \operatorname{Disc}(k)^{4s-2} \sum_\beta c_{\alpha\beta}(s)\hat{\xi}_{k,\beta}(s)$$

$$\ll_{[k:\mathbb{Q}],\delta,\epsilon} (1+|t|)^{(4+4\delta)[k:\mathbb{Q}]+\epsilon} \operatorname{Disc}(k)^{9/2+4\delta+\epsilon} h_2(k).$$

The general result follows upon using the Phragmen–Lindelöf principle [IK04, Theorem 5.53] applied to the function $\frac{(s-1)(s-5/6)}{(s+1)^2} \xi_{k,\alpha}(s)$ and letting δ be sufficiently small. Specifically, we find for any $-1/2 - \delta < \sigma < 3/2 + \delta$ that

$$\xi_{k,\alpha}(\sigma + it) \ll_{[k:\mathbb{Q}],\delta,\epsilon} (1+|t|)^{2[k:\mathbb{Q}](\frac{3}{2}+\delta-\sigma)+\epsilon} \operatorname{Disc}(k)^{\frac{7}{2}+2\delta-2\sigma+\epsilon}.$$

Upon choosing $\delta = \epsilon$ and then replacing ϵ in the equation above by $\epsilon/(1 + 2[k : \mathbb{Q}])$, we obtain the required statement. $\square$

Now we apply the functional equation in Proposition 3.7 and the above lemmas to bound the number of cubic rings $N^3_{k,\alpha}(X)$.

Proof of Proposition 3.6. Let $\phi(x)$ be a positive smooth function satisfying $\phi(x) \geq 1$ whenever $0 \leq x \leq 1$ and whose Mellin transform exhibits rapid decay away from the real axis; for example, we may take $\phi(x) = e^{1-x}$. Letting R run over cubic rings over k, we have

$$N^3_{k,\alpha}(X) = \sum_{\substack{0 < \operatorname{Disc}(R/\mathcal{O}_k) \leq X \\ \operatorname{sgn}(R) = \alpha}} 1 \ll_\phi \sum_{\substack{0 < \operatorname{Disc}(R/\mathcal{O}_k) \\ \operatorname{sgn}(R) = \alpha}} \frac{\phi(\operatorname{Disc}(R/\mathcal{O}_k)/X)}{|\operatorname{Aut}_{\mathcal{O}_k}(R)|}.$$

This latter term may be evaluated via Perron's formula and the full Shintani zeta function $\xi_{k,\alpha}(s)$,

$$\sum_{\substack{0 < \operatorname{Disc}(R/\mathcal{O}_k) \\ \operatorname{sgn}(R) = \alpha}} \frac{\phi(\operatorname{Disc}(R/\mathcal{O}_k)/X)}{|\operatorname{Aut}_{\mathcal{O}_k}(R)|} = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \xi_{k,\alpha}(s)\Phi(s)X^s \, ds,$$

where $\Phi(s)$ is the Mellin transform of $\phi(x)$. By Lemma 3.11, the exponential decay of $\Phi(s)$ off the real axis allows us to shift the contour to the line $\Re(s) = -1/2 - \epsilon$ for any $\epsilon > 0$. Doing so, we must account for the poles of $\xi_{k,\alpha}(s)$ at $s = 1$ and $s = 5/6$ and of $\Phi(s)$ at $s = 0$. From Proposition 3.7, it follows that the contribution from the pole at $s = 1$ subsumes that of the pole at $s = 5/6$. Moreover, Lemma 3.8 shows that in fact the integrand has no pole at $s = 0$ owing to the zero of $\xi_{k,\alpha}(s)$ at $s = 0$. Altogether, the contribution from the poles is seen to be $O_{[k:\mathbb{Q}]}(X \cdot \operatorname{Res}_{s=1}\zeta_k(s))$.

Finally, appealing to the functional equation and Lemma 3.10, we find

$$\frac{1}{2\pi i} \int_{-1/2-\epsilon-i\infty}^{-1/2-\epsilon+i\infty} \xi_{k,\alpha}(s)\Phi(s)X^s \, ds$$

$$= \frac{1}{2\pi i} \int_{3/2+\epsilon-i\infty}^{3/2+\epsilon+i\infty} \left(\frac{3^{(6s-2)}}{\pi^{4s}} \Gamma(s)^2 \Gamma(s-1/6)\Gamma(s+1/6) \right)^{[k:\mathbb{Q}]} \operatorname{Disc}(k)^{4s-2}\hat{\xi}(s)\Phi(1-s)X^{1-s} \, ds$$

$$\ll_{[k:\mathbb{Q}],\epsilon} \operatorname{Disc}(k)^{9/2+\epsilon} h_2(k)X^{-1/2-\epsilon},$$

where $\hat{\xi}(s) = \sum_\beta c_{\alpha\beta}(s)\hat{\xi}_{K,\beta}(s)$.

We conclude that for any number field k and any $X \geq 1$, we have

$$N^3_{k,\alpha}(X) \ll_{[k:\mathbb{Q}],\epsilon} X \cdot \operatorname{Res}_{s=1}\zeta_k(s) + X^{-1/2-\epsilon} h_2(k)\operatorname{Disc}(k)^{9/2+\epsilon}. \tag{3.3}$$

Using the well-known upper bound $\operatorname{Res}_{s=1}\zeta_k(s) \ll_{[k:\mathbb{Q}],\epsilon} \operatorname{Disc}(k)^\epsilon$ due to Landau (see also [Bra47, Lemma 3]), we conclude the proposition. $\square$

3.3 Intermediate range: propagation of orders

In this section, our main proposition is the following bound on $N_k(S_3, X)$ that is better than both Proposition 3.4 and 3.6 when X is a bit smaller than the region allowed by Proposition 3.6. Let $\kappa_k :=$ $\text{Res}_{s=1}\zeta_k(s)$.

Proposition 3.12. *Let k a number field and let $X \geq 1$. We have*

$$N_k(S_3, X) \ll_{[k:\mathbb{Q}],\epsilon} \text{Disc}(k)^{1/2+\epsilon}\kappa_k^{-2}X^{1/2}(\text{Disc}(k)h_2(k)^{1/3} + X^{1/2}).$$

The key idea is that Proposition 3.6 actually gives an upper bound on the number of cubic rings over k instead of cubic fields, and if there are too many cubic fields in this intermediate range, then the orders inside these fields would overrun these bounds. We will first apply this idea to bound the average 3-class number of quadratic extensions of k, and then we apply class field theory to bound the number $N_k(S_3, X)$ of general S_3 cubic fields.

We begin with the following lemma.

Lemma 3.13. *Let F/k be a quadratic extension of number fields, and let $\mathcal{R}(F)$ denote the set of isomorphism classes of cubic rings R over k whose underlying cubic étale algebra $A := R \otimes_{\mathbb{Q}} k$ has discriminant $\text{disc}(F/k)$ and is either of the form $A \simeq k \times F$ or $A \simeq K$ for a non-Galois cubic extension K/k with quadratic resolvent F/k. Then we have*

$$\sum_{R \in \mathcal{R}(F)} \frac{|\text{Aut}_k(A)|^{-1}}{\text{Disc}(R/\mathcal{O}_k)^s} = \frac{h_3(F/k)}{2\text{Disc}(F/k)^s}\zeta_k(2s)\zeta_k(6s-1) \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_F \text{ sq.free} \\ [\mathfrak{a}] \in 3\text{Cl}_F + \text{Cl}_k}} \frac{1}{\text{Nm}(\mathfrak{a})^{2s}},$$

where the summation on the right-hand side runs over those squarefree ideals of $\mathcal{O}_F$ whose classes are in the subgroup $3\,\text{Cl}_F + \text{Cl}_k \subseteq \text{Cl}_F$.

Proof. If $R \in \mathcal{R}(F)$, then $\text{Disc}(R/\mathcal{O}_k) = \text{Disc}(F/k)[\mathcal{O}_A : R]^2$. Thus, with the notation of Lemma 3.9, we have

$$\sum_{R \in \mathcal{R}(F)} \frac{|\text{Aut}_k(A)|^{-1}}{\text{Disc}(R/\mathcal{O}_k)^s} = \text{Disc}(F/k)^{-s} \cdot \left(\frac{1}{2}f_{k \times F}(s) + \sum_{\substack{[K:k]=3 \\ \text{disc}(K/k)=\text{disc}(F/k) \\ F \subseteq \widetilde{K}/k}} f_K(s) \right).$$

Note that the summation on the right is restricted to those cubic extensions K/k with quadratic resolvent F and which satisfy $\text{disc}(K/k) = \text{disc}(F/k)$. For each such K/k, by Lemma 3.9 we have

$$f_K(s) = \zeta_k(4s)\zeta_k(6s-1)\frac{\zeta_K(2s)}{\zeta_K(4s)} = \zeta_k(2s)\zeta_k(6s-1)\frac{L(2s, \chi_{\widetilde{K}/F})}{L(4s, \chi_{\widetilde{K}/F})}, \tag{3.4}$$

where $\widetilde{K}$ is the Galois closure of K over k, and $\chi_{\widetilde{K}/F}$ is one of the non-trivial cyclic cubic characters of the class group $\mathcal{C} = \text{Cl}_F/\text{Cl}_k$ that cuts out $\widetilde{K}/F$. The second equality comes from the relation $\zeta_K(s)/\zeta_k(s) = L(s, \chi_{\widetilde{K}/F})$. In fact, we have $L(s, \chi_{\widetilde{K}/F}) = L(s, \chi^2_{\widetilde{K}/F}) = L(s, \overline{\chi}_{\widetilde{K}/F})$, since all are equal to the irreducible degree 2 Artin L-function of K/k. Thus, we obtain also

$$f_K(s) = \zeta_k(2s)\zeta_k(6s-1)\frac{L(2s, \chi_{\widetilde{K}/F})}{L(4s, \chi^2_{\widetilde{K}/F})}.$$

Meanwhile, the Dirichlet series for orders inside $F \times k$ is

$$f_{F \times k}(s) = \zeta_k(2s)\zeta_k(6s-1)\frac{\zeta_F(2s)}{\zeta_F(4s)}. \tag{3.5}$$

Notice that $\zeta_F(s)$ is the L-function attached to the trivial character of $\mathcal{C}$. Therefore,

$$\sum_{R \in \mathcal{R}(F)} \frac{|\mathrm{Aut}_k(A)|^{-1}}{\mathrm{Disc}(R/\mathcal{O}_k)^s} = \frac{\zeta_k(2s)\zeta_k(6s-1)}{2\mathrm{Disc}(F/k)^s} \sum_{\chi \in \widehat{\mathcal{C}}[3]} \frac{L(2s, \chi_{\widetilde{K}/F})}{L(4s, \chi^2_{\widetilde{K}/F})}$$

$$= \frac{\zeta_k(2s)\zeta_k(6s-1)}{2\mathrm{Disc}(F/k)^s} \sum_{\mathfrak{a} \subseteq \mathcal{O}_F \text{ sq. free}} \frac{1}{\mathrm{Nm}(\mathfrak{a})^{2s}} \sum_{\chi \in \widehat{\mathcal{C}}[3]} \chi(\mathfrak{a})$$

$$= \frac{h_3(F/k)\zeta_k(2s)\zeta_k(6s-1)}{2\mathrm{Disc}(F/k)^s} \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_F \text{ sq. free} \\ \mathfrak{a} \in 3\,\mathrm{Cl}_F + \mathrm{Cl}_k}} \frac{1}{\mathrm{Nm}(\mathfrak{a})^{2s}},$$

by orthogonality of characters and the relation $|\widehat{\mathcal{C}}[3]| = h_3(F/k)$. $\qquad\square$

We next have the following simple lemma.

Lemma 3.14. *Let k be a number field and let $\delta > 0$. There is an effectively computable constant C, depending at most on δ and $[k : \mathbb{Q}]$, such that for any $X \geq C\mathrm{Disc}(k)^{1/2+\delta}\kappa_k^{-1}$, we have*

$$\#\{\mathfrak{a} \subseteq \mathcal{O}_K \text{ ideal} : \mathrm{Nm}(\mathfrak{a}) \leq X\} \gg_{[k:\mathbb{Q}],\delta} \kappa_k X.$$

Proof. Let $m \geq \frac{[k:\mathbb{Q}]}{2} + 2$ be an integer. Then

$$\#\{\mathfrak{a} \subseteq \mathcal{O}_K \text{ ideal} : \mathrm{Nm}(\mathfrak{a}) \leq X\} \geq \sum_{\mathrm{Nm}(\mathfrak{a}) \leq X} \left(1 - \frac{\mathrm{Nm}(\mathfrak{a})}{X}\right)^m = \frac{m!}{2\pi i} \int_{2-i\infty}^{2+i\infty} \zeta_k(s) X^s \frac{ds}{s(s+1)\ldots(s+m)}.$$

The convexity bound for $\zeta_k(s)$ (see [IK04, Equation (5.20)], for example) implies that when $\sigma := \Re(s)$ lies in the critical strip $0 \leq \sigma \leq 1$, we have

$$(s-1)\zeta_k(s) \ll_{[k:\mathbb{Q}],\epsilon} \mathrm{Disc}(k)^{(1-\sigma)/2+\epsilon}(1+|s|)^{\frac{[k:\mathbb{Q}](1-\sigma)}{2}+1+\epsilon}. \tag{3.6}$$

Thus, the integral above conveges absolutely when the line of integration is moved anywhere inside the critical strip. Taking it arbitrarily close to the line $\Re(s) = 0$, we conclude that

$$\#\{\mathfrak{a} \subseteq \mathcal{O}_K \text{ ideal} : \mathrm{Nm}(\mathfrak{a}) \leq X\} \gg_{[k:\mathbb{Q}],\epsilon} X \cdot \mathrm{Res}_{s=1}\zeta_k(s) + O(X^\epsilon \mathrm{Disc}(k)^{\frac{1}{2}+\epsilon}).$$

The result follows. $\qquad\square$

We can now apply our count of orders to get an upper bound on the average 3-class number of quadratic extensions.

Proposition 3.15. *Let k a number field and let $X \geq 1$. We have*

$$\sum_{\substack{[F:k]=2 \\ \mathrm{Disc}(F/k) \leq X}} h_3(F/k) \ll_{[k:\mathbb{Q}],\epsilon} \mathrm{Disc}(k)^{1/2+\epsilon}\kappa_k^{-2}X^{1/2}(\mathrm{Disc}(k)h_2(k)^{1/3} + X^{1/2}).$$

Proof. Let Y be given by

$$Y := \max\left\{\mathrm{Disc}(k)^3 h_2(k)^{2/3}, \kappa_k^{-2} X C^2 \mathrm{Disc}(k)^{1+\epsilon}\right\}, \tag{3.7}$$

where C is the constant from Lemma 3.14. For each quadratic extension F/k with discriminant at most X, we consider the contribution to $N_k^3(Y)$ from the orders in the family $\mathcal{R}(F)$ from Lemma 3.13. For any $R \in \mathcal{R}(F)$, any ring automorphism extends to an automorphism of the étale algebra $A = R \otimes_{\mathbb{Q}} k$. Thus, $|\mathrm{Aut}_{\mathcal{O}_k}(R)| \leq |\mathrm{Aut}_k(A)|$, and we obtain an inequality of generating functions,

$$\sum_{R \in \mathcal{R}(F)} \frac{|\mathrm{Aut}_{\mathcal{O}_k}(R)|^{-1}}{\mathrm{Disc}(R/\mathcal{O}_k)^s} \geq \sum_{R \in \mathcal{R}(F)} \frac{|\mathrm{Aut}_k(A)|^{-1}}{\mathrm{Disc}(R/\mathcal{O}_k)^s},$$

16

which is the Dirichlet series from Lemma 3.13. Appealing to Lemma 3.13, this series is in turn bounded below by

$$\frac{h_3(F/k)}{2\mathrm{Disc}(F/k)^s}\zeta_k(2s)\zeta_k(6s-1) \geq \frac{h_3(F/k)}{2\mathrm{Disc}(F/k)^s}\zeta_k(2s),$$

since the summation over ideals $\mathfrak{a}$ has non-negative coefficients. It then follows from our assumption $Y \geq \kappa_k^{-2}XC^2\mathrm{Disc}(k)^{1+\epsilon}$ that we may appeal to Lemma 3.14 (with $X = Y^{1/2}/\mathrm{Disc}(F/k)^{1/2}$) to find that the contribution to $N_k^3(Y)$ of orders arising in $\mathcal{R}(F)$ is

$$\gg_{[k:\mathbb{Q}],\epsilon} \frac{h_3(F/k)Y^{1/2}\kappa_k}{\mathrm{Disc}(F/k)^{1/2}}.$$

Thus,

$$N_k^3(Y) \gg_{[k:\mathbb{Q}],\epsilon} \sum_{\substack{[F:k]=2 \\ X/2 \leq \mathrm{Disc}(F/k) \leq X}} \frac{h_3(F/k)Y^{1/2}\kappa_k}{\mathrm{Disc}(F/k)^{1/2}},$$

and we conclude that

$$\sum_{\substack{[F:k]=2 \\ X/2 \leq \mathrm{Disc}(F/k) \leq X}} h_3(F/k) \ll_{[k:\mathbb{Q}],\epsilon} \frac{N_k^3(Y)X^{1/2}}{Y^{1/2}\kappa_k}.$$

Finally, by Proposition 3.6, we have $N_k^3(Y) \ll_{[k:\mathbb{Q}],\epsilon} \mathrm{Disc}(k)^{\epsilon/2}Y$ whenever $Y \geq \mathrm{Disc}(k)^3h_2(k)^{2/3}$, and the result follows using dyadic summation and the fact that $\kappa_k \ll_{[k:\mathbb{Q}],\epsilon} \mathrm{Disc}(k)^{\epsilon/2}$. $\qquad\square$

Proof of Proposition 3.12. Following the proof of Lemma 6.2 in [DW88], for a square-free ideal $\mathfrak{q}$ of k of norm $\mathrm{Nm}\,\mathfrak{q} \leq X^{1/2}$, the number of S_3 cubic fields K/k with quadratic resolvent F/k and $\mathrm{disc}(K/k) = \mathfrak{q}^2\,\mathrm{disc}(F/k)$ is bounded by $O(4^{\omega(\mathfrak{q})}h_3(F/k))$, where $\omega(\mathfrak{q})$ denotes the number of prime ideals dividing $\mathfrak{q}$. Thus, for fixed $\mathfrak{q}$, the number of S_3-extensions K/k with $\mathrm{disc}(K/k) \leq X$ whose discriminant is $\mathfrak{q}^2$ times that of their quadratic resolvent, may be bounded by a uniform constant times

$$\sum_{\substack{[F:k]=2 \\ \mathrm{Disc}(F/k) \leq X/\mathrm{Nm}(\mathfrak{q})^2}} 4^{\omega(\mathfrak{q})}h_3(F/k) \ll_{[k:\mathbb{Q}],\epsilon} 4^{\omega(\mathfrak{q})}\mathrm{Disc}(k)^{1/2+\epsilon}\kappa_k^{-2}\left(\frac{\mathrm{Disc}(k)h_2(k)^{1/3}X^{1/2}}{\mathrm{Nm}(\mathfrak{q})} + \frac{X}{\mathrm{Nm}(\mathfrak{q})^2}\right),$$

the latter inequality provided by Proposition 3.15.

When $X \geq \mathrm{Disc}(k)^2h_2(k)^{2/3}$, the expression is parentheses above is bounded by twice the second term, and adding the above inequality across $\mathfrak{q}$ with norm at most $X^{1/2}$, we have

$$N_k(S_3, X) \ll_{[k:\mathbb{Q}],\epsilon} \mathrm{Disc}(k)^{1/2+\epsilon}\kappa_k^{-2}X.$$

Otherwise, $X \leq \mathrm{Disc}(k)^3$, and adding over $\mathfrak{q}$ have have

$$N_k(S_3, X) \ll_{[k:\mathbb{Q}],\epsilon} \mathrm{Disc}(k)^{3/2+\epsilon}\kappa_k^{-2}h_2(k)^{1/3}X^{1/2+\epsilon} \ll_{[k:\mathbb{Q}],\epsilon} \mathrm{Disc}(k)^{3/2+4\epsilon}\kappa_k^{-2}h_2(k)^{1/3}X^{1/2},$$

and the proposition follows. $\qquad\square$

3.4   Proof of Theorem 3.1

We can now combine our results in the various ranges to prove Theorem 3.1. By the bijection between 3-torsion elements in relative class groups of quadratic extensions and S_3 relative cubic extensions with square-free discriminant ideal [DW88, Section 5], we have

$$\sum_{\substack{[F:k]=2 \\ \mathrm{Disc}(F/k) \leq X}} h_3(F_2/k) \leq 2N_k(S_3, X) + N_k(C_2, X). \tag{3.8}$$

Using this, the first case follows directly from Proposition 3.4. The second and third cases follow from Propositions 3.15 and 3.12 and the fact that $\mathrm{Res}_{s=1}\zeta_k(s) \gg_{[k:\mathbb{Q}],\epsilon} \mathrm{Disc}(k)^{-\epsilon}$ (though, this is only known to hold with an effectively computable implied constant when $\zeta_k(s)$ does not have an exceptional Landau–Siegel zero; see [Sta74]). The fifth case follows from (3.8) and Proposition 3.6, and the fourth from the observation that $N_k(S_3, X) \leq N_k(S_3, D_k^3h^{2/3})$ for any $X \leq D_k^3h^{2/3}$ (and analogously for class numbers).

4 Zero-density estimates for ray class L-functions

In this section, we collect the results we need on zero-density estimates for ray class L-functions and use them to show that most quadratic extensions will have sufficiently many small split primes. This will allow us to apply our relative Ellenberg–Venkatesh Lemma 2.1 and get a non-trivial bound on $h_3(F/k)$ for most quadratic F/k.

Let χ be a nontrivial ray class character of a number field k with conductor $\mathfrak{f}_\chi$. The associated L-function $L(s, \chi)$ is defined by

$$L(s, \chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\mathrm{Nm}(\mathfrak{a})^s},$$

the series running over the integral ideals of k. Let $r_1^+(\chi)$ denote the number of real places of k that are split in the cyclic extension of k cut out by χ, let $r_1^-(\chi)$ denote the number of real places that are ramified in the extension, and let r_2 denote the number of complex places of k. If we define

$$\gamma_\chi(s) := \pi^{-[k:\mathbb{Q}]s/2} \Gamma\left(\frac{s}{2}\right)^{r_1^+(\chi)+r_2} \Gamma\left(\frac{s+1}{2}\right)^{r_1^-(\chi)+r_2},$$

then the completed L-function $\Lambda(s, \chi) := (\mathrm{Nm}(\mathfrak{f}_\chi)\mathrm{Disc}(k))^{s/2}\gamma_\chi(s)L(s, \chi)$ is entire and satisfies a functional equation, $\Lambda(1 - s, \chi) = \varepsilon(\chi)\Lambda(s, \bar{\chi})$. The poles of $\gamma_\chi(s)$ thus lend $L(s, \chi)$ its trivial zeros; these are the non-positive even integers with multiplicity $r_1^+(\chi) + r_2$, and the negative odd integers with multiplicity $r_1^-(\chi) + r_2$.

The following lemma summarizes the analytic properties we shall need.

Lemma 4.1. *Assume notation as above and set $q_\chi = \mathrm{Nm}(\mathfrak{f}_\chi)\mathrm{Disc}(k)$. Then:*

1. *For any $t \geq 0$, the number of non-trivial zeros $\rho = \beta + i\gamma$ of $L(s, \chi)$ with $|\gamma - t| \leq 1$ is $O_{[k:\mathbb{Q}]}(\log((t + 1)q_\chi))$.*

2. *For any s with $-3/2 \leq \Re(s) \leq 2$, we have*

$$-\frac{L'}{L}(s, \chi) = -\frac{r_1^+(\chi) + r_2}{s} - \frac{r_1^-(\chi) + r_2}{s+1} - \sum_{\substack{\rho: \\ |s-\rho|<1}} \frac{1}{s - \rho} + O_{[k:\mathbb{Q}]}(\log((|s| + 1)q_\chi)),$$

where the sum runs over the nontrivial zeros ρ of $L(s, \chi)$.

Proof. These are standard properties of L-functions. For example, see Proposition 5.7 in Iwaniec and Kowalski [IK04]. The second conclusion is stated there only for $-1/2 \leq \Re(s) \leq 2$, but in the region $-3/2 \leq \Re(s) \leq -1/2$, the functional equation relates $-\frac{L'}{L}(s, \chi)$ to $-\frac{L'}{L}(1 - s, \bar{\chi})$, which is absolutely convergent. Thus, the conclusion is easier in this case, with the factors arising from the functional equation being dominant. $\square$

We next recall a consequence of Proposition A.2 in the appendix by Lemke Oliver and Thorner to work of Pasten [Pas17], which follows upon taking π to be the trivial representation of k. See also [TZ21, Theorem 1.2] for a somewhat stronger statement, which would allow also $\epsilon = 0$ below with an explicit value of c.

Theorem 4.2. *Let k be a number field, and for any ray class character χ of k, let*

$$N_\chi(\sigma, T) := \#\{\rho : L(\rho, \chi) = 0, \Re(\rho) \in (\sigma, 1), |\Im(\rho)| \leq T\}.$$

Then there is a constant $c > 0$, depending only on the degree $[k : \mathbb{Q}]$, such that for any $Q, T > 1$, any $1/2 \leq \sigma < 1$, and any $\epsilon > 0$, we have

$$\sum_{\mathrm{Nm}(\mathfrak{q}) \leq Q} \sideset{}{'}\sum_{\chi \,(\mathrm{mod}\,\mathfrak{q})} N_\chi(\sigma, T) \ll_{[k:\mathbb{Q}],\epsilon} (\mathrm{Disc}(k)QT)^{c(1-\sigma)+\epsilon}.$$

Here, the outer summation runs over ideals $\mathfrak{q}$ of $\mathcal{O}_k$ with bounded norm and the inner summation runs over primitive ray class characters of conductor $\mathfrak{q}$.

Theorem 4.2 implies that over a general number field k, most ray class L-functions do not have zeros near $s = 1$. Therefore we will utilize Theorem 4.2 to show that for most quadratic extensions over k we can find enough prime ideals with a specified splitting behavior. Recall that $\pi_k(Y)$ denotes the prime ideal counting function of k, and for an extension F/k, $\pi_k(Y; F, e)$ denotes the number of primes in k of norm at most Y that are split in F.

Lemma 4.3. *Let k be a number field and let $\mathcal{F}_2(X)$ be the set of quadratic extensions of k with $\mathrm{Disc}(F/k) \leq X$. Let $c = c_{[k:\mathbb{Q}]}$ be the constant as given in Theorem 4.2. For any $\epsilon_1 > 0$ and $X \geq 2$, there exists a set $\mathcal{E} = \mathcal{E}(k, X, \epsilon_1) \subset \mathcal{F}_2(X)$ of exceptional quadratic extensions F/k such that:*

1. *for all $F \in \mathcal{F}_2(X) \setminus \mathcal{E}$, for all $4 \leq Y \leq X$ there exists a constant $C_{[k:\mathbb{Q}],\epsilon_1}$ depending only on $[k : \mathbb{Q}], \epsilon_1$ such that*
$$\pi_k(Y; F, e) \geq \frac{1}{8}\pi_k(Y/2) - C_{[k:\mathbb{Q}],\epsilon_1} Y^{\sigma_1} \log^2(X \mathrm{Disc}(k)),$$
   where $\sigma_1 = \max(1 - \frac{\epsilon_1}{4c}, 1/2)$; and

2. *$|\mathcal{E}| \ll_{[k:\mathbb{Q}],\epsilon_1} \mathrm{Disc}(k)^{\epsilon_1} X^{\epsilon_1}$.*

Proof. For each quadratic extension F/k, there is a unique quadratic ray class character $\chi_{F/k}$ with conductor $\mathrm{disc}(F/k)$ such that $\frac{\zeta_F(s)}{\zeta_k(s)} = L(s, \chi_{F/k})$. As in the statement of the lemma, we set $\sigma_1 = 1 - \epsilon_1/4c$ and define

$$\mathcal{E} := \{F \in \mathcal{F}_2(X) : \exists \rho \text{ s.t. } L(\rho, \chi_{F/k}) = 0, \Re(\rho) \in (\sigma_1, 1), \text{ and } |\Im(\rho)| \leq X^{1/2}\}.$$

Then Theorem 4.2 implies $|\mathcal{E}| \ll_{[k:\mathbb{Q}],\epsilon_1/4} (\mathrm{Disc}(k)X^{3/2})^{c(1-\sigma_1)+\epsilon_1/4} \ll_{[k:\mathbb{Q}],\epsilon_1} \mathrm{Disc}(k)^{\epsilon_1} X^{\epsilon_1}$.

Suppose $F \notin \mathcal{E}$. In order to bound from below the number of primes of k with $\chi_{F/k}(\mathfrak{p}) = 1$, we first observe that, away from the $O(\log \mathrm{Disc}(F))$ ramified primes, the function $(1 + \chi_{F/k}(\mathfrak{p}))/2$ is precisely 1 or 0 according to whether $\mathfrak{p}$ is split or inert. As is standard, we first consider a version weighted by the von Mangoldt function Λ_k of k, and we observe

$$\sum_{\mathrm{Nm}(\mathfrak{a}) \leq Y} \Lambda_k(\mathfrak{a}) \frac{1 + \chi_{F/k}(\mathfrak{a})}{2} \geq \sum_{\mathrm{Nm}(\mathfrak{a}) \leq Y} \Lambda_k(\mathfrak{a}) \frac{1 + \chi_{F/k}(\mathfrak{a})}{2} \left(1 - \frac{\mathrm{Nm}(\mathfrak{a})}{Y}\right)$$
$$= \frac{1}{2} \sum_{\mathrm{Nm}(\mathfrak{a}) \leq Y} \Lambda_k(\mathfrak{a}) \left(1 - \frac{\mathrm{Nm}(\mathfrak{a})}{Y}\right) + \frac{1}{2} \sum_{\mathrm{Nm}(\mathfrak{a}) \leq Y} \chi_{F/k}(\mathfrak{a})\Lambda_k(\mathfrak{a}) \left(1 - \frac{\mathrm{Nm}(\mathfrak{a})}{Y}\right).$$

The first term is related to $\pi_k(Y)$ by means of partial summation, so our goal is to show that the second is small.

Via Perron's formula, we find

$$\sum_{|\mathfrak{a}| \leq Y} \chi_{F/k}(\mathfrak{a})\Lambda_k(\mathfrak{a}) \left(1 - \frac{\mathrm{Nm}(\mathfrak{a})}{Y}\right) = \frac{-1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{L'}{L}(s, \chi_{F/k}) \cdot \frac{Y^s}{s(s+1)} ds.$$

It follows from Lemma 4.1 and the functional equation that the integral converges absolutely over any vertical line. Thus, we may shift the contour all the way to the left, finding

$$\sum_{\mathrm{Nm}(\mathfrak{a}) \leq Y} \chi_{F/k}(\mathfrak{a})\Lambda_k(\mathfrak{a}) \left(1 - \frac{\mathrm{Nm}(\mathfrak{a})}{Y}\right) = -\sum_{\substack{\rho: \\ L(\rho,\chi)=0 \\ \rho \neq 0, -1}} \frac{Y^\rho}{\rho(\rho+1)} - \mathrm{Res}_0 - \mathrm{Res}_{-1},$$

where the summation runs over all zeros of $L(s, \chi)$, nontrivial or trivial, and where Res_0 and Res_{-1} denote the residues of the integrand at $s = 0$ and $s = -1$, respectively. The trivial zeros of $L(s, \chi_{F/k})$ occur at negative integers, and each has multiplicity at most $[k : \mathbb{Q}]$, so their total contribution to the sum may be bounded uniformly by $O_{[k:\mathbb{Q}]}(Y^{-2})$. Using Lemma 4.1, the residue Res_{-1} is bounded by $O_{[k:\mathbb{Q}]}((\log Y)(\log X\mathrm{Disc}(k))Y^{-1})$, which is sufficient. Again using Lemma 4.1, we see that

$$\mathrm{Res}_0 = -(r_1^+(\chi) + r_2)\log Y + \sum_{\substack{\rho: \\ |\rho| \leq 1}} \frac{1}{\rho} + O_{[k:\mathbb{Q}]}(\log(X\mathrm{Disc}(k)))$$
$$\ll_{[k:\mathbb{Q}]} \frac{\log(X\mathrm{Disc}(k))}{1 - \sigma_1},$$

19

since $F \notin \mathcal{E}$ and $Y \leq X$.

By Lemma 4.1, the summation over zeros of height greater than $T = X^{1/2}$ is bounded

$$\sum_{\substack{\rho: \\ L(\rho,\chi)=0 \\ |\Im(\rho)| \geq T}} \frac{Y^\rho}{\rho(\rho+1)} \ll_{[k:\mathbb{Q}]} \frac{Y \log(X \operatorname{Disc}(k)T)}{T} \ll_{[k:\mathbb{Q}]} Y^{1/2} \log(X \operatorname{Disc}(k)).$$

Notice that by definition of $\mathcal{E}$, for $F \notin \mathcal{E}$ there are no zeros for $L(s, \chi_{F/k})$ with $\Re(\rho) > \sigma_1$ and $|\Im(\rho)| \leq T = X^{1/2}$. Using the functional equation, there are also no zeros with $\Re(\rho) \in (0, 1-\sigma_1)$ and $|\Im(\rho)| \leq T$. The summation over low lying zeroes of $L(s, \chi_{F/k})$ may therefore be bounded by

$$\sum_{\substack{\rho: \\ L(\rho,\chi)=0 \\ |\Im(\rho)| < T}} \frac{Y^\rho}{\rho(\rho+1)} \ll_{[k:\mathbb{Q}]} \frac{Y^{\sigma_1} \log(X \operatorname{Disc}(k)T)}{1-\sigma_1} \ll_{[k:\mathbb{Q}],\epsilon_1} Y^{\sigma_1} \log(X \operatorname{Disc}(k)).$$

Finally, by the standard translation from the von Mangoldt function to the prime counting function, we can conclude the lemma. $\qquad\square$

In order to apply Lemma 4.3 efficiently, we need the following effective lower bound on the number of prime ideals in a general number field k.

Lemma 4.4 ([Zam17]). *There exist absolute, effective constants γ, β, and $D_0 > 0$ such that if k is a number field with $\operatorname{Disc}(k) \geq D_0$, then for $Y \geq \operatorname{Disc}(k)^\beta$, we have*

$$\pi_k(Y) \gg_{[k:\mathbb{Q}]} \frac{1}{\operatorname{Disc}(k)^\gamma} \cdot \frac{Y}{\log Y}.$$

An effective lower bound, weaker than that above, can be derived from [LMO79], but Zaman [Zam17] was the first to prove a bound of this strength; he did so with $\beta = 35$ and $\gamma = 19$. It follows from [TZ17] that $\beta = 694$ and $\gamma = 5$ are also admissible, and from [TZ19a] that $\gamma = 1/[k : \mathbb{Q}]$ is admissible with an inexplicit value of β.

5   A Uniform Tail Estimate

A 2-*extension* is a G-extension for some 2-group G. In this section, our main goal is to prove the following theorem on a tail estimate for the 3-torsion in class groups of 2-extensions with a uniform dependence on the base field k. It will be the critical input for the proof of our main theorems in Section 6.

Theorem 5.1. *Let k be a number field. For each $m \geq 2$, there exist constants $\delta_m > 0$ and α_m depending at most on m and the degree $[k : \mathbb{Q}]$ such that for any $X, Y > 0$, we have*

$$\sum_{\substack{F_m/F_{m-1}/\cdots/F_1/k \\ \operatorname{Disc}(F_{m-1}) \geq Y \\ X/2 \leq \operatorname{Disc}(F_m) \leq X}} h_3(F_m/k) = O_{\epsilon,[k:\mathbb{Q}],m}\left(\left(\frac{X}{Y^{1-\epsilon}} + X^{1-\delta_m} \right) \cdot \operatorname{Disc}(k)^{\alpha_m} \right), \tag{5.1}$$

where the summation is over all towers $F_m/F_{m-1}/\cdots F_1/F_0 = k$ in $\bar{\mathbb{Q}}$ with F_{i+1}/F_i being quadratic extensions for each $0 \leq i \leq m-1$.

We emphasize the point that Theorem 5.1 is stated with respect to the absolute discriminant, while the results of Section 3 are with respect to the relative discriminant.

Remark 5.2. *The statement of Theorem 5.1 for $m = 1$ is empty except when $Y \leq \operatorname{Disc}(k)$. If $Y \leq \operatorname{Disc}(k)$, the statement for $m = 1$ is non-trivial, but follows from Corollary 3.2, and noting that it is stated with respect to* relative *discriminant, we may take α_1 to be any constant greater than $1/3$.*

Remark 5.3. *For our purposes, the actual values of δ_m and α_m are irrelevant; it suffices to know only that the constants δ_m and α_m exist. However, in the course of the proof, we provide explicit but non-optimal values. This will show that the value of δ_2 may be chosen without dependence on $[k:\mathbb{Q}]$. We choose specific non-optimal values of many related exponents in the course of the proof, because we wish to avoid tracking further dependencies of implied constants that would come with avoiding such choices.*

Note that the tail estimate we prove in Theorem 5.1 handles all 2-extensions due to the following easy lemma.

Lemma 5.4 ([KW20], Lemma 2.3). *Let $n = \ell^r$ be a prime power and $G \subset S_n$ be an ℓ-group and E/F be an extension of number fields with $\mathrm{Gal}(E/F) \cong G$. Then there exists a tower of fields*

$$F = F_0 \subset F_1 \subset \ldots \subset F_{r-1} \subset F_r = E \tag{5.2}$$

such that $\mathrm{Gal}(F_{i+1}/F_i) = C_\ell$ for all $0 \leq i \leq r - 1$.

We will prove Theorem 5.1 first for $m = 2$. Then treating $m = 2$ as the base case, we will apply an inductive proof to prove Theorem 5.1 for general m. For $m = 2$, the theorem requires us to sum over all towers $F_2/F_1/F_0 = k$ of relative quadratic extensions. We will separate the discussion depending on how large $\mathrm{Disc}(F_1)$ is. In Section 5.1, we will consider the summation when $\mathrm{Disc}(F_1)$ is away from $X^{1/3}$ using results established in Section 3. In Section 5.2, we will consider the summation when $\mathrm{Disc}(F_1)$ is near $X^{1/3}$ using results established in Section 2 and 4.

Taking $Y = 1$ in Theorem 5.1, we get the following immediate corollary, essentially an analogue of Corollary 3.2, which will be useful in the induction argument to come.

Corollary 5.5. *Let k be a number field. For each $m \geq 2$, let α_m be the constant from Lemma 5.1. Then for any $X \geq 1$, we have*

$$\sum_{\substack{F_m/F_{m-1}/\cdots/F_1/k \\ X/2 \leq \mathrm{Disc}(F_m) \leq X}} h_3(F_m/k) = O_{[k:\mathbb{Q}],m}\Big(X\,\mathrm{Disc}(k)^{\alpha_m}\Big).$$

5.1 Base Case: Non-critical Range

In this subsection, we will consider the following summation:

$$\sum_{\substack{F_2/F_1/k \\ \mathrm{Disc}(F_1) \in \mathfrak{N}(X,Y) \\ X/2 \leq \mathrm{Disc}(F_2) \leq X}} h_3(F_2/k), \tag{5.3}$$

where $\mathfrak{N}(X,Y) := [Y, X^{1/3-\delta_0}) \cup (X^{1/3+\delta_0}, X^{1/2}]$ for an arbitrary small number δ_0 satisfying $0 < \delta_0 < 1/6$. We regard this range for F_1 as non-critical because the results of Section 3 together with the following lemma on the 2-class number of relative 2-extensions will give the desired bound (Lemma 5.7) in this range.

Lemma 5.6 ([KW20], Theorem 2.7). *Let k be a number field and let F/k be a 2-extension. Then for any $\epsilon > 0$, we have $h_2(F) \ll_{[F:\mathbb{Q}],\epsilon} \mathrm{Disc}(F)^\epsilon h_2(k)^{[F:k]}$.*

Lemma 5.7. *Let k be a number field and let $\delta_0 \in (0, 1/6)$. There exists $\delta > 0$, only depending on δ_0, and an absolute constant $\alpha > 0$ such that for all $X, Y > 0$, we have*

$$\sum_{\substack{F_2/F_1/k \\ \mathrm{Disc}(F_1) \in \mathfrak{N}(X,Y) \\ X/2 \leq \mathrm{Disc}(F_2) \leq X}} h_3(F_2/k) = O_{\epsilon,[k:\mathbb{Q}],\delta_0}\Big(\frac{X}{Y^{1-\epsilon}} + X^{1-\delta}\Big) \cdot \mathrm{Disc}(k)^\alpha, \tag{5.4}$$

where the summation is over all towers $F_2/F_1/F_0 = k$ with F_2/F_1 and F_1/F_0 being relative quadratic extensions and where $\mathfrak{N}(X,Y) = [Y, X^{1/3-\delta_0}) \cup (X^{1/3+\delta_0}, X^{1/2}]$.

Proof of Lemma 5.7. Writing $D := \mathrm{Disc}(F_1)$ and $h := h_2(F_1)$, from Section 3 (and the translation from relative to absolute discriminant), we have

$$\sum_{\substack{F_2/F_1 \\ X/2 \leq \mathrm{Disc}(F_2) \leq X}} h_3(F_2/F_1) \ll_{[k:\mathbb{Q}],\epsilon} h \cdot D^\epsilon \begin{cases} X^{3/2}D^{-5/2}, & \text{for all } D^2 \leq X \leq D^3, \\ X^{1/2}D^{1/2} + XD^{-3/2}, & \text{for all } D^2 \leq X, \\ XD^{-2}, & \text{if } X \geq D^5 h^{2/3}. \end{cases} \tag{5.5}$$

Specifically, the first line follows from Proposition 3.4 and (3.8), the second from Proposition 3.15, and the third from the final case of Theorem 3.1.

We will use the first line of (5.5) for $\mathrm{Disc}(F_1) \in (X^{1/3+\delta_0}, X^{1/2}]$, the second line for $\mathrm{Disc}(F_1) \in [Y_0, X^{1/3-\delta_0})$, and the third line for $\mathrm{Disc}(F_1) \in [Y, Y_0)$, where we choose a value for Y_0 so that we can apply the third line to the range $[Y, Y_0)$ for every F_1/k. In particular, if $C_{[K:\mathbb{Q}]}$ is such that we always have $h(K)^{2/3} \leq C_{[K:\mathbb{Q}]} \mathrm{Disc}(K)$, we can choose $Y_0 = C_{2[k:\mathbb{Q}]}^{-1/6} X^{1/6}$. Applying (5.5) as described and applying Lemma 5.6 to bound h, we find

$$\sum_{\substack{F_2/F_1/k \\ \mathrm{Disc}(F_1) \in \mathfrak{N}(X,Y) \\ X/2 \leq \mathrm{Disc}(F_2) \leq X}} h_3(F_2/k) \ll_{\epsilon',\epsilon,[k:\mathbb{Q}]} h_2(k)^2 \cdot X^{3/2} \sum_{\substack{F_1/k \\ \mathrm{Disc}(F_1) \in (X^{1/3+\delta_0}, X^{1/2})}} h_3(F_1/k) \mathrm{Disc}(F_1)^{-5/2+\epsilon'}$$

$$+ h_2(k)^2 \cdot X^{1/2} \sum_{\substack{F_1/k \\ \mathrm{Disc}(F_1) \in [Y_0, X^{1/3-\delta_0})}} h_3(F_1/k) \mathrm{Disc}(F_1)^{1/2+\epsilon'}$$

$$+ h_2(k)^2 \cdot X \sum_{\substack{F_1/k \\ \mathrm{Disc}(F_1) \in [Y_0, X^{1/3-\delta_0})}} h_3(F_1/k) \mathrm{Disc}(F_1)^{-3/2+\epsilon'} \tag{5.6}$$

$$+ h_2(k)^2 \cdot X \sum_{\substack{F_1/k \\ \mathrm{Disc}(F_1) \in (Y, Y_0)}} h_3(F_1/k) \mathrm{Disc}(F_1)^{-2+\epsilon}$$

$$\ll_{\epsilon',\epsilon,[k:\mathbb{Q}]} \mathrm{Disc}(k)^{1/3+\epsilon} \cdot \left(X^{1-3\delta_0/2+\epsilon'} + X^{11/12+\epsilon'} + \frac{X}{Y^{1-\epsilon}}\right),$$

where for the last inequality we have applied partial summation and Corollary 3.2, as well as the trivial bound for $h_2(k)$. Then we can choose, for example, $\delta = \min\{\delta_0, 1/15\}$, and $\alpha = 2/5$. Above if we take $\epsilon' = \min\{\delta_0/2, 1/60\}$, then the lemma follows for $0 < \epsilon \leq \alpha - 1/3$, and hence for all $\epsilon > 0$. $\qquad\square$

5.2 Base Case: Critical Range

In this section, we will consider the following summation:

$$\sum_{\substack{F_2/F_1/k \\ \mathrm{Disc}(F_1) \in \mathfrak{C}(X,Y) \\ X/2 \leq \mathrm{Disc}(F_2) \leq X}} h_3(F_2/k), \tag{5.7}$$

where $\mathfrak{C}(X, Y) = \mathfrak{C}(X) = [X^{1/3-\delta_0}, X^{1/3+\delta_0}]$, which we regard as the critical range of $\mathrm{Disc}(F_1)$. In this range, summing the best bound for each F_1 is not sufficient, and we need to extract additional savings from the sum over F_1. We will apply the results developed in Sections 2 and 4 to obtain this savings.

It will be convenient to use the following simple bound on the number of relative quadratic extensions.

Lemma 5.8. *Let k be a number field. Then*

$$N_k(C_2, X) = O_{[k:\mathbb{Q}],\epsilon}(h_2(k) \mathrm{Disc}(k)^\epsilon X).$$

Proof. By class field theory, the number $N_k(C_2, X)$ is bounded by the product of $h_2(k)$ and the number of integral ideals with bounded norm. The latter can be counted by integrating $\zeta_k(s)$. If a_n denotes the number

of integral ideals of norm n, then by Perron's formula we have

$$\sum_{n \leq X} a_n \leq \sum_{n=1}^{\infty} a_n e^{1 - \frac{n}{X}} = \frac{e}{2\pi i} \int_{1+\epsilon-i\infty}^{1+\epsilon+i\infty} \zeta_k(s) \cdot \Gamma(s) \cdot X^s \, ds. \tag{5.8}$$

Shifting the contour integral to $\Re(s) = 1 - \epsilon$ and using the convexity bound (3.6) on $\zeta_k(s)$, we get the upper bound

$$\sum_{n \leq X} a_n = \mathrm{Res}(\zeta_k(s)\Gamma(s)X^s)_{s=1} + O_{[k:\mathbb{Q}],\epsilon}(\mathrm{Disc}(k)^{\epsilon/2} X^{1-\epsilon}) = O_{[k:\mathbb{Q}],\epsilon}(\mathrm{Disc}(k)^{\epsilon} X), \tag{5.9}$$

where the upper bound on the residue of the Dedekind zeta function comes from Landau. $\square$

Lemma 5.9. *Let k be a number field and let $\delta_0 \in (0, 1/100]$. There exists an absolute positive constant δ, and a value α, depending only on $[k : \mathbb{Q}]$, such that for all $X \geq 1$ we have*

$$\sum_{\substack{F_2/F_1/k \\ \mathrm{Disc}(F_1) \in \mathfrak{C}(X) \\ X/2 \leq \mathrm{Disc}(F_2) \leq X}} h_3(F_2/k) = O_{[k:\mathbb{Q}]}\left(X^{1-\delta}\right) \cdot \mathrm{Disc}(k)^{\alpha}, \tag{5.10}$$

where the summation is over all towers $F_2/F_1/F_0 = k$ with F_2/F_1 and F_1/F_0 being relative quadratic extensions and $\mathfrak{C}(X) = [X^{1/3-\delta_0}, X^{1/3+\delta_0}]$.

Proof. We first give the idea of the proof in broad terms to motivate the notation that is to follow. Exploiting the factorization $h_3(F_2/k) = h_3(F_2/F_1)h_3(F_1/k)$, Corollary 3.2 provides strong control on the average of $h_3(F_1/k)$, while Lemma 2.1 provides a non-trivial bound on $h_3(F_2/F_1)$ if there are "enough" small primes that split in F_2/F_1. Lemma 4.4 ensures there are enough small primes in k. Applying Lemma 4.3 twice, we see first that "most" extensions F_1/k have roughly the same number of small primes as k, and then second that in "most" extensions F_2/F_1 for such F_1, many of those small primes are split. This lets us apply Lemma 2.1, and yields the lemma.

To make this precise, and in preparation for applying Lemma 4.3, we let $\delta_1 = 1/20$ and $\epsilon_1 = 1/30$. We set $\sigma_1 = \max(1 - \epsilon_1/4c, 1/2)$, where $c = c_{[k:\mathbb{Q}]}$ is the constant given in Theorem 4.2. Throughout the proof, we will make assumptions on X, including that X is at least any absolute constant necessary to apply the results we use, and then we will handle the remaining values of X at the end of the proof. Applying Lemma 4.3 the first time, we obtain an exceptional set $\mathcal{E}_0 = \mathcal{E}(k, X^{1/3+\delta_0}, \epsilon_1)$. Then for each $F_1/k \notin \mathcal{E}_0$, we apply Lemma 4.3 a second time to obtain an exceptional set $\mathcal{E}(F_1) = \mathcal{E}(F_1, X/\mathrm{Disc}(F_1)^2, \epsilon_1)$. By Lemma 4.3, both exceptional sets contain few elements:

$$|\mathcal{E}_0| \ll_{[k:\mathbb{Q}]} \mathrm{Disc}(k)^{\epsilon_1} X^{\epsilon_1} \quad \text{and} \quad |\mathcal{E}(F_1)| \ll_{[k:\mathbb{Q}]} \mathrm{Disc}(k)^{\epsilon_1} X^{\epsilon_1}. \tag{5.11}$$

We now consider the consequences of Lemma 4.3 for fields outside the exceptional sets. For $F_1/k \notin \mathcal{E}_0$ with $\mathrm{Disc}(F_1) \in \mathfrak{C}(X)$ and $x = (X/(2\mathrm{Disc}(F_1)^2))^{\delta_1} \leq X^{1/3+\delta_0}$, by Lemma 4.3 we have, for X sufficiently large,

$$\pi_{F_1}(x/2) \geq \pi_k(x/2; F_1, e) \geq \frac{1}{8}\pi_k(x/4) - C_{[k:\mathbb{Q}],\epsilon_1}(x/2)^{\sigma_1} \log^2(X^{1/3+\delta_0} \mathrm{Disc}(k)). \tag{5.12}$$

We next assume that $X \geq 4^{\frac{1}{(1/3-2/100)\delta_1}} \mathrm{Disc}(k)^A$ where $A = \frac{\max\{\beta, 8c(\gamma+2)/\epsilon_1\}}{(1/3-2/100)\delta_1} = A([k : \mathbb{Q}])$, and γ and β are absolute constants for which Lemma 4.4 holds; let also D_0 be an absolute constant such that Lemma 4.4 holds for those γ and β. If $\mathrm{Disc}(k) \geq D_0$, we use Lemma 4.4, and for $X \geq \mathrm{Disc}(k)^A$ and X sufficiently large given $[k : \mathbb{Q}]$, we obtain

$$\frac{1}{8}\pi_k(x/4) - C_{[k:\mathbb{Q}],\epsilon_1}(x/2)^{\sigma_1} \log^2(X^{1/3+\delta_0} \mathrm{Disc}(k)) \gg_{[k:\mathbb{Q}]} \frac{x}{\mathrm{Disc}(k)^{\gamma} \log x}. \tag{5.13}$$

We require that X is large enough so that (5.13) holds also for the finitely many fields k with $\mathrm{Disc}(k) \leq D_0$. Under these assumptions, we conclude for $F_1 \notin \mathcal{E}_0$ that

$$\pi_{F_1}(x/2) \gg_{[k:\mathbb{Q}]} \frac{x}{\mathrm{Disc}(k)^{\gamma} \log x}. \tag{5.14}$$

Next, for $F_2/F_1 \notin \mathcal{E}(F_1)$, by Lemma 4.3 and (5.14), and the assumptions above on X, we have

$$\pi_{F_1}(x; F_2, e) \gg_{[k:\mathbb{Q}]} \frac{x}{\operatorname{Disc}(k)^\gamma \log x}. \tag{5.15}$$

We now consider the contribution to the summation from the various kinds of exceptional and non-exceptional fields. First, we consider the summation $F_2/F_1/k$ where $F_1/k \in \mathcal{E}_0$. Using the trivial bound on the class group and the sparsity of exceptional fields along with Lemmas 5.8 and 5.6, we find

$$\sum_{\substack{F_2/F_1/k \\ \operatorname{Disc}(F_1) \in \mathfrak{C}(X) \\ X/2 \le \operatorname{Disc}(F_2) \le X, F_1/k \in \mathcal{E}_0}} h_3(F_2/k) \ll_{[k:\mathbb{Q}],\epsilon} X^{1/2+\epsilon} \sum_{\substack{F_1/k \in \mathcal{E}_0 \\ \operatorname{Disc}(F_1) \in \mathfrak{C}(X)}} \sum_{\substack{F_2/F_1 \\ X/2 \le \operatorname{Disc}(F_2) \le X}} 1$$
$$\ll_{[k:\mathbb{Q}],\epsilon} h_2(k)^2 \operatorname{Disc}(k)^{\epsilon_1} \cdot X^{5/6+2\delta_0+\epsilon_1+\epsilon}$$
$$\ll_{[k:\mathbb{Q}],\epsilon} \operatorname{Disc}(k)^{1+\epsilon} \cdot X^{5/6+2\delta_0+\epsilon_1+\epsilon}. \tag{5.16}$$

Second, we consider the contribution from those $F_2/F_1/k$ where $F_1 \notin \mathcal{E}_0$ but $F_2/F_1 \in \mathcal{E}(F_1)$. Using the trivial bound on relative class group $h_3(F_2/F_1)$ and an average bound on $h_3(F_1/k)$, we find

$$\sum_{\substack{F_2/F_1/k \\ \operatorname{Disc}(F_1) \in \mathfrak{C}(X) \\ X/2 \le \operatorname{Disc}(F_2) \le X \\ F_2/F_1 \in \mathcal{E}(F_1)}} h_3(F_2/k) \ll_{[k:\mathbb{Q}],\epsilon} \sum_{\substack{F_1/k \\ \operatorname{Disc}(F_1) \in \mathfrak{C}(X)}} h_3(F_1/k) \sum_{\substack{F_2/F_1 \\ X/2 \le \operatorname{Disc}(F_2) \le X \\ F_2/F_1 \in \mathcal{E}(F_1)}} \operatorname{Disc}(F_2/F_1)^{1/2+\epsilon} \operatorname{Disc}(F_1)^{1/2+\epsilon}$$
$$\ll_{[k:\mathbb{Q}],\epsilon} \operatorname{Disc}(k)^{\epsilon_1} X^{1/2+\epsilon_1+\epsilon} \sum_{\substack{F_1/k \\ \operatorname{Disc}(F_1) \in \mathfrak{C}(X)}} h_3(F_1/k) \operatorname{Disc}(F_1)^{-1/2+\epsilon}$$
$$\ll_{[k:\mathbb{Q}],\epsilon} \operatorname{Disc}(k)^{4/3+\epsilon_1+\epsilon} \cdot X^{2/3+\delta_0/2+\epsilon_1+\epsilon}. \tag{5.17}$$

Precisely, the first inequality follows from Lemma 2.5. The second inequality follows from the estimate $|\mathcal{E}(F_1)| \ll_{[k:\mathbb{Q}],\epsilon_1} \operatorname{Disc}(k)^{\epsilon_1} X^{\epsilon_1}$ from (5.11). The third inequality follows from Corollary 3.2 and partial summation.

We now consider the contribution from those $F_2/F_1/k$ where neither $F_1/k \notin \mathcal{E}_0$ nor $F_2/F_1 \notin \mathcal{E}(F_1)$. Using the relative Ellenberg–Venkatesh method developed in Section 2 and existence of small split primes for non-exceptional fields developed in Section 4 and made explicit in (5.15), we find

$$\sum_{\substack{F_2/F_1/k \\ \operatorname{Disc}(F_1) \in \mathfrak{C}(X) \\ X/2 \le \operatorname{Disc}(F_2) \le X \\ F_1 \notin \mathcal{E}_0, F_2/F_1 \notin \mathcal{E}(F_1)}} h_3(F_2/k)$$
$$\ll_{[k:\mathbb{Q}],\epsilon} \operatorname{Disc}(k)^\gamma \cdot \sum_{\substack{F_1/k \\ \operatorname{Disc}(F_1) \in \mathfrak{C}(X)}} h_3(F_1/k) \left(\sum_{\substack{F_2/F_1 \\ F_2 \notin \mathcal{E}(F_1) \\ X/2 \le \operatorname{Disc}(F_2) \le X}} \operatorname{Disc}(F_2/F_1)^{1/2-\delta_1+\epsilon} \operatorname{Disc}(F_1)^{1/2+\epsilon} \right) \tag{5.18}$$
$$\ll_{[k:\mathbb{Q}],\epsilon} \operatorname{Disc}(k)^\gamma \cdot h_2(k)^2 \cdot \left(\sum_{\substack{F_1/k \\ \operatorname{Disc}(F_1) \in \mathfrak{C}(X)}} h_3(F_1/k) \cdot \left(\frac{X}{\operatorname{Disc}(F_1)^2}\right)^{3/2-\delta_1+\epsilon} \cdot \operatorname{Disc}(F_1)^{1/2+\epsilon} \right)$$
$$\ll_{[k:\mathbb{Q}],\epsilon} \operatorname{Disc}(k)^{\gamma+7/3+\epsilon} X^{1-\frac{\delta_1}{3}+\delta_0(\frac{3}{2}-2\delta_1)+\epsilon}.$$

Precisely, the first inequality comes from Lemma 2.1 and (5.15). The second inequality follows from Lemma 5.8 and Lemma 5.6. We apply Corollary 3.2 and partial summation for the last inequality.

24

Finally, in the complementary case that X is not sufficiently large, we may assume that $X \ll_{[k:\mathbb{Q}]} \text{Disc}(k)^A$, so that by applying the trivial bound $h_3(F_2/k) \ll_{[k:\mathbb{Q}],\epsilon} X^{1/2+\epsilon}$, we find

$$
\sum_{\substack{F_2/F_1/k \\ \text{Disc}(F_1) \in \mathfrak{C}(X) \\ X/2 \leq \text{Disc}(F_2) \leq X}} h_3(F_2/k) \ll_{[k:\mathbb{Q}],\epsilon} X^{1/2+\epsilon} \cdot \sum_{\substack{F_2/F_1/k \\ \text{Disc}(F_1) \in \mathfrak{C}(X) \\ X/2 \leq \text{Disc}(F_2) \leq X}} 1
$$

$$
\ll_{[k:\mathbb{Q}],\epsilon} X^{4/3+\delta_0+\epsilon} h_2(k)^3 \text{Disc}(k)^{-2+\epsilon}
$$

$$
\ll_{[k:\mathbb{Q}],\epsilon} \text{Disc}(k)^{(4/3+\delta_0+\epsilon)A-1/2+\epsilon}.
$$

(5.19)

Here the second inequality follows from Lemma 5.8 twice, and the last inequality follows from the bound on X.

So to deduce the statement of the lemma, we note we have four upper bounds of the form $\text{Disc}(k)^{a_i} X^{b_i+\epsilon}$. We can take, e.g. $\epsilon = 1/1000$, and note that each of the b_i is less than $998/1000$. Then we can take $\delta = 1/1000$, and α can be taken to be $\max_i a_i$, which depends on $[k:\mathbb{Q}]$. $\qquad \square$

5.3 Induction

Finally, in this section, we will prove Theorem 5.1 in general. We will use an induction argument with the initial case $m = 2$.

Proof of Theorem 5.1. The statement for $m = 2$ follows from the combination of Lemma 5.7 and 5.9. Now assume for some i that we can prove the lemma for every $m \leq i$. Our goal is to prove the lemma for $m = i+1$.

Firstly, we treat the summation when $\text{Disc}(F_i) \in \mathfrak{N}(X,Y) = [Y, X^{1/3-\delta_0}) \cup (X^{1/3+\delta_0}, X^{1/2}]$, the non-critical range. We use an argument similar with that in Lemma 5.7 where non-critical range is treated for $m = 2$. For any $0 < \delta_0 < 1/6$ and $Y \geq 1$, using the results on counting cubic fields in Section 3, as collected in (5.5), and the induction hypothesis in the form of Corollary 5.5, we find

$$
\sum_{\substack{F_{i+1}/F_i/\cdots/F_1/k \\ \text{Disc}(F_i) \in \mathfrak{N}(X,Y) \\ X/2 \leq \text{Disc}(F_{i+1}) \leq X}} h_3(F_{i+1}/k) = \sum_{\substack{F_i/\cdots/F_1/k \\ \text{Disc}(F_i) \in \mathfrak{N}(X,Y)}} h_3(F_i/k) \sum_{\substack{F_{i+1}/F_i \\ X/2 \leq \text{Disc}(F_{i+1}) \leq X}} h_3(F_{i+1}/F_i)
$$

$$
\ll_{[k:\mathbb{Q}],i,\epsilon',\epsilon} \text{Disc}(k)^{\alpha_i - 2^{i-1}+\epsilon} \left(X^{1-\frac{3\delta_0}{2}+\epsilon'} + X^{11/12+\epsilon'} + \frac{X}{Y^{1-\epsilon}} \right).
$$

(5.20)

The inequality above follows as in (5.6), with F_i in place of F_1, using the cases of (5.5) in three ranges of $\text{Disc}(F_i)$ followed by partial summation with Corollary 5.5 (in place of Corollary 3.2), and the $h_2(k)^2$ factor from bounding $h_2(F_1)$ is replaced by $h_2(k)^{2^i}$ in the bound for $h_2(F_i)$.

We now treat the contribution from towers with $\text{Disc}(F_i) \in \mathfrak{C}(X) = [X^{1/3-\delta_0}, X^{1/3+\delta_0}]$. We separate the discussion into two cases depending on the size of $\text{Disc}(F_{i-1})$. Fix $1 \leq Y_2 \leq X^{\frac{1}{6}-\frac{\delta_0}{2}}$. Then, we find

$$
\sum_{\substack{F_{i+1}/F_i/\cdots/F_1/k \\ \text{Disc}(F_{i-1}) \geq Y_2 \\ \text{Disc}(F_i) \in \mathfrak{C}(X) \\ X/2 \leq \text{Disc}(F_{i+1}) \leq X}} h_3(F_{i+1}/k) = \sum_{\substack{F_i/\cdots/F_1/k \\ \text{Disc}(F_{i-1}) \geq Y_2 \\ \text{Disc}(F_i) \in \mathfrak{C}(X,Y)}} h_3(F_i/k) \sum_{\substack{F_{i+1}/F_i \\ X/2 \leq \text{Disc}(F_{i+1}) \leq X}} h_3(F_{i+1}/F_i)
$$

$$
\ll_{[k:\mathbb{Q}],i,\epsilon} h_2(k)^{2^i} \sum_{\substack{F_i/\cdots/F_1/k \\ \text{Disc}(F_{i-1}) \geq Y_2 \\ \text{Disc}(F_i) \in \mathfrak{C}(X)}} h_3(F_i/k) \cdot \text{Disc}(F_i)^{1/2+\epsilon} \cdot \left(\frac{X}{\text{Disc}(F_i)^2} \right)^{3/2+\epsilon}
$$

$$
\ll_{[k:\mathbb{Q}],i,\epsilon} h_2(k)^{2^i} \text{Disc}(k)^{\alpha_i} \cdot X^{3/2+\epsilon} \cdot \left(\frac{X^{-\frac{1}{2}+\frac{3\delta_0}{2}}}{Y_2^{1-\epsilon}} + X^{-(1/3-\delta_0)(3/2+\delta_i)} \right)
$$

$$
\ll_{[k:\mathbb{Q}],i,\epsilon} \text{Disc}(k)^{\alpha_i+2^{i-1}+\epsilon} \cdot \left(\frac{X^{1+3\delta_0/2+\epsilon}}{Y_2^{1-\epsilon}} + X^{1+3\delta_0/2-\delta_i/3+\delta_0\delta_i+\epsilon} \right).
$$

(5.21)

25

Precisely, the first inequality follows from (3.8), Proposition 3.4, Lemma 5.8, and Lemma 5.6. The second inequality follows from partial summation, and the induction hypothesis with $m = i$ applied to $F_i/\cdots/F_1/k$ with Y_2 being the lower bound for $\mathrm{Disc}(F_{i-1})$. The third inequality follows from the trivial bound on $h_2(k)$.

Finally we consider those towers with $\mathrm{Disc}(F_{i-1}) \leq Y_2$. Let δ_2' and α_2' be the constants associated to $[F_{i-1} : \mathbb{Q}]$ and $m = 2$. We have

$$
\sum_{\substack{F_{i+1}/F_i/\cdots/F_1/k \\ \mathrm{Disc}(F_{i-1}) \leq Y_2 \\ \mathrm{Disc}(F_i) \in \mathfrak{C}(X) \\ X/2 \leq \mathrm{Disc}(F_{i+1}) \leq X}} h_3(F_{i+1}/k) = \sum_{\substack{F_{i-1}/\cdots/F_1/k \\ \mathrm{Disc}(F_{i-1}) \leq Y_2}} h_3(F_{i-1}/k) \sum_{\substack{F_{i+1}/F_i/F_{i-1} \\ \mathrm{Disc}(F_i) \in \mathfrak{C}(X) \\ X/2 \leq \mathrm{Disc}(F_{i+1}) \leq X}} h_3(F_{i+1}/F_{i-1})
$$

$$
\ll_{[k:\mathbb{Q}],i,\epsilon} \sum_{\substack{F_{i-1}/\cdots/F_1/k \\ \mathrm{Disc}(F_{i-1}) \leq Y_2}} h_3(F_{i-1}/k)\left(X^{2/3+\delta_0+\epsilon} + X^{1-\delta_2'}\right) \cdot \mathrm{Disc}(F_{i-1})^{\alpha_2'} \tag{5.22}
$$

$$
\ll_{[k:\mathbb{Q}],i} \mathrm{Disc}(k)^{\alpha_{i-1}} X^{\max\{3/4+\delta_0, 1-\delta_2'\}} Y_2^{1+\alpha_2'}.
$$

Here precisely, the first inequality follows from the induction hypothesis with $m = 2$ and base field $k = F_{i-1}$. The second inequality follows from the induction hypothesis with $m = i - 1$.

If we let $Y_2 = X^b$, then to obtain the desired bound, (5.21) requires us to choose δ_0 small, given b and δ_i, and (5.22) requires us to take b small given δ_2' and α_2' (as long as we have taken δ_0 absolutely sufficiently small). Since we can do this by choosing b and then δ_0, we will be able to obtain the theorem. In particular, making the convenient but non-optimal choices $b = \min\{\delta_2'/(2(1+\alpha_2')), 1/(8(1+\alpha_2'))\}$ and $Y_2 = X^b$ and $\delta_0 = \min\{\delta_i/9, b/2, 1/16\}$, we conclude that the statement of the theorem holds for $m = i + 1$ with

$$
\alpha_{i+1} = \max\{\alpha_i + 2^i, \alpha_{i-1}\} \quad \text{and} \quad \delta_{i+1} = \min\{\frac{\delta_2'}{2}, \frac{b}{8}, \frac{\delta_i}{36}, \frac{1}{32}\}.
$$

$\square$

6 Average of 3-torsion in Class Groups of 2-extensions

In this section, we will prove a refined version of Theorem 1.1, in Theorem 6.1 below, using crucially the tail estimates from Section 5. We use the same approach to prove Theorem 1.2. The *group signature* Σ of K/k is the ordered tuple $(\Sigma_v)_v$, where v ranges over the real places of k, and Σ_v is the conjugacy class of complex conjugation in $\mathrm{Gal}(K/k)$ over v. This further refines the enriched signature of Cohen and Martinet. Let $E_k(m, X)$ be the set of degree 2^m 2-extensions K/k (in $\bar{\mathbb{Q}}$) with $\mathrm{Disc}\, K \leq X$. Let $E_k(G, X)$ be the set of G-extensions K/k (in $\bar{\mathbb{Q}}$) with $\mathrm{Disc}\, K \leq X$ and let $E_k^{\Sigma}(G, X)$ be those with group signature Σ.

Theorem 6.1. *Let k be a number field and m a positive integer. Then there exists $C_m > 0$ such that*

$$
\lim_{X \to \infty} \frac{1}{|E_k(m, X)|} \sum_{K \in E_k(m, X)} h_3(K) = C_m. \tag{6.1}
$$

Moreover, let $G \subset S_{2^m}$ be a transitive permutation 2-group containing a transposition and Σ a group signature that occurs for some G-extension of k. Then there exists $C_{G,\Sigma}, C_G > 0$ such that

$$
\lim_{X \to \infty} \frac{1}{|E_k^{\Sigma}(G, X)|} \sum_{K \in E_k^{\Sigma}(G, X)} h_3(K) = C_{G,\Sigma} \qquad and \qquad \lim_{X \to \infty} \frac{1}{|E_k(G, X)|} \sum_{K \in E_k(G, X)} h_3(K) = C_G.
$$

$$
\tag{6.2}
$$

The proof of Theorem 6.1 gives the constants explicitly. We let $r_1(F)$ denote the number of real places of F, and $r_2(F)$ the number of pairs of complex places of F. We have

$$
C_m = \left(\sum_{F \in E_k(m-1, \infty)} \frac{h_3(F)\mathrm{Res}_{s=1}\zeta_F(s)}{2^{r_2(F)}\zeta_F(2)\mathrm{Disc}(F)^2} \cdot \left(1 + \frac{2^{r_1(F)}}{3^{r_1(F)+r_2(F)}}\right) \right) \left(\sum_{F \in E_k(m-1, \infty)} \frac{\mathrm{Res}_{s=1}\zeta_F(s)}{2^{r_2(F)}\zeta_F(2)\mathrm{Disc}(F)^2} \right)^{-1}.
$$

When the group G has a transposition, Lemma 6.6 below shows that $G = C_2 \wr H$ for some transitive subgroup $H \subseteq S_{2^{m-1}}$. The image of a group signature Σ for G gives a group signature $\bar{\Sigma}$ for H. So a G-extension K/k of signature Σ has an index 2 subfield F/k which is an H-extension of signature $\bar{\Sigma}$, and there is a number $u(\Sigma)$, depending only on Σ, which gives the number of infinite places of F that are split in K, or equivalently, $\operatorname{rk} \mathcal{O}_K^* - \operatorname{rk} \mathcal{O}_F^*$, the relative unit rank of K/F. Then we have

$$C_{G,\Sigma} = \left(\sum_{F \in E_k^{\bar{\Sigma}}(H,\infty)} \frac{h_3(F)\operatorname{Res}_{s=1}\zeta_F(s)}{\zeta_F(2)\operatorname{Disc}(F)^2} \cdot \left(1 + 3^{-u(\Sigma)} \right) \right) \left(\sum_{F \in E_k^{\bar{\Sigma}}(H,\infty)} \frac{\operatorname{Res}_{s=1}\zeta_F(s)}{\zeta_F(2)\operatorname{Disc}(F)^2} \right)^{-1},$$

$$C_G = \left(\sum_{F \in E_k(H,\infty)} \frac{h_3(F)\operatorname{Res}_{s=1}\zeta_F(s)}{\zeta_F(2)\operatorname{Disc}(F)^2} \cdot \left(1 + \frac{2^{r_1(F)}}{3^{r_1(F)+r_2(F)}} \right) \right) \left(\sum_{F \in E_k(H,\infty)} \frac{\operatorname{Res}_{s=1}\zeta_F(s)}{\zeta_F(2)\operatorname{Disc}(F)^2} \right)^{-1}.$$

Before proving Theorem 6.1, we first give a result on the asymptotic number of 2-extensions, i.e. the denominator in Theorem 6.1.

Theorem 6.2. *Let k be a number field and let m be a positive integer. There exists $D_m > 0$ such that*

$$|E_k(m,X)| \sim D_m X. \tag{6.3}$$

Moreover, let $G \subset S_{2^m}$ be a transitive permutation 2-group containing a transposition and Σ a group signature. Then there exists $D_{G,\Sigma} \geq 0$ and $D_G > 0$ such that

$$|E_k^{\Sigma}(G,X)| \sim D_{G,\Sigma} X \quad \text{and} \quad |E_k(G,X)| \sim D_G X. \tag{6.4}$$

If there exists an H-extension of k with group signature $\bar{\Sigma}$, then $D_{G,\Sigma} > 0$. Further, if $G \subset S_{2^m}$ is a transitive permutation 2-group not containing a transposition, then $|E_k(G,X)| = O_{k,G,\epsilon}(X^{1/2+\epsilon})$.

Proof. Malle [Mal02, Mal04] conjectured that for 2-groups $|E_k(G,X)|$ has linear growth if and only if G contains a transposition. When G has no transpositions, it is proved by [KM04, Corollary 7.3] that $|E_k(G,X)| = O_{k,G,\epsilon}(X^{1/2+\epsilon})$. When G contains a transposition, by [Klü12, Lemma 5.5] G must be isomorphic to $C_2 \wr H$ for some permutation 2-group H. It is proved in [Klü12, Theorem 5.8] that when there exists a H-extension and $|E_k(H,X)|$ is not growing too fast, Malle's conjecture $|E_k(G,X)| \sim D_G X$ holds for $G = C_2 \wr H$. The existence of 2-group extensions is shown by a celebrated theorem of Shafarevich [Š54], and the upper bound for $|E_k(H,X)|$ is known for all permutation 2-groups H, again by [KM04, Corollary 7.3]. This gives the first statement of the theorem and a version of the second statement without signature conditions. Following Klüners proof, or a simpler version of the proof of Theorem 6.1, one can obtain a version with the signature condition and also with the precise constants

$$D_m = \sum_{F \in E_k(m-1,\infty)} \frac{\operatorname{Res}_{s=1}\zeta_F(s)}{2^{r_2(F)}\zeta_F(2)\operatorname{Disc}(F)^2},$$

$$D_{G,\Sigma} = \sum_{F \in E_k^{\bar{\Sigma}}(H,\infty)} \frac{p_{\Sigma} 2^{2^{m-1}-r_2(F)}\operatorname{Res}_{s=1}\zeta_F(s)}{\zeta_F(2)\operatorname{Disc}(F)^2}, \quad \text{and} \quad D_G = \sum_{F \in E_k(H,\infty)} \frac{2^{2^{m-1}-r_2(F)}\operatorname{Res}_{s=1}\zeta_F(s)}{\zeta_F(2)\operatorname{Disc}(F)^2},$$

where $\bar{\Sigma}$ is the group signature on H given from Σ via the quotient map $G \to H$, and p_{Σ} is the proportion of the $2^{r_1(F)}$ possible behaviors at infinity for a quadratic extension K/F such that when K is a G-extension with such behavior then it has group signature Σ. (We note that p_{Σ} is determined group theoretically from Σ and is non-zero—see the proof of Theorem 6.1.) $\square$

Theorem 6.2 shows that, among 2-extensions of a given degree, the fields with Galois groups without transpositions are *thin* families. Thus, the restriction in Theorem 6.1 to groups G with transpositions is natural. In fact, while Theorem 6.1 does not give class number averages for the thin families of extensions with Galois group G for G without transpositions, a key step in its proof is to show that class group elements arising from such extensions give a negligible contribution to the average in (6.1). This is a result of independent interest that complements Theorem 6.1. Thus, we begin by considering thin families in Section 6.1, which culminates in Theorem 6.5 that makes this discussion precise. Then, in Section 6.2, we turn to the proof of Theorem 6.1.

6.1 Thin families of 2-extensions

In this section, we focus on studying 3-torsion in class groups of 2-extensions with a permutation Galois group G without a transposition. We begin by proving an upper bound on the count of these extensions, but with explicit base field discriminant dependence. We first give the following lemma, which is a uniform version of Theorem 1.6 in [KW20] for $\ell = 2$.

Lemma 6.3. *Let k be a number field. Then there exists $\alpha_m > 0$ depending at most on $[k : \mathbb{Q}]$ and m such that the number of degree 2^m 2-extension K/k with $\mathrm{Disc}(K/k) = D$ is bounded by $O_{[k:\mathbb{Q}],m,\epsilon}(D^\epsilon \mathrm{Disc}(k)^{\alpha_m})$.*

Proof. We proceed by induction over m. For $m = 1$, we know from class field theory (see the proof of Lemma 3.5) that the number of relative quadratic extension K/k with $\mathrm{Disc}(K/k) = D$ is at most $O_{[k:\mathbb{Q}],\epsilon}(h_2(k) \cdot D^\epsilon) = O_{[k:\mathbb{Q}],\epsilon}(D^\epsilon \mathrm{Disc}(k)^{1/2+\epsilon})$. Now assuming the statement is true for $m = i$, we will prove that it also holds for $m = i + 1$. By Lemma 5.4, it suffices to count quadratic extensions of degree 2^i 2-extensions F/k with $\mathrm{Disc}(F/k)^2|D$. The number of such F is bounded by $O_{[k:\mathbb{Q}],\epsilon,i}(D^\epsilon \mathrm{Disc}(k)^{\alpha_i})$ by the induction hypothesis. For each such F, the number of quadratic relative extension K/F with $\mathrm{Disc}(K/F) = D/\mathrm{Disc}(F/k)^2$ is bounded by $O_{[F:\mathbb{Q}],\epsilon}(h_2(F) \cdot D^\epsilon)$ from class field theory. Applying Lemma 5.6 and summation over all divisors of D, we obtain the upper bound $O_{[k:\mathbb{Q}],i+1,\epsilon}(D^\epsilon \mathrm{Disc}(k)^{\alpha_{i+1}})$, where α_{i+1} can be taken as $\alpha_i + 2^{i-1}$. $\square$

Theorem 6.4. *Let k be a number field k and let $G \subseteq S_{2^m}$ be a transitive permutation 2-group without a transposition. Then there exists $\alpha > 0$ depending at most on $[k : \mathbb{Q}]$ and m such that*

$$|E_k(G, X)| = O_{[k:\mathbb{Q}],m,\epsilon}(X^{1/2+\epsilon} \mathrm{Disc}(k)^\alpha).$$

Proof. Notice that when G does not contain a transposition, the discriminant ideal $\mathrm{disc}(K/k)$ must have exponent at least 2 at every ramified prime, i.e., it is powerful. Thus, its norm, $\mathrm{Disc}(K/k)$, must be a powerful integer, and there are $O(X^{1/2})$ powerful integers below X. The result now follows from Lemma 6.3. $\square$

The ℓ-torsion conjecture then would imply that the summation of $|\mathrm{Cl}_K[3]|$ for G-extensions K without a transposition should be also thin, i.e. $O(X^{1/2+\epsilon})$. By applying the trivial bound for class group $h_3(K) = O_{[K:\mathbb{Q}],\epsilon}(\mathrm{Disc}(K)^{1/2+\epsilon})$, we can conclude immediately that $\sum_{K \in E_k(G,X)} h_3(K) = O_{k,\epsilon}(X^{1+\epsilon})$. However, it is crucial for our main theorem that we prove something slightly better than this.

Theorem 6.5. *Let k be a number field and let $G \subset S_{2^m}$ be a transitive permutation 2-group without a transposition. Then there exist $\delta > 0$ and α depending on G and $[k : \mathbb{Q}]$ such that*

$$\sum_{K \in E_k(G,X)} h_3(K/k) = O_{[k:\mathbb{Q}],G}(X^{1-\delta} \cdot \mathrm{Disc}(k)^\alpha).$$

Proof. A G-extension K can be constructed as a relative quadratic extension over a degree 2^{m-1} 2-extension F with $\mathrm{Gal}(F/k) =: H \subset S_{2^{m-1}}$ by Lemma 5.4. We fix $\delta_1 = 1/24$ and $\epsilon_1 = 1/4$. Let γ, β and D_0 be absolute constants allowable in Lemma 4.4. Let $Y = X^{\delta'}$ for some δ' that we will choose sufficiently small in terms of m and $[k : \mathbb{Q}]$. Then by Theorem 5.1 and dyadic summation, taking $\delta' \leq \delta_m$, we have

$$\sum_{\substack{K/F/k \\ \mathrm{Disc}(K) \leq X \\ \mathrm{Disc}(F) \geq Y}} h_3(K/k) \ll_{[k:\mathbb{Q}],m,\epsilon} \mathrm{Disc}(k)^{\alpha_m} X^{1-\delta'+\epsilon}.$$

Therefore it suffices to consider the summation over G-extensions where the associated H-extension F/k has $\mathrm{Disc}(F) \leq Y = X^{\delta'}$.

We will apply an argument similar to Section 5.2 to complete the proof. For each F, denote the set $\mathcal{E}(F) = \mathcal{E}(F, X/\mathrm{Disc}(F)^2, \epsilon_1)$ of exceptional quadratic extensions as given by Lemma 4.3, for $X \gg 1$. The set has size $|\mathcal{E}(F)| \ll_{[F:\mathbb{Q}],\epsilon_1} X^{\epsilon_1}$. Let $x = (X/(2Y^2))^{\delta_1}$. We assume X is sufficiently large in terms of $[k : \mathbb{Q}]$ and δ' sufficiently small in terms of our absolute constants, so that for $\sigma_1 = \max\{1 - \epsilon_1/4c, 1/2\}$

with $c = c_{[F:\mathbb{Q}]}$ in Theorem 4.2 and F with $\mathrm{Disc}(F) \geq D_0$, we may apply Lemmas 4.3 and 4.4 in concert to conclude for $K \notin \mathcal{E}(F)$,

$$\pi_F(x; K, e) \geq \frac{1}{8}\pi_F(x/2) - C_{[F:\mathbb{Q}],\epsilon_1} x^{\sigma_1} (\log(X\,\mathrm{Disc}(F)))^2 \gg_{[k:\mathbb{Q}],\epsilon} \frac{x}{\mathrm{Disc}(F)^\gamma \log x}. \tag{6.5}$$

We also assume that X is sufficiently large that this holds for the finite number of fields F with $\mathrm{Disc}(F) \leq D_0$.

Using the trivial bound for $h_3(K/k)$, the summation over $K/F/k$ with $K/F \in \mathcal{E}(F)$ is

$$\sum_{\substack{K/F/k \\ \mathrm{Disc}(F) \leq Y \\ \mathrm{Disc}(K) \leq X \\ K/F \in \mathcal{E}(F)}} h_3(K/k) \ll_{[k:\mathbb{Q}],\epsilon} \sum_{\mathrm{Disc}(F) \leq Y} \sum_{K/F \in \mathcal{E}(F)} \mathrm{Disc}(K)^{1/2+\epsilon}$$

$$\ll_{[k:\mathbb{Q}],\epsilon_1,m,\epsilon} \mathrm{Disc}(k)^{\alpha_{m-1}} \cdot X^{1/2+\epsilon_1+\epsilon} Y, \tag{6.6}$$

where the last inequality follows from combining the bound on $|\mathcal{E}(F)|$ with an upper bound on the number of such F, for example as is provided by Corollary 5.5 and dyadic summation.

For fields $K/F \notin \mathcal{E}(F)$, we use Lemma 2.1, (6.5), and the trivial bound on $h_3(F/k)$ to obtain that $h_3(K/k) \ll_{[k:\mathbb{Q}],m,\epsilon} X^{1/2-\delta_1+\epsilon} Y^{2\delta_1+\gamma}$. Then we find

$$\sum_{\substack{K/F/k \\ X/2 \leq \mathrm{Disc}(K) \leq X \\ \mathrm{Disc}(F) \leq Y \\ K/F \notin \mathcal{E}(F) \\ \mathrm{Gal}(K/k)=G}} h_3(K/k) \ll_{[k:\mathbb{Q}],m,\epsilon} \sum_{\substack{K/k \\ X/2 \leq \mathrm{Disc}(K) \leq X \\ \mathrm{Disc}(F) \leq Y \\ \mathrm{Gal}(K/k)=G}} X^{1/2-\delta_1+\epsilon} Y^{2\delta_1+\gamma}$$

$$\ll_{[k:\mathbb{Q}],m,\epsilon} \mathrm{Disc}(k)^\alpha X^{1-\delta_1+\epsilon} Y^{2\delta_1+\gamma},$$

by Theorem 6.4, where α is associated to $[k:\mathbb{Q}]$ in Theorem 6.4. We can use dyadic summation to remove the lower bound on $\mathrm{Disc}(K)$ and obtain the same bound (with a different implied constant).

Finally, for $X \ll_{[k:\mathbb{Q}],\delta'} 1$, we have

$$\sum_{\substack{K/F/k \\ X/2 \leq \mathrm{Disc}(K) \leq X \\ \mathrm{Disc}(F) \leq Y \\ \mathrm{Gal}(K/k)=G}} h_3(K/k) \ll_{[k:\mathbb{Q}],m,\delta'} \mathrm{Disc}(F)^{\alpha_m} \leq X^{\delta'\alpha_m}$$

by Corollary 5.5. Choosing δ' and sufficiently small in terms of $[k:\mathbb{Q}]$ and m, we conclude the theorem. $\quad\square$

6.2 Proof of the Main Theorem

Now we are ready to prove Theorem 6.1. We start with the following lemmas that allow us to move from summing over G extensions to summing over H-extensions, where $G \simeq C_2 \wr H$.

Lemma 6.6. *A transitive permutation 2-group $G \subset S_{2d}$ contains a transposition if and only if $G \simeq C_2 \wr H$ for some $H \subset S_d$. For such a G, if K/k is a G-extension, then there exists a unique subfield F/k with $[K:F] = 2$. Moreover, F/k is an H-extension. For such a G, there is only one permutation group H up to isomorphism such that $G \simeq C_2 \wr H$.*

Proof. The first statement is Lemma 5.5 in [Klü12]. For the second statement, we claim if M is a subgroup of G and contains $\mathrm{Stab}_G(1)$ as a proper subgroup, then $C_2^d \rtimes \mathrm{Stab}_H(1) \subset M$. To show the claim, we write $\mathrm{Stab}_G(1) = C_2^{d-1} \rtimes \mathrm{Stab}_H(1)$ where C_2^{d-1} is the subspace of C_2^d with first entry 0. Suppose $g = v \rtimes h \in M$ and $g \notin \mathrm{Stab}_G(1)$. If $h \in \mathrm{Stab}_H(1)$, then $v_1 \neq 0$, and multiplication by all $u \rtimes h^{-1} \in \mathrm{Stab}_G(1)$ shows that $C_2^d \subset M$. If $h \notin \mathrm{Stab}_H(1)$, then for $u \in C_2^{d-1}$ with a 1 in position $h^{-1}(1)$ and 0's elsewhere, we have that $(v \rtimes h)u(v \rtimes h)^{-1} \in C_2^d$ with a 1 in position 1 and 0's elsewhere, so we conclude the claim. The second and third statements of lemma then follow by Galois theory. If $G \simeq C_2 \wr H$, then H acts on 2-element blocks of the elements that G acts on, and all elements of G preserve the block structure. From this, it follows that two elements are together in a block if and only if G contains a transposition that interchanges them. From this it follows that H is determined uniquely as a permutation group. $\quad\square$

We now want to be precise about exactly what we mean by permutation group isomorphisms.

Definition 6.7. *A permutation group G is a group G, a set B_G, and a faithful action of G on B_G. The degree of G is $|B_G|$. An isomorphism of permutation groups $G \to H$ is a bijection $\sigma : B_G \to B_H$ so that the induced map $\sigma_* : G \to H$ is a a group isomorphism (where $\sigma_*(g)(b) = \sigma g \sigma^{-1}(b)$). We write $\mathrm{Aut}_{\mathrm{perm}}(G)$ for the group of permutation automorphisms of G, which is also the normalizer $N_{S_{B_H}}(H)$ of H in the symmetric group S_{B_H}.*

In particular, a G-extension K/k includes the data of a bijection between the embeddings $K \to \bar{k}$ and B_G. Note that $B_{C_2 \wr H} = \{1, 2\} \times B_H$.

Lemma 6.8. *Let G be a transitive permutation 2-group and $G = C_2 \wr H$, with H a permutation group of degree d. Given an H-extension $F \in E_k(H, \infty)$, and a quadratic extension K/F (in $\bar{\mathbb{Q}}$), then either (1)$\mathrm{Gal}(K/k)$ does not contain a transposition or (2)K/k can be realized as a G-extension with 2^d choices of $\mathrm{Gal}(K/k) \simeq G$ (i.e. choices of $\{K \to \tilde{K}\} \to B_G$) that are compatible with the permutation group isomorphism $\mathrm{Gal}(F/k) \simeq H$ (i.e. choice of $\{F \to \tilde{F}\} \to B_H$) in the quotient. Moreover, any G-extension $K \in E_k(G, \infty)$ arises in this construction from a unique F, one quadratic extension K/F, and one of the 2^d choices of $\mathrm{Gal}(K/k) \simeq G$.*

Proof. Given $F \in E_k(H, \infty)$ and a quadratic extension K/F, we have 2^d choices of identification of the embeddings $K \to \tilde{K}$ with $\{1, 2\} \times B_H$ that are compatible with the map from the embeddings of F to B_H. Any of these gives an injection of groups $\mathrm{Gal}(K/k) \subset C_2 \wr H$ compatible with the permutation actions. Any transposition in $C_2 \wr H$ is an element of C_2^d that is non-trivial in exactly one coordinate. Since H is transitive, this implies that any subgroup of $C_2 \wr H$ containing a transposition and with image in H all of H must contain all of C_2^d and thus be all of $C_2 \wr H$. So if $\mathrm{Gal}(K/k)$ contains a transposition, we see that $\mathrm{Gal}(K/k) \simeq G$, and there are 2^d ways of choosing such a permutation group isomorphism that are compatible with the map from the embeddings of F to B_H.

Given a G-extension $K \in E_k(G, \infty)$, from Lemma 6.6 we see that it arises in this way from a unique F, and the lemma follows. $\qquad \square$

Next we recall the following important result by Datskovsky–Wright [DW88].

Theorem 6.9 (Datskovsky–Wright)**.** *Let F be a number field. For a group signature Σ of a quadratic extension K/F, let $u(\Sigma)$ be the number of infinite places of F where Σ is trivial (which is also the relative unit rank of K/F). Then*

$$\sum_{\substack{[K:F]=2 \\ \text{signature } \Sigma \\ |\mathrm{Disc}(K/F)| \leq X}} h_3(K/F) \sim X \cdot \frac{\mathrm{Res}_{s=1}\zeta_F(s)}{2^{r_1(F)+r_2(F)}\zeta_F(2)}(1 + 3^{-u(\Sigma)}) \quad \text{and} \quad \sum_{\substack{[K:F]=2 \\ \text{signature } \Sigma \\ |\mathrm{Disc}(K/F)| \leq X}} 1 \sim X \cdot \frac{\mathrm{Res}_{s=1}\zeta_F(s)}{2^{r_1(F)+r_2(F)}\zeta_F(2)}.$$

Proof. This follows from combining Theorems 4.2 and 5.1 in [DW88]. $\qquad \square$

We now turn to the proof of our main theorem.

Proof of Theorem 6.1. Suppose $G \subseteq S_{2^m}$ is a 2-group with a transposition, so by Lemma 6.6, $G = C_2 \wr H$ for a unique $H \subseteq S_{2^{m-1}}$. Let $\bar{\Sigma}$ be the group signature for H that is the image of Σ. So a G-extension K/k with group signature Σ has an index two subfield F/k with the group signature $\bar{\Sigma}$. We next wish to show that the group signature of K/k is determined by F and the group signature of K/F.

We first consider the structure of order 2 elements of G, to understand the possible group signatures. For $g \in G = C_2 \wr H$, let $\bar{g}$ denote the image of g in H. The group H acts on a set of 2^{m-1} elements B_H. The element $g \in G$ has order 2 if and only if $\bar{g}$ has order 2 and the C_2 coordinates of g (of which there is one for each element of B_H) are constant on $\bar{g}$ orbits of B_H. Moreover, if $\bar{g}$ transposes two elements a, b of B_H, and g' is obtained from g by changing the C_2 coordinates at positions a, b, then g' is conjugate to g. In particular, a conjugacy class $[g]$ of an element $g \in G$ is determined by the image of the conjugacy class in H, and for any element h of that conjugacy class in H, the C_2 coordinates of the h fixed points of B_H.

Next, we need to relate the infinite places of F above a place v of k to the permutation group H. To do this, at each real place v of k we choose an embedding $i_v : \bar{\mathbb{Q}} \to \mathbb{C}$ that restricts to v on k. If F is an H-extension, the elements B_H correspond to embeddings $\tau : F \to \tilde{F}$ (as part of the data of the H-extension),

and via $i_v : \bar{\mathbb{Q}} \to \mathbb{C}$ these correspond to embeddings $i_v \circ \tau : F \to \mathbb{C}$. So for each real place v of k, we now have a correspondence between B_H and the complex embeddings of F that restrict to i_v on k. With these choices of i_v, we can now specify an actual element of H corresponding to complex conjugation over v (as opposed to a conjugacy class). Precisely, we define $\sigma_v(F)$ to be the element of H that acts on the embeddings $\tau : F \to \tilde{F}$ so that $\sigma_v(F)(\tau) = i_v^{-1} \circ \overline{i_v \circ \tau}$, where the bar denotes complex conjugation, i.e. $\sigma_v(F)$ is the pullback of complex conjugation via i_v. Similarly, for a G-extension K/k of group signature Σ, we have $\sigma_v(K) \in \Sigma_v$. If F/k is the index two subfield of K, then at the fixed points of $\sigma_v(F)$, our chosen complex conjugation, on B_H, the C_2 coordinate of $\sigma_v(K)$ is trivial when K/F is split at the corresponding place of F and non-trivial when K/F is ramified at that place. Using the conclusion of the previous paragraph, we conclude that if K/k is a G-extension with index two subfield F/k, the conjugacy class of $\sigma_v(K)$, and hence the group signature of K/k, is determined by F and the group signature of K/F.

Next, we wish to determine the number of group signatures of the quadratic extension K/F that will lead to group signature Σ for K/k. Let F/k be an H-extension with group signature $\bar{\Sigma}$. Let M_F be the set of group signatures Σ_2 for quadratic extensions of F such that K/k has group signature Σ when K/F has group signature Σ_2. For a G-extension K/k of group signature Σ, we let $u(\Sigma)$ be the difference in unit ranks between K and F, which only depends on Σ. Note that for any $\Sigma_2 \in M_F$, we have that $u(\Sigma)$ is the number of split places in Σ_2. Also let $M_\Sigma := |M_F|$, and note that it only depends on Σ, since if we choose $\sigma_v \in \Sigma_v$ for all real places v of k, then M_Σ is the product over v of the number of elements $u \in C_2^{(B_H^{\sigma_v})}$ such that $u\sigma_v$ is conjugate to σ_v (where $B_H^{\sigma_v}$ denotes the elements of B_H fixed by σ_v). Given an H-extension F, let $\mathcal{Q}_F^\Sigma$ be the set of quadratic extensions K/F (in $\bar{\mathbb{Q}}$) of group signature in M_F.

Let $Y \geq 1$, and suppose $X_0 = X_0(Y)$ is sufficiently large so that: 1) $X_0 \geq Y^2$; 2) and for any $X \geq X_0$ and each $F \in E_k(H, Y)$, we have

$$\left| \sum_{\substack{K \in \mathcal{Q}_F^\Sigma \\ \mathrm{Disc}(K/F) \leq \frac{X}{\mathrm{Disc}(F)^2}}} h_3(K/F) - \frac{X}{\mathrm{Disc}(F)^2} \cdot \frac{\mathrm{Res}_{s=1} \zeta_F(s)}{2^{r_1(F)+r_2(F)} \zeta_F(2)} \cdot \left(1 + 3^{-u(\Sigma)}\right) \right| \leq \frac{X}{2^{2^{m-1}} h_3(F) Y |E_k(H, Y)|}.$$

(6.7)

Since there are only finitely many fields $F \in E_k(H, Y)$, such an X_0 formally exists by Theorem 6.9. By Theorem 5.1 and dyadic summation, we find for any $X \geq X_0$

$$\sum_{K \in E_k^\Sigma(G, X)} h_3(K) = \sum_{\substack{K \in E_k^\Sigma(G, X) \\ \mathrm{Disc}(F) \leq Y}} h_3(K) + O_{k,m,\epsilon}(X/Y^{1-\epsilon} + X^{1-\delta_m}),$$

where $F \in E_k^{\bar{\Sigma}}(H, Y)$ is the unique index 2 subfield of K containing k. Then by Lemma 6.8 and Theorem 6.5, we find, for $X \geq X_0$,

$$\sum_{\substack{K \in E_k^\Sigma(G, X) \\ \mathrm{Disc}(F) \leq Y}} h_3(K) = \sum_{F \in E_k^{\bar{\Sigma}}(H, Y)} h_3(F) \sum_{\Sigma_2 \in M_F} 2^{2^{m-1}} \sum_{\substack{[K:F]=2 \\ \text{signature } \Sigma_2 \\ \mathrm{Disc}(K/F) \leq X/\mathrm{Disc}(F)^2}} h_3(K/F) + O_k(X^{1-\delta}).$$

Then by (6.7), for $X \geq X_0$,

$$\sum_{\substack{K \in E_k^\Sigma(G, X) \\ \mathrm{Disc}(F) \leq Y}} h_3(K) = X \sum_{F \in E_k^{\bar{\Sigma}}(H, Y)} \frac{M_\Sigma 2^{2^{m-1}} h_3(F) \mathrm{Res}_{s=1} \zeta_F(s)}{2^{r_1(F)+r_2(F)} \zeta_F(2) \mathrm{Disc}(F)^2} \cdot \left(1 + 3^{-u(\Sigma)}\right) + O_k(X^{1-\delta}) + O(X/Y),$$

and thus also

$$\frac{1}{X} \sum_{K \in E_k^\Sigma(G, X)} h_3(K) = \sum_{F \in E_k^{\bar{\Sigma}}(H, Y)} \frac{M_\Sigma 2^{2^{m-1}} h_3(F) \mathrm{Res}_{s=1} \zeta_F(s)}{2^{r_1(F)+r_2(F)} \zeta_F(2) \mathrm{Disc}(F)^2} \cdot \left(1 + 3^{-u(\Sigma)}\right) + O_{k,m,\epsilon}(Y^{-1+\epsilon} + Y^{-\delta_m} + Y^{-\delta}),$$

since we assumed $X \geq X_0 \geq Y^2$. Letting $Y \to \infty$, the sum over $F \in E_k^{\bar{\Sigma}}(H, Y)$ converges by virtue of Theorem 6.2, the trivial bounds $h_3(F) \ll_{[F:\mathbb{Q}],\epsilon} \mathrm{Disc}(F)^{1/2+\epsilon}$ and $\mathrm{Res}_{s=1} \zeta_F(s) \ll_{[F:\mathbb{Q}],\epsilon} \mathrm{Disc}(F)^\epsilon$, and partial

summation. The error term on the right-hand side also converges, so the left-hand side must converge as well. It follows that

$$\lim_{X\to\infty}\frac{1}{X}\sum_{K\in E_k^{\Sigma}(G,X)}h_3(K)=\sum_{F\in E_k^{\bar{\Sigma}}(H,\infty)}\frac{M_{\Sigma}2^{2^{m-1}}h_3(F)\mathrm{Res}_{s=1}\zeta_F(s)}{2^{r_1(F)+r_2(F)}\zeta_F(2)\,\mathrm{Disc}(F)^2}\cdot\left(1+3^{-u(\Sigma)}\right).$$

Let Σ_0 be a group signature for an H-extension F/k. Then

$$\sum_{\substack{\Sigma\\ \bar{\Sigma}=\Sigma_0}}M_{\Sigma}=2^{r_1(F)}\quad\text{and}\quad\sum_{\substack{\Sigma\\ \bar{\Sigma}=\Sigma_0}}M_{\Sigma}3^{-u(\Sigma)}=\sum_{i=0}^{r_1(F)}\binom{r_1(F)}{i}3^{-i-r_2(F)}=\frac{2^{2r_1(F)}}{3^{r_1(F)+r_2(F)}}.$$

where the sums are over group signatures Σ for G-extensions, since the choices of Σ with i real places of F split have $u(\Sigma)=i+r_2(F)$. We can then sum over all group signatures to obtain

$$\lim_{X\to\infty}\frac{1}{X}\sum_{K\in E_k(G,X)}h_3(K)=\sum_{\bar{\Sigma}}\sum_{\substack{\Sigma\\ \text{given }\bar{\Sigma}}}\sum_{F\in E_k^{\bar{\Sigma}}(H,\infty)}\frac{M_{\Sigma}2^{2^{m-1}}h_3(F)\mathrm{Res}_{s=1}\zeta_F(s)}{2^{r_1(F)+r_2(F)}\zeta_F(2)\,\mathrm{Disc}(F)^2}\cdot\left(1+3^{-u(\Sigma)}\right)$$

$$=\sum_{F\in E_k(H,\infty)}\frac{2^{2^{m-1}}h_3(F)\mathrm{Res}_{s=1}\zeta_F(s)}{2^{r_2(F)}\zeta_F(2)\,\mathrm{Disc}(F)^2}\cdot\left(1+\frac{2^{r_1(F)}}{3^{r_1(F)+r_2(F)}}\right).$$

To count each field K exactly once (instead of once for each G extension structure), we can divide the above sum by $|\mathrm{Aut}_{\mathrm{perm}}(G)|$. We then sum over (isomorphism classes of) G of the form $C_2\wr H$, and by Lemma 6.6 this will give a sum over T_m, the set of all (isomorphism classes of) transitive permutation 2-groups H of degree 2^{m-1}. Using Theorem 6.5, we obtain

$$\lim_{X\to\infty}\frac{1}{X}\sum_{K\in E_k(m,X)}h_3(K)$$

$$=\sum_{H\in T_m}\frac{1}{|\mathrm{Aut}_{\mathrm{perm}}(C_2\wr H)|}\sum_{F\in E_k(H,\infty)}\frac{2^{2^{m-1}}h_3(F)\mathrm{Res}_{s=1}\zeta_F(s)}{2^{r_2(F)}\zeta_F(2)\,\mathrm{Disc}(F)^2}\cdot\left(1+\frac{2^{r_1(F)}}{3^{r_1(F)+r_2(F)}}\right).$$

Above, each field F appears in the sum $|\mathrm{Aut}_{\mathrm{perm}}(H)|$ times. Next, we claim that the factors have value $|\mathrm{Aut}_{\mathrm{perm}}(H)|/|\mathrm{Aut}_{\mathrm{perm}}(C_2\wr H)|=2^{-2^{m-1}}$. The blocks of B_G that $C_2\wr H$ acts on are the pairs that appear in G as transpositions, so these are preserved by any permutation isomorphism of $C_2\wr H$, and we have a map $\mathrm{Aut}_{\mathrm{perm}}(C_2\wr H)\to\mathrm{Aut}_{\mathrm{perm}}(H)$. It is easy to see this is a surjection and the kernel is given by all the permutations of $\{1,2\}\times B_H$ that fix the B_H coordinate, showing the claim. Thus we have

$$\lim_{X\to\infty}\frac{1}{X}\sum_{K\in E_k(m,X)}h_3(K)=\sum_{F\in E_k(m-1,\infty)}\frac{h_3(F)\mathrm{Res}_{s=1}\zeta_F(s)}{2^{r_2(F)}\zeta_F(2)\,\mathrm{Disc}(F)^2}\cdot\left(1+\frac{2^{r_1(F)}}{3^{r_1(F)+r_2(F)}}\right).$$

Combined with Theorem 6.2, this yields the theorem. (Note we may obtain the constants in Theorem 6.2 by the same argument as above, using the count of quadratic extensions of F in Theorem 6.9 in place of the average 3-torsion result.) $\qquad\square$

6.3 Relative Class Group Averages

For the families in Theorem 6.1, the approach of the proof of Theorem 6.1 also permits us to determine the average size of the 3-torsion subgroup of the relative class group $\mathrm{Cl}_{K/F}$, where F is the index two subfield of K, proving Theorem 1.2. These averages are particularly nice when the Galois closure group and $u:=r_1(K)+r_2(K)-r_1(F)-r_2(F)$ is fixed. For G a transitive permutation 2-group with a transposition, let $E_k^u(G,X)$ denote the set of G-extensions K/k with $\mathrm{Disc}\,K\le X$ and K/F of relative unit rank u, where F/k is the unique index 2 subfield of K.

32

Theorem 6.10. *Let k be a number field, m a positive integer, and $G \subseteq S_{2^m}$ a transtive 2-group with a transposition. If u is such that $E_k^u(G, \infty)$ is non-empty, then*

$$\lim_{X \to \infty} \frac{1}{|E_k^u(G, X)|} \sum_{K \in E_k^u(G, X)} h_3(K/F) = 1 + 3^{-u}.$$

Proof. The proof uses the main input we have built for the proof of Theorem 6.1 and is nearly identical to that proof, so we will be brief. Let F/k be the index 2 subfield of K. In particular, using the trivial inequality $h_3(K/F) \leq h_3(K/k)$, it follows from Theorem 5.1 that for any $X, Y > 0$,

$$\sum_{K \in E_k^u(G, X)} h_3(K/F) = \sum_{\substack{K \in E_k^u(G, X) \\ \mathrm{Disc}(F) \leq Y}} h_3(K/F) + O_{k, m, \epsilon}(X/Y^{1-\epsilon} + X^{1-\delta_m}).$$

Again using the trivial inequality $h_3(K/F) \leq h_3(K/k)$, we see from Lemma 6.8 and Theorem 6.5 that

$$\sum_{\substack{K \in E_k^u(G, X) \\ \mathrm{Disc}(F) \leq Y}} h_3(K/F) = \sum_{F \in E_k(H, X)} 2^{2^{m-1}} \sum_{\substack{[K:F]=2 \\ \mathrm{Disc}(K/F) \leq X/\mathrm{Disc}(F)^2 \\ \mathrm{rk}(\mathcal{O}_K^\times / \mathcal{O}_F^\times) = u}} h_3(K/F) + O_{m, k}(X^{1-\delta}),$$

for some $\delta > 0$ depending on m and k. Let r be the number of group signatures of quadratic extensions of F such that K/F of that signature have $\mathrm{rk}(\mathcal{O}_K^\times / \mathcal{O}_F^\times) = u$. We take $X_0(Y)$ as in the proof of Theorem 6.1, and have, for $X \geq X_0$

$$\sum_{\substack{K \in E_k^u(G, X) \\ \mathrm{Disc}(F) \leq Y}} h_3(K/F) = \sum_{F \in E_k(H, X)} \frac{r 2^{2^{m-1} - r_1(F) - r_2(F)} \mathrm{Res}_{s=1} \zeta_F(s)}{\zeta_F(2) \mathrm{Disc}(F)^2} \cdot \left(1 + 3^{-u}\right) + O_{m, k}(X^{1-\delta} + X/Y)$$

Proceeding as in the proof of Theorem 6.1, the result follows. $\qquad\square$

7 Comparison to the Cohen–Martinet heuristics

7.1 Cohen–Martinet prediction for the average of $h_3(K/F)$

Theorem 6.10 verifies new cases of the Cohen–Martinet heuristics, as we now show.

Proposition 7.1. *The Cohen–Martinet heuristics [CM90, Hypothése 6.6] predict that the average of Theorem 6.10 is as proved in the theorem.*

Proof. Let G be a transitive permutation 2-group with a transposition and S_K the stabilizer of an element $1 \in B_G$. Our $K \in \mathcal{F}^u(G)$ is then the S_K fixed field of a Galois G extension $\tilde{K}/k$ with Galois group G. By Lemma 6.6, we have $G = C_2 \wr H$, where H is a permutation group of degree d. In this notation, we have that $S_K = (1 \times C_2^{d-1}) \rtimes \mathrm{Stab}_H(1)$, where $1 \in B_H$ is the image of $1 \in B_G$. Then we define $S_F = (C_2^d) \rtimes \mathrm{Stab}_H(1)$ (the fixed field of S_F will be the field we call F, the index 2 subfield of K). Let U be the sign representation of S_F/S_K over $\mathbb{F}_3$.

We claim $h_3(K/F) = |\mathrm{Hom}_{S_F}(\mathrm{Cl}_{\tilde{K}/k}, U)|$, where Hom_{S_F} denotes morphisms of S_F modules. To see this, let $e \in \mathbb{F}_3[G]$ be the element $e = |S_K|^{-1} \sum_{g \in S_K} g$. We have a map $m_e : \mathrm{Cl}_{\tilde{K}/k}/3 \to \mathrm{Cl}_{K/k}/3$ given by multiplication by e, which is a surjection (as inclusion of ideals gives a section). Since e acts as the identity on U, we have that any element of $\mathrm{Hom}_{S_F}(\mathrm{Cl}_{\tilde{K}/k}, U)$ factors through m_e, so is determined by a map $\mathrm{Hom}_{S_F}(\mathrm{Cl}_{K/k}/3, U)$. Now $\mathrm{Cl}_{K/k}/3$ is a product of ± 1 eigenspaces for S_F/S_K, and $\mathrm{Cl}_{K/F}/3$ is exactly the -1 eigenspace, which proves the claim.

Let $V := \mathrm{Ind}_{S_F}^G U$. We claim that V is an irreducible representation of G. If h_i are coset representatives of $\mathrm{Stab}_H(1)$ in H, then $1 \rtimes h_i$ are coset representatives for S_F in G. Then V has a basis $e_i := (1 \rtimes h_i)e_1$. The action of G on V is $(x \rtimes s)e_i = x_{s(i)}e_{s(i)}$. So on the one hand, it is permuting the e_i from the permutation action of s, and on the other hand, it can change the sign for any particular basis independently. Thus if

$\sum c_i e_i$ is a non-zero element of V, we can act by some $g \in G$ to obtain $gx = e_1$, and thus we can generate all of V from G actions, which shows that V is irreducible.

So,

$$|\operatorname{Hom}_{S_F}(\operatorname{Cl}_{\tilde{K}/k}, U)| = |\operatorname{Hom}_G(\operatorname{Cl}_{\tilde{K}/k}, V)| = 1 + |\operatorname{Sur}_G(\operatorname{Cl}_{\tilde{K}/k}, V)|.$$

From [WW21, Theorem 6.2 and Theorem 4.1], we have that Cohen and Martinet predict the average of $|\operatorname{Sur}_G(\operatorname{Cl}_{\tilde{K}/k}, V)|$ to be $\prod_v = |V^{\sigma_v}|^{-1}$, where the product is over infinite places of the base field k, and σ_v is a decomposition group for v. (Note that we can subdivide our family, which only has a fixed relative unit rank of K/F, based on their decomposition groups at each of the infinite places of k. We will see that the prediction for each of these subfamilies is the same, and only depends on the relative unit rank of K/F.) The action of σ_v on the elements that H acts on, or equivalently the cosets $h_i S_F$, has fixed points corresponding to the infinite places of F (over v) that are split over k and 2-cycles corresponding to infinite places of F (over v) that are ramified over k. We can write σ_v as generated by $x_v \rtimes r_v$. If h_i corresponds to a fixed point of r_v, then $\sigma_v \mathbb{F}_3 e_i = \mathbb{F}_3 e_i$, and the corresponding infinite place of F is split in K if and only if the ith coordinate of x_v is trivial, which happens if and only if $\mathbb{F}_3 e_i$ is a trivial representation of σ_v. If h_i and h_j correspond to a 2-cycle of r_v, then $\mathbb{F}_3 e_i + \mathbb{F}_3 e_j$ is the regular representation of σ_v and has one dimension of trivial representation. Thus $\sum_v \dim_{\mathbb{F}_3} V^{\sigma_v}$ is the number of infinite places of F that are not ramified in K, which is exactly the relative unit rank as defined above. $\qquad \square$

7.2 Cohen–Martinet prediction for the average of $h_3(K/k)$

Using a similar approach, we can determine the Cohen–Martinet prediction for the average of $h_3(K/k)$ for G-extensions K/k of a particular enriched or group signature. In the case when $G = D_4$, we give below a numerical computation of the proven average for comparison.

Let G be a transitive permutation 2-group with a transposition and S_K the stabilizer of an element. We consider the representation $\operatorname{Ind}_{S_K}^G \mathbb{F}_3$ of G over $\mathbb{F}_3$ (which is the permutation representation of G). Define S_K, S_F, U, and V as in the proof of Proposition 7.1. Then $\operatorname{Ind}_{S_K}^G \mathbb{F}_3 = \operatorname{Ind}_{S_F}^G \operatorname{Ind}_{S_K}^{S_F} \mathbb{F}_3 = \operatorname{Ind}_{S_F}^G \mathbb{F}_3 \times V$. Let $W = \operatorname{Ind}_{S_F}^G \mathbb{F}_3$, which is the permutation representation of H. We see that W contains no copies of the irreducible representation V, since the action G on W factors through H and the action of G on V does not.

Suppose that $W = \prod_i V_i^{a_i}$, where the V_i are irreducible representations of G (and note they all have G-action that factors through H). We note that by Frobenius reciprocity that W contains exactly one copy of the trivial representation, and let W' be the quotient of of W by this trivial representation.

We have $h_3(K/k) = |\operatorname{Hom}(\operatorname{Cl}_{K/k}, \mathbb{F}_3)|$. Let e, m_e be as in the proof of Proposition 7.1. Since any element of $\operatorname{Hom}_{S_K}(\operatorname{Cl}_{\tilde{K}}, \mathbb{F}_3)$ factors through $m_e \operatorname{Cl}_{\tilde{K}/k} = \operatorname{Cl}_{K/k}$, we have a natural bijection between $\operatorname{Hom}(\operatorname{Cl}_{K/k}, \mathbb{F}_3)$ and $\operatorname{Hom}_{S_K}(\operatorname{Cl}_{\tilde{K}/k}, \mathbb{F}_3)|$. Also $|\operatorname{Hom}_{S_K}(\operatorname{Cl}_{\tilde{K}/k}, \mathbb{F}_3)| = |\operatorname{Hom}_G(\operatorname{Cl}_{\tilde{K}/k}, W \times V)|$. If we let $e' = |G|^{-1} \sum_{g \in G} g$, we have that the map $m_e : \operatorname{Cl}_{\tilde{K}} \to \operatorname{Cl}_k$ is a map whose kernel is exactly the relative class group $\operatorname{Cl}_{\tilde{K}/k}$, and it is also the map that gives the maximal trivial representation quotient of any G representation. Thus $\operatorname{Cl}_{\tilde{K}/k}$ has no trivial representation part, and $h_3(K/k) = |\operatorname{Hom}_G(\operatorname{Cl}_{\tilde{K}/k}, W' \times V)|$.

From [WW21, Theorem 6.2, Theorem 4.1], for a G-representation Z with no trivial component, we have that Cohen and Martinet predict the average of $|\operatorname{Sur}_G(\operatorname{Cl}_{\tilde{K}}, Z)|$ to be $\prod_v = |Z^{\sigma_v}|^{-1}$, where the product is over infinite places v of the base field k, in a family of G-extensions where $\sigma_v \in G$ is an element of the conjugacy class of complex conjugation over v. Thus the predicted average of $h_3(K/k)$ is

$$\left(1 + \prod_v |V^{\sigma_v}|^{-1}\right) \prod_i \left(1 + \prod_v |V_i^{\sigma_v}|^{-1} + \cdots + \prod_v |V_i^{\sigma_v}|^{-a_i}\right),$$

where the left product is the predicted average of $h_3(K/F)$ and the right product is the predicted average of $h_3(F/k)$ (as can be worked out similarly to the above) for families with the corresponding behavior at infinite places.

Let F/k be the index two subfield of K. The action of σ_v on the permutation basis elements of W has fixed points corresponding to the split places of F (over v) and 2-cycles corresponding to the ramified places of F (over v). Thus $\prod_v |W^{\sigma_v}| = 3^{r_1(F)+r_2(F)}$ and $\prod_v |(W')^{\sigma_v}| = 3^{r_1(F)+r_2(F)-r_1(k)-r_2(k)}$. If W' is irreducible, this gives a nice formula for the predicted average of $h_3(K/k)$, which is $(1 + 3^{-u(K/F)})(1 + 3^{-u(F/k)})$, where

$u(K/F)$ is the difference in unit ranks of K and F in the given family (and similarly for $u(F/k)$) . However, when W is not irreducible, the formula can be more complicated.

Example 7.2. *Let $H = C_2$, so $G = D_4 = \langle(1234),(24)\rangle$ and $S_K = \langle(24)\rangle$ and $S_F = \langle(13),(24)\rangle$. Here W' is irreducible, the sign representation of H, and thus the average conjecture by Cohen and Martinet is $(1 + 3^{-u(K/F)})(1 + 3^{-u(F/k)})$. For example, if $k = \mathbb{Q}$, in the following table we give the averages of $h_3(K)$ predicted by the Cohen–Martinet heuristics, and a numerical computation of the proven averages from Theorem 6.1, in families with the given group signatures.*

σ_v	F	$r_1(K)$	$|V^{\sigma_v}|$	$|(W')^{\sigma_v}|$	*CM predicted average of $h_3(K)$*	*Thm 6.1 proven average of $h_3(K)$*
$()$	*real*	*4*	*9*	*3*	$(1 + 1/9)(1 + 1/3) = 40/27 \approx 1.48$	≈ 1.12
(24)	*real*	*2*	*3*	*3*	$(1 + 1/3)(1 + 1/3) = 16/9 \approx 1.78$	≈ 1.34
$(13)(24)$	*real*	*0*	*1*	*3*	$(1 + 1)(1 + 1/3) = 8/3 \approx 2.67$	≈ 2.01
$(12)(34)$	*imag.*	*0*	*3*	*1*	$(1 + 1/3)(1 + 1) = 8/3 \approx 2.67$	≈ 1.41

Essentially, in the proof of Theorem 6.1, we see that the averages of the $h_3(K/F)$ and $h_3(F/k)$ factors are independent, and the $h_3(K/F)$ has average as predicted by Cohen and Martinet. When we order fields in a family up to discriminant X, and take a uniform average and then let $X \to \infty$, we will call this a *discriminant-uniform* average. A consequence of Cohen and Martinet's conjecture is that the discriminant-uniform average *over G extensions K* of $h_3(F_K/k)$ is the same as the discriminant-uniform average *over H extensions F* of $h_3(F/k)$ when the G and H extensions have corresponding behavior at infinite places (see [WW21, Theorem 9.2]).

In contrast, what we see in the proof of Theorem 6.1 is that discriminant-uniform average over G extensions K of $h_3(F_K/k)$ is provably a *weighted* average of $h_3(F/k)$ over F, against the measure on H-extensions in which a field F has measure proportional to $\text{Res}_{s=1}\, \zeta_F(s)/(\zeta_F(2)\,\text{Disc}(F)^2)$. There is no particular reason to think that this weighted average of $h_3(F/k)$ over F will give the same result as the discriminant-uniform average over F. Indeed, the weighted average is heavily influenced by the F of small discriminant. When $H = C_2$, the discriminant uniform average over C_2-extensions F of $h_3(F/k)$ is known by Datskovsky–Wright, and is as predicted by Cohen–Martinet.

Since the quadratic fields of small discriminant have very little 3-torsion in their class groups, one expects the weighted average of $h_3(F/k)$ to be smaller than the discriminant-uniform average over F, and indeed that is what we see in the chart above.

8   Averages for other groups

Our methods apply to more groups than just 2-groups. We focus here on results that may be obtained purely from the results of Section 3, and whose proofs in particular do not rely on arguments from Sections 2 and 4. This permits a proof of the following general result.

Theorem 8.1. *Let $H \subseteq S_n$ be transitive and set $G = C_2 \wr H$. Then G-extensions K of a number field k have a unique index two subfield F_K/k. Moreover F_K is an H-extension of k. For $u \in \mathbb{Z}$, let $E_k^u(G,X) \subseteq E_k(G,X)$ be the subset of those K for which $\text{rk}\,\mathcal{O}_K^* - \text{rk}\,\mathcal{O}_{F_K}^* = u$.*

1) If $E_k^u(G,\infty)$ is non-empty and $|E_k(H,X)| \ll_{k,H,\epsilon} X^{2/3+\epsilon}$ for every $X \geq 1$, then

$$\lim_{X \to \infty} \frac{1}{E_k^u(G,X)} \sum_{K \in E_k^u(G,X)} h_3(K/F_K) = 1 + 3^{-u}.$$

2) If $E_k(H,\infty)$ is non-empty and

$$\sum_{F \in E_k(H,X)} h_3(F/k) \ll_{k,H,\epsilon} X^{2/3+\epsilon}$$

for every $X \geq 1$, then there is an explicit constant $c_{k,G,3}$ such that

$$\lim_{X \to \infty} \frac{1}{E_k(G,X)} \sum_{K \in E_k(G,X)} h_3(K) = c_{k,G,3}.$$

35

Before we discuss the proof of Theorem 8.1, we note that the hypotheses of the first case are satisfied, for example, by any group $H \neq C_2$ in its regular representation that occurs as a Galois group over k [EV06, Proposition 1.3], and by any nilpotent group H without a transposition [Alb20, Corollary 1.8]. The hypotheses of the second case are satisfied for any p-group with $p \neq 5$ odd, as follows from [KM04, Corollary 7.3] and the trivial bound on $h_3(F/k)$ for $p \geq 7$, and from [KW20] for $p = 3$.

Proof. The claims about the subfield F_K follows as in Lemma 6.6. Suppose now that $E_k^u(G, \infty)$ is non-empty. We mimic the proof of Theorem 6.1, indicating the necessary modifications. Let $X \geq 1$. From Corollary 3.2, it follows for any $Y \geq 1$ that

$$\sum_{\substack{K \in E_k^u(G,X) \\ \mathrm{Disc}(F_K) \geq Y}} h_3(K/F_K) \ll_{[k:\mathbb{Q}],G,\epsilon} \sum_{F \in E_k(H,X^{1/2}) \setminus E_k(H,Y)} \frac{h_2(F)^{2/3} X}{\mathrm{Disc}(F)^{1-\epsilon}} \ll_{[k:\mathbb{Q}],G,\epsilon} \frac{X}{Y^{\frac{1}{3n[k:\mathbb{Q}]}-\epsilon}},$$

where the second inequality is by partial summation and [BST$^+$20, Theorem 1.1]. This provides an analogue of Theorem 5.1. We now establish a soft analogue of Theorem 6.5, with the remainder of the proof then proceeding as in those of Theorems 6.1 and 6.10. Note that if $G' \subseteq G$ surjects onto H and contains an element conjugate to $\sigma = (1, 0, \ldots, 0) \rtimes 1_H$ in G, then in fact $G' = G$.

For any fixed H-extension F with discriminant at most Y, let $\mathcal{P}$ be a finite set of primes of k that split completely in F. If some prime of F above a prime $\mathfrak{p} \in \mathcal{P}$ is inert in a quadratic extension K/F, while all the other primes of F above $\mathfrak{p}$ are split in K, then by the note above we have that K/k is a $C_2 \wr H$ extension. If this happens, then we say that $\mathfrak{p}$ is bad for K/F. It follows from the methods of Datskovsky and Wright [DW86, DW88] (see also [BSW15, Theorem 2]) that

$$\sum_{\substack{[K:F]=2 \\ \text{group signature } \Sigma \\ \mathrm{Disc}(K/F) \leq X \\ \forall \mathfrak{p} \in \mathcal{P}, \mathfrak{p} \text{ not bad}}} h_3(K/F) \sim X \prod_{\mathfrak{p} \in \mathcal{P}} \left(1 - \frac{n \, \mathrm{Nm}_{k/\mathbb{Q}} \mathfrak{p}^n}{2^n (\mathrm{Nm}_{k/\mathbb{Q}} \mathfrak{p} + 1)^n}\right) \cdot \frac{\mathrm{Res}_{s=1} \zeta_F(s)}{2^{r_1(F)+r_2(F)} \zeta_F(2)} (1 + 3^{-u(\Sigma)}).$$

The expressions in the product above are uniformly (in $\mathfrak{p}$) bounded away from 1, and in particular the product is $O(\beta_n^{\#\mathcal{P}})$ for some constant $\beta_n < 1$ depending at most on n. Since there are infinitely many primes that split completely in F, this product may be made arbitrarily small, and thus

$$\sum_{\substack{[K:F]=2 \\ \mathrm{Disc}(K/F) \leq X \\ \mathrm{Gal}(K/k) \not\simeq G}} h_3(K/F) = o_F(X).$$

Proceeding now as in the proof of Theorem 6.1, the first claim follows. The second follows analogously. $\square$

References

[Alb20]   Brandon Alberts. The weak form of Malle's conjecture and solvable groups. *Res. Number Theory*, 6(1):Paper No. 10, 23, 2020.

[An20]   Chen An. ℓ-torsion in class groups of certain families of D_4-quartic fields. *Journal de Théorie des Nombres de Bordeaux*, 32(1):1–23, 2020.

[ASVW21] S. Ali Altuğ, Arul Shankar, Ila Varma, and Kevin H. Wilson. The number of D_4-fields ordered by conductor. *J. Eur. Math. Soc. (JEMS)*, 23(8):2733–2785, 2021.

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

[BL20]   Alex Bartel and Hendrik W. Lenstra. On class groups of random number fields. *Proceedings of the London Mathematical Society*, 121(4):927–953, 2020.

[Bra47]   Richard Brauer. On the zeta-functions of algebraic number fields. *Amer. J. Math.*, 69:243–250, 1947.

[BST13]   M. Bhargava, A. Shankar, and J. Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.*, 193:439–499, 2013.

[BST+20]   M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *J. Amer. Math. Soc.*, 33(4):1087–1099, 2020.

[BSW15]   Manjul Bhargava, Arul Shankar, and Xiaoheng Wang. Geometry-of-numbers methods over global fields i: Prehomogeneous vector spaces. 2015.

[BTT21]   Manjul Bhargava, Takashi Taniguchi, and Frank Thorne. Improved error estimates for the Davenport-Heilbronn theorems. *arXiv:2107.12819 [math]*, July 2021.

[BV16]   Manjul Bhargava and Ila Varma. The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders. *Proc. Lond. Math. Soc. (3)*, 112(2):235–266, 2016.

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

[CM87]   H. Cohen and J. Martinet. Class groups of number fields: Numerical heuristics. *Mathematics of Computation*, 48(177):123–137, 1987.

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

[CyDO02]   H. Cohen, F. Diaz y Diaz, and M. Olivier. Enumerating quartic dihedral extensions of $\mathbb{Q}$. *Compositio Math.*, 133(1):65–93, 2002.

[DH71]   H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London. Ser. A*, 322(1551):405–420, 1971.

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

[DW88]   Boris Datskovsky and David J. Wright. Density of discriminants of cubic extensions. *J. Reine Angew. Math.*, 386:116–138, 1988.

[EPW17]   Jordan Ellenberg, Lillian B. Pierce, and Melanie Matchett Wood. On ℓ-torsion in class groups of number fields. *Algebra Number Theory*, 11(8):1739–1778, 2017.

[EV06]   J. S. Ellenberg and A. Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math.*, pages 723–741, 2006.

[EV07]   Jordan S. Ellenberg and Akshay Venkatesh. Reflection principles and bounds for class group torsion. *Int. Math. Res. Not. IMRN*, (1):Art. ID rnm002, 18, 2007.

[FK06]   Étienne Fouvry and Jürgen Klüners. On the 4-rank of class groups of quadratic number fields. *Inventiones mathematicae*, 167(3):455–513, November 2006.

[FS99]   Eduardo Friedman and Nils-Peter Skoruppa. Relative regulators of number fields. *Invent. Math.*, 135(1):115–144, 1999.

[FW18]   Christopher Frei and Martin Widmer. Average bounds for the ℓ-torsion in class groups of cyclic extensions. *Research in Number Theory*, 4(3):34, August 2018.

[FW21]   Christopher Frei and Martin Widmer. Averages and higher moments for the ℓ-torsion in class groups. *Mathematische Annalen*, 379(3):1205–1229, April 2021.

[HL21]   Robert Hough and Eun Hye Lee. Subconvexity of Shintani's zeta functions, 2021.

[HP17]   D. R. Heath-Brown and L. B. Pierce. Averages and moments associated to class numbers of imaginary quadratic fields. *Compositio Mathematica*, 153(11):2287–2309, November 2017.

[HV06]   H. A. Helfgott and A. Venkatesh. Integral points on elliptic curves and 3-torsion in class groups. *J. Amer. Math. Soc.*, 19(3):527 – 550, 2006.

[IK04]   Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

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

[Kly20]   Jack Klys. The distribution of p-torsion in degree p cyclic fields. *Algebra Number Theory*, 14(4):815–854, 2020.

[KM04]   Jürgen Klüners and Gunter Malle. Counting nilpotent Galois extensions. *J. Reine Angew. Math.*, 572:1–26, 2004.

[KW20]   Jürgen Klüners and Jiuya Wang. ℓ-torsion bounds for the class group of number fields with an ℓ-group as galois group. 2020.

[LMO79]   J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54(3):271–296, 1979.

[LOTZ21]   Robert J. Lemke Oliver, Jesse Thorner, and Asif Zaman. An approximate form of Artin's holomorphy conjecture and non-vanishing of Artin L-functions. 2021.

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

[Mal04]   G. Malle. On the distribution of Galois groups, II. *Experiment. Math.*, 13(2):129–135, 2004.

[Pas17]   Hector Pasten. Shimura curves and the abc conjecture. Appendix by R.J. Lemke Oliver and J. Thorner. *arXiv e-prints*, page arXiv:1705.09251, May 2017.

[Pie05]   L. B. Pierce. The 3-part of class numbers of quadratic fields. *J. London Math. Soc.*, 71:579–598, 2005.

[Pie06]   L. B. Pierce. A bound for the 3-part of class numbers of quadratic fields by means of the square sieve. *Forum Math.*, (18):677–698, 2006.

[PTBW20]   Lillian B. Pierce, Caroline L. Turnage-Butterbaugh, and Melanie Matchett Wood. An effective Chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups. *Invent. Math.*, 219(2):701–778, 2020.

[Sch08]   R. Schoof. Computing arakelov class groups. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 447–495. Cambridge Univ. Press, Cambridge, 2008.

[Shi72]   Takuro Shintani. On Dirichlet series whose coefficients are class numbers of integral binary cubic forms. *J. Math. Soc. Japan*, 24:132–188, 1972.

[Smi17]   Alexander Smith. 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. *arXiv:1702.02325 [math]*, February 2017.

[Sou00]   K. Soundararajan. Divisibility of class numbers of imaginary quadratic fields. *J. London Math. Soc. (2)*, 61(3):681–690, 2000.

[Sta74]   H. M. Stark. Some effective cases of the Brauer-Siegel theorem. *Invent. Math.*, 23:135–152, 1974.

[Tan06]   Takashi Taniguchi. Distributions of discriminants of cubic algebras. *arXiv Mathematics e-prints*, page math/0606109, Jun 2006.

[Tho11]   F. Thorne. Four perspectives on secondary terms in the Davenport-Heilbronn theorems. *Integers Volume 12 B, Proceedings of the Integers Conference 2011*, 2011.

[TT13]   T. Taniguchi and F. Thorne. Secondary terms in counting functions for cubic fields. *Duke Math. J.*, 162(13):2451–2508, 2013.

[TZ17]   Jesse Thorner and Asif Zaman. An explicit bound for the least prime ideal in the Chebotarev density theorem. *Algebra Number Theory*, 11(5):1135–1197, 2017.

[TZ19a]   Jesse Thorner and Asif Zaman. A unified and improved Chebotarev density theorem. *Algebra Number Theory*, 13(5):1039–1068, 2019.

[TZ19b]   Jesse Thorner and Asif Zaman. A zero density estimate for Dedekind zeta functions. *arXiv:1909.01338 [math]*, September 2019.

[TZ21]   Jesse Thorner and Asif Zaman. An unconditional GL_n large sieve. *Adv. Math.*, 378:107529, 24, 2021.

[Š54]   I. R. Šafarevič. Construction of fields of algebraic numbers with given solvable Galois group. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 18:525–578, 1954.

[Wan20]   Jiuya Wang. Pointwise Bound for ℓ-torsion in Class Groups II: Nilpotent Extensions. *arXiv:2006.10295 [math]*, June 2020.

[Wan21]   Jiuya Wang. Pointwise bound for ℓ-torsion in class groups: Elementary abelian extensions. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2021(773):129–151, April 2021.

[Wid18]   Martin Widmer. Bounds for the ℓ-torsion in class groups. *Bulletin of the London Mathematical Society*, 50(1):124–131, 2018.

[Woo18]   Melanie Matchett Wood. Cohen-Lenstra heuristics and local conditions. *Research in Number Theory*, 4(4):41, September 2018.

[Wri82]   David James Wright. *DIRICHLET SERIES ASSOCIATED WITH THE SPACE OF BINARY CUBIC FORMS WITH COEFFICIENTS IN A NUMBER FIELD*. ProQuest LLC, Ann Arbor, MI, 1982. Thesis (Ph.D.)–Harvard University.

[Wri85]   David J. Wright. The adelic zeta function associated to the space of binary cubic forms. I. Global theory. *Math. Ann.*, 270(4):503–534, 1985.

[Wri89]   David J. Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc. (3)*, 58(1):17–50, 1989.

[WW21]   Weitong Wang and Melanie Matchett Wood. Moments and interpretations of the Cohen–Lenstra–Martinet heuristics. *Commentarii Mathematici Helvetici*, 96(2):339–387, June 2021.

[Zam17]   A. Zaman. Analytic estimates for the Chebotarev density theorem and their applications. *Ph.D. thesis, University of Toronto*, 2017.