Spring 2020

Counting Number Fields by Discriminant

Harsh Mehta

Counting number fields by discriminant

by

Harsh Mehta

Bachelor of Science
University of Michigan Ann Arbor, 2013

Submitted in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy in

Mathematics

College of Arts and Sciences

University of South Carolina

2020

Accepted by:

Frank Thorne, Major Professor

Duncan Buell, Committee Member

Matthew Boylan, Committee Member

Ognian Trifonov, Committee Member

Alexander Duncan, Committee Member

Cheryl L. Addy, Vice Provost and Dean of the Graduate School

Dedication

I'd like to dedicate this to my family.

Acknowledgments

I'd like to thank the following people for helping me get to this point in time of my life, in a mathematical sense and in a non mathematical sense.

1. My advisor Frank Thorne for introducing me to the world of counting number fields. I'd like to thank him for his ability to know when I should question my half formed ideas and when I should encourage me pursue them a bit more. He has also drilled in, despite my stubbornness to accept, the importance of good writing. Without Frank, none of this would have been possible.

2. Alex Duncan for helping me think through various group theoretic problems that I have had along the way.

3. Ognian Trifonov for engaging in many conversations about analytic number theory with me.

4. Jeffrey Lagarias and Hugh Montgomery for introducing me to the world of mathematical research and giving me fun hands on problems.

5. My friends for helping me remain sane and having fun conversations with me, in particular, Rachel, Duncan, Hays, Chris and Aditya.

Abstract

The central topic of this dissertation is counting number fields ordered by discriminant. We fix a base field k and let $N_d(k, G; X)$ be the number of extensions N/k up to isomorphism with $\mathcal{N}_{k/\mathbb{Q}}(d_{N/k}) \leq X$, $[N : k] = d$ and the Galois closure of N/k is equal to G.

We establish two main results in this work. In the first result we establish upper bounds for $N_{|G|}(k, G; X)$ in the case that G is a finite group with an abelian normal subgroup. Further, we establish upper bounds for the case $N_{|F|}(k, G; X)$ where G is a Frobenius group with an abelian Frobenius kernel F.

In the second result we establish is an asymptotic expression for $N_6(\mathbb{Q}; A_4; X)$. We show that $N_6(\mathbb{Q}, A_4; X) = CX^{1/2} + O(X^{0.426\cdots})$ and indicate what is expecedted under the ℓ-torsion conjecture and the Lindelöf Hypothesis.

We begin this work by stating the results that are established here precisely, and giving a historical overview of the problem of counting number fields.

In Chapter 2, we establish background material in the areas of ramification of prime numbers and analytic number theory.

In Chapter 3, we establish the asymptotic result for $N_6(\mathbb{Q}, A_4; X)$.

In Chapter 4, we establish upper bounds for $N_d(k, G; X)$ for groups with a normal abelian subgroup and for Frobenius groups. Finally we conclude with Chapter 5 with certain extensions of the method. In particular, we indicate how to count extensions of different degrees and discuss how to use tools about average results on the size of the torsion of the class group on almost all extensions in a certain family.

Table of Contents

Chapter 1

Notation

Note that throughout this work, we say $f(X) \ll_{a,b} g(X)$ when there exist positive constants C and N such that for all $X > N$, we have $|f(X)| \leq C|g(X)|$ where the constant C depends on the parameters a and b.

We say that $f(X) = O_{a,b}(g(X))$ if and only if $f(X) \ll_{a,b} g(X)$.

We say that $f(X) = o(g(X))$ when $\lim_{X\to\infty} f(X)/g(X) = 0$.

We say $f(X) \sim g(X)$ when $\lim_{X\to\infty} f(X)/g(X) = 1$.

G will represent a finite group.

$\mathcal{O}_k$ will denote the ring of integers of the number field k.

$d_{N/k}$ will always represent the relative discriminant of the field extension N/k.

$\mathcal{N}_{M/\mathbb{Q}}(\mathfrak{a})$ will denote the relative norm of an element $\mathfrak{a}$ in M over $\mathbb{Q}$.

Cl_k will denote the class group of the number field k.

p will denote a prime number.

ϵ will always be an arbitrarily small positive constant.

Chapter 2

Preliminaries

The central topic of this work, and a central theme in arithmetic statistics, is counting number fields ordered by discriminant. Asking how many number fields exist, after restricting certain parameters, is a natural question to ask. In this chapter we indicate some of the main areas of study in arithmetic statistics, state the results that will be established here and indicate some of the prevalent methods used to attack these problems.

The central questions are variants of how many number fields exist. One can order them by invariants such as discriminant, conductor, or product of primes that divide the discriminant. One can focus their investigation on dependencies on the degree of the extension, or the Galois group. A problem closely related to counting the number of abelian extensions of number fields is the problem of uncovering information about the size of the torsion of the class group. In this work we will investigate counting number fields ordered by discriminant and realize some of the connections to the size of the torsion of the class group.

Before we explore the techniques used to count number fields, we explore what we expect. The works of Hermite (1857) together with Minkowski's lattice point theorem imply that up to isomorphism there are only a finite number of number fields with any given fixed discriminant. A conjecture usually attributed to Linnik states:

Conjecture 2.0.1. *The number of extensions of any base field k with any fixed degree d with discriminant at most X is $O_{d,k}(X)$.*

This conjecture is far from resolved, but there is a lot of progress in this direction once we fix the Galois closure. We now introduce some terminology. Let $G \neq \{1\}$ be a represented as a transitive subgroup of S_d. Let $N_d(k, G; X)$ be defined as follows

$$N_d(k, G; X) := |\{K/k : \mathrm{Gal}(\hat{K}/k) \cong G, [K : k] = d, \text{ and } \mathcal{N}_{k/\mathbb{Q}}(d_{K/k}) \leq X\}|. \quad (2.0.1)$$

There is a conjecture towards the expected size of $N_d(k, G; X)$ stated by Malle which we explain in the next section.

The first result along these lines is counting the number of quadratic extensions of $\mathbb{Q}$ ordered by discriminant, $N_2(\mathbb{Q}, X)$. We will summarize a strategy to count quadratic extensions. Each discriminant is either such that $d_{k/\mathbb{Q}} \equiv 1 \pmod 4$ and square free, or $d_{k/\mathbb{Q}} = 4n$ where $n \equiv 2, 3 \pmod 4$ and n is square free. The first step is to create a Dirichlet series $\Psi(C, 2, s) = \sum_{|d_{k/\mathbb{Q}}|} |d_{k/\mathbb{Q}}|^{-s} = \sum_{n \geq 1} a_n n^{-s}$ and attain an Euler product representation of $\Psi(C_2, s)$. The Euler product that is attained is

$$\Psi(C_2, s) = \sum_{n \geq 1} \frac{a_n}{n^s} = \left(1 - \frac{1}{2^s} + \frac{2}{2^{2s}}\right) \frac{\zeta(s)}{\zeta(2s)} - 1.$$

Now using Perron's formula and the residue theorem, we can calculate $\sum_{n \leq X} a_n$. To evaluate the zeta function in the critical strip, we use the subconvexity estimate $|\zeta(1/2 + it)| \ll t^{1/6} \log(t)$ that was established by Hardy and Littlewood (see Titchmarsh (1986) Chapter 5). Putting the prices together gives us

$$N_2(\mathbb{Q}, X) = \frac{6}{\pi^2} X + o(X^{1/2}).$$

As stated in Cohen, Diaz y Diaz, and Olivier (2002b), under the Riemann Hypothesis, we expect it to be $O(X^{8/25})$. We elaborate on subconvexity estimates and Perron's formula in Chapater 3.

Counting number fields in higher degree gets a more difficult. Once we start controlling parameters such as the Galois group, we are able to make more breakthroughs, especially in terms of establishing upper bounds. Finding asymptotic expressions associated to $N_d(k, G; X)$ is quite difficult, but it has been done in some cases.

In the remainder of this chapter we will state the results that will be proved in this work and give some context to where they fit in the area of arithmetic statistics. In Section 2.2 we survey known results and briefly describe some of the approaches that are used to find an upper bound for or asymptotic expression for $N_d(k, G; X)$.

In Chapter 3 we go over background material that will be necessary to prove the main results. Section 3.1 will cover information about how primes ramify in number field extensions. Section 3.2 will cover information in complex analysis and analytic number theory.

In Chapter 4 we derive an asymptotic expression for $N_6(\mathbb{Q}, A_4; X)$. In Chapter 5 we derive upper bounds for $N_d(k, G; X)$ in the case that G is a group that has an abelian normal subgroup and in the case that G is a Frobenius group.

Finally, in Chapter 6.1 we explain two extensions of the the method. The first extension indicates how to count extensions of degrees that don't correspond to Galois extensions of Frobenius extensions. The second extension explains how recent developments in understanding the size of the torsion of the class group for almost all number fields in a specified family may be applicable to our results.

2.1 Statement of main results

In this section we state the main results that will be established in this work and try to provide some context of where they belong in the field of arithmetic statistics. First we state Malle's conjecture.

Definition 2.1.1. Let G be a non-trivial subgroup of the permutation group S_d. Let G act transitively on $[d] := \{1, 2, \ldots, d\}$ and let $g \in G$.

1. The index of g, is $\text{ind}(g) := d-$ the number of orbits of g on $[d]$.
2. $\text{ind}(G) := \min\{\text{ind}(g) : 1 \neq g \in G\}$.
3. $a(G, d) := 1/\text{ind}(G)$.

In Malle (2002), Malle conjectured that:

Conjecture 2.1.2. (Malle's weak conjecture) *For any non-trivial group $G \leq S_d$ acting transitively on $[d]$, and any number field k,*

$$X^{a(G,d)} \ll N_d(k, G; X) \ll X^{a(G,d)+\epsilon} \tag{2.1.1}$$

holds for all $\epsilon > 0$ as $X \to \infty$.

In fact Malle (2004) went on to refine his conjecture by getting rid of the X^{ϵ} above and making a conjecture of the shape

$$N_d(k, G; X) \sim c(k, G) X^{a(G,d)} \left(\log(X)\right)^{b(k,G)}$$

for an explicitly stated constant $b(k, G)$. This conjecture was shown to be false by Klüners (2005). It is still believed to be mostly true outside of a few cases. With that said, there are still no known counter examples to his weak conjecture. We present some instances of the implications of his conjecture here.

Example 2.1.3.

1. Let $G = S_n$ act on the set of n elements by its usual permutation representation. Every permutation group has a transposition ρ and the transposition is the element with most orbits. Consequently, $\mathrm{ind}(\rho) = n-(n-1)$ and hence $a(S_n, n) = 1$. This shows that (if we expect Malle's conjecture) Linnik's conjecture is best possible unless we fix the Galois group.

   For $n \leq 5$ we have an asymptotic main term for $N_n(\mathbb{Q}, S_n; X)$ thanks to the works of Davenport and H. Heilbronn (1971), Bhargava (2005) and Bhargava (2010).

2. Let $G = A_n$ be the alternating group with $n > 3$ acting on the set of n elements. In this case, A_n always has an element ρ that is a 3 cycle, and the three cycles are the elements with the most number of orbits. Hence $\mathrm{ind}(\rho) = 2$ and $a(A_n, n) = 1/2$.

3. Let G be any finite abelian group acting on the set of $|G|$ elements where the action is the same as left multiplication of G acting on itself. Let $\rho \in G$ be an element of order p such that p is the smallest prime divisor of $|G|$. In this case ρ is the element with the most orbits, $|G|/p$ orbits in particular. Hence $a(G, |G|) = p/(|G|(p-1))$ and $N_{|G|}(k, G; X) = O(X^{a(G,|G|)+\epsilon})$. This has been established by Wright (1989).

4. Let $G = D_\ell = \{r, s | r^\ell = s^2 = (sr)^2 = 1\}$ be the dihedral group of size 2ℓ, with ℓ an odd prime. Let G act on $[\ell] = \{1, \ldots, \ell\}$. In particular,

$$s = (1)(\ell \;\; 2)(\ell - 1 \;\; 3)(\ell - 2 \;\; 4)\ldots\left(\frac{\ell+3}{2} \;\; \frac{\ell+1}{2}\right)$$
$$r^k = (1 \;\; 1+k \;\; 1+2k \;\; \ldots \;\; 1+(\ell-1)k)$$

and elements of the form sr^k will be a product of transpositions of the form $((1+xk) \;\; (\ell+1-(x+1)k))$ with a fixed point at $(1+\frac{\ell-1}{2}k)$. The rotations r^k, with $\ell \nmid k$ have one orbit, therefore $\text{ind}(r^k) = \ell - 1$. Elements of the form sr^k have one fixed point and $(\ell-1)/2$ transpositions implying there are $(\ell+1)/2$ orbits in total. This implies that $\text{ind}(s) = (\ell-1)/2$. Thus $a(D_\ell, \ell) = 2/(\ell-1)$.

The first main result is an upper bound result for $N_d(k, G; X)$ for a family of groups. The family of groups is defined as follows:

Definition 2.1.4. Let $\mathcal{F}_1$ be the set of groups $\{1\} \neq G \leq S_d$ that act transitively on $[d]$ such that $G = F \rtimes H$ where F is non-trivial and abelian. We define $\mathcal{F}$ to be the following set

$$\mathcal{F} = \{G : G \in \mathcal{F}_1 \text{ and } G \text{ is a Frobenius group}\}.$$

A group G is said to be Frobenius when for all $g \in G \setminus H$, $H \cap H^g = \{1\}$ where $H^g := \{ghg^{-1} : h \in H\}$.

With $G \in \mathcal{F}_1$ we develop the work of Klüners (2006) and Ellenberg and Venkatesh (2006) to obtain an upper bound for $N_{|G|}(k, G; X)$. Moreover, if G is a Frobenius group with an abelian Frobenius kernel F, we make use of a Brauer relation to obtain upper bounds for $N_{|F|}(k, G; X)$. Corresponding to the groups above we fix the following notation.

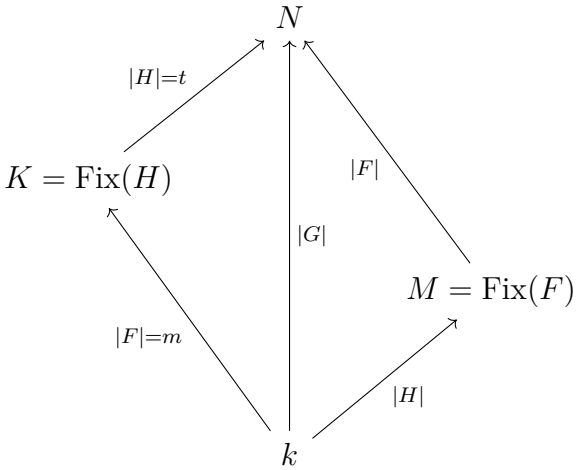
Notation 2.1.5. With $\mathcal{F}$, $\mathcal{F}_1$, F, G, and H as defined earlier, we assume that all groups in $\mathcal{F}_1$ are finite. Let $|F| = m$ and $|H| = t$. Let p and p_1 denote the smallest prime divisors of m and t respectively. Let M/k be a Galois extension with Galois group H. Let $\mathrm{Cl}_M[m]$ be the m-torsion elements of the ideal class group of M. Let $\mathcal{D}$ be defined as

$$\mathcal{D} = \mathcal{D}(k, H, m) := \limsup_{d_{M/\mathbb{Q}}} \frac{\log(|\mathrm{Cl}_M[m]|)}{\log(|d_{M/\mathbb{Q}}|)}. \tag{2.1.2}$$

Let $a_1(G, d)$ denote the smallest known constant such that

$$N_d(k, G; X) \ll X^{a_1(G,d)+\epsilon}.$$

Let $a(G, d)$ denote the conjectured value of $a_1(G, d)$ as defined in Definition 2.1.1. Corresponding to this notation, we have the following field diagram.



(2.1.3)

Theorem 2.1.6. *With notation as above, we have*

$$N_d(k, G; X) \ll X^{A(G,d)+\epsilon}$$

where $A(G, d)$, d, and G are given by:

G	d	$A(G,d)$
$G \in \mathcal{F}$	m	$\max\left(\frac{(\mathcal{D}+a_1(H,t))\times t}{m-1}, \frac{p}{m(p-1)}\right)$
$G \in \mathcal{F}_1$	mt	$\max\left(\frac{a_1(H,t)+\mathcal{D}}{m}, \frac{p}{mt(p-1)}\right)$

Here, $\mathcal{D} = \mathcal{D}(k,H,m)$ is as defined in (2.1.2).

If we are able to attain better upper bounds for $\mathcal{D}$ then $A(G,d)$ may reduce, implying a tighter upper bound. It is believed that $\mathcal{D} = 0$.

Conjecture 2.1.7. (ℓ-torsion conjecture) *Let $K/\mathbb{Q}$ be a number field of degree n. For every $\ell \in \mathbb{N}$, $|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\epsilon} d_{K/\mathbb{Q}}^{\epsilon}$.*

The impetus for this conjecture may be found in Duke (1998), Zhang (2005) and Brumer and Silverman (1996). Using this we have the following results.

Proposition 2.1.8. *We have:*

1. *The number of degree 6 extensions N/k with a cubic subfield M/k and fixed Galois group G satisfies the following*

$$N_6(k,G;X) \ll X^{1+\epsilon}.$$

2. *We have that, for odd m,*

$$\begin{aligned} N_m(k,D_m;X) &\ll X^{\frac{3}{m-1}-\frac{2}{m-1}\min(\frac{1}{2m},\frac{1}{2[k:\mathbb{Q}]})+\epsilon} \\ N_{2m}(k,D_m;X) &\ll X^{\frac{3}{2m}-\frac{1}{m}\min(\frac{1}{2m},\frac{1}{2[k:\mathbb{Q}]})+\epsilon}. \end{aligned} \tag{2.1.4}$$

3. *Let $G = F \rtimes H \in \mathcal{F}_1$. If H is abelian, or $G = F \times H$, under the assumption of the ℓ-torsion conjecture and the assumption of Malle's conjecture for $N_{|H|}(k,H;X)$, we achieve Malle's predicted upper bound for $N_{|G|}(k,G;X)$.*

The first part of the Proposition above stems from studying quadratic extensions of cubic extensions. The second part of the Proposition above stems from incorporating improved bounds on the ℓ-torsion of the class group. Similar upper bounds for

$N_p(k, D_p; X)$ and $N_{2p}(k, D_p; X)$ have been previously established by Klüners (2006) . Using a similar method with improved bounds of the m torsion on the class group by Frei and Widmer (2018b) imply the result of the proposition above. In fact Frei and Widmer have also improved the upper bound of Klüners for the case $k = \mathbb{Q}$. And for the case $k = \mathbb{Q}$ the result of Frei and Widmer is better than the one stated in this proposition. The last part is a direct application of the ℓ-torsion conjecture on the main theorem.

We now showcase some examples of applying the above result.

Example 2.1.9. The results in the table below are the best known upper bounds for $N_d(k, G; X)$ for the specified conditions.

G	Conditions	d	$A(G,d)$	$a(G,d)$
$C_\ell \rtimes C_{\ell-1}$	ℓ is an odd prime	ℓ	$\frac{1}{2} + \frac{2}{\ell-1}$	$2/\ell - 1$
$C_\ell \rtimes C_{\ell-1}$	ℓ is an odd prime	$\ell^2 - \ell$	$\frac{1}{2\ell} + \frac{2}{\ell(\ell-1)}$	$2/(\ell(\ell-1))$
A_4	$k = \mathbb{Q}$	4	0.7783	1/2
$C_2^3 \rtimes (C_7 \rtimes C_3)$		8	27/14	1/4
$C_2^3 \rtimes (C_7 \rtimes C_3)$	ℓ-torsion conjecture	8	1/4	1/4
$C_2^3 \rtimes C_7$	$k = \mathbb{Q}$	8	$0.595\ldots$	1/4
$C_{103} \rtimes C_{17}$	$k = \mathbb{Q}$	103	0.09369	0.0104
S_4	$k = \mathbb{Q}$	6	1/2	1/2

Computations for $a(G, d)$ for the degree 4, degree 6 and degree 8 extensions may be found in Dummit (2017). The first 3 examples are direct consequences of Theorem 2.1.6. The first three groups are instances of Frobenius groups. We use that $\mathcal{D} = 0.278\ldots$ in the $N_4(\mathbb{Q}, A_4; X)$ case and $\mathcal{D} = 1/2$ otherwise. The upper bounds for $N_8(k, C_2^3 \rtimes (C_7 \rtimes C_3))$ are instances of applying the main result twice. These upper bounds are better than the upper bound established in Dummit (2014). To see the first case, we set $\mathcal{D} = 1/2$ and note that the theorem implies $N_{21}(k, C_7 \rtimes C_3; X) \ll$

$X^{1/7+\epsilon}$ first and then using the theorem once more with $a_1(C_7 \rtimes C_3, 21) = 1/7, t = 21, m = 8$ we get the stated result. In the case that we assume the ℓ torsion conjecture, we set $\mathcal{D} = 0$ and go over the same method. The next two examples stem from improved results on $\mathcal{D}$. From Bhargava et al. (2017), we know that the two torsion of a degree 7 extensions of $\mathbb{Q}$ has $\mathcal{D} = 1/2-1/14$. Using this and the fact that $C_2^3 \rtimes C_7$ is a Frobenius group, the statement of the theorem implies $N_8(\mathbb{Q}, C_2^3 \rtimes C_7; X) \ll X^{25/42+\epsilon}$. From the work of Frei and Widmer as states in Section 6.1 we will improved results of the 103-torsion of the class group of a field M such that $[M : \mathbb{Q}] = 17$. The last example indicates that the method can be used to obtain upper bounds for $N_d(k, G; X)$ for $d \neq mt$ in certain cases. In fact, the last example implies that, unconditionally, we have $N_6(k, S_4; X) \ll X^{1/2+\epsilon}$ which is exactly as Malle's conjecture predicts. Details regarding these extensions may be found in Section 6.1.

The second main result we show in this work can be stated as follows.

Theorem 2.1.10. *1. Up to isomorphism, the number of sextic extensions of $\mathbb{Q}$ with Galois group A_4 and absolute value of discriminant bounded above by X is*

$$N_6(\mathbb{Q}, A_4; X) = CX^{1/2} + O(X^{\frac{1+B+\epsilon}{3}}). \tag{2.1.5}$$

Here,

$$C = \lim_{X\to\infty} \sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}|\leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \left(\lim_{s=1}(s-1)\frac{1}{3}M_1(s) \prod_{p\mathcal{O}_M=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1+\frac{3}{p^s}\right)\right) |d_{M/\mathbb{Q}}|^{-1} \tag{2.1.6}$$

where $M_1(s)$ depends on the ramification of 2 in the cyclic cubic field $M/\mathbb{Q}$ and is defined precisely in Theorem 4.0.4 below. The constant B is the smallest positive constant such that for a cubic extension $M/\mathbb{Q}$, the following always holds $|\mathrm{Cl}_M[2]| \ll |d_{M/\mathbb{Q}}|^{B+\epsilon}$. The current state of the art result is due to Bhargava et al. (2017) who are able to show $B \leq 0.278 + \ldots$ implying

$$N_6(\mathbb{Q}, A_4; X) = CX^{1/2} + O(X^{0.426\cdots+\epsilon}).$$

2. *With the constant C as defined above, if we assume the ℓ-torsion conjecture, we have*

$$N_6(\mathbb{Q}, A_4; X) - CX^{1/2} \ll X^{5/14+\epsilon}.$$

3. *Under the assumption of the Lindelöf Hypothesis, we have*

$$N_6(\mathbb{Q}, A_4; X) - CX^{1/2} \ll X^{0.389\ldots}.$$

4. *Under the assumption of both the Lindelöf Hypothesis and the ℓ-torsion conjecture, we have*

$$N_6(\mathbb{Q}, A_4; X) - CX^{1/2} \ll X^{1/4+\epsilon}.$$

2.2 Survey of known results

We go over some of the major results in the area of counting number fields. There are three main techniques to count number fields. The first technique is to use some information about group actions on an underlying vector space. These methods are not easy to generalize and have only been shown to exist for number fields with degree at most 5.

The second method is to bound the number of possible minimal polynomials that have roots in a certain lattice. This method is quite general and is only applicable for attaining upper bounds.

The last method revolves around decomposing an extension into two extensions and using information about the smaller extension to say something about the larger extension. We will discuss all three methods in this section.

First we survey the beginnings of explorations in this area, and in particular the contributions of Gauss. Gauss studied $\mathrm{SL}_2(\mathbb{Z})$ actions on quadratic forms and introduced the notion of equivalent quadratic forms. Gauss defined two forms $g(x, y)$

and $g(x,y)$ as equivalent if there exists a matrix $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$f(x,y) \circ \begin{pmatrix} A & B \\ C & D \end{pmatrix} = f(Ax+By, Cx+Dy) = g(x,y).$$

The discriminant of this form is $d(f) = b^2 - 4ac$. The group action of $\mathrm{SL}_2(\mathbb{Z})$ preserves the discriminant of the form. In fact, Gauss essentially proved that the set of $\mathrm{SL}_2(\mathbb{Z})$-orbits on integral binary quadratic forms having a fixed discriminant D form a finite abelian group under the operation of composition that he defined. We call this group $\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}$. The size of this group is the class number for discriminant D. Gauss went on to make related conjectures such as:

1. We have
$$\sum_{-X<D<0} |\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}| \sim \frac{\pi}{18} X^{3/2}. \tag{2.2.1}$$
2. The number of negative discriminants D such that $|\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}|$ is equal to any fixed integer is finite.
3. There are infinitely many positive integers D such that $|\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}| = 1$.

The first part of the conjecture is a result of Mertens (1941). Landau (1918) proved, under the generalized Riemann hypothesis, that if D is a negative quadratic discriminant then as $D \to -\infty$, $|\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}| \to \infty$. Hecke proved that if the generalized Riemann hypothesis does not hold, then if D is a negative quadratic discriminant as $D \to -\infty$, $|\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}| \to \infty$. Hecke's result was published in H. Heilbronn (1934) where Landau cites that the proof is from a lecture of Hecke. Their results together imply the second conjecture. The third conjecture is still not known.

Gauss formulated these conjectures before class groups were studied and defined as they are today. Before discussing further progress it is important to note what the current notion of the class group is. The modern definition is as follows:

Definition 2.2.1. The class group Cl_F of a number field $F/\mathbb{Q}$ is the quotient group J_F/P_F where J_F is the group of fractional ideals of F and P_F is the group of principal ideals of F.

These conjectures for class groups of quadratic forms often lend themselves to analogous conjectures about discriminants on various other forms. However the fact that $\mathrm{SL}_2(\mathbb{Z})$ has a group action on binary quadratic forms is not easily generalized. One extension is by Levi (1914). This extension shows a a bijection between discriminant preserving $\mathrm{GL}_2(\mathbb{Z})$ action on ternary quadratic forms and isomorphism classes of cubic rings. This is known as the Delone-Fadeev correspondence as it was also presented in the work of Delone and Faddeev (1940). To describe it, we first establish some notation. Let $V(\mathbb{Z})$ be the set of integral binary cubic forms

$$V(\mathbb{Z}) := \{f(x,y) = ax^3 + bx^3y + cxy^2 + dy^3 : a,b,c,d \in \mathbb{Z}\}$$

with the discriminant of such a form given by

$$d(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

The action can be described as follows, a matrix $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ acts on a form $f(x,y)$ by

$$\gamma \circ f(x,y) = \frac{1}{det(\gamma)} f((x,y)\gamma).$$

Two forms $f(x,y)$ and $g(x,y)$ are equivalent if there exists $\gamma \in \mathrm{GL}(\mathbb{Z})$ such that $f = \gamma \circ g$. A cubic form $f(x,y)$ is said to be irreducible if it is irreducible as a polynomial over $\mathbb{Q}$. An order is a ring of finite rank over $\mathbb{Z}$ that is also an integral domain.

Theorem 2.2.2. *There is a natural, discriminant-preserving bijection between the set of* $\mathrm{GL}_2(\mathbb{Z})$*-orbits on* $V(\mathbb{Z})$ *and the set of isomorphism classes of cubic rings. Under this correspondence, irreducible cubic forms correspond to orders in cubic fields, and*

if a cubic form f corresponds to a cubic ring R, then $\mathrm{Stab}_{GL_2(\mathbb{Z})}(f)$ *is isomorphic to* $\mathrm{Aut}(R)$.

Once this was established, Davenport and Heilbronn discovered the following maximality condition.

Theorem 2.2.3. *Under the correspondence in Theorem 2.2.2, a cubic ring R is maximal if any only if its corresponding cubic form f belongs to the set $U_p \subset V(\mathbb{Z})$ for all p, defined by the following equivalent conditions:*

- *The ring R is not contained in any other cubic ring with index divisible by p.*
- *The cubic form f is not a multiple of p, and there is no $GL_2(\mathbb{Z})$-transformation of $f(x,y) = ax^3 + bx^3y + cxy^2 + dy^3$ such that a is a multiple of p^2 and b is a multiple of p.*

Using this, Davenport and Heilbronn were able to show:

Theorem 2.2.4. *Denote by $N_3(\mathbb{Q}, (A,B])$ the number of cubic extensions $F/\mathbb{Q}$ such that the discriminant $d_{F/\mathbb{Q}}$ of the extension lies in the interval $(A,B]$. Then we have the following*

$$\begin{aligned} N_3(\mathbb{Q}; (0,X]) \sim& \frac{1}{12\zeta(3)}X, \\ N_3(\mathbb{Q}; [-X,0)) \sim& \frac{1}{4\zeta(3)}X, \\ \sum_{0<D<X} |\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}[3]| =& \frac{4}{3}\sum_{0<D<X} 1 + o(X), \\ \sum_{-X<D<0} |\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}[3]| =& 2\sum_{-X<D<0} 1 + o(X). \end{aligned}$$

where D varies over discriminants of quadratic extensions.

These error terms have since been improved multiple times, by Belabas, Bhargava, and Pomerance (2010), Bhargava, Shankar, and Tsimerman (2013), and Taniguchi and Thorne (2013) and the present record error term is in an unpublished result by

Bhargava, Taniguchi and Thorne. Davenport and Heilbronn's idea for the proof was to count lattice points in a fundamental domain for the action of $\mathrm{GL}_2(\mathbb{Z})$, bounded by the constraint $|d(f)| < X$.

Bhargava used a certain parametrization of quartic and quintic rings to obtain more such results by discovering other group actions on other lattices.

Theorem 2.2.5 (Bhargava)**.**

- *The average size of the 2-torsion subgroup in the class group of cubic fields having positive discriminants is* $5/4$.
- *The average size of the 2-torsion subgroup in the class group of cubic fields having negative discriminants is* $3/2$.
- *82% of the number of quartic fields with discriminant at most X have Galois group S_4 and 100% of quintic number fields with discriminant at most X have Galois group S_5. Moreover, we have*

$$N_4(\mathbb{Q}, S_4, X) \sim \frac{5}{24} \prod_p \left(1 + p^{-2} - p^{-3} - p^{-4}\right) X + o(X)$$
$$N_5(\mathbb{Q}, X) \sim \frac{13}{120} \prod_p \left(1 + p^{-2} - p^{-4} - p^{-5}\right) X + o(X)$$

The proofs involve understanding properties of higher composition laws. These methods do not easily extend to instances of higher degrees. The other extensions that contribute non zero density to quartic extensions have Galois group D_4. Cohen, Diaz y Diaz, and Olivier (2002a) attained an asymptotic expression

$$N_4(\mathbb{Q}, D_4; X) \sim cX$$

where $c = .052326\ldots$. These results imply that Linnik's conjecture (Conjecture 2.0.1) holds for $d \leq 5$ with $k = \mathbb{Q}$. The order of magnitude for $N_2(k; X)$ and $N_3(k; X)$ for general k were obtained by Datskovsky and Wright (1988). They showed

$$N_2(k; X) = C'_k X + o(X) \qquad N_3(k; X) = C_k X + o(X).$$

For arbitrary k, Bhargava, Shankar, and Wang (2015) compute explicit constants c_d for $N_d(k, S_d; X) = c_d X + o(X)$ for $d = 4$ and 5.

The first general upper bound result towards the counting number fields problem for all degrees was established by Schmidt (1995). He was able to show:

Theorem 2.2.6. *For all $n \geq 2$ and all base fields k,*

$$N_n(k, X) \ll X^{(n+2)/4}.$$

The approach of Schmidt can be summarized as follows. Let K/k be a degree n extension. First construct a lattice attached to the ring of integers $\mathcal{O}_K$ and use Minkowski's lattice theorem to find an element α with small Euclidean norm compared to the degree of the number field. Using this, we can bound the size of the coefficients of terms in the minimal polynomial on α and therefore bound the number of possible minimal polynomials. This technique was then modified by Ellenberg and Venkatesh allowing them to show their result which improves on the result of Schmidt. Ellenberg and Venkatesh (2006) establish upper bounds for all $d > 3$, precisely, they show for a positive constant C,

$$N_d(k; X) \ll X^{\exp(C\sqrt{\log d})}.$$

This technique was further streamlined by Couveignes (2019). He was able to show that there exists a positive constant C_1 such that for all $n > C_1$,

$$N_n(\mathbb{Q}, X) \leq n^{C_1 n \log^3(n)} X^{C_1 \log^3(n)}.$$

In the same work mentioned above, Ellenberg and Venkatesh establish that for any Galois extension with Galois group G with $|G| \geq 4$ and base field k,

$$N_{|G|}(k, G; X) \ll_{k,G,\epsilon} X^{3/8+\epsilon}.$$

The proof of this result is quite similar to the proof presented here to bound $N_{|G|}(k, G; X)$ for $G \in \mathcal{F}_1$. Their strategy is to use induction on the size of $|G|$, and we briefly sketch

their approach here. Let F be a minimal normal subgroup of G such that

$$0 \to F \to G \to H \to 0.$$

This implies that F is a direct sum of copies of a simple group (Robinson (2012) in (3.3.15)). Let $M = \mathrm{Fix}(F)$ be the fixed field of F, and now we break the argument into two cases, the first is when F is abelian, the second when F is not abelian. When F is abelian, $F = (\mathbb{Z}/p\mathbb{Z})^r$. Then they use the following equation

$$N_{|G|}(k, G; X) = \sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k}) \leq X^{1/p^r} \\ \mathrm{Gal}(M/k)=H}} \sum_{\substack{N/M \\ [N:M]=p^r,\ \mathrm{Gal}(N/k)=G \\ \mathcal{N}_{M/\mathbb{Q}}(d_{N/M}) \leq X \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{-p^r}}} 1.$$

They bound the number of F extensions of M such that $\mathcal{N}_{M/\mathbb{Q}}(d_{N/M}) = Y$ by $Y^{\epsilon} d_{M/\mathbb{Q}}^{r/2}$. They do so by noting that the number of F extensions of M ramified such that $\mathcal{N}_{M/\mathbb{Q}}(d_{N/M}) = Y$ is bounded above by $|\mathrm{Hom}(G_Y(M), F)|$ where $G_Y(M)$ is the Galois group of the maximal extension of M unramified away from primes dividing Y. They bound $|\mathrm{Hom}(G_Y(M), F)|$ by bounding the size of the kernel and image of a homomorphism to $\bigoplus_{\substack{\mathfrak{p}|(Y) \\ \mathfrak{p} \subseteq \mathcal{O}_M}} \mathrm{Hom}(I_{\mathfrak{p}}, F)$ where $\mathfrak{p}$ is a prime in $\mathcal{O}_M$ and $I_{\mathfrak{p}}$ is the inertia group. They use the Brauer-Siegel theorem to bound to rth power of the class group. They then use ramification information from the fact that the extension is Galois. Using this idea and then inducting on $N_{|H|}(k, H; X)$ gives the statement of the theorem in the case that F is abelian. In the case that F is not abelian, they use the bound of Schmidt to count the number of F extensions of M and proceed in a similar manner.

Before Bhargava established the size of $N_4(k, S_4; X)$, Baily (1980) published a work that established upper and lower bounds for $N_4(k, G; X)$ for all possible groups G. He established

$$X \ll N_4(\mathbb{Q}, S_4; X) \ll X^{3/2+\epsilon}$$

$$X^{1/2} \ll N_4(\mathbb{Q}, A_4; X) \ll X^{1+\epsilon}$$

His main obstruction for establishing better upper bounds was the two rank of the class group of a cubic field, something that Bhargava addressed in his work. One of

the key tools Baily used in studying $N_4(\mathbb{Q}, S_4; X)$ and $N_4(\mathbb{Q}, A_4; X)$ was the work of Hilbert (1898) that connected the discriminant of the quartic extensions $K/\mathbb{Q}$ to the discriminant of the cubic extension $M/\mathbb{Q}$ and the quadratic extension N_1/M of the cubic extension. Precisely, he used

$$d_{N_1/\mathbb{Q}} = d_{M/\mathbb{Q}} d_{K/\mathbb{Q}}.$$

He also established non trivial ramification information. Precisely, he established that if a prime p is unramified in $M/\mathbb{Q}$ and p ramifies in the sextic extension, then $p^2 | \mathcal{N}_{M/\mathbb{Q}}(d_{N_1/M})$. He also established that $d_{K/\mathbb{Q}} \leq 2^9 d_{M/\mathbb{Q}}$. Cohen and Thorne (2016b) make the relation between the quartic and the sextic extensions of A_4 and S_4 precise. We will talk about their result in more depth in Chapter 4. We will use these tools to establish the asymptotic for $N_6(\mathbb{Q}, A_4; X)$.

Klüners was the first to explicitly study a Frobenius group, $G = D_\ell$ where ℓ is an odd prime. We generalize his technique to all groups in $\mathcal{F}$. Klüners showed the following

$$N_\ell(k, D_\ell; X) \ll X^{\frac{3}{\ell-1}+\epsilon} \qquad N_{2\ell}(k, D_\ell; X) \ll X^{\frac{3}{2\ell}+\epsilon}. \tag{2.2.2}$$

Under the assumption of an implication of a conjecture of Cohen and Lenstra, he was able to show Malle's predicted bounds. Precisely, he assumed that

$$\sum_{|D| \leq X} |\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}[\ell]| = O(X)$$

where D varies over fundamental discriminants. His method implied that the only obstruction that there is to showing Malle's weak conjecture (see Example 2.1.3 for what is expected) is that we do not have the necessary information about the ℓ-torsion of the class group of quadratic number fields. His method can be summarized as follows: First use a non trivial discriminant relation. In particular with G, F and H as in Diagram 2.1.3 where $D_\ell = C_\ell \rtimes C_2 = F \rtimes H$, we have

$$d_{K/k} = d_{M/k}^{\frac{\ell-1}{2}} \mathcal{N}_{M/k}(d_{N/M})^{1/2}.$$

Under this notation,

$$N_\ell(k, D_\ell; X) = \sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k}) \leq X^{2/(\ell-1)} \\ \mathrm{Gal}(M/k)=C_2}} \sum_{\substack{N/M, [N:M]=\ell \\ \mathrm{Gal}(N/k)=D_\ell,\ \mathrm{Gal}(N/M)=C_\ell \\ \mathcal{N}_{M/\mathbb{Q}}(d_{N/M}) \leq X^2 \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{-(\ell-1)}}} 1.$$

Using class field theory and some ramification information he computes the inner sum in terms of the ℓ-torsion of the class group of M. He counts the number of M/k using the work of Wright (1989). After this work was established, the upper bounds for $N_\ell(k, D_\ell; X)$ when $k = \mathbb{Q}$ have been improved multiple times. First Cohen and Thorne (2016c) improved $N_\ell(\mathbb{Q}, D_\ell; X)$ and their methods also imply an improvement in $N_{2\ell}(\mathbb{Q}, D_\ell; X)$. This result was further improved upon by Frei and Widmer (2018b). Both these works use improved results on the average size of the ℓ-torsion of the class group. Frei and Widmer establish upper bounds for the average size of the ℓ-torsion in class groups for any ℓ for extensions with small degree over $\mathbb{Q}$. Using their results on the size of the ℓ-torsion of quadratic extensions, the method in this paper establishes the same result. They show that

$$N_\ell(\mathbb{Q}, D_\ell; X) \ll X^{\frac{3}{\ell-1} - \frac{2}{(\ell+2)(\ell-1)} + \epsilon} \qquad N_{2\ell}(\mathbb{Q}, D_\ell; X) \ll X^{\frac{3}{2\ell} - \frac{1}{\ell(\ell+2)} + \epsilon}. \tag{2.2.3}$$

The work of Frei and Widmer (Theorem 6.2.1) also implies an improvement in the upper bounds for $N_m(k, D_m; X)$ and $N_{2m}(k, D_m; X)$ for odd m, which we make precise here. As one might suspect, the obstacle from reaching Malle's conjectured upper bounds is that we do not have the necessary information about the torsion of the class groups of quadratic extensions. At the same time as Frei and Widmer (2018b) was being worked on Pierce, Turnage-Butterbaugh, and Wood (2017) establish non-trivial upper bounds for the size of the ℓ-torsion of the class group for almost all Galois extensions $M/\mathbb{Q}$ with a wide range of possible Galois groups. Their results stem from finding improved zero free regions in most Dedekind zeta functions of specified type.

For the Frobenius group $C_5 \rtimes C_4$, Bhargava, Cojocaru and Thorne show

$$N_5(\mathbb{Q}, C_5 \rtimes C_4; X) \ll X^{39/40+\epsilon} \tag{2.2.4}$$

which is a tighter upper bound then the one we establish here. The expected bound upper bound is $N_5(k, C_5 \rtimes C_4; X) \ll X^{1/2+epsilon}$ and the restriction we have from reaching there is lack of information about the 5 torsion of degree 4 extensions.

At the same time as this work was being done, Alberts (2018) independently established upper bounds for $N_d(k, G; X)$ in the case that G is a solvable group. The set of solvable groups is a subset of the groups in $\mathcal{F}_1$. Upper bounds for $N_{|G|}(k, G; X)$ for solvable groups that we are able to show in this paper are as tight. For Frobenius groups $G \in \mathcal{F}$, upper bounds for $N_{|F|}(k, G; X)$ when F is not cyclic are tighter in this work than they are in Alberts (2018). When F is cyclic and $G \in \mathcal{F}$, the bounds in both works are the same. Alberts' method may be used to count number fields ordered by an invariant other than the discriminant, such as the conductor. Alberts is also able to obtain upper bounds for $N_d(k, G; X)$ for all $d \neq |G|$. His work also establishes Malle's conjecture for solvable groups G under the assumption of the ℓ-torsion conjecture. The method used here is different from the method in the paper of Alberts as it focuses on using a Brauer relation to count Frobenius extensions, whereas the work of Alberts involves studying the structure of central series of groups.

At this time, Alberts is working on another work (Alberts (2019)) that computes lower bounds for $N_d(k, G; X)$ for $G \in \mathcal{F}_1$. His work largely focuses on trying to reformulate a stronger form of Malle's conjecture.

Chapter 3

Background

This chapter covers background material; it is divided into two sections. The first section covers some basic algebraic number theory, in particular, material about ramification of primes. The second section covers areas in complex analysis and analytic number theory.

3.1 Ramification of primes

In this section we review the study of how primes ramify in field extensions. Denote the ring of integers in the number field K is indicated as $\mathcal{O}_K$ and the Galois group of the closure of $K/\mathbb{Q}$ by G. Let $\sigma : K \to \widehat{\mathbb{Q}}$ vary over the different $\mathbb{Q}$ embeddings of K into $\widehat{\mathbb{Q}}$. Then the norm of an element $\alpha \in \mathcal{O}_K$, is

$$\mathcal{N}_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma} \sigma(\alpha).$$

Similarly, the trace of an element $\alpha \in K$ is defined as

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{\sigma} \sigma(\alpha).$$

Since the norm is a completely multiplicative function, we have that if a prime factorization of the ideal α is

$$(\alpha) = \prod_{i=1}^{j} \mathfrak{p}_i^{a_i}$$

then

$$\mathcal{N}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{j} \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}_i)^{e_i}$$

where each $\mathfrak{p}_i$ is a prime ideal in $\mathcal{O}_K$. The norm of any prime ideal $\mathfrak{p}$ is always the power of a prime $p \in \mathbb{Z}$. We can be more precise if we know the image of p in $\mathcal{O}_K$. In particular, if

$$\prod_{i=1}^{g} \mathfrak{p}_i^{e_i} = p\mathcal{O}_K$$

then $\mathcal{N}(\mathfrak{p}_i) = p^{f_i}$, where f_i is known as the inertia degree. The e_i here are known as the ramification degrees. To capture this information succinctly we say that the ramification type of p in K is $(f_1^{e_1} f_2^{e_2} \dots f_g^{e_g})$. A prime is said to be unramified in the extension $K/\mathbb{Q}$ if and only if all of the $e_i = 1$. A prime p is said to be tamely ramified in $K/\mathbb{Q}$ if and only if $\gcd(e_i, p) = 1$ for all i. If a prime is not tamely ramified, it is said to be wildly ramified. Depending on whether or not the extension is a Galois extension, we can gather further information about what the ramification and the inertia degrees can be. For any extension $K/\mathbb{Q}$, we know that

$$\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}].$$

If the extension is a Galois extension with Galois group G then we have that all the ramification degrees are the same, e and all the inertia degrees are the same, f and hence,

$$efg = |G|.$$

In a tower of extensions, the ramification and inertia degrees are multiplicative. More precisely, let $L/K/\mathbb{Q}$ be a tower of extensions then have

$$p\mathcal{O}_K = \prod_{i=1}^{g(K)} \mathfrak{p}_i^{e_i} \qquad \mathfrak{p}_i\mathcal{O}_L = \prod_{j=1}^{g(L/K)} \mathfrak{P}_{j,i}^{e_{j,i}}$$

with inertia degrees f_i and $f_{j,i}$ respectively. If $L/\mathbb{Q}$ is a Galois extension, then all the $f_{j,i}$ and $e_{j,i}$ are equal to each other. In this case the inertia degree of p in $\mathcal{O}_L$ would be $f_i \times f_{j,i}$ for any pair i, j. Using this information we know that a prime will be wildly ramified in an extension if and only if the prime divides the size of the Galois group and the discriminant of the extension. Hence the number of wildly ramified

primes for any extension with Galois group G is $\omega(|G|)$ where $\omega(n)$ is the number of prime divisors of n.

Let K be a number field over k. Let $\{\sigma_i\}_{i=1}^n$ be the set of embeddings of K into $\mathbb{C}$ which are the identity on k. If $\{b_j\}_{j=1}^n$ is any basis of K over k, let $M = (\sigma_j(b_i))_{i,j=1}^n$ be a square matrix, let $d(b_1, \ldots, d_n) = det(M)^2$. Then $d_{K/k}$ is defined as the ideal generated by $d(b_1, \ldots, b_n)$ as $\{b_j\}$ varies over all bases of K over k such such that the elements of the basis are contained in $\mathcal{O}_K$. In particular, $d_{K/k} \in \mathcal{O}_k$. We define *Dedekind's complementary module* of the inverse different ideal as

$$\mathfrak{d}^{-1} = \{x \in K : \mathrm{Tr}(x\mathcal{O}_K) \subseteq \mathcal{O}_k\}.$$

The inverse of this fractional ideal is known as the different ideal $\mathfrak{d}_{K/k}$. The different ideal lies in $\mathcal{O}_K$ and $\mathcal{N}_{K/k}(\mathfrak{d}_{K/k}) = d_{K/k}$. From Neukirch (2013) Chapter 3, section 2, we have that in a tower of extensions, $K/k/\mathbb{Q}$,

$$\mathfrak{d}_{K/\mathbb{Q}} = \mathfrak{d}_{K/k}\mathfrak{d}_{k/\mathbb{Q}}.$$

This in particular implies the discriminant relation $d_{K/\mathbb{Q}} = d_{k/\mathbb{Q}}^{[K:k]}\mathcal{N}_{k/\mathbb{Q}}(d_{K/k})$. Using this and Theorem 2.6 of Neukirch (2013) chapter 3, we have that

Theorem 3.1.1. *A prime ideal $\mathfrak{p}$ of K is ramified over k if and only if $\mathfrak{p}|\mathfrak{d}_{K/k}$. Let $\nu_\mathfrak{p}(\mathfrak{d}_{K/k})$ be the exact power of $\mathfrak{p}$ that divides the different ideal. Let e be the ramification index of $\mathfrak{p}$ over p. Then $\nu_\mathfrak{p}(\mathfrak{d}_{K/k}) = e - 1$ when $\mathfrak{p}$ is tamely ramified, and $e \leq \nu_\mathfrak{p}(\mathfrak{d}_{K/k}) \leq \nu_\mathfrak{p}(e) + e - 1$ when $\mathfrak{p}$ is wildly ramified.*

We see what this implies when the base field is $\mathbb{Q}$. For an arbitrary extension $k/\mathbb{Q}$, and prime $p \in \mathbb{Z}$ we have if p has splitting type $(f_1^{e_1}, \ldots f_g^{e_g})$ that

$$\begin{cases} \nu_p(\mathcal{N}(d_{k/\mathbb{Q}})) = 0 & p \text{ is unramified in } \mathcal{O}_k \\ \nu_p(\mathcal{N}(d_{k/\mathbb{Q}})) = \sum_{i=1}^g f_i(e_i - 1) & p \text{ is tamely ramified in } \mathcal{O}_k. \end{cases} \tag{3.1.1}$$

Finally, if p is wildly ramified in the extension as

$$p\mathcal{O}_k = \prod_{i=1}^{g(k)} \mathfrak{p}_i^{e_i}$$

then

$$\sum_{\substack{i \\ p|e_i}} e_i f_i \leq \nu_p(\mathcal{N}(d_{k/\mathbb{Q}})) - \sum_{\substack{i \\ p\nmid e_i}} f_i(e_i - 1) \leq \sum_{\substack{i \\ p|e_i}} (e_i - 1 + \nu_{\mathfrak{p}_i}(e_i\mathcal{O}_k))f_i.$$

Here $\nu_{\mathfrak{p}_i}(e_i\mathcal{O}_k) = \beta$ where $\mathfrak{p}_p^{\beta}\alpha = (e_i)$ where (e_i) is the ideal generated by e_i in $\mathcal{O}_k$.

3.2 Complex analysis and analytic number theory

In this section we review some facts from complex analysis and analytic number theory. We review the Phragmén Lindelöf principle, basic facts about Dedekind zeta functions, Perron's formula and Abel summation or partial summation. The Phragmén Lindelöf principle is an extension of the maximum modulus theorem. We recall what the maximum modulus principle is.

Theorem 3.2.1 (Maximum modulus principle)**.** *Let D be a connected closed and bounded set of the complex plane and let $f(s)$ be bounded and holomorphic for all $s \in D$. If $h \in D$ is such that $|f(h)| \geq |f(s)|$ for any s in D, then h is located on the boundary of D.*

The Phragmén Lindelöf principle is a technique that enables us to extend the spirit of the maximum modulus principle to unbounded sets in the complex plane. We are interested in this to be able to find an upper bound to the zeta function in the critical strip. Detailed applications and extensions of this can be found in the work of Rademacher (1958).

Theorem 3.2.2. *(Phragmén Lindelöf Principle)*

Let $f(s)$ be holomorphic on an open neighborhood of the strip $a \leq \sigma \leq b$, for some real numbers $a < b$, such that $|f(s)| \ll \exp(|s|^A)$ for some $A > 0$. Assume that

$$|f(a + it)| \leq M_a(1 + |t|)^{\alpha} \qquad |f(b + it)| \leq M_b(1 + |t|)^{\beta}$$

for all $t \in \mathbb{R}$ and some fixed α, $\beta \in \mathbb{R}$. Then we have

$$|f(\sigma + it)| \ll M_a^{\ell(\sigma)} M_b^{1-\ell(\sigma)} (1 + |t|)^{\alpha\ell(\sigma)+\beta(1-\ell(\sigma))}$$

for all s in the strip where ℓ is the linear function such that $\ell(a) = 1$ and $\ell(b) = 0$.

Proof. The proof may be split into showing the result in the upper half plane, showing the result in the lower half plane and in the middle. Precisely, fix a constant $t_0 > 2$. Then we have that $f(s)$ is bounded in the bounded region of the strip with $|t| < t_0$. Using this, we prove the result in the upper half place. Showing the result in the lower half plane is done in the same manner.

Assume that $a \leq \sigma \leq b$ and $t > t_0$. Let $F(s) = F(\sigma + it) = (1/7)f(s)(M_a(1 + s)^{\alpha})^{\frac{\sigma-b}{b-a}}(M_b(1 + s)^{\beta})^{\frac{\sigma-a}{a-b}}$. Without loss of generality, we may assume that $a = 0$ and $b = 1$, we can do this by showing the result for $g(s)$ where $g(s) = F((s - a)/(b - a))$. This implies that $|F(it)| \leq 1$ and $|F(1 + it)| \leq 1$ hold. Now for s with real part between 0 and 1, let $F_n(s) = F(s)e^{s^{4\lceil A\rceil-2}/n}$, then $F_n(s)$ tends to 0, as $|s| \to \infty$, for any $n \in \mathbb{N}$ and satisfies $F_n(s) \ll 1$ on the boundary of the strip. To elaborate on the above let $m = 4\lceil A\rceil - 2$, hence $m > A$ is a non zero even integer that is 2 modulo 4. As $|t| \to \infty$ we have

$$(\sigma + it)^m = (it)^m + \sum_{k=0}^{m-1} \binom{m}{k} (it)^k \sigma^{m-k} = -t^m + O(t^{m-1}).$$

Hence as $|t|$ gets bigger, $-t^m \to -\infty$. Consequently, for large $|t|$, $|f(s)| \ll e^{|t|^A}$ implying that $|F(s)| \ll e^{|t|^A}$ hence

$$|F_n(s)| \ll e^{|t|^A - t^m/n + O(t^{m-1})}.$$

By applying the maximum modulus principle to $F_n(s)$ we see that $|F_n(s)| \ll 1$ everywhere in the upper half of the strip. By noting that $\lim_{n\to\infty} F_n(s) = F(s)$, we may say the same about $F(s)$. This implies the stated result in the upper half plane.

□

The above is a critical tool that allows us to integrate zeta functions in the critical strip. We briefly recall some properties about Dedekind zeta functions. All the proofs for these facts may be found in Neukirch (2013), Chapter 7. Given a number field $k/\mathbb{Q}$, we define $\zeta_{k/\mathbb{Q}}(s) = \zeta_k(s)$, the Dedekind zeta function of $k/\mathbb{Q}$ as

$$\zeta_{k/\mathbb{Q}}(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_k} \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{a})^{-s}$$

for s with real part strictly bigger than 1. Using information from the previous section, we can rewrite this as an Euler product,

$$\zeta_{k/\mathbb{Q}}(s) = \prod_p \prod_{i=1}^{g(p)} \left(1 - p^{-f_i(p)s}\right)^{-1} \tag{3.2.1}$$

where $p\mathcal{O}_k = \mathfrak{p}_i^{e_1(p)} \dots \mathfrak{p}_{g(p)}^{e_{g(p)}(p)}$. For instance, if the extension was Galois with Galois group C_q where q is a prime number, then we have

$$\zeta_k(s) = \prod_{p\mathcal{O}_k = (1^q)} (1 - p^{-s})^{-1} \prod_{p\mathcal{O}_k = (q)} (1 - p^{-qs})^{-1} \prod_{p\mathcal{O}_k = (1 \dots 1)} (1 - p^{-s})^{-q}.$$

Dedekind zeta functions have a simple pole at $s = 1$. If $k/\mathbb{Q}$ is a degree d extension with r_1 real embeddings and r_2 complex embeddings, then $\zeta_k(s)$ satisfies the following functional equation

$$\zeta_k(s) = \epsilon(k) |d_{k/\mathbb{Q}}|^{1/2-s} \pi^{d(s-1/2)} \left(\frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)} \right)^{r_1+r_2} \left(\frac{\Gamma\left(1 - \frac{s}{2}\right)}{\Gamma\left(\frac{1+s}{2}\right)} \right)^{r_2} \zeta_k(1-s) \tag{3.2.2}$$

where $\epsilon(k)$ is a constant that depends on k and $|\epsilon(k)| = 1$. For large values of t, the Phragmén Lindelöf Principle implies $|\zeta_k(1 + it)| \ll t^{\epsilon}$. In fact Granville and Soundararajan (2005) show that $|\zeta(1+it)| \ll (\log(t))^{2/3}$ for an explicit constant, and under the Riemann Hypothesis, $|\zeta(1+it)| \leq e^{\gamma}(\log\log(t) + \log\log\log(t) + O(1))$. Using the functional equation, we see that $|\zeta_k(0 + it)| \ll (|d_{k/\mathbb{Q}}|t^d)^{1/2+\epsilon}$. The Phragmén Lindelöf Principle can be used to show that for large values of t and $\sigma \in (0, 1)$

$$|\zeta_k(\sigma + it)| \ll (|d_{k/\mathbb{Q}} t^d|)^{(1-\sigma)/2+\epsilon}. \tag{3.2.3}$$

This is known as the convexity bound. Anything better than this is known as a subconvexity bound. It is useful because it gives an upper bound for the zeta function not only in terms of the imaginary part of s, but also in terms of the discriminant of the number field. Heath-Brown (1978) (Theorem 1 and Theorem 2) established sub-convexity estimates for Dirichlet L functions in the critical strip. This implies improvements in upper bounds for convexity estimates for the Dedekind zeta functions $\zeta_M(s)$ such that $M/\mathbb{Q}$ is an abelian cyclic extension. Precisely, when $[M:\mathbb{Q}] = d$, he established

$$|\zeta_M(1/2+it)| \ll |d_{M/\mathbb{Q}}|^{3/16+\epsilon}|t|^{d/4} \qquad |\zeta_M(1/2+it)| \ll |d_{M/\mathbb{Q}}|^{1/5+\epsilon}|t|^{d/5}. \tag{3.2.4}$$

In general, we expect zeta functions to be quite small in the critical strip with real part greater than 1/2. One of the biggest unsolved problems in analytic number theory is the Lindelöf Hypothesis.

Conjecture 3.2.3 (Lindelöf Hypothesis)**.** *For any positive value of* ϵ

$$\left|\zeta_k\left(\frac{1}{2}+it\right)\right| = o\left(\left(|d_{k/\mathbb{Q}}|\left(|t|+1\right)\right)^{\epsilon}\right)$$

.

Another important piece of information about zeta functions is their residue at $s=1$. Let R denote a quantity known as the regulator of $\zeta_k(s)$. Let the number of roots of unity in k be w, then

$$\mathrm{res}_{s=1}(\zeta_k(s)) = \frac{2^{r_1+r_2}\pi^{r_2}|\mathrm{Cl}_k|R}{w\sqrt{|d_{k/\mathbb{Q}}|}}. \tag{3.2.5}$$

This is known as the class number formula Neukirch (2013) (Chapter 7 Section 5 after Corollary 5.11). The residue of the zeta function will come into play when we are integrating the zeta function whilst using Perron's formula. We now state what exactly this is. Let

$$g(s) = \sum_{n\geq 1}\frac{a(n)}{n^s}$$

such that $g(s)$ is uniformly convergent for in the domain with real part of s greater than σ. Then for $c > \sigma$, we have

$$\sum_{n \leq X} a(n) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} g(s) \frac{X^s}{s} ds.$$

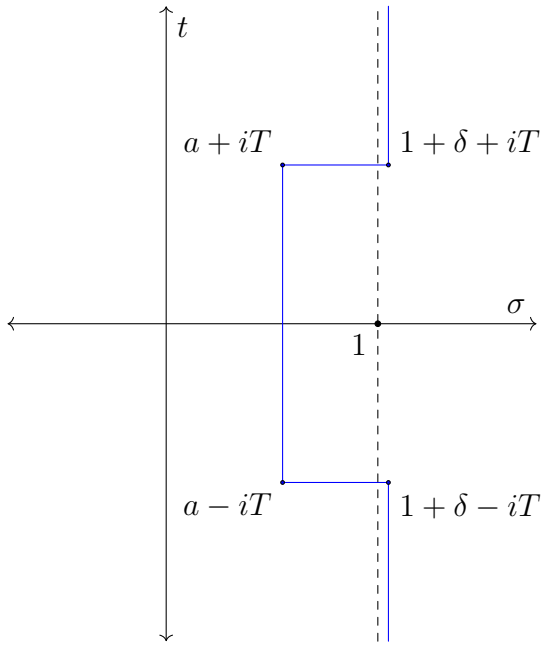
Integrating on this contour will play an important role for us later on, and we briefly describe how to break the contour up first. If $g(s) = \zeta_k(s)$, we have $c > 1$, we set $\delta > 0$ and let $c = 1 + \delta$. We let a, T be positive real numbers such that $0 < a < 1$ and $1000 < T$. Let C denote the rectangular anti-clockwise contour that connects the points $c - iT, c + iT, a + iT, a - iT$, then by the residue theorem

$$\int_{c-iT}^{c+iT} \zeta_k(s) \frac{X^s}{s} ds = 2\pi i \text{res}_{s=1} \left(\zeta_k(s) \frac{X^s}{s} \right) - \int_C \zeta_k(s) \frac{X^s}{s} ds + \int_{c-iT}^{c+iT} \zeta_k(s) \frac{X^s}{s}.$$

This implies that

$$\begin{aligned} \int_{c-i\infty}^{c+i\infty} \zeta_k(s) \frac{X^s}{s} ds = 2\pi i \text{res}_{s=1} \left(\zeta_k(s) \frac{X^s}{s} \right) + \int_{c-i\infty}^{c-iT} \zeta_k(s) \frac{X^s}{s} ds + \int_{c-iT}^{a-iT} \zeta_k(s) \frac{X^s}{s} ds \\ + \int_{a-iT}^{a+iT} \zeta_k(s) \frac{X^s}{s} ds + \int_{a+iT}^{c+iT} \zeta_k(s) \frac{X^s}{s} ds + \int_{c+iT}^{c+i\infty} \zeta_k(s) \frac{X^s}{s} ds. \end{aligned} \tag{3.2.6}$$

We represent the contours above in the diagram below.



(3.2.7)

Another tool we need for establishing upper bounds for partial sums of a Dirichlet series is stated below.

Lemma 3.2.4. *Let*

$$G(s) = \sum_n \frac{a_n}{n^s} = \prod_p \left(1 + \alpha_1 p^{-s} + \alpha_2^{-2s} + \cdots + \alpha_\ell p^{-\ell s}\right) \tag{3.2.8}$$

with all the $\alpha_i \in \mathbb{R}_{\geq 0}$. *Let* $j \in \mathbb{N}$ *be the smallest natural number such that* $\alpha_j \neq 0$. *Then, we have*

$$\sum_{n \leq X} a_n \ll X^{1/j+\epsilon} \tag{3.2.9}$$

where the implied constant depends on ϵ *and the* α_i.

Proof. Let $s = \sigma + it$ where σ and t are real numbers. For $\sigma > 1$ we have

$$\begin{aligned}\frac{G(s)}{\zeta^{\alpha_j}(js)} &= \prod_p \left(1 + \frac{\alpha_j}{p^{js}} + \frac{\alpha_{j+1}}{p^{(j+1)s}} + \cdots + \frac{\alpha_\ell}{p^{\ell s}}\right)\left(1 - \frac{\alpha_j}{p^{js}} + \frac{\alpha_j(\alpha_j - 1)}{2p^{2js}} + \dots\right) \\ &= \prod_p \left(1 + O(p^{-(j+1)s})\right).\end{aligned}$$

Thus, $G(s)\zeta^{-\alpha_j}(js)$ converges absolutely for all s with $\sigma > 1/(j+1)$. This implies that we can write

$$G(s) = \zeta^{\alpha_j}(js) \times (G(s)\zeta^{-\alpha_j}(js))$$

as a product of two functions, one with a pole at $s = 1/j$ and the other that converges for all $\mathbb{R}(s) > 1/(j+1)$. From the work of Chambert-Loir and Tschinkel (2001) (Theorem A.1) we have the following Tauberian theorem.

Theorem 3.2.5. *Let* $\{\lambda_n\}$ *be an increasing sequence of strictly positive real numbers and* $\{a_n\}$ *be a sequence of non-negative real numbers. Set* $f(s) = \sum_{n=1}^{\infty} a_n \lambda_n^{-s}$ *and* $F(X) = \sum_{\lambda_n \leq X} a_n$. *Let* $s = \sigma + it$. *Assume that* $f(s)$ *converges in the right half plane* $\sigma > a > 0$ *and that for some* $\delta_0 > 0$, $f(s)$ *has a meromorphic continuation in the right half plane where* $\sigma > a - \delta_0 > 0$ *with only a pole of order* b *at* $s = a$. *Furthermore suppose that there exists some* $\kappa > 0$ *such that for* $\sigma > a - \delta_0$,

$$\left| f(s) \frac{(s-a)^b}{s^b} \right| = O((1 + |t|)^\kappa).$$

Set $A = \lim_{s\to a} f(s)(s-a)^b > 0$. *Then there exists a monic polynomial* P *of degree* $b-1$ *such that,*

$$F(X) = \frac{A}{a(b-1)!}X^a P(\log(X)) + o(X^a) \tag{3.2.10}$$

This, together with the Phragmén Lindelöf principle implies $\sum_{n\leq X} a_n \ll X^{1/j+\epsilon}$.

□

Another important tool that we will use repeatedly to evaluate series is partial summation or Abel summation, which can be found in any introductory text such as in the Appendix of Montgomery and Vaughan (2007).

Proposition 3.2.6. (Abel Summation) *Let* f *and* g *be functions with* $f : (\mathbb{N} \cap [1, X]) \to \mathbb{C}$ *and let* g *be a differentiable function on* $[1, X]$. *Let* $M_f(X) := \sum_{n\leq X} f(n)$. *Then we have*

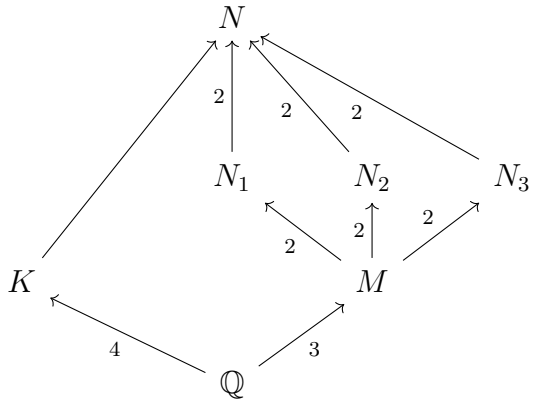
$$\sum_{n\leq X} f(n)g(n) = M_f(X)g(X) - \int_1^X M_f(t)g'(t)dt. \tag{3.2.11}$$

Chapter 4

Counting sextic extensions with Galois group A_4

In this chapter we establish an asymptotic expression for the number of sextic fields of $\mathbb{Q}$ with Galois group A_4 and discriminant bounded above by X. In particular, we prove Theorem 2.1.10 in this chapter. In this section, we set up notation and discuss the tools that are used to prove the result. In Section 4.1 we set up the notation and indicate what the main tools are to prove Theorem 2.1.10. In section 4.2 we go over the details, in particular the contour integrals.

Notation 4.0.1. Throughout this chapter we will fix the name of field extensions as given in the diagram below.



(4.0.1)

Here, $N/\mathbb{Q}$ is a Galois extension with Galois group A_4. M is the unique cubic subfield of $N/\mathbb{Q}$. $M/\mathbb{Q}$ is a Galois extension with Galois group C_3. There are 4 isomorphic quartic extensions which we represent by just one $K/\mathbb{Q}$. The three sextic fields N_1, N_2 and N_3 are isomorphic to each other and from now on we only refer to

$N_1/\mathbb{Q}$ as the sextic extension. $M/\mathbb{Q}$ is referred to as the cubic resolvent of $K/\mathbb{Q}$. All of this material can be found in the introduction of Cohen and Thorne (2016a).

We use Notation 4.0.1 throughout this chapter. Now we set up an equation to count $N_6(\mathbb{Q}, A_4; X)$. We use the discriminant relation

$$d_{N_1/\mathbb{Q}} = d_{M/\mathbb{Q}}^2 \mathcal{N}_{M/\mathbb{Q}}(d_{N_1/M}) \tag{4.0.2}$$

to set up the desired equation

$$N_6(\mathbb{Q}, A_4; X) = \sum_{\substack{M/\mathbb{Q} \\ \mathcal{N}(d_{M/\mathbb{Q}}) \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q}) = C_3}} \sum_{\substack{N_1/M \\ [N_1:M]=2 \\ \mathrm{Gal}(N_1/\mathbb{Q}) = A_4 \\ \mathcal{N}_{M/\mathbb{Q}}(d_{N_1/M}) \leq X \mathcal{N}(d_{M/\mathbb{Q}})^{-2}}} 1. \tag{4.0.3}$$

The outer sum can be computed using partial summation and the works of Cohn (1954) and Cohen, Diaz y Diaz, and Olivier (2002b) that imply

$$N_3(\mathbb{Q}, C_3; X) = c_1 X^{1/2} + O(X^{1/3+\epsilon}) \tag{4.0.4}$$

for an explicit constant c_1. Now we focus on computing the inner sum of (4.0.3). To do so we gather and state the following information.

1. A correspondence between the quartic extensions $K/\mathbb{Q}$ and the quadratic extensions N_i/M as first indicated by Baily (1980).

2. Establish a discriminant relation between the $K/\mathbb{Q}$, $M/\mathbb{Q}$ and N_1/M as stated by Baily (1980).

3. Make use of an expression established by Cohen and Thorne (2016b) that counts the number of quartic extensions $K/\mathbb{Q}$ ordered by discriminant with a fixed cubic resolvent $M/\mathbb{Q}$.

The correspondence between the quartic extensions and the quadratic extensions of the cubic resolvent can be set up as follows:

Definition 4.0.2. We will say that an element $\alpha \in M^* \setminus (M^*)^2$ has square norm if $\mathcal{N}_{M/\mathbb{Q}}(\alpha)$ is a square in $\mathbb{Q}^*$. We say that a quadratic extension N_1/M has trivial norm if $N_1 = M(\sqrt{\alpha})$ where $\alpha \in M^*$ has square norm.

Theorem 4.0.3 (Cohen and Thorne (2016a))**.** *Let M, K, N_1, N_2, N_3 and N be as in diagram* (4.0.1) *above. There is a correspondence between isomorphism classes of A_4 quartic fields $K/\mathbb{Q}$, and pairs (M, N_i), with $i \in \{1, 2, 3\}$, where M is the cubic resolvent field of K, and $N_1 = M(\sqrt{\alpha})$ is a quadratic extension of trivial norm. Similarly, N_2/M and N_3/M are quadratic extensions of a root of α or either of its non-trivial conjugates. Under this correspondence any one of the N_i yield the same K up to isomorphism.*

The relation above is useful thanks to a result of Heilbronn (1971) who observed that the fields K, M and N_1 share the following discriminant relation

$$d_{K/\mathbb{Q}} = d_{M/\mathbb{Q}} \mathcal{N}_{M/\mathbb{Q}}(d_{N_1/M}). \tag{4.0.5}$$

Now we state a result from Cohen and Thorne (2016b) who establish an expression that counts quartic fields $K/\mathbb{Q}$ ordered by discriminant with a fixed cubic resolvent. For each fixed $M/\mathbb{Q}$, we define $\mathcal{G}(M)$ to be the set of all A_4 quartic fields $K/\mathbb{Q}$ that have cubic resolvent isomorphic to $M/\mathbb{Q}$. Precisely, they establish an exact expression for

$$f(M, s) = \frac{1}{3} + \sum_{K \in \mathcal{G}(M)} \frac{1}{\mathcal{N}_{M/\mathbb{Q}}(d_{N_1/M})^{s/2}} \tag{4.0.6}$$

where $N_1/\mathbb{Q}$ is the sextic extension that corresponds to $K/\mathbb{Q}$. We make use of this by denoting $f(M, s) =: \sum_n f_M(n) n^{-s}$ and restating equation (4.0.3) as

$$N_6(\mathbb{Q}, A_4; X) = \sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q}) = C_3}} \sum_{n \leq X^{1/2} |d_{M/\mathbb{Q}}|^{-1}} f_M(n). \tag{4.0.7}$$

Finding an asymptotic expression for $\sum_{n \leq X} f_M(n)$ will be the subject of Section 4.1, first we state the expression for $f(M, s)$. In order to do so, we set up notation.

Let $\mathcal{L}(M) \subset \mathcal{G}(M)$ denote the set of quartic extensions $K/\mathbb{Q}$ with cubic resolvent $M/\mathbb{Q}$ with the additional restriction that $K/\mathbb{Q}$ is totally real when $M/\mathbb{Q}$ is totally real. We define $\mathcal{L}(M)$ as

$$\mathcal{L}(M) := \{K : K \in \mathcal{L}(M) \text{ and } |d_{K/\mathbb{Q}}| = |d_{M/\mathbb{Q}}|\}. \tag{4.0.8}$$

With the ramification notation established Section 3.1, we have the following result.

Theorem 4.0.4. *[Cohen and Thorne, Prop 6.4 and Thm 1.4] We have*

$$\begin{aligned} f(M,s) = \sum_n \frac{f_M(n)}{n^s} &= \frac{1}{3} M_1(s) \prod_{p\mathcal{O}_M=(111)} \left(1+\frac{3}{p^s}\right) \\ &+ \sum_{K\in\mathcal{L}(M)} M_{2,K}(s) \prod_{\substack{p\mathcal{O}_M=(111)\\ p\mathcal{O}_K=(1111)\\ p\neq 2}} \left(1+\frac{3}{p^s}\right) \prod_{\substack{p\mathcal{O}_M=(111)\\ p\mathcal{O}_K=(22)\\ p\neq 2}} \left(1-\frac{1}{p^s}\right) \end{aligned} \tag{4.0.9}$$

where $M_1(s)$ and $M_{2,K}(s)$ depend on how the prime 2 ramifies in M and in K respectively. To elaborate:

M split	*K split*	$M_1(s)$	$M_{2,K}(s)$
(3)	(31)	$1+3/2^{3s}$	$1+3/2^{3s}$
(111)	(1111)	$1+3/2^{2s}+4/2^{6s}+2/2^{4s}$	$1+3/2^{2s}+6/2^{3s}+6/2^{4s}$
(111)	(22)	$1+3/2^{2s}+4/2^{3s}+2/2^{4s}$	$1+3/2^{2s}-2/2^{3s}-2/2^{4s}$
(1^3)	(1^31)	$1+1/2^s+2/2^{3s}$	$1+1/2^s+2/2^{3s}$

We also have from Proposition 6.4 of Cohen and Thorne (2016b),

$$|\mathcal{L}(M)| = \frac{|\mathrm{Cl}_M[2]|-1}{3}. \tag{4.0.10}$$

Note that Proposition 6.4 from Cohen and Thorne (2016b) follows from the work of Heilbronn (1971).

4.1 Computing the main term and the error terms for $N_6(\mathbb{Q}, A_4; X)$

We use the same notation as established in the previous section. We now focus on obtaining an expression for $\sum_{n\leq X} f_M(n)$, where $\sum_n f_M(n)/n^s$ is as defined in

equation (4.0.9). From the definition of $f(M,s)$ we see that there are two main parts that contribute to $\sum_n f_M(n)/n^s$. We examine the two parts separately and set up notation to do so.

$$\begin{aligned} f(M,s) =& f_1(M,s) + \sum_{K\in\mathcal{L}(M)} f_2(M,K,s) \\ f_1(M,s) =& \sum_n \frac{f_{M,1}(n)}{n^s} := \frac{1}{3}M_1(s) \prod_{p\mathcal{O}_M=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1+\frac{3}{p^s}\right) \\ f_2(M,K,s) =& \sum_n \frac{f_{M,K}(n)}{n^s} := M_{2,K}(s) \prod_{\substack{p\mathcal{O}_M=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \\ p\mathcal{O}_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 \\ p\neq 2}} \left(1+\frac{3}{p^s}\right) \prod_{\substack{p\mathcal{O}_M=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \\ p\mathcal{O}_K=\mathfrak{p}_1\mathfrak{p}_2 \\ p\neq 2}} \left(1-\frac{1}{p^s}\right) \end{aligned} \tag{4.1.1}$$

Using the above with equation (4.0.7) implies

$$\begin{aligned} N_6(\mathbb{Q},A_4;X) = & \sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}|\leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{n\leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} f_{M,1}(n) \\ & + \sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}|\leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{K\in\mathcal{L}(M)} \sum_{n\leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} f_{M,K}(n). \end{aligned} \tag{4.1.2}$$

Now we focus on computing $\sum_{n\leq X} f_{M,1}(n)$. From the definition, $f_1(M,s)$ is similar to $\zeta_M(s)$, hence we break it into a product of two Dirichlet series as

$$f_1(M,s) = \zeta_M(s) \times \frac{f_1(M,s)}{\zeta_M(s)}.$$

The corresponding partial sums are:

$$\begin{aligned} \sum_{n\leq X} f_{M,1}(n) &= \sum_{n\leq X} g_M(n) \sum_{m\leq X/n} h_M(m), \\ \sum_{n\geq 1} \frac{h_M(n)}{n^s} &:= \zeta_M(s), \\ \sum_{n\geq 1} \frac{g_M(n)}{n^s} &:= \frac{f_1(M,s)}{\zeta_M(s)}. \end{aligned} \tag{4.1.3}$$

Now by multiplying Euler products or using equation (3.2.1)

$$\sum_n \frac{g_M(n)}{n^s} = r_M(s) \prod_{\substack{p\mathcal{O}_M=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \\ p\neq 2}} \left(1-\frac{6}{p^{2s}}+\frac{8}{p^{3s}}-\frac{3}{p^{4s}}\right) \prod_{\substack{p\mathcal{O}_M=\mathfrak{p}_1 \\ p\neq 2}} \left(1-\frac{1}{p^{3s}}\right). \tag{4.1.4}$$

The function $r_M(s)$ is the contribution from the ramified primes and the prime 2. Note that since the number of primes that ramify is at most $O(\omega(\mathcal{N}_{M/\mathbb{Q}}(d_{N_1/M})))$, the contribution of $r_M(s)$ to $\sum_{n\leq X} g_M(n)$ is at most X^{ϵ}. By Lemma 3.2.4 we have that $\sum_{n\leq X} g_M(n) \ll X^{1/2+\epsilon}$ where the constant does not depend on M. We now focus on evaluating $\sum_{n\leq X} h_M(n)$. Using Perron's formula, as in equation (3.2.6), we integrate $\zeta_M(s)X^s s^{-1}$ over the five contours C_1, C_2, C_3, C_4 and C_5. Recall the contours are the straight lines that connect the following set of points:

Contour	Start point	End Point
C_1	$1+\delta-i\infty$	$1+\delta-iT$
C_2	$1+\delta-iT$	$a-iT$
C_3	$a-iT$	$a+iT$
C_4	$a+iT$	$1+\delta+iT$
C_5	$1+\delta+iT$	$1+\delta+i\infty$

Table 4.1: Table of Contours

This is succinctly represented in Diagram (3.2.7). Here a is a constant in the interval $(0,1)$. In the next section we will show the following.

Proposition 4.1.1. *Let $\sum_n h_M(n)n^{-s} = \zeta_M(s)$. For any arbitrarily small positive constants ϵ and δ with $\epsilon > \delta > 0$, and $a \in (0, 0.5)$, we have*

$$\sum_{n\leq X} h_M(n) = \mathrm{res}_{s=1}\zeta_M(s)X + O\left(\frac{X^{1+\epsilon}}{T} + |d_{M/\mathbb{Q}}|^{1/2-a/2}X^{a+\epsilon}|T|^{3/2(1-a)}\right). \tag{4.1.5}$$

Similarly when $a \in [0.5, 1)$ we have

$$\sum_{n\leq X} h_M(n) = \mathrm{res}_{s=1}\zeta_M(s)X + O\left(\frac{X^{1+\epsilon}}{T} + X^{a+\epsilon}|d_{M/\mathbb{Q}}|^{(2-2a)/5+\epsilon}T^{(6-6a)/5}\right). \tag{4.1.6}$$

We will use the above to evaluate $\sum_{n\leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} f_{M,1}(n)$. Since

$$\sum_{n\leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} f_{M,1}(n) = \sum_{n\leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} g_M(n) \sum_{m\leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}n^{-1}} h_M(m), \tag{4.1.7}$$

Proposition 4.1.1 implies that for $a \in (0, 1/2)$ we have

$$\sum_{m \leq \frac{X^{1/2}}{|d_{M/\mathbb{Q}}|n}} h_M(m) = \mathrm{res}_{s=1}\zeta_M(s)\frac{(X/n^2)^{1/2}}{|d_{M/\mathbb{Q}}|} + O\left(\frac{(X/n^2)^{1/2+\epsilon}}{T|d_{M/\mathbb{Q}}|^{1+\epsilon}} + |d_{M/\mathbb{Q}}|^{1/2-3a/2}(X/n^2)^{a/2+\epsilon}|T|^{3/2(1-a)}\right) \tag{4.1.8}$$

and for $a \in [1/2, 1)$, we have

$$\sum_{m \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}n^{-1}} h_M(m) = \mathrm{res}_{s=1}\zeta_M(s)\frac{(X/n^2)^{1/2}}{|d_{M/\mathbb{Q}}|} + O\left(\frac{(X/n^2)^{1/2+\epsilon}}{T|d_{M/\mathbb{Q}}|^{1+\epsilon}} + |d_{M/\mathbb{Q}}|^{(2-7a)/5}(X/n^2)^{a/2+\epsilon}|T|^{6/5(1-a)}\right). \tag{4.1.9}$$

We denote the error term above as

$$E_T(a) = E(a) := \sum_{m \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}n^{-1}} h_M(m) - \mathrm{res}_{s=1}\zeta_M(s)\frac{(X/n^2)^{1/2}}{|d_{M/\mathbb{Q}}|}.$$

First we establish the main term, this is done by summing over the n. As indicated in equation (4.1.2) and (4.1.7), the main term may be obtained by finding the value of

$$\sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} g_M(n)\mathrm{res}_{s=1}\zeta_M(s)\frac{(X/n^2)^{1/2}}{|d_{M/\mathbb{Q}}|}$$

$$= X^{1/2} \sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \frac{\mathrm{res}_{s=1}\zeta_M(s)}{|d_{M/\mathbb{Q}}|} \sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} \frac{g_M(n)}{n}.$$

Note that by Louboutin (2011) we have

$$|\mathrm{res}_{s=1}\zeta_M(s)| = O(\log^2(|d_{M/\mathbb{Q}}|)) \tag{4.1.10}$$

where the implied constant is independent of M. Using this and the fact that $\sum_{n \leq X} g_M(n) \ll X^{1/2+\epsilon}$, we have that

$$\sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \frac{\mathrm{res}_{s=1}\zeta_M(s)}{|d_{M/\mathbb{Q}}|} \sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} \frac{g_M(n)}{n}$$

is bounded above by a constant. By the way $\sum g_M(n)n^{-s}$ is defined, and letting $X \to \infty$ we see that the above is

$$C := \sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \geq 1 \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \frac{\mathrm{res}_{s=1}(f_1(M,s))}{|d_{M/\mathbb{Q}}|} = \sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \frac{\mathrm{res}_{s=1}\zeta_M(s)}{|d_{M/\mathbb{Q}}|} \sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} \frac{g_M(n)}{n}. \tag{4.1.11}$$

Hence we have that the coefficient of $X^{1/2}$ is C. Hence we have that

$$\begin{aligned} N_6(\mathbb{Q}, A_4; X) =& CX^{1/2} + \sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{K \in \mathcal{L}(M)} \sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} f_{M,K}(n) \\ &+ O\left(\sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} g_M(n)E(a) \right). \end{aligned} \tag{4.1.12}$$

We now take the sum over n and then minimize the error term with respect to T and a. Note that

$$\sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} \frac{g_M(n)}{n^a} \ll \left(\left(\frac{X^{1/4}}{|d_{M/\mathbb{Q}}|^{1/2}} \right)^{1-2a} + 1 \right).$$

Hence when $a \in (0, 1/2)$ we have that the error in (4.1.12), using (4.1.8) is

$$\begin{aligned} & \sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} g_M(n)E(a) \\ \ll & \sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \frac{X^{1/2+\epsilon}}{T|d_{M/\mathbb{Q}}|^{1+\epsilon}} \sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} \frac{g_M(n)}{n^{1+\epsilon}} \\ & + \sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \frac{X^{a/2+\epsilon}}{T^{3/2(a-1)}|d_{M/\mathbb{Q}}|^{(3a-1)/2}} \sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} \frac{g_M(n)}{n^{a+\epsilon}} \\ \ll & \sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \frac{X^{1/2+\epsilon}}{T|d_{M/\mathbb{Q}}|^{1+\epsilon}} + |d_{M/\mathbb{Q}}|^{1/2-3a/2}X^{a/2+\epsilon}|T|^{3/2(1-a)} \left(\left(\frac{X^{1/4}}{|d_{M/\mathbb{Q}}|^{1/2}} \right)^{1-2a} + 1 \right). \end{aligned} \tag{4.1.13}$$

Similarly by noting that when $a \in [1/2, 1)$,

$$\left(\left(\frac{X^{1/4}}{|d_{M/\mathbb{Q}}|^{1/2}}\right)^{1-2a} + 1\right) \ll 1$$

since $|d_{M/\mathbb{Q}}| < X^{1/2}$, using (4.1.9), the error term is in (4.1.12) is

$$\begin{aligned} &\sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} g_M(n)E(a) \\ \ll &\sum_{\substack{M/\mathbb{Q} \\ |d_{M/\mathbb{Q}}| \leq X^{1/2} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \frac{X^{1/2+\epsilon}}{T|d_{M/\mathbb{Q}}|^{1+\epsilon}} + |d_{M/\mathbb{Q}}|^{(2-7a)/5} X^{a/2+\epsilon}|T|^{6/5(1-a)}. \end{aligned} \tag{4.1.14}$$

We say that $E1_T(a)$ is (4.1.13) when $a \in (0, 1/2)$ and $E1_T(a)$ is (4.1.14) when $a \in [1/2, 1)$. Now we minimize $E1(a) = E1_T(a)$ with respect to T. We allow T to vary with M. We need to ensure that $T > 1$ and is in fact increasing with X to ensure that the bounds from our integrals hold. We minimize $E1(a)$ with respect to T. Let $\epsilon > 0$ be any arbitrarily small positive constant, then we have the following table. The first column denotes a value of a that we fix. Having fixed that value of a, the error term is minimized when we have T being the size indicated in the second column. The third column represents that size of $E1_T(a)$ after having fixed a and T. The last column represents the condition we need so that $T > 1$ holds.

a	T	$E1_T(a)$ is	$\lvert d_{M/\mathbb{Q}}\rvert$
ϵ	$O(\lvert d_{M/\mathbb{Q}}\rvert^{-2/5+\epsilon} X^{1/10+\epsilon})$	$O(\lvert d_{M/\mathbb{Q}}\rvert^{-3/5+\epsilon} X^{2/5+\epsilon})$	$\lvert d_{M/\mathbb{Q}}\rvert < X^{1/4}$
$1/2$	$O(\lvert d_{M/\mathbb{Q}}\rvert^{-7/16+\epsilon} X^{5/32+\epsilon})$	$O(\lvert d_{M/\mathbb{Q}}\rvert^{-9/16+\epsilon} X^{11/32+\epsilon})$	$\lvert d_{M/\mathbb{Q}}\rvert < X^{5/14}$
$1-\epsilon$	$O(X^{\epsilon})$	$O(\lvert d_{M/\mathbb{Q}}\rvert^{-1+\epsilon} X^{1/2+\epsilon})$	

Given this we see that when $|d_{M/\mathbb{Q}}| < X^{5/14}$, $|d_{M/\mathbb{Q}}|^{-9/16} X^{11/32} < X^{1/2}|d_{M/\mathbb{Q}}|^{-1+\epsilon}$ implying that $E1(1/2) < E1(1-\epsilon)$. We also see that $E1(1/2) < E1(\epsilon)$ for all the range of $|d_{M/\mathbb{Q}}|$ that we are concerned with. Let $A(a)$ denote the exponent of $|d_{M/\mathbb{Q}}|$ in $E1(a)$ and let $A_1(a)$ denote the exponent of X in $E1(a)$ after having fixed T. So

for instance, by the table above, $A(1/2) = -9/16+\epsilon$ and $A_1(1/2) = 11/32+\epsilon$. Under this notation, we minimize the error terms as follows:

$$\begin{aligned}\sum_{\substack{M/\mathbb{Q}\\ |d_{M/\mathbb{Q}}|\le X^{1/2}\\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} X^{A_1(a)}|d_{M/\mathbb{Q}}|^{A(a)} \ll & \sum_{\substack{M/\mathbb{Q}\\ |d_{M/\mathbb{Q}}|< X^{5/14}\\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} E1(1/2) + \sum_{\substack{M/\mathbb{Q}\\ X^{5/14}\le|d_{M/\mathbb{Q}}|\le X^{1/2}\\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} E1(1-\epsilon)\\ \ll & X^{11/32+\epsilon} + X^{9/28+\epsilon}\\ \ll & X^{11/32+\epsilon} \ll X^{0.3438\cdots+\epsilon}.\end{aligned} \tag{4.1.15}$$

This implies

$$N_6(\mathbb{Q}, A_4; X) = CX^{1/2} + \sum_{\substack{M/\mathbb{Q}\\ |d_{M/\mathbb{Q}}|\le X^{1/2}\\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{K\in\mathcal{L}(M)} \sum_{n\le X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} f_{M,K}(n) + O(X^{11/32+\epsilon}). \tag{4.1.16}$$

Recall the definition of $\sum f_{M,K}(s)n^{-s}$ in (4.1.1). Now we address evaluating $\sum_{K\in\mathcal{L}(M)}\sum_{n\le X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} f_{M,K}(n)$. For each K we observe that $\sum_n f_{M,K}(n)n^{-s}$ is similar to $\zeta_K(s)/\zeta(s)$, and we break the terms up as follows:

$$\begin{aligned}&\sum_{n\le X} f_{M,K}(n) = \sum_{n\le X} g_{M,K}(n) \sum_{m\le X/n} h_{M,K}(m),\\ &\sum_{n\ge 1}\frac{h_{M,K}(n)}{n^s} = \frac{\zeta_K(s)}{\zeta(s)},\\ &\sum_{n\ge 1}\frac{g_{M,K}(n)}{n^s} = f_2(M,K,s)\frac{\zeta(s)}{\zeta_K(s)}.\end{aligned} \tag{4.1.17}$$

Here the Euler product for $\sum_n \frac{g_{M,K}(n)}{n^s}$ for real part of s bigger than 1 is

$$r_{M,K}(s)\prod_{\substack{p\mathcal{O}_K=(1111)\\ p\neq 2}}\left(1-\frac{1}{p^s}\right)^3\left(1+\frac{3}{p^s}\right)\prod_{\substack{p\mathcal{O}_K=(22)\\ p\neq 2}}\left(1-\frac{1}{p^{2s}}\right)^2\prod_{\substack{p\mathcal{O}_K=(31)\\ p\neq 2}}\left(1-\frac{1}{p^{3s}}\right) \tag{4.1.18}$$

where $r_{M,K}(s)$ is the contribution from the ramified primes and the prime 2. By Lemma 3.2.4, $\sum_{n\le X} g_{M,K}(n) = O(X^{1/2+\epsilon})$. We now state a result that we will establish in the next section.

Proposition 4.1.2. *Let $\sum_n h_{M,K}(n)n^{-s} = \zeta_K(s)/\zeta(s)$. For arbitrarily small positive constants ϵ and δ with $\epsilon > \delta > 0$, and $a \in (0,1)$, we have*

$$\sum_{n \leq X} h_{M,K}(n) = O\left(\frac{X^{1+\epsilon}}{T} + X^a T^{3(1-a)/2} |d_{M/\mathbb{Q}}|^{1/2-a/2}\right). \tag{4.1.19}$$

We will use the above to evaluate $\sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} f_{M,K}(n)$. Since as indicated in equation (4.1.17),

$$\sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} f_{M,K}(n) = \sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} g_{M,K}(n) \sum_{m \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}n^{-1}} h_{M,K}(m),$$

Proposition 4.1.2 implies that for $a \in (0,1)$ we have

$$\sum_{m \leq \frac{X^{1/2}}{|d_{M/\mathbb{Q}}|n}} h_{M,K}(m) = O\left(\frac{(X/n^2)^{1/2+\epsilon}}{T|d_{M/\mathbb{Q}}|^{1+\epsilon}} + |d_{M/\mathbb{Q}}|^{1/2-3a/2}(X/n^2)^{a/2+\epsilon}|T|^{3/2(1-a)}\right).$$

Now we take the sum over n to get that the above is

$$\ll \frac{X^{1/2+\epsilon}}{T|d_{M/\mathbb{Q}}|^{1+\epsilon}} + |d_{M/\mathbb{Q}}|^{1/2-3a/2} X^{a/2+\epsilon}|T|^{3/2(1-a)} \left(\left(\frac{X^{1/4}}{|d_{M/\mathbb{Q}}|^{1/2}}\right)^{1-2a} + 1\right).$$

Denoting the above as $E2_T(a)$, we minimize the above with respect to T in the table below. The first column denotes a value of a that we fix. Having fixed that value of a, the error term is minimized when we have T being the size indicated in the second column. The third column represents that size of $E1_T(a)$ after having fixed a and T. The last column represents the condition we need so that $T > 1$ holds.

a	T	$E2(a)$	$\lvert d_{M/\mathbb{Q}}\rvert$
$1/2$	$O(\lvert d_{M/\mathbb{Q}}\rvert^{-3/7+\epsilon} X^{1/7+\epsilon})$	$O(\lvert d_{M/\mathbb{Q}}\rvert^{-4/7+\epsilon} X^{5/14+\epsilon})$	$\lvert d_{M/\mathbb{Q}}\rvert < X^{1/3}$
$1-\epsilon$	$O(X^\epsilon)$	$O(\lvert d_{M/\mathbb{Q}}\rvert^{-1+\epsilon} X^{1/2+\epsilon})$	

Recall that $|\mathcal{L}(M)| = (|\mathrm{Cl}_M[2]| - 1)/3$. We set B to be the smallest known constant such that $|\mathrm{Cl}_M[2]| \ll_\epsilon |d_{M/\mathbb{Q}}|^{B+\epsilon}$. Hence we have that

$$\sum_{\substack{M/\mathbb{Q}\\ |d_{M/\mathbb{Q}}|\leq X^{1/2}\\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{K\in\mathcal{L}(M)} \sum_{n\leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} f_{M,K}(n)$$

$$\ll \sum_{\substack{M/\mathbb{Q}\\ |d_{M/\mathbb{Q}}|< X^{1/3}\\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} |\mathrm{Cl}_M[2]|E2(1/2) + \sum_{\substack{M/\mathbb{Q}\\ X^{1/3}\leq|d_{M/\mathbb{Q}}|\leq X^{1/2}\\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} |\mathrm{Cl}_M[2]|E2(1-\epsilon) \tag{4.1.20}$$

$$\ll X^{5/14} + X^{\frac{B-(1/14)}{3}+\epsilon} + X^{\frac{B+1}{3}+\epsilon} + X^{\frac{1+2B}{4}+\epsilon} + \ll X^{0.426\ldots}$$

Here we used the result in Bhargava et al. (2017) that states $B = 0.278\ldots$ is the best we can do at the moment. Hence, combining all the above with equation (4.1.16) we have,

$$N_6(\mathbb{Q}, A_4; X) = CX^{1/2} + O(X^{0.426+\epsilon}).$$

Under the assumption of the $\ell-$torsion conjecture (Conjecture 2.1.7), $B = 0$ which implies that

$$N_6(\mathbb{Q}, A_4; X) = CX^{1/2} + O(X^{5/14+\epsilon}).$$

The next section is devoted to computing the contour integrals.

4.2 The contour integrals

The purpose of this section is to justify the claims in Proposition 4.1.1 and Proposition 4.1.2. By equation (4.1.3), equation (4.1.17) and Perron's formula we have

$$\sum_{n\leq X} h_M(n) = \mathrm{res}_{s=1}\zeta_M(s)X + \frac{1}{2\pi i}\left(\int_{C_1}+\int_{C_2}+\int_{C_3}+\int_{C_4}+\int_{C_5}\zeta_M(s)\frac{X^s}{s}ds\right), \tag{4.2.1}$$

$$\sum_{n\leq X} h_{M,K}(n) = \frac{1}{2\pi i}\left(\int_{C_1}+\int_{C_2}+\int_{C_3}+\int_{C_4}+\int_{C_5}\frac{\zeta_K(s)}{\zeta(s)}\frac{X^s}{s}ds\right). \tag{4.2.2}$$

where the contours are the straight lines that connect the points as stated in Table 4.1. Throughout this section we assume that $\epsilon > \delta > 0$ are arbitrarily small positive constants. The integrals over C_1 and C_5 may be treated similarly and the integrals

over C_2 and C_4 may be treated similarly. We break this section into subsections that address integrating over each of the given contours. Such methods may be found in other analytic number theory works such as Atkinson (1941).

4.2.1 Integrating over C_1 and C_5

In this subsection we establish

$$\int_{C_1} \zeta_M(s)\frac{X^s}{s}ds = O\left(\frac{X^{1+\epsilon}}{T}\right) \tag{4.2.3}$$

and

$$\int_{C_1} \frac{\zeta_K(s)}{\zeta(s)}\frac{X^s}{s}ds = O\left(\frac{X^{1+\epsilon}}{T}\right). \tag{4.2.4}$$

The integrals over C_5 can be bounded above in the same way. The method to integrate $\zeta_M(s)$ is the same as the method to integrate $\zeta_K(s)/\zeta(s)$, here we only integrate $\zeta_M(s)$.

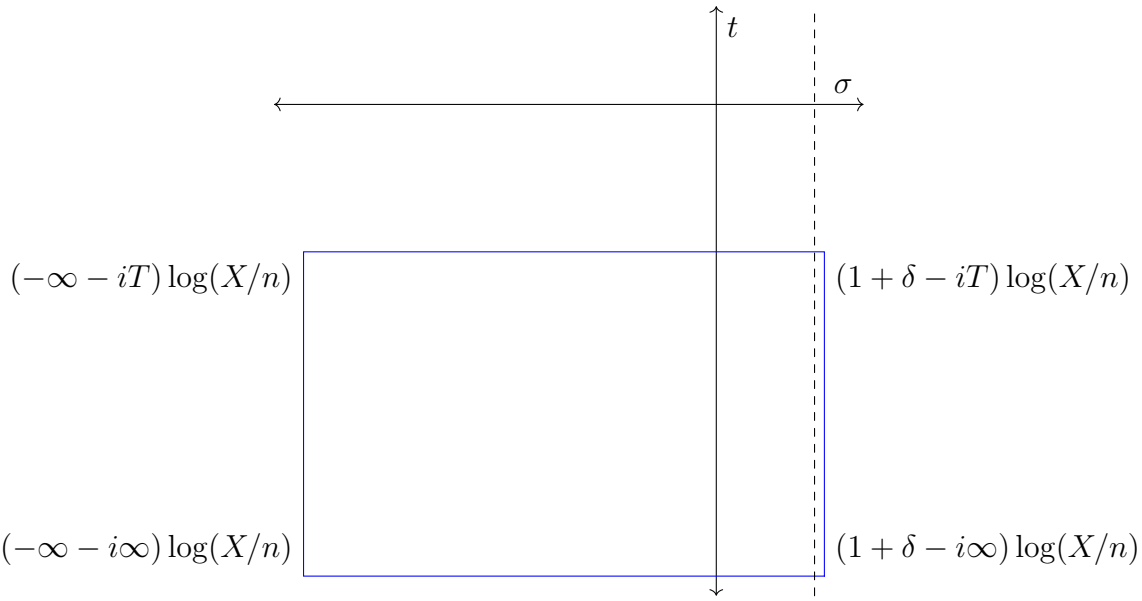
We begin by interchanging the order of summation, and have

$$\int_{1+\delta-i\infty}^{1+\delta-iT} \zeta_M(s)\frac{X^s}{s}ds = \sum_n h_M(n)\int_{1+\delta-i\infty}^{1+\delta-iT} \frac{(X/n)^s}{s}ds.$$

Observe that

$$\int_{1+\delta-i\infty}^{1+\delta-iT} \frac{(X/n)^s}{s}ds = \int_{(1+\delta-i\infty)\log(X/n)}^{(1+\delta-iT)\log(X/n)} \frac{e^s}{s}ds$$

Note that $X \neq n$. The integral is over a contour that does not cross a point with $t = 0$, hence e^s/s has no poles in the contour. We bound this integral by forming a rectangle to the left as indicated by the diagram below. Note here we assume that $\log(X/n) > 0$ and the dotted line represents $\sigma = 1$.



(4.2.5)

Since the function e^s/s has no poles in the rectangle and σ tends to negative infinity, e^s/s tends to zero uniformly in t, we have

$$\int_{(1+\delta-iT)\log(X/n)}^{(1+\delta-i\infty)\log(X/n)} \frac{e^s}{s} = \int_{(1+\delta-iT)\log(X/n)}^{(-\infty-iT)\log(X/n)} \frac{e^s}{s}ds + \int_{(1+\delta-i\infty)\log(X/n)}^{(-\infty-i\infty)\log(X/n)} \frac{e^s}{s}ds.$$

Hence

$$\int_{(1+\delta-iT)\log(X/n)}^{(-\infty-iT)\log(X/n)} \left|\frac{e^s}{s}\right|ds \leq \frac{1}{T\log(X/n)} \int_{-\infty}^{(1+\delta)\log(X/n)} e^s ds \ll \frac{(X/n)^{1+\delta}}{T\log(X/n)}.$$

Bounding $\int_{(1+\delta-i\infty)\log(X/n)}^{(-\infty-i\infty)\log(X/n)} \frac{e^s}{s}ds$ is similar. This gives us

$$\int_{1+\delta-i\infty}^{1+\delta-iT} \frac{(X/n)^s}{s}ds \ll \frac{1}{T}\frac{(X/n)^{1+\delta}}{\log(X/n)}.$$

Hence

$$\int_{1+\delta-i\infty}^{1+\delta-iT} \zeta_M(s)\frac{X^s}{s}ds = O\left(\frac{X^{1+\delta}}{T}\sum_n \frac{h_M(n)}{n^{1+\delta}\log(X/n)}\right).$$

We break the ranges of the summation as

$$\sum_n = \sum_{n\leq X/2} + \sum_{n=X/2}^{X} + \sum_{n=X}^{2X} + \sum_{n>2X}.$$

Notice that we have for $n \leq X/2$, $(\log(X/n))^{-1} \leq (\log(2))^{-1}$. The $h_M(n)$ are bounded above in size by $d_3(n)$ where $d_3(n)$ is the number of ways to write n as the product

of 3 natural numbers. This implies $h_M(n) \leq d_3(n)$ and we know that $d_3(n) = o(n^\delta)$. Using these facts and partial summation we have that

$$\sum_{n \leq X/2} \frac{h_M(n)}{n^{1+\delta} \log(X/n)} = O(1).$$

Similarly

$$\sum_{n \geq 2X} \frac{h_M(n)}{n^{1+\delta} \log(X/n)} = O(1).$$

We fix X to be a fourth of an odd integer. For $n \in (X/2, X]$, we have

$$(\log(X/n))^{-1} = O\left(\frac{X}{X-n}\right).$$

This implies

$$\sum_{n \geq X/2}^{X} \frac{h_M(n)}{n^{1+\delta} \log(X/n)} = O\left(\sum_{n \geq X/2}^{X} \frac{n^\epsilon}{n^{1+\delta}} \frac{X}{X-n}\right) = O\left(\sum_{n \geq X/2}^{X} \frac{1}{X-n}\right) = O(\log(X)).$$

The part of the series with $n \in (X, 2X)$ can be treated similarly. This implies

$$\int_{C_1} \zeta_M(s) \frac{X^s}{s} ds = O\left(\frac{X^{1+\delta} \log(X)}{T}\right)$$

where the implied constant depends on δ. Similarly, noting that $h_{M,K}(n) \leq d_4(n) = o(n^\delta)$ we have the result in equation (4.2.4).

4.2.2 Integrating over C_2, C_4 and C_3

In this subsection we establish

$$\int_{C_2+C_3+C_4} \zeta_M(s) \frac{X^s}{s} ds \ll \frac{X^{1+\delta}}{T} + X^{a+\epsilon} |d_{M/\mathbb{Q}}|^{(2-2a)/5+\epsilon} T^{(6-6a)/5} \tag{4.2.6}$$

for an arbitrarily small positive ϵ and $a \in [0.5, 1)$. For $a \in (0, 0.5)$ we have

$$\int_{C_2+C_3+C_4} \zeta_M(s) \frac{X^s}{s} ds \ll \frac{X^{1+\epsilon}}{T} + |d_{M/\mathbb{Q}}|^{1/2-a/2} X^a |T|^{3/2(1-a)}. \tag{4.2.7}$$

Similarly for $a \in (0, 1)$ we have

$$\int_{C_2+C_3+C_4} \frac{\zeta_K(s)}{\zeta(s)} \frac{X^s}{s} ds \ll \frac{X^{1+\epsilon}}{T} + |d_{M/\mathbb{Q}}|^{1/2-a/2} X^a T^{3(1-a)/2}. \tag{4.2.8}$$

We may establish the same upper bound for the integral over C_2 as the upper bound of the integral over C_4. Since the method to establish this upper bound is exactly the same, we only discuss how to establish the upper bound over C_4 in this subsection.

The method to establish the bounds for the integrals over $\zeta_M(s)$ and $\zeta_K(s)/\zeta(s)$ is the same. We establish the bound in detail for $\zeta_M(s)$ and only indicate any differences in the method for establishing bounds for $\zeta_K(s)/\zeta(s)$. To establish these upper bounds we use the sub-convexity bound established by Heath-Brown (1978) as stated in equation (3.2.4). Heath-Brown established upper bounds for $|L(\chi, \frac{1}{2}+it)|$ where χ is a Dirichlet character. Since $M/\mathbb{Q}$ is a cyclic cubic extension,

$$\zeta_M(s) = \prod_{\chi} L(s, \chi)$$

where χ are the cubic characters. We will use

$$|\zeta_M(1/2+it)| \ll |d_{M/\mathbb{Q}}|^{1/5+\epsilon}|t|^{3/5}. \tag{4.2.9}$$

The Phragmén Lindelöf principle (Theorem 3.2.2) then implies that for $\sigma \in [1/2, 1]$ we have

$$|\zeta_M(\sigma+it)| \ll |d_{M/\mathbb{Q}}|^{(2-2\sigma)/5+\epsilon}|t|^{3(2-2\sigma)/5}. \tag{4.2.10}$$

For $\sigma \in (0, 1/2)$ we will use the standard convexity bound. Before we get around to using this, we have to address the pole at $s = 1$ of $\zeta_M(s)$. To address the pole at $s = 1$, we define $V(s)$ as

$$V(s) := \zeta_M(s) - \frac{\mathrm{res}_{s=1}(\zeta_M(s))}{s-1}.$$

This implies we have

$$\int_{C_2+C_3+C_4} \zeta_M(s)\frac{X^s}{s}ds = \int_{C_2+C_3+C_4} V(s)\frac{X^s}{s}ds + \int_{C_2+C_3+C_4} \frac{\mathrm{res}_{s=1}(\zeta_M(s))}{s-1}\frac{X^s}{s}ds.$$

First we show that

$$\int_{C_2+C_3+C_4} \frac{\mathrm{res}_{s=1}(\zeta_M(s))}{s-1}\frac{X^s}{s}ds \ll \frac{X^{1+\delta}}{T^2} + X^{a+\delta}. \tag{4.2.11}$$

Integrating over C_2 we have

$$\int_{a+iT}^{1+\delta+iT} \frac{\mathrm{res}_{s=1}(\zeta_M(s))}{s-1}\frac{X^s}{s}ds \ll \mathrm{res}_{s=1}(\zeta_M(s))X^{1+\delta}T^{-2}$$

and similarly over C_3 we have

$$\int_{a-iT}^{a+iT} \frac{\mathrm{res}_{s=1}(\zeta_M(s))}{s-1}\frac{X^s}{s}ds \ll \mathrm{res}_{s=1}(\zeta_M(s))X^{a}.$$

As indicated in (4.1.10) the residue is a small in comparison to the discriminant. Since the discriminant of $M/\mathbb{Q}$ is at most a small finite power of X, we have (4.2.11).

Now we address the integral over $V(s)$. We integrate on the contours C_2, C_3 and C_4 by finding upper bounds on the size of $V(s)$ on those contours. To establish upper bounds, first we note that by the triangle inequality,

$$|V(s)| \leq |\zeta_M(s)| + \left|\frac{\mathrm{res}_{s=1}(\zeta_M(s))}{s-1}\right|.$$

Note for s on C_2 with $|T| > 1000$,

$$\max_{s\in C_2}\left(\frac{\mathrm{res}_{s=1}(\zeta_M(s))}{s-1}\right) = O\left(X^{\epsilon}\right).$$

Hence if $a \geq 1/2$ then we have,

$$\begin{aligned}
&\int_{C_2} V(s)\frac{X^s}{s}ds \ll \int_{a+iT}^{1+\delta+iT} \left(|\zeta_M(s)| + X^{\epsilon}\right)\left|\frac{X^s}{s}\right|ds \\
\ll &\int_a^{1+\delta} |d_{M/\mathbb{Q}}|^{(2-2\sigma)/5}T^{3(2-2\sigma)/5}\frac{X^{\sigma+\epsilon}}{T}d\sigma \\
\ll &|d_{M/\mathbb{Q}}|^{2/5}T^{1/5}X^{\epsilon}\int_a^{1+\delta}\left(\frac{X}{|d_{M/\mathbb{Q}}|^{2/5}T^{6/5}}\right)^{\sigma}d\sigma \\
\ll &|d_{M/\mathbb{Q}}|^{2/5}T^{1/5}X^{\epsilon}\left(\frac{X^{1+\delta}}{|d_{M/\mathbb{Q}}|^{2(1+\delta)/5}T^{6(1+\delta)/5}} + \frac{X^{a}}{|d_{M/\mathbb{Q}}|^{2a/5}T^{6a/5}}\right) \\
\ll &\frac{X^{1+\epsilon}}{T} + \frac{X^{a+\epsilon}|d_{M/\mathbb{Q}}|^{2(1-a)/5}}{T^{(6/5)(a-1)+1}}.
\end{aligned} \tag{4.2.12}$$

Similarly, when $a \leq 1$, we have

$$\left|\frac{\mathrm{res}_{s=1}(\zeta_M(s))}{a+it-1}\right| = O(X^{\epsilon}).$$

Consequently with $a \in [1/2, 1)$

$$\begin{aligned}\int_{C_3} V(s)\frac{X^s}{s}ds &\ll \int_{a+iT}^{a-iT} (|\zeta_M(s)| + X^\epsilon)\left|\frac{X^s}{s}\right|ds \\ &\ll \int_{-T}^{T} |d_{M/\mathbb{Q}}|^{(2-2a)/5}|t|^{3(2-2a)/5}\frac{X^{a+\epsilon}}{t+\epsilon}dt \\ &\ll |d_{M/\mathbb{Q}}|^{(2-2a)/5}X^{a+\epsilon}\int_{-T}^{T}|t|^{3(2-2a)/5}\frac{1}{t+\epsilon}dt. \\ &\ll |d_{M/\mathbb{Q}}|^{(2-2a)/5}X^{a+\epsilon}T^{3(2-2a)/5}.\end{aligned} \tag{4.2.13}$$

Note that while $T > 1$, we have that

$$\frac{X^{a+\epsilon}|d_{M/\mathbb{Q}}|^{2(1-a)/5}}{T^{(6/5)(a-1)+1}} < X^{a+\epsilon}|d_{M/\mathbb{Q}}|^{(2-2a)/5+\epsilon}T^{(6-6a)/5}.$$

Combining equations (4.2.13), (4.2.12), (4.2.11), (4.2.3) and (4.2.1) we have for $a \in [1/2, 1)$ equation (4.1.6).

In the case that $a < 1/2$, we will use the standard convexity bound. We have

$$\begin{aligned}&\int_{a+iT}^{1+iT} (|\zeta_M(s)| + X^\epsilon)\left|\frac{X^s}{s}\right|ds \\ \ll &\int_{a}^{1+\delta} |d_{M/\mathbb{Q}}|^{1/2-\sigma/2}T^{3/2-3/2\sigma}\frac{X^{\sigma+iT+\epsilon}}{T}d\sigma \\ \ll &|d_{M/\mathbb{Q}}|^{1/2}T^{1/2}X^\epsilon\int_a^{1+\delta}\left(\frac{X}{T^{3/2}|d_{M/\mathbb{Q}}|^{1/2}}\right)^\sigma d\sigma \\ \ll &\frac{X^{1+\delta}}{T} + \frac{X^{a+\epsilon}|d_{M/\mathbb{Q}}|^{1/2-a/2}}{T^{3a/2-1/2}}.\end{aligned} \tag{4.2.14}$$

Hence, when $a \leq 1/2$

$$\int_{C_2} V(s)\frac{X^s}{s}ds \ll \frac{X^{1+\delta}|d_{M/\mathbb{Q}}|^{-\delta}}{T} + \frac{X^{a+\epsilon}|d_{M/\mathbb{Q}}|^{1/2-a/2}}{T^{3a/2-1/2}}. \tag{4.2.15}$$

Similarly, we have

$$\begin{aligned}\int_{C_3} V(s)\frac{X^s}{s}ds &\ll \int_{-T}^{T} |d_{M/\mathbb{Q}}|^{1/2-a/2}|t|^{3/2(1-a)}\frac{X^{a+\epsilon}}{t+\epsilon}dt \\ &\ll |d_{M/\mathbb{Q}}|^{1/2-a/2}X^{a+\epsilon}\int_{-T}^{T}|t|^{3/2(1-a)}\frac{1}{t+\epsilon}dt \\ &\ll |d_{M/\mathbb{Q}}|^{1/2-a/2}X^{a+\epsilon}|T|^{3/2(1-a)}.\end{aligned} \tag{4.2.16}$$

Similarly, since we set $T > 1$, we have that

$$\frac{X^{a+\epsilon}|d_{M/\mathbb{Q}}|^{1/2-a/2}}{T^{3a/2-1/2}} < |d_{M/\mathbb{Q}}|^{1/2-a/2}X^{a+\epsilon}|T|^{3/2(1-a)}.$$

Combining equations (4.2.16), (4.2.15), (4.2.11) and (4.2.3) shows equation (4.1.5).

Now we address the case of $\zeta_K(s)/\zeta(s)$. We no longer have sub-convexity estimates, and must resort to the standard convexity estimate. We note that $\zeta_K(s)/\zeta(s)$ is entire. We find upper bounds for $\zeta_K(s)/\zeta(s)$ by using the Phragmén Lindelöf principle and the functional equation as stated in equation (3.2.2). Hence we have

$$\begin{aligned}\int_{C_2} \frac{\zeta_K(s)}{\zeta(s)}\frac{X^s}{s}ds \ll& \int_a^{1+\delta} |d_{M/\mathbb{Q}}|^{1/2-\sigma/2}T^{3/2-3/2\sigma}\frac{X^{\sigma+iT}}{T}d\sigma \\ \ll& |d_{M/\mathbb{Q}}|^{1/2}T^{1/2}\int_a^{1+\delta}\left(\frac{X}{T^{3/2}|d_{M/\mathbb{Q}}|^{1/2}}\right)^{\sigma}d\sigma \\ \ll& \frac{X^{1+\delta}}{T} + \frac{X^a|d_{M/\mathbb{Q}}|^{1/2-a/2}}{T^{3a/2-1/2}}.\end{aligned} \tag{4.2.17}$$

Similarly whilst integrating over C_3 we have

$$\begin{aligned}\int_{C_3} \frac{\zeta_K(s)}{\zeta(s)}\frac{X^s}{s}ds \ll& \int_{-T}^{T} |d_{M/\mathbb{Q}}|^{1/2-a/2}|t|^{3/2(1-a)}\frac{X^a}{t+\epsilon}dt \\ \ll& |d_{M/\mathbb{Q}}|^{1/2-a/2}X^a\int_{-T}^{T}|t|^{3/2(1-a)}\frac{1}{t+\epsilon}dt \\ \ll& |d_{M/\mathbb{Q}}|^{1/2-a/2}X^a|T|^{3/2(1-a)}.\end{aligned} \tag{4.2.18}$$

Gathering (4.2.4) and the two bounds above implies the bound in equation (4.1.19).

Now we explore the consequences of assuming better subconvexity bounds. Under the assumption of the Lindelöf Hypothesis (Conjecture 3.2.3), we may set $a = 1/2$ and we have that

$$\int_{C_2+C_3+C_4} \zeta_M(s)\frac{X^s}{s}ds \ll X^{1/2+\epsilon}T^{\epsilon} + \frac{X^{1+\epsilon}}{T^{1+\epsilon}}|d_{M/\mathbb{Q}}|^{\epsilon}.$$

Similarly, under the Lindelöf Hypothesis, with $a = 1/2$ we have

$$\int_{C_2+C_3+C_4} \frac{\zeta_K(s)}{\zeta(s)}\frac{X^s}{s}ds \ll X^{1/2+\epsilon}T^{\epsilon} + \frac{X^{1+\epsilon}}{T^{1+\epsilon}}|d_{M/\mathbb{Q}}|^{\epsilon}.$$

Hence for $a \in [1/2, 1)$, we have

$$\sum_{m \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}n^{-1}} h_M(m) = \mathrm{res}_{s=1}\zeta_M(s)\frac{(X/n^2)^{1/2}}{|d_{M/\mathbb{Q}}|} + O\left(\frac{(X/n^2)^{1/2+\epsilon}}{T|d_{M/\mathbb{Q}}|^{1+\epsilon}} + \left(\frac{X^{1/2}}{|d_{M/\mathbb{Q}}|n}\right)^{1/2+\epsilon} T^{\epsilon}\right)$$

and

$$\sum_{m \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}n^{-1}} h_{M,K}(m) \ll \frac{(X/n^2)^{1/2+\epsilon}}{T|d_{M/\mathbb{Q}}|^{1+\epsilon}} + \left(\frac{X^{1/2}}{|d_{M/\mathbb{Q}}|n}\right)^{1/2+\epsilon} T^{\epsilon}.$$

We will get the same main term $CX^{1/2}$ as in (4.1.11). We set B to be the smallest known constant such that $|\mathrm{Cl}_M[2]| \ll_\epsilon |d_{M/\mathbb{Q}}|^{B+\epsilon}$. As in the previous section observe that that $\sum_{n \leq X} g_M(n)n^{-1/2-\epsilon} \ll X^{\epsilon}$, $\sum_{n \leq X} g_{M,K}(n)n^{-1/2-\epsilon} \ll 1$ and that

$$\sum_{\substack{M/\mathbb{Q} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3 \\ |d_{M/\mathbb{Q}}|<X}} |d_{M/\mathbb{Q}}|^{-1/2-\epsilon} \ll 1,$$

$$\sum_{\substack{M/\mathbb{Q} \\ \mathrm{Gal}(M/\mathbb{Q})=C_3 \\ |d_{M/\mathbb{Q}}|<X^{1/2}}} |\mathrm{Cl}_M[2]||d_{M/\mathbb{Q}}|^{-1/2-\epsilon} \ll X^{B/2}.$$

Using these observations, we note that

$$\sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} g_M(n) \sum_{m \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}n^{-1}} h_M(m) \ll \sum_{m \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} h_M(m)$$

and

$$\sum_{n \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} g_{M,K}(n) \sum_{m \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}n^{-1}} h_{M,K}(m) \ll \sum_{m \leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} h_{M,K}(m).$$

By letting $T = X^{1/4+\epsilon}/|d_{M/\mathbb{Q}}|^{1/2}$ we see that $T \geq 1$ for all M that we are concerned with. Now note that under the assumption for the size of T and the Lindelöf hypothesis, we have

$$\sum_{\substack{M/\mathbb{Q}\\ |d_{M/\mathbb{Q}}|\leq X^{1/2}\\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{K\in\mathcal{L}(M)} \sum_{n\leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} f_{M,K}(n) \ll \sum_{\substack{M/\mathbb{Q}\\ |d_{M/\mathbb{Q}}|\leq X^{1/2}\\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{K\in\mathcal{L}(M)} \sum_{n\leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} h_{M,K}(n)$$

$$\ll \sum_{\substack{M/\mathbb{Q}\\ |d_{M/\mathbb{Q}}|\leq X^{1/2}\\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{K\in\mathcal{L}(M)} \frac{X^{1/4+\epsilon}}{|d_{M/\mathbb{Q}}|^{1/2+\epsilon}}$$

$$\ll X^{1/4+\epsilon} \sum_{\substack{M/\mathbb{Q}\\ \mathrm{Gal}(M/\mathbb{Q})=C_3\\ |d_{M/\mathbb{Q}}|<X^{1/2}}} |\mathrm{Cl}_M[2]||d_{M/\mathbb{Q}}|^{-1/2-\epsilon} \ll X^{1/4+B/2+\epsilon}.$$

After going through similar calculations for

$$\sum_{\substack{M/\mathbb{Q}\\ |d_{M/\mathbb{Q}}|\leq X^{1/2}\\ \mathrm{Gal}(M/\mathbb{Q})=C_3}} \sum_{n\leq X^{1/2}|d_{M/\mathbb{Q}}|^{-1}} f_M(n)$$

we see that

$$N_6(\mathbb{Q}, A_4; X) = CX^{1/2} + O(X^{B/2+1/4+\epsilon}).$$

Under the assumption of the Lindelöf Hypothesis and the assumption that

$$|\mathrm{Cl}_M[2]| \ll |d_{M/\mathbb{Q}}|^{\epsilon}$$

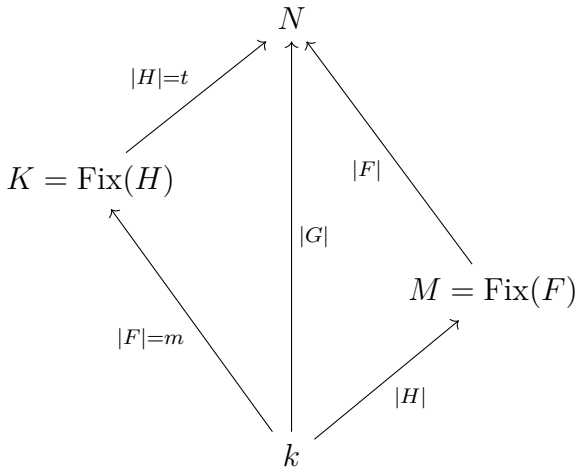
we have

$$N_6(\mathbb{Q}, A_4; X) = CX^{1/2} + O(X^{0.25}).$$

Chapter 5

Counting number fields with Frobenius Galois group

We will use the same notation we set up in Notation 2.1.5. Recall that N/k is a Galois extension with Galois group $G \in \mathcal{F}_1$. The group $G = F \rtimes H$ and the fixed field of F is M, the fixed field of H is K. In our case, F is always abelian. The field diagram of interest is:



(5.0.1)

We outline the main ideas behind obtaining an upper bound for $N_{mt}(k, G; X)$ for $G \in \mathcal{F}_1$.

- With the notation above, we fix a base field k and exploit the discriminant relation $d_{N/k} = d_{M/k}^m N_{M/k}(d_{N/M})$.
- For each fixed M/k, we count the number of abelian extensions N/M of degree m with the discriminant $d_{N/M}$ having a certain fixed support. To count $N_{mt}(k, G; X)$, we sum over all M/k and the corresponding possible supports of

$d_{N/M}$. Precisely, $N_{mt}(k, G; X)$ is bounded above by

$$N_{mt}(k, G; X) \leq \sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k}) \leq X^{1/m} \\ [M:k]=t, \mathrm{Gal}(M/k)=H}} N_m\left(M, F; \frac{X}{\mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^m}\right)$$

- Show that the number of distinct integer values $\mathcal{N}_{M/\mathbb{Q}}(d_{N/M}) \leq X$ above can take is $O(X^{1/R(G)})$ for some function R that depends only on G. This is made precise in Lemma 5.0.3.

Obtaining upper bounds for $N_m(k, G; X)$ for groups in $\mathcal{F}$ is done in the same manner as above, however we use another discriminant relation. In particular, the Frobenius extension K/k need not have any subfields so a discriminant relation that depends on subfields may not have been applicable. Instead, we use a Brauer relation, that connects $d_{K/k}$ with $d_{M/k}$ and $d_{N/M}$.

Theorem 5.0.1. (Fieker and Klüners (2003), Theorem 4) *Fix an algebraic number field k. Let $G = F \rtimes H$ be any Frobenius group. Let N/k be a normal extension with $\mathrm{Gal}(N/k) = G$. Let K be the fixed field of H and M be the fixed field of F. Then*

$$d_{K/k} = d_{M/k}^{(|F|-1)/|H|} \mathcal{N}_{M/k}(d_{N/M})^{1/|H|}. \tag{5.0.2}$$

Using these discriminant relations, we have the following equations. For $G \in \mathcal{F}_1$,

$$N_{mt}(k, G; X) = \sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k}) \leq X^{1/m} \\ \mathrm{Gal}(M/k)=H}} \sum_{\substack{N/M \\ [N:M]=m, \\ \mathcal{N}_{M/\mathbb{Q}}(d_{N/M}) \leq X \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{-m} \\ \mathrm{Gal}(N/M)=F,\ \mathrm{Gal}(N/k)=G}} 1. \tag{5.0.3}$$

Similarly for $G \in \mathcal{F}$, using (5.0.2) we have

$$N_m(k, G; X) = \sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k}) \leq X^{t/(m-1)} \\ \mathrm{Gal}(M/k)=H}} \sum_{\substack{N/M \\ [N:M]=m, \\ \mathcal{N}_{M/\mathbb{Q}}(d_{N/M}) \leq X^t \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{-(m-1)}, \\ \mathrm{Gal}(N/M)=F,\ \mathrm{Gal}(N/k)=G}} 1. \tag{5.0.4}$$

To compute the inner sum we fix M/k as ask how many abelian extensions N/M exist with a certain finite support. We have the following results and we present a proof in the next section.

Lemma 5.0.2. *Let M/k be a finite extension. Let P be a finite set of primes in $\mathcal{O}_M$. The number of abelian extensions N/M with $\mathrm{Gal}(N/k) = G$ of degree m which are at most ramified in P is bounded above by*

$$O_{G,k,\epsilon}\left(C^{|P|}\mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\mathcal{D}+\epsilon}\right).$$

Here,

$$\mathcal{D} = \mathcal{D}(k, H, m) := \limsup_{d_{M/\mathbb{Q}}} \frac{\log(|\mathrm{Cl}_M[m]|)}{\log(|d_{M/\mathbb{Q}}|)}. \tag{5.0.5}$$

This Lemma gives an upper bound for the number of abelian extensions N/M with fixed degree m and with a fixed support for $d_{N/M}$. Adding this number of abelian extensions over all possible supports for discriminant less than X gives us an upper bound for $N_m(M, F; X)$. The Lemma below counts the number of degree m abelian extensions of M with discriminant at most X.

Lemma 5.0.3. *Fix a tower of number fields $M/k/\mathbb{Q}$. Fix $F \rtimes H = G \in \mathcal{F}_1$. Let M/k be a Galois extension with Galois group H. For any integer s such that $s|m$ and $s > 1$ we define the set*

$$A(G, M, k, s, X) = \left\{ L/M : \begin{array}{c} [L : M] = s,\ L/M \text{ is abelian} \\ \mathrm{Gal}(\hat{L}/k) = G,\ \mathcal{N}_{M/\mathbb{Q}}(d_{L/M}) \leq X \end{array} \right\}.$$

Then we have

$$A(G, M, k, s, X) \ll_{G,\epsilon,k} C^{\omega(\mathcal{N}_{k/\mathbb{Q}}(d_{M/k}))}\mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\mathcal{D}+\epsilon}X^{1/R+\epsilon} \tag{5.0.6}$$

where $R = mt(1 - p^{-1})$ when $s = m$ and $R = p - 1$ otherwise. Here p is the smallest prime divisor of m.

We first bound (5.0.4). Here, we do not use that the Galois group of N/M is F, so we drop that condition from the subscript. By Lemma 5.0.3 we have

$$\sum_{\substack{N/M \\ [N:M]=m,\ \mathrm{Gal}(N/k)=G \\ \mathcal{N}_{M/\mathbb{Q}}(d_{N/M})\leq X^t \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{-(m-1)}}} 1 \ll X^{\frac{1}{m(1-p^{-1})}+\epsilon} \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\mathcal{D}-\frac{m-1}{mt(1-p^{-1})}+\epsilon} C^{\omega(\mathcal{N}_{k/\mathbb{Q}}(d_{M/k}))}.$$

Note that by a result of Robin (1983), $\omega(n) \leq 2\log(n)/\log\log(n)$ for $n \geq 3$. By the upper bound on $\omega(n)$ and the observation that $\mathcal{N}_{k/\mathbb{Q}}(d_{M/k}) \leq X^{t/(m-1)}$, we have that

$$\mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\epsilon} C^{\omega(\mathcal{N}_{k/\mathbb{Q}}(d_{M/k}))} \ll_{k,m,t} X^{\epsilon}.$$

This implies that

$$N_m(k,G;X) \ll X^{\frac{p}{m(p-1)}+\epsilon} \sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})\leq X^{t/(m-1)} \\ \mathrm{Gal}(M/k)=H}} \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\mathcal{D}-\frac{m-1}{mt(1-p^{-1})}}. \tag{5.0.7}$$

By assumption we have

$$\sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})\leq Y \\ \mathrm{Gal}(M/k)=H}} 1 = N_t(k,H;Y) \ll Y^{a_1(H,t)+\epsilon}. \tag{5.0.8}$$

Consequently, by Abel summation, (5.0.7) is bounded above by

$$\begin{aligned} N_m(k,G;X) &\ll X^{\frac{p}{m(p-1)}} \left(X^{\frac{t}{m-1}\left(a_1(H,t)+\mathcal{D}-\frac{m-1}{mt(1-p^{-1})}\right)} + O(1) \right) \\ &\ll X^{\frac{p}{m(p-1)}+\epsilon} + X^{\frac{t(a_1(H,t)+\mathcal{D})}{m-1}+\epsilon}. \end{aligned} \tag{5.0.9}$$

From (5.0.3) we now obtain the upper bound for $N_{mt}(k,G;X)$ in similar fashion.

$$\begin{aligned} N_{mt}(k,G;X) &\ll X^{\frac{p}{mt(p-1)}+\epsilon} \sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})\leq X^{1/m} \\ \mathrm{Gal}(M/k)=H}} \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\mathcal{D}-\frac{p}{t(p-1)}} \\ &\ll X^{\frac{p}{mt(p-1)}+\epsilon} \left(X^{\frac{1}{m}\left(a_1(H,t)+\mathcal{D}-\frac{p}{t(p-1)}\right)} + O(1) \right) \\ &\ll X^{\frac{p}{mt(p-1)}+\epsilon} + X^{\frac{a_1(H,t)+\mathcal{D}}{m}+\epsilon}. \end{aligned} \tag{5.0.10}$$

This proves Theorem 2.1.6.

Assuming Malle's conjecture for $N_t(k, H; X)$ and the ℓ-torsion conjecture, equation (5.0.10) implies that

$$\begin{aligned} N_{mt}(k, G; X) &\ll X^{\frac{p}{mt(p-1)}+\epsilon}\left(X^{\frac{1}{m}\left(a(H,t)-\frac{p}{t(p-1)}\right)}+O(1)\right) \\ &\ll X^{\frac{a(F,m)}{t}+\epsilon}+X^{\frac{a(H,t)}{m}+\epsilon}. \end{aligned}$$

This follows from the fact that F is an abelian group hence $a(F, m) = (m(1-p^{-1}))^{-1}$. In case of $G = F \times H$, this is exactly as predicted by Malle's conjecture (See Lemma 4.1 of Malle (2002)). If G is not a direct product, but H is abelian, then this also implies Malle's conjecture.

Remark 5.0.4. In equation (5.0.9), we can make use of Abel summation differently if we have information about

$$\sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})\leq X \\ \mathrm{Gal}(M/k)=H}} |\mathrm{Cl}_M[m]|.$$

We may use this information in place of equation (5.0.8) in equation (5.0.7). Using this information allows us to bypass the need for a point-wise bound on the m torsion of the class group. We use this in an application in the section 6.2.

5.1 Proof of lemmas

Here we prove the lemmas in the previous section.

Lemma 5.1.1. *Let M/k be a finite extension. Let P be a finite set of primes in $\mathcal{O}_M$. The number of abelian extensions N/M with $\mathrm{Gal}(N/k) = G$ of degree m which are at most ramified in P is bounded above by*

$$O_{G,k,\epsilon}\left(C^{|P|}\mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\mathcal{D}+\epsilon}\right).$$

Proof. Define a modulus $\mathfrak{m}$ as $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ such that $\mathfrak{m}_0$ is a product of primes in P and $\mathfrak{m}_\infty$ consists of the real places of M. A modulus $\mathfrak{m}$ has the form

$$\mathfrak{m} = \prod_{\substack{\mathfrak{p} \\ \mathfrak{p}\in P}} \mathfrak{p}^{e_\mathfrak{p}} \prod_{\substack{\nu \\ \nu|\mathfrak{m}_\infty}} \nu.$$

Every abelian extension N/M admits a modulus $\mathfrak{m}$ such that N/M is not ramified outside of $\mathfrak{m}$. Call a modulus $\mathfrak{f}(N/M)$, the conductor if it is the smallest modulus such that the Artin map factors through the ray class field of $\mathfrak{f}(N/M)$. The abelian extensions of M that admit a modulus $\mathfrak{m}$ such that $\mathfrak{f}(N/M)|\mathfrak{m}$ are in bijection with the subfields of the ray class field associated to $\mathfrak{f}(N/M)$. The subfields N/M of degree m of the ray class field of $\mathfrak{f}(N/M)$ are in bijection with subgroups of index m of the ray class group $\mathrm{Cl}_M(\mathfrak{f}(N/M))$ (Chapter 5, Corollary 3.7, Milne 1997). To count the subgroups of the ray class group we use the following exact sequence for ray class groups (Chapter 5, Theorem 1.7, Milne 1997),

$$\mathcal{O}_M^\times \to (\mathcal{O}_M/\mathfrak{m})^\times \to \mathrm{Cl}_M(\mathfrak{m}) \to \mathrm{Cl}_M \to 1.$$

Thus we compute the m-torsion of the ray class group $\mathrm{Cl}_M(\mathfrak{m})$ where $\mathfrak{m} = \mathfrak{f}(N/M)$. By the exact sequence above,

$$|\mathrm{Cl}_M(\mathfrak{m})[m]| \leq |(\mathcal{O}_M/\mathfrak{m})^\times[m]| \times |\mathrm{Cl}_M[m]|.$$

By the Chinese remainder theorem, with M_ν denoting the completion of M with respect to the norm ν, we have

$$(\mathcal{O}_M/\mathfrak{m})^\times = (\mathcal{O}_M/\mathfrak{m}_0)^\times \oplus (\mathcal{O}_M/\mathfrak{m}_\infty)^\times = \prod_{\mathfrak{p}\in P} (\mathcal{O}_M/\mathfrak{p}^{e_\mathfrak{p}})^\times \oplus \prod_{\nu|\mathfrak{m}_\infty} M_\nu^\times/M_\nu^+.$$

Hence we have that $|(\mathcal{O}_M/\mathfrak{m}_0)^\times[m]|$ is bounded above by $(2m)^{[M:\mathbb{Q}]|P|}$. There are at most $[M:\mathbb{Q}]$ distinct real places, hence the contribution to the $|(\mathcal{O}_M/\mathfrak{m})^\times[m]|$ from the real places is bounded above by $2^{[M:\mathbb{Q}]}$. Hence, by choosing $C \geq (2m)^{[M:\mathbb{Q}]}$,

$$|(\mathcal{O}_M/\mathfrak{m})^\times[m]| \leq C^{|P|}.$$

By (2.1.2),

$$|\mathrm{Cl}_M[m]| \ll d_{M/\mathbb{Q}}^{\mathcal{D}+\epsilon} \ll (d_{k/\mathbb{Q}}^t \mathcal{N}_{k/\mathbb{Q}}(d_{M/k}))^{\mathcal{D}+\epsilon} \ll_k \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\mathcal{D}+\epsilon}.$$

By combining the pieces above, we have that the number of abelian extensions of degree m with discriminant supported on $\mathfrak{m}$ is bounded above by

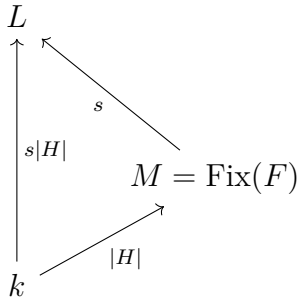
$$C^{|P|}O_k(|\mathrm{Cl}_M[m]) \ll_{G,k,\epsilon} C^{|P|}\mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\mathcal{D}+\epsilon} \tag{5.1.1}$$

□

Notation 5.1.2. Let $N/M/k$ be a tower of number fields. Let $P_{N/M}(\mathcal{O}_k)$ denote the set of primes in k that divide $\mathcal{N}_{M/k}(d_{N/M})$. Let p be a prime in $\mathbb{Z}$ and let $x \in \mathbb{Z}$. Let $\nu_p(x)$ be the non negative integer such that $p^{\nu_p(x)}|x$ and $p^{\nu_p(x)+1} \nmid x$.

Now we prove Lemma 5.0.3.

Proof. The tower of fields $L/M/k$ may be represented as follows.



Note that if $s = m$ then L/k is a Galois extension. Let ℓ denote a prime in $\mathbb{Z}$. Note that $|P_{L/M}(\mathbb{Z})| = O_{k,G}(|P_{L/M}(\mathcal{O}_M)|)$. Fix a set of primes $\mathcal{P}$ in $\mathbb{Z}$ and let $P_{L/M}(\mathbb{Z}) \subseteq \mathcal{P}$. By Lemma 5.0.2 we have

$$\sum_{\substack{L/M \\ [L:M]=s,\ L/M \text{ is abelian} \\ \ell|\mathcal{N}_{M/\mathbb{Q}}(d_{L/M})\Rightarrow \ell\in P_{L/M}(\mathbb{Z})}} 1 \ll_{G,\epsilon,k} |\mathrm{Cl}_M[s]|C^{|P_{L/M}(\mathbb{Z})|}.$$

Now we relax the condition that $P_{L/M}(\mathbb{Z})$ is fixed and consider all extensions with $\mathcal{N}_{M/\mathbb{Q}}(d_{L/M}) \leq X$. We define $\mathbb{P}_M(X)$ as

$$\mathbb{P}_M(X) := \{P_{L/M}(\mathbb{Z}) : [L:M] = s, L/M \text{ is abelian}, \mathcal{N}_{M/\mathbb{Q}}(d_{L/M}) \leq X\}.$$

Hence we have

$$\sum_{\substack{L/M \\ [L:M]=s,\ L/M \text{ is abelian} \\ \mathrm{Gal}(\widehat{L}/M)=F,\ \mathrm{Gal}(\widehat{L}/k)=G \\ \mathcal{N}_{M/\mathbb{Q}}(d_{L/M})\leq X}} 1 \ll |\mathrm{Cl}_M[s]| \sum_{P_{L/M}(\mathbb{Z})\in\mathbb{P}_M(X)} C^{|P_{L/M}(\mathbb{Z})|}. \tag{5.1.2}$$

We split each $P_{L/M}(\mathbb{Z})$ into the union of two disjoint sets, $P_{L/M}(\mathbb{Z}) = U_{L/M}(\mathbb{Z}) \cup V_{L/M}(\mathbb{Z})$ such that

- Every $\ell \in U_{L/M}(\mathbb{Z})$ is such that ℓ is tamely ramified in $L/\mathbb{Q}$ and $\ell \nmid d_{M/\mathbb{Q}}$.
- Every $\ell \in V_{L/M}(\mathbb{Z})$ is such that $\ell | d_{M/\mathbb{Q}}[k:\mathbb{Q}]mt$.

Let $\mathbb{U}_M(X) = \{U_{L/M}(\mathbb{Z}) : U_{L/M}(\mathbb{Z}) \subseteq P_{L/M}(\mathbb{Z}) \text{ and } P_{L/M}(\mathbb{Z}) \in \mathbb{P}_M(X)\}$ and $\mathbb{V}_M(X) = \{V_{L/M}(\mathbb{Z}) : V_{L/M}(\mathbb{Z}) \subseteq P_{L/M}(\mathbb{Z}) \text{ and } P_{L/M}(\mathbb{Z}) \in \mathbb{P}_M(X)\}$.

This implies that

$$\sum_{P_{L/M}(\mathbb{Z})\in\mathbb{P}_M(X)} C^{|P_{L/M}(\mathbb{Z})|} \ll \sum_{U_{L/M}(\mathbb{Z})\in\mathbb{U}_M(X)} C^{|U_{L/M}(\mathbb{Z})|} \sum_{V_{L/M}(\mathbb{Z})\in\mathbb{V}_M(X)} C^{|V_{L/M}(\mathbb{Z})|}. \tag{5.1.3}$$

As $d_{M/\mathbb{Q}}[k:\mathbb{Q}]mt$ is fixed,

$$\sum_{V_{L/M}(\mathbb{Z})\in\mathbb{V}_M(X)} C^{|V_{L/M}(\mathbb{Z})|} \leq \sum_{d|d_{M/\mathbb{Q}}[k:\mathbb{Q}]mt} \mu^2(d)C^{\omega(d)} = (C+1)^{\omega(d_{M/\mathbb{Q}}[k:\mathbb{Q}]mt)} \ll_{k,G} C_1^{\omega(d_{M/\mathbb{Q}})}. \tag{5.1.4}$$

Using that discriminants are non zero integers and that $d_{M/\mathbb{Q}} = d_{k/\mathbb{Q}}^t \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})$, we have

$$C_1^{\omega(d_{M/\mathbb{Q}})} \leq C_1^{\omega(d_{k/\mathbb{Q}})} C_1^{\omega(\mathcal{N}_{k/\mathbb{Q}}(d_{M/k}))}.$$

For a prime $\ell \in U_{L/M}(\mathbb{Z})$, since ℓ is tamely ramified, we have

$$\ell\mathcal{O}_L = \prod_{i=1}^{g_\ell(L/\mathbb{Q})} \mathfrak{P}_i^{e(\mathfrak{P}_i,\ell)} \qquad \nu_\ell(\mathcal{N}_{M/\mathbb{Q}}(d_{L/M})) = \sum_{i=1}^{g_\ell(L/\mathbb{Q})} f(\mathfrak{P}_i,\ell)(e(\mathfrak{P}_i,\ell)-1)$$

where $e(\mathfrak{P}_i,\ell)$ and $f(\mathfrak{P}_i,\ell)$ are the respective ramification degrees and inertia degrees. Consider first the case that L/k is a Galois extension. In this case $m = [L:M]$ and

$\nu_\ell(\mathcal{N}_{M/\mathbb{Q}}(d_{L/M})) \geq |G|(1-p^{-1})$ where p is the smallest prime divisor of m. Hence we have

$$\sum_{U_{L/M}(\mathbb{Z})\in\mathbb{U}_M(X)} C^{|U_{L/M}(\mathbb{Z})|} \ll \sum_{n^{|G|(1-p^{-1})}\leq X} \mu^2(n)C^{\omega(n)} \ll_{k,G} X^{\frac{1}{|G|(1-p^{-1})}+\epsilon}. \tag{5.1.5}$$

If L/k is not a Galois extension, then the smallest any $e(\mathfrak{P}_i,\ell) > 1$ can be is p where p is the smallest prime divisor of $|F|$. By combining (5.1.2), (5.1.4) and (5.1.5), we get

$$\begin{aligned} A(G,M,k,m,X) &\ll_{G,\epsilon,k} C^{\omega(\mathcal{N}_{k/\mathbb{Q}}(d_{M/k}))}|\mathrm{Cl}_M[m]|X^{\frac{1}{|G|(1-p^{-1})}+\epsilon} \\ A(G,M,k,s,X) &\ll_{G,\epsilon,k} C^{\omega(\mathcal{N}_{k/\mathbb{Q}}(d_{M/k}))}|\mathrm{Cl}_M[s]|X^{\frac{1}{p-1}+\epsilon}. \end{aligned} \tag{5.1.6}$$

Now using

$$|\mathrm{Cl}_M[s]| \ll \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\mathcal{D}+\epsilon}$$

we have the statement of the theorem.

□

Chapter 6

Extensions

In this chapter, we explore extensions to work done here. One of the objective is to given an indication of how to prove the examples in Example 2.1.9. The section has two parts. The first part addresses the flexibility of the method of proof as we may use it to count subfields of various degrees. In particular we establish results such as $N_6(\mathbb{Q}, S_4; X) \ll X^{1/2+\epsilon}$. It is noteworthy since the extension is not a Frobenius extension, nor is it a Galois extension. The method of proof shows the effect of further ramification information. We also make use of average results of the two torsion of the class group of cubic fields here as opposed to point-wise bounds.

The next part addresses the occasions in which we can say something non-trivial about the size of the m-torsion of the class group. In particular we show how we to use results such as that of Frei and Widmer. They establish a point-wise upper bound on the size of the ℓ torsion of the class group of 100% of number fields in a certain family of number fields. Such results suffice to prove $N_m(k, D_m; X) \ll X^{3/(m-1)-\frac{2}{m-1}\min(\frac{1}{2m}, \frac{1}{2[k:\mathbb{Q}]})+\epsilon}$.

6.1 Sub-fields

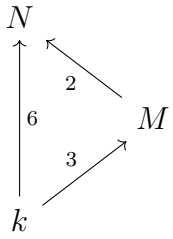
In this section we obtain upper bounds for certain sextic extensions of a number field. In the cases of certain groups, we achieve the results conjectured by Malle. In particular we show Malle's conjecture for $N_6(\mathbb{Q}, C_3^2 \rtimes C_4; X)$, $N_6(\mathbb{Q}, S_4; X)$ and $N_6(k, A_4; X)$. The proof for $N_6(k, A_4; X) \ll X^{1/2+\epsilon}$ is independent of the method in chapter 3. In terms of MAGMA notation, we obtain upper bounds for $N_6(\mathbb{Q}, 6T10; X)$,

$N_6(\mathbb{Q}, 6T7; X)$ and $N_6(k, 6T4; X)$. The method used to obtain these bounds is an extension of the method used to prove Theorem 2.1.6, and can be used to bound $N_d(k, G; X)$ for various d that depend on G. This section also shows how we can make use of average results on the size of the ℓ torsion of the class group to count families of number fields.

Proposition 6.1.1. *The number of degree* 6 *extensions* N/k *with a cubic subfield* M/k *and fixed Galois group* G *satisfies the following*

$$N_6(k, G; X) \ll X^{1+\epsilon}. \tag{6.1.1}$$

Proof. Note that every quadratic extension is an abelian extension. We have the following field diagram:



Note that $d_{N/k} = \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^2 \mathcal{N}_{M/\mathbb{Q}}(d_{N/M})$. Let the Galois group of $\hat{M}/k$ be H. H can be C_3 or S_3 and we treat the cases separately. Hence we have

$$N_6(k, G; X) \leq \sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k}) \leq X^{1/2} \\ \mathrm{Gal}(M/k)=H}} \sum_{\substack{N/M \\ [N:M]=2 \\ \mathrm{Gal}(\hat{N}/k)=G \\ \mathcal{N}_{M/\mathbb{Q}}(d_{N/M}) \leq X d_{M/\mathbb{Q}}^{-2}}} 1. \tag{6.1.2}$$

We do not know if $|G| = 6$ or not, hence for a prime ℓ that divides $\mathcal{N}_{M/\mathbb{Q}}(d_{N/M})$, we cannot say that $v_\ell(\mathcal{N}_{M/\mathbb{Q}}(d_{N/M})) > 1$. Now by Lemma 5.0.2 and Lemma 5.0.3, we have that

$$N_6(k, G; X) \ll \sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k}) \leq X^{1/2} \\ \mathrm{Gal}(M/k)=H}} \frac{X^{1+\epsilon}}{d_{M/k}^2} \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\mathcal{D}}.$$

Recall a result of Datskovsky and Wright (1988) that states $N_3(k, H; X) \ll_k X$ and recall that as indicated by the definition in (2.1.2), $|\mathrm{Cl}_M[2]| \ll_{k,\epsilon} \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\mathcal{D}}$.

The Minkowski bound implies $|\mathrm{Cl}_M[2]| \ll_{k,\epsilon} \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{1/2+\epsilon}$. Using this and partial summation, we have

$$N_6(k, G; X) \ll_{k,\epsilon} X^{1+\epsilon}\left((X^{1/2})^{1-2+\mathcal{D}} + O(1)\right) \ll_{k,\epsilon} X^{1+\epsilon}.$$

This shows the claim of the proposition. With this in mind, in certain cases we can do better. In particular, a result of Klüners gives us more ramification information.

Lemma 6.1.2. *[Klüners (2012), Lemma 4] Let $N/M/k$ be extensions of number fields with $\mathrm{Gal}(M/k) = H$ and $[N : M] = 2$. Assume there exists a prime $p \in \mathbb{Z}$ which is unramified in M with $p||\mathcal{N}_{M/\mathbb{Q}}(d_{N/M})$. Then $\mathrm{Gal}(\hat{N}/k) = C_2 \wr H$.*

We can use this information as follows. We assume that $G \neq C_2 \wr H$. This implies that for each prime ℓ that is unramified in M and divides $\mathcal{N}_{M/\mathbb{Q}}(d_{N/M})$, we have $v_\ell(\mathcal{N}_{M/\mathbb{Q}}(d_{N/M})) \geq 2$. Using that $\mathcal{N}_{M/\mathbb{Q}}(d_{N/M})$ is generally a square, we get more information when evaluating the inner sum in (6.1.2), which results in

$$\begin{aligned} N_6(k, G; X) &\ll_{k,\epsilon} \sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k}) \leq X^{1/2} \\ \mathrm{Gal}(M/k)=H}} \frac{X^{1/2+\epsilon}}{d_{M/k}} \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\mathcal{D}} \\ &\ll_{k,\epsilon} X^{1/2+\epsilon}\left((X^{1/2})^{a_1(H,3)-1+\mathcal{D}} + O(1)\right) \end{aligned} \tag{6.1.3}$$

where $a_1(H, 3)$ is the best known constant such that $N_3(k, H; X) \ll X^{a_1(H,3)+\epsilon}$. This implies that if $G \neq C_2 \wr H$ then $N_6(k, G; X) \ll X^{3/4+\epsilon}$. We can do better if we know more about $a_1(H, 3)$. In the case that $H = C_3$ and $G \neq C_2 \wr C_3$, using $N_3(k, C_3; X) \ll X^{1/2}$ we have (6.1.3) as

$$N_6(k, G; X) \ll_{k,\epsilon} X^{1/2+\epsilon}\left((X^{1/2})^{1/2-1+\mathcal{D}} + O(1)\right) \ll_{k,\epsilon} X^{1/2+\epsilon}. \tag{6.1.4}$$

This implies results such as $N_6(k, A_4; X) \ll X^{1/2+\epsilon}$. Note this is a partial generalization of the results in chapter 3 in the sense that it holds for any base field. If we do not have that $H = C_3$, but we have that $k = \mathbb{Q}$ then we may make use of a result

about the average size of the two torsion of cubic fields. In particular, as implied by equation (5.1.6) and (6.1.2), we see that when $G \neq C_2 \wr H$,

$$N_d(k, G; X) \ll_{k,\epsilon} \sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k}) \leq X^{1/2} \\ \mathrm{Gal}(M/k)=S_3}} \frac{X^{1/2+\epsilon}}{d_{M/k}} |\mathrm{Cl}_M[2]|.$$

In Bhargava (2005), Bhargava shows

$$\sum_{\substack{M/\mathbb{Q} \\ [M:\mathbb{Q}]=3 \\ |d_{M/\mathbb{Q}}| \leq X}} |\mathrm{Cl}_M[2]| \ll X. \tag{6.1.5}$$

When $k = \mathbb{Q}$ we may use this in our partial summation to show that

$$N_6(\mathbb{Q}, G; X) \ll X^{1/2+\epsilon}$$

when $G \neq C_2 \wr H$ and $H = S_3$. This implies results such as $N_6(\mathbb{Q}, S_4; X) \ll X^{1/2+\epsilon}$.

□

6.2 Size of the class group

The best general upper bound for $\mathcal{D}$ is $1/2$, however we can do better in certain cases. For instance, in Example 2.1.9 the result $N_4(\mathbb{Q}, A_4; X) \ll X^{0.77+\epsilon}$ makes use of $|\mathrm{Cl}_M[2]| \ll_\epsilon |d_{M/\mathbb{Q}}^{0.2784\cdots+\epsilon}|$. We examine what kind of results towards to size of the torsion of the class group will be useful in this method. We look at works that show non trivial bounds for $|\mathrm{Cl}_M[\ell]|$ for 100% of the fields $M/\mathbb{Q}$ with prescribed Galois group H.

We describe the work in Frei and Widmer (2018a) here. In order to do this precisely, we establish some notation. Let $\mathcal{C}(k, n)$ be the set of Galois extensions M/k with Galois group C_n satisfying the following condition: every prime ideal of $\mathcal{O}_k$ that does not divide n is either unramified, or totally ramified in M. Consequently, this statement holds whenever $\mathrm{Gal}(M/k) = C_{p_1}$ where p_1 is a prime.

Theorem 6.2.1. [Frei and Widmer (2018a), Theorem 1.3] *Suppose k and $\mathbb{Q}(\mu_n(\hat{k}))$ are linearly disjoint over $\mathbb{Q}$. Let $\mathcal{C}(k,n;X)$ be the subset of field extensions M/k of $\mathcal{C}(k,n)$ with $|d_{M/\mathbb{Q}}| \leq X$. Let $\epsilon \to 0$. Define $\mathcal{C}_2(k,n;X) \subset \mathcal{C}(k,n;X)$ to be the set such that for all $M \in \mathcal{C}_2(k,n;X)$ we have that*

$$|\mathrm{Cl}_M[\ell]| \ll_{k,n,\ell,\epsilon} |d_{M/\mathbb{Q}}|^{1/2-\min(\frac{1}{2\ell(n-1)},\delta)+\epsilon}. \tag{6.2.1}$$

We call $\mathcal{C}_1(k,n;X) := \mathcal{C}(k,n;X) \setminus \mathcal{C}_2(k,n;X)$ the set of exceptional fields. We have that

$$|\mathcal{C}_1(k,n;X)| = O_{k,n,\epsilon}(X^{\frac{1}{n-1}-\min(\frac{1}{2\ell(n-1)},\delta)})$$

where the constant δ is defined as

$$\delta = \delta(n,k) = \begin{cases} \frac{1}{8\phi(n)(n-1)} & k = \mathbb{Q} \\ \frac{1}{2[k:\mathbb{Q}]\phi(n)(n-1)} & k \neq \mathbb{Q} \end{cases}$$

Remark 6.2.2. Any result that shows a power saving in the ℓ torsion of the class group and a zero density exceptional set can be used. In particular, any result that shows

$$|\mathrm{Cl}_M[\ell]| \ll_{k,n,\ell} |d_{M/\mathbb{Q}}|^{b(k,n,\ell)}$$

with $\lim_{X\to\infty} |\mathcal{C}_1(k,n;X)|/|\mathcal{C}(k,n;X)| < X^{-\epsilon}$ can be applied to our method. At the same time as this result was announced, Pierce, Turnage-Butterbaugh, and Wood (2017) announced results of a similar shape, however their results are only applicable to degree n extensions of $\mathbb{Q}$. They are able to show $|\mathrm{Cl}_M[\ell]| \ll_{n,\ell} |d_{M/\mathbb{Q}}|^{b(n,\ell)}$ with $b(n,\ell) < 1/2$ for extensions with Galois groups other than C_n with a set of exceptional fields is smaller then the set of exceptional fields in Theorem 6.2.1. We make use of this in Example 2.1.9 where we show that $N_{103}(\mathbb{Q}, C_{103} \rtimes C_{17}; X) \ll X^{0.09369+\epsilon}$ (as opposed to what we would get otherwise, ie, $\ll X^{0.09375+\epsilon}$).

An application of Theorem 6.2.1 is the second part of Proposition 2.1.8. In particular, we will now show that for $k \neq \mathbb{Q}$ and for any odd integer m,

$$N_m(k, D_m; X) \ll X^{\frac{3}{m-1}-\frac{2}{m-1}\min(\frac{1}{2m},\frac{1}{2[k:\mathbb{Q}]})+\epsilon} \qquad N_{2m}(k, D_{2m}; X) \ll X^{\frac{3}{2m}-\frac{1}{m}\min(\frac{1}{2m},\frac{1}{2[k:\mathbb{Q}]})+\epsilon}.$$

We now make precise how to use their results. Let $G = F \rtimes C_{p_1} \in \mathcal{F}$, where F is any abelian group with $|F| = m$. We find an upper bound for $N_m(k, G; X)$. Let $M = \mathrm{Fix}(F)$ and let k be our base field. We use the same notation as in Theorem 6.2.1.

From (5.0.7) we have that

$$\begin{aligned} N_m(k, F \rtimes C_{p_1}; X) \ll & X^{\frac{p}{m(p-1)}+\epsilon} \sum_{\substack{M/k \\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k}) \le X^{p_1/(m-1)} \\ \mathrm{Gal}(M/k)=C_{p_1}}} \frac{|\mathrm{Cl}_M[m]| C^{\omega(\mathcal{N}_{k/\mathbb{Q}}(d_{M/k}))}}{\mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\frac{m-1}{mp_1(1-p^{-1})}}} \\ \ll & X^{\frac{p}{m(p-1)}+\epsilon} \sum_{\substack{M \in \mathcal{C}_1(k,p_1;X^{p_1/(m-1)}|d_{k/\mathbb{Q}}^{-p_1}|) \\ \mathrm{Gal}(M/k)=C_{p_1}}} \frac{|\mathrm{Cl}_M[m]| C^{\omega(\mathcal{N}_{k/\mathbb{Q}}(d_{M/k}))}}{\mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\frac{m-1}{mp_1(1-p^{-1})}}} \\ & + X^{\frac{p}{m(p-1)}+\epsilon} \sum_{\substack{M \in \mathcal{C}_2(k,p_1;X^{p_1/(m-1)}|d_{k/\mathbb{Q}}^{-p_1}|) \\ \mathrm{Gal}(M/k)=C_{p_1}}} \frac{|\mathrm{Cl}_M[m]| C^{\omega(\mathcal{N}_{k/\mathbb{Q}}(d_{M/k}))}}{\mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\frac{m-1}{mp_1(1-p^{-1})}}} \end{aligned} \tag{6.2.2}$$

Using the fact that $N_{p_1}(k, C_{p_1}; X) \ll X^{1/(p_1-1)}$, partial summation and the result of Theorem 6.2.1, we have that the first series in (6.2.2) is

$$\begin{aligned} & \sum_{\substack{M/k \in \mathcal{C}_1(k,p_1;X^{p_1/(m-1)}|d_{k/\mathbb{Q}}^{-p_1}|) \\ \mathrm{Gal}(M/k)=C_{p_1}}} \frac{|\mathrm{Cl}_M[m]| C^{\omega(\mathcal{N}_{k/\mathbb{Q}}(d_{M/k}))}}{\mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\frac{m-1}{mp_1(1-p^{-1})}}} \\ & \qquad \ll_k \left(X^{p_1/(m-1)}\right)^{1/(p_1-1)-\min(\frac{1}{2m(p_1-1)},\delta)-\frac{m-1}{mp_1(1-p^{-1})}+1/2+\epsilon} + 1 \end{aligned}$$

where

$$\delta = \begin{cases} \frac{1}{8(p_1-1)^2} & k = \mathbb{Q} \\ \frac{1}{2[k:\mathbb{Q}](p_1-1)^2} & k \neq \mathbb{Q}. \end{cases}$$

Similarly, for the second term in (6.2.2)

$$\sum_{\substack{M/k\notin\mathcal{C}_2(k,p_1;X^{p_1/(m-1)}|d_{k/\mathbb{Q}}^{-p_1}|)\\ \mathcal{N}_{k/\mathbb{Q}}(d_{M/k})\leq X^{p_1/(m-1)}\\ \mathrm{Gal}(M/k)=C_{p_1}}} \frac{|\mathrm{Cl}_M[m]|C^{\omega(\mathcal{N}_{k/\mathbb{Q}}(d_{M/k}))}}{\mathcal{N}_{k/\mathbb{Q}}(d_{M/k})^{\frac{m-1}{mp_1(1-p^{-1})}}}$$

$$\ll \left(X^{p_1/(m-1)}\right)^{1/(p_1-1)-\min(\frac{1}{2m(p_1-1)},\delta)-\frac{m-1}{mp_1(1-p^{-1})}+1/2+\epsilon}+1.$$

Combining the above, we have that

$$N_m(k,F\rtimes C_{p_1};X)\ll X^{\frac{p_1}{(p_1-1)(m-1)}+\frac{p_1}{(m-1)}(\frac{1}{2}-\min(\frac{1}{2m(p_1-1)},\delta))+\epsilon}+X^{\frac{p}{m(p-1)}+\epsilon}. \tag{6.2.3}$$

A corollary of this is that $N_m(k,D_m;X)\ll X^{3/(m-1)-\frac{2}{m-1}\min(\frac{1}{2m},\frac{1}{2[k:\mathbb{Q}]})+\epsilon}+X^{\frac{2}{m}+\epsilon}$ as stated in (2.1.4). Doing the same procedure with (5.0.3) we get the result for $N_{2m}(k,D_m;X)$ in (2.1.4).

Bibliography

Alberts, B. (2018). "The Weak Form of Malle's Conjecture and Solvable Groups". In: URL: https://arxiv.org/pdf/1804.11318.pdf.

— (2019). "Statistics of the First Galois Cohomology Group: A Refinement of Malle's Conjecture". In: URL: https://arxiv.org/pdf/1907.06289.pdf.

Atkinson, F. (1941). "A divisor problem". In: *The Quarterly Journal of Mathematics* 1, pp. 193–200.

Baily, A. (1980). "On the density of discriminants of quartic fields". In: *Journal für die reine und angewandte Mathematik* 315, pp. 190–210.

Belabas, K., M. Bhargava, and C. Pomerance (2010). "Error estimates for the Davenport-Heilbronn theorems". In: *Duke Mathematical Journal* 153.1, pp. 173–210.

Bhargava, M. (2005). "The density of discriminants of quartic rings and fields". In: *Annals of Mathematics* 162.2, pp. 1031–1063.

— (2010). "The density of discriminants of quintic rings and fields". In: *Annals of Mathematics* 172.3, pp. 1559–1591.

Bhargava, M., A. Cojocaru, and F. Thorne. "The number of non S_5 quintic extensions of bounded discriminant". In: *In preparation.*

Bhargava, M., A. Shankar, and J. Tsimerman (2013). "On the Davenport–Heilbronn theorems and second order terms". In: *Inventiones mathematicae* 193.2, pp. 439–499.

Bhargava, M., A. Shankar, and X. Wang (2015). "Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces". In: URL: https://arxiv.org/pdf/1512.03035.pdf.

Bhargava, M. et al. (2017). "Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves". In: URL: https://arxiv.org/pdf/1701.02458.pdf.

Brumer, A. and J. Silverman (1996). "The number of elliptic curves over $\mathbb{Q}$ with conductor N". In: *manuscripta mathematica* 91.1, pp. 95–102.

Chambert-Loir, A. and Y. Tschinkel (2001). "Fonctions zêta des hauteurs des espaces fibrés". In: *Rational points on algebraic varieties*. Springer, pp. 71–115.

Cohen, H., F. Diaz y Diaz, and M. Olivier (2002a). "Enumerating Quartic Dihedral Extensions of $\mathbb{Q}$". In: *Compositio Mathematica* 133.1, pp. 65–93.

— (2002b). "On the density of discriminants of cyclic extensions of prime degree". In: *Journal für die reine und angewandte Mathematik* 550, pp. 169–210.

Cohen, H. and H. Lenstra (1984). "Heuristics on class groups of number fields". In: *Number Theory Noordwijkerhout 1983*. Springer, pp. 33–62.

Cohen, H. and F. Thorne (2016a). "Appendix to: Dirichlet series associated to quartic fields with given resolvent". In: URL: `http://people.math.sc.edu/thornef/papers/ct4-appendix.pdf`.

— (2016b). "Dirichlet series associated to quartic fields with given cubic resolvent". In: *Research in Number Theory* 2.1, p. 29.

— (2016c). "On D_ℓ-extensions of odd prime degree ℓ". In: URL: `https://arxiv.org/pdf/1609.09153.pdf`.

Cohn, H. (1954). "The density of abelian cubic fields". In: *Proceedings of the American Mathematical Society Volume 5.3*, pp. 476–477.

Couveignes, J. (2019). "Enumerating Number Fields". In: URL: `https://arxiv.org/pdf/1907.13617.pdf`.

Datskovsky, B. and D. Wright (1988). "Density of discriminants of cubic extensions". In: *Journal für die reine und angewandte Mathematik* 386, pp. 116–138.

Davenport, H. and H. Heilbronn (1971). "On the density of discriminants of cubic fields. II". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 322.1551, pp. 405–420.

Delone, B. and D. Faddeev (1940). "Theory of irrationalities of third degree". In: *Trudy Matematicheskogo Instituta imeni VA Steklova* 11, pp. 3–340.

Duke, W. (1998). "Bounds for arithmetic multiplicities". In: 2, pp. 163–172.

Dummit, E. (2014). "Counting Number Field Extensions of Given Degree, Bounded Discriminant, and Specified Galois Closure". PhD thesis. University of Wisconsin Madison.

— (2017). "Counting G-extensions by discriminant". In: URL: https://arxiv.org/pdf/1704.03124.pdf.

Ellenberg, J. and A. Venkatesh (2006). "The number of extensions of a number field with fixed degree and bounded discriminant". In: *Annals of Mathematics*, pp. 723–741.

Fieker, C. and J. Klüners (2003). "Minimal discriminants for fields with small Frobenius groups as Galois groups". In: *Journal of Number Theory* 99.2, pp. 318–337.

Frei, C. and M. Widmer (2018a). "Average bounds for the ℓ-torsion in class groups of cyclic extensions". In: *Research in Number Theory Volume 4.3*, p. 34.

— (2018b). "Averages and higher moments for the ℓ-torsion in class groups". In: URL: https://arxiv.org/pdf/1810.04732.pdf.

Gan, W., B. Gross, G. Savin, et al. (2002). "Fourier coefficients of modular forms on G_2". In: *Duke Mathematical Journal* 115.1, pp. 105–169.

Granville, A. and K Soundararajan (2005). "Extreme values of $|\zeta(1 + it)|$". In: URL: https://arxiv.org/pdf/math/0501232.pdf.

Heath-Brown, R. (1978). "Hybrid bounds for Dirichlet L-functions". In: *Inventiones mathematicae* 47.2, pp. 149–170.

Heilbronn, H (1971). "On the 2-classgroup of cubic fields". In: *Studies in Pure Math*, pp. 117–119.

— (1934). "On the class-number in imaginary quadratic fields". In: *The Quarterly Journal of Mathematics* 1, pp. 150–160.

Hermite, C. (1857). "Sur le nombre limité d'irrationalités auxquelle se réduisent les racines des équationsa coefficients entiers complexes d'un degré et d'un discriminant donnés (Extrait d'une lettrea M. Borchardt)". In: *Journal für die reine und angewandte Mathematik* 53, pp. 182–192.

Hess, F., S. Pauli, and M. Pohst (2003). "Computing the multiplicative group of residue class rings". In: *Mathematics of Computation* 72.243, pp. 1531–1548.

Hilbert, D. (1898). "Über die Theorie des relativquadratischen Zahlkörpers". In: *Mathematische Annalen* 51.1, pp. 1–127.

Klüners, J. (2005). "A counter example to Malle's conjecture on the asymptotics of discriminants". In: *Comptes Rendus Mathematique* 340.6, pp. 411–414.

— (2006). "Asymptotics of number fields and the Cohen-Lenstra heuristics". In: *Journal de théorie des nombres de Bordeaux* 18.3, pp. 607–615.

— (2012). "The distribution of number fields with wreath products as Galois groups". In: *International Journal of Number Theory* 8.03, pp. 845–858.

Landau, E. (1918). "Uber die Klassenzahl imaginär-quadratischer Zahlkörper". In: *Gottinger Nachr.*

Levi, F. (1914). "Kubische Zahlkörper und binäre kubische Formenklassen". In: *Ber. Sächs. Akad. Wiss. Leipzig, Math.-Naturwiss* 66, pp. 26–37.

Louboutin, S. (2011). "Upper bounds for residues of Dedekind zeta functions and class numbers of cubic and quartic number fields". In: *Mathematics of computation* 80.275, pp. 1813–1822.

Malle, G. (2002). "On the distribution of Galois groups". In: *Journal of Number Theory* 92.2, pp. 315–329.

— (2004). "On the distribution of Galois groups, II". In: *Experimental Mathematics* 13.2, pp. 129–135.

Mertens, F. (1941). "Ueber einige asymptotische Gesetze der Zahlentheorie." In: *Journal für die reine und angewandte Mathematik* 77, pp. 289–338.

Milne, J. (1997). "Class Field Theory". In: URL: `https://www.jmilne.org/math/CourseNotes/CFT.pdf`.

Montgomery, H. and R. Vaughan (2007). *Multiplicative number theory I: Classical theory*. Vol. 97. Cambridge university press.

Neukirch, J. (2013). *Algebraic number theory*. Vol. 322. Springer.

Pierce, L., C. Turnage-Butterbaugh, and M. Wood (2017). "An effective Chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups". In: *https://arxiv.org/pdf/1709.09637.pdf*.

Rademacher, H. (1958). "On the Phragmén Lindelöf theorem and some applications". In: *Mathematische Zeitschrift* 72.

Robin, G. (1983). "Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n". In: *Acta Arithmetica* 42.4, pp. 367–389.

Robinson, D. (2012). *A Course in the Theory of Groups*. Vol. 80. Springer.

Schmidt, W. (1995). "Number fields of given degree and bounded discriminant". In: *Astérisque* 228.4, pp. 189–195.

Taniguchi, T. and F. Thorne (2013). "Secondary terms in counting functions for cubic fields". In: *Duke Mathematical Journal* 162.13, pp. 2451–2508.

Titchmarsh, E. (1986). *The theory of the Riemann zeta-function*. Oxford University Press.

Wright, D. (1989). "Distribution of discriminants of abelian extensions". In: *Proceedings of the London Mathematical Society* 3.1, pp. 17–50.

Zhang, S. (2005). "Equidistribution of CM-points on quaternion Shimura varieties". In: *International Mathematics Research Notices* 2005.59, pp. 3657–3689.