A DENSITY OF RAMIFIED PRIMES

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Christine Elizabeth McMeekin

August 2018

A DENSITY OF RAMIFIED PRIMES

Christine Elizabeth McMeekin, Ph.D.

Cornell University 2018

The gestalt of this thesis can be seen in Theorem 4.5.2 and Theorem 4.5.4 which give formulas for the density of rational primes that satisfy a certain spin relation. We use the spin of prime ideals, a special case of class field theory, and the infrastructure developed throughout this thesis in order to prove under reasonable assumptions, the surprising formula in conditional Theorem 5.4.3 giving the expected density of rational primes that exhibit a prescribed *ramified* factorization in a number field depending on the prime in question. This density is strictly between 0 and 1.

BIOGRAPHICAL SKETCH

Christine McMeekin was born in Connecticut where she obtained her Bachelors of Arts in mathematics at the University of Connecticut. During her time at the University of Connecticut, Christine became interested in algebraic number theory, working closely with Alvaro Lozono-Robledo and Keith Conrad. Christine was greatly influenced by being a counselor at PROMYS, a summer school in number theory for high school students at Boston University. Christine is also a visual artist, singer/song-writer, and electronic music composer. She is drawn to mathematics for its intensely creative nature. While it is "difficult to hold the paintbrush or even to see the paint", she attests that mathematics is the most beautiful medium of fine art.

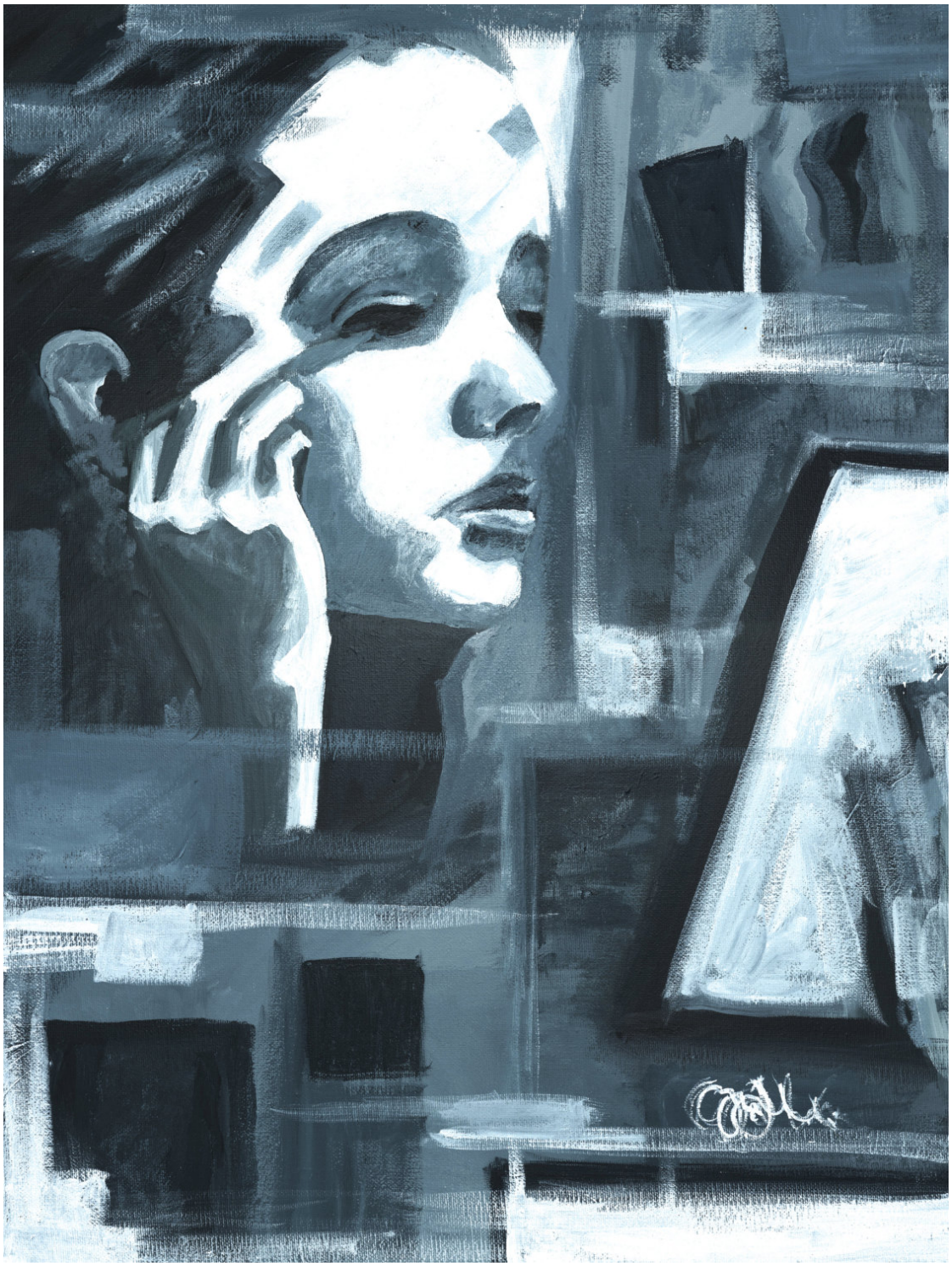


Figure 1: “Mirror”
by Christine McMeekin
acrylic on canvas

I dedicate this thesis to my father, John McMeekin for showing me the value of hard work and perseverance.

ACKNOWLEDGEMENTS

Doing research in mathematics at Cornell University has helped me to comprehend and grow from some of the greatest obstacles I have faced in my life and I have deep gratitude for having had this opportunity.

First and foremost, I would like to thank my advisor, Ravi Ramakrishna. It is because of Ravi's guidance that I became the mathematician I am today. His vast knowledge of number theory and his commitment to understanding my exceptional cognitive processes made this dissertation possible. As we worked together, I would ask "is it true that if A then B?" and Ravi would either respond "that's an open problem" or "that's true because..." and then I would say "then I have a proof that if C then D". We kept doing this until between my creativity and Ravi's expertise, we converged on a proof of the formula I conjectured.

Brian Hwang was extremely helpful in the translation of my ideas into a language that other mathematicians can easily understand. One semester, Brian met with me weekly to discuss the journal I keep of my research thoughts. The work I did with Brian and Ravi that semester was necessary not only for the outcome of these results, but also for the outcome of my personal well-being. I can not thank them enough.

Enormous thanks goes to Keith Conrad and Àlvaro Lozano-Robledo for recognizing my potential when I was an undergraduate at the University of Connecticut. They saw something in me and encouraged me to succeed early in my mathematical career. Keith is still answering my math-overflow questions thoughtfully and thoroughly.

I would also like to thank my committee members Shankar Sen and David Zywina, John Hubbard for his encouragement, and I would like to thank Christian Maire for our mathematical conversations and for believing in me.

Lemma 4.1.2 is due to my colleague Sam Mundy. I posted the question on facebook, looking for a proof, and Sam rose to the challenge.

I would also like to thank the authors of "The Spin of Prime Ideals" [6], John Friedlander, Henryk Iwaniec, Barry Mazur, and Karl Rubin. This work was possible because of their work in [6].

My computations would not have been possible without the help of Steve Gaarder. Steve provided me with indispensable computing resources and furthermore took the time to educate me in computing.

Beyond the mathematics, there were many people who helped to make my PhD possible. In the fall semester of 2017, shortly after I conjectured the formula that is now Theorem 4.5.2, I suffered a medical misfortune that stopped my progress for some time, but thanks to the help of my community it did not stop me from proving my conjecture and including it in this dissertation. I have deep gratitude for the Cornell Graduate School, Student Disability Services, and the Mathematics Department at Cornell for making it possible for me to continue my research that semester during my recovery. I would also like to thank my doctors and Emily Sorel for helping me to be well. These results would not have been possible without them.

Last, but certainly not least, I would like to thank my friends, my family, and the many people who helped me get to where I am today by recognizing my strengths and encouraging me to succeed. Thank you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

PROLOGUE

Dirichlet's Infinite Song

In the words of Leonard Cohen, "it goes like this the 4th the 5th". Leonard was referring to the 4th and 5th notes in the seven-note scale. For example, in the key of **C** major, we have the seven-note scale, [**C**, **D**, **E**, **F**, **G**, **A**, **B**] and while Leonard Cohen sings these words, he plays the chords **C**, **F**, then **G** on the guitar which is the 1st, the 4th, and then the 5th note in the **C** major 7-note scale.

What is the 8th? It's just **C** again. What about the 9th? That would be **D**. The pattern continues so that for example the 18th would be **F** because $18 = 7 \times 2 + 4$ This is the idea behind modular arithmetic. Here, we are working modulo 7. We say that 8 is congruent to 1 mod 7 and 9 is congruent to 2 mod 7 etc...

C	**D**	**E**	**F**	**G**	**A**	**B**
1	2^*	3^*	4	5^*	6	7^*
8	9	10	11^*	12	13^*	14
15	16	17^*	18	19^*	20	21

Imagine an infinitely long song such that the sequence of notes is exactly the sequence of prime numbers modulo p for some prime number p. Let's use the **C** major 7-note scale (so $p = 7$).

The first note in the song corresponds to the first prime number, 2 so the first note is a **D**. The next note corresponds to the next prime number 3 so the next

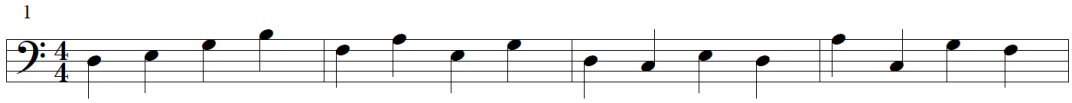


Figure 2: The first four measures of Dirichlet's Infinite Song

note is **E**. The next integer 4 is not prime because $4 = 2 \times 2$ so the next note corresponds to the next prime which is 5 or **G**. Then comes **B** for 7. The next prime is 11 which is **F** since 11 is 4 more than a multiple of 7 etc...

The note **B** will only be played once throughout the infinitely long song because 7 is the only prime divisible by 7, but how often are the other notes played?

Dirichlet's theorem on primes in arithmetic progression, later generalized by Chebotarev, tells us that except for **B**, each note is played with "probability" $\frac{1}{6}$. There are 6 notes remaining so this means the notes in Dirichlet's Infinite Song are *equidistributed*. In other words, Dirichlet's theorem gives us a way to partition the primes so that the probability that an arbitrary prime is in the first class is equal to the probability that the prime is in the next class etc...

In Theorems 4.5.2 and 4.5.4, we will see an entirely new way to partition the primes in an asymptotically predictably distributed fashion coming from a Hilbert symbol relation given in [6] between the spins of a prime ideal.

Background and References

Throughout this thesis, we assume knowledge of algebraic number theory at the level of an introductory graduate course . For references regarding background, I recommend consulting the following sources for the following audiences.

- *Number Fields* by Marcus [8] is a great place to start to learn some algebraic number theory. I'm a fan of Algebraic Number Theory by Milne [10] which is available for free online. I also highly recommend Keith Conrad's expository notes [5] which include a variety of topics in algebraic number theory.
- For readers who are familiar with algebraic number theory, but have not had exposure to class field theory, I recommend consulting *Class Field Theory* by Artin and Tate [1], *Class Field Theory* by Childress [4], or Class Field Theory by Milne [11] (also free online).
- *Algebraic Number Theory* by Neukirch [13] is a good resource for those readers who have (at least some) familiarity with class field theory already and are primarily looking for a reference. Note that Neukirch does everything in the narrow setting, meaning that all infinite places are included in the conductors. This thesis also takes place in the narrow setting.

Chapter 1 is intended as a reference and to establish common background and notation. It also serves as an expository tour through class field theory for readers with background in algebraic number theory.

Unless explicitly defined otherwise, all ray class groups/fields in this thesis are assumed to be narrow, meaning that all infinite places of the base field di-

vide the modulus/conductor. We refer to a narrow modulus by it's finite part, an ideal in the ring of integers of the base field. Chapter 2 gives an exposition of a particular case of class field theory.

In Chapter 3, we will discuss the spin of prime ideals and known results regarding dependence and distribution of spin. The spin of prime ideals was originally defined in [6] by Friedlander, Iwaniec, Mazur, and Rubin. Though a simple algebraic condition, the spin of prime ideals provides a powerful, modern, and novel approach to studying prime numbers.

Chapter 4 is original work; it ties together the previous Chapters into Theorems 4.5.2 and 4.5.4 which give formulas for the density of primes satisfying a spin relation. The densities in these Theorems will be applied in Chapter 5 to conditional Theorem 5.4.3, which gives a formula for the density of rational primes p that split as completely as possible in a number field depending on p given the necessary ramification. In particular, the formula in conditional Theorem 5.4.3 gives a density of ramified primes that is strictly between 0 and 1.

CHAPTER 1

CLASS FIELD THEORY EXPOSITION

In Chapter 1, we give an expository tour through class field theory following [11] and [13]. The purpose of Chapter 1 is to establish a common language. We restrict ourselves to the narrow setting; in a narrow ray class field, ramification is allowed at all infinite places. We assume K to be a totally real number field throughout this thesis and we will impose further restrictions as we procede.

1.1 Ray Class Groups

Let K be a totally real number field (i.e. every embedding of K into $\mathbb{C}$ lays in $\mathbb{R}$).

A *modulus* for K is defined as a formal product

$$\mathfrak{m} := \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}}$$

taken as $\mathfrak{p}$ varies over all finite and infinite places of K such that only finitely many $a_{\mathfrak{p}} \in \mathbb{Z}_{\geq 0}$ are non-zero and for $\mathfrak{p}$ an infinite place, $a_{\mathfrak{p}} \in \{0, 1\}$.

Let $\mathfrak{m} := \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}}$ be a modulus. When $\mathfrak{p}$ is infinite, we let $\sigma_{\mathfrak{p}} : K \hookrightarrow \mathbb{R}$ denote the corresponding embedding. We say that a place $\mathfrak{p}$ *divides* the modulus $\mathfrak{m}$ whenever $a_{\mathfrak{p}} > 0$. For $\alpha \in K^{\times}$, we write

$$\alpha \equiv^{*} 1 \bmod \mathfrak{m}$$

whenever $\mathrm{ord}_{\mathfrak{p}}(\alpha - 1) \geq a_{\mathfrak{p}}$ for all finite $\mathfrak{p}$ dividing $\mathfrak{m}$ and $\sigma_{\mathfrak{p}}(\alpha) > 0$ for all infinite $\mathfrak{p}$ dividing $\mathfrak{m}$.

We say a modulus is narrow when $a_\mathfrak{p} = 1$ for all infinite $\mathfrak{p}$ of K. We say a modulus is wide when $a_\mathfrak{p} = 0$ for all infinite $\mathfrak{p}$. For our purposes, it will usually suffice to consider only the narrow case. When it is clear that we are in the narrow case, we refer to a modulus by its finite part $\mathfrak{m}_0 := \prod_\mathfrak{p} \mathfrak{p}^{a_\mathfrak{p}}$ where now the product is taken as $\mathfrak{p}$ varies over all *finite* places of K and only finitely many $a_\mathfrak{p} \in \mathbb{Z}_{\geq 0}$ are non-zero. Note that $\mathfrak{m}_0$ is then easily identified with an honest ideal of O_K, the ring of integers of K. Given $\alpha \in K$, we write $\alpha > 0$ to mean that α is totally positive (i.e. $\sigma(\alpha) > 0$ for all embeddings $\sigma : K \hookrightarrow \mathbb{R}$). In the case when $\mathfrak{m}$ is narrow, $\alpha \equiv^* 1 \bmod \mathfrak{m}$ implies $\alpha > 0$.

We now define narrow ray class groups. Let $\mathfrak{m}$ be a narrow modulus with finite part $\mathfrak{m}_0$. Let $J_K^\mathfrak{m}$ denote the group of fractional ideals of K co-prime to $\mathfrak{m}_0$, the finite part of $\mathfrak{m}$. Let $P_K^\mathfrak{m}$ denote the subgroup formed by principal ideals which have a generator $\alpha \in K^\times$ such that $\alpha \equiv^* 1 \bmod \mathfrak{m}$. Note that we are abusing language slightly. A fractional ideal in $J_K^\mathfrak{m}$ can be written as $\frac{\mathfrak{a}}{\mathfrak{b}}$ for some integral ideals $\mathfrak{a}, \mathfrak{b} \subseteq O_K$. When we say that $\alpha^\times$ is a *generator* for $\frac{\mathfrak{a}}{\mathfrak{b}}$, we mean that $\alpha = \frac{a}{b}$ where $a, b \in O_K$ are honest generators of $\mathfrak{a}$ and $\mathfrak{b}$ respectively.

Definition 1.1.1. *Define the narrow ray class group over K of conductor $\mathfrak{m}$ to be*

$$\mathrm{nCl}_K^\mathfrak{m} := J_K^\mathfrak{m} / P_K^\mathfrak{m}.$$

Example 1.1.2. *For example in the case $K = \mathbb{Q}$, taking $\mathfrak{m}$ to be the narrow modulus with finite part $\mathfrak{m}_0 = (m)$ for $m > 0$,*

$$\mathrm{nCl}_\mathbb{Q}^\mathfrak{m} \cong (\mathbb{Z}/m)^\times.$$

Proposition 1.1.3. *Every element of $\mathrm{nCl}_K^\mathfrak{m}$ is represented by an integral ideal $\mathfrak{a}$, and two integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ represent the same element of $\mathrm{nCl}_K^\mathfrak{m}$ if and only if there exist*

nonzero $a, b \in \mathcal{O}_K$ *such that* $a\mathfrak{a} = b\mathfrak{b}$ *and*

$$a \equiv b \equiv 1 \bmod \mathfrak{m}_0,$$

$$ab \succ 0.$$

Proof. V.1.6[11]. □

For a totally real number field K with ring of integers $\mathcal{O}_K$ and a narrow modulus $\mathfrak{m}$ with finite part $\mathfrak{m}_0$, define

$$K_{\mathfrak{m}} := \{\alpha \in K^\times : \mathrm{ord}_{\mathfrak{p}}(\alpha) = 0 \text{ for all } \mathfrak{p}|\mathfrak{m}_0\},$$

$$K_{\mathfrak{m},1} := \{\alpha \in K^\times : \mathrm{ord}_{\mathfrak{p}}(\alpha - 1) \geq a_{\mathfrak{p}} \text{ for all } \mathfrak{p}|\mathfrak{m}_0 \text{ and } \alpha \succ 0\},$$

$$U := \mathcal{O}_K^\times \quad \text{(the group of units)},$$

$$U_{\mathfrak{m},1} := K_{\mathfrak{m},1} \cap U.$$

Let C_K denote the quotient of the group of fractional ideals of K by the subgroup of principal ideals. That is, C_K is the wide ray class group of conductor 1 over K which is the usual class group of K.

Theorem 1.1.4. *Let K be a totally real number field of degree $n := [K : \mathbb{Q}]$. For every narrow modulus $\mathfrak{m}$ of K, there is an exact sequence*

$$1 \to U/U_{\mathfrak{m},1} \to K_{\mathfrak{m}}/K_{\mathfrak{m},1} \to \mathrm{n}Cl_K^{\mathfrak{m}} \to C \to 1$$

and a canonical isomorphism

$$K_{\mathfrak{m}}/K_{\mathfrak{m},1} \cong (\mathbb{Z}/2)^n \times (\mathcal{O}_K/\mathfrak{m}_0)^\times.$$

Therefore, $\mathrm{n}Cl_K^{\mathfrak{m}}$ *is a finite group of order*

$$h_{\mathfrak{m}} = \frac{2^n h \,\mathrm{Norm}(\mathfrak{m}_0) \prod_{\mathfrak{p}|\mathfrak{m}_0} \left(1 - \frac{1}{\mathrm{Norm}(\mathfrak{p})}\right)}{[U : U_{\mathfrak{m},1}]}$$

where $h = \#C_K$ is the class number of K.

Proof. V.1.7[11]. □

1.2 The Frobenius

Let K be a number field and let L be a finite abelian[1] Galois extension of K. Let $\mathrm{Gal}(L/K)$ denote the Galois group of the extension. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{P}$ be a prime of L laying above $\mathfrak{p}$. Recall O_K denotes the ring of integers of K and similarly, let O_L denote the ring of integers of L.

Definition 1.2.1. *The decomposition group of $\mathfrak{P}$ for the extension L/K is defined as*

$$D(\mathfrak{P}) := \{\tau \in \mathrm{Gal}(L/K) : \mathfrak{P}^\tau = \mathfrak{P}\}$$

and the inertia group of $\mathfrak{P}$ for the extension L/K is defined as

$$E(\mathfrak{P}) := \{\tau \in \mathrm{Gal}(L/K) : \alpha^\tau \equiv \alpha \bmod \mathfrak{P} \quad \forall \alpha \in O_L\}.$$

For $\tau \in E(\mathfrak{P})$, consider $\alpha \in O_L$ such that $\alpha \equiv 0 \bmod \mathfrak{P}$ to see that $\tau \in D(\mathfrak{P})$ showing that $E(\mathfrak{P})$ is a subgroup of $D(\mathfrak{P})$.

Definition 1.2.2. *Define the ramification index of $\mathfrak{P}$ for the extension L/K to be the size of the inertia group,*

$$e_{L/K}(\mathfrak{P}) := \#E(\mathfrak{P}).$$

Define the inertia degree of $\mathfrak{P}$ for the extension L/K to be the index of the inertia group in the decomposition group,

$$f_{L/K}(\mathfrak{P}) := (D(\mathfrak{P}) : E(\mathfrak{P})).$$

[1] See V.1[11] for the non-abelian case.

In fact, $f_{L/K}(\mathfrak{P}) = \#\,\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ because there is an isomorphism

$$d_{\mathfrak{P}} : D(\mathfrak{P})/E(\mathfrak{P}) \xrightarrow{\sim} \mathrm{Gal}\,((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$$

induced by the natural map as explained in Chapter 4 of [8].

The Galois group of the residue fields $\mathrm{Gal}\,((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ is cyclic with a canonical generator φ which maps $x \in \mathcal{O}_L/\mathfrak{P}$ to x^q where $q := \#\mathcal{O}_K/\mathfrak{p} = \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p})$. (Letting p be the rational prime such that $\mathfrak{p}$ lies above p, then $q = p^{f_{K/\mathbb{Q}}(\mathfrak{p})}$).

Definition 1.2.3. *The Frobenius element of* $\mathrm{Gal}(L/K)$ *at* $\mathfrak{P}$*, (a prime of* L *unramified in* L/K*) is defined as*

$$\mathrm{Frob}_{L/K}(\mathfrak{P}) := d_{\mathfrak{P}}^{-1}(\varphi).$$

Since we are in the case in which $\mathrm{Gal}(L/K)$ is abelian, by property 1.9 in Chapter V of [11], $\mathrm{Frob}_{L/K}(\mathfrak{P}_1) = \mathrm{Frob}_{L/K}(\mathfrak{P}_2)$ for any two primes $\mathfrak{P}_1$ and $\mathfrak{P}_2$ of L laying above a common prime of K. Therefore, we can unambiguously use the notation

$$\mathrm{Frob}_{L/K}(\mathfrak{p}) := \mathrm{Frob}_{L/K}(\mathfrak{P})$$

where $\mathfrak{P}$ is any prime of L laying above $\mathfrak{p}$, a prime of K.

1.3 The Artin Map and Ray Class Fields

As in Section 1.1, we let $J_K^{\mathfrak{m}}$ denote the group of fractional ideals of K co-prime to $\mathfrak{m}_0$, the finite part of the modulus $\mathfrak{m}$ of K and we let $P_K^{\mathfrak{m}}$ denote the subgroup of $J_K^{\mathfrak{m}}$ generated by prime ideals of $\mathcal{O}_K$ which have a totally positive generator α such that $\alpha \equiv^* 1 \bmod \mathfrak{m}$.

Let L/K be a finite abelian Galois extension. Assume that all primes which ramify in L/K divide the modulus $\mathfrak{m}$ of K. Then the (global) Artin map is the homomorphism

$$\mathrm{Art}_{L/K} : J_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$

induced by the map which sends primes $\mathfrak{p}$ of K (unramified in L/K) to $\mathrm{Frob}_{L/K}(\mathfrak{p})$.

Theorem 1.3.1. *Let L/K be a finite abelian Galois extension. Let $\mathfrak{m}$ be a modulus of K such that if $\mathfrak{p}$ ramifies in L/K then $\mathfrak{p}|\mathfrak{m}$. Then the Artin map*

$$\mathrm{Art}_{L/K} : J_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$

is a surjective homomorphism which factors through $\mathrm{nCl}_K^{\mathfrak{m}}$.

Proof. V.3.5[11]. □

Definition 1.3.2. *Given a finite abelian extension L/K, define the conductor of L/K to be the greatest common divisor of all moduli $\mathfrak{m}$ of K such that the Artin map factors through $\mathrm{nCl}_K^{\mathfrak{m}}$.*

Another way of saying that $\mathrm{Art}_{L/K}$ factors through $\mathrm{nCl}_K^{\mathfrak{m}}$ is that defining $H_L := \ker(\mathrm{Art}_{L/K})$, we have

$$P_K^{\mathfrak{m}} \subseteq H_L \subseteq J_K^{\mathfrak{m}}.$$

Such a subgroup of $J_K^{\mathfrak{m}}$ is called a congruence subgroup modulo $\mathfrak{m}$.

Theorem 1.3.3. *For every congruence subgroup H modulo $\mathfrak{m}$, there exists a finite abelian extension L/K such that $H = \ker(\mathrm{Art}_{L/K})$.*

Proof. V.3.6 [11]. □

In particular, taking $H := P_K^{\mathfrak{m}}$, Theorem 1.3.3 shows the existence of the narrow ray class field over K of conductor $\mathfrak{m}$.

Definition 1.3.4. *Let $\mathfrak{m}$ be a narrow modulus for K. Then the narrow ray class field over K of conductor $\mathfrak{m}$ is the finite abelian extension $\mathrm{nR}_K^{\mathfrak{m}}$ of K such that the Artin map induces an isomorphism*

$$\mathrm{Art}_{\mathrm{nR}^{\mathfrak{m}}/K} : \mathrm{nCl}_K^{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(\mathrm{nR}_K^{\mathfrak{m}}/K).$$

Corollary 1.3.5. *Fixing a modulus $\mathfrak{m}$ of K, there is a bijection from the set of abelian extensions of K contained in $\mathrm{nR}_K^{\mathfrak{m}}$ to the set of subgroups of $\mathrm{nCl}_K^{\mathfrak{m}}$ given by the map*

$$L \mapsto H_L.$$

where $H_L := \ker(\mathrm{Art}_{L/K})$. Furthermore,

$$L_1 \subseteq L_2 \iff H_{L_1} \supseteq H_{L_2}$$

$$H_{L_1 L_2} = H_{L_1} \cap H_{L_2}$$

$$H_{L_1 \cap L_2} = H_{L_1} H_{L_2}.$$

Proof. V.3.7[11]. □

1.4 Dirichlet's Density Theorem

Definition 1.4.1. *Let S be a set of primes and let $R \subseteq S$. The density of primes $\mathfrak{p} \in S$ which lay in R is defined as*

$$d(R|S) := \lim_{N \to \infty} \frac{\#R_N}{\#S_N}$$

where S_N and R_N denote the set of primes in S and R respectively of norm less than $N \in \mathbb{Z}_+$.

For a finite abelian extension L/K and an element $\sigma \in \mathrm{Gal}(L/K)$, we define $\mathrm{Ray}_{L|K}(\sigma)$ to be the the set of odd[2] primes of K which map to σ via the Artin map. That is, letting $\mathscr{P}_K^{2\ell}$ denote the set of primes of K co-prime to 2ℓ where ℓ is the conductor of K,

$$\mathrm{Ray}_{L|K}(\sigma) := \{\mathfrak{p} \in \mathscr{P}_K^{2\ell} : \mathrm{Art}_{L|K}(\mathfrak{p}) = \sigma\}.$$

We now state Dirichlet/Chebotarev's Theorem for finite abelian extensions. In this thesis, we will use the version of Chebotarev's Theorem for cyclic number fields using natural density.

Theorem 1.4.2 (Dirichlet-Chebotarev)**.** *Let $L|K$ be a finite abelian extension. Then for every $\sigma \in \mathrm{Gal}(L/K)$, the set $\mathrm{Ray}_{L|K}(\sigma)$ has a density and it is given by*

$$d\left(\mathrm{Ray}_{L|K}(\sigma)|\mathscr{P}_K^{2l}\right) = \frac{1}{\#\,\mathrm{Gal}(L/K)}.$$

Proof. [14] provides a discussion of various forms of Chebotarev's Theorem with references to various proofs. Most treatments of this Theorem use Dirichlet density for ease, e.g. Theorem 13.4 in Chapter VII of [13] (note that we assume L/K to be abelian). As stated in [7], due to the Wiener-Ikehara tauberian Theorem, extending the proof to natural density requires a proof of the non-vanishing of L-functions on the line $\mathrm{Re}(s) = 1$ (as opposed to only at $s = 1^+$ for the Dirichlet density version). □

[2] odd meaning co-prime to 2

CHAPTER 2

THE COINCIDENCE OF NARROW AND WIDE

At the foundation of this thesis lays the study of totally real number fields that satisfy an elegant class field theoretic coincidence. While computing class groups is difficult in general, this class field theoretic coincidence is easy to test for computationally and when this coincidence occurs, it gives us the tools to prove results that are more powerful than what we could prove otherwise.

2.1 A Unique Quadratic Subextension of Ray Class Fields

Let K be a totally real number field with ring of integers O_K. Let

$$U_T := \{u \in O_K^\times : u > 0\}$$

denote the group of totally positive units of K and let $U^2 := (O_K^\times)^2$ denote the group of square units of K. Note that in general,

$$U^2 \subseteq U_T.$$

Our first lemma asserts that the subgroups above coincide exactly when the narrow and wide Hilbert class fields of K coincide.

Lemma 2.1.1. *Let K be a totally real number field. Then $U_T = U^2$ in K if and only if the narrow and wide Hilbert class groups of K coincide.*

Proof. Let $n := [K : \mathbb{Q}]$. Since K is totally real, $U \cong \mathbb{Z}/2 \times \mathbb{Z}^{n-1}$ by Dirichlet's Unit Theorem so $U/U^2 \cong (\mathbb{Z}/2)^n$.

Let $\mathfrak{m}_\infty$ denote the narrow modulus with finite part 1. That is, $\mathfrak{m}_\infty$ is the product of all infinite places. From Theorem 1.1.4, since $U_{\mathfrak{m}_\infty,1} = U_T$, we have the following exact sequence

$$1 \to U/U_T \to K_\mathfrak{m}/K_{\mathfrak{m}_\infty,1} \to \mathrm{nCl}_K^{\mathfrak{m}_\infty} \to C_K \to 1$$

and since $\mathfrak{m}_0 = 1$, there is a canonical isomorphism $K_\mathfrak{m}/K_{\mathfrak{m}_\infty,1} \cong (\mathbb{Z}/2)^n$. This induces an exact sequence

$$1 \to (\mathbb{Z}/2)^n/(U/U_T) \to \mathrm{nCl}_K^{\mathfrak{m}_\infty} \to C_K \to 1$$

which shows that $U/U_T \cong (\mathbb{Z}/2)^n$ if and only if $\mathrm{nCl}_K^{\mathfrak{m}_\infty} = C_K$. Therefore $U/U_T \cong U/U^2$ if and only if $\mathrm{nCl}_K^{\mathfrak{m}_\infty} = C_K$. Since $U^2 \subseteq U_T$, we have proven the desired result.

□

Remark 2.1.2. *Note that by the definitions of narrow and wide Hilbert class groups, these two groups coincide precisely when every principal ideal has a totally positive generator. Therefore $U_T = U^2$ if and only if every principal ideal has a totally positive generator.*

Lemma 2.1.3. *Let K be a totally real number field, Galois over $\mathbb{Q}$ such that $h(K)$ is odd and U_T=U^2. Let $\mathfrak{p}$ be an odd prime of K. Then the narrow ray class field over K of conductor $\mathfrak{p}$ has a unique quadratic subextension.*

Proof. We first show that the narrow ray class group over K of conductor $\mathfrak{p}$ has even order. We then show the 2-part of the narrow ray class group over K of conductor $\mathfrak{p}$ is cyclic.

Let $\mathfrak{m}$ be the narrow modulus with finite part $\mathfrak{p}$. Then by Theorem 1.1.4, since

K is totally real,

$$h_{\mathfrak{m}} = \frac{2^n(p-1)h}{(U : U_{\mathfrak{m},1})}.$$

where $p := \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p})$ and $h := h(K) = \#C_K$ is the class number of K.

Observe $U_{\mathfrak{m},1} \subseteq U_T$ since $\mathfrak{m}$ is narrow. Then since $U_T = U^2$,

$$(U : U_{\mathfrak{m},1}) = (U : U_T)(U_T : U_{\mathfrak{m},1}) = 2^n(U^2 : U_{\mathfrak{m},1})$$

$$\implies \quad h_{\mathfrak{m}} = \frac{(p-1)h}{(U^2 : U_{\mathfrak{m},1})}.$$

Consider the injection

$$\frac{U^2}{U_{\mathfrak{m},1}} \hookrightarrow \left(\frac{O_K}{\mathfrak{p}}\right)^{\times}$$

coming from the exact sequence and canonical isomorphism in Theorem 1.1.4.

The image is contained in $\left(\left(\frac{O_K}{\mathfrak{p}}\right)^{\times}\right)^2$ so $(U^2 : U_{\mathfrak{m},1})|\frac{p-1}{2}$. Then $(U_T : U_{\mathfrak{m},1})|\frac{p-1}{2}$. Therefore $h_{\mathfrak{m}}$ is even.

Next, we show the 2-part of the ray class group over K of conductor $\mathfrak{m}$ is cyclic.

Let $L_{\mathfrak{p}}$ denote the maximal 2-extension of the ray class field over K of conductor $\mathfrak{m}$ where $\mathfrak{p}$ is a prime in K. Suppose $L_{\mathfrak{p}}/K$ is not cyclic and consider the inertia group at $\mathfrak{p}$, denoted E. Note that $L_{\mathfrak{p}}/K$ is tamely ramified at $\mathfrak{p}$ since this is a 2-extension and 2 is prime to $\mathfrak{p}$. This implies E is cyclic so E is a proper subgroup of $G = \mathrm{Gal}(L_{\mathfrak{p}}/K)$. Then the fixed field of E, denoted L_E, is a nontrivial even extension of K in which $\mathfrak{p}$ is unramified, but this implies L_E is contained in the ray class field over K of conductor $\mathfrak{m}_\infty$, which is odd by Lemma 2.1.1 since $h(K)$ is odd so this is a contradiction. □

2.2 The Primes to The Units

Definition 2.2.1. *For n an odd rational prime, define $K(n,\ell)$ to be the degree n absolute subfield of the ℓ^{th} cyclotomic field;*

- *$n = [K(n,\ell) : \mathbb{Q}]$ is prime.*
- *The conductor of $K(n,\ell)/\mathbb{Q}$ is ℓ.*

Note that $K(n,\ell)$ automatically satisfies the following properties

- *$K(n,\ell)$ is totally real.*
- *$K(n,\ell)$ is Galois over $\mathbb{Q}$ with cyclic Galois group.*

When we write $K := K(n,\ell)$ for arbitrary n and ℓ, then K is also assumed to satisfy the following conditions;

- *$U_T = U^2$.*
- *The class number of $K(n,\ell)$, denoted $h(K)$ is odd.*
- *2 and 5 are inert in $K(n,\ell)/\mathbb{Q}$.*

Lemma 2.2.2. *Let $K := K(n,\ell)$ with odd class number h. Let $\mathfrak{p}$ be an odd prime of K. Let $\mathfrak{p}^h = (\alpha)$ where $\alpha \succ 0$. Then there exits a unit $u \in \mathcal{O}_K^\times$ such that $u\alpha$ is a square element in $\mathrm{nR}_K^{\mathfrak{p}}$ and u is uniquely determined modulo squares.*

Proof. By Lemma 2.1.3, there exists a unique quadratic subextension of $\mathrm{nR}^{\mathfrak{p}}/K$. Let $\beta \in \mathcal{O}_K$ such that $L := K(\sqrt{\beta}) \subseteq \mathrm{nR}_K^{\mathfrak{p}}$. Let $\mathcal{O}_L$ denote the ring of integers of L.

Write

$$\beta\mathcal{O}_K = \mathfrak{q}_1^{r_1} \cdots \mathfrak{q}_m^{r_m},$$

the unique factorization of $\beta\mathcal{O}_K$ into distinct prime ideals of $\mathcal{O}_K$ where $0 \leq m$. Then as elements of $\mathcal{O}_K$,

$$\beta^h = us_1^{r_1} \cdots s_m^{r_m}$$

where $s_i \in \mathcal{O}_K$ is a generator of the principal ideal $\mathfrak{q}_i^h$ and u is some unit in $U = \mathcal{O}_K^\times$. Observe that since the class number $h = h(K)$ is odd,

$$L = K(\sqrt{\beta}) = K(\sqrt{\beta^h}) = K\left(\sqrt{us_1^{r_1} \cdots s_m^{r_m}}\right).$$

If $2|r_i$ then $\beta^h\mathcal{O}_K/\mathfrak{q}_i^{hr_i}$ is a principal ideal $\gamma\mathcal{O}_K$ such that $L = K(\sqrt{\beta}) = K(\sqrt{\gamma})$ with $\mathfrak{q}_i$ not dividing $\gamma\mathcal{O}_K$. Therefore we may assume that $\beta\mathcal{O}_K$ is a product of distinct prime ideals

$$\beta\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_m.$$

To show that $m = 1$ and $\mathfrak{q}_1 = \mathfrak{p}$, we will show that each $\mathfrak{q}_i$ is ramified in L. Let $\mathfrak{q} \subseteq \mathcal{O}_K$ be a prime ideal dividing $\beta\mathcal{O}_K$ such that $\mathfrak{q}^2 \nmid \beta\mathcal{O}_K$.

Write

$$\beta\mathcal{O}_K = \mathfrak{q}\mathfrak{a}$$

where $\mathfrak{q} \nmid \mathfrak{a}$. Then $\mathfrak{q} = \mathfrak{q}^2 + \beta\mathcal{O}_K$ since $\mathfrak{q}$ and $\mathfrak{a}$ are coprime ideals of $\mathcal{O}_K$. Lifting to $\mathcal{O}_L$, we get

$$\mathfrak{q}\mathcal{O}_L = (\mathfrak{q}^2\mathcal{O}_L + \beta\mathcal{O}_L).$$

Let $I := \mathfrak{q}\mathcal{O}_L + \sqrt{\beta}\mathcal{O}_L$. Since $\mathfrak{q}\mathcal{O}_L \subseteq I$ and $\sqrt{\beta}\mathcal{O}_L \subseteq I$,

$$\mathfrak{q}^2\mathcal{O}_L \subseteq I^2$$

$\beta\mathcal{O}_L \subseteq I^2$. Therefore $(\mathfrak{q}^2\mathcal{O}_L + \beta\mathcal{O}_L) \subseteq I^2$. We showed $\mathfrak{q}\mathcal{O}_L = (\mathfrak{q}^2\mathcal{O}_L + \beta\mathcal{O}_L)$ so

$$\mathfrak{q}\mathcal{O}_L \subseteq I^2.$$

The reverse inclusion is also true; $I^2 \subseteq \mathfrak{q}\mathcal{O}_L$ because an arbitrary element of I has the form $q + b$ for some $q \in \mathfrak{q}\mathcal{O}_L$ and $b \in \sqrt{\beta}\mathcal{O}_L$ so an arbitrary element of I^2 has the form

$$(q + b)^2 = q^2 + 2qb + b^2$$

and $q^2 + 2qb \in \mathfrak{q}\mathcal{O}_L$ and $b^2 \in \beta\mathcal{O}_L \subseteq \mathfrak{q}\mathcal{O}_L$.

Therefore $\mathfrak{q}\mathcal{O}_L = I^2$ so $\mathfrak{q}$ is ramified in L. Since $L \subseteq \mathrm{nR}_K^{\mathfrak{p}}$, we know that $\mathfrak{p}$ is the only finite prime that ramifies in L. Therefore $0 \leq m \leq 1$ since $\mathfrak{p}$ is the only prime of K that divides the square-free part of β.

If $L = K(\sqrt{u})$ for a unit $u \in \mathcal{O}_K^\times$ then L would be a nontrivial even extension of K unramified at all finite places, but by Lemma 2.1.1, since $h(K)$ is odd, there are no such extensions of K. Therefore $m = 1$ and $\mathfrak{q}_1 = \mathfrak{p}$. Then letting α be a totally positive generator of $\mathfrak{p}^h$, we have

$$\beta^h \mathcal{O}_K = \alpha \mathcal{O}_K \implies \beta^h = u\alpha$$

for some unit $u \in \mathcal{O}_K^\times$. Then $u\alpha$ is a square in L by construction of L.

Suppose there are two such units $u, v \in \mathcal{O}_K^\times$. That is, suppose $u\alpha$ and $v\alpha$ are both squares in $\mathrm{nR}_K^{\mathfrak{p}}$. Then by uniqueness in Lemma 2.1.3,

$$K(\sqrt{u\alpha}) = K(\sqrt{v\alpha})$$

so $u \equiv v$ in U/U^2 where $U = \mathcal{O}_K^\times$. □

Let $\mathscr{P}_K^2$ denote the set of primes of K that are co-prime to 2. The following map $\mathbf{v}_K$ is well-defined by Lemma 2.2.2.

Definition 2.2.3. *Let K be a totally real number field of odd class number such that $U_T = U^2$ and 2 is inert in $K/\mathbb{Q}$. Define the map*

$$\mathbf{v}_K : \mathscr{P}_K^2 \to {}^{U}\!/_{U^2}$$
$$\mathfrak{p} \mapsto u_{\mathfrak{p}}$$

such that $u_{\mathfrak{p}}\alpha_{\mathfrak{p}}$ is a square (element) in $\mathrm{nR}_K^{\mathfrak{p}}$ where $\alpha_{\mathfrak{p}} \in O_K$ is a totally positive generator of $\mathfrak{p}$.

In Lemma 4.2.2, we will see that this map induces a well-defined surjective homomorphism from the narrow ray class group over K of conductor $\mathfrak{q}$,

$$\varphi : \mathrm{nCl}_K^{\mathfrak{q}} \twoheadrightarrow M_q$$

where for q a power of 2,

$$M_q := (O_K/q)^{\times} / \left((O_K/q)^{\times}\right)^2 .$$

This homomorphism allows us to define a map in Theorem 4.4.2 that will allow us to prove Theorem 4.5.2 and Theorem 4.5.4 giving the density of primes that satisfy a certain spin relation. First, we discuss the spin of prime ideals.

CHAPTER 3

THE SPIN OF PRIME IDEALS

In Chapter 3, we give an exposition of known results regarding the spin of prime ideals. In Chapter 4 we will give a formula describing the asymptotics of a spin dependence relation. In Chapter 5, we use this formula together with results from [6] on the distribution of spin to prove under reasonable assumptions, the surprising formula in Theorem 5.4.3 giving the density of rational primes p that exhibit a prescribed ramified factorization in a number field depending on K and p.

3.1 The Spin of Prime Ideals

Recall that we write $K := K(n, \ell)$ to mean that K is an arbitrary number field satisfying the following properties listed on page 16.

Definition 3.1.1 ([6]). *Let K be a totally real number field which is cyclic over $\mathbb{Q}$ of degree $n \geq 3$ such that $U_T = U^2$. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be a generator. Given an odd principal ideal $\mathfrak{a}$, we define the spin of $\mathfrak{a}$ (with respect to σ) to be*

$$spin(\mathfrak{a}, \sigma) = \left(\frac{\alpha}{\mathfrak{a}^\sigma}\right)$$

where $\mathfrak{a} = (\alpha)$, α is totally positive, and $\left(\frac{\alpha}{\mathfrak{b}}\right)$ denotes the quadratic residue symbol in K.

Spin is well-defined; since $U_T = U^2$, the choice of totally positive generator α does not affect the quadratic residue.

Lemma 11.1 in [6] states that the product

$$\text{spin}(\mathfrak{p}, \sigma)\text{spin}(\mathfrak{p}, \sigma^{-1})$$

is a product of Hilbert symbols at places dividing 2. We make this statement more explicit in Lemma 3.1.2.

For a place v of K, the Hilbert Symbol is defined such that $(a, b)_v := 1$ for $a, b \in K$ co-prime to v if the equation $ax^2 + by^2 = z^2$ has a solution $(x, y, z) \in K_{(v)}$ where at least one of x, y, or z is nonzero and $(a, b)_v := -1$ otherwise.

Lemma 3.1.2 ([6]). *[spindep] Let $K := K(n, \ell)$. Let α be a totally positive generator of the odd prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$. Then*

$$spin(\mathfrak{p}, \sigma)spin(\mathfrak{p}, \sigma^{-1}) = \prod_{v|2} (\alpha, \alpha^\sigma)_v.$$

In particular, if $\alpha \equiv 1 \bmod 4$ then $\prod_{v|2}(\alpha, \alpha^\sigma)_v = 1$.

Since 2 is assumed inert in $K(n, \ell)/\mathbb{Q}$,

$$spin(\mathfrak{p}, \sigma)spin(\mathfrak{p}, \sigma^{-1}) = (\alpha, \alpha^\sigma)_2.$$

Proof. We now prove Lemma 3.1.2 using the fact that

$$\prod_{v} (\alpha, \alpha^\sigma)_v = 1.$$

- We know $(\alpha, \alpha^\sigma)_v = 1$ for all infinite places v because α is totally positive.
- Next we'll show $(\alpha, \alpha^\sigma)_v = 1$ for all finite places v away from $\mathfrak{p}$, $\mathfrak{p}^\sigma$, and 2. Set $v = \mathfrak{q} \neq \mathfrak{p}, \mathfrak{p}^\sigma$ such that $\mathfrak{q} \nmid 2$. Our strategy will be to show there exists $x_0, y_0 \in \mathcal{O}_K/\mathfrak{q}$ such that $\alpha^\sigma x^2 + \alpha y^2 \equiv 1 \bmod \mathfrak{q}$ then apply Hensel's Lemma. Consider this equation rewritten as

$$\alpha^\sigma x^2 \equiv 1 - \alpha y^2 \bmod \mathfrak{q}.$$

There are $\frac{N(\mathfrak{q})+1}{2}$ squares in $\mathcal{O}_K/\mathfrak{q}$ so the left hand side and the right hand side each take on $\frac{N(\mathfrak{q})+1}{2}$ values (since $\mathfrak{q} \neq \mathfrak{p}_i, \mathfrak{p}_j$ implies the coefficients of x and y are non-zero. Then the pigeon hole principal implies there exists $x_0, y_0 \in \mathcal{O}_K/\mathfrak{q}$ such that

$$\alpha^\sigma x_0^2 \equiv 1 - \alpha y_0^2 \bmod \mathfrak{q}.$$

It can not be the case that both x_0 and y_0 are 0.

If $x_0 \not\equiv 0 \bmod \mathfrak{q}$ then $x_0^2 - \frac{1-\alpha y_0^2}{\alpha^\sigma} \equiv 0 \bmod \mathfrak{q}$. Then since $\mathfrak{q}$ is prime to 2 and $x_0 \not\equiv 0$, Hensel's Lemma implies there exists $x \in \mathcal{O}_{K(\mathfrak{q})}$ such that $x^2 = \frac{1-\alpha_j y_0^2}{u_i \alpha_i}$. Therefore $(\alpha, \alpha^\sigma)_\mathfrak{q} = 1$. If y_0 is nonzero, a similar argument works.

- We now show that $(\alpha, \alpha^\sigma)_\mathfrak{p} = \text{spin}(\mathfrak{p}, \sigma^{-1})$ and $(\alpha, \alpha^\sigma)_{\mathfrak{p}^\sigma} = \text{spin}(\mathfrak{p}, \sigma)$.

  If $\sigma \neq \tau \in \text{Gal}(K/\mathbb{Q})$, then $\text{spin}(\mathfrak{p}, \sigma) = \text{spin}(\mathfrak{p}^\tau, \sigma)$;

$$\text{spin}(\mathfrak{p}, \sigma) = \left(\frac{\alpha}{\mathfrak{p}^\sigma}\right) = \left(\frac{\alpha^\tau}{\mathfrak{p}^{\tau\sigma}}\right) = \text{spin}(\mathfrak{p}^\tau, \sigma).$$

  Therefore

$$\text{spin}(\mathfrak{p}, \sigma^{-1}) = \text{spin}(\mathfrak{p}^\sigma, \sigma^{-1}) = \left(\frac{\alpha^\sigma}{\mathfrak{p}^{\sigma\sigma^{-1}}}\right) = \left(\frac{\alpha^\sigma}{\mathfrak{p}}\right).$$

  Then using properties of the Hilbert symbol,

$$\begin{aligned}(\alpha, \alpha^\sigma)_\mathfrak{p} &= \left(\frac{\alpha^\sigma}{\mathfrak{p}}\right) \quad \text{since } \alpha \text{ generates } \mathfrak{p} \\ &= \left(\frac{\alpha}{\mathfrak{p}^{\sigma^{-1}}}\right) = \text{spin}(\mathfrak{p}, \sigma^{-1})\end{aligned}$$

  by applying the action of σ^{-1} to the equation defining the Hilbert symbol. Also,

$$(\alpha, \alpha^\sigma)_{\mathfrak{p}^\sigma} = \left(\frac{\alpha}{\mathfrak{p}^\sigma}\right) = \text{spin}(\mathfrak{p}, \sigma).$$

Then since $\prod_v (\alpha, \alpha^\sigma)_v = 1$, we are done. □

3.2 Aside; Character Sums

In the next section we will state results of Friedlander, Iwaniec, Mazur, and Rubin [6] on the distribution of spin. For $n > 3$, these results rely on a conjectural improvement to Burgess's result on short character sums [3]. In this section, we introduce Burgess's result and Friedlander, Iwaniec, Mazur, and Rubin's conjectural improvement.

Let χ be a non-principal real character mod q. We define

$$S_\chi(M,N) := \sum_{M<n<M+N} \chi(n).$$

Theorem 3.2.1 (Burgess)**.**

$$S_\chi(M,N) << N^{1-\frac{1}{r}} q^{\frac{r+1}{4r^2}+\epsilon},$$

with any integer $r \geq 1$ and any $\epsilon > 0$, the implied constant depending only on r and ϵ.

Proof. See [3]. □

The bound is only non-trivial when $N > q^{\frac{r+1}{4r}}$. When $[K : \mathbb{Q}] = 3$, this will be enough, but when $[K : \mathbb{Q}] > 3$, we will need something stronger.

Conjecture 3.2.2 (C_n)**.** *[6] Let χ be a non-principal real character mod q. Let $n \geq 3$, $Q \geq 3$, $N \leq Q^{\frac{1}{n}}$, and $q \leq Q$. Then*

$$S_\chi(M,N) << Q^{\frac{1-\delta}{n}+\epsilon},$$

with some $\delta = \delta(n) > 0$ and any $\epsilon > 0$, the implied constant depending only on ϵ and δ.

Conjecture C_n is true for $n = 3$; take $r = 6$ in Burgess's bound to obtain

$$\begin{aligned} S_\chi(M,N) &<< N^{1-\frac{1}{6}} q^{\frac{7}{144}+\epsilon} \\ &\leq Q^{\frac{47}{144}+\epsilon} \end{aligned}$$

since $N \leq Q^{\frac{1}{3}}$, and $q \leq Q$. Taking $\delta = \frac{1}{48}$, conjecture C_n states

$$S_\chi(M,N) << Q^{\frac{47}{144}+\epsilon}$$

so we have proven conjecture C_n for the case $n = 3$.

3.3 The Distribution of Spin; Known Results

Theorem 3.3.1. *[6] Let $K := K(n, \ell)$. Assume Conjecture C_n with exponent $\delta \leq \frac{2}{n}$. Letting $\mathfrak{p}$ run over odd prime principal ideals in K,*

$$\left| \sum_{\mathbb{N}(\mathfrak{p}) \leq x} \text{spin}(\mathfrak{p}, \sigma) \right| << x^{1-\nu+\epsilon}$$

where $\nu(n) = \frac{\delta}{2n(12n+1)}$. Here the implied constant depends only on ϵ and K.

Since conjecture C_n is true for $n = 3$ with $\delta = \frac{1}{48}$ as shown in Section 3.2, the Theorem holds unconditionally for $[K : \mathbb{Q}] = 3$ where $\nu = \frac{1}{10656}$.

Furthermore, the results of Friedlander, Iwaniec, Mazur, and Rubin hold regardless of congruence conditions.

Theorem 3.3.2. *[6] The bound in Theorem 3.3.1 still holds when the sum is further restricted to prime principal ideals which have a totally positive generator π satisfying $\pi \equiv \mu \bmod \mathfrak{M}$.*

Recall the definition of density given in Definition 1.4.1. Define

$$\Pi := \{\text{principal prime ideals of } O_K\ \}, \quad \Lambda_\sigma := \{\mathfrak{p} \in \Pi : \text{spin}(\mathfrak{p}, \sigma) = 1\}.$$

Let S' denote the set of primes of K that split completely in $K/\mathbb{Q}$.

Corollary 3.3.3. *Let $K := K(n, \ell)$ Assume Conjecture 3.2.2 for $n = [K : \mathbb{Q}]$. Let $\sigma \in \text{Gal}(K/\mathbb{Q})$ be non-trivial. Then*

$$d(\Lambda_\sigma|\Pi) = d(\Lambda_\sigma \cap S'|S') = \frac{1}{2}.$$

Proof. Define

$$\Pi_N := \{\mathfrak{p} : \text{principal prime ideals of } O_K \text{ st. } \text{Norm}_{K/\mathbb{Q}}(\mathfrak{p}) < N\}.$$

$$\Lambda_{\sigma,N} := \{\mathfrak{p} \in \Pi_N : \text{spin}(\mathfrak{p}, \sigma) = 1\}.$$

where $\sigma \in \text{Gal}(K/\mathbb{Q})$ is non-trivial. Then we want to show

$$\lim_{N\to\infty} \frac{\#\Lambda_{\sigma,N}}{\#\Pi_N} = \frac{1}{2}.$$

By Theorem 3.3.1, the following limit is bounded above;

$$\lim_{x\to\infty} \frac{\left|\sum_{\mathbb{N}(\mathfrak{p})\le x} \text{spin}(\mathfrak{p}, \sigma)\right|}{x^{1-\nu+\epsilon}} \le 1.$$

Therefore, since

$$\lim_{x\to\infty} \frac{x^{1-\nu+\epsilon}}{\left(\frac{x}{\log(x)}\right)} = 0,$$

we can deduce that the limit of the product is 0. That is,

$$\lim_{x\to\infty} \frac{\left|\sum_{\mathbb{N}(\mathfrak{p})\le x} \text{spin}(\mathfrak{p}, \sigma)\right|}{\left(\frac{x}{\log(x)}\right)} = 0.$$

The prime number theorem says that

$$\lim_{x\to\infty} \frac{\#\Pi_x}{\left(\frac{x}{\log(x)}\right)} = 1$$

so applying the prime number theorem, we get

$$\lim_{x\to\infty} \frac{\left|\sum_{\mathbb{N}(\mathfrak{p})\leq x} \text{spin}(\mathfrak{p},\sigma)\right|}{\#\Pi_x} = 0. \tag{3.1}$$

Observe that

$$\sum_{\mathbb{N}(\mathfrak{p})\leq x} \text{spin}(\mathfrak{p},\sigma) = \sum_{\mathfrak{p}\in\Lambda_{\sigma,x}} 1 + \sum_{\mathfrak{p}\in\Pi_x-\Lambda_{\sigma,x}} (-1) = \#\Lambda_{\sigma,x} - \#(\Pi_x - \Lambda_{\sigma,x})$$

$$= 2\#\Lambda_{\sigma,x} - \#\Pi_x.$$

Subbing $\sum_{\mathbb{N}(\mathfrak{p})\leq x} \text{spin}(\mathfrak{p},\sigma) = 2\#\Lambda_{\sigma,x} - \#\Pi_x$ to equation 3.1, we get

$$\lim_{x\to\infty} \left|\frac{2\#\Lambda_{\sigma,x} - \#\Pi_x}{\#\Pi_x}\right| = 0.$$

Therefore

$$d(\Lambda_\sigma|\Pi) == \frac{1}{2}.$$

By Theorem 3.3.2,

$$d(\Lambda_\sigma \cap S'|S') = d(\Lambda_\sigma|\Pi).$$

□

3.4 Quadratic Reciprocity

The proof of Lemma 3.1.2 used Hilbert Symbols to prove that the condition

$$\text{spin}(\mathfrak{p},\sigma) = \text{spin}(\mathfrak{p},\sigma^{-1})$$

is equivalent to a Hilbert symbol condition at places dividing 2. This next Theorem uses a similar strategy to prove a quadratic-reciprocity style result, this

time invoking the map $\mathbf{v}_K$ from Definition 2.2.3 instead of using totally positive elements.

Theorem 3.4.1. *Let $K := K(n, \ell)$. Let $\mathfrak{p}$ be an odd prime of K such that $\mathfrak{p}^{h(K)}$ has totally positive generator $\alpha \in O_K$. Let $\sigma \neq 1 \in \mathrm{Gal}(K/\mathbb{Q})$. Let $u := \mathbf{v}_K(\mathfrak{p})$. Then*

$$\left(\frac{u\alpha}{\mathfrak{p}^\sigma}\right) = \left(\frac{\alpha^\sigma}{\mathfrak{p}}\right).$$

Proof. It is a property of Hilbert symbols that

$$\prod_v (u\alpha, \alpha^\sigma)_v = 1$$

as we vary v over all places of K. Let $K_{(v)}$ denote the completion of K at v. Our strategy will be to prove that

$$(u\alpha, \alpha^\sigma)_v = 1 \quad \text{for all places } v \neq \mathfrak{p}, \mathfrak{p}^\sigma. \tag{3.2}$$

We then show that

$$(u\alpha, \alpha^\sigma)_{\mathfrak{p}} = \left(\frac{\alpha^\sigma}{\mathfrak{p}}\right) \quad \text{and}$$
$$(u\alpha, \alpha^\sigma)_{\mathfrak{p}^\sigma} = \left(\frac{u\alpha}{\mathfrak{p}^\sigma}\right)$$

which proves the result.

Recall that $(a, b)_v := 1$ for $a, b \in K$ if the equation $ax^2 + by^2 = z^2$ has a nontrivial solution $(x, y, z) \in K_{(v)}$ where at least one of x, y, or z is nonzero and $(a, b)_v := -1$ otherwise.

First consider the infinite places. Since α^σ is totally positive, $u\alpha x^2 + \alpha^\sigma y^2 = z^2$ always has the solution $(x, y, z) = (0, 1, \sqrt{\alpha^\sigma})$ in $K_{(v)} = \mathbb{R}$ so 3.2 is proven for all infinite places.

Next let $\mathfrak{q}$ be any finite place away from 2, $\mathfrak{p}$, $\mathfrak{p}^\sigma$. We will show that $u\alpha x^2 + \alpha^\sigma y^2 \equiv 1 \bmod \mathfrak{q}$ has a nontrivial solution in $\mathcal{O}_K/\mathfrak{q}$ using the pigeon hole principal and then we will apply Hensel's Lemma.

We want to show there exist $x, y \in \mathcal{O}_K/\mathfrak{q}$ such that

$$u\alpha x^2 \equiv 1 - \alpha^\sigma y^2 \bmod \mathfrak{q}. \tag{3.3}$$

Since $\mathfrak{q} \neq \mathfrak{p}, \mathfrak{p}^\sigma$, then $u\alpha, \alpha^\sigma \not\equiv 0 \bmod \mathfrak{q}$. Then there are $\frac{\mathrm{Norm}(\mathfrak{q})+1}{2}$ squares in $\mathcal{O}_K/\mathfrak{q}$ so the left hand side and the right hand side each take on $\frac{\mathrm{Norm}(\mathfrak{q})+1}{2}$ values. The pigeon-hole principal implies there is a solution, $x, y \in \mathcal{O}_K/\mathfrak{q}$ to equation 3.3.

Note that it can not be the case that $x = y = 0$. If $x \not\equiv 0 \bmod \mathfrak{q}$ then $x^2 - \frac{1-\alpha^\sigma y^2}{u\alpha} \equiv 0 \bmod \mathfrak{q}$. Then since $\mathfrak{q} \neq 2$ and $x \not\equiv 0$, Hensel's Lemma implies there exists $x \in \mathcal{O}_{K_{(\mathfrak{q})}}$ such that $x^2 = \frac{1-\alpha^\sigma y^2}{u\alpha}$. Setting $z = 1$, we have $(u\alpha, \alpha^\sigma)_\mathfrak{q} = 1$. If y is nonzero, a similar argument works.

Recall that 2 is inert in $K/\mathbb{Q}$ by assumption. We now prove that equation 3.2 holds for $v = 2$. Let $L := K_{(2)}(\sqrt{u\alpha})$. Note that $K(\sqrt{u\alpha})$ is a subfield of the narrow ray class field over K of conductor $\mathfrak{p}$ by the definition of $u = \mathbf{v}_K(\mathfrak{p})$ so 2 is unramified in L/K.

If 2 splits in $L/K_{(2)}$ then $u\alpha$ is a square in $K_{(2)}$ so $u\alpha x^2 + \alpha^\sigma y^2 = z^2$ has the solution $(x, y, z) = (0, 1, \sqrt{\alpha^\sigma})$ in $K_{(2)}$.

Otherwise 2 is inert in $L/K_{(2)}$. Then by Corollary V.1.2 in [13],

$$\mathrm{Norm}_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_{K_{(2)}}^\times$$

so α^σ is a norm in L, a quadratic extension of K. That is, there exist $x, z \in K_{(2)}$ such that

$$\alpha^\sigma = z^2 - u\alpha x^2,$$

which implies that equation 3.2 is true for $v = 2$.

We have proven equation 3.2 holds for all places away from $\mathfrak{p}$ and $\mathfrak{p}^\sigma$ so since the product of Hilbert symbols over all places is 1,

$$(u\alpha, \alpha^\sigma)_{\mathfrak{p}}(u\alpha, \alpha^\sigma)_{\mathfrak{p}^\sigma} = 1.$$

It is a standard fact of Hilbert symbols that

$$(u\alpha, \alpha^\sigma)_{\mathfrak{p}} = \left(\frac{\alpha^\sigma}{\mathfrak{p}}\right) \quad \text{and}$$
$$(u\alpha, \alpha^\sigma)_{\mathfrak{p}^\sigma} = \left(\frac{u\alpha}{\mathfrak{p}^\sigma}\right)$$

because α^σ is a generator of $\mathfrak{p}^\sigma$ and $u\alpha$ is a generator of $\mathfrak{p}$. This completes the proof that

$$\left(\frac{u\alpha}{\mathfrak{p}^\sigma}\right) = \left(\frac{\alpha^\sigma}{\mathfrak{p}}\right).$$

□

CHAPTER 4

THE DENSITY OF A SPIN RELATION

The gestalt of this Chapter is Theorem 4.5.2 which gives the "surprising" part of the formula in Theorem 5.4.3. The work in this Chapter is available as a preprint [9] and is pending publication. Inspired by the statement of Lemma 3.1.2 in [6], to define M_4, I imagined sculpting a group with a Galois action by quotienting as I saw intuitively fit in order to be left only with the properties of the Hilbert symbol we wanted to preserve. The units of a number field were the clay and the Hilbert symbol was the chisel.

4.1 An Important Group; M_4

Recall that $K(n, \ell)$ denotes the number field of prime degree n over $\mathbb{Q}$ that is the unique subextension of the ℓ^{th} cyclotomic field of degree n where $\ell \in \mathbb{Z}_+$ such that $\ell \equiv 1 \bmod n$. We highlight some important assumptions and properties of $K := K(n, \ell)$;

* K is totally real.
* $n = [K : \mathbb{Q}]$ is prime.
* $U_T = U^2$.
* K is Galois over $\mathbb{Q}$ with cyclic Galois group.
* The class number $h(K)$ is odd.
* 2 and 5 are inert in $K/\mathbb{Q}$.

Definition 4.1.1. *For q a power of 2, we define the group*

$$M_q := \left(\mathcal{O}_K/q\mathcal{O}_K\right)^\times \Big/ \left(\left(\mathcal{O}_K/q\mathcal{O}_K\right)^\times\right)^2.$$

The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ *acts on* M_q *in the natural way.*

We will primarily be interested in M_4, though we will also consider M_8. We will see in Remark 4.2.3 that M_4 is a quotient of the narrow ray class group over K of conductor 4.

Lemma 4.1.2. *Let K be a cyclic number field of odd degree n over $\mathbb{Q}$ such that 2 is inert in K. Then as* $\mathrm{Gal}(K/\mathbb{Q})$*-modules,*

$$M_4 \cong (\mathbb{Z}/2)^n$$

and the invariants of the action of $\mathrm{Gal}(K/\mathbb{Q})$ *are exactly* $\pm 1 \in M_4$.

Proof. This proof is due to Sam Mundy [12]. Consider the exact sequence

$$0 \to 1 + 2(\mathcal{O}_K/4) \to (\mathcal{O}_K/4)^\times \to (\mathcal{O}_K/2)^\times \to 1. \tag{4.1}$$

Note that $\mathcal{O}_K/2 \cong \mathbb{F}_{2^n}$ because K is cyclic of odd degree and 2 is inert in K. Also, $G \cong \mathrm{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2)$.

Viewing $\mathbb{F}_{2^n}$ as an additive group with Galois action by $G \cong \mathrm{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2)$, there is an isomorphism of Galois modules given by

$$\psi : \mathbb{F}_{2^n} \cong \mathcal{O}_K/2 \to 1 + 2(\mathcal{O}_K/4)$$

$$\psi : x \mapsto 1 + 2x.$$

This map is easily seen to be a Galois equivariant homomorphism. Injectivity and surjectivity follow from considering 2-adic expansions of elements in $\mathcal{O}_K/4$.

Since ψ is an isomorphism we can rewrite the exact sequence of Galois modules in equation 4.1 as

$$0 \to \mathbb{F}_{2^n} \to (\mathcal{O}_K/4)^\times \to \mathbb{F}_{2^n}^\times \to 1. \tag{4.2}$$

Next consider the diagram of exact sequences below.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{F}_{2^n} & \longrightarrow & (\mathcal{O}_K/4)^\times & \longrightarrow & \mathbb{F}_{2^n}^\times & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle 2(\cdot)} & & \downarrow{\scriptstyle (\cdot)^2} & & \downarrow{\scriptstyle (\cdot)^2} & & \\
0 & \longrightarrow & \mathbb{F}_{2^n} & \longrightarrow & (\mathcal{O}_K/4)^\times & \longrightarrow & \mathbb{F}_{2^n}^\times & \longrightarrow & 1
\end{array}$$

The first vertical map is multiplication by 2, which is the zero map. The next two vertical maps are squaring. The third vertical map is an isomorphism because $\mathbb{F}_{2^n}^\times$ is cyclic of odd order. Recall that

$$M_4 := (\mathcal{O}_K/4\mathcal{O}_K)^\times \text{/squares}.$$

Then we apply the snake lemma to the diagram below.

$$\begin{array}{ccccccccc}
 & & & & & & 1 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & \mathbb{F}_{2^n} & \longrightarrow & (\mathcal{O}_K/4)^\times & \longrightarrow & \mathbb{F}_{2^n}^\times & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle (\cdot)^2} & & \downarrow{\scriptstyle (\cdot)^2} & & \\
0 & \longrightarrow & \mathbb{F}_{2^n} & \longrightarrow & (\mathcal{O}_K/4)^\times & \longrightarrow & \mathbb{F}_{2^n}^\times & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathbb{F}_{2^n} & \longrightarrow & M_4 & \longrightarrow & 1 & &
\end{array}$$

The snake lemma gives us the exact sequence of G-modules

$$0 \to \mathbb{F}_{2^n} \to M_4 \to 1.$$

Therefore $M_4 \cong \mathbb{F}_{2^n}$ as G-modules. The invariants of $\mathbb{F}_{2^n}$ are $\mathbb{F}_2$. Tracing through the isomorphism we see that this corresponds to the invariants $\{\pm 1\}$ in M_4. $\square$

4.2 A Surprising Homomorphism

Recall the properties satisfied by $K := K(n, \ell)$ listed in definition 2.2.1. Let $\mathbb{M}_{q,G}$ denote the set of $\mathrm{Gal}(K/\mathbb{Q})$-orbits of M_q for q a power of 2.

Letting $\mathfrak{m}$ denote a narrow modulus with finite part $\mathfrak{m}_0$, as in Section 1.1, let $J_K^{\mathfrak{m}} = J_K^{\mathfrak{m}_0}$ denote the group of fractional ideals of K prime to $\mathfrak{m}_0$ and let $P_K^{\mathfrak{m}} = P_K^{\mathfrak{m}_0}$ denote the subgroup of $J_K^{\mathfrak{m}}$ formed by the principal ideals with generator $\alpha \in K^\times$ such that $\alpha \equiv^* 1 \bmod \mathfrak{m}$. Note that since $\mathfrak{m}$ is assumed narrow, $\alpha \equiv^* 1 \bmod \mathfrak{m} \implies \alpha \succ 0$. We let $\mathscr{P}_K^{\mathfrak{m}} = \mathscr{P}_K^{\mathfrak{m}_0}$ denote the set of prime ideals of O_K co-prime to $\mathfrak{m}_0$ so that $J_K^{\mathfrak{m}}$ is generated by $\mathscr{P}_K^{\mathfrak{m}}$.

Definition 4.2.1. *Let $K := K(n, \ell)$. Let $q \geq 4$ be a power of 2.*

(a) Let $\mathscr{P}_K^2$ denote the set of primes of K which are co-prime to 2.

$$\begin{aligned} \mathbf{r}_0 : \mathscr{P}_K^2 &\to M_q \\ \mathfrak{p} &\mapsto \alpha \end{aligned}$$

where $\alpha \in O_K$ is a totally positive generator for the principal ideal $\mathfrak{p}^{h(K)}$.

(b) Let $\mathscr{P}_{\mathbb{Q}}^2$ denote the set of odd rational primes. Define the map

$$\begin{aligned} \mathbf{r} : \mathscr{P}_{\mathbb{Q}}^2 &\to \mathbb{M}_{q,G} \\ p &\mapsto [\mathbf{r}_0(\mathfrak{p})] \end{aligned}$$

where $\mathfrak{p}$ is any prime in K above p. Here $[\alpha]$ denotes the $\mathrm{Gal}(K/\mathbb{Q})$-orbit of $\alpha \in M_4$ considered in $\mathbb{M}_{q,G}$.

The map $\mathbf{r}_0$ is well-defined out of $\mathscr{P}_K^2$; recall that by Lemma 2.1.1, $U_T = U^2$ is equivalent to the coincidence of the narrow and wide Hilbert class groups so $U_T = U^2$ if and only if all principal ideals have a totally positive generator. Since squares are trivial in M_q by definition and $U_T = U^2$, the map $\mathbf{r}_0$ is well-defined.

The map $\mathbf{r}$ is well-defined out of $\mathscr{P}_{\mathbb{Q}}^2$ because $\mathbb{M}_{q,G}$ is the quotient of M_q by the $\mathrm{Gal}(K/\mathbb{Q})$-action so different choices of primes $\mathfrak{p}$ of K above p give the same result; $\mathbf{r}_0(\mathfrak{p}^\sigma) = \mathbf{r}_0(\mathfrak{p})^\sigma$ for $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and $\mathfrak{p}$ an odd prime of K.

The map

$$\mathbf{r}_0 : \mathscr{P}_K^2 \to M_q$$

sends primes $\mathfrak{p} \in \mathscr{P}_K^2$ to the congruence class in M_q corresponding to a totally positive generator of $\mathfrak{p}^{h(K)}$. Since J_K^q is generated by $\mathscr{P}_K^q = \mathscr{P}_K^2$, the map $\mathbf{r}_0$ induces a homomorphism

$$\varphi_0 : J_K^q \to M_q.$$

Lemma 4.2.2. *Let $K := K(n, \ell)$. Then the homomorphism $\varphi_0 : J_K^q \to M_q$ induces a well-defined surjective homomorphism*

$$\varphi : \mathrm{nCl}_K^q \twoheadrightarrow M_q.$$

Proof. By Proposition 1.1.3, every element of nCl^q is represented by an integral ideal. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two integral ideals representing the same element of nCl^q. Then by Proposition 1.1.3, there exist nonzero $a, b \in O_K$ such that

$$b\mathfrak{a} = a\mathfrak{b},$$

$$a \equiv b \equiv 1 \bmod q, \quad \text{and}$$

$$ab \succ 0.$$

Since $\varphi_0 : J_K^q \to M_q$ is a homomorphism,

$$\varphi_0(b\mathcal{O}_K)\varphi_0(\mathfrak{a}) = \varphi_0(a\mathcal{O}_K)\varphi_0(\mathfrak{b}).$$

Noting that $h(K)$ is odd and squares are trivial in M_q by definition, φ_0 maps any principal integral ideal (α) to the class in M_q containing the representative $\alpha \in \mathcal{O}_K$ where α is a totally positive generator.

Since $U_T = U^2$, every principal ideal of $\mathcal{O}_K$ has a totally positive generator so there exists a unit $u \in \mathcal{O}_K^\times$ such that $ua \succ 0$ and $\varphi_0(a) = ua$. Since $ab \succ 0$, then $u^{-1}b \succ 0$ so $\varphi_0(b) = u^{-1}b$. We know that $a \equiv b \equiv 1 \bmod q$. Since squares are trivial in M_q by the definition of M_q, this implies

$$\begin{aligned} & u^2 a \equiv b \quad \text{in } M_q \\ \implies & ua \equiv u^{-1}b \quad \text{in } M_q \\ \implies & \varphi_0(a\mathcal{O}_K) = \varphi_0(b\mathcal{O}_K). \\ \implies & \varphi_0(\mathfrak{a}) = \varphi_0(\mathfrak{b}) \end{aligned}$$

Therefore the homomorphism φ_0 induces a well-defined homomorphism from nCl_K^q.

We now show surjectivity. Let $X \in M_q$. Let $\mathfrak{m}$ be the narrow modulus with finite part q and consider the exact sequence from Theorem 1.1.4;

$$1 \to U/U_{\mathfrak{m},1} \to K_\mathfrak{m}/K_{\mathfrak{m},1} \to \mathrm{nCl}_K^\mathfrak{m} \to C \to 1$$

and the canonical isomorphism

$$K_\mathfrak{m}/K_{\mathfrak{m},1} \cong (\pm)^n \times (\mathcal{O}_K/q)^\times . \tag{4.3}$$

Consider only the 2-part of each group. Then since $h(K)$ is odd, by Lemma

A.0.1 we have the short exact sequence

$$1 \to (U/U_{\mathfrak{m},1})[2^\infty] \to (K_\mathfrak{m}/K_{\mathfrak{m},1})[2^\infty] \to (\mathrm{n}Cl_K^{\mathfrak{m}})[2^\infty] \to 1.$$

Note that since squaring sends all signatures to the trivial signature, the canonical isomorphism in equation 4.3 induces a canonical isomorphism on the 2-part modulo squares;

$$(K_\mathfrak{m}/K_{\mathfrak{m},1})[2^\infty]/(K_\mathfrak{m}/K_{\mathfrak{m},1})[2^\infty]^2 \cong (\pm)^n \times M_q.$$

Consider the squaring map and apply the snake lemma to get the following commutative diagram of exact sequences;

$$\begin{array}{ccccccccc}
1 & \longrightarrow & (U/U_{\mathfrak{m},1})[2^\infty] & \longrightarrow & (K_\mathfrak{m}/K_{\mathfrak{m},1})[2^\infty] & \longrightarrow & (\mathrm{n}Cl_K^q)[2^\infty] & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle (\cdot)^2} & & \downarrow{\scriptstyle (\cdot)^2} & & \downarrow{\scriptstyle (\cdot)^2} & & \\
1 & \longrightarrow & (U/U_{\mathfrak{m},1})[2^\infty] & \longrightarrow & (K_\mathfrak{m}/K_{\mathfrak{m},1})[2^\infty] & \longrightarrow & (\mathrm{n}Cl_K^q)[2^\infty] & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & U/U^2 & \longrightarrow & (\pm)^n \times M_q & \xrightarrow{\psi} & \mathrm{n}Cl_K^q/(\mathrm{n}Cl_K^q)^2 & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

Then ψ induces an isomorphism

$$\psi : {}^{((\pm)^n \times M_q)}\!/_{\mathrm{image}(U/U^2)} \longrightarrow {}^{\mathrm{n}Cl_K^q}\!/_{(\mathrm{n}Cl_K^q)^2}.$$

Tracing through the definitions of the maps, $\varphi \circ \psi$ is surjective (it is essentially the identity). Therefore φ is surjective. □

Remark 4.2.3. *For* $K := K(n, \ell)$,

$$\varphi : \mathrm{n}Cl_K^4 \to M_4$$

is a canonical surjective homomorphism with

$$\#\ker(\varphi) = \frac{h(2^n - 1)}{(U^2 : U_{\mathfrak{m},1})}$$

where $\mathfrak{m}$ *denotes the narrow modulus of finite part 4.*

Proof. Lemma 4.2.2 shows that $\varphi : \mathrm{n}Cl_K^4 \to M_4$ is a well-defined surjective group homomorphism.

We let $\mathfrak{m}$ denote the narrow modulus with finite part 4 and $h_{\mathfrak{m}} := \#\mathrm{n}Cl_K^4$. Recall that $K(n, \ell)$ is totally real by assumption and 2 is inert so $\mathrm{Norm}(2) = 2^n$ and by Theorem 1.1.4,

$$h_{\mathfrak{m}} = 4^n \frac{h(2^n - 1)}{(U : U_{\mathfrak{m},1})}$$

Also recall that $U_T = U^2$ for $K(n, \ell)$ so

$$(U : U_{\mathfrak{m},1}) = (U : U^2)(U^2 : U_{\mathfrak{m},1}) = 2^n(U^2 : U_{\mathfrak{m},1}).$$

Therefore

$$h_{\mathfrak{m}} = 2^n \frac{h(2^n - 1)}{(U^2 : U_{\mathfrak{m},1})}.$$

Since $\varphi : \mathrm{n}Cl_K^4 \to M_4$ is a well-defined surjective finite group homomorphism,

$$\frac{h_{\mathfrak{m}}}{\#\ker(\varphi)} = \#M_4$$

Recall that Lemma 4.1.2 shows $\#M_4 = 2^n$. Therefore

$$\begin{aligned} \#\ker(\varphi) &= \frac{h_{\mathfrak{m}}}{2^n} \\ &= \frac{h(2^n - 1)}{(U^2 : U_{\mathfrak{m},1})} \end{aligned}$$

proving our second assertion. (In particular, we have proven that $(U^2 : U_{\mathfrak{m},1})$ divides $h(2^n - 1)$). □

Example 4.2.4. *Let $K = \mathbb{Q}$. Then $U/U^2 = \{\pm 1\}$. For p an odd prime, $\mathrm{nR}_{\mathbb{Q}}^{p} = \mathbb{Q}(\zeta_p)$, the p^{th} cyclotomic field, and $\mathrm{nCl}_{\mathbb{Q}}^{4} \cong (\mathbb{Z}/4)^{\times}$.*

When $K = \mathbb{Q}$ and $\mathfrak{q} = 4$, Remark 4.2.3 implies that φ from Lemma 4.2.2 is an isomorphism.

Letting p be a positive odd prime, then

$$\mathbf{v}_{\mathbb{Q}} : p \mapsto \begin{cases} 1 & \text{if } p \text{ is a square in } \mathbb{Q}(\zeta_p) \\ -1 & \text{if } -p \text{ is a square in } \mathbb{Q}(\zeta_p). \end{cases}$$

One can show that this is equivalent to

$$\mathbf{v}_{\mathbb{Q}} : p \mapsto \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv -1 \bmod 4. \end{cases}$$

4.3 Equidistribution

Definition 4.3.1. *Let $K = K(n, \ell)$. Define the following sets of rational primes.*

$$S := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : f_{K/\mathbb{Q}}(p) = 1\},$$
$$I := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : f_{K/\mathbb{Q}}(p) = n\}.$$

Define the following sets of primes of K.

$$S' := \{\mathfrak{p} \in \mathscr{P}_{K}^{2\ell} : f_{K/\mathbb{Q}}(\mathfrak{p}) = 1\},$$
$$I' := \{\mathfrak{p} \in \mathscr{P}_{K}^{2\ell} : f_{K/\mathbb{Q}}(\mathfrak{p}) = n\}.$$

That is, $S \subseteq \mathscr{P}_{\mathbb{Q}}^{2\ell}$ is the set of (odd) rational primes which split completely in $K/\mathbb{Q}$ and $I \subseteq \mathscr{P}_{\mathbb{Q}}^{2\ell}$ is the set of odd rational primes which are inert in $K/\mathbb{Q}$. Furthermore, S' is the set of primes of K laying above the primes in S and I' is the set of primes of K laying above the primes in I.

Note that since $K/\mathbb{Q}$ is cyclic of prime degree n, then $f_{K/\mathbb{Q}}(p) = 1$ or n for all $p \in \mathscr{P}_{\mathbb{Q}}^{2\ell}$ so in this case, $\mathscr{P}_{\mathbb{Q}}^{2\ell}$ is the disjoint union of S and I. The next Lemma asserts that for $K := K(n, \ell)$, the primes are equidistributed in M_4. Although the equidistribution generalizes to M_q for q a power of 2, note that the number of elements of M_8 for example is different than the number of elements of M_4 so the generalized statement would need to be adjusted accordingly.

Lemma 4.3.2. *Let $K := K(n, \ell)$.*

(a) For any $\alpha \in M_4$, the density of $\mathfrak{p} \in \mathscr{P}_K^{2\ell}$ such that $\varphi(\mathfrak{p}) = \alpha$ is $\frac{1}{2^n}$. That is,

$$d(\mathbf{r}_0^{-1}(\alpha)|\mathscr{P}_K^{2\ell}) = \frac{1}{\#M_4} = \frac{1}{2^n}.$$

(b) Furthermore, the density does not change when we restrict to primes of K that split completely in $K/\mathbb{Q}$. That is,

$$d(\mathbf{r}_0^{-1}(\alpha) \cap S'|S') = \frac{1}{\#M_4} = \frac{1}{2^n}.$$

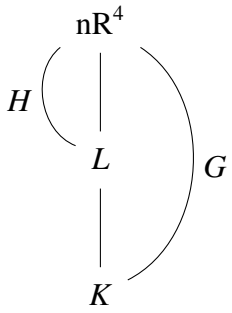
Proof. Recall that $\mathrm{nR}^4 = \mathrm{nR}_K^4$ denotes the narrow ray class field over K of conductor $4\mathfrak{m}_\infty$. Let $G := \mathrm{Gal}(\mathrm{nR}^4/K)$. Define $H \leq G$ to be

$$H := \mathrm{Art}(\ker(\varphi))$$

where Art denotes the Artin isomorphism. Then we have the following commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \ker(\varphi) & \longrightarrow & \mathrm{nCl}^4 & \xrightarrow{\varphi} & M_4 & \longrightarrow & 1 \\ & & \downarrow \mathrm{Art} & & \downarrow \mathrm{Art} & & \downarrow \mathrm{id.} & & \\ 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & M_4 & \longrightarrow & 1 \end{array}$$

where surjectivity of φ is proven in Lemma 4.2.2. Let L be the fixed field of H so that $\mathrm{Gal}(L/K) \cong G/H$.



This induces a canonical isomorphism

$$M_4 \cong G/H \cong \mathrm{Gal}(L/K).$$

For $\alpha \in M_4$, define $P(\alpha)$ to be the set of odd unramified prime ideals of K which map to α via φ. Then letting $\sigma \in G/H$ corresponding to α,

$$P(\alpha) = \mathrm{Ray}_{L|K}(\sigma).$$

Then by Theorem 1.4.2, $P(\alpha)$ has a density and it is given by

$$\frac{1}{\#\,\mathrm{Gal}(L/K)} = \frac{1}{\#M_4}.$$

The first asserted equality of part (a) is proved. The second equality is true by Lemma 4.1.2.

To prove part (b), observe that

$$d(\mathbf{r}_0^{-1}(\alpha)|\mathscr{P}_K^{2\ell}) = d(\mathbf{r}_0^{-1}(\alpha) \cap S'|S')d(S'|\mathscr{P}_K^{2\ell}) + d(\mathbf{r}_0^{-1}(\alpha) \cap I'|I')d(I'|\mathscr{P}_K^{2\ell}).$$

Since $d(S'|\mathscr{P}_K^{2\ell}) = 1$, $d(I'|\mathscr{P}_K^{2\ell}) = 0$, and $0 \leq d(\mathbf{r}_0^{-1}(\alpha) \cap I'|I') \leq 1$,

$$d(\mathbf{r}_0^{-1}(\alpha)|\mathscr{P}_K^{2\ell}) = d(\mathbf{r}_0^{-1}(\alpha) \cap S'|S').$$

□

4.4 Property Star and the Starlight invariant

Let $K := K(n, \ell)$. Recall the map $\mathbf{v}_K$ defined in Definition 2.2.3,

$$\mathbf{v}_K : \mathscr{P}_K^2 \to {}^{U}\!/_{U^2}$$
$$\mathfrak{p} \mapsto u_{\mathfrak{p}}$$

such that $u_{\mathfrak{p}}\alpha_{\mathfrak{p}}$ is a square (element) in $\mathrm{nR}_K^{\mathfrak{p}}$ where $\alpha_{\mathfrak{p}} \in \mathcal{O}_K$ is a totally positive generator of $\mathfrak{p}$. Recall the definition of spin from Definition 3.1.1.

Theorem 4.4.1. *Let $K := K(n, \ell)$. Let $\mathfrak{p}$ be a prime of K coprime to 2 such that $\mathfrak{p}^{h(K)}$ has totally positive generator $\alpha \in \mathcal{O}_K$. Let σ be a generator of the Galois group, $Gal(K/\mathbb{Q})$. Then the following are equivalent.*

(a) $\mathrm{spin}(\mathfrak{p}, \sigma) = \mathrm{spin}(\mathfrak{p}, \sigma^{-1})$

(b) $(\alpha, \alpha^{\sigma})_2 = 1$

(c) $\left(\frac{\mathbf{v}_K(\mathfrak{p})^{\sigma}}{\mathfrak{p}}\right) = 1$

Proof. Part (a) is equivalent to part (b) by Lemma 3.1.2. We will prove that part (a) is also equivalent to part (c).

Observe that if $\sigma \neq \tau \in \mathrm{Gal}(K/\mathbb{Q})$, then $\mathrm{spin}(\mathfrak{p}, \sigma) = \mathrm{spin}(\mathfrak{p}^{\tau}, \sigma)$;

$$\mathrm{spin}(\mathfrak{p}, \sigma) = \left(\frac{\alpha}{\mathfrak{p}^{\sigma}}\right) = \left(\frac{\alpha^{\tau}}{\mathfrak{p}^{\tau\sigma}}\right) = \mathrm{spin}(\mathfrak{p}^{\tau}, \sigma).$$

Therefore

$$\mathrm{spin}(\mathfrak{p}, \sigma^{-1}) = \mathrm{spin}(\mathfrak{p}^{\sigma}, \sigma^{-1}) = \left(\frac{\alpha^{\sigma}}{\mathfrak{p}^{\sigma\sigma^{-1}}}\right) = \left(\frac{\alpha^{\sigma}}{\mathfrak{p}}\right).$$

Then

$$\begin{aligned}\operatorname{spin}(\mathfrak{p},\sigma)\operatorname{spin}(\mathfrak{p},\sigma^{-1}) &= \left(\frac{\alpha}{\mathfrak{p}^{\sigma}}\right)\left(\frac{\alpha^{\sigma}}{\mathfrak{p}}\right)\\ &= \left(\frac{\mathbf{v}_K(\mathfrak{p})}{\mathfrak{p}^{\sigma}}\right) \quad \text{by Theorem 3.4.1}\\ &= \left(\frac{\mathbf{v}_K(\mathfrak{p})^{\sigma^{-1}}}{\mathfrak{p}}\right).\end{aligned}$$

By Lemma 3.1.2 and since 2 is inert in $K/\mathbb{Q}$,

$$\operatorname{spin}(\mathfrak{p},\sigma)\operatorname{spin}(\mathfrak{p},\sigma^{-1}) = (\alpha,\alpha^{\sigma})_2 = \left(\alpha^{\sigma^{-1}},\alpha\right)_2 = \left(\alpha,\alpha^{\sigma^{-1}}\right)_2.$$

We have shown that

$$(\alpha,\alpha^{\sigma^{-1}})_2 = \left(\frac{\mathbf{v}_K(\mathfrak{p})^{\sigma^{-1}}}{\mathfrak{p}}\right).$$

Replacing σ^{-1} with σ and vise versa, we obtain a proof of the desired statement.

□

Recall that $\mathbb{M}_{4,G}$ denotes the set of $\mathrm{Gal}(K/\mathbb{Q})$-orbits of M_4.

Theorem 4.4.2. *Let $K := K(n,\ell)$. Assume 5 is inert in $K/\mathbb{Q}$. Let $\alpha \in O_K$ denote a representative of $[\alpha] \in \mathbb{M}_{4,G}$. Define the map*

$$\begin{aligned}\star : \mathbb{M}_{4,G} &\to \{\pm 1\}\\ [\alpha] &\mapsto \begin{cases} 1 & \text{if } (\alpha,\alpha^{\sigma})_2 = 1 \text{ for all non-trivial } \sigma \in \mathrm{Gal}(K/\mathbb{Q})\\ -1 & \text{otherwise}\end{cases}\end{aligned}$$

Then $\star$ is a well-defined map.

Proof. We will show that $\star$ is well-defined out of M_4. Then we show $\star$ is a property of the full Galois orbit.

Let $\alpha, \beta \in O_K$ be two representatives of the same class in M_4 so

$$\alpha \equiv \beta\gamma^2 \bmod 4O_K \quad \text{for some } \gamma \in O_K.$$

If $\alpha \equiv \beta\gamma^2 \bmod 8O_K$ then we can apply Lemma 2.3 from [6] to see that $(\alpha, \alpha^\sigma)_2 = (\beta, \beta^\sigma)_2$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Therefore, we may assume

$$\alpha \equiv 5\beta\gamma^2 \bmod 8O_K.$$

Suppose $(\alpha, \alpha^\sigma)_2 = 1$. Then by Lemma 2.3 in [6], since $\alpha \equiv 5\beta\gamma^2 \bmod 8O_K$,

$$\begin{aligned} &\left(5\beta\gamma^2, \left(5\beta\gamma^2\right)^\sigma\right)_2 = 1 \\ \implies &(5\beta, (5\beta)^\sigma)_2 = 1 \quad \text{by a property of Hilbert symbols.} \end{aligned}$$

Using bimultiplicativity of the Hilbert symbol,

$$(5\beta, (5\beta)^\sigma)_2 = (5,5)_2(\beta,5)_2(5,\beta^\sigma)_2(\beta,\beta^\sigma)_2.$$

Notice that since 5 is inert in $K/\mathbb{Q}$, applying the Galois action to the quadratic form for $(\beta, 5)_2$ yields the form for $(5, \beta^\sigma)_2$ so the cross terms cancel one another. Therefore

$$(5\beta, (5\beta)^\sigma)_2 = (5,5)_2(\beta,\beta^\sigma)_2.$$

Since $5 \times 2^2 + 5 \times 1^2 = 5^2$, $(5,5)_2 = 1$. Therefore

$$(5\beta, (5\beta)^\sigma)_2 = (\beta, \beta^\sigma)_2$$

so

$$(\alpha, \alpha^\sigma)_2 = 1 \implies (\beta, \beta^\sigma)_2 = 1.$$

Therefore $\star$ is a well-defined map from M_4.

We now prove that if $\alpha, \beta \in M_4$ are the in same Galois orbit, then $\star(\alpha) = \star(\beta)$. Let $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\alpha^\tau = \beta$ for $\alpha, \beta \in M_4$.

Suppose $(\alpha, \alpha^\sigma)_2 = 1$ for all $\sigma \neq 1$ in $\mathrm{Gal}(K/\mathbb{Q})$. Then in $K_{(2)}$, the completion of K at $2\mathcal{O}_K$, there is a nontrivial solution x, y, z to

$$\alpha x^2 + \alpha^\sigma y^2 = z^2.$$

Applying the action of τ yields a nontrivial solution to

$$\beta x^2 + \beta^\sigma y^2 = z^2$$

so $(\beta, \beta^\sigma) = 1$ for all $\sigma \neq 1$. □

Recall that by Lemma 4.1.2, the elements of M_4 that are invariant under the $\mathrm{Gal}(K/\mathbb{Q})$-action are exactly ± 1. The following lemma fully describes $\star$ on these invariants.

Lemma 4.4.3. *Let* $K := K(n, \ell)$.

(a) $\star(1) = 1$.

(b) $\star(-1) = -1$.

Proof. Observe that $(1, 1)_2 = 1$ because $x^2 + y^2 = z^2$ has the solution $(x, y, z) = (1, 0, 1)$.

If $(-1, -1)_2 = 1$, there would be a non-trivial solution to $x^2 + y^2 + z^2 \equiv 0 \bmod 4$. Since there is no such solution, $(-1, -1)_2 = -1$. □

I've named the following invariant after John Friedlander, Henryk Iwaniec, Barry Mazur, and Karl Rubin; this invariant comes from a dependence relation

between the spins of a prime ideal which was originally pointed out as a Hilbert symbol condition in section 11 of [6].

Recall the properties satisfied by $K(n,\ell)$ listed on page 16.

Definition 4.4.4. *Let $K := K(n,\ell)$. Define the Starlight invariant, m_K to be the number of $\mathrm{Gal}(K/\mathbb{Q})$-orbits X of M_4 of non-trivial size such that $\star(X) = 1$. That is, for σ a generator of $\mathrm{Gal}(K/\mathbb{Q})$,*

$$m_K = \#\{X \in \mathbb{M}_{4,G} : \#X = n \text{ and } \star(X) = 1\}.$$

Remark 4.4.5. *By Lemma 4.4.3, it is equivalent to define the Starlight invariant, m_K as*

$$m_K := \#\star^{-1}(1) - 1.$$

Here $\star$ refers to the map $\star : \mathbb{M}_{4,G} \to \pm 1$ given in Theorem 4.4.2.

Definition 4.4.6. *Define*

$$\star : \mathscr{P}_K^2 \to \{\pm 1\} \quad \text{and} \quad \star : \mathscr{P}_{\mathbb{Q}}^2 \to \{\pm 1\}$$

as the composition of $\star$ as defined in Theorem 4.4.2 and $\mathbf{r}_0$ and $\mathbf{r}$ respectively as defined in Definition 4.2.1.

That is, letting $p \in \mathscr{P}_{\mathbb{Q}}^2$ and letting $\mathfrak{p} \in \mathscr{P}_K^2$ be any prime of K,we define $\star(\mathfrak{p}) := \star \circ \mathbf{r}_0$ and we define $\star(p) := \star \circ \mathbf{r}$, the composition of the maps $\mathbf{r}_0$ and $\mathbf{r}$ respectively with the map $\star$ from Definition 4.2.1.

We say that a prime $\mathfrak{p} \in \mathscr{P}_K^2$ (respectively $p \in \mathscr{P}_{\mathbb{Q}}^2$) has property $\star$ or that $\star$ is true for $\mathfrak{p}$ (respectively p) whenever $\star(\mathfrak{p}) = 1$ (respectively $\star(p) = 1$).

The main results of this Chapter, Theorem 4.5.2 and Theorem 4.5.4 give formulas in terms of n and m_K for the density of rational primes (assumed to split completely in Theorem 4.5.2) that satisfy property $\star$.

4.5 The Little Density Theorem

Recall that $\mathscr{P}_{\mathbb{Q}}^{2\ell}$ denotes the set of odd rational primes unramified in $K/\mathbb{Q}$. For $p \in \mathscr{P}_{\mathbb{Q}}^{2\ell}$, let $f_{K/\mathbb{Q}}(p) := f_{K/\mathbb{Q}}(\mathfrak{p})$ denote the inertia degree of $\mathfrak{p}$ for the extension $K/\mathbb{Q}$ where $\mathfrak{p}$ is any prime in K laying above p. Note that $K(n,\ell)$ is Galois so $f_{K/\mathbb{Q}}(p)$ is well-defined. Recall from Definition 4.3.1,

$$S := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : f_{K/\mathbb{Q}}(p) = 1\}, \quad I := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : f_{K/\mathbb{Q}}(p) = n\},$$
$$S' := \{\mathfrak{p} \in \mathscr{P}_{K}^{2\ell} : f_{K/\mathbb{Q}}(\mathfrak{p}) = 1\}, \quad I' := \{\mathfrak{p} \in \mathscr{P}_{K}^{2\ell} : f_{K/\mathbb{Q}}(\mathfrak{p}) = n\}.$$

Definition 4.5.1. *Let $K = K(n,\ell)$. Define the following sets of rational primes.*

$$B := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : \star(p) = 1\}$$
$$R := B \cap S.$$

Recall that for sets of primes $R \subseteq S$, we use the notation $d(R|S)$ to denote the relative density of primes $p \in S$ that lay in R; see definition 1.4.1.

Theorem 4.5.2. *Let $K = K(n,\ell)$ such that $n \neq 2$ is prime. Then*

$$d_K := d(R|S) = \frac{1 + m_K n}{2^n}.$$

Proof. Let $N \in \mathbb{Z}_+$. Let R_N and S_N denote the sets of primes in R and S respectively of norm less than N. We will show that

$$\lim_{N\to\infty} \frac{\#R_N}{\#S_N} = \frac{\#\{X \in M_4 : \star(X) = 1\}}{\#M_4} = \frac{1 + m_K n}{2^n}. \tag{4.4}$$

Let $R'_N \subseteq \mathscr{P}_K^{2\ell}$ denote the set of primes of K which lay above rational primes in $R_N \subseteq \mathscr{P}_{\mathbb{Q}}^{2\ell}$ and define S'_N similarly with respect to $S_N \subseteq \mathscr{P}_{\mathbb{Q}}^{2\ell}$. Let $\mathbf{r}_{0,N}$ denote

the restriction of $\mathbf{r}_0$ to $S'_N \subseteq \mathscr{P}_K^{2\ell}$. Since we have restricted to primes that split completely in $K/\mathbb{Q}$,

$$\frac{\#R_N}{\#S_N} = \frac{\#R'_N}{\#S'_N}$$

and that

$$R'_N = \bigcup_{\star(\alpha)=1} \mathbf{r}_{0,N}^{-1}(\alpha)$$

where the above is a disjoint union over elements $\alpha \in M_4$ such that $\star(\alpha) = 1$. Therefore

$$\frac{\#R'_N}{\#S'_N} = \frac{1}{\#S'_N} \sum_{\star(\alpha)=1} \#\mathbf{r}_{0,N}^{-1}(\alpha).$$

By Lemma 4.3.2, this implies

$$\begin{aligned}\lim_{N\to\infty} \frac{\#R'_N}{\#S'_N} &= \sum_{\star(\alpha)=1} \lim_{N\to\infty} \frac{\#\mathbf{r}_{0,N}^{-1}(X)}{\#S'_N} \\ &= \sum_{\star(\alpha)=1} \frac{1}{2^n} \\ &= \frac{\#\{\alpha \in M_4 : \star(\alpha) = 1\}}{2^n}.\end{aligned}$$

This proves the first equality in equation 4.4. Let σ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$. By Lemma 4.1.2, the elements of $\alpha \in M_4$ such that $\alpha^\sigma = \alpha$ are $\alpha = \pm 1$ and we know that $\star(1) = 1$ and $\star(-1) = -1$ by Lemma 4.4.3. Recalling that $m_K = \#\{[\alpha] \in \mathbb{M}_{4,G} : \alpha^\sigma \neq \alpha, \star(\alpha) = 1\}$, this implies

$$\#\{\alpha \in M_4 : \star(\alpha) = 1\} = m_K n + 1.$$

since $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic so Galois orbits $X \in \mathbb{M}_{4,G}$ such that $X^\sigma \neq X$ each contain n elements. □

We now state an extended version of Lemma 4.3.2 which handles the inert case allowing us to give a formula for $d(B|\mathscr{P}_{\mathbb{Q}}^{2\ell})$, the overall density of rational primes which satisfy $\star$.

Lemma 4.5.3. *Let $K := K(n, \ell)$.*

(a) For any $\alpha \in M_4$, the density of $\mathfrak{p} \in \mathscr{P}_K^{2\ell}$ such that $\varphi(\mathfrak{p}) = \alpha$ is $\frac{1}{2^n}$. That is,

$$d(\mathbf{r}_0^{-1}(\alpha)|\mathscr{P}_K^{2\ell}) = \frac{1}{\#M_4} = \frac{1}{2^n}.$$

(b) Restricting to primes of K which split completely in $K/\mathbb{Q}$,

$$d(\mathbf{r}_0^{-1}(\alpha) \cap S'|S') = \frac{1}{\#M_4} = \frac{1}{2^n}.$$

(c) Restricting to inert primes of K,

$$d(\mathbf{r}_0^{-1}(\alpha) \cap I'|I') = \begin{cases} \frac{1}{2} & \text{if } \alpha = \pm 1 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Part (a) and part (b) were proven in Lemma 4.3.2.

If $\alpha \neq \pm 1$ (for $\alpha \in M_4$) then $\mathbf{r}_0^{-1}(\alpha) \cap I' = \emptyset$ since ± 1 are the only invariants of the $\mathrm{Gal}(K/\mathbb{Q})$-action on M_4 by Lemma 4.1.2. Therefore $d(\mathbf{r}_0^{-1}(\alpha) \cap I'|I') = 0$ if $\alpha \neq \pm 1$.

Now fix $s = \pm 1$. Then

$$\mathbf{r}_0^{-1}(s) \cap I' = \left\{\mathfrak{p} \in I' : \left(\frac{\alpha}{4}\right)_K = s\right\}$$

where $\left(\frac{\alpha}{4}\right)_K$ denotes the quadratic residue symbol in O_K for $\alpha \in O_K$ a totally positive generator of $\mathfrak{p}^{h(K)}$. This is a congruence condition so it is routine to show that

$$d(\mathbf{r}_0^{-1}(s) \cap I'|I') = \frac{1}{2}.$$

by Theorem 1.4.2. □

Theorem 4.5.4. *Let $K = K(n, \ell)$ such that $n \neq 2$ is prime. Then*

$$d(B|\mathscr{P}_{\mathbb{Q}}^{2\ell}) = \frac{2^{n-1} + (m_K n + 1)(n-1)}{2^n n}.$$

Proof. Let $N \in \mathbb{Z}_+$. Let I_N and S_N denote the sets of (rational) primes in I and S respectively with positive generator less than N. Let $I'_N \subseteq \mathscr{P}_K^{2\ell}$ denote the set of primes of K which lay above rational primes in $I_N \subseteq \mathscr{P}_{\mathbb{Q}}^{2\ell}$ and define S'_N similarly with respect to $S_N \subseteq \mathscr{P}_{\mathbb{Q}}^{2\ell}$. Note that while $S'_N = \{\mathfrak{p} \in S' : \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p}) < N\}$,

$$I'_N = \{\mathfrak{p} \in I' : \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p}) < N^n\}.$$

Observe that since we have restricted to primes which are inert in $K/\mathbb{Q}$,

$$\frac{\#B \cap I_N}{\#I_N} = \frac{\#B' \cap I'_N}{\#I'_N}$$

where $B' := \{\mathfrak{p} \in \mathscr{P}_K^{2\ell} : \star(\mathfrak{p}) = 1\} = \{\mathfrak{p} \in \mathscr{P}_K^{2\ell} : \mathfrak{p} \text{ lays above some } p \in B\}$.

Let $\mathbf{r}_{0,N}$ denote the restriction of $\mathbf{r}_0$ to $I'_N \subseteq \mathscr{P}_K^{2\ell}$. Observe that $\mathfrak{p} \in I'$ implies $\mathfrak{p}^\sigma = \mathfrak{p}$ so $\mathbf{r}_0(\mathfrak{p}) = \pm 1$ for all $\mathfrak{p} \in I'$ by Lemma 4.1.2. Lemma 4.4.3 states that $\star(1) = 1$ and $\star(-1) = -1$. Therefore

$$B' \cap I'_N = \mathbf{r}_0^{-1}(1) \cap I'_N.$$

Therefore $d(B' \cap I'|I') = \frac{1}{2}$ by part (c) of Lemma 4.5.3. Then since $\frac{\#B \cap I_N}{\#I_N} = \frac{\#B' \cap I'_N}{\#I'_N}$, we have proven that

$$d(B \cap I|I) = \frac{1}{2}. \tag{4.5}$$

Note that since $K/\mathbb{Q}$ is cyclic, $\mathscr{P}_{\mathbb{Q}}^{2\ell}$ is the disjoint union of S and I.

$$\begin{aligned} d(B|\mathscr{P}_{\mathbb{Q}}^{2\ell}) &= \lim_{N\to\infty} \frac{\#B_N}{\#\mathscr{P}_{\mathbb{Q},N}^{2\ell}} = \lim_{N\to\infty} \left(\frac{\#B \cap I_N}{\#I_N} \frac{\#I_N}{\#\mathscr{P}_{\mathbb{Q},N}^{2\ell}} + \frac{\#B \cap S_N}{\#S_N} \frac{\#S_N}{\#\mathscr{P}_{\mathbb{Q},N}^{2\ell}} \right) \\ &= \left(\frac{1}{2}\right)\left(\frac{1}{n}\right) + \left(\frac{m_K n + 1}{2^n}\right)\left(\frac{n-1}{n}\right) \quad \text{by Theorem 4.5.2} \\ &= \frac{2^{n-1} + (m_K n + 1)(n-1)}{2^n n}. \end{aligned}$$

□

4.6 Computed Starlight Invariants

Table 4.1 gives some computed values of the Starlight invariant m_K for the number fields $K := K(n, \ell)$ for the specified $n = [K : \mathbb{Q}]$ and conductor ℓ. See Appendix B for the code used to compute these values in magma [2]. Recall that Definition 2.2.1 asserted the following conditions;

* $U_T = U^2$.
* The class number of $K(n, \ell)$, is odd.
* 2 and 5 are inert in $K(n, \ell)/\mathbb{Q}$.

These conditions are met by the number fields in Table 4.1 with the exception that an asterisk denotes a number field in which 2 and/or 5 is not inert. In the last row, Table 4.1 gives the restricted density coming from Theorem 4.5.2 of primes p that split as completely as possible in $K(p)/\mathbb{Q}$ given the necessary ramification, restricted to primes that split completely in $K/\mathbb{Q}$. For example, the second column of Table 4.1 tells us that if $K := K(5, 11)$, the unique subextension of the 11^{th} cyclotomic field of degree 5 over $\mathbb{Q}$, then $m_K = 1$ and Theorem 4.5.2 states that the density of primes $p \in S$ that lay in R is $\frac{3}{16}$.

n	3	5	7	11	13	17	19
l	7	11	43	23	53	103	191
m_K	1	1	3	3	5	17	27
$d(R\|S)$	$\frac{1}{2}$	$\frac{3}{16}$	$\frac{11}{64}$	$\frac{17}{1024}$	$\frac{33}{4096}$	$\frac{145}{65536}$	$\frac{257}{262144}$

Table 4.1: Computed Starlight invariants

4.7 Bounds

Lemma 4.7.1. *Let $K := K(n, \ell)$. For all $\alpha \in M_4$,*

$$\star(\alpha) = 1 \implies \star(-\alpha) = -1.$$

Proof. By Lemma 4.4.3, $(-1, -1)_2 = -1$.

Next note that $(a, b)_2 = (a^\sigma, b^\sigma)_2$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ since 2 is inert in K.

Assume $\star(\alpha) = 1$. Then $(\alpha, \alpha^\sigma)_2 = 1$ for all nontrivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be nontrivial. By bimultiplicativity of Hilbert symbols,

$$\begin{aligned}(-\alpha, -\alpha^\sigma)_2 &= (-\alpha, -1)_2(-\alpha, \alpha^\sigma)_2 \\ &= (-1, -1)_2(\alpha, -1)_2(-1, \alpha^\sigma)_2(\alpha, \alpha^\sigma)_2.\end{aligned}$$

Next observe $(\alpha, -1)_2 = (-1, \alpha)_2 = (-1, \alpha^\sigma)_2$, the second equality coming from the Galois-invariance shown earlier in this proof. Therefore $(\alpha, -1)_2(-1, \alpha^\sigma)_2 = 1$. Then since $(\alpha, \alpha^\sigma)_2 = 1$ and $(-1, -1)_2 = -1$, we get that

$$(-\alpha, -\alpha^\sigma)_2 = -1.$$

Therefore $\star(-\alpha) = -1$. □

Recall the Definitions 4.3.1 and 4.5.1 defining S and R.

Theorem 4.7.2. *Let $K := K(n, \ell)$.*

$$\frac{1}{2^n} \leq d(R|S) \leq \frac{1}{2}.$$

Proof. By Theorem 4.5.2,

$$d(R|S) = \frac{1 + m_K n}{2^n} = \frac{\#\{\alpha \in M_4 : \star(\alpha) = 1\}}{2^n}.$$

Lemma 4.7.1 implies the upper bound; note that $\alpha \neq -\alpha$ in M_4 because -1 is not a square modulo $4\mathcal{O}_K$.

The lower bound is true because $\star(1) = 1$ by Lemma 4.4.3 so

$$\#\{\alpha \in M_4 : \star(\alpha) = 1\} \geq 1.$$

□

CHAPTER 5

A DENSITY OF RAMIFIED PRIMES

5.1 A Family of Number Fields Depending on p

Let $K := K(n, \ell)$ as defined on page 16. Recall that Lemma 2.1.3 showed that for odd primes $\mathfrak{p}$, there exists a unique quadratic subextension of the narrow ray class field over K of conductor $\mathfrak{p}$.

Definition 5.1.1. *Let $K := K(n, \ell)$. Let $p \in \mathscr{P}_{\mathbb{Q}}^{2\ell}$ (i.e. p is an odd rational prime unramified in $K/\mathbb{Q}$). Define the number field $K(p)$ depending on p and K to be the composite of the fields $\{R(\mathfrak{p})\}_{\mathfrak{p}}$ as $\mathfrak{p}$ varies over all primes of K laying above p where $R(\mathfrak{p})$ is the unique quadratic subextension of $\mathrm{nR}^{\mathfrak{p}}/K$, the narrow ray class field over K of conductor $\mathfrak{p}$.*

Remark 5.1.2. *$K(p)/\mathbb{Q}$ is a normal extension. Therefore*

$$efg = [K(p) : \mathbb{Q}] = 2^{g_0} n$$

where e, f, and g denote respectively the ramification index, the inertia degree, and the number of distinct primes laying above p all relative to the extension $K(p)/\mathbb{Q}$. Here g_0 denotes the number of distinct primes of K laying above the rational prime p.

Since $K := K(n, \ell)$ includes the assumption that K is cyclic over $\mathbb{Q}$, then $g_0 = 1$ or n depending on whether $p \in I$ or $p \in S$ where I and S are as defined on page 38;

$$S := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : f_{K/\mathbb{Q}}(p) = 1\}, \quad I := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : f_{K/\mathbb{Q}}(p) = n\},$$
$$S' := \{\mathfrak{p} \in \mathscr{P}_{K}^{2\ell} : f_{K/\mathbb{Q}}(\mathfrak{p}) = 1\}, \quad I' := \{\mathfrak{p} \in \mathscr{P}_{K}^{2\ell} : f_{K/\mathbb{Q}}(\mathfrak{p}) = n\}.$$

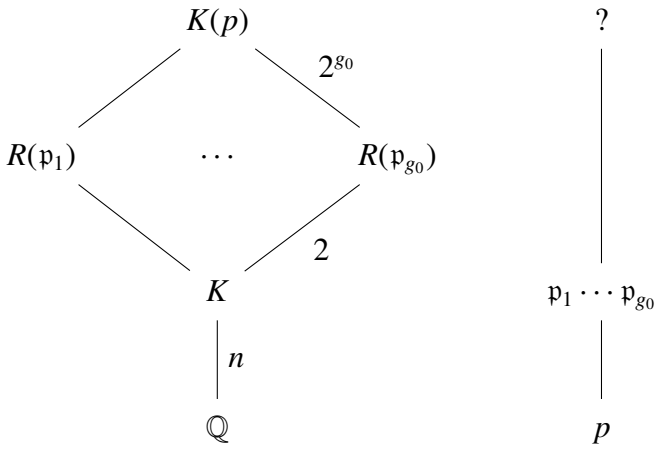


Figure 5.1: A field diagram depicting $K(p)$.

When $p \in I$, there is only one way that p can factor in $K(p)/\mathbb{Q}$; in this case $[K(p) : \mathbb{Q}] = 2n$ with $e = 2$ and $f = n$. The case $p \in S$ is more interesting. Proposition 5.1.3 states that $e = 2$ (so p is always ramified in $K(p)/\mathbb{Q}$) and the inertia degree can only be 1 or 2. This completely determines the factorization of p in $K(p)/\mathbb{Q}$ since the extension is normal.

Proposition 5.1.3. *Given $p \in S$, there are two ways that p can factor in $K(p)/\mathbb{Q}$;*

Case 1: $e = 2$, $f = 1$, and $g = 2^{n-1}n$.

Case 2: $e = 2$, $f = 2$, and $g = 2^{n-2}n$.

Proof. We know that $e = 2$ because each prime $\mathfrak{p}$ of K above p is totally ramified in the quadratic extension $R(\mathfrak{p})$ and is unramified in each $R(\mathfrak{q})$ for $\mathfrak{p} \neq \mathfrak{q}$. We also know $n|g$ since p splits completely in $K/\mathbb{Q}$. This means f must divide 2^{n-1}, but in fact f must divide 2 because f is the degree of the residue field extension which is cyclic and embeds into the Galois group of $K(p)/\mathbb{Q}$, but $K(p)/K$ has no even cyclic subextension of degree greater than 2. Therefore $f|2$. □

Fixing a prime $\mathfrak{p}$ of K above p, we can determine how p factors in $K(p)/\mathbb{Q}$ if

we know how $\mathfrak{p}$ factors in each $R(\mathfrak{p}^\sigma)$ for $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Remark 5.1.4. *Fix a prime $\mathfrak{p}$ of K above $p \in S$. Let $R_\sigma := R(\mathfrak{p}^\sigma)$ denote the unique quadratic subextension of the narrow ray class field over K of conductor $\mathfrak{p}^\sigma$.*

(a) If $f_{R_\sigma/K}(\mathfrak{p}) = 1$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ then $f_{K(p)/K}(\mathfrak{p}) = 1$, which implies we are in case 1 of Proposition 5.1.3.

(b) If there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $f_{R_\sigma/K}(\mathfrak{p}) = 2$ then $f_{K(p)/K}(\mathfrak{p}) = 2$, which implies we are in case 2 of Proposition 5.1.3.

It is an exercise in algebraic number theory to show part (a) of Remark 5.1.4. One could apply Theorem 29 in Chapter 4 of [8] for example. Part (b) is true because inertia degrees are divisible in towers.

Using the $\mathrm{Gal}(K/\mathbb{Q})$ action, the next Proposition implies that knowing the factorization of $\mathfrak{p}$ in each R_σ is equivalent to knowing the factorization of each $\mathfrak{p}^\sigma$ in R_1. This is more useful for computations since only one ray class field needs to be computed in order to determine how p factors in $K(p)/\mathbb{Q}$.

Let $K := K(n, \ell)$. Let $p \in S$. Fix a prime $\mathfrak{p}$ of K above p and let $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$. Let $f_\sigma(\tau)$ denote the inertia degree of $\mathfrak{p}^\tau$ in the quadratic extension $R(\mathfrak{p}^\sigma)/K$ where $R(\mathfrak{p}^\sigma)$ is the unique quadratic subextension of the narrow ray class field over K of conductor $\mathfrak{p}^\sigma$. Then we have the following Proposition.

Proposition 5.1.5. *Let $K := K(n, \ell)$. Let $p \in S$. Fix a prime $\mathfrak{p}$ of K above p and let σ, τ, $\omega \in \mathrm{Gal}(K/\mathbb{Q})$. Then*

$$f_\sigma(\tau) = f_{\omega\sigma}(\omega\tau)$$

Proof. Apply the action of $\omega \in \mathrm{Gal}(K/\mathbb{Q})$. □

Example 5.1.6. *For example, set $n = 3$ and let $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ denote the three primes of K above p. Then Proposition 5.1.5 implies*

$$f_{R(\mathfrak{p}_2)/K}(\mathfrak{p}_1) = f_{R(\mathfrak{p}_3)/K}(\mathfrak{p}_2) = f_{R(\mathfrak{p}_1)/K}(\mathfrak{p}_3) \quad \textit{and}$$

$$f_{R(\mathfrak{p}_3)/K}(\mathfrak{p}_1) = f_{R(\mathfrak{p}_2)/K}(\mathfrak{p}_3) = f_{R(\mathfrak{p}_1)/K}(\mathfrak{p}_2)$$

so we only need two pieces of data in order to determine how p factors in $K(p)$. In general this implies we need $n-1$ pieces of data to determine how p factors in $K(p)$.

If any of the $n-1$ inertia degrees are 2, then the inertia degree of p in $K_p/\mathbb{Q}$ is also 2 by Remark 5.1.4. Fixing τ, the likelihood of each $f(\sigma)_\tau$ being equal to 1 is $\frac{1}{2}$ as $\sigma \neq \tau$ varies, which suggests the naive heuristic that the density of primes p which split completely in $K_p/\mathbb{Q}$ might be

$$\frac{1}{2^{n-1}}.$$

However, this assumes independence of the $n-1$ pieces of data, which is not the case, and magma data will verify that this naive heuristic does not work for $n > 3$. It does work for $n = 3$, but this is essentially a coincidence because some 2's cancel.

5.2 $K(p)$ and Spin

Let $K := K(n, \ell)$. Fix a prime $\mathfrak{p} \in S'$; $\mathfrak{p}$ is a prime of K that lays above an odd rational prime that splits completely in $K/\mathbb{Q}$. For $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, let $R(\mathfrak{p}^\sigma)$ denote the unique quadratic subextension of the narrow ray class field over K of conductor $\mathfrak{p}^\sigma$ noting that $R(\mathfrak{p}^\sigma)$ exists uniquely by Lemma 2.1.3. Recall $f_\sigma(\tau)$ denotes the inertia degree $f_{R(\mathfrak{p}^\sigma)/K}(\mathfrak{p}^\tau)$ of $\mathfrak{p}^\tau$ considered in $R(\mathfrak{p}^\sigma)/K$.

Lemma 5.2.1. *Let $K := K(n, \ell)$. Fix a prime $\mathfrak{p} \in S'$. Then*

$$\text{spin}(\mathfrak{p}, \sigma) = \left(\frac{\alpha}{\mathfrak{p}^\sigma}\right) = 1 \quad \iff \quad \mathfrak{p} \textit{ splits in } R(\mathfrak{p}^\sigma)/K$$
$$\iff f_\sigma(1) = 1$$

Proof. Recall the map $\mathbf{v}_K$ defined in Definition 2.2.3. Let $u := \mathbf{v}_K(\mathfrak{p})$ and $u^\sigma := \mathbf{v}_K(\mathfrak{p})^\sigma = \mathbf{v}_K(\mathfrak{p}^\sigma)$. We prove $\left(\frac{u^\sigma \alpha^\sigma}{\mathfrak{p}}\right) = 1$ if and only if $\mathfrak{p}$ splits in $R(\mathfrak{p}^\sigma)$ and then apply Theorem 3.4.1. Consider the natural injective homomorphism of residue fields

$$O_K/\mathfrak{p} \hookrightarrow O_{R(\mathfrak{p}^\sigma)}/\mathfrak{P}$$

where $\mathfrak{P}$ is a prime above $\mathfrak{p}$ in $R(\mathfrak{p}^\sigma)$.

If $\left(\frac{u^\sigma \alpha^\sigma}{\mathfrak{p}}\right) = 1$ then there exists $x \in O_K/\mathfrak{p}$ such that $u^\sigma \alpha^\sigma \equiv x^2 \bmod \mathfrak{p}$.

Then considered in $O_{R(\mathfrak{p}^\sigma)}/\mathfrak{P}$, $u^\sigma \alpha^\sigma$ is a square so the natural injective homomorphism of residue fields is surjective which implies $f_{R(\mathfrak{p}^\sigma)/K(\mathfrak{p})} = 1$, i.e. $\mathfrak{p}$ splits completely in $R(\mathfrak{p}^\sigma)/K(\mathfrak{p})$.

Conversely, if $\mathfrak{p}$ splits in $R(\mathfrak{p}^\sigma)$ then the residue field inclusion is surjective so there exists $x \in O_K/\mathfrak{p}$ such that $x = \sqrt{u_j \alpha_j}$ in $O_{R(\mathfrak{p}^\sigma)}/\mathfrak{P}$. Then $x^2 = u^\sigma \alpha^\sigma$ so injectivity implies $\left(\frac{u^\sigma \alpha^\sigma}{\mathfrak{p}}\right) = 1$. □

5.3 Two Conjectures

As in Corollary 3.3.3, for $\sigma \in \text{Gal}(K/\mathbb{Q})$ define

$$\Pi := \{\text{principal prime ideals of } O_K\} \quad \text{and} \quad \Lambda_\sigma := \{\mathfrak{p} \in \Pi : \text{spin}(\mathfrak{p}, \sigma) = 1\}.$$

Recall the definitions of R and B from Definition 4.5.1;

$$B := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : \star(p) = 1\}$$
$$R := B \cap S$$

and note that $\star(p) = 1$ exactly when for $\mathfrak{p} \in \mathscr{P}_K^{2\ell}$ above $p \in \mathscr{P}_{\mathbb{Q}}^{2\ell}$,

$$\text{spin}(\mathfrak{p}, \sigma) = \text{spin}(\mathfrak{p}, \sigma^{-1}) \quad \text{for all } \sigma \neq 1 \in \text{Gal}(K/\mathbb{Q})$$

by Theorem 4.4.1 and Theorem 4.4.2.

The next Conjecture asserts that Corollary 3.3.3 still holds restricting to primes $\mathfrak{p} \in \Pi$ such that $\text{spin}(\mathfrak{p}, \sigma) = \text{spin}(\mathfrak{p}, \sigma^{-1})$ for all non-trivial $\sigma \in \text{Gal}(K/\mathbb{Q})$. Note that Theorem 3.3.2 does not apply.

Conjecture 5.3.1. *Let $K := K(n, \ell)$. Assume Conjecture 3.2.2 for $n = [K : \mathbb{Q}]$. Let $\sigma \in \text{Gal}(K/\mathbb{Q})$ be non-trivial. Recall*

$$\Lambda_\sigma := \{\mathfrak{p} \in \Pi : \text{spin}(\mathfrak{p}, \sigma) = 1\} \quad \textit{and} \quad B := \{\mathfrak{p} \in \Pi : \text{spin}(\mathfrak{p}, \sigma) = \text{spin}(\mathfrak{p}, \sigma^{-1}) \forall \sigma \neq 1\}$$

Then

$$d(\Lambda_\sigma \cap B | B) = d(\Lambda_\sigma | \Pi).$$

In Section 11 of [6], Friedlander, Iwaniec, Mazur, and Rubin pose a problem; for $n > 3$, aside from the dependence relation given in Theorem 3.1.2, are there any other dependence relations between $\text{spin}(\mathfrak{p}, \sigma)$ and $\text{spin}(\mathfrak{p}, \tau)$ for $\sigma, \tau \in \text{Gal}(K/\mathbb{Q})$? The following is my conjectural answer to a weak version of this problem in which we only consider the *asymptotic* dependence of spins of a fixed prime ideal. Conjecture 5.3.2 asserts the asymptotic independence of spin. The conjecture is supported by data obtained from magma.

Conjecture 5.3.2 (A_n). *Let $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$ non-trivial such that $\sigma \neq \tau$ and $\sigma \neq \tau^{-1}$. Then*

$$d(\Lambda_\sigma \cap \Lambda_\tau | \Pi) = d(\Lambda_\sigma | \Pi) d(\Lambda_\tau | \Pi) \quad \textit{and}$$

and

$$d(\Lambda_\sigma \cap \Lambda_\tau \cap B | B) = d(\Lambda_\sigma \cap B | B) d(\Lambda_\tau \cap B | B).$$

Note that Conjecture 5.3.2 is vacuously true for $n = 3$. The data on pages 61 and 62 supports Conjecture 5.3.2 for $n = 5, 7$. If there are no dependence relations between σ and τ then Conjecture 5.3.2 is true, but not conversely.

Tables 5.1 (for $n = 3$), 5.2 (for $n = 5$), and 5.3 (for $n = 7$) give a sense of intuition for the rate of convergence of the relative density $d(F|S)$ in Theorem 5.4.3 of rational primes that split "as completely as possible" in $K(p)$, restricted to those that split completely in $K/\mathbb{Q}$.

The tables for $n = 5$ and $n = 7$ support Conjecture 3.2.2 and Conjecture 5.3.2 in the cases $n = 5$ and $n = 7$. Each row represents a number field K with the desired properties; namely K is the subextension of the ℓ^{th} cyclotomic field of degree n over $\mathbb{Q}$ for the given values of ℓ. Each column of the table gives the percentage of the time p lays in a set F after checking the first 10^4, 10^5, 10^6, or 10^7 rational primes p that split completely in $K/\mathbb{Q}$. That is, each column gives

$$\frac{\#F_N}{\#S_N}$$

for some N such that $\#S = 10^4, 10^5, 10^6$, or 10^7.

An asterisk * denotes when 2 splits in $K/\mathbb{Q}$. Note that our results are only proven if 2 is inert in $K/\mathbb{Q}$. Nevertheless the densities seem to work out as predicted.

ℓ	10^4	10^5	10^6	10^7
7	24.8	24.989	24.9866	24.99925
13	25.16	25.045	24.9815	24.99505
19	25.32	24.946	24.988	25.00635
31*	24.81	24.852	25.0435	25.01285
37	26.19	24.998	25.0008	25.00079
43*	25.22	24.872	24.9834	24.98046
61	24.65	24.999	24.9525	
67	24.83	25.028	25.01	
73	24.46	25.111	24.9675	
79	24.49	24.843	25.094	
Average	24.993	24.9683	25.00078	
Median	24.82	24.9935	24.9873	
Standard Deviation	0.5132911238	0.088857001	0.040929039	
Theorem 5.4.3 Prediction	25.0	25.0	25.0	25.0

Table 5.1: Data for $n = 3$; The percentage of primes p (that split completely in $K/\mathbb{Q}$) that exhibit the given ramified factorization in $K(p)/\mathbb{Q}$.

ℓ	10^4	10^5	10^6	10^7
11	4.49	4.746	4.6908	4.68969
31	4.70	4.649	4.6663	4.68322
41	4.36	4.586	4.6774	4.68479
61	4.39	4.613	4.6888	
71	4.84	4.788	4.7014	
101	4.67	4.623	4.7224	
131	4.48	4.596	4.6806	
151*	4.77	4.627	4.7143	
181	4.96	4.770	4.6496	
191	4.51	4.718	4.6580	
Average	4.617	4.6716	4.68496	
Median	4.59	4.638	4.6847	
Standard Deviation	0.201221271	0.076200321	0.023530699	
Theorem 5.4.3 Prediction	4.6875	4.6875	4.6875	4.6875

Table 5.2: Data for $n = 5$; The percentage of primes p (that split completely in $K/\mathbb{Q}$) that exhibit the given ramified factorization in $K(p)/\mathbb{Q}$.

ℓ	10^4	10^5	10^6
43	1.91	2.176	2.1498
71	2.33	2.107	2.1501
127	2.2	2.091	2.1283
211	1.92	2.119	2.1736
281	2.11	2.204	2.1646
337	2.22	2.203	2.1509
Average	2.115	2.150	2.152883333
Median	2.155	2.1475	2.1505
Standard Deviation	0.170029409	0.050382537	0.015440132
Theorem 5.4.3 Prediction	2.1484375	2.1484375	2.1484375

Table 5.3: Data for $n = 7$; The percentage of primes p (that split completely in $K/\mathbb{Q}$) that exhibit the given ramified factorization in $K(p)/\mathbb{Q}$.

5.4 A Density of Ramified Primes

Recall Definition 4.3.1;

$$S := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : f_{K/\mathbb{Q}}(p) = 1\}, \quad I := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : f_{K/\mathbb{Q}}(p) = n\},$$

$$S' := \{\mathfrak{p} \in \mathscr{P}_{K}^{2\ell} : f_{K/\mathbb{Q}}(\mathfrak{p}) = 1\}, \quad I' := \{\mathfrak{p} \in \mathscr{P}_{K}^{2\ell} : f_{K/\mathbb{Q}}(\mathfrak{p}) = n\}.$$

Definition 5.4.1. *Let $K := K(n, \ell)$. Define*

$$F := \{p \in S : f_{K(p)/\mathbb{Q}}(p) = 1\} \quad \textit{and}$$

$$F' := \{\mathfrak{p} \in S' : \mathfrak{p} \textit{ lays above some } p \in F\}.$$

By Remark 5.1.4, an odd rational prime p which splits completely in $K/\mathbb{Q}$ factors in $K(p)/\mathbb{Q}$ with inertia degree 1 if and only if $\mathfrak{p}$ splits completely in $R(\mathfrak{p}^\sigma)/K$ for all non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ where $\mathfrak{p}$ is a prime of K above p. Therefore by Lemma 5.2.1, we have the following equivalent definition of F.

Remark 5.4.2.

$$F = \{p \in S : \mathrm{spin}(\mathfrak{p}, \sigma) = 1 \textit{ for all } \sigma \neq 1 \in \mathrm{Gal}(K/\mathbb{Q}) \textit{ where } \mathfrak{p} \in S' \textit{ lays above } p\}.$$

$$F' = \{\mathfrak{p} \in S' : \mathrm{spin}(\mathfrak{p}, \sigma) = 1 \textit{ for all } \sigma \neq 1 \in \mathrm{Gal}(K/\mathbb{Q})\}.$$

Theorem 5.4.3. *Let $K := K(n,\ell)$. Assume Conjecture 3.2.2 and Conjecture 5.3.2 (both are true for $n = 3$). Also assume Conjecture 5.3.1.*

Let $K := K(n,\ell)$. Assume the narrow ray class group over K of conductor 2 is trivial. Then

$$D := d(F|S) = \frac{m_K n + 1}{2^{n+\frac{n-1}{2}}}.$$

Proof. Recall the definition of R from Definition 4.5.1;

$$B := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : \star(p) = 1\}$$
$$R := B \cap S.$$

and note that $\star(p) = 1$ exactly when

$$\text{spin}(\mathfrak{p}, \sigma) = \text{spin}(\mathfrak{p}, \sigma^{-1}) \quad \text{for all } \sigma \neq 1 \in \text{Gal}(K/\mathbb{Q})$$

by Theorem 4.4.1 and Theorem 4.4.2.

Since by Remark 5.4.2,

$$F = \{p \in S : \text{spin}(\mathfrak{p}, \sigma) = 1 \text{ for all } \sigma \neq 1 \in \text{Gal}(K/\mathbb{Q}) \text{ where } \mathfrak{p} \in S' \text{ lays above } p\},$$

then

$$F \subseteq R.$$

Therefore assuming the limits exist,

$$d(F|S) = d(F|R)d(R|S). \tag{5.1}$$

We know that

$$d(R|S) = \frac{1 + m_K n}{2^n}$$

by Theorem 4.5.2.

It remains to show that

$$d(F|R) = \left(\frac{1}{2}\right)^{\frac{n-1}{2}}.$$

Let R' denote the set of primes of K laying above some $p \in R = B \cap S$ so that

$$R' = \{\mathfrak{p} \in S' : \text{spin}(\mathfrak{p}, \sigma) = \text{spin}(\mathfrak{p}, \sigma^{-1}) \text{ for all } \sigma \neq 1 \in \text{Gal}(K/\mathbb{Q})\}.$$

Since we have assumed all primes in R split completely, the ns in the right-hand limits below cancel so

$$d(F|R) = d(F'|R').$$

By Remark 5.4.2,

$$F' = \bigcap_{\substack{\sigma \neq 1 \\ \sigma \in \text{Gal}(K/\mathbb{Q})}} \Lambda_\sigma \cap S.$$

Fix a generator τ of $\text{Gal}(K/\mathbb{Q})$. Define

$$H := \left\{\tau^i : i = 1, ..., \frac{n-1}{2}\right\}$$

so that $\text{Gal}(K/\mathbb{Q})$ is the disjoint union

$$\text{Gal}(K/\mathbb{Q}) = \{1\} \cup H \cup \{\tau^{-1} : \tau \in H\}.$$

Let

$$\Gamma_\sigma := \Lambda_\sigma \cap B$$

where Λ_σ is as defined on page 25. Then $\Gamma_\sigma = \Gamma_{\sigma^{-1}}$ for all nontrivial $\sigma \in \text{Gal}(K/\mathbb{Q})$ so

$$F' = \bigcap_{\substack{\sigma \neq 1 \\ \sigma \in \text{Gal}(K/\mathbb{Q})}} \Lambda_\sigma \cap S' = \bigcap_{\sigma \in H} \Gamma_\sigma \cap S'.$$

Therefore applying Conjecture 5.3.2 (on asymptotic independence of spin) gives

$$d(F|R) = d(F'|R') = \prod_{\sigma \in H} d(\Gamma_\sigma \cap S'|R'). \tag{5.2}$$

Applying Conjecture 5.3.1 gives

$$\begin{aligned} d(\Gamma_\sigma \cap S'|R') &= d(\Lambda_\sigma \cap S'|S') \\ &= d(\Lambda_\sigma \cap \Pi|\Pi) \quad \text{by Theorem 3.3.2} \\ &= \frac{1}{2} \quad \text{by Corollary 3.3.3.} \end{aligned}$$

Therefore equation 5.2 implies

$$d(F|R) = \prod_{\sigma \in H} \frac{1}{2} = \left(\frac{1}{2}\right)^{\frac{n-1}{2}}.$$

□

APPENDIX A

A COMMUTATIVE ALGEBRA LEMMA

The followimg Lemma is used in the proof of surjectivity in Lemma 4.2.2.

Lemma A.0.1. *Let X, Y, Z, W be finite abelian groups equipped with an action from a finite abelian group G where W has odd order and suppose there is an exact sequence of groups*

$$1 \to X \to Y \to Z \to W \to 1$$

where each group homomorphism respects the action from G. Then there is a short exact sequence

$$1 \to X[2^\infty] \to Y[2^\infty] \to Z[2^\infty] \to 1$$

on the 2-parts of these groups induced by the original homomorphisms.

Proof. Let X, Y, Z, W be finite abelian groups (assume $\#W$ is odd) equipped with an action from a group G and suppose there is an exact sequence of groups

$$1 \to X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W \to 1$$

where each group homomorphism f, g, and h respects the action from G. We denote the operation additively. Consider the commutative diagram below where the vertical maps are given by multiplication by 2^N for N sufficiently large.

$$\begin{array}{ccccccccccc}
1 & \longrightarrow & X & \xrightarrow{f_1} & Y & \xrightarrow{g_1} & Z & \xrightarrow{h_1} & W & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle d} & & \\
1 & \longrightarrow & X & \xrightarrow[f_2]{} & Y & \xrightarrow[g_2]{} & Z & \xrightarrow[h_2]{} & W & \longrightarrow & 1
\end{array}$$

Let $x \in \ker(a)$. Then $f_2(a(x)) = f_2(1) = 1$ so commutativity of the diagram shows that $b(f_1(x)) = 1$. Therefore $f_1(x) \in \ker(b)$ so f_1 induces

$$\ker(a) \xrightarrow{f_0} \ker(b)$$

and injectivity of f_0 follows from injectivity of f_1.

Next let $y \in \ker(b)$. Then $g_2(b(y)) = g_2(1) = 1$ so commutativity of the diagram shows that $c(g_1(y)) = 1$ so $g_1(y) \in \ker(c)$. Therefore g induces

$$\ker(b) \xrightarrow{g_0} \ker(c).$$

Let $x \in \ker(a)$. Then $g_0(f_0(x)) = g_1(f_1(x)) = 1$ by exactness so $\text{image}(f_0) \subseteq \ker(g_0)$. Let $y \in \ker(g_0)$. Then $y \in \ker(b) \cap \ker(g_1)$ so $y \in \ker(g_1) = \text{image}(f_1)$ by exactness so $y \in \ker(b) \cap \text{image}(f_1)$. Then there exists some $x \in X$ such that $f_1(x) = y$ and $b(f_1(x)) = 1$. Commutativity of the diagram implies $f_2(a(x)) = 1$. Therefore $a(x) = 1$ by injectivity of f_2 so $x \in \ker(a)$ proving $y \in \text{image}(f_0)$. Therefore $\ker(g_0) = \text{image}(f_0)$.

To summarize, commutative algebra gives the following commutative diagram of exact sequences.

$$\begin{array}{ccccccccccc}
 & & 1 & & 1 & & 1 & & & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & \ker(a) & \longrightarrow & \ker(b) & \xrightarrow{g_0} & \ker(c) & & & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & W & \longrightarrow & 1 \\
 & & \downarrow a & & \downarrow b & & \downarrow c & & \downarrow d & & \\
1 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & W & \longrightarrow & 1
\end{array}$$

To show that g_0 is surjective, we use the assumption that $\#W$ is odd and the fact that the size of the kernel of multiplication by 2^N for N sufficiently large is the largest power of 2 dividing the order of the group. That is

$$\begin{aligned} \#\ker(a) &= 2^{\mathrm{ord}_2(\#X)}, \\ \#\ker(b) &= 2^{\mathrm{ord}_2(\#Y)}, \quad \text{and} \\ \#\ker(c) &= 2^{\mathrm{ord}_2(\#Z)}. \end{aligned}$$

Exactness implies $\#X\#Z = \#Y\#W$ so

$$\mathrm{ord}_2(\#X) + \mathrm{ord}_2(\#Z) = \mathrm{ord}_2(\#Y) + \mathrm{ord}_2(\#W)$$

and $\mathrm{ord}_2(\#W) = 0$ because $\#W$ is odd so

$$\begin{aligned} &\mathrm{ord}_2(\#X) + \mathrm{ord}_2(\#Z) = \mathrm{ord}_2(\#Y) \\ \implies &\#\ker(a)\#\ker(c) = \#\ker(b). \end{aligned}$$

We know that g_0 induces an injective homomorphism

$$\ker(b)/\ker(a) \xrightarrow{g} \ker(c).$$

Since the cardinalities match, g is an isomorphism so g_0 is surjective. □

APPENDIX B

COMPUTATIONS AND CODE

This appendix gives the code used to generate the values given in Table 4.1. All programs are written for magma [2].

B.1 Number Field Hypotheses

```
function Kl(n,l);
    /* return the (unique) n^th degree/Q subfield of
    the lth cyclotomic field where
    l=1 mod 2n is prime */
    assert Type(l) eq RngIntElt;    //l is integer
    assert IsPrime(l);    //l is prime
    assert l gt 0;
    assert (l mod 2*n) eq (1 mod 2*n);

    F:=CyclotomicField(l);
    G:=GaloisGroup(F);
    U:=sub<G|G.1^n>;
    f:=GaloisSubgroup(F,U);
    K:=NumberField(f);
    return K;
end function;

function FProd(L);
    /* return product L[i] for i:=1..#L where #L=#N*/
    prod:=L[1];
    i:=2;
```

```
    while i le #L do
        prod:=prod*L[i];
        i:=i+1;
    end while;
    return prod;
end function;

function PowerList(L);
    /* return list of all sublists of the list L */
    result:=[[]];
    for x in L do
        for sbst in result do
            newsbst:=Append(sbst,x);
            Append(~result, newsbst);
        end for;
    end for;
    return result;
end function;

function UmodSquares(K);
    /* return a list of distinct representatives of units in K
    mod squares excluding the class of squares */
    G,phi:=UnitGroup(K);
    U:=[K!phi(G.i): i in [1..Ngens(G)]];
    PL:=PowerList(U);
    Exclude(~PL, []);
    Ums:=[];
    for L in PL do
        Append(~Ums, FProd(L));
```

```
    end for;
    return Ums;
end function;

function UT2(K);
    /* return true if the totally positive units in K are
    exactly the square units and false otherwise.
    K is a totally real number field.*/
    // L = list of nontrivial elements of U/U^2
    L:=UmodSquares(K);
    for u in L do
        if IsTotallyPositive(u) then
            return false;
        end if;
    end for;
    return true;
end function;

function IsGalois(K);
    /* return true if the numberfield K is Galois over Q */
    return #GaloisGroup(K) eq Degree(K);
end function;

function Hyp(K);
    SetClassGroupBounds("GRH");
    n:=Degree(K);
    OK:=MaximalOrder(K);
    if not (n gt 2) then
        return <false, "K must have degree at least 3." >;
```

```
    elif not IsTotallyReal(K) then
        return <false, "K must be totally real." >;
    elif not (IsPrime(n)) then
        return <false, "K must have prime degree." >;
    elif not (IsGalois(K)) then
        return <false, "K must be Galois over the rationals." >;
    elif not UT2(K) then
        return <false, "K must have U_T=U^2.
        Equivalently, the narrow and wide Hilbert class fields
        of K must coincide." >;
    elif not ClassNumber(K) mod 2 eq 1 then
        return <false, "K must have odd class number.">;
    elif not (Order(RayClassGroup(2*OK,[1..n])) mod 2 eq 1) then
        return <false, "2 can not divide the order of the
        narrow ray class group over K of conductor 2.
        (narrow:= all infinite places divide the conductor.)">;
    elif not IsInert(2*OK) then
        return <false, "2 must be inert in K/Q." >;
    elif not IsInert(5*OK) then
        return <false, "5 must be inert in K/Q." >;
    end if;
    return <true, ":)">;
end function;

function HypBool(K);
    return Hyp(K)[1];
end function;

function HypReason(K);
```

```
    return Hyp(K)[2];
end function;
```

B.2 Computing the Starlight Invariant

```
function IsGenGal(sigma,K);
    /* Assumes the extension K/Q is Galois.
    return value is true iff sigma is a generator of Gal(K/Q). */
    G:=Automorphisms(K);
    n:=#G;
    //assert K/Q is Galois. (Then G is the Galois group.)
    assert n eq Degree(K);
    Divs:=Divisors(n);
    B:=true;
    for d in Divs do
        if (sigma^d)(K.1) eq K.1 then
            if not d eq n then
                return false;
            end if;
        end if;
    end for;
    return true;
end function;

function S(n,L);
    /* return the list of all (lists of size n with entries in L).
    n is a positive integer.
    Helper function for finding square units mod 4. */
```

```
    if n eq 1 then
        SS:=[];
        for i in L do
            Append(~SS,[i]);
        end for;
        return SS;
    elif n gt 1 then
        SS:=[];
        Sprev:=S(n-1,L);
        for s in Sprev do
            for i in L do
                Append(~SS, Append(s,i));
            end for;
        end for;
        return SS;
    else
        return "error: n must be a positive integer.";
    end if;
end function;

function Starlight(K);
    /*  return the number of orbits of non-trivial size
        of the action of G:=Gal(K/Q) on M_K such that
        Star(alpha) is true for some representative alpha
        of the orbit (equiv for all alpha) where
        M_K:=((OK/4)^x)/squares for OK:=MaximalOrder(K) and
        Star(alpha) is true iff
        HilbertSymbol(alpha,alpha^sigma,2*OK)=1
        for all non-triv sigma in G
```

```
    (equiv for all non-triv sigma in H:={tau^i}
     for i=1..(n-1)/2 where tau generates G). */

n:=Degree(K);
OK:=MaximalOrder(K);
U,ugp:=UnitGroup(K);
Umsq,msq:=quo<U|2*U>;
yinv:=Inverse(ugp)*msq;
y:=Inverse(yinv);
OK4,m4:=quo<OK|4*OK>;
U4,ugp4:=UnitGroup(OK4);
MK,msq4:=quo<U4|2*U4>;
x:=m4*Inverse(ugp4)*msq4;
xinv:=Inverse(x);
// Phi: Umsq -> MK is the natural map where
// Umsq=U/U^2 and MK=((OK/4)^x)/squares
Phi:=y*x;

//Find tau, a generator of G:=Gal(K/Q)
GalGen1:=[];
assert IsGalois(K);
while #GalGen1 lt 1 do
    for i in [1..n] do
        sig:=Automorphisms(K)[i];
        if IsGenGal(sig, K) then
            Append(~GalGen1,sig);
        end if;
    end for;
end while;
```

```
tau:=GalGen1[1];

d:=Integers()!((n-1)/2);
H:=[(tau^k): k in [1..d]];
Galnontriv:=[(tau^k): k in [1..n-1]];

// G-orbits of MK st. star is true.
StarPos:=[];
// G-orbits of MK st. star is false.
StarNeg:=[];
// G-orbits that have been checked.
DONEORBITS:=[];

//Indices of UmsqK and UmsqMK correspond via natural map Phi
//initialize list of reps of Umsq:=U/U2 as elements of K.
UmsqK:=[];
//initialize list of reps of Umsq:=U/U2 as elements of OK.
UmsqOK:=[];
//initialize list of reps of Umsq:=U/U2 as elements of MK.
UmsqMK:=[];

//Param parametrizes elements of Umsq:=U/U2.
Param:=S(n,[0,1]);
for s in Param do
    u:=(s[1])*(Umsq.1);
    for i in [2..n] do
        u:=u+((s[i])*(Umsq.(i)));
    end for;
    // u: an element of Umsq (~s in S(n,[0,1]))
```

```
    // u is expressed in terms of gens of Usq
    Append(~UmsqK,K!y(u));
    Append(~UmsqOK,y(u));
    Append(~UmsqMK,Phi(u));
end for;

// Each tuple in InfoRep corresponds to a representative of U/U^2.
// tuple[1] in K, tuple[2] in OK, tuple[3] in MK
// (using the natural map, Phi).
InfoRep:=[];
for i in [1..2^n] do
    Append(~InfoRep, <UmsqK[i],UmsqOK[i],UmsqMK[i]>);
end for;

Orbits:=[];
MKDONE:=[];
for i in [1..2^n] do
    inforep:=InfoRep[i];
    orbMK:=[inforep];
    for j in [1..n-1] do
        prev:= orbMK[#orbMK];
        uK:=prev[1];
        uOK:=prev[2];
        uMK:=prev[3];
        for k in [1..2^n] do
            inforepTESTER:=InfoRep[k];
            if x(tau(prev[1])) eq x(inforepTESTER[1]) then
                Append(~orbMK,inforepTESTER);
            end if;
```

```
        end for;
    end for;
    Append(~Orbits,Set(orbMK));
end for;

for orb in Orbits do
    orbreps:=[inforep[1]:inforep in orb];
    //alpha is a representative (tuple) of the orbit orb.
    alpha:=orbreps[1];
    star:=true;
    for sig in H do
        a:=alpha;
        b:=sig(alpha);
        if not HilbertSymbol(a,b,2*OK) eq 1 then
            star:=false;
        end if;
    end for;
    if star then
        Append(~StarPos,orb);
    else
        Append(~StarNeg,orb);
    end if;
end for;

StarPos:=Set(StarPos);
StarNeg:=Set(StarNeg);

// 2*(b+1) = # orbits of G acting on MK
b:=Integers()!((2^(n-1)-1)/n);
```

```
    return #StarPos-1;
end function;
```

B.3 Automated Examples

```
KnlSamples:=[[3,7],[5,11],[7,43],[11,23],[13,53],[17,103],[19,191]];

function HypExamples(:info:=true);
    /* check each example number field for the necessary hypotheses */
    MissingHyp:=[];
    for Knl in KnlSamples do
        n:=Knl[1];
        l:=Knl[2];
        K:=Kl(n,l);
        if info then
            print "[K:Q] = ",n, " conductor = ",l;
        end if;
        if not HypBool(K) then
            Append(~MissingHyp,[n,l]);
            if info then
                print "missing hypothesis: ", HypReason(K);
            end if;
        else
            if info then
                print "all hypotheses satisfied";
            end if;
        end if;
```

```
        if info then
            print "-----------------------------";
        end if;
    end for;
    return MissingHyp;
end function;

function StarlightExamples(:info:=true, samples:=KnlSamples);
    /* return a list L=[n,l,mK,d1,d2], each entry of L corresponding to
    a numberfield K where
    <n,l> gives the absolute degree and conductor of K respectively,
    mK:=Starlight(K) is the Starlight invariant,
    d1 is the restricted density (coming from Theorem 4.5.2)
        of rational primes p that satisfy the spin relation
        spin(pp,sigma)=spin(pp,sigma^{-1}) for all sigma in the
        Galois group of K/Q where pp any prime in K above p,
    d2 is the (unrestricted) density of rational primes satisfying
        the same spin relation.

    Input is a list of [n,l] specifying the degrees and conductors
    respectively of number fields satisfying the necessary hypotheses.

    If optional parameter info=true (true by default) then information
    is printed in real time. */

    L:=[];
    for Knl in samples do
        n:=Knl[1];
        l:=Knl[2];
```

```
        K:=Kl(n,l);
        mK:=Starlight(K);
        d1:= (1 + mK*n)/(2^n);
        d2:= (1/(2*n)) + ((n-1)/n)*d1;
        Append(~L,[n,l,mK,d1,d2]);
        if info then
            print "[K:Q] = ",n, " conductor = ",l;
            print "Starlight invariant m_K = ",mK;
            print "restricted density of spin relation = ",d1;
            print "density of spin relation = ",d2;
            print "--------------------------------";
        end if;
    end for;
    return L;
end function;
```

M_4 The multiplicative group with $\mathrm{Gal}(K/\mathbb{Q})$-action,

$$\left(\mathcal{O}_K/4\right)^\times / \left(\left(\mathcal{O}_K/4\right)^\times\right)^2$$

. viii, 30–33, 39, 40, 42–46, 48, 52, 53, 84, 85

$K(p)$ See Definition 5.1.1. xi, 50, 54–56, 60, 62

narrow We call a modulus *narrow* when all real infinite places of the base field divide the modulus. We call a ray class group or field *narrow* when the conductor is narrow . 3, 5, 6, 13, 14, 37, 82

wide We call a modulus *wide* when no real infinite places of the base field divide the modulus. We call a ray class group or field *wide* when the conductor is wide. 6, 13

$\mathrm{n}Cl_K^{\mathfrak{m}}$ the narrow ray class group over K of conductor $\mathfrak{m}$ (Definition 1.1.1) . 6, 10

decomposition group See Definition 1.2.1 . 8

inertia group See Definition 1.2.1 . 8

ramification index See Definition 1.2.2 . 8

inertia degree See Definition 1.2.2 . 8, 46

Frobenius element See Definition 1.2.3 . 9

$\mathrm{Frob}_{L/K}(\mathfrak{p})$ See the remarks following Definition 1.2.3 . 9, 10

$J_K^{\mathfrak{m}}$ the group of fractional ideals of K generated by the primes of K that are coprime to $\mathfrak{m}_0$, the finite part of $\mathfrak{m}$ where $\mathfrak{m}$ is a (narrow) modulus of K. . 9, 10, 82, 83

$P_K^{\mathfrak{m}}$ the subgroup of $J_K^{\mathfrak{m}}$ generated by primes of K which have a generator $\alpha \succ 0$ such that $\alpha \equiv^* 1 \bmod \mathfrak{m}$. . 9–11, 83

Artin map See the beginning of Section 1.3 . 10

conductor see Definition 1.3.2. 10

congruence subgroup a congruence subgroup modulo $\mathfrak{m}$ is a subgroup of $J_K^{\mathfrak{m}}$ containing $P_K^{\mathfrak{m}}$. 10

narrow ray class field see Definition 1.3.4 . 11

$\mathrm{nR}_K^{\mathfrak{m}}$ see Definition 1.3.4 . 11

density see Definition 1.4.1 . 11, 46, 83, 85

$d(R|S)$ the density of primes $p \in S$ which lay in $R \subseteq S$. 11

$\mathrm{Ray}_{L|K}(\sigma)$ the set of primes $\mathfrak{p}$ of K unramified in L/K, a finite abelian extension, such that $\mathrm{Art}_{L|K}(\mathfrak{p}) = \sigma$. 12

U_T The totally positive units of a number field. 13, 14, 16, 19, 20, 30, 50, 83

U^2 The square units of a number field. 13, 14, 16, 19, 20, 30, 50, 83

$h(K)$ The class number of the number field K. 14, 16, 27, 30, 33, 41, 83

$K(n, \ell)$ a number field of degree n over $\mathbb{Q}$ and conductor ℓ that satisfies all of the following conditions.

- K is totally real.
- n is odd.
- $U_T = U^2$.
- K is Galois over $\mathbb{Q}$ with cyclic Galois group.
- The class number $h(K)$ is odd.
- 2 is inert in $K/\mathbb{Q}$.

. 16, 20, 21, 24, 25, 27, 30, 33, 34, 36–39, 41, 42, 44–46, 48, 50, 52, 54, 56–59, 62, 63

BIBLIOGRAPHY

[1] Emil Artin and John Tate. *Class field theory*. AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] D. A. Burgess. On character sums and L-series. II. *Proc. London Math. Soc. (3)*, 13:524–536, 1963.

[4] Nancy Childress. *Class field theory*. Universitext. Springer, New York, 2009.

[5] Keith Conrad. Expository papers. Available at http://www.math.uconn.edu/ kconrad/blurbs/.

[6] J. B. Friedlander, H. Iwaniec, B. Mazur, and K. Rubin. The spin of prime ideals. *Invent. Math.*, 193(3):697–749, 2013.

[7] H. Heilbronn. Zeta-functions and L-functions. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 204–230. Thompson, Washington, D.C., 1967.

[8] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York-Heidelberg, 1977. Universitext.

[9] Christine McMeekin. On the asymptotics of a prime spin relation, 2018. (pre-print) arXiv:1807.00892.

[10] James S. Milne. Algebraic number theory (v3.01), 2008. Available at www.jmilne.org/math/.

[11] J.S. Milne. Class field theory (v4.02), 2013. Available at www.jmilne.org/math/.

[12] Sam Mundy. Conversation.

[13] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German

original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[14] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2):26–37, 1996.