Special Cases of Density Theorems in Algebraic Number Theory

Nathaniel A. Gaertner

Masters Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Mathematics

Dr. Daniel Farkas, Chair
Dr. Charles Parry
Dr. Griff Elder

May 9, 2006
Blacksburg, Virginia

Keywords: Cheboterev, Dirichlet, Density, Number Theory, Algebraic Number Theory, Frobenius

Copyright 2006, Nathaniel A. Gaertner

Special Cases of Density Theorems in Algebraic Number Theory

Nathaniel A. Gaertner

(ABSTRACT)

This paper discusses the concepts in algebraic and analytic number theory used in the proofs of Dirichlet's and Cheboterev's density theorems. It presents special cases of results due to the latter theorem for which greatly simplified proofs exist.

Contents

Chapter 1

Introduction and Construction of Basic Algebraic Structures

1.1 Introduction

In this thesis, we will develop the concepts necessary to understand density theorems in the field of number theory. To begin, the concept of *density* can be thought of as a way to compare the relative size of a set to some larger set containing it. For finite sets, this is a trivial problem. We can just compare the number of elements in each set. If we are dealing with infinite sets, comparison becomes more difficult. Certainly there are meaningful ways in which we can compare the size of two infinite sets. Consider the set of integers which end in 1. This set contains every tenth integer, so we would be inclined to say it is a tenth the size of the set of all integers, or that the density of the smaller set in the larger set is $\frac{1}{10}$. This is still not that interesting a result, but say we take as our larger set the set of all prime integers and as our smaller set the set of all prime integers that end in 1. Now we have two sets for which it is far more difficult to make any meaningful comparison. The question of whether it is possible to define density in some way which will give us information about these types of sets (in particular sets of prime integers) will be discussed. In fact, we will see that, given a certain definition of density, the density of the primes that end in 1 in the set of all primes is still $\frac{1}{10}$. This is due to a theorem proved by Dirichlet in 1837, which states that the primes relatively prime to any given integer m are distributed equally over the equivalence classes of $\mathbb{Z}/(m)^*$.

In algebraic number theory, the theory of algebraic field extensions is used to explore the structures created by adjoining an algebraic number to the field of rational numbers $\mathbb{Q}$, which is itself the quotient field of the integers. Using this material, many theorems pertaining to the integers can be generalized to larger structures. Indeed, each finite algebraic extension of $\mathbb{Q}$ contains a subring which can be thought of in an analogous way to the subring $\mathbb{Z}$ of

$\mathbb{Q}$, and there is a generalization of Dirichlet's theorem for these larger rings. For reasons we shall see, this theorem, proven by Nikolai Cheboterev in 1922, makes a statement about the prime ideals (that is, ideals for which modding out by the ideal produces an integral domain) of these rings, rather than prime elements. Since this theorem is a generalization of Dirichlet's theorem, we will develop the algebraic number theory necessary to understand the broader theorem first.

After we have discussed the Cheboterev theorem, we will note some results due to the theorem which, it turns out, can be shown without resorting to calculations of density at all! Briefly, the statement the theorem makes about the distribution of prime ideals over certain equivalence classes of ideals can be weakened in some cases to a statement merely indicating the presence of prime ideals in those equivalence classes, and this statement remains useful in the proofs of certain results.

1.2 Extending the Integers

The most basic structure involved in this discussion is the number field. Simply, a number field is a finite algebraic extension of the rational numbers, $\mathbb{Q}$. In particular, we will be concerned with number fields which are also Galois extensions of $\mathbb{Q}$. Not all the statements made will apply only to Galois extensions, but eventually, it will become necessary to restrict ourselves to eliminate complications which arise in non-Galois extensions. Since all number fields are algebraic extensions of the rational numbers, they must all lie inside the complex numbers, $\mathbb{C}$, since $\mathbb{C}$ is an algebraically closed extension of $\mathbb{Q}$. Another important subset of $\mathbb{C}$ is the set of *algebraic integers* $\mathbb{A}$. We define this set as the set of all roots of monic polynomials over the integers, $\mathbb{Z}$. (We say such a root is *integral* over $\mathbb{Z}$). Then we say the set of algebraic integers of a number field, $\mathbf{K}$ is the intersection $\mathbf{K} \cap \mathbb{A}$. Certainly all elements of $\mathbb{Z}$ are algebraic integers, but it is easily seen that there are others. $\sqrt{2}$ for example is a root of $x^2 - 2$, and the imaginary number $\imath$ is a root of $x^2 + 1$. We might hope that the algebraic integers of $\mathbb{Q}$ are exactly the normal integers, so that we may think of the algebraic integers as an extension of the integers into larger number fields. This is indeed the case.

Proposition 1.1. *The algebraic integers in $\mathbb{Q}$ are exactly the normal integers $\mathbb{Z}$.*

Proof. Let α be the root of a monic polynomial in $\mathbb{Z}[x]$. Then

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

for some $a_{n-1} \cdots a_0 \in \mathbb{Z}$. Assume $\alpha = b/c$ with $b, c \in \mathbb{Z}$, and gcd(b, c)= 1. Then

$$c^n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = b^n + a_{n-1}cb^{n-1} + \cdots + a_1c^{n-1}b + a_0c^n = 0.$$

But then $c|b^n$ and b and c are relatively prime, so $c = 1$; hence, α is an integer and $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$. □

Next we wish to see that the algebraic integers form a ring. It suffices to show that the set is closed under addition and multiplication. It is not obvious that $\alpha+\beta$ and $\alpha\beta$ are roots of monic integer polynomials, so we take a different tack and prove a more general result which will serve to prove what we want.

Lemma 1.2. *Let α be an element of $\mathbb{C}$. The following are equivalent:*

1. *α is integral over $\mathbb{Z}$.*
2. *$\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.*
3. *$\mathbb{Z}[\alpha]$ is contained in a subring of $\mathbb{C}$ which is a finitely generated $\mathbb{Z}$-module.*
4. *There is a $\mathbb{Z}[\alpha]$-module $\mathbf{M}$ such that $\mathbf{M}$ is a finitely generated $\mathbb{Z}$-module, and the only element a of $\mathbb{Z}[\alpha]$ such that $a\mathbf{M}= 0$ is 0.*

Proof. (1)⇒(2): If α is a root of a monic n-th degree polynomial, it is easily seen that $1, \alpha, \cdots, \alpha^{n-1}$ form a basis for $\mathbb{Z}[\alpha]$ over $\mathbb{Z}$. (2)⇒(3): $\mathbb{Z}[\alpha]$ is contained in itself. (3)⇒(4): The subring of $\mathbb{C}$ from (3) satisfies the requirements for M, since it contains 1. (4)⇒(1): Let $m_1, m_2, \cdots, m_n$ be a set of generators for $\mathbf{M}$ over $\mathbb{Z}$. Let

$$\alpha m_i = \sum_{j=1}^{n} a_{ij} m_j.$$

Let $A = \alpha I - [a_{ij}]$ and let B be the adjoint matrix of A. Then $BA = \det(A)I$, so

$$A(m_1, m_2, \cdots, m_n)^T = 0 \Rightarrow BA(m_1, m_2, \cdots, m_n)^T = 0 \Rightarrow \det(A)(m_1, m_2, \cdots, m_n)^T = 0,$$

so det(A)$\mathbf{M}$= 0. By assumption, det(A)= 0. Then

$$f(x) = \det(xI - [a_{ij}])$$

is a monic polynomial with α as a root. □

Now we have that $\mathbb{A}$ is a ring: let x and y be integral over $\mathbb{Z}$. Then $\mathbb{Z}[xy]$ and $\mathbb{Z}[x + y]$ are contained in $\mathbb{Z}[x, y]$, which is finitely generated over $\mathbb{Z}$, so by (3)⇒(1) of the lemma, they are both integral.

Thus the algebraic integers of a number field form a subring (called the *number ring*) of the number field.

Definition. If $\mathbf{R}$ is an integral domain, the *integral closure* of $\mathbf{R}$ in its field of fractions $\mathbf{K}$ is the set of all elements of $\mathbf{K}$ which are integral over $\mathbf{R}$.

We say $\mathbf{R}$ is *integrally closed* if it is its own integral closure. We next wish to see that number rings are integrally closed in their number fields.

Proposition 1.3. *For any number field* $\mathbf{K}$*,* $\mathbf{R}= \mathbb{A} \cap \mathbf{K}$ *is integrally closed in* $\mathbf{K}$

Proof. Let α be integral over $\mathbf{R}$. Then

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

with the a_i's in $\mathbf{R}$. Then

$$\mathbb{Z}[a_0, a_1, \cdots, a_{n-1}]$$

is finitely generated over $\mathbb{Z}$ and α is integral over

$$\mathbb{Z}[a_0, a_1, \cdots, a_{n-1}],$$

so

$$\mathbb{Z}[a_0, a_1, \cdots, a_{n-1}, \alpha]$$

is finitely generated over

$$\mathbb{Z}[a_0, a_1, \cdots, a_{n-1}],$$

and thus also over $\mathbb{Z}$. It follows that $\mathbb{Z}[\alpha]$ must also be finitely generated over $\mathbb{Z}$ by (3)⇒(2) in the Lemma above. □

Now, all number fields are separable extensions of $\mathbb{Q}$, since $char\mathbb{Q} = 0$. This implies that, given any number field $\mathbf{K}$, $\mathbf{K}= \mathbb{Q}(\alpha)$ for some $\alpha \in \mathbf{K}$. We can actually choose α to be in the number ring $\mathbf{R}$ of $\mathbf{K}$. To see this, say

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

is the minimal polynomial for α. Then $a_n\alpha$ has minimal polynomial

$$x^n + a_{n-1}x^{n-1} + a_n a_{n-2}x^{n-2} + \cdots + a_n^{n-2}a_1 x + a_n^{n-1}a_0,$$

and $a_n\alpha$ must still generate $\mathbf{K}$ over $\mathbb{Q}$, since $\frac{1}{a_n} \in \mathbb{Q}$ implies $\alpha \in \mathbb{Q}(a_n\alpha)$. Given that we can now assume that α is in $\mathbf{R}$, it is tempting to guess that $\mathbf{R}$ is $\mathbb{Z}(\alpha)$. Unfortunately, it is not even always the case that $\mathbf{R}$ can be generated over $\mathbb{Z}$ by a single element. (However, this actually is the case for quadratic extensions, as we will see later.)

Proposition 1.4. *There exist number rings which are not of the form* $\mathbb{Z}[\alpha]$

Proof. Let $\mathbf{K}= \mathbb{Q}(\sqrt{7}, \sqrt{10})$. To illustrate that $\mathbf{R}$ cannot be generated by only one algebraic integer α over $\mathbb{Z}$, we will produce four elements of $\mathbf{R}$, $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ with the property that for $i \neq j, \alpha_i\alpha_j/3$ is an algebraic integer but for $i = j, \alpha_i\alpha_j/3$ is not. To see the significance of this, let $f(x)$ be the minimal polynomial of α over $\mathbb{Z}$, and let $f_i(x)$ be such that $\alpha_i = f_i(\alpha)$. Such a polynomial must exist under the assumption that $\mathbf{R}= \mathbb{Z}[\alpha]$. Now, for any polynomial $g(x)$, let $\overline{g}(x)$ denote the reduction of $g(x)$ mod(3). (That is, we reduce the coefficients of $g(x)$ modulo 3). Now we want to see that $g(\alpha)$ is divisible by 3 in $\mathbb{Z}[\alpha] \Leftrightarrow \overline{f}(x)|\overline{g}(x)$ Assume

$g(\alpha)$ divisible by 3 in $\mathbb{Z}[\alpha]$. Then $g(\alpha)/3 \in \mathbb{Z}[\alpha]$. This implies that α is a root of $\overline{g}(x)$. In fact, since $g(\sigma(\alpha))/3 \in \mathbb{Z}[\alpha]$ for all σ in the Galois group, we know that all $\sigma(\alpha)$ are roots of $\overline{g}(x)$. Thus $\overline{g}(x)$ is of at least degree 4, and has as roots all of the the roots of $\overline{f}(x)$, which is of at most degree 4. This implies that $\overline{f}(x)|\overline{g}(x)$. Going in the other direction, $\overline{f}(x)|\overline{g}(x)$ implies that α is a root of $\overline{g}(x)$, which immediately implies that 3 divides $g(\alpha)$ in $\mathbb{Z}[\alpha]$. Now we see that if we can produce the desired α_i's, we will have produced $f_i(x)$'s such that $\overline{f}(x)|\overline{f_i}(x)\overline{f_j}(x) \Leftrightarrow i \neq j$. This implies that $\overline{f}(x)$ has distinct factors not dividing each $\overline{f_i}(x)$. Since there are 4 $f_i(x)$'s, this implies that $\overline{f}(x)$ splits into 4 distinct linear factors. This is ridiculous, since $\mathbb{Z}/(3)[x]$ only contains 3 linear polynomials. The task now is to demonstrate that these α_i's exist. Getting back to our chosen field $\mathbf{K}$, we choose

$$\alpha_1 = (1+\sqrt{7})(1+\sqrt{10}), \alpha_2 = (1+\sqrt{7})(1-\sqrt{10}),$$

$$\alpha_3 = (1-\sqrt{7})(1+\sqrt{10}), \alpha_4 = (1-\sqrt{7})(1-\sqrt{10}).$$

These are all algebraic integers, since for any number $\gamma = a + b\sqrt{m}$, γ is a root of the polynomial

$$x^2 - 2ax + a^2 - b^2m,$$

and we have shown $\mathbf{R}$ is closed under multiplication. Now any product $\alpha_i\alpha_j, i \neq j$ contains either

$$(1+\sqrt{7})(1-\sqrt{7}) = -6 \text{ or } (1+\sqrt{10})(1-\sqrt{10}) = -9.$$

So all these products are divisible by 3. All that remains is to show that the square of any α_i is not divisible by 3. To this end, we define the *trace* function of $\mathbf{K}$ over $\mathbb{Q}$.

Definition. The trace of an element, $Tr(\gamma)$, is defined by

$$Tr(\gamma) = \sigma_1(\gamma) + \sigma_2(\gamma) + \cdots + \sigma_n(\gamma),$$

where the σ_i's are all the elements of the Galois group.

A useful attribute of the trace function that we will use is that the trace of an algebraic integer is an integer. This is seen by observing that, given an algebraic integer γ, the minimal polynomial of γ splits into

$$(x-\gamma)(x-\sigma_1(\gamma))\cdots(x-\sigma_n(\gamma))$$

in any normal extension of $\mathbf{K}$ and that if we multiply this out, the negative of the coefficient of x^{n-1} is the sum of the constant terms in every factor. This is exactly the trace of γ. (Alternatively we could note that the trace is a symmetric sum of algebraic integers, and thus fixed by the Galois group. This implies that $Tr(\gamma) \in \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$). Armed with this observation, we note that

$$Tr(\alpha_i^n) = \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n$$

and that, because $3|\alpha_i\alpha_j, i \neq j$, this is congruent to

$$(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n \bmod 3.$$

Summing the α_i's, we see that

$$Tr(\alpha_i^n) \equiv 4^n \equiv 1 \text{ mod } 3.$$

Then $Tr(\alpha_i^n/3) \notin \mathbb{Z}$, so $\alpha_i^n/3$ is not an algebraic integer. □

We have now succeeded in showing that there exist number fields with number rings not generated by one element over $\mathbb{Z}$.

1.3 Number Rings are UFD's for Ideals

Another complication that presents itself is the fact that arbitrary number rings are not necessarily principal ideal domains and consequently, not unique factorization domains either. Examples of this are more easily created than in the above discussion. $\mathbf{R} = \mathbb{Z}[\sqrt{-13}]$ is a good example (We'll see why this is definitely a number ring later). In this ring, the number 14 admits to its usual factorization: $2 \cdot 7 = 14$. It also factors into two different numbers: $(1-\sqrt{-13})\cdot(1+\sqrt{-13})$. The question now becomes: are these really different factorizations? Right now we could have an example no more remarkable than saying $18 \cdot 2 = 36 = 9 \cdot 4$. The relevant concern is whether or not these are irreducible factors. All elements of $\mathbf{R}$ are of the form $a + b\sqrt{-13}$, so let us try to factor 2 and 7. Say

$$(a + b\sqrt{-13}) \cdot (c + d\sqrt{-13}) = 2.$$

Then we know that

$$(a - b\sqrt{-13}) \cdot (c - d\sqrt{-13}) = 2,$$

since 2 is in the fixed field of the Galois group. Multiplying both equations together, we get

$$(a + 13b^2) \cdot (c + 13d^2) = 4,$$

implying that $a+13b^2$ and $c+13d^2$ can only be 1, 2, or 4. Thus $b = d = 0$, so the factorization can only be the normal factorization of 2 in $\mathbb{Z}$, which is trivial. The same argument works for 7, so we have demonstrated that 2 and 7 are irreducible in $\mathbf{R}$. Now, it is possible that $(1 - \sqrt{-13})$ and $(1 + \sqrt{-13})$ differ from 2 and 7 only by units, in which case we would have a situation analogous to factoring a number into its positive and negative divisors. If this is true, either $(1-\sqrt{-13})/2$ or $(1+\sqrt{-13})/2$ should be a unit of $\mathbf{R}$. When we later discuss the number rings of quadratic number fields, we will see that this is impossible, since neither of these are even elements of $\mathbf{R}$, much less units. Thus we have demonstrated that $\mathbf{R}$ is not a UFD and hence not a PID either. The next point of curiosity is to actually produce a non-principal ideal. This is not particularly difficult. $(2, 1+\sqrt{-13})$ suffices. To demonstrate that this is indeed a proper ideal, we note that

$$(2, 1 + \sqrt{-13})^2 = (4, 2 + 2\sqrt{-13}, -12 + 2\sqrt{-13})$$

(we are defining ideal multiplication in the usual way, with the elements of a product of ideals being sums of the products of every pairing of generators), and that we can manipulate these generators to see that 2 is contained in this ideal, and thus that the ideal (2) is contained in it as well. Since all the generators are multiples of 2, this shows that

$$(2, 1 + \sqrt{-13})^2 = (2).$$

We argue that $(2, 1 + \sqrt{-13}) \neq \mathbf{R}$. Otherwise, its square would also be $\mathbf{R}$, and we know that it cannot be principle, since this would require a common divisor of both generators, which we've shown does not exist in $\mathbf{R}$. This factorization of the ideal (2) raises an interesting question: we couldn't factor the number 2, but we could factor the ideal. What then will happen if we find factorizations of the rest of the relevant principal ideals? It turns out that we get

$$(1 - \sqrt{-13}) = (2, 1 + \sqrt{-13}) \cdot (7, 1 - \sqrt{-13}), (1 + \sqrt{-13}) = (2, 1 + \sqrt{-13}) \cdot (7, 1 + \sqrt{-13}),$$

$$\text{and } (7) = (7, 1 + \sqrt{-13}) \cdot (7, 1 - \sqrt{-13}).$$

This result seems to imply that, if we factor our divisors of 14 further into ideals, these two factorizations are actually the same. In fact, number rings do have the unique factorization property, but for ideals rather than for elements. We show that this holds for a larger class of rings known as Dedekind domains.

Definition. An integral domain is a *Dedekind domain* if the following hold:

1. It is Noetherian.
2. Every nonzero prime ideal is maximal.
3. It is integrally closed.

We will begin by noting that we have already shown that number rings satisfy the third condition. It remains to show that they satisfy the first two. Before we do that, let us see what exactly is relevant about these conditions. In particular, let us see how these conditions are related to the problem of unique factorization for ideals. To do this, we will look at some examples of rings which do not satisfy these conditions and see how unique factorization can fail.

First, we look at a non-Noetherian ring. Consider the ring $\mathbf{R}$ generated over $\mathbb{Z}$ by all p^n-th roots of 2 for some prime p. Then we can make an infinitely ascending chain of ideals by simply taking the chain $A_1 \subset A_2 \subset A_3 \ldots$ where $A_i = (2^{1/p^i})$. The problem is immediately apparent. Any member of this chain has an infinite number of factors. A factorization like this really isn't that useful to us. What we're really after is the ability to talk about the entire set of ideals as generated by a subset of irreducibles.

Second, take a ring which does not satisfy the second property, but is Noetherian and integrally closed. $\mathbf{R} = \mathbf{F}[x, y]$, $\mathbf{F}$ a field, will work. We know that $\mathbf{R}$ is Noetherian by the Hilbert Basis Theorem. Now, consider the ideal (x^2, y^2). Any prime ideal containing this ideal contains both x and y, so the only candidate is (x, y). Hence, if (x^2, y^2) is a product of prime ideals, it must be some power of (x, y).

$$(x, y)^2 = (x^2, xy, y^2), \text{ and } (x, y)^3 = (x^3, x^2y, xy^2, y^3).$$

The former must contain (x^2, y^2) properly, since xy is not in (x^2, y^2), and the latter must be properly contained in (x^2, y^2), since it does not contain x^2 or y^2. Note also that if we let $\mathbf{K}$ be the field of fractions of $\mathbf{R}$; and we try to find an inverse of (x, y), we will fail: Assume such an inverse exists. Call it $\mathfrak{N}$. $\mathfrak{N}(x, y) = \mathbf{R}$, so $1 \in \mathfrak{N}(x, y)$. Then $\mathfrak{N}$ must contain the inverse of some polynomial in (x, y), say $g(x, y)^{-1}$. Then $xg(x, y)^{-1} \in \mathbf{R}$, so

$$xg(x, y)^{-1} = f(x, y)$$

for some polynomial $f(x, y)$. Then

$$x = g(x, y)f(x, y).$$

The only possiblities for $g(x, y)$ and $f(x, y)$ are then x and 1. 1 is not in (x, y), so $g(x, y) = x$, but if we replace x with y in this argument, we have $g(x, y) = y$. This is a contradiction, so $\mathfrak{N}$ cannot exist.

We start out proof of unique factorization of ideals with the following definition:

Definition. An ideal $\mathfrak{A}$ is said to be invertible if there exists an $\mathbf{R}$-module $\mathfrak{A}^{-1}$, finitely generated by elements of $\mathbf{K}$, such that $\mathfrak{A}\mathfrak{A}^{-1} = \mathbf{R}$.

Now we will show that in a Dedekind domain, prime ideals are invertible. Given $\mathfrak{P}$, define $\mathfrak{N}$ as $\{a : a \in \mathbf{K}, a\mathfrak{P} \subseteq \mathbf{R}\}$. For any $a \in \mathfrak{P}$, $a\mathfrak{N} \subseteq \mathbf{R}$, so $\mathfrak{N} \subseteq a^{-1}\mathbf{R}$. $\mathbf{R}$ is Noetherian, and $a^{-1}\mathbf{R}$ is a finitely generated $\mathbf{R}$ module, so $\mathfrak{N}$ must be as well. $\mathfrak{P} \subseteq \mathfrak{P}\mathfrak{N} \subseteq \mathbf{R}$. Hence $\mathfrak{P}\mathfrak{N} = \mathfrak{P}$ or $\mathbf{R}$. Say it equals $\mathfrak{P}$. Then for any $n \in \mathfrak{N}$; $a \in \mathfrak{P}$, $n^i a \in \mathfrak{P}$ for all i. Thus we have that $\mathfrak{B} = \sum_{i=1}^{\infty}(n^i a)$ is an ideal of $\mathbf{R}$. $\mathbf{R}$ is Noetherian, so this must be finitely generated. Say $\{n^i a : i \in I, I \text{ a finite set of natural numbers}\}$ generates $\mathfrak{B}$. Then let j be any natural number not in I.

$$n^j = \sum_{i \in I} n^i a r_i$$

for some $r_i \in \mathbf{R}$. Thus we have that all $n \in \mathfrak{N}$ are integral over $\mathbf{R}$. Since $\mathbf{R}$ is integrally closed, this implies $\mathfrak{N} \subseteq \mathbf{R}$. If we can show that this is not true, we must have $\mathfrak{N}\mathfrak{P} = \mathbf{R}$. Given any $a \in \mathfrak{P}$, we have that $\mathfrak{P}\mathfrak{C} \subseteq (a)$ for some ideal $\mathfrak{C}$ not contained in (a). Thus there exists $b \in \mathfrak{C}$ with the property $b\mathfrak{P} \subseteq (a)$. Then $\frac{b}{a} \in \mathfrak{N}$, but $\frac{b}{a} \notin \mathbf{R}$, because $b \notin (a)$. Now we have our contradiction, and $\mathfrak{N}\mathfrak{P}$ must be $\mathbf{R}$. Thus we have that prime ideals are invertible.

We can use this to show that Dedekind domains have the unique factorization property for ideals. Given any ideal $\mathfrak{A} \subset \mathbf{R}$, we know that $\mathfrak{A}$ must contain some product of prime ideals.

If not, there must exist a maximal ideal $\mathfrak{B}$ that does not contain a product of primes, by the fact that $\mathbf{R}$ is Noetherian. $\mathfrak{B}$ cannot be prime, so there must be some elements a and b of $\mathbf{R}$ with $ab \in \mathfrak{B}$. Then $(a)(b) \subseteq \mathfrak{B}$. But then (a) and (b) must contain products of primes, since they properly contain $\mathfrak{B}$. Then $(a)(b)$ contains the product of the products of primes contained in (a) and (b), so $\mathfrak{B}$ must also contain this product. Now say $\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_n \subseteq \mathfrak{A}$ is the shortest product of primes contained in $\mathfrak{A}$. (That is, n is minimal.) If $n = 1, \mathfrak{A}$ is prime and we are done. For $n \geq 1, \mathfrak{A}$ is not prime, so there exists a prime ideal $\mathfrak{P}$ containing $\mathfrak{A}$. Then $\mathfrak{P}$ contains the product $\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_n$, so $\mathfrak{P}$ contains one of the $\mathfrak{P}_i$. Since primes are maximal, $\mathfrak{P}_i = \mathfrak{P}$. Say $i = 1$. Then we have

$$\mathfrak{P}\mathfrak{P}^{-1} \subseteq \mathfrak{A}\mathfrak{P}^{-1} \subseteq \mathfrak{P}_2\mathfrak{P}_3\cdots\mathfrak{P}_n.$$

Then, inducting, $\mathfrak{A}\mathfrak{P}^{-1}$ is a product of prime ideals. Thus $\mathfrak{A}$ must be this product multiplied by $\mathfrak{P}$. Finally, to show that the factorization must be unique, let

$$\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_n = \mathfrak{Q}_1\mathfrak{Q}_2\cdots\mathfrak{Q}_m.$$

Then for each $\mathfrak{P}_i$, we have

$$\mathfrak{Q}_1\mathfrak{Q}_2\cdots\mathfrak{Q}_m \subset \mathfrak{P}_i,$$

so $\mathfrak{Q}_j = \mathfrak{P}_i$ for some $\mathfrak{Q}_j$. Multiplying both sides by $\mathfrak{P}_i^{-1} = \mathfrak{Q}_j^{-1}$ gives a shorter product on both sides, and continuing this process must eventually lead us to the equivalence of the two factorizations.

Now we finish by proving the following:

Proposition 1.5. *Number rings are Dedekind domains.*

Proof. We will require the following definition:

Definition. The *norm* of an element $\alpha \in \mathbf{R}$ is defined as

$$N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$$

where G is the galois group of the extension.

We've already shown that number rings are integrally closed. We need to show that the other two conditions hold. Showing that each nonzero prime ideal is maximal hinges on being able to show that $\mathbf{R}$ is Noetherian: We know that $\mathbf{R}/\mathfrak{P}$ is an integral domain for any prime ideal $\mathfrak{P}$. If we can show that it is finite, we will have shown that it is a field, and thus that $\mathfrak{P}$ is maximal. Certainly, $\mathfrak{P}$ contains the norms of its elements, which are in $\mathbb{Z}$, so the order of $\mathbf{R}/\mathfrak{P}$ is less than the order of $\mathbf{R}/(m)$ for some integer m. If we can show that $\mathbf{R}$ is a finitely generated $\mathbb{Z}$ module, we will have both the Notherian and the maximal ideal requirements. We have shown already that $\mathbf{R}$ cannot necessarily be generated over $\mathbb{Z}$ by one element of $\mathbf{R}$, but since $\mathbf{K}$ is a separable extension of $\mathbb{Q}$, we know it is equal to $\mathbb{Q}(\theta)$

for some $\theta \in \mathbf{K}$. In fact, we can choose θ to be in $\mathbf{R}$, since multiplying θ by any integer does not affect its ability to generate $\mathbf{K}$, as $\mathbf{K}$ contains all of $\mathbb{Q}$. So we can choose some $\theta \in \mathbf{R}$ with $\mathbb{Z}[\theta] \subseteq \mathbf{R} \subset \mathbb{Q}[\theta]$. This leads us to prove the following lemma:

Lemma 1.6. *There exists a finite set of elements of* $\mathbb{Q}[\theta]$ *which generate* $\mathbf{R}$.

Proof. Let α be any element of $\mathbf{R}$ and set

$$\alpha = q_0 + q_1\theta + \cdots q_{n-1}\theta^{n-1}, q_i \in \mathbb{Q}.$$

Now we form the matrix equation:

$$\begin{pmatrix} 1 & \theta & \cdots & \theta^{n-1} \\ 1 & \sigma_1(\theta) & \cdots & \sigma_1(\theta^{n-1}) \\ 1 & \sigma_2(\theta) & \cdots & \sigma_2(\theta^{n-1}) \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_{n-1}(\theta) & \cdots & \sigma_{n-1}(\theta^{n-1}) \end{pmatrix} \begin{pmatrix} q_0 \\ q_1 \\ q_2 \\ \vdots \\ q_{n-1} \end{pmatrix} = \begin{pmatrix} \alpha \\ \sigma_1(\alpha) \\ \sigma_2(\alpha) \\ \vdots \\ \sigma_{n-1}(\alpha) \end{pmatrix}$$

We can solve for the q_i's using Cramer's rule to get $q_i = A_i/det(\sigma_i(\theta^j))$ where A_i is the determinant of the matrix obtained from replacing the i'th column of $(\sigma_i(\theta^j))$ with the vector on the right. The important thing to note is that these A_i's are in $\mathbf{R}$, and $det(\sigma_i(\theta^j))$ is an algebraic integer which itself is not fixed by the Galois group, but whose square is (the determinant of a matrix may have its sign changed by re-ordering the rows, but the magnitude remains the same.) Say $d = (det(\sigma_i(\theta^j)))^2$, then $dq_i = A_i det(\sigma_i(\theta^j)) \in \mathbf{R}$. But $dq_i \in \mathbb{Q}$ as well, so it is in $\mathbb{Z}$. □

Now we have shown that θ does generate $\mathbf{R}$ over $\frac{1}{d}\mathbb{Z}$, or more familiarly,

$$\mathbf{R} = \mathbb{Z}[1/d, \theta/d, \theta^2/d, \cdots, \theta^{n-1}/d].$$

Thus $\mathbf{R}$ is a finitely generated $\mathbb{Z}$ module of at most degree n, the degree of the field extension $\mathbf{K}$ over $\mathbb{Q}$. Indeed, we know that $1, \theta, \theta^2, \cdots, \theta^{n-1}$ are linearly independent in $\mathbf{R}$, so $\mathbf{R}$ is exactly an nth degree $\mathbb{Z}$ module. Since $\mathbb{Z}$ is a Noetherian ring, this gives us that $\mathbf{R}$ is Noetherian. Of course, this immediately implies that all prime ideals are maximal by the work we did above. □

We have now shown that number rings satisfy all the conditions for being Dedekind domains.

1.4 Fractional Ideals and the Class Group

Definition. A *fractional ideal* is an $\mathbf{R}$-module which is finitely generated by elements of $\mathbf{K}$.

When we are discussing fractional ideals, we refer to ideals contained in $\mathbf{R}$ as *integral ideals*. If we define multiplication on fractional ideals in the same way as we did for integral ideals, it is easy to see that the fractional ideals form a group. They are certainly closed under multiplication, and $\mathbf{R}$ serves as the identity. It remains to show that inverses exist for every element. We have already shown that inverses exist for prime ideals in $\mathbf{R}$. Given a fractional ideal $\mathfrak{M}$, we can find an element a of $\mathbf{R}$ such that $a\mathfrak{M} \subseteq \mathbf{R}$. Then $a\mathfrak{M}$ has a unique factorization into prime ideals. Let

$$a\mathfrak{M} = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_n$$

$$\mathfrak{M} = a^{-1}\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_n$$

$$\mathfrak{M}^{-1} = a\mathfrak{P}_1^{-1}\mathfrak{P}_2^{-1}\cdots\mathfrak{P}_n^{-1}.$$

Thus the fractional ideals form a group, which we refer to as the *ideal group*.

We can go further than this and form a smaller group out of the ideals by defining an equivalence relation which places all the principal ideals in a class together. We call this group the *class group*. We say two fractional ideals $\mathfrak{A}$ and $\mathfrak{B}$ are equivalent if there exist a and b in $\mathbf{K}$ such that $a\mathfrak{A} = b\mathfrak{B}$. Since multiplication is commutative, this is symmetric. Setting $a = b = 1$ gives us reflexivity, and if $a\mathfrak{A} = b\mathfrak{B}$ and $c\mathfrak{B} = d\mathfrak{C}$, then $a\mathfrak{A} = b\mathfrak{B} = bdc^{-1}\mathfrak{C}$, so the relation is transitive. Multiplication on the set of equivalence classes is defined in the obvious way: $[\mathfrak{A}][\mathfrak{B}] = [\mathfrak{A}\mathfrak{B}]$. To see that this is well defined, let $a\mathfrak{A} = b\mathfrak{B}, c\mathfrak{C} = d\mathfrak{D}$. Then $ac\mathfrak{A}\mathfrak{C} = bd\mathfrak{B}\mathfrak{D}$. We set the equivalence class of principal ideals to be the identity, and the existence of inverses is automatic from the existence of inverses in the ideal group. Notice that every equivalence class must contain an integral ideal. This gives us the result that, given any integral ideal, there must be another integral ideal such that their product is principal. If the class group is finite, we further have that given any integral ideal, some power of that ideal must be principal. The class group will show up later in the discussion of density of ideals in a subset of the ideal group, but for now we move on to some discussion of the behavior of primes in field extensions.

Chapter 2

Application of Galois Theory to Number Fields

2.1 Factoring a prime of $\mathbb{Z}$ in $\mathbf{R}$

Given a prime number p in $\mathbb{Z}$, we know $p\mathbf{R}$ is an ideal of $\mathbf{R}$, but not necessarily a prime ideal. We can see this in an example: $\mathbb{Z}[\sqrt{-5}]$. 3 is a prime number, but the ideal $3\mathbf{R}$ is not prime at all. $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are not in $3\mathbf{R}$, but their product, 6, is. On the other hand, we know that ideals of $\mathbf{R}$ are products of prime ideals, so $p\mathbf{R} = \mathfrak{P}_1^{a_1}\cdots\mathfrak{P}_g^{a_g}$.

$$3\mathbf{R} = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}),$$

for example. Note that these ideals are conjugates of each other. In general, we can make the following statements:

Proposition 2.1. *1. Given any σ in the Galois group G of $\mathbf{K}$ over $\mathbb{Q}$, $\sigma(p) = p$.*

2. $\sigma(\mathfrak{P})$ is a prime ideal sitting over p for any prime ideal $\mathfrak{P}$ sitting over p.

3. Given $\mathfrak{P}_1, \mathfrak{P}_2$, there exists $\sigma \in G$ such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.

Proof. 1. This is obvious, since p is in the fixed field of G.

2. Given any $ab \in \sigma(\mathfrak{P})$, we have $\sigma^{-1}(ab) \in \mathfrak{P}$. Since σ^{-1} is a homomorphism, one of $\sigma^{-1}(a), \sigma^{-1}(b)$ must be in $\mathfrak{P}$. Thus one of a, b must be in $\sigma(\mathfrak{P})$. So $\sigma(\mathfrak{P})$ must be a prime ideal. What's more, it must contain p, since $p = \sigma(p) \in \mathfrak{P}$. So $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$ for some $1 \leq j \leq g$.

3. Given a prime $\mathfrak{P}$ sitting over p, say there is no $\sigma \in G$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}_i$ for a certain $\mathfrak{P}_i$ sitting over p. Then we can find an element α which is in $\mathfrak{P}$, but such that

$\sigma(\alpha) \notin \mathfrak{P}_i$ for any σ. But we know that $N(\alpha) \in \mathfrak{P} \cap \mathbb{Z}$ which must be a prime ideal of $\mathbb{Z}$ and thus must be p. This is a contradiction, since $p \subset \mathfrak{P}_i$.

□

So we have that G permutes the primes sitting over p transitively. Now we have actually obtained the fact that in a normal extension, all the exponents of the primes dividing p must be equal. That is, we actually have $p = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ for some integer e. It is tempting now to assume that the product $\sigma_1(\mathfrak{P}) \cdots \sigma_n(\mathfrak{P}) = p\mathbf{R}$. Unfortunately, this is not actually the case; we may have a prime ideal of $\mathbb{Z}$ which is also prime as an ideal of $\mathbf{R}$. As an example, the number ring of the field $\mathbb{Q}[\sqrt{7}]$ is $\mathbb{Z}[\sqrt{7}]$, and the prime 5 in $\mathbb{Z}$ remains prime in $\mathbb{Z}[\sqrt{7}]$: let

$$(a + b\sqrt{7})(c + d\sqrt{7}) = 5\alpha$$

for some $\alpha \in \mathbb{Z}[\sqrt{7}]$. Then taking the norms of both sides, we have

$$(a^2 - 7b^2)(c^2 - 7d^2) = 25k$$

for some integer k. Thus

$$(ac)^2 - 7((bc)^2 + (ad)^2) + 49(bd)^2 = 25k,$$

so $(ac)^2 \equiv 7 \bmod(25)$, which implies $(ac)^2 \equiv 2 \bmod(5)$, which is impossible, since 2 is not a square mod(5). Then the product $\sigma_1(5)\sigma_2(5) = 25$, not 5, as we hoped. On the other hand, $\mathbf{R}/(5)$ is a finite field of order 25, which leads us to wonder: is

$$\prod_{\sigma \in G} \sigma(\mathfrak{P}) = |\mathbf{R}/\mathfrak{P}|\mathbf{R}?$$

If so, then we also have

$$\prod_{\sigma \in G} \sigma(\mathfrak{P}) = |\mathbf{R}/\mathfrak{P}_i|\mathbf{R}$$

for any $\mathfrak{P}_i$ sitting over p, since there is a natural isomorphism between $\mathbf{R}/\mathfrak{P}$ and $\mathbf{R}/\mathfrak{P}_i$ given by the element σ of the Galois group which sends $\mathfrak{P}$ to $\mathfrak{P}_i$. The result we rely on to answer this question is the analog for ideals of the Chinese Remainder Theorem for the integers.

Theorem 2.2. *(Chinese Remainder Theorem) Given a set of ideals with the property that we can choose elements u, v from any pair of the ideals such that $u + v = 1$, then we can find an element of* $\mathbf{R}$ *such that the element is congruent to a given value in the residue field of each ideal.*

Proof. For two ideals, $\mathfrak{A}_1, \mathfrak{A}_2$, this is easy. Let x_1 and x_2 be the two desired values in the residue fields. Then set $x = x_2u + x_1v$ Since $v \equiv 1 \bmod(\mathfrak{A}_1)$ and $u \equiv 1 \bmod(\mathfrak{A}_2)$, the result follows. We then induct on the number of ideals by finding an element of $\mathbf{R}$ which is in all the ideals we have previously dealt with, but which is congruent to 1 mod our new ideal. Our condition says that this is possible. Therefore we can map $\mathbf{R}$ surjectively to the direct sum $\oplus\mathbf{R}/\mathfrak{A}_n$. □

The kernel of the map is the product of all the ideals, so in the case of the primes dividing p above, we have $\mathbf{R}/(p) \cong \oplus \mathbf{R}/\mathfrak{P}_n^e$. Mapping $\mathbf{R}/\mathfrak{P}^e$ into $\mathbf{R}/\mathfrak{P}^{e-1}$ by the obvious homomorphism, we see that the kernel of the map is $\mathfrak{P}^{e-1}/\mathfrak{P}^e$. Thus

$$|\mathbf{R}/\mathfrak{P}^e| = |\mathbf{R}/\mathfrak{P}^{e-1}||\mathfrak{P}^{e-1}/\mathfrak{P}^e|.$$

Inducting, we can see that

$$|\mathbf{R}/\mathfrak{P}^e| = \prod_{i=1}^{n} |\mathfrak{P}^{i-1}/\mathfrak{P}^i|.$$

The invertibility of prime ideals gives us an isomorphism between $\mathfrak{P}^{i-1}/\mathfrak{P}^i$ and $\mathbf{R}/\mathfrak{P}$. Thus $|\mathbf{R}/\mathfrak{P}^e| = e|\mathbf{R}/\mathfrak{P}|$. Now from the Chinese Remainder Theorem, we have

$$p^n = |\mathbf{R}/(p)| = \prod |\mathbf{R}/\mathfrak{P}_n^e| = |\mathbf{R}/\mathfrak{P}_n|^e g,$$

where g is the number of primes dividing p. It follows then that $|\mathbf{R}/\mathfrak{P}_n| = p^{n/eg}$. We say $f = n/eg$ is the *inertial degree* or just degree of $\mathfrak{P}_n$. With one more clarification, this gives that

$$\prod_{\sigma \in G} \sigma(\mathfrak{P}) = |\mathbf{R}/\mathfrak{P}|\mathbf{R}.$$

Definition. The *decomposition group* D of a prime $\mathfrak{P}$ is the subgroup of G that fixes $\mathfrak{P}$ (not necessarily element-wise.)

Let σD be a coset of D in G. Then since G permutes the primes sitting over p transitively, there exists a σ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$ for all $\mathfrak{P}_j$ sitting over p and if $\sigma_1(\mathfrak{P}) = \sigma_2(\mathfrak{P})$, then $\sigma_2^{-1}\sigma_1 \in D$, so there are exactly g cosets of D in G, implying that $|D| = ef$. Now we know there must be exactly ef copies of each $\mathfrak{P}_i$ in $\prod_{\sigma \in G} \sigma(\mathfrak{P})$. Since $p = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$,

$$\prod_{\sigma \in G} \sigma(\mathfrak{P}) = p^f \mathbf{R},$$

just as we suspected.

2.2 The Frobenius Substitution

Since we now know that the residue field $\mathbf{R}/\mathfrak{P}$ of a given prime ideal $\mathfrak{P}$ sitting over p is a finite field of order p^f, we know that it can be thought of as a finite field extension of $\mathbb{Z}/(p)$. Consequently, there must be a generator $\overline{\sigma}$ for the Galois group $\overline{G}$ of $\mathbf{R}/\mathfrak{P}$ which acts on elements of the residue field by $\overline{\sigma}(x) = x^p$. This generator is called the *Frobenius automorphism* of the Galois group.

Definition. The *Frobenius substitution* of $\mathfrak{P}$ is a (not necessarily unique) pre-image of the Frobenius automorphism under the obvious homomorphism from the decomposition group D into $\overline{G}$.

To show that it always exists, we must show that this homomorphism is actually onto.

Proposition 2.3. *The natural homomorphism from D to $\overline{G}$ is onto.*

Proof. Let T be the kernel of the homomorphism. Then T consists of all $\sigma \in D$ such that $\sigma(x) \cong x \bmod(\mathfrak{P})$. Since we know $|D| = ef$ and $|\overline{G}| = f$, our task is to show that $|T| = e$. We know that we have a tower of fields:

$$\mathbf{K} \supset \mathbf{K}_T \supset \mathbf{K}_D \supset \mathbb{Q},$$

where $\mathbf{K}_T$ and $\mathbf{K}_D$ are the fixed fields of T and D respectively. If we can show that the degree of the extension $\mathbf{K}_T$ over $\mathbf{K}_D$ is f, this will imply our desired result. Say $\mathfrak{P}_D$ is the prime in $\mathbf{R}_D$ sitting under $\mathfrak{P}$. Then $\mathfrak{P}$ is the only prime sitting over $\mathfrak{P}_D$, since D is the Galois group of $\mathbf{K}$ over $\mathbf{K}_D$, and D fixes $\mathfrak{P}$. Additionally, there can only be one prime sitting between them in $\mathbf{R}_T$. Given any $\alpha \in \mathbf{R}/\mathfrak{P}$, we can create a symmetric polynomial

$$f(X) = \prod_{\sigma \in T}(X - \sigma(\alpha))$$

which then must be in $\mathbf{R}_T/\mathfrak{P}_T$. But then

$$f(X) = (X - \alpha)^{|T|} \text{ mod } (\mathfrak{P}).$$

Since any minimal polynomial for α must divide $f(X)$, we have a trivial Galois group for $\mathbf{R}/\mathfrak{P}$ over $\mathbf{R}_T/\mathfrak{P}_T$. Thus the relative degree of $\mathfrak{P}$ over $\mathfrak{P}_T$ is 1. It follows that the relative degree of $\mathfrak{P}_T$ over $\mathfrak{P}_D$ must be f, since we also have a tower of field extensions:

$$\mathbf{R}/\mathfrak{P} \supset \mathbf{R}_T/\mathfrak{P}_T \supset \mathbf{R}_D/\mathfrak{P}_D \supset \mathbb{Z}/(p).$$

(Technically, these containments are the result of embedding each field in the larger ones via a homomorphism.) Thus $|D/T| \geq f$, but we've already seen that D/T is embedded in $\overline{G}$, so its order can be no larger than f. □

We now have what we want, $D/T \cong \overline{G}$. Now we know the Frobenius substitution exists, with one hitch. The pre-image of the Frobenius automorphism is actually a coset of T in D. If we wish to have a unique Frobenius substitution for each prime sitting over p, we require the prime decomposition of $p\mathbf{R}$ to only contain single powers of primes. When this is the case, we say p is *unramified.* Not surprisingly, if p is divisible by some higher power of a prime, we say p is *ramified.* Now, given a Frobenius substitution ϕ for $\mathfrak{P}$, we know that every other prime sitting over p is $\tau(\mathfrak{P})$ for some $\tau \in G$. Accordingly, the decomposition group of $\tau(\mathfrak{P})$ is $\tau D \tau^{-1}$, and its Frobenius substitution is $\tau\phi\tau^{-1}$.

2.3 A Test for Ramification

With one more tool, we will be ready to move on to the density theorems which interest us. We just stated that we want to deal with unramified primes, as this allows us to uniquely define the Frobenius substitution. The question now arises: is there an easy test for ramification? The answer is yes, and the key to figuring this out is noting that for ramified primes the intersection of all the primes dividing p properly contains p, but at the same time, for each $\mathfrak{P}$ dividing p, $\mathfrak{P} \cap \mathbb{Z} = \mathbb{Z}p$. For example, in $\mathbb{Z}[\sqrt{-5}]$,

$$(2) = (2, 1 + \sqrt{-5})^2.$$

$1+\sqrt{-5} \in (2, 1+\sqrt{-5})$, but certainly $1+\sqrt{-5} \notin (2)$. Now, since we have found an element which is in every divisor of p (simple in our example, since there is only one divisor,) every image of our element under the operation of the Galois group is in every divisor. Most tellingly, it turns out, the trace of our element is in every divisor. The trace is symmetric and must be in $\mathbb{Z}$, as we showed earlier. This implies that the trace of our element must be in p. Our example bears this out, as $Tr(1+\sqrt{-5}) = 2$. This is unique to ramified primes, since in the unramified case, in order for the trace of an element to be in any of the divisors, the element must be contained in all of the divisors, which in the unramified case simply means it is contained in p. Not so now, as we have found an element α such that $Tr(\alpha\beta) = 0$ in $\mathbf{R}/(p)$ for any $\beta \in \mathbf{R}/(p)$. Thus the bilinear form $(\gamma, \beta) = Tr(\gamma\beta)$ defined on $\mathbf{R}/(p)$ is degenerate. We could certainly leave it at that and use the degeneracy of this bilinear form as our test for ramification, but a handy mechanism offers itself. If we let $\alpha_1, \cdots \alpha_n$ be a generating set for $\mathbf{R}$ over $\mathbb{Z}$, then the bilinear form defined above is completely defined by its action on the generating set. Let $[(\alpha_i, \alpha_j)]$ be the matrix with (α_i, α_j) in the i, jth position. Note that this matrix is equal to

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}.$$

Since the α_i's are a generating set for $\mathbf{R}$ over $\mathbb{Z}$, we know our particular

$$\alpha = m_1\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n.$$

Thus, multiplying $[(\alpha_i, \alpha_j)]$ by $[m_1, m_2, \cdots, m_n]^T$ gives us a vector with entries of the form

$$\sum_{j=1}^{n} \sum_{\sigma \in G} \sigma(\alpha_i\alpha_j m_j) = \sum_{\sigma \in G} \sigma(\sum_{j=1}^{n} \alpha_i\alpha_j m_j) = 0 \bmod(p)$$

by the degeneracy of the bilinear form. Thus the determinant of the matrices above must be 0 mod(p). The determinant of the above product of matrices is important enough that we name it. It is called the *discriminant* of the generating set $\alpha_1, \alpha_2, \cdots, \alpha_n$. If it seems familiar, we used the discriminant of another generating set when we proved that **R** was finitely generated over $\mathbb{Z}$.

We have now seen that primes which are ramified must divide the discriminant. This is in fact an if and only if statement. Assume that $p|\text{disc}(\alpha_1, \alpha_2, \cdots, \alpha_n)$. This means that, modulo p, $[(\alpha_i, \alpha_j)]$ is singular. Thus the rows and columns must be linearly dependent modulo p. So we can find coefficients $m_1, m_2, \cdots, m_n$, not all divisible by p, such that for all j,

$$\sum_{i=1}^{n} m_i Tr(\alpha_i \alpha_j)$$

is divisible by p. Since the α_j's form a basis for **R**, This means we have an element

$$\alpha = m_1\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n$$

with Tr($\alpha\mathbf{R}$)$\in p\mathbb{Z}$. Of course, since not all the m_i's are divisible by p, α is not divisible by p, since the α_i's form a basis for **R**. This implies that the bi-linear form defined by (γ, β) =Tr($\gamma\beta$) is degenerate modulo p. We already said this can only happen if p is ramified. If it is not, there is no way to find an element which is in every divisor of p but not in p itself.

Chapter 3

Use of Analysis for Density Computation

3.1 Analytic and Dirichlet Density for the Integers

Now we look at methods of calculating the relative size of subsets of the set of primes. If the set of primes were finite, we would simply compare the number of primes in the subset to the number of primes overall. Unfortunately, we know that this is not the case. We will actually prove this using the techniques we will develop here, but to see this fact simply, Euclid's proof suffices: given a finite list of primes $p_1, \cdots, p_n$; $p_1 \cdots p_n + 1$ must be divisible by some prime not in the list, since any prime dividing $p_1 \cdots p_n$ and $p_1 \cdots p_n + 1$ must also divide 1, which is impossible. Note that this proof basically develops an infinite list of primes inductively, and thus does not particularly give us any information about any infinite set of primes as a whole, but rather deals with arbitrarily large finite subsets. It is this kind of thinking which leads us to what is probably the most intuitive measure of the relative size of a set of primes. Say I is the set of all primes, and $S \subseteq I$.

Definition. The *analytic density* of S, $\delta(S) =$

$$\lim_{n\to\infty} \frac{|\{p : p \in S, p \leq n\}|}{|\{p : p \in I, p \leq n\}|}$$

(This is assuming that this limit exists. In all our definitions of density, we say that a set S has a density only if this lim does exist.) Unfortunately, when we are dealing with infinite sets, considering any finite subset really gives us no information about the value of the limit above. Without any pre-existing concept of the distribution of the primes being considered, the limit above seems incalculable. Take for example the primes congruent to 3 mod(10) (the primes with last digit 3). There is nothing in particular that says the fraction of primes less than, say, 50 which are congruent to 3 is even close to the fraction of such primes less than $10,000$. This problem becomes even more vexing if we consider prime ideals of a number ring, which do not necessarily have a complete ordering. As we have seen before, we can use the norm to bring our calculations back into the realm of the normal integers, but then, for a set of ideals S, we are faced with a definition such as

$$\lim_{n\to\infty}\frac{|\{\mathfrak{P}:\mathfrak{P}\in S, N(\mathfrak{P})\leq n\}|}{|\{\mathfrak{P}:\mathfrak{P}\in \mathbf{R}, N(\mathfrak{P})\leq n\}|}$$

If the limit involving primes of the integers doesn't seem to submit to any easy solution, this certainly doesn't either! We need a meaningful way to compare a measure of all the primes in a given set to a measure of all the primes in general by using finite values. The tool we use is convergent infinite series. Consider the series

$$\sum_{p\in I}\frac{1}{p^s}$$

Then for any $s \in \mathbb{R} > 1$, we know this series converges to some finite value, since we certainly have

$$\sum_{p\in I}\frac{1}{p^s}\leq\sum_{n=1}^{\infty}\frac{1}{n^s}$$

and we know the sum on the right is convergent for any $s > 1$. So now, instead of taking the limit as we count primes in some bounded set, we can take the limit of these sums involving all the primes as $s \rightarrow 1$. We define the *Dirichlet density* of a set S of primes.

Definition. The Dirichlet density of a set of primes S, is $\delta(S) =$

$$\lim_{s\to 1}\frac{\sum_{p\in S}\frac{1}{p^s}}{\sum_{p\in I}\frac{1}{p^s}}$$

Now, if we let s be in $\mathbb{C}$, we can think of these sums as complex functions which are analytic on the half plane $\mathrm{Re}(s) > 1$. To get some handle on their behavior we create a correspondence between the behavior of the series $f(s) = \sum_{p\in I}\frac{1}{p^s}$ and the zeta function $\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$, then show that $\zeta(s)$ can be continued to a meromorphic function in a neighborhood of 1. (More precisely, we show that $(s-1)\zeta(s)$ can be continued to an analytic function in a neighborhood of 1, which also gives us the order of the pole at 1.) This correspondence will be extremely useful to us later when we will have to manipulate this series in some specific density calculations.

Proposition 3.1.

$$\sum_{p\in I}\frac{1}{p^s} = \log(\zeta(s)) + g(s)$$

for some function $g(s)$ which is analytic around 1.

Proof. To begin, we represent $\zeta(s)$ as the product

$$\prod_{p\in I}(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\frac{1}{p^{3s}}\cdots) = \prod_{p\in I}(\frac{1}{1-\frac{1}{p^s}}).$$

$\zeta(s)$ is equal to the first product, since each integer n is uniquely representable as a product of primes; and the first product equals the second simply by the familiar identity for geometric series. Given this infinite product, which must converge normally on the half plane $\mathrm{Re}(s) > 1$, We can define a branch of $\log(z)$, slitting along the negative real axis, such that we have the Laurent series expansion $-\log(1-z) = z + \frac{z^2}{2} + \frac{z^3}{3} + \cdots$. Then we can define the log of the infinite product above as the sum of the logs of each of its terms (at least on the half plane of normal convergence) and get

$$\log(\prod_{p\in I}(\frac{1}{1-\frac{1}{p^s}})) = \sum_{p\in I} -\log(1-\frac{1}{p^s}) = \sum_{p\in I}(\frac{1}{p^s}+\frac{1}{2p^{2s}}+\frac{1}{3p^{3s}}+\cdots) =$$

$$\sum_{n=1}^{\infty}\sum_{p\in I}(\frac{1}{p^{ns}}) = \sum_{p\in I}(\frac{1}{p^s}) + \sum_{n=2}^{\infty}\sum_{p\in I}\frac{1}{np^{ns}}$$

If we can prove that the summation over all $n \geq 2$ in the last statement is bounded in a neighborhood of 1, we will have shown that the summation over the primes has poles precisely where $\log(\zeta(s))$ does with precisely the same orders. For s near 1, we have

$$\sum_{n=2}^{\infty}\frac{1}{np^{ns}} \leq \sum_{n=2}^{\infty}\frac{1}{2p^{ns}} < \frac{1}{p^{2s}}.$$

Now the final term in our above sum is less than

$$\sum_{p\in I}\frac{1}{p^{2s}} < \sum_{n=1}^{\infty}\frac{1}{n^2} < \infty$$

for s near 1. □

We know our log function will be defined and finite everywhere that $\zeta(s)$ is finite and not on the negative real axis. Since we know $\zeta(s)$ takes on positive real values on the real axis in a neighborhood of s, we know that we can find a neighborhood of 1 small enough in $\mathbb{C}$

such that $\zeta(s)$ has positive real part on that neighborhood. Thus $\log(\zeta(s))$ will be defined everywhere in this neighborhood, with poles precisely where $\zeta(s)$ has poles. Now it remains to prove the following proposition:

Proposition 3.2. $(s-1)\zeta(s)$ *can be continued to an analytic function in a neighborhood of* 1.

Proof. Consider the function

$$\zeta'(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s}$$

which is convergent (and thus analytic) in a neighborhood of 1. $\zeta' = \zeta(s) - \frac{1}{2^{s-1}}\zeta(s)$. Reorganizing, we have $\zeta(s) = (1-\frac{1}{2^{s-1}})^{-1}\zeta'(s)$, which has a first order pole wherever $2^{s-1} = 1$, that is, where $s = 1 + 2k\pi i/\log(2)$. □

Now, $\log((s-1)\zeta(s)) = \log(s-1) + \log(\zeta(s))$. So we now have

$$\lim_{s\to 1} \sum_{p\in I} \frac{1}{p^s} + \log(s-1) + g(s) = \log((s-1)\zeta(s))$$

for some function $g(s)$ which is analytic in a neighborhood of 1. Thus, since $(s-1)\zeta(s)$ is analytic around 1, we have

$$\sum_{p\in I} \frac{1}{p^s} = -\log(s-1) + g(s)$$

for some function $g(s)$ analytic around 1. More generally, we have

$$\lim_{s\to 1} \frac{\sum_{p\in I} \frac{1}{p^s}}{-\log(s-1)} = 1 + \lim_{s\to 1} \frac{g(s)}{-\log(s-1)} = 1$$

This automatically gives us another proof that there are an infinite number of primes. If there were a finite number, then the series would be convergent and the limit above would be 0. We can now reformulate our definition of Dirichlet density as follows:

$$\lim_{s\to 1} \frac{\sum_{p\in S} \frac{1}{p^s}}{\sum_{p\in I} \frac{1}{p^s}} =$$

$$\lim_{s\to 1} \frac{\sum_{p\in S} \frac{1}{p^s}}{-\log(s-1)+g(s)} = \lim_{s\to 1} \frac{\sum_{p\in S} \frac{1}{p^s}}{-\log(s-1)}$$

Now, since we have unique factorization into prime ideals for ideals in any number ring, we can perform all the same manipulations with the series $\sum_{\mathfrak{A}\subseteq \mathbf{R}} \frac{1}{N(\mathfrak{A})^s}$ to get

$$\log(\sum_{\mathfrak{A}\subseteq \mathbf{R}} \frac{1}{N(\mathfrak{A})^s}) = \sum_{\mathfrak{P}\subseteq \mathbf{R}} \frac{1}{N(\mathfrak{P})^s} + g(s)$$

where the $\mathfrak{P}$ are prime ideals of $\mathbf{R}$. If we want to obtain the same result about the poles of the sum over norms of ideals as we did for the sum over integers, we need to obtain some bound for the number of ideals with a specific norm. Doing this is actually quite difficult. The results obtained in this realm involve mapping $\mathbf{R}$ into the Euclidean space $\mathbb{R}^n$ and viewing ideals as lattices with specific volumes. The work that leads to the results in this realm is due to Minkowski, for discussion of the work, see [1]. We will not cover this here, but simply assume the results. Before we state the actual results, we need to discuss another topic further, as we actually obtain formulae more specific than we desire for the above calculations, and which depend on defining a new equivalence relation on ideals. These formulae will be extremely useful in the discussion ahead. We will start by constructing a motivating problem.

3.2 A Particular Case of The Cheboterev Density Theorem

Theorem 3.3. *(Cheboterev Density Theorem) Given an extension of number fields $\mathbf{K} \subset \mathbf{L}$ and $\sigma \in G$ an element of the Galois group of $\mathbf{L}$ over $\mathbf{K}$, the set of prime ideals $\mathfrak{p}$ in $\mathbf{K}$ with $\mathfrak{p} \subset \mathfrak{P}$, where $\mathfrak{P}$ is a prime ideal of $\mathbf{L}$ with Frobenius substitution σ, has density equal to the number of conjugates of σ in G divided by the order of G.*

To illustrate some of the concepts this theorem entails, take the case of the generic quadratic extension of $\mathbb{Q}, \mathbf{K} = \mathbb{Q}(\sqrt{m})$, m square-free. Now there are three possibilities for prime splitting in $\mathbf{R}$:

1. a prime p of $\mathbb{Z}$ may remain prime in $\mathbf{R}$, in which case we have $e = g = 1, f = 2$.
2. p may split into two distinct primes in $\mathbf{R}$, in which case we have $e = f = 1, g = 2$.
3. p may be the square of a single prime in $\mathbf{R}$, in which case $f = g = 1, e = 2$.

Since we only care about unramified primes, we may ignore this last case. Actually, since ramified primes must divide the discriminant, we know there can be only finitely many such primes. Thus, intuitively, throwing them out shouldn't skew our density calculations at all. Now, we know that the Galois group of this extension must be the group with two elements, $\mathbb{Z}/(2)$. Then, since this group is abelian, every element has only one conjugate. Thus, viewing the Galois group as an additive group, the primes with Frobenius substitution 0 must have density $\frac{1}{2}$, as should the primes with Frobenius substitution 1. Now, from the definition of the Frobenius substitution, we know that, in this case, primes that remain prime in $\mathbf{R}$ should have a Frobenius substitution of order 2, and primes that split into two primes in $\mathbf{R}$ should have a Frobenius substitution of order 1. (This results from the fact that the order of the Frobenius substitution is f, the inertial degree of p.) Thus, what the theorem states in this case is that the density of the set of primes that split and the density of primes that remain prime is $\frac{1}{2}$. There is a simple way to characterize each of these sets:

Proposition 3.4. *p remains prime in $\mathbf{R}$ if and only if m is not a square mod(p).*

Proof. The polynomial $X^2 - m$ has a root in $\mathbf{R}/\mathfrak{P}$ for any prime $\mathfrak{P}$ sitting over p but does not have a root in $\mathbb{Z}/(p)$. Thus p has inertial degree > 1, so it must be 2, so p must remain prime. On the other hand, if m is a square mod(p), then given any $a+b\sqrt{m}+\mathfrak{P} \in \mathbf{R}/\mathfrak{P}$, the minimal polynomial of this element must have a root in $\mathbb{Z}/(p)$, since we can find $r \in \mathbb{Z}/(p)$ such that $r^2 = m$. □

Now our statement has become: the density of primes p such that a given square-free integer m is a square mod(p) is $\frac{1}{2}$. In the following arguments, we might be concerned about the case where $p|m$. We have actually already thrown out these cases by getting rid of ramified primes. We know that such primes are exactly those which divide the discriminant, and in this case the discriminant is divisible by m (to see why, see the discussion in the last section of this paper.) Now, we want to flip this around, so we have a statement about the residues of p mod(m) which implies our result for the residues of m mod(p). The result we wish to use is Dirichlet's famous theorem on primes in arithmetic progressions:

Theorem 3.5. *(Dirichlet's theorem) Given any integer n and any i in $\mathbb{Z}/(n)^*$, the set of primes congruent to i mod(n) has density $\frac{1}{\phi(n)}$. Generally, the primes not dividing n are distributed equally among the residues of n.*

Proposition 3.6. *For a quadratic extention $\mathbb{Q}(\sqrt{m})$, Dirichlet's theorem implies Cheboterev's theorem.*

Proof. First, consider $(\frac{q}{p})$ where q is an odd prime. If $q \equiv 1$ mod(4), $(\frac{q}{p}) = (\frac{p}{q})$ for all p. Since half the residues mod any integer are squares, this gives us our result in the case where $q \equiv 1$ mod(4), since exactly $\frac{\phi(q)}{2}$ residues are squares mod(q) and the density of the set of primes congruent to each residue is $\frac{1}{\phi(q)}$, so the density of primes which are squares mod(q)

is

$$\frac{\phi(q)}{2}\frac{1}{\phi(q)} = \frac{1}{2},$$

and the primes that are squares mod(q) are exactly the primes for which q is a square. In the other case, $q \equiv 3$ mod(4), there is more difficulty. Now, if $p \equiv 1$ mod(4), $(\frac{q}{p}) = (\frac{p}{q})$, but if $p \equiv 3$ mod(4), $(\frac{q}{p}) = -(\frac{p}{q})$. To deal with this, consider Dirichlet's theorem applied to $4q$. This tells us that the density of the primes in each equivalence class of $\mathbb{Z}/(4q)^*$ is $\frac{1}{\phi(4q)}$. The Chinese remainder theorem says that exactly half these equivalence classes contain the primes congruent to 1 mod(4). Thus, if we consider only the set of primes congruent to 1 mod(4), the primes in this set congruent to a given $a \in \mathbb{Z}/(q)^*$ must have density $\frac{1}{\phi(q)}$. For primes in this set, $(\frac{q}{p}) = (\frac{p}{q})$, so the density of primes in this set for which q is a square must be $\frac{1}{2}$. Considering the set of primes congruent to 3 mod(4), the fact that the density of primes in this set which are not squares mod(q) must be $\frac{1}{2}$ gives us the same result. Thus the density of all primes for which q is a square must be $\frac{1}{2}$. Now, if we let $m = q_1q_2\cdots q_n$ where all the q_i are distinct, we can obtain the same result if we consider that the primes congruent to 1 mod(4) are equally distributed over $\mathbb{Z}/(m)^*$ and that for primes p in this set,

$$(\frac{q_1q_2\cdots q_{n-1}}{p})$$

is completely determined by the residue of p mod$(q_1q_2\cdots q_{n-1})$. Then if we consider the subset A of these primes congruent to a given a mod$(q_1q_2\cdots q_{n-1})$, the subset of primes in A congruent to a given b mod(q_n) must have density $\frac{1}{\phi(q_n)}$ in A. Then

$$(\frac{m}{p}) = (\frac{q_1q_2\cdots q_{n-1}}{p})(\frac{q_n}{p}).$$

For primes in A, the former factor is constant, and the set of primes for which the latter factor is 1 has density $\frac{1}{2}$. Thus m is a square mod(p) for half the primes in A. Since a was arbitrary, the density of primes congruent to 1 mod(4) for which m is a square must be $\frac{1}{2}$. A similar argument applies for the primes congruent to 3 mod(4), so we achieve our result in general: the density of primes for which a given m is a square is $\frac{1}{2}$. □

3.3 The Definition of the Ray Class Group and Minkowski's Counting Result for Ideals

Now to prove our special case of the Cheboterev density theorem, we need to prove Dirichlet's theorem. We reformulate its statement in a way which will allow us to use Minkowski's formulae.

Definition. The *localization* $\mathbf{R}_{\mathfrak{P}}$ of a ring at a prime ideal $\mathfrak{P}$ is $\mathbf{R}S^{-1}$ where $S = \mathbf{R} - \mathfrak{P}$.

Definition. $\alpha \equiv^* \beta \bmod(p^n)$ if α and $\beta \in \mathbb{Q}^*$, $\alpha = \frac{a}{b}, \beta = \frac{c}{d}$, with a, b, c, d relatively prime to p^n and α and β are in the same coset of $1 + p^n\mathbb{Z}_p$ in $\mathbb{Q}^*$. Then $\alpha \equiv^* \beta \bmod(m)$ if $\alpha \equiv^* \beta \bmod(p^n)$ for all $p^n | m$.

Definition. $\mathbb{Q}_{m,1}$ is the set of $\alpha \in \mathbb{Q}^*, \alpha \equiv^* 1 \bmod(m)$, or alternatively, the set of $\frac{x}{y}, x, y \in \mathbb{Z}$, x, y relatively prime to m such that $x \equiv^* y \bmod(m)$.

Proposition 3.7. *The cosets of $\mathbb{Q}_{m,1}$ in $\mathbb{Q}^* - \{\frac{a}{b}, a$ or b dividing $m\}$ are $a\mathbb{Q}_{m,1}$, where $a \in \mathbb{Z}/(m)^*$.*

Proof. Say $\alpha\mathbb{Q}_{m,1}, \beta\mathbb{Q}_{m,1}$ are two cosets of $\mathbb{Q}_{m,1}$. Then the two cosets are the same if and only if $\alpha\beta^{-1} \in \mathbb{Q}_{m,1}$, which is to say, $\alpha \equiv^* \beta \bmod(m)$. Say α not an integer. Then $\alpha = \frac{a}{b}, a, b \in \mathbb{Z}$, and since for some integer x relatively prime to m, $\alpha\mathbb{Q}_{m,1} = x\mathbb{Q}_{m,1}$ means $\alpha \equiv^* x \bmod(m)$, or

$$\frac{a}{b} = x + xp^n r/s,$$

with s relatively prime to p^n, we can manipulate this last expression to read

$$a = bx + bxp^n r/s.$$

Choosing $s = bx$, which is fine, since both b and x are relatively prime to p^n, we have $a = bx + p^n r$. Since r is arbitrary, this is equivalent to saying $a \equiv bx \bmod(p^n)$. By the Chinese remainder theorem, we can find an x that satisfies this for all p^n dividing m. Thus there is an integer relatively prime to m such that the coset $x\mathbb{Q}_{m,1} = \alpha\mathbb{Q}_{m,1}$. So we can assume α and β are integers. Now, if two cosets $\alpha\mathbb{Q}_{m,1}$ and $\beta\mathbb{Q}_{m,1}$ are equal, this means $\alpha \equiv^* \beta \bmod(m)$, or

$$\alpha = \beta + \beta p^n r/s$$

for all some r, s for all p^n dividing m. We can choose s to be β and now we have simply that $\alpha \equiv \beta \bmod(p^n)$. Thus there is a bijection between residues in $\mathbb{Z}/(m)^*$ and cosets of $\mathbb{Q}_{m,1}$. □

This construction may seem somewhat overwrought, but we may extend our definition to any number field $\mathbf{K}$ and let $\mathfrak{m}$ be any product of prime ideals, and instead of considering cosets in $\mathbb{Q}^* - \{\frac{a}{b}, a$ or b dividing $m\}$, consider cosets in the fractional ideal group generated by all prime ideals not dividing $\mathfrak{m}$. Note that this is a generalization of what we did with the $\mathbb{Q}$ case, since $\mathbb{Z}$ is a PID. Now all the above arguments still hold. (To be thorough, the complete definition of this equivalence relation also includes the condition that if we choose a finite number of real embeddings $\sigma \in G$ of $\mathbf{K}$ (that is, elements of the Galois group which map $\mathbf{K}$ into $\mathbb{R}$,) $a \equiv^* b$ only if $\sigma(a)$ has the same sign as $\sigma(b)$. We don't require this condition for the work we will be covering, so we may assume there are no real embeddings being considered in the definition of the equivalence relation.) Now let the fractional ideal group defined above be called $\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}$. Then we have the following definition:

Definition. The group $\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m},1}$, where $\mathbf{K}_{\mathfrak{m},1}$ is defined in an analogous way to $\mathbb{Q}_{m,1}$, is called the *ray class group* of $\mathbf{K}$.

Now we may reformulate our desired result for the Dirichlet theorem as the statement that the density of primes in each coset of $\mathbb{Q}_{m,1}$ is the same, and thus must be the inverse of the index of $\mathbb{Q}_{m,1}$ in $\mathbf{I}_{\mathbb{Q}}^{m}$, which we now know is $\frac{1}{\phi(m)}$.

The ray class group gives us the structure for which the results of Minkowski's work on counting ideals holds. Say $\mathbf{k}$ is any coset of $\mathbf{K}_{\mathfrak{m},1}$. Then define $\zeta_{\mathbf{K}}(\mathbf{k}, s)$ to be

$$\sum_{\mathfrak{A}\in\mathbf{k},\mathfrak{A}\subset\mathbf{R}} \frac{1}{N(\mathfrak{A})^s}$$

The result we now wish to use is:

Theorem 3.8. *(Minkowski)* $\lim_{s\to1}(s-1)\zeta_{\mathbf{K}}(\mathbf{k}, s)$ *is a finite constant* $g_{\mathfrak{m}}$ *independent of the coset* $\mathbf{k}$.

We are also given that there are finitely many cosets, so this gives us that $\zeta_{\mathbf{K}}(s)$ is meromorphic in a neighborhood of 1 with a single order pole at 1. Since we have unique factorization of ideals of $\mathbf{R}$, we can extend the arguments we used in the case where $\mathbf{K} = \mathbb{Q}$ to obtain

$$\log(\zeta_{\mathbf{K}}(s)) = \sum_{\mathfrak{P}\in\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}},\mathfrak{P}\subset\mathbf{R}} \frac{1}{N(\mathfrak{P})^s} + g(s)$$

where $g(s)$ is analytic at 1, and accordingly

$$-\log(s-1) = \sum_{\mathfrak{P}\in\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}},\mathfrak{P}\subset\mathbf{R}} \frac{1}{N(\mathfrak{P})^s} + g(s)$$

for some $g(s)$ analytic at 1. We may now extend our definition of Dirichlet density to primes of an arbitrary number ring in the expected way as

$$\lim_{s\to1} \frac{\sum_{\mathfrak{P}\in S}\frac{1}{N(\mathfrak{P})^s}}{-\log(s-1)}.$$

Here is one result that quickly falls out of this definition

Proposition 3.9. *The primes of inertial degree* 1 *have density* 1.

Proof. Let S be the set of primes with inertial degree 1. Then the norm of any prime of $\mathbf{R}$ not in S must be p^f where p is some prime of $\mathbb{Z}$ and $f \geq 2$ There can be at most n primes of $\mathbf{R}$ sitting over a given prime of $\mathbb{Z}$, so if we sum over the primes not in S, we obtain

$$\lim_{s\to 1} \sum_{\mathfrak{P}\notin S} \frac{1}{N(\mathfrak{P})^s} < \sum_{p\in I} \frac{n}{p^2} < \sum_{m=1}^{\infty} \frac{n}{m^2}.$$

We know that the series on the right converges, so the limit in our definition of density must be 0. Since we can certainly make the statement

$$\lim_{s\to 1} \frac{\sum_{\mathfrak{P}\in S} \frac{1}{N(\mathfrak{P})^s}}{-\log(s-1)} + \lim_{s\to 1} \frac{\sum_{\mathfrak{P}\notin S} \frac{1}{N(\mathfrak{P})^s}}{-\log(s-1)} = \lim_{s\to 1} \frac{\sum_{\mathfrak{P}\subset \mathbf{R}} \frac{1}{N(\mathfrak{P})^s}}{-\log(s-1)} = 1$$

we have that the density of primes in the complement of any set S is equal to 1 minus the density of primes in S. So the primes of inertial degree 1 have density 1. □

3.4 Characters, L-Series, and the Proof of Dirichlet's Theorem

Unfortunately, we cannot do the same manipulations with each $\zeta_{\mathbf{K}}(\mathbf{k}, s)$ that we made with $\zeta_{\mathbf{K}}(s)$, since there is no guarantee that the primes dividing an ideal in a given coset are in that coset. (For example, say $\mathbf{K} = \mathbb{Q}$ and $m = 3$. Then $11 * 17 \equiv 1 \text{ mod}(3)$, but $11 \equiv 17 \equiv 2 \text{ mod}(3)$.) Looking back to our motivating problem (that of showing the density of primes in each coset of $\mathbb{Q}_{m,1}$ is equal to 1 over the number of cosets), we desire a way to capture the index of a coset in our density calculation. To this end, we define a generalization of our zeta functions which will employ *characters* of the group $\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}/\mathbf{K}_{\mathfrak{m},1}$.

Definition. A character of a finite abelian group is an injective homomorphism from the group to the unit circle in $\mathbb{C}$.

There are two formulae involving characters which will be particularly useful to us.

Proposition 3.10. *Let A be a finite abelian group and let $\overline{A}$ be the set of characters of A. Let χ_0 be the character that sends all elements of A to 1. Then*

$$\sum_{a\in A} \chi(a) = \begin{cases} 0 & \chi \neq \chi_0 \\ |A| & \chi = \chi_0 \end{cases},$$

$$\sum_{\chi\in\overline{A}} \chi(a) = \begin{cases} 0 & a \neq 1 \\ |A| & a = 1 \end{cases}$$

Proof. In the first formula, the case where $\chi = \chi_0$ is obvious. If $\chi \neq \chi_0$ then we can find $b \in A$ with $\chi(b) \neq 1$. We know $Ab = A$ and $\chi(ab) = \chi(b)\chi(a)$. Thus we have

$$\sum_{a\in A} \chi(a) = \sum_{a\in A} \chi(ab) = \chi(b) \sum_{a\in A} \chi(a)$$

Since $\chi(b) \neq 1$, the sum must be 0. To confirm the second formula in a similar way, we show that $\overline{A}$ is a group. Define multiplication by $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$. The product is still a homomorphism, and the unit circle in $\mathbb{C}$ is closed under multiplication, so the product is still a character of A. With this multiplication, χ_0 becomes the identity. Given any $\chi \in \overline{A}$, χ^{-1} must be defined by $\chi^{-1}(a) = (\chi(a))^{-1}$. We need to see that χ^{-1} is a character of A. Certainly, $(\chi(a))^{-1}$ is in the unit circle.

$$\chi^{-1}(ab) = (\chi(ab))^{-1} = (\chi(a)\chi(b))^{-1} =$$
$$(\chi(a))^{-1}(\chi(b))^{-1} = \chi^{-1}(a)\chi^{-1}(b).$$

So χ^{-1} is a character of A. There remains one further obstacle to confirming the formula. Given an $a \in A$ with $a \neq 1$, is it always possible to find a character χ such that $\chi(a) \neq 1$? We answer this in the affirmative by noting that if a has order n in A; and θ_n is a primitive nth root of unity, then the map sending a^t to θ_n^t and all other elements of A to 1 is a character of A. Now, given $a \in A$, $a \neq 1$, let χ_1 be such that $\chi_1(a) \neq 1$. Then

$$\sum_{\chi\in\overline{A}} \chi(a) = \sum_{\chi\in\overline{A}} \chi_1(a)\chi(a) = \chi_1(a) \sum_{\chi\in\overline{A}} \chi(a)$$

Since $\chi_1(a) \neq 1$, the sum must be 0. The case where $a = 1$ is obvious. □

It is these summation formulae that give us our tool for capturing the index of a given subgroup of the ray class in our density calculations. We generalize our zeta functions as follows:

Definition. An *L-series* of a subgroup H of the ray class is a series

$$L(\chi, s) = \sum_{\mathfrak{A}\in\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}} \frac{\chi(\mathfrak{A})}{N(\mathfrak{A})^s}$$

where χ is a character of $\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}/H$, and $\chi(\mathfrak{A})$ is actually $\chi(\mathfrak{A}H)$, a given coset of H.

Note that if we take $H = \mathbf{K}_{\mathfrak{m},1}$,

$$L(\chi, s) = \sum_{\mathbf{k}} \chi(\mathbf{k})\zeta(s, \mathbf{k}).$$

Also, there is nothing that stops us from doing the same manipulations on the L-series that we did on the zeta functions to achieve the result that

$$\log(L(\chi, s)) = \sum_{\mathfrak{P} \in \mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}} \frac{\chi(\mathfrak{P})}{N(\mathfrak{P})^s} + g_{\chi}(s)$$

where $g_{\chi}(s)$ is analytic at 1. Additionally, we know that $(s-1)L(\chi, s)$ is analytic at 1, since $(s-1)\zeta_{\mathbf{K}}(\mathbf{k}, s)$ is finite for each coset. Now we state one of the useful results that we obtain from the introduction of characters:

$$\sum_{\chi \in \overline{\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}/H}} \chi(\mathfrak{P}) = \begin{cases} 0 & \mathfrak{P} \notin H \\ |\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}/H| & \mathfrak{P} \in H \end{cases}$$

So if we sum over the logs of all the L-series of H, we obtain

$$\sum_{\chi \neq \chi_0} (\log(L(\chi, s)) + g_{\chi}(s)) + \log(L(\chi_0, s)) + g_{\chi_0}(s) =$$

$$|\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}/H| \sum_{\mathfrak{P} \in H} \frac{\chi_0(\mathfrak{P})}{N(\mathfrak{P})^s} = |\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}/H| \sum_{\mathfrak{P} \in H} \frac{1}{N(\mathfrak{P})^s}$$

Now, we know that $\mathbf{K}_{\mathfrak{m},1}$ is a subgroup of H, so we may split up any L-series of H into a sum of zeta functions of cosets of $\mathbf{K}_{\mathfrak{m},1}$ over the cosets of H:

$$L(\chi, s) = |H/\mathbf{K}_{\mathfrak{m},1}| \sum_{\mathbf{l} \text{ cosets of } H} \chi(\mathbf{l})\zeta(s, \mathbf{k})$$

Accordingly, we know that

$$\lim_{s \to 1} (s-1)L(\chi, s) = \begin{cases} 0 & \chi \neq \chi_0 \\ g > 0 & \chi = \chi_0 \end{cases}$$

by the summation results we proved for characters. This tells us that $L(s, \chi)$ is actually finite for $\chi \neq \chi_0$. Thus $\log(L(\chi, s))$ is bounded away from positive infinity. Since $L(\chi_0, s)$ is exactly $\zeta(s)$ with a finite number of primes removed, we have that the density of the primes in H is bounded by $\frac{1}{|\mathbf{I}_{\mathbf{K}}^{\mathbf{m}}|}$ and is in fact equal to this quantity if and only if all the $(L(\chi, s))$ are non-zero at 1. Going back to our attempt to prove Dirichlet's theorem, we now know that the density of the set of primes contained in $\mathbb{Q}_{m,1}$ is at most $\frac{1}{\phi(m)}$. We are a step closer to showing that it is exactly this. We prove the other direction:

Proposition 3.11. *The density of the primes in* $\mathbb{Q}_{m,1}$ *is* $\frac{1}{\phi(m)}$.

Proof. Consider the cyclotomic extension $\mathbb{Q}(\theta_m)$ where θ_m is a primitive mth root of unity. The Galois group of this extension is well known to be isomorphic to $\mathbb{Z}/(m)^*$, which has order $\frac{1}{\phi(m)}$. We wish to show that the set of primes that split completely (that is, primes with $f = e = 1$) in $\mathbb{Q}(\theta_m)$ accounts for almost all the primes in $\mathbb{Q}_{m,1}$. Take any prime $p \in \mathbb{Q}_{m,1}$. Then $p \equiv 1 \text{ mod}(m)$. So raising to the pth power is equivalent to the identity automorphism in $\mathbb{Q}(\theta_m)$. Thus, if we take any prime $\mathfrak{P}$ that sits over one of these p's, we have that the Frobenius Substitution of $\mathfrak{P}$, which acts on $\mathbf{R}/\mathfrak{P}$ by $x \to x^p$ and generates the Galois group of $\mathbf{R}/\mathfrak{P}$ over $\mathbb{Z}/(p)$ must be the identity, which in turn implies that $\mathfrak{P}$ has inertial degree 1. Since only a finite number of primes in $\mathbb{Q}(\theta_m)$ are ramified, this implies that almost all of the p's in $\mathbb{Q}_{m,1}$ split completely (have $f = e = 1$). Reversing these arguments, we see that if a prime splits completely, the residue field of any prime sitting over it must have a trivial Galois group, so that the automorphism that acts by $x \to x^p$ must be the identity on the residue field. Since the inertial group is trivial $e = 1$ for all but a finite set of primes, this means that $p \equiv 1 \text{ mod}(m)$ for almost all primes p that split completely. Also since $e = 1$ for almost all primes of $\mathbb{Q}(\theta_m)$, we have that the primes that sit over primes that split completely are almost all the primes with inertial degree 1 Thus the set of primes sitting over primes that split completely has density 1. Say the set of primes that split completely is S, then we have

$$\sum_{\mathfrak{P}:p\subset\mathfrak{P},p\in S} \frac{1}{N(\mathfrak{P})^s} = \phi(m)\sum_{p\in S}\frac{1}{p^s}$$

since $N(\mathfrak{P}) = p$ and there are exactly $\phi(m)$ primes sitting over each $p \in S$. So the density of the primes that split completely is $\frac{1}{\phi(m)}$. □

We have seen that this implies that $L(\chi, s) \neq 0$ at 1 for all characters of $\mathbb{Q}_{m,1}$. Now we need to somehow extend this result to all cosets of $\mathbb{Q}_{m,1}$. This is actually another fairly simple application of the summation rules for characters.

Proposition 3.12. *The density of the primes in any coset of* $\mathbb{Q}_{m,1}$ *is* $\frac{1}{\phi(m)}$.

Proof. Let $\mathbf{l}$ be any coset of $\mathbb{Q}_{m,1}$. Then sum together the logs of all the L-series of $\mathbb{Q}_{m,1}$:

$$\log(L(\chi_0, s)) + \sum_{\chi\neq\chi_0}\log(L(\chi, s)) = \sum_{\chi\in\mathbf{I}_{\mathbb{Q}}^m/\mathbb{Q}_{m,1}}\sum_{p\in\mathbf{I}_{\mathbb{Q}}^m}(\frac{1}{p^s} + g_\chi(s)) =$$

$$\sum_{\mathbf{k}\in\mathbf{I}_{\mathbb{Q}}^{m}/\mathbb{Q}_{m,1}} \sum_{\chi\in\overline{\mathbf{I}_{\mathbb{Q}}^{m}/\mathbb{Q}_{m,1}}} \chi(\mathbf{k}) \sum_{p\in\mathbf{k}} \frac{1}{p^s} + g(s)$$

where g(s) is some function analytic at 1. Now if we multiply each term of the sum over the characters by $\chi(\mathbf{l}^{-1})$, we obtain

$$\log(L(\chi_0, s)) + \sum_{\chi\neq\chi_0} \chi(\mathbf{l}^{-1}) \log(L(\chi, s)) = \sum_{\mathbf{k}\in\mathbf{I}_{\mathbb{Q}}^{m}/\mathbb{Q}_{m,1}} \sum_{\chi\in\overline{\mathbf{I}_{\mathbb{Q}}^{m}/\mathbb{Q}_{m,1}}} \chi(\mathbf{k}\mathbf{l}^{-1}) \sum_{p\in\mathbf{k}} \frac{1}{p^s} + g(s)$$

Now, we know that the $\log(L(\chi, s)), \chi \neq \chi_0$ are bounded, and we know that the sum over the characters on the right is 0 except when $\mathbf{k} = \mathbf{l}$, when it equals $\phi(m)$, so this equation collapses quite a bit to give

$$\log(L(\chi_0)) = \phi(m) \sum_{p\in l} \frac{1}{p^s} + g(s)$$

where g(s) is analytic at 1. We have seen that this implies the density of primes in $\mathbf{l}$ is $\frac{1}{\phi(m)}$. □

At long last we have proven Dirichlet's theorem, and consequently, Cheboterev's theorem for quadratic number fields.

Chapter 4

Algebraic Proofs of Results from Cheboterev's Theorem

4.1 Lenstra and Stevenhagen's Lemma, with a Specific Formula for Quadratic Extensions

To continue down the path of the previous chapter and complete the proof of the full Cheboterev density theorem requires that we prove that the L-series of any subgroup of $\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}$ are non-zero for all characters, and also involves a fair degree of class field theory. Instead of delving into this subject, we switch to thinking about some results due to this theorem which don't necessarily require that we talk about density or engage in analysis.

Assuming we have proven in general that the primes of a field are evenly distributed across the cosets of $\mathbf{K}_{\mathfrak{m},1}$, and knowing that the primes of intertial degree 1 over primes of $\mathbb{Q}$ account for all the density, we obtain the fact that the primes of inertial degree 1 generate the entire ray class. Noting that if we take $\mathfrak{m} = 1$, the ray class actually becomes the class group, this implies that the class group is also generated by the primes of inertial degree 1. In [2], H.W. Lenstra and P. Stevenhagen show how this result can be obtained without the use of analysis or density arguments. The proofs are dependent on the following lemma:

Lemma 4.1. *Given number fields* $\mathbf{K}$ *and* $\mathbf{L} = \mathbf{K}(\alpha)$ *for some algebraic integer* α*, and* $\mathbf{R}$ *and* $\mathbf{S}$ *the number rings of* $\mathbf{K}$ *and* $\mathbf{L}$ *respectively, choose* $d \neq 0 \in \mathbf{R}$ *such that* $d\mathbf{S} \subseteq \mathbf{R}\alpha$*. Let* $\mathfrak{Q}$ *be a prime of* $\mathbf{S}$ *that does not divide* $d\mathbf{S}$*. If the inertial degree* f *of* $\mathfrak{Q} = f > 1$*, then there exists an element* $x \neq 0$ *of* $\mathbf{S}$ *such that* $x \equiv 1$ *mod* $d\mathbf{S}$ *and* $\mathbf{S}x = \mathfrak{Q}\prod_{i=1}^{t}\mathfrak{B}_i$*, where the* $\mathfrak{B}_i$*'s are primes of* $\mathbf{S}$ *of degree* $< f$*. (This part of the lemma is sufficient to establish the results of the first theorem, which only deals with the equivalence relations of the class group. The next part allows us to also establish relations in the ray class) Additionally, for a finite number of real embeddings of* $\mathbf{S}$*,* x *can be chosen so that it is positive under all the embeddings.*

It would be pointless to rewrite the entire proof of the general case here, but a few details should be pointed out to elucidate the calculations done in the specific cases covered. Specifically, the element x is obtained from Kummer's theorem, which states as one of its results the fact that $\mathfrak{Q}$ can be generated by $\mathfrak{P}\mathbf{S}$ and an element of $\mathbf{S}$ produced by reducing the minimal polynomial of $\beta = d\alpha$ mod $\mathfrak{P}$ and plugging β into the factor associated with $\mathfrak{Q}$ by the theorem. Additionally, it is always possible to choose d to be the discriminant of $\mathbf{S}$ [1].

Let us first look at the general quadratic case where $\mathbf{K}= \mathbb{Q}$ and $\mathbf{L}= \mathbf{K}(\sqrt{m})$, where m is square-free. Since the degree of the extension is 2 in this case, the only primes with $f > 1$ are those which remain prime in $\mathbf{S}$. So we need to determine d and also which primes of $\mathbf{R}$ remain prime in $\mathbf{S}$. Though we will complete it anyway, the former is actually unnecessary for applying the lemma to quadratic number fields, since the number ring is generated by a single element already:

Proposition 4.2. *If* $\mathbf{L}= \mathbb{Q}(\sqrt{m})$, *then*

$$\mathbf{S} = \begin{cases} \mathbb{Z}[\sqrt{m}] \text{ if } m \equiv 2, 3 \ mod(4) \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] \text{ if } m \equiv 1 \ mod(4) \end{cases}$$

Proof. Any element $\frac{a}{b} + \frac{c}{f}\sqrt{m}$ of $\mathbf{L}$ is a root of the polynomial

$$x^2 + 2\frac{a}{b}x + (\frac{a}{b})^2 - m(\frac{c}{f})^2,$$

so $\frac{a}{b} + \frac{c}{f}\sqrt{m}$ is an algebraic integer iff the coefficients of this polynomial are in $\mathbb{Z}$. From the first degree coefficient, we see that $b|2$, so $\frac{a}{b} = \frac{a}{2}$ with a not necessarily relatively prime to 2. *Case 1*: $m \equiv 2$ mod(4). Then we have

$$\frac{a^2}{4} - (2 + 4k)\frac{c^2}{f^2} = l$$

for some integer l and $m = 2 + 4k$. Clearing denominators, we get

$$a^2 f^2 - (2 + 4k)4c^2 = lf^2.$$

So f^2 divides $(2 + 4k)4c^2$. Since m is square free, it is evident from looking at the prime decompositions of both f^2 and $4mc^2$ that $f^2|4c^2$. Thus $f|2c$, so $\frac{c}{f} = \frac{e}{2}$, and we have

$$\frac{a^2}{4} - (2 + 4k)\frac{e^2}{4} = l.$$

From this, the requirement that l be an integer implies

$$a^2 - 2e^2 \equiv 0 \text{ mod}(4).$$

Since 2 is not a square mod(4), this can only happen if

$$a^2 \equiv e^2 \equiv 0 \text{ mod}(4).$$

This implies that both $\frac{a}{b}$ and $\frac{c}{f}$ are integers, and the first case is complete.
Case 2: $m \equiv 3 \bmod(4)$. The argument is exactly the same as above, except that we wind up with

$$a^2 - 3e^2 \equiv 0 \bmod(4).$$

Since 3 is not a square mod(4), the same result follows.
Case 3: $m \equiv 1 \bmod(4)$. Once again, the argument goes exactly the same up to the equivalence

$$a^2 - e^2 \equiv 0 \bmod(4).$$

Now there is no restriction implying that a^2 and e^2 must be divisible by 4. The equivalence does imply that $a \equiv b \bmod(2)$, as required, and now it is obvious that the element given does indeed generate the number ring in this case. □

Since we already have a single generator for our number ring, we could technically set $d = 1$ in the statement of the lemma, but in order to better illustrate the calculations involved in the proof, we will use the discriminant of $\mathbf{S}$ for d. Since in this case the discriminant is the discriminant of the minimal polynomial of our generator, we have $d = 4m$ if $m \equiv 2, 3 \bmod(4)$; and $d = m$ if $m \equiv 1 \bmod(4)$.

Now we are ready to go through the construction of the lemma. We deal with the cases seperately: First assume $m \equiv 2, 3 \bmod(4)$ and let $\beta = d\alpha = 4m\sqrt{m}$. Then the minimal polynomial for β is $x^2 - 16m^3$. Since p is relatively prime to β, we know that β generates $\mathbf{S}/p\mathbf{S}$. Thus $x^2 - 16m^3$ is irreducible mod(p), since if it were reducible, the inertial degree of $p\mathbf{S}$ over p would be < 2. Thus the polynomial generated by Kummer's theorem, which we will be manipulating to obtain the desired element, is $x^2 - 16m^3$. So the element we start with is $\beta^2 - 16m^3 = 0$. As we alter this element to fit the conditions of the lemma, we will always denote it by z We wish for this element to be nonzero yet still have the property that it generate $p\mathbf{S}$ along with $p\mathbf{S}$. (This statement is ridiculously trivial in this case, but in cases where the prime of $\mathbf{S}$ we are concerned with is not necessarily a prime of $\mathbb{Z}$ as well, it makes more sense). Obviously in this case, any element of $p\mathbf{S}$ will do, so adding p to z would suffice for this condition. We also want $z \equiv 1 \text{mod}(d)$. Merely adding p will not necessarily suffice for this condition. Fortunately, p is relatively prime to $d\mathbb{Z}$, so adding $p^{\phi(d)}$ (where ϕ is the totient function) will work fine. Thus, the first condition on z is ensured. The next manipulation ensures the second condition. (that all the primes aside from $p\mathbf{S}$ dividing z have inertial degree $< f$). We want the coefficient of the 1st degree term of our polynomial in β ($f - 1$st degree term in the general case) to *not* be a sum of 2 (generally, f) conjugates of $-\beta$. In this case, that means we want the first degree term to not be 0. Adding p to this coefficient works nicely in this case, as it is the simplest way of retaining the inclusion of z in $p\mathbf{S}$ while satisfying the condition. In the general case, there is an additional requirement that the constant term must be divisible by each prime which is relatively prime to p and also divides

$$y = \prod_{c \in C} (p + v_{f-1})$$

where C is the collection of sums of f conjugates of β and v_{f-1} is the $f-1$st coefficient of our polynomial. This condition is trivial in our case, since $v_{f-1} = p$. The previous condition suffices for us, as we now have a z which is equal to $p\beta + p^{\phi(d)}$, which is in $p\mathbf{S}$ but not in p and thus must have a prime decomposition in $\mathbf{S}$,

$$z = p\mathbf{S}\prod_{i=1}^{t}\mathfrak{B}_i,$$

where the $\mathfrak{B}_i$'s are relatively prime to $p\mathbf{S}$ and congruent to 1 mod($d\mathbf{S}$). To see that each $\mathfrak{B}_i$ is of intertial degree 1, it is sufficient to note that β must generate $\mathbf{S}/\mathfrak{B}_i$ and satisfies the polynomial $pX + p^{\phi(d)}$, since $\mathfrak{B}_i$ divides z.

The second case turns out to be a trivial variation of the first. Assume $m \equiv 1$ mod(4) and let

$$\beta = d\alpha = \frac{m + m\sqrt{m}}{2}.$$

Then the minimal polynomial for β is

$$x^2 - mx + \frac{m - m^3}{2}.$$

The same argument as in the first case shows that this is the polynomial used to generate z, thus we still begin with $z = 0$ and proceed exactly as above.

In either case, there are only real embeddings of $\mathbf{L}$ if $m > 0$, in which case there are two: the identity automorphism, and the automorphism sending $\sqrt{m}$ to $-\sqrt{m}$. In the former case, z is positive without any manipulation. In the latter case, increasing the constant term to $p^{m\phi(d)}$ will suffice, since

$$p^m > pm > p\sqrt{m}.$$

4.2 The Formula for a Specific Cyclotomic Extension

The calculations for cyclotomic fields get ugly fast. Even calculating the discriminant for a generic cyclotomic field is fairly messy. For example, the formula for the discriminant of the p^rth cyclotomic field is

$$p^{p^{r-1}(p^r - r - 1)}.$$

Instead of trying to complete all the necessary calculations for the general cyclotomic field, we apply the lemma to a specific cyclotomic field which will exhibit more complex behavior than the quadratic fields. We choose the 8th cyclotomic field, $\mathbb{Q}(e^{2\imath\pi/8})$. The degree of this extension of $\mathbb{Q}$ is well known to be $\phi(8) = 4$ with minimal polynomial $x^4 + 1$. To calculate the discriminant of this field, we could use the formula given above, but since we haven't derived it, that doesn't seem quite honest. Instead, we note that the discriminant of a number ring $\mathbf{S} \subset \mathbf{L} = \mathbb{Q}(\alpha)$ is the square of the Van Der Monde determinant equal to

$$\prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$$

where the α_i's and α_j's are the conjugates of α. If one expands $\mathrm{N}(f'(\alpha))$, it is easily seen that this quantity is equal to the Van Der Monde determinant described above. Applying this to our chosen field,

$$f'(e^{\imath\pi/4}) = 4e^{3\imath\pi/4} \text{ so } N(f'(e^{\imath\pi/4})) = 4^4 N(e^{3\imath\pi/4}) = 4^4.$$

For this field, $\beta = d\alpha = 4^4 e^{\imath\pi/4}$, so the minimal polynomial for β is $x^4 + 4^{16}$. Now we wish to choose a prime in $\mathbb{Z}$ which splits into primes of inertial degree > 1 in the number ring of $\mathbb{Q}(e^{\imath\pi/4})$. We employ the following proposition:

Proposition 4.3. *Let* $\mathbf{L}= \mathbb{Q}(\alpha)$ *be the mth cyclotomic field,* $\mathbf{S}$ *its number ring, and p be a prime of* $\mathbb{Z}$ *not dividing m. Then any prime* $\mathfrak{Q}$ *of* $\mathbf{S}$ *sitting over p has inertial degree f =ord(p) mod(m).*

Proof. It is well established that the Galois group of the mth cyclotomic field is isomorphic to $\mathbb{Z}_m$, and that the automorphism associated with the equivalence class of a given $q \in \mathbb{Z}_m$ acts by raising α to the qth power. Thus, if f is the order of p mod(m), $\alpha^{p^f} = \alpha$. $\mathbf{S}/\mathfrak{Q}$ is a field of order p^a for some a, and we know that the Galois group for the field extension from $\mathbb{F}_p$ to $\mathbb{F}_{p^a}$ is the cyclic group of order a generated by the automorphism which acts by sending every element to its pth power. Since $\mathbf{S}/\mathfrak{Q}$ is generated as a field extention of $\mathbb{Z}_p$ by α, the inertial degree of $\mathfrak{Q}$ can be no more than f. We now seek to prove equality. Assume $\alpha^{p^a} \equiv \alpha \text{ mod}(\mathfrak{Q})$. $p^a \equiv x \text{ mod}(m)$ with $1 \leq x \leq m$, so we have $\alpha^x \equiv \alpha \text{ mod}(\mathfrak{Q})$, and thus $\alpha^{x-1} - 1 \equiv 0 \text{ mod}(\mathfrak{Q})$. Now from the equality

$$y^{m-1} + y^{m-2} + \cdots + y + 1 = \frac{y^m - 1}{y - 1} = \prod_{i=1}^{m-1} (y - \alpha^i)$$

we obtain

$$\prod_{i=1}^{m-1} (1 - \alpha^i) = m$$

implying that $\alpha^{x-1} - 1$ divides m in $\mathbf{S}$, further implying that $m \in \mathfrak{Q}$ if $x > 1$. This is impossible, since p does not divide m, so $x = 1$ and we have proven that $a > f$. Thus the inertial degree of $\mathfrak{Q}$ must be f. □

With this proposition in place, our task becomes one of finding a prime with order mod(8) greater than 1. Since we'd also like to deal with a situation fairly different from the quadratic case, we'd also like a prime that does not remain prime in the extension. Thus we look for a prime of order 2. In fact, it would be quite difficult to find an odd prime that doesn't fit this requirement, as every element of $\mathbb{Z}_8^*$ has order 2. At random, we choose 7. The first thing to do is reduce the minimal polynomial for β mod(7). Unlike the quadratic case, this is not trivial. $4^4 \equiv 4$ mod(7), so the polynomial reduces to

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2).$$

Again choosing at random, let

$$\mathfrak{Q} = 7\mathbf{S} + (\beta^2 + 2\beta + 2).$$

Then $z = \beta^2 + 2\beta + 2$. z is obviously non-zero, so the first condition to concern ourselves with is for $z \equiv 1$ mod(d). Currently, we have $z \equiv 2$ mod(d). So we'd like to add a multiple of 7 which is congruent to -1 mod(256). Applying the trusty Euclidean algorithm, we find that $511 = 73 * 7$ works, so z becomes $\beta^2 + 2\beta + 513$. 2 is fairly obviously not the sum of 2 conjugates of $-\beta$, so we don't need to modify the term at all. On the other hand, the element

$$y = \prod_{c \in C} (p + v_{f-1})$$

where P is the collection of sums of f conjugates of β no longer presents us with a trivial case for the final condition. In our case, y comes out to 34,359,738,336, which factors into $2^5 * 3^2 * 7 * 11 * 31 * 151 * 331$. The final condition requires that the constant term of our polynomial in β be divisible by all primes dividing y which do not divide dp. In our case, $dp = 7 * 2^8$, so our constant term must divide 3, 11, 31, 151, and 331. Of course, we also must maintain the condition that the constant term be congruent to 1 mod(256), and we must satisfy these conditions by adding multiples of 7. This is merely a matter of applying the Chinese Remainder Theorem. After much crunching of large numbers, we obtain an appropriate value: 51,283,954,689. So our z becomes

$$\beta^2 + 2\beta + 51,283,954,689.$$

z then factors into prime ideals:

$$\mathfrak{Q} \prod_{i=1}^{t} \mathfrak{B}_i,$$

where the $\mathfrak{B}_i$'s do not divide d or p. (Because $z \equiv 1$ mod(d) and because if $\mathfrak{B}_i$ divided p, $\mathfrak{B}_i$ would contain $\mathfrak{Q}$). Now, since β satisfies

$$\beta^2 + 2\beta + 51,283,954,689 \equiv 0 \text{ mod}(\mathfrak{B}_i)$$

for each $\mathfrak{B}_i$, and the $\mathfrak{B}_i$'s don't divide $\beta\mathbf{S}$, each $\mathfrak{B}_i$ must have inertial degree $\leq f$. We want them to have intertial degree strictly less than f, and it turns out we do (good thing too, after all that). For each $\mathfrak{B}_i$,

$$\beta^2 + 2\beta + 51,283,954,689$$

must divide the minimal polynomial of $\beta \bmod(\mathfrak{B}_i)$, so we must have $2 \equiv c \bmod(\mathfrak{B}_i)$ for some $c \in C$. But then $y \equiv 0 \bmod(\mathfrak{B}_i)$, so the prime sitting under $\mathfrak{B}_i$ must divide y, but cannot divide dp, so we must have

$$51,283,954,689 \equiv 0 \bmod(\mathfrak{B}_i).$$

This implies that $\beta^2 + 2\beta \equiv 0 \bmod(\mathfrak{B}_i)$, which implies our desired result.

4.3 Results Obtained From the Lemma

Once the lemma is in place, it is fairly easy to show the following proposition:

Proposition 4.4. *Both the class group and the ray class group can be generated by the ideal classes (ray classes) of primes of inertial degree* 1 *which lie outside a given finite set* S*.*

Proof. First we must see that the groups can be generated by the ideal classes of primes outside a finite set S. In the case of the class group, let $[\mathfrak{A}]$ be any ideal class. Let $\{\mathfrak{P}_1, \mathfrak{P}_2, \cdots \mathfrak{P}_g\}$ be the set of primes in S. Then $\mathfrak{A} = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_g^{a_g}\mathfrak{B}$ for some ideal $\mathfrak{B}$ which is not divisible by any primes in S. Let α_i be an element of $\mathfrak{P}_i$ which is not in $\mathfrak{P}_i^2$ and is congruent to 1 modulo each $\mathfrak{P}_j$ with $j \neq i$. Let $\alpha = \prod_{n=1}^{g} \alpha_i^{a_i}$. Then $\alpha^{-1}\mathfrak{A}$ will not be divisible by any primes lying in S. Therefore the class group is generated by ideal classes of primes lying outside of S. To get the analogous result for the ray class group, we only need to extend our definition of the α_i's to be congruent to 1 (under the congruency used to define the ray class) modulo the product of primes used to define the ray class. (note that we don't have to worry about $\mathfrak{P}_i$ being in this product, since we are only dealing with ideals which are not divisible by those primes.) This shows that the class group and ray class group are generated by classes of primes outside any given finite set. Now we show that these primes can be chosen to be of inertial degree 1. Let $[\mathfrak{P}]$ be a prime ideal not in S, of inertial degree $f > 1$. We know from the lemma that there are primes $\mathfrak{Q}_i$ not in S with inertial degree $< f$ such that $\mathfrak{P} \prod \mathfrak{Q}_i^{-1} = x$. It follows that $[\mathfrak{P}] = \prod[\mathfrak{Q}_i^{-1}]$. If we induct on the inertial degree of the primes, assuming that all ideal classes generated by primes of inertial degree $< f$ are in the set generated by primes of inertial degree 1, then we are finished. Similarly, since we can assume $x \equiv 1$ modulo any prime dividing d in the lemma, if we choose d divisible by all primes in the set S and all primes in the product used to define the ray class group, we may apply the same induction arguement to prove the result for the ray class group. □

Now the result is proven, without resorting to density arguments.

In some proofs, the statement that the primes of degree 1 generate the ray class group may be used to replace the statement that the primes of degree 1 have density 1. The latter certainly implies the former, and for some results, the former is all that is required. As an example, we present one such proof.

Proposition 4.5. *Let* $\mathbf{K}$ *be a number field and let* $\mathbf{L}$ *be an extension of* $\mathbf{K}$*. If almost all primes of degree* 1 *in* $\mathbf{K}$ *split completely in* $\mathbf{L}$*, then* $\mathbf{K} = \mathbf{L}$*.*

Proof. We know that the primes that split completely in $\mathbf{L}$ split completely in the normal closure $\mathbf{L}'$ of $\mathbf{L}$ over $\mathbf{K}$. Let $\mathbf{K}'$ be an extension of $\mathbf{K}$ such that $\mathbf{L}'$ sits over $\mathbf{K}'$ and the Galois group of this extension is cyclic. If $\mathbf{L}' \neq \mathbf{K}$, we can assume $[\mathbf{L}' : \mathbf{K}'] > 1$. Then by the fundamental equality of class field theory, we know that for a given ray class group ${\mathbf{I}_{\mathbf{K}'}}^{\mathfrak{m}}/{\mathbf{K}'}_{\mathfrak{m},1}$,

$$[{\mathbf{I}_{\mathbf{K}'}}^{\mathfrak{m}} : N_{\mathbf{L}'/\mathbf{K}'}({\mathbf{I}_{\mathbf{L}'}}^{\mathfrak{m}}){\mathbf{K}'}_{\mathfrak{m},1}] > 1.$$

But we know that $N_{\mathbf{L}'/\mathbf{K}'}({\mathbf{I}_{\mathbf{L}'}}^{\mathfrak{m}})$ contains all primes of $\mathbf{K}'$ that split completely in $\mathbf{L}'$. By the assumption, it also contains almost all the primes of degree 1 of $\mathbf{K}'$. Then by the lemma, it must be the entire ray class group. This is a contradiction, so $\mathbf{K} = \mathbf{L}$. □

Bibliography

[1] G. Janusz; *Algebraic Number Fields.* American Mathematical Society, Graduate Studies in Mathematics **7**; 1996.

[2] H.W. Lenstra, P. Stevenhagen; *Primes of Degree One and Algebraic Cases of Cheboterev's Theorem.* L'Enseignement Mathematique **37**; 1991, 17-30.

Vita

Nathaniel A. Gaertner

Education

M.S. Mathematics, Virginia Tech, 2006. Thesis: Special Cases of Density Theorems in Algebraic Number Theory.

B.S. Mathematics, Virginia Tech, 2004.

Positions Held

Graduate Teaching Assistant, Department of Mathematics, Virginia Tech, 2004-2006.

Raconteur, Roustabout, and Renaissance Man, 1981-Present.