DIRICHLET L-FUNCTIONS AND DEDEKIND ζ-FUNCTIONS

FRIMPONG A. BAIDOO

Abstract. We begin by introducing Dirichlet L-functions which we use to prove Dirichlet's theorem on arithmetic progressions. From there, we discuss algebraic number fields and introduce the tools needed to define the Dedekind zeta function. We then use it to prove the class number formula for imaginary quadratic fields.

Contents

1. Introduction

L-functions are a class of functions that generalize the Riemann zeta function. In this paper, we will look at two kinds of L-functions, namely, Dirichlet L-functions and Dedekind zeta functions. The manner in which we will exposit on these two types of L-functions will essentially be the same. First, we provide preliminary information necessary to make sense of the L-function. After this, we define the L-function and then apply it to a problem in number theory to show how the L-function reveals arithmetic information.

In section 2, we introduce the Riemann zeta function, the prototype of all L-functions, study its pole and, in the process, prove Euclid's theorem that there are infinitely many prime numbers. In Sections 3 and 4, we aim to define the Dirichlet L-function. In section 5, we give a proof of Dirichlet's theorem on arithmetic progressions, which states that for two coprime positive integers a and n, there will be infinitely many prime numbers of the form $a+mn$, where m is a natural number. The next three sections then describe algebraic number fields and the aspects of it

Date: 30th August 2016.

necessary for providing context to the Dedekind zeta function. In section 9, we then define the Dedekind zeta function, describe the ideal class group and then highlight the Dedekind zeta function's role in the class number formula. Finally, following what was done in [5], we use the Dedekind zeta function to prove the class number formula for imaginary quadratic fields.

2. The Riemann Zeta Function

We begin by taking a brief look at the prototypical L-function, the Riemann Zeta function, highlighting properties we will be using. The Riemann zeta function is given by

$$\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}\,, \qquad \text{for} \quad s = \sigma + it \quad \text{where } \sigma, t \in \mathbb{R} \text{ and } \sigma > 1 \tag{2.1}$$

and one can use the Fundamental Theorem of Arithmetic to prove that the above series can be written as an infinite product

$$\zeta(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}}, \qquad \text{where } \mathcal{P} \text{ is the set of prime numbers.} \tag{2.2}$$

The zeta function is important because it contains a wealth of information regarding the field of rational numbers, $\mathbb{Q}$ (or, more precisely, the prime numbers). One such piece of information regarding the behaviour of prime numbers is the following

Theorem 2.3 (Euclid)**.** *There are infinitely many prime numbers.*

We will prove this theorem by showing that as $s \to 1$, the function $\sum_{p \in \mathcal{P}} p^{-s}$ is asymptotic the function $\log\left(\frac{1}{s-1}\right)$. Thus the series $\sum_{p \in \mathcal{P}} p^{-1}$ diverges, proving the theorem. For this, we first establish a fact regarding the Riemann zeta function.

Lemma 2.4. *$\zeta(s) = \frac{1}{s-1} + \psi(s)$ where $\psi(s)$ is some function that is holomorphic in the half-plane $\sigma > 0$.*

This lemma tells us that it is possible to define the zeta function so that it is holomorphic in $\sigma > 0$ except for $s = \sigma = 1$ where it will have a simple pole. By contrast, equations (2.1) and (2.2) only tell us that the zeta function is holomorphic in $\sigma > 1$.

Proof. We will prove that $\psi(s) = \zeta(s) - \frac{1}{s-1}$ defines a function that is holomorphic in the half-plane $\sigma > 0$.

First notice that

$$\frac{1}{s-1} = \int_1^{\infty} t^{-s}\, dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s}\, dt$$

We thus have that

$$\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{\infty} \int_n^{n+1} \frac{1}{n^s} - \frac{1}{t^s}\, dt \tag{2.5}$$

and it suffices to show that the right hand side of the equation (2.5) converges absolutely on the half-plane $\sigma > 0$.

Because

$$\int_n^{n+1} \frac{1}{n^s} - \frac{1}{t^s}\, dt = \int_n^{n+1} \int_t^n \frac{s}{x^{s+1}}\, dx\, dt$$

One can check that

$$\left| \int_n^{n+1} \frac{1}{n^s} - \frac{1}{t^s}\, dt \right| \leq \frac{|s|}{n^{\sigma+1}}$$

Thus we can use the comparison test to show that the right hand side of (2.5) converges absolutely for all $\sigma > 0$. □

Remark 2.6. It is actually possible to extend the zeta function to the entire complex plane. However, we do not need to do this for the proof of Dirichlet's theorem.

Proof of theorem 2.3. The presence of a pole at $s = 1$ means that the zeta function is non-zero on some neighbourhood of this point. We can therefore take the logarithm of both sides of the equation

$$\prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}} = \frac{1}{s-1} + \psi(s) \tag{2.7}$$

for $s \neq 1$ within this neighbourhood.

Taylor expanding the logarithm of the left hand side of (2.7) will then give

$$\sum_{p \in \mathcal{P}} \frac{1}{p^s} + \sum_{p \in \mathcal{P}} \sum_{k \geq 2} \frac{1}{p^{ks}} = \log\left(\frac{1}{s-1} + \psi(s) \right) \tag{2.8}$$

since $\psi(s)$ will be holomorphic (and thus bounded) on this neighbourhood, the right hand side of (2.8) will be asymptotic to $\log\left(\frac{1}{s-1}\right)$ as $s \to 1$. So now we only need to show that the double series on the left hand side of (2.8) remains bounded in order to prove Theorem 2.3.

It can be seen that the double series is actually a series whose terms are geometric series. Thus

$$\sum_{p \in \mathcal{P}} \left(\sum_{k \geq 2} \frac{1}{p^{ks}} \right) = \sum_{p \in \mathcal{P}} \frac{1}{p^s(p^s - 1)} \tag{2.9}$$

The series on the right is contained within the series $\sum \frac{1}{n^s(n^s-1)}$, which converges absolutely in the half-plane $\sigma > \frac{1}{2}$. Thus once we ensure that the region on which (2.8) is defined falls within a circle of radius $\frac{1}{2}$ centered at $s = 1$, we immediately prove that

$$\sum_{p \in \mathcal{P}} \frac{1}{p^s} \sim \log\left(\frac{1}{s-1} \right)$$

□

The asymptotic relation from the proof of Theorem 2.3, allows us to define the density of subsets of the prime numbers.

Definition 2.10. The *analytic density* (or *Dirichlet density*) of a subset $\mathcal{P}_a$ of the prime numbers $\mathcal{P}$ is defined to be the number k such that

$$\sum_{p \in \mathcal{P}_a} \frac{1}{p^s} \sim k \left(\log \left(\frac{1}{s-1} \right) \right)$$

as $s \to 1$. Notice that this immediately implies that $0 \leq k \leq 1$.

Remark 2.11. It can be shown that if a subset of the primes has a density defined in the most "natural sense" (the limit of the ratio of the number of elements in the subset to the number of prime numbers), then it will have an analytic density of the same value. However, the converse is false and this makes the analytic density a better way to define the density of subsets of the primes.

We now state a more precise version of Dirichlet's theorem that we will prove.

Theorem 2.12 (Dirichlet's Theorem on Arithmetic Progressions)**.** *Let a and n be two positive integers that are coprime and let $\mathcal{P}_a$ denote the set of prime numbers $p \equiv a \ (mod n)$. Then the set $\mathcal{P}_a$ has analytic density $\frac{1}{\phi(n)}$, where $\phi(n)$ is the Euler totient function.*

This theorem is stronger than the one stated in the introduction because, it not only says that $\mathcal{P}_a$ is an infinite set (if $\mathcal{P}_a$ were finite, its density would be 0) but also shows, as we will soon be able to see, that the set $\mathcal{P}$ distributes itself equally among all the $\mathcal{P}_a$, for a coprime to n.

Example 2.13. For $n = 5$ and $a \in \{0, 1, 2, 3, 4\}$, the portion of the arithmetic progressions less than 500 is shown on each line of the figure below with the prime numbers in the arithmetic progression circled.

For each $a \neq 0$, Dirichlet's theorem not only states that the sequence of circled primes for fixed a never ends but also shows that the probability of (almost) every prime number falling into one of the four arithmetic progressions is one-fourth.

3. Dirichlet Characters

Consider the ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n, where n is some fixed positive integer. As with any ring, the set of elements with multiplicative inverses $(\mathbb{Z}/n\mathbb{Z})^\times$ forms a group. It can be shown that $(\mathbb{Z}/n\mathbb{Z})^\times$ consists of those classes represented by integers coprime to n. Thus, the order of this group is $\phi(n)$, where ϕ is the Euler totient function.

Definition 3.1. A *Dirichlet Character (mod n)* is a group homomorphism

$$\chi \colon (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathbb{C} \backslash \{0\}$$

The Dirichlet character χ can then be extended to all of $\mathbb{Z}/n\mathbb{Z}$ by setting its value to zero for all the elements that do not belong to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$.

As a group homomorphism, a Dirichlet character satisfies the following properties:

(1) $\chi(1) = 1$

(2) for any $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$, $\chi(a \cdot b) = \chi(a) \cdot \chi(b)$

Furthermore, because Euler's theorem states that every element $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ is such that $a^{\phi(n)} \equiv 1 \pmod{n}$, we have that

$$\chi(a)^{\phi(n)} = \chi(a^{\phi(n)}) = 1$$

In other words,

$$\chi\colon (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \{\phi(n)\text{-th roots of unity}\}$$

Example 3.2. Consider $(\mathbb{Z}/3\mathbb{Z})^\times = \{1, 2\}$

For $\chi : (\mathbb{Z}/3\mathbb{Z})^\times \longrightarrow \{1, -1\}$ there will be only two possible Dirichlet characters:

(1) $\chi_1 \equiv 1$. Dirichlet characters that take this form are called *trivial characters*.

(2) $\chi_2(a) = \begin{cases} 1 & a = 1 \\ -1 & a = 2 \end{cases}$

The set of all possible Dirichlet characters of $(\mathbb{Z}/n\mathbb{Z})^\times$ along with point-wise multiplication also forms a group. In fact, it can be shown that the group of Dirichlet characters of $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. Thus, there are $\phi(n)$ possible Dirichlet characters mod n.

We now have enough information to prove some properties that will be important to the upcoming study of Dirichlet L-functions.

Proposition 3.3.

$$\sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi(a) = \begin{cases} \phi(n) & \text{if } \chi \text{ is the trivial character} \\ 0 & \text{if } \chi \text{ is not the trivial character} \end{cases}$$

Proof. The first part is obvious because there are $\phi(n)$ elements in $(\mathbb{Z}/n\mathbb{Z})^\times$ and $\chi(a) = 1$ for each of them.

For the second part, notice that for an element of the multiplicative group y such that $\chi(y) \neq 1$

$$\chi(y) \left(\sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi(a) \right) = \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi(a \cdot y) = \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi(a)$$

Thus we have that

$$(\chi(y) - 1) \cdot \left(\sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi(a) \right) = 0$$

This implies that the second part of the proposition is true.

□

Proposition 3.4.

$$\sum_{\chi} \chi(a) = \begin{cases} \phi(n) & a = 1 \\ 0 & \text{otherwise} \end{cases}$$

where the sum is over all the Dirichlet characters mod n.

Proof. The proof is essentially the same as that of Proposition 3.2. We could also make use of the isomorphism between the group of Dirichlet characters and the multiplicative group. □

It is also possible to say something more about the values which the group of Dirichlet characters take for a particular element of the multiplicative group.

Proposition 3.5. *If a is an element of the multiplicative group of order f, then $\chi(a)$ is an f-th root of unity for all the Dirichlet characters mod n. Furthermore, each f-th root of unity occurs $\frac{\phi(n)}{f}$ times among the Dirichlet characters.*

Proof. We have that $a^f = 1$. Thus $\chi(a)^f = 1$, proving the first part of the proposition.

Now suppose ρ is an arbitrary f-th root of unity and consider

$$\sum_{\chi} \sum_{m=1}^{f} \frac{\chi(a^m)}{\rho^m} = \sum_{\chi} \sum_{m=1}^{f} \left(\frac{\chi(a)}{\rho} \right)^m \tag{3.6}$$

If $\chi(a) \neq \rho$, then

$$\sum_{m=1}^{f} \frac{\chi(a^m)}{\rho^m} = 0$$

(recall that for an f-th root of unity $\epsilon \neq 1$, $\epsilon^{f-1} + \cdots + \epsilon + 1 = 0$)

but if $\chi(a) = \rho$, then

$$\sum_{m=1}^{f} \frac{\chi(a^m)}{\rho^m} = f$$

Thus (3.6) equals gf, where g is the number of times that $\chi(a) = \rho$.

At the same time, if we exchange the summation signs on the left hand side of (3.6) and apply Proposition 3.4, we will find that (3.6) also equals $\phi(n)$.

Thus we have $\phi(n) = gf$ which just means that $g = \frac{\phi(n)}{f}$.

□

4. Dirichlet L-functions

The Dirichlet L-function associated to a given Dirichlet character mod n is given by

$$L(s, \chi) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s} \tag{4.1}$$

We need to clarify that in the above equation, $\chi(k)$ actually refers to the value of χ for the element of $\mathbb{Z}/n\mathbb{Z}$ that is congruent to k mod n.

Similar to the Riemann zeta function, we can use the fundamental theorem of arithmetic and the multiplicative property of χ to prove that (4.1) can also be written as

$$L(s, \chi) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}}, \qquad \text{for } \sigma > 1 \tag{4.2}$$

For the trivial character χ_1, a comparison to equation (2.2) yields an immediate observation.

Proposition 4.3.

$$L(s,\chi_1) = \zeta(s)\cdot\left(\prod_{p|n}(1-p^{-s})\right), \qquad \textit{for } \sigma > 1$$

As a consequence, $L(s,\chi_1)$ has a simple pole at $s=1$.

The presence of non-trivial characters in Dirichlet L-functions has an interesting effect on their value at $s=1$. We shall now set out to prove a very crucial point for the proof of Dirichlet's theorem: non-trivial Dirichlet L-functions converge to a non-zero value at $s=1$.

Lemma 4.4. *For a sequence of complex numbers (a_k), let $S(K) = a_1+a_2+\cdots+a_K$. Suppose that for all K, there exists a fixed non-negative number r such that $\left|\frac{S(K)}{K^r}\right| \leq M$, where M is a constant independent of K. Then the series $\sum \frac{a_k}{k^s}$ converges for all $\sigma > r$.*

Proof. We will have that

$$\left|\sum_{k=K}^{T}\frac{a_k}{k^s}\right| = \left|\sum_{k=K}^{T}\frac{S(k)-S(k-1)}{k^s}\right| = \left|\frac{S(T)}{T^s} - \frac{S(K-1)}{K^s} + \sum_{k=K}^{T-1} S(k)\left(\frac{1}{k^s}-\frac{1}{(k+1)^s}\right)\right|$$

Using the fact that

$$\frac{1}{k^s} - \frac{1}{(k+1)^s} = s\int_k^{k+1}\frac{dx}{x^{s+1}}$$

We can show that

$$\left|\sum_{k=K}^{T}\frac{a_k}{k^s}\right| \;\leq\; \frac{2M}{(K-1)^{\sigma-r}} \;+\; \sigma\sum_{k=K}^{T-1}\frac{M}{k^{1+(\sigma-r)}}$$

Thus if $\sigma > r$, the tail end of the series will approach zero as K and T approach infinity.

□

We now show, first of all, that the non-trivial Dirichlet L-functions converge for $s=1$.

Lemma 4.5. *For a non-trivial Dirichlet character χ, the series $L(s,\chi)$ converges in the half-plane $\sigma > 0$. In particular, $L(1,\chi)$ is defined.*

Proof. Proposition 3.3 makes it possible to see that

$$\left|\sum_{k=1}^{K}\chi(k)\right| \leq \phi(n), \qquad \text{independent of } K.$$

Thus Lemma 4.4 shows that non-trivial L-functions converge in the half-plane $\sigma > 0$.

□

Now for any prime p that does not divide n , let $f(p)$ be the order of the image of p in $(\mathbb{Z}/n\mathbb{Z})^\times$ and let $g(p) = \frac{\phi(n)}{f(p)}$. Define the function

$$\zeta_{\omega_n}(s) = \prod_{\chi} L(s,\chi) = \prod_{\chi}\prod_{p\nmid n}\frac{1}{1-\frac{\chi(p)}{p^s}}$$

Using Proposition 3.5, we can simplify the second expression for $\zeta_{\omega_n}(s)$ to

$$\zeta_{\omega_n}(s) = \prod_{p \nmid n} \left(1 - \frac{1}{p^{f(p)s}}\right)^{-g(p)} \tag{4.6}$$

Theorem 4.7. *$L(1, \chi) \neq 0$ for all non-trivial Dirichlet characters mod n*

Proof. If $L(1, \chi) \neq 0$ for all non-trivial characters, then $\zeta_{\omega_n}(s)$ has a simple pole at $s = 1$, by Proposition 4.3.

On the other hand, suppose, for a contradiction, that there is a non-trivial character for which $L(1, \chi) = 0$. This then implies that $\zeta_{\omega_n}(s)$ converges for all $\sigma > 0$ by Lemma 4.5.

If we consider just $s \in \mathbb{R}$, we then have that

$$\left(1 - \frac{1}{p^{\phi(n)s}}\right)^{-1} = \sum_{k=0}^{\infty} \frac{1}{p^{k\phi(n)s}} \leq \left(\sum_{k=0}^{\infty} \frac{1}{p^{kf(p)s}}\right)^{g(p)} = \left(1 - \frac{1}{p^{f(p)s}}\right)^{-g(p)}$$

This implies that

$$\zeta_{\omega_n}(s) \geq \prod_{p \nmid n} \left(1 - \frac{1}{p^{\phi(n)s}}\right)^{-1}$$

However, the expression on the right hand side of the inequality is basically the zeta function with a finite number of terms removed and will diverge for $s = \frac{1}{\phi(n)}$, implying that $\zeta_{\omega_n}(s)$ also diverges for this value of s. We thus contradict our assumption that $\zeta_{\omega_n}(s)$ converges for all $\sigma > 0$.

□

5. Dirichlet's Theorem on Arithmetic Progressions

Let

$$d_\chi(s) = \sum_{p \nmid n} \frac{\chi(p)}{p^s}$$

For $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ we shall be able to prove that the set of all prime numbers congruent to a mod n, $\mathcal{P}_a$, is such that

$$h_a(s) = \sum_{p \in \mathcal{P}_a} \frac{1}{p^s} \sim \frac{1}{\phi(n)} \log\left(\frac{1}{s-1}\right) \quad \text{as } s \to 1 \tag{5.1}$$

by looking at the behaviour of $d_\chi(s)$ as s approaches one.

Our first observation is that for the trivial character χ_1,

$$d_1(s) = \sum_{p \nmid n} \frac{1}{p^s} \sim \log\left(\frac{1}{s-1}\right)$$

by Theorem 2.3 because it differs from $\sum_{p \in \mathcal{P}} \frac{1}{p^s}$ by only a finite number of terms.

The next thing would be to prove that

Proposition 5.2. *For the non-trivial characters, $d_\chi(s)$ remains bounded as s approaches one.*

It is here that Theorem 4.7 will play a crucial role.

Proof. The proof of this proposition is quite similar to the proof of Theorem 2.3 and we will, in fact, use equation (2.9) from that proof here.

Because we have been able to establish that $L(1,\chi) \neq 0$, we can take the logarithm of both sides of equation (4.2) for some neighbourhood around $s = 1$. We can also Taylor expand the logarithm of the terms on the right hand side of (4.2) because $\left|\frac{\chi(p)}{p^s}\right| < 1$. This gives us

$$\log(L(s,\chi)) = d_\chi(s) + \sum_{p \nmid n} \sum_{k=2}^{\infty} \frac{\chi(p)^k}{p^{ks}}$$

Lemma 4.5 and Theorem 4.7 imply that $\log(L(s,\chi))$ will remain bounded as s approaches one. What is more, the second term on the right hand side will remain bounded as s approaches one because comparing it to equation (2.9) would prove that it converges absolutely on some neighbourhood of one. Put together, this would imply that $d_\chi(s)$ remains bounded as s approaches one.

□

The final step to proving Dirichlet's theorem is to show that

Proposition 5.3.

$$h_a(s) = \frac{1}{\phi(n)} \sum_{\chi} \chi(a^{-1}) d_\chi(s)$$

From what we have seen so far this would immediately imply that

$$h_a(s) \sim \frac{d_1(s)}{\phi(n)} \sim \frac{1}{\phi(n)} \log\left(\frac{1}{s-1}\right)$$

Proof.

$$\sum_{\chi} \chi(a^{-1}) d_\chi(s) = \sum_{p \nmid n} \sum_{\chi} \frac{\chi(a^{-1}) \cdot \chi(p)}{p^s}$$

Whenever p is congruent to a mod n, $\chi(a^{-1}) \cdot \chi(p) = 1$ thus the sum over all characters evaluates to $\phi(n)$ by Proposition 3.4. Proposition 3.4 also shows that if p is not congruent to a, then the sum over all characters evaluates to zero. Thus the above equation simplifies to

$$\sum_{p \in P_a} \frac{\phi(n)}{p^s} = \phi(n) h_a(s)$$

With this, we prove Dirichlet's theorem on arithmetic progressions.

□

6. Algebraic Number Fields

In the preceding sections, we focused on generalising the Riemann zeta function in order to obtain information about the field $\mathbb{Q}$. We shall now generalize the Riemann zeta function in order to obtain information about a larger class of fields called algebraic number fields.

Definition 6.1. An *algebraic number field* is a finite field extension of $\mathbb{Q}$.

First of all, this means that it is a field that contains $\mathbb{Q}$ as a sub-field. However, a more detailed explanation is that an algebraic number field is a finite-dimensional vector space over the field $\mathbb{Q}$. The dimension of this vector space is called its *degree*.

Polynomials with rational coefficients play an important part in the description of algebraic number fields and we therefore take a brief look at them. For any two polynomials with rational coefficients $f(x)$ and $g(x)$, we say that $g(x)$ divides $f(x)$ if there exists another polynomial of rational coefficients $q(x)$ such that

$$f(x) = q(x)g(x)$$

Thus every rational polynomial $f(x)$ is trivially divisible by any non-zero rational number c and the polynomial $\frac{1}{c}f(x)$. We say that a polynomial is irreducible (over $\mathbb{Q}$) if it is only divisible by these trivial factors.

Example 6.2. x^2+1 can only be non-trivially factored into $x+i$ and $x-i$. However these are not rational polynomials and thus x^2+1 is irreducible.

It can be shown that an irreducible (rational) polynomial of degree n will have n distinct roots and that if a rational polynomial $g(x)$ shares a root with an irreducible polynomial, then $g(x)$ will be divisible by the irreducible polynomial (Theorems 48 and 49 of [2]).

An algebraic number θ is a number that is a root of some rational polynomial. Among all the the rational polynomials for which θ is a root, there will necessarily be an irreducible polynomial of smallest degree as a result of the previous statement. Assume the degree of this polynomial is n. If we create a field $\mathbb{Q}(\theta)$ by adjoining θ to $\mathbb{Q}$, it will be an algebraic number field of degree n because it can be shown that every element of $\mathbb{Q}(\theta)$ can be uniquely represented as $p_{n-1}\theta^{n-1}+\cdots+p_2\theta^2+p_1\theta+p_0$ where $p_i \in \mathbb{Q}$ for $0 \leq i \leq n-1$ (Theorem 53 of [2]). That is to say that the set $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ forms a basis of $\mathbb{Q}(\theta)$.

Example 6.3. Examples of Algebraic Number Fields

(1) The field $\mathbb{Q}$ is a trivial example. Its degree is one.
(2) The field $\mathbb{Q}(\sqrt{-n}) = \{a + b\sqrt{-n} : \ a, b \in \mathbb{Q}\}$, where n is a square-free integer. The degree of such a field will be two. They are referred to as imaginary quadratic fields.
(3) The field obtained by adjoining a primitive n-th root of unity (a root of unity for which the smallest power that equals one is n). The degree of these fields is $\phi(n)$ and they are called cyclotomic fields.

Finally it is important to note that every element x of an algebraic number field is the root of some rational polynomial (in other words, every element of an algebraic number field is an algebraic number) because x^k must be dependent on $\{1, x, \ldots, x^{k-1}\}$ for some k.

7. The Ring of Integers

Now that we have generalised the rational numbers $\mathbb{Q}$, we turn our attention to also generalising the integers $\mathbb{Z}$ within $\mathbb{Q}$. For any rational polynomial, we can divide all of its coefficients by the leading coefficient in order to make it a monic rational polynomial (the leading coefficient equals one) and this will have no effect on its roots. Thus, we can restrict our attention to just the monic polynomials in our study of algebraic number fields.

Definition 7.1. An *algebraic integer* is a number that is the root of some monic polynomial with integer coefficients.

Once again, it can be shown that among the monic integer polynomials for which an algebraic integer α_1 is a root, there is an irreducible polynomial of smallest degree n having n distinct roots $\{\alpha_1, \alpha_2, ..., \alpha_n\}$. We shall call these n distinct roots *conjugates*.

The first thing we should notice is that every element t in $\mathbb{Z}$ is an algebraic integer because it is the root of the polynomial $f(x) = x - t$. In fact, one could show that the elements of $\mathbb{Z}$ are the only rational algebraic integers. Just as the set of rational integers $\mathbb{Z}$ form a ring in $\mathbb{Q}$, the set of algebraic integers of a given algebraic number field form a ring within the field. For this reason, the set of algebraic integers of an algebraic number field K is referred to as the ring of integers $\mathcal{O}_K$. The elements of $\mathcal{O}_K$ that have multiplicative inverses are called the *units* of $\mathcal{O}_K$. They play a role analogous to ± 1 in $\mathbb{Z}$ and one can easily see that ± 1 will always be among the units of any ring of integers. If the division of any two elements of $\mathcal{O}_K$ results in a unit, then the two elements are said to be *associates*.

Given the various similarities between $\mathcal{O}_K$ and $\mathbb{Z}$ we have seen so far, it is now reasonable to ask whether $\mathcal{O}_K$ also admits unique factorisation into "prime" elements like $\mathbb{Z}$ does. Unfortunately, the answer is not always yes. The classic example is found in the ring of integers $\mathbb{Z}[\sqrt{-5}]$ where
$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ although the elements 2, $3, 1 + \sqrt{-5}$, $1 - \sqrt{-5}$ are each *irreducible* in $\mathbb{Z}\sqrt{-5}$, meaning that they can only be factored into a unit and an associate. However, all hope is not lost. Unique factorization may not always exist for the elements of a ring of integers but it always exists for ring theoretic structures in $\mathcal{O}_K$ called *ideals*. In fact, the study of ideals provides a deeper insight into the nature of factorization in a ring of integers.

8. Ideals of the Ring of Integers

Definition 8.1. An *ideal* $\mathfrak{a}$ is a subset of $\mathcal{O}_K$ such that:

(1) if α and β belong in $\mathfrak{a}$ then so will $\alpha + \beta$ and $\alpha \cdot \beta$
(2) for every $\gamma \in \mathcal{O}_K$ and $\alpha \in \mathfrak{a}$, $\gamma\alpha$ will belong in $\mathfrak{a}$

A very important example of an ideal will be the set

$$(\alpha) = \{\gamma\alpha \colon \gamma \in \mathcal{O}_K\}$$

Ideals of this form are called *principal ideals*. Similar to (α), one can define an ideal

$$(\alpha_1, \ldots, \alpha_k) = \{\gamma_1\alpha_1 + \cdots + \gamma_k\alpha_k \colon \gamma_i \in \mathcal{O}_K\}$$

It can be shown that every ideal in $\mathcal{O}_K$ can be written in this form (Theorem 65 of [2]).

We now define addition and multiplication of ideals of $\mathcal{O}_K$. We begin with addition where for two ideals $\mathfrak{a}$ and $\mathfrak{b}$,

$$\mathfrak{a} + \mathfrak{b} = \{\alpha + \beta \colon \alpha \in \mathfrak{a} \text{ and } \beta \in \mathfrak{b}\}$$

If we let $\mathfrak{a} = (\alpha_1, ..., \alpha_k)$ and $\mathfrak{b} = (\beta_1, ..., \beta_j)$, then the above definition will be equivalent to $\mathfrak{a} + \mathfrak{b} = (\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_j)$. From this, one can see that the additive identity will be the zero ideal (0).

As for multiplication,

$$\mathfrak{a} \cdot \mathfrak{b} = \{a_1b_1 + ... + a_rb_r \colon a_i \in \mathfrak{a} \text{ and } b_i \in \mathfrak{b}\}$$

that is, the set of all sums of the products of elements of $\mathfrak{a}$ and $\mathfrak{b}$. This definition is the same as $\mathfrak{a} \cdot \mathfrak{b} = (\alpha_1\beta_1, \ldots, \alpha_i\beta_t, \ldots, \alpha_k\beta_j)$. From this definition, it can be seen that the unit ideal $(1) = \mathcal{O}_K$ will serve as the multiplicative identity. One should note that $(1) =$ (any unit of $\mathcal{O}_K$) because $1 = u \times u^{-1}$, where u is a unit of $\mathcal{O}_K$.

With multiplication, we can now define divisibility of ideals. The ideal $\mathfrak{b}$ is said to divide $\mathfrak{a}$ if there exists another ideal $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$. Thus every ideal is divisible by (1) and itself. In analogy to $\mathbb{Z}$, we can therefore define a *prime ideal* $\mathfrak{p}$ to be any ideal, not equal to (1) or (0), that can only be factored as $(1) \cdot \mathfrak{p}$.

For any ideals $\mathfrak{c}$ and $\mathfrak{d}$ we will have that $\mathfrak{b} = \mathfrak{c} \cdot \mathfrak{d} \subseteq \mathfrak{c}$ because, by the above definition of multiplication of ideals, every element of $\mathfrak{c} \cdot \mathfrak{d}$ will be an element of $\mathfrak{c}$. It turns out that the converse statement is also true: if the ideal $\mathfrak{b}$ is a subset of the ideal $\mathfrak{c}$, then $\mathfrak{c}$ divides $\mathfrak{b}$ (Theorems 66 to 69 of [2]). These considerations allow us to conclude that

Proposition 8.2. *If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then it is maximal. In other words, if an ideal $\mathfrak{a}$ contains $\mathfrak{p}$, then either $\mathfrak{a} = \mathfrak{p}$ or $\mathfrak{a} = (1)$.*

Proposition 8.3. *If a prime ideal $\mathfrak{p}$ divides $\mathfrak{a} \cdot \mathfrak{b}$, then $\mathfrak{p}$ divides either $\mathfrak{a}$ or $\mathfrak{b}$.*

Proof. Without loss of generality, assume $\mathfrak{p}$ does not divide $\mathfrak{a}$. We first pick an element $a \in \mathfrak{a}$ that does not belong in $\mathfrak{p}$. Notice that for every $b \in \mathfrak{b}$, we have that $ab \in \mathfrak{p}$. Since the only way to factor the prime ideal $\mathfrak{p}$ is as $(1) \cdot \mathfrak{p}$ and since a does not belong in $\mathfrak{p}$ (obviously $a \in (1)$), we conclude that b has to belong in $\mathfrak{p}$ in order for $ab \in \mathfrak{p}$. Thus, every element of $\mathfrak{b}$ belongs in $\mathfrak{p}$, that is, $\mathfrak{b} \subseteq \mathfrak{p}$ and hence $\mathfrak{p}$ divides $\mathfrak{b}$.

□

The next thing we turn our attention to is the notion of residue classes modulo an ideal. For an ideal $\mathfrak{a} \neq (0)$, the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is created by placing into an equivalence class all elements $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha - \beta \in \mathfrak{a}$. It can be shown that the new ring $\mathcal{O}_K/\mathfrak{a}$ will have a finite number of elements (in fact, [2] gives an explicit formula for calculating this number in Theorem 76) and we refer to this number as the norm of the ideal $N(\mathfrak{a})$. The norm of an ideal is a completely multiplicative function, that is $N(\mathfrak{b} \cdot \mathfrak{c}) = N(\mathfrak{b}) \cdot N(\mathfrak{c})$. This implies that if $\mathfrak{a} \subset \mathfrak{b}$, then $N(\mathfrak{a}) > N(\mathfrak{b})$.

Theorem 8.4 (The Fundamental Theorem of Ideal Theory)**.** *Every non-trivial ideal can be uniquely factored as a product of prime ideals. That is,*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_k^{e_k}$$

Proof. The proof is carried out by induction on $N(\mathfrak{a})$.

If the ideal $\mathfrak{a}$ is prime, then there is nothing left to prove. Otherwise, by definition, the ideal can be factored as $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$, where neither $\mathfrak{b}$ nor $\mathfrak{c}$ is (1) and $1 \leq N(\mathfrak{b}) < N(\mathfrak{a})$ and $1 \leq N(\mathfrak{c}) < N(\mathfrak{a})$. If either $\mathfrak{b}$ or $\mathfrak{c}$ is a prime ideal, we stop trying to factorize it. Otherwise we proceed to factor it into the product of ideals and the norms of the factors will be smaller than the factored ideal. Repeat.

Because the norms keep reducing at each factorization step, we are guaranteed to stop after a finite number of steps. At this point we would be left with only a product of prime ideals.

Now all that is left to prove is that this final product of primes is unique. Suppose

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i = \prod_{j=1}^{l} \mathfrak{q}_j$$

where $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are prime ideals. Proposition 8.3 implies that (without loss of generality) $\mathfrak{p}_1 = \mathfrak{q}_1$. We can therefore remove them from the equation above. Repeating this process for the equation that remains, will show that each $\mathfrak{p}_i$ is equal to some particular $\mathfrak{q}_j$. Hence the prime factorization we obtain is unique. □

We can now return to the counterexample of unique factorization of elements in the ring of integers $\mathbb{Z}[\sqrt{-5}]$, namely, $6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. We look to the corresponding principal ideals for some insight.

$$(6) = (2) \times (3) = (1+\sqrt{-5}) \times (1-\sqrt{-5})$$

By Theorem 8.4, the principal ideals $(2), (3), (1+\sqrt{-5})$ and $(1-\sqrt{-5})$ cannot be prime. And indeed, these principal ideals have the following prime factorizations

$$\begin{aligned}
(2) &= (2, 1+\sqrt{-5}) \times (2, 1-\sqrt{-5}) \\
(3) &= (3, 1+\sqrt{-5}) \times (3, 1-\sqrt{-5}) \\
(1+\sqrt{-5}) &= (2, 1+\sqrt{-5}) \times (3, 1+\sqrt{-5}) \\
(1-\sqrt{-5}) &= (2, 1-\sqrt{-5}) \times (3, 1-\sqrt{-5})
\end{aligned}$$

Thus the failure of unique factorization of elements in the ring $\mathbb{Z}[\sqrt{-5}]$ is just a reflection of the fact that the corresponding principal ideals are not prime even though the elements $2, 3, 1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Either way we are left with the fact that

$$(6) = (2, 1+\sqrt{-5}) \times (2, 1-\sqrt{-5}) \times (3, 1+\sqrt{-5}) \times (3, 1-\sqrt{-5})$$

9. The Dedekind Zeta Function and The Class Number Formula

We now have the necessary tools to introduce another L-function.

The *Dedekind Zeta Function* of an algebraic number field K is the function

$$\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \left(\frac{1}{N(\mathfrak{a})}\right)^s \qquad \sigma > 1 \tag{9.1}$$

We can apply the fundamental theorem of ideal theory to show that (9.1) can also be written as an infinite product of the norms of prime ideals, much like the Riemann zeta function.

$$\zeta_K(s) = \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{1 - \left(\frac{1}{N(\mathfrak{p})}\right)^s} \qquad \sigma > 1 \tag{9.2}$$

In fact, when $K = \mathbb{Q}$, the Dedekind zeta function becomes the Riemann zeta function.

Proof. Notice that every ideal in $\mathbb{Z}$ is a principal ideal because any ideal (a, b) for two integers a and b, contains their greatest common divisor d. Consequently $(a, b) = (d)$ because d divides every element of (a, b) (i.e. $(a, b) \subseteq (d)$) and at the same time every element of (d) is an element of (a, b) (i.e. $(d) \subseteq (a, b)$). Also for any number n, $(n) = (-n)$. Thus we can assume that n is a positive integer.

The norm of the ideal (n) is going to be the number of elements in the ring $\mathbb{Z}/(n)$. This happens to be the number of elements in $\mathbb{Z}/n\mathbb{Z}$, which is n

Thus using (9.1),

$$\zeta_{\mathbb{Q}}(s) = \sum_{(n) \subseteq \mathbb{Z}} \frac{1}{N(n)^s} = \sum_{n \in \mathbb{Z}^+} \frac{1}{n^s} = \zeta(s)$$

□

We have already encountered a second Dedekind zeta function. The function $\zeta_{\omega_n}(s)$ from equation (4.6) is the Dedekind zeta function for the n-th cyclotomic field. The proof of Theorem 4.7 implies that this zeta function converges for all $\sigma > 0$ except at the point $s = 1$ where it has a simple pole, just like the Riemann zeta function. This property is actually shared by the all Dedekind zeta functions, not just the two we have encountered. What's more, all Dedekind zeta function can be extended to the entire complex plane, where they are subject to the Riemann Hypothesis (The non-trivial zeros of the function lie on the line $\sigma = \frac{1}{2}$).

Dedekind zeta functions encode information about their respective algebraic number fields and in this section we will highlight their role in the class number formula.

We begin by defining the ideal class group. Ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}_K$ are placed into the same equivalence class if there exist principal ideals (a) and (b) (for non-zero a and b) such that $\mathfrak{a} \times (a) = \mathfrak{b} \times (b)$. The set of these equivalence classes form a group under multiplication called the *ideal class group*. All principal ideals fall into the same equivalence class $\mathcal{C}_1$ because $(a) \times (b) = (b) \times (a)$. Now notice that for any (non-zero) principal ideal (a), $\mathfrak{a}$ and $\mathfrak{a} \cdot (a)$ always belong to the same equivalence class. This means that $\mathcal{C}_1$ is the identity element of the ideal class group. We now look into the inverse of an equivalence class.

Proposition 9.3. *For any ideal $\mathfrak{a}_1$ there exists an ideal $\mathfrak{b}_1$ (not unique) for which $\mathfrak{a}_1 \cdot \mathfrak{b}_1$ is a principal ideal. Furthermore, if $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are in the same class and $\mathfrak{a}_2 \cdot \mathfrak{b}_2$ is a principal ideal, then $\mathfrak{b}_1$ and $\mathfrak{b}_2$ are in the same class.*

Proof. $\mathfrak{a}_1$ can be factored uniquely into prime ideals. That is

$$\mathfrak{a}_1 = \prod_{i=1}^{k} \mathfrak{p}_i$$

For each $\mathfrak{p}_i$, we pick one element $\alpha_i \in \mathfrak{p}_i$. We will have that $(\alpha_i) \subseteq \mathfrak{p}_i$ by the definition of an ideal. Thus, $\mathfrak{p}_i$ divides (α_i).
In other words

$$(\alpha_i) = \prod_{j=1}^{m(i)} \mathfrak{p}_{ij} \qquad \text{where } \mathfrak{p}_i = \mathfrak{p}_{i1}$$

If we pick

$$\mathfrak{b}_1 = \prod_{i=1}^{k} \prod_{j=2}^{m(i)} \mathfrak{p}_{ij}$$

then we will have

$$\mathfrak{a}_1 \cdot \mathfrak{b}_1 = \prod_{i=1}^{k} (\alpha_i)$$

Of course, $\mathfrak{b}_1$ is not the only ideal that we can multiply $\mathfrak{a}_1$ by to obtain a principal ideal. The ideal $\mathfrak{a}_1 \cdot \mathfrak{b}_1^2$, for example, will give the square of the principal ideal we obtained above.

To prove the second part of the proposition, let $(a_1) \cdot \mathfrak{a}_1 = (a_2) \cdot \mathfrak{a}_2$ and let $\mathfrak{a}_1 \cdot \mathfrak{b}_1 = (c_1)$ whilst $\mathfrak{a}_2 \cdot \mathfrak{b}_2 = (c_2)$

Now consider the principal ideal $(c_1 \cdot c_2 \cdot a_1 \cdot a_2) = (a_1) \cdot \mathfrak{a}_1 \cdot \mathfrak{b}_1 \cdot (c_2 \cdot a_2)$, which can also be written as $(c_1 \cdot c_2 \cdot a_1 \cdot a_2) = (a_2) \cdot \mathfrak{a}_2 \cdot \mathfrak{b}_2 \cdot (c_1 \cdot a_1)$.

Combining these two equations gives us

$$(a_2) \cdot \mathfrak{a}_2 \cdot \mathfrak{b}_2 \cdot (c_1 \cdot a_1) = (a_1) \cdot \mathfrak{a}_1 \cdot \mathfrak{b}_1 \times (c_2 \cdot a_2)$$

Because $(a_1) \cdot \mathfrak{a}_1 = (a_2) \cdot \mathfrak{a}_2$, the above equation simplifies to

$$(c_1 \cdot a_1) \cdot \mathfrak{b}_1 = (c_2 \cdot a_2) \cdot \mathfrak{b}_2$$

Thus $\mathfrak{b}_1$ and $\mathfrak{b}_2$ belong to the same equivalence class.

□

The ideal class group of an algebraic number field is always finite and the number of elements in the group is called the *class number*, h. The class number allows us to determine whether the elements of a ring of integers can be uniquely factored into irreducible elements.

Theorem 9.4. *The elements of a ring of integers $\mathcal{O}_K$ can be uniquely factored if and only if the class number of $\mathcal{O}_K$, h, is trivial, that is, if and only if $h = 1$.*

Proof. Let us first assume that $h = 1$. This means that every ideal in $\mathcal{O}_K$ is a principal ideal. By the Fundamental Theorem of Ideal Theory, for any element $\alpha \in \mathcal{O}_{\mathbb{K}}$

$$(\alpha) = \prod_{i=1}^{k} (r_i), \quad \text{where each } (r_i) \text{ is a prime ideal.}$$

This then implies that α is equal to the product of the terms r_i. Because each (r_i) is a prime ideal we have that r_i will be irreducible. Thus, we prove unique factorization when $h = 1$.

Now let us assume the ring $\mathcal{O}_K$ has unique factorization. Our goal is to show that every ideal of $\mathcal{O}_K$ is a principal ideal. We first prove that the principal ideal of an irreducible element r will be a prime ideal. Suppose that (r) can be factored non-trivially as $(r) = \mathfrak{a} \cdot \mathfrak{b}$. Then there exists an element of $\mathfrak{a}$ - let us call it a - and an element of $\mathfrak{b}$ - let us call it b - such that a and b do not belong in (r), but their product ab is in (r). This is a contradiction because ab is divisible by r and thus unique factorization implies that r divides either a or b. In other words, either a or b belongs in (r). Thus, (r) has to be a prime ideal.

We now prove that every ideal in $\mathcal{O}_K$ can be factored into principal ideals of irreducible elements. By Proposition 9.3, we can multiply any ideal $\mathfrak{a}$ in $\mathcal{O}_K$ by some ideal $\mathfrak{b}$ in order to obtain a principal ideal (α). Due to unique factorisation, α can be factored into irreducible elements r_i. Thus,

$$(\alpha) = \mathfrak{a} \cdot \mathfrak{b} = \prod_{i=1}^{k} (r_i)$$

By Proposition 8.3, this implies that both $\mathfrak{a}$ and $\mathfrak{b}$ factor into the principal ideals of irreducible elements of $\mathcal{O}_K$. This means that $\mathfrak{a}$ is a principal ideal. □

The *class number formula* connects the class number, along with other important invariants of an algebraic number field K, to the residue of the Dedekind zeta function's pole at $s = 1$.

$$\lim_{s \to 1} (s-1)\zeta_K = \frac{2^{r_1} (2\pi)^{r_2} \mathcal{R}\, h}{\omega \sqrt{d_K}} \tag{9.5}$$

Here, r_1 is the number of real embeddings of K, r_2 is the number of pairs of complex embeddings, $\mathcal{R}$ is the regulator of K, ω is the number of roots of unity in K and d_K is the discriminant. These invariants are very important in their own right and worthy of good exposition. Unfortunately, we do not have the space for this here. Thus, we present the class number formula here just to emphasize how valuable the arithmetic data stored in the Dedekind zeta function can be.

10. Imaginary Quadratic Fields

We now set out to prove the class number formula for the case of imaginary quadratic fields. For an imaginary quadratic field $\mathbb{Q}[\sqrt{-n}\,]$, the corresponding ring of integers $\mathcal{O}_{-n}$ will come in one of two forms.

$$\mathcal{O}_{-n} = \begin{cases} \mathbb{Z}[\sqrt{-n}\,] & \text{if } n \equiv 1, 2 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{-n}}{2}] & \text{if } n \equiv 3 \pmod 4 \end{cases}$$

The class number formula is slightly different in the two cases but the proof is the same. Thus for simplicity, we shall use the first case, $\mathcal{O}_{-n} = \mathbb{Z}[\sqrt{-n}\,]$.

The first course of action will be to write the Dedekind zeta function $\zeta_{-n}(s)$ as an infinite product over the prime numbers. To do this, we first use the *Legendre symbol* to separate the prime numbers into three sets which we shall call P_{-1}^n, P_1^n and P_0^n. For an odd prime number p, the Legendre symbol is

$$\left(\frac{k}{p}\right) = \begin{cases} 1 & k \equiv x^2 \pmod p \text{ for some integer } x \\ -1 & k \not\equiv x^2 \pmod p \text{ for any integer } x \\ 0 & k \equiv 0 \pmod p \end{cases}$$

For fixed n, we define the set $P_{-1}^n = \left\{p\colon \left(\frac{-n}{p}\right) = -1\right\}$. The sets P_1^n and P_0^n are also defined in the same manner. For a prime number p, the prime ideals that factor (p) take a distinctive form based on which of the three sets p belongs to. Since every prime ideal contains exactly one prime number $p \in \mathbb{Z}$, this implies that we can give a characterization of all the prime ideals in our ring of integers. Before we do this we have to look at how we calculate norms of ideals in the case of imaginary quadratic fields.

For an element $\alpha = a+b\sqrt{-n}$, the conjugate of α is $\bar{\alpha} = a-b\sqrt{-n}$ because they are the roots of the irreducible monic polynomial $x^2+2ax+(a^2+nb^2)$. Now when we consider an ideal $\mathfrak{a}$, the corresponding ideal $\widetilde{\mathfrak{a}} = \{\bar{\alpha}\colon \alpha \in \mathfrak{a}\}$, when multiplied by $\mathfrak{a}$, gives a principal ideal (d) for some positive integer d (Lemma 2.13 of [5]). It so happens that this number d is the norm of $\mathfrak{a}$. Notice that if d is a prime number, then $\mathfrak{a}$ is a prime ideal because it can only be factored into an ideal with norm equal to one (which could only be the ideal (1)) and another ideal of norm p ($\mathfrak{a}$ itself). With this in mind,

Proposition 10.1. *Fix n and let p be an odd prime number. Then the principal ideal (p) factors into prime ideals as follows:*

$$(p) = \begin{cases} (p) & \text{if } p \in P_{-1}^n \\ (p, a-\sqrt{-n}\,) \times (p, a+\sqrt{-n}\,) & \text{if } p \in P_1^n, \text{ where } a^2 \equiv -n \pmod{p} \\ (p, \sqrt{-n}\,)^2 & \text{if } p \in P_0^n \end{cases}$$

Proof. We begin with the P_1^n.

$$\begin{aligned} \left(p, a+\sqrt{-n}\right) \times \left(p, a-\sqrt{-n}\right) &= \left(p^2, ap+p\sqrt{-n}\,, ap-p\sqrt{-n}\,, a^2+n\right) \\ &= (p) \end{aligned}$$

(To see why this is the case, it helps to bear in mind that by assumption, $a^2+n \equiv 0 \pmod{p}$.)

We now need to show that these factors are prime ideals. One can check that each ideal is the set of conjugates of the other. From our foregoing discussion, this implies that both ideals have norm equal to p and that implies that they are prime.

The above procedure can then be used to prove the prime ideal factorization in the case where $p \in P_0^n$

For $p \in P_{-1}^n$, the norm of (p) will be p^2, thus we need to prove that (p) is prime by other means.

Now notice that (p) can only possibly be factored non-trivially by two ideals each of norm p. Suppose there exist such ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$. This means that there is an element $\alpha = a+b\sqrt{-n}$ which belongs in $\mathfrak{p}_1$ but not in (p). The fundamental theorem of prime ideals implies that because $(p) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ (by our assumption), we must have that $\mathfrak{p}_2 = \widetilde{\mathfrak{p}}_1$. Thus, $\bar{\alpha} = a-b\sqrt{-n} \in \mathfrak{p}_2$ and, what is more, $\alpha \cdot \bar{\alpha} = a^2+nb^2 \in (p)$

This means that a^2+nb^2, a rational integer, is divisible by p. In other words, $(ab^{-1})^2 \equiv -n \pmod{p}$. This contradicts the fact that $p \in P_{-1}^n$ and thus we can't have prime factors of (p) that have norm p. Thus the ideal (p) has to be prime. □

For the ideal (2), a similar method of proof shows that

$$(2) = \begin{cases} (2, 1+\sqrt{-n}\,)^2 & n \equiv 1 \pmod{4} \\ (2, \sqrt{-n}\,)^2 & n \equiv 2 \pmod{4} \\ (2) & n \equiv 3 \pmod{8} \\ (2, \sqrt{-n}\,) \cdot (2, 1+\sqrt{-n}\,) & n \equiv 7 \pmod{8}\text{, if } \mathcal{O}_{-n} = \mathbb{Z}[\sqrt{-n}\,] \end{cases}$$

Making use of this fact greatly complicates the equations we are about to see but does not change the argument we will make. The decomposition of (2) has therefore been omitted in what follows.

For an imaginary quadratic field, we can write equation (9.2) as

$$\zeta_{-n}(s) = \prod_{p \in P_{-1}^n} \frac{1}{1-p^{-2s}} \times \prod_{p \in P_1^n} \frac{1}{(1-p^{-s})^2} \times \prod_{p \in P_0^n} \frac{1}{1-p^{-s}}$$

Taylor expanding the terms of the product gives us

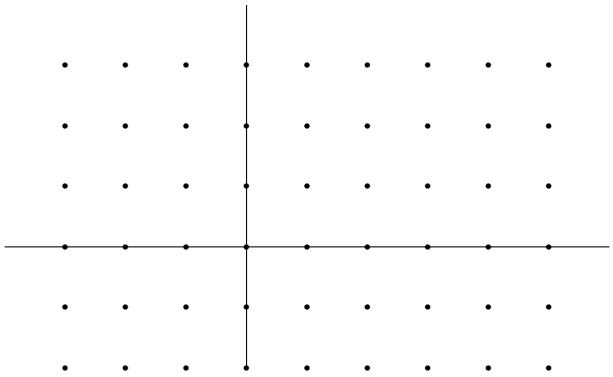
$$\zeta_{-n}(s) = \prod_{p \in P_{-1}^n} \sum_{j=0}^{\infty} \frac{1}{(p^{2j})^s} \times \prod_{p \in P_1^n} \sum_{j=0}^{\infty} \frac{j}{(p^{j-1})^s} \times \prod_{p \in P_0^n} \sum_{j=0}^{\infty} \frac{1}{(p^j)^s} \tag{10.2}$$

The thing to notice about this new form is that for each fraction $\frac{c}{(p^k)^s}$, the numerator c is the number of ideals in $\mathcal{O}_{-n}$ that have norm p^k. The number of ideals that have a norm m is a multiplicative function of m. That is, if m and m' are coprime, then $c_m \cdot c_{m'} = c_{mm'}$. To see this, look at the map that takes an ideal of norm m and an ideal of norm m' to their product and use the fundamental theorem of ideal theory to show that this map is bijective. When we expand (10.2), we thus get

$$\zeta_{-n}(s) = \sum_{m=0}^{\infty} \frac{c_m}{m^s} \tag{10.3}$$

where c_m is the number of ideals with norm m.

We now turn our attention to actually counting the number of ideals that have norm less than or equal to m. For two complex numbers α and β whose ratio is not a real number, a lattice $\langle \alpha, \beta \rangle$ is the set $\{a\alpha + b\beta \colon a, b \in \mathbb{Z}\}$. Visually, a lattice looks like a grid of points on the complex plane (in other words like a lattice). The lattice $\langle 1, \imath \rangle$ is shown below



It turns out that when the elements of an ideal are plotted on the complex plane, they produce the lattice $\langle m, a + b\sqrt{-n} \rangle$, where m is the smallest positive integer in the ideal and $a + b\sqrt{-n}$ has the smallest possible positive value of b (Lemma 3.5 of [5]). The lattice $\langle 1, \sqrt{-n} \rangle$ of the ideal (1) is what interests us (This is the form the lattice for (1) takes when $\mathcal{O}_{-n} = \mathbb{Z}[\sqrt{-n}]$). Because (1) contains every element in the ring of integers, each point $\alpha = r + q\sqrt{-n}$ in the lattice represents the principal ideal (α) and the square of the distance of that point from the origin

is the norm of the ideal $N(\alpha) = r^2 + nq^2$. Thus the problem of counting the number of principal ideals with norm less than or equal to M is actually about finding the number of points in the lattice $\langle 1, \sqrt{-n} \rangle$ that fall in the circle of radius $\sqrt{M}$ centred at the origin but with a slight complication. Because we have that $(\alpha) = (\text{unit of } \mathcal{O}_{-n} \times \alpha)$, the number of points in the circle is an overestimate of the number of principal ideals with norm less than or equal to M. To account for this, we have to divide the number of points that we count by the number of units in $\mathcal{O}_{-n}$ which we denote by ω.

A natural way to estimate the number of points of the lattice $\langle 1, \sqrt{-n} \rangle$ that fall within a circle of radius $\sqrt{M}$ centred at the origin is to calculate the area of the smallest rectangle in the lattice and divide the area of the circle by this. The area of the smallest rectangle in $\langle 1, \sqrt{-n} \rangle$ is $\sqrt{-n}$. Once we factor in the overestimate due to the number of units in the ring of integers, we can calculate how much our estimate of the number of principal ideals with norm less than or equal to M differs from the the actual number of principal ideals with norm less than or equal to M, $\mathrm{C}_M(\mathcal{C}_1)$. One such calculation yields

$$\left| \mathrm{C}_M(\mathcal{C}_1) - \frac{M\pi}{\omega\sqrt{-n}} \right| \leq k\sqrt{M} \quad \text{for some constant } k.$$

Remarkably, the above inequality also holds when we consider the number of ideals that have norm less than or equal to M and belong to a particular equivalence class of the ideal class group (Proposition 5.2 of [5]). Recalling that the class number h is finite, this implies that the number of ideals of $\mathbb{Z}[\sqrt{-n}]$ with norm less than or equal to M, C_M, satisfies the inequality

$$\left| \mathrm{C}_M - \frac{Mh\pi}{\omega\sqrt{-n}} \right| \leq K\sqrt{M} \quad \text{for some constant } K \tag{10.4}$$

It bears mentioning that the number of ideals with norm less than or equal to M is simply the sum of the number of ideals with norm $m \leq M$, that is

$$\mathrm{C}_M = \sum_{m=1}^{M} c_m$$

because the above inequality implies that

$$\left| \frac{\mathrm{C}_M}{M} \right| \leq \left(\frac{h\pi}{\omega\sqrt{-n}} + K \right)$$

Thus by Lemma 4.4, the series $\sum \frac{c_m}{m^s}$, which happens to be the Dedekind zeta function, converges for $\sigma > 1$.

The final step is to calculate the residue of the Dedekind zeta function at $s = 1$ in order to obtain the class number formula. For this we define the following function

$$f(s) = \sum_{m=1}^{\infty} \left(c_m + \frac{h\pi}{\omega\sqrt{-n}} \right) m^{-s}$$

The inequality (10.4) used in conjunction with Lemma 4.4 will show that $f(s)$ converges for all $\sigma > \frac{1}{2}$, which implies that it converges for $s = 1$.

Thus for some region around $s = 1$, we have that

$$\zeta_{-n}(s) = f(s) + \frac{h\pi}{\omega\sqrt{-n}}\zeta(s)$$

Thus applying Lemma 2.4 will show that

$$\lim_{s\to 1}(s-1)\zeta_{-n}(s) = \frac{h\pi}{\omega\sqrt{-n}}$$

This is the class number formula for imaginary quadratic fields for which $\mathcal{O}_{-n} = \mathbb{Z}[\sqrt{-n}]$.

For $\mathcal{O}_{-n} = \mathbb{Z}\left[\frac{1+\sqrt{-n}}{2}\right]$, the class number formula is

$$\lim_{s\to 1}(s-1)\zeta_{-n}(s) = \frac{2h\pi}{\omega\sqrt{-n}}$$

Acknowledgements. I would like to thank my mentor Drew Moore for the enormous time and effort he put into working with me during this REU. It would not have been possible to learn so much in so little time were it not for his valuable help and I cannot be thankful enough. That said, I should also thank him for allowing me to use the picture in Example 2.13. I would also like to express my gratitude to the director of the program, Professor Peter May, for providing the students in the program, myself included, with the opportunity to have such a valuable learning experience in mathematics.

References

[1] J-P Serre. A Course in Arithmetic. Graduate Texts in Mathematics 7. Springer-Verlag New York Inc 1973.

[2] Erich Hecke. Lectures on the Theory of Algebraic Numbers. Graduate Texts in Mathematics 77. Translated by George U. Brauer and Jay R. Goldman with the assistance of R. Kotzen. Springer-Verlag New-York Inc. 1981

[3] Keith Conrad. Ideal Factorization. http://www.math.uconn.edu/∼kconrad/blurbs/gradnumthy/idealfactor.pdf

[4] Serge Lang. Algebraic Number Theory (Second Edition). Graduate Texts in Mathematics 110. Springer-Verlag New York Inc, 1986

[5] Tom Weston. Lectures on the Dirichlet Class Number Formula for Imaginary Quadratic Fields.