AMERICAN UNIVERSITY OF BEIRUT

A PROOF OF THE CLASS NUMBER FORMULA

by

AMIR MONJED JABER CHEHAYEB

A thesis
submitted in partial fulfillment of the requirements
for the degree of Master of Science
to the Department of Mathematics
of the Faculty of Arts and Sciences
at the American University of Beirut

Beirut, Lebanon
April 2024

AMERICAN UNIVERSITY OF BEIRUT

A PROOF OF THE CLASS NUMBER FORMULA

by

AMIR MONJED JABER CHEHAYEB

Approved by:

Dr. Kamal Khuri Makdisi, Professor — Advisor
Mathematics

Dr. Wissam Raji, Professor — Member of Committee
Mathematics

Dr. Guiseppe Delle Sala, Associate Professor — Member of Committee
Mathematics

Date of thesis defense: April 15, 2024

Acknowledgements

I would like to thank Dr. Kamal Khuri-Makdisi for his contagious passion for math, and also for the exceptional patience and kindness he always maintains.

I would like to thank my friends for their daily encouragement and support.

I would like to thank Fayha Choir, Maestro Barkev Taslakian, and Dr. Edward Torikian for their contributions to Arabic A cappella music which has added so much light and purpose to my life as I completed this Master's degree.

Finally, I would like to thank my family - Mom, Dad, Rachel, and Daniel - whose hugs and love make life worth living.

Abstract
# of the Thesis of

Amir Monjed Jaber Chehayeb for Master of Science
Major: Mathematics

Title: A Proof of the Class Number Formula

The Class Number Formula helps compute several invariants of a number field, including its Class Number, by relating them to the behavior of its Dedekind Zeta function. The Class Number of a field is useful because it helps determine the extent to which unique factorization fails in the associated number ring. A proof of the general Class Number Formula is presented and a more refined version is computed for the real quadratic case.

Table of Contents

Illustrations

Chapter 1

Introduction

The existence of unique prime factorization for integers is an invaluable tool that underpins a lot of the common applications of math. Any positive integer can be uniquely expressed as a product of primes.

This doesn't hold true in broader mathematical settings. Even with some notion of indecomposable prime-like elements, we can still have distinct factorizations for the same element. For instance, in the ring $\mathbb{Z}[\sqrt{10}]$, we have two distinct factorizations of 6 despite all factors below being "irreducible"

$$6 = 2 \times 3 \quad ; \quad 6 = (4 + \sqrt{10})(4 - \sqrt{10})$$

Fortunately, some notion of unique factorization can still be established via subsets of rings called ideals.

In chapter 2, we concretely define the mathematical space we'll be working in to be the number ring associated with finite extensions of $\mathbb{Q}$ known as number fields. Then, we introduce important notions and study the additive structure of the ring.

In chapter 3, we will develop the notion of ideal classes and introduce the ideal class group. We explain unique factorization into prime ideals in Dedekind domains and show that number rings are indeed Dedekind domains. We then explore the splitting of primes in quadratic fields and conclude by proving that the ideal class group is finite. We call its order the class number.

In Chapter 4, we study the distribution of ideals in ideal classes for real quadratic number fields, and then for number fields in general.

In Chapter 5, we define the Dedekind Zeta function of a number field, and relate its behavior to several invariants of the number field including the Class number. This yields the Class number formula. We introduce characters of abelian groups and L-sries, then use them to compute a more refined form in the case of real quadratic number fields.

Chapter 2

Number Rings

We define a *number field* to be a subfield of $\mathbb{C}$ having finite dimension as a vector space over $\mathbb{Q}$. For instance, given any square-free positive integer m, the set

$$\mathbb{Q}\left[\sqrt{m}\,\right] = \{a + b\sqrt{m}\ \left| a, b \in \mathbb{Q}\right\}$$

is a vector space of dimension 2 over $\mathbb{Q}$ having basis $\{1, \sqrt{m}\}$. We call it a *real quadratic field.* More generally, if α is a root of some monic degree n polynomial $f \in \mathbb{Q}[x]$ which is irreducible over $\mathbb{Q}$, then $K = \mathbb{Q}[\alpha]$ is the $\mathbb{Q}$-vector space with basis $\{1, \alpha, \cdots, \alpha^{n-1}\}$. We call f the *minimal polynomial* of α, and denote by $[K : \mathbb{Q}] = n$ the index of $\mathbb{Q}[\alpha]$ which coincides with its dimension and the degree of f.

2.1 Embeddings

Conjugates are numbers that share the same minimal polynomial over $\mathbb{Q}$. Conjugates are vital in the study of *embeddings* - injective homomorphisms of K which restrict to the identity on $\mathbb{Q}$. Suppose σ is an embedding, then by the above definition

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$$

Therefore, an embedding must map an element to one of its conjugates. Hence, noting that an embedding of $Q[\alpha]$ is entirely defined by how it maps α, we deduce that there are exactly n embeddings corresponding to the n conjugates of α.

In more general settings, given number fields $K \subset L$, we can view L as a vector space over K whose dimension we define as the *index* of L over $K = [L : K]$. For $\alpha \in L$, the minimal polynomial of α is defined as the monic irreducible polynomial $f \in K[x]$ having α as a root. Embeddings of L can be constructed from those of K. In fact,

Proposition 2.1. Every embedding of K in $\mathbb{C}$ extends to exactly $[L : K]$ embeddings of L.

Proof. We argue by induction on the index. It's trivially true for $[L : K] = 1$ in which case $L = K$. Otherwise, assume the statement holds for subfields whose index is smaller than $[L : K]$. Suppose σ is an embedding of K in $\mathbb{C}$.

Then, fix $\alpha \in L \setminus K$, and denote by f its minimal polynomial over K. Let g be the polynomial constructed by applying σ to the coefficients of f. Note that g must be irreducible over σK. Otherwise, applying the reverse of the above construction (embeddings are injective) on its factors would yield that f is reducible. For each root β of g, the map $K[\alpha] \to \sigma K[\beta]$ that maps α to β and mimics σ on K is an isomorphism and thus an embedding of $K[\alpha]$. Then, noting that the degree of $f =$ degree of $g = [K[\alpha] : K]$, we get $[K[\alpha] : K]$ such embeddings.

Finally, since $[L : K[\alpha]] < [L : K]$, each of those embeddings extends to $[L : K[\alpha]]$ embeddings of L by the inductive hypothesis. This yields $[L : K[\alpha]] \cdot [K[\alpha] : K] = [L : K]$ embedding extensions of σ as required. □

A similar approach helps us characterize finite fields.

Proposition 2.2. Given K and L as before, $L = K[\alpha]$ for some α.

Proof. If $[L : K] = 1$, $L = K$ so it's true. Otherwise, assume the statement holds for indices smaller than $[L : K]$. Then, fix $\alpha \in L \setminus K$. By the inductive hypothesis, since $[L : K[\alpha]] < [L : K]$, we have $L = K[\alpha][\beta] = K[\alpha, \beta]$ for some β.

Consider $K[\alpha + c\beta]$ for $c \in K$. If it is not equal to L, then $\alpha + c\beta$ must have fewer than $[L : K]$ conjugates. But, we know that the identity on K extends to $[L : K]$ embeddings of L. Recall that embeddings must map an element to its conjugates. Therefore, we deduce that at least two of those embeddings of L that fix K point-wise, σ_1 and σ_2, must map $\alpha + c\beta$ to the same conjugate. Then,

$$\sigma_1(\alpha + c\beta) = \sigma_2(\alpha + c\beta) \implies c = \frac{\sigma_1(\alpha) - \sigma_2(\alpha)}{\sigma_1(\beta) - \sigma_2(\beta)}$$

Note that the denominator is not 0 since if the embeddings agree on β, then they also agree on α by the first equation, rendering them the same embedding. Therefore, only finitely many c satisfy our assumption that $K[\alpha+c\beta] \neq L$. But K has infinitely many elements, which completes our proof. □

2.2 Integrality

Definition 2.3. An **algebraic integer** is a complex number if is the root of a monic polynomial is in $\mathbb{Z}[x]$.

We denote the set of algebraic integers by $\mathbb{A}$. We also note that the definition above is equivalent to saying that the minimal polynomial of α is monic in $\mathbb{Z}[x]$ due to the following proposition.

Proposition 2.4. Suppose $\alpha \in \mathbb{A}$, and let f be the monic polynomial of lowest degree in $\mathbb{Z}[x]$ that admits α as a root. Then, f is irreducible over $\mathbb{Q}$, making it the minimal polynomial of α.

We admit the following version of Gauss' lemma. (Marcus [1], p.10)

Lemma 2.5. If $f = gh$, where f is monic in $\mathbb{Z}[x]$ and g, h are monic in $\mathbb{Q}[x]$, then g, h are in fact in $\mathbb{Z}[x]$.

Proof. (of proposition) If f were reducible over $\mathbb{Q}$, then write $f = gh$ where both g, h are monic. By the lemma, it follows that g and h are actually in $\mathbb{Z}[x]$. At least one of them admits α as a root, and this leads to a contradiction since they're both of a smaller degree than f. □

Given a number field K, we denote by $\mathbb{A}_K = \mathbb{A} \cap K$ the set of algebraic integers contained in K. We call $\mathbb{A}_K$ the *number ring* associated with the number field K. Clearly, $A_{\mathbb{Q}} = \mathbb{Z}$. (The minimal polynomial of a/b is $bx - a$ which is only monic if $b = 1$.) Number rings are in fact rings. Before we prove it, we develop equivalent charachterizations for integrality.

Proposition 2.6. $\alpha \in \mathbb{A} \Leftrightarrow \alpha G \subset G$ for some finitely generated additive subgroup $G \subset \mathbb{C}$.

Proof. The forward direction is straightforward. If α is a root of a monic polynomial of degree n over $\mathbb{Z}$, then all powers of α having degree n or higher can be expressed as a $\mathbb{Z} - linear$ combination of $1, \alpha, \cdots, \alpha^{n-1}$. Therefore, taking G to be $\mathbb{Z}[\alpha]$ which is finitely generated completes the argument.

For the reverse direction, suppose G is generated by $a_1, \cdots, a_n$. Then, expressing αa_i as a combination of the generators yields

$$\begin{pmatrix} \alpha a_1 \\ \vdots \\ \alpha a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

for some matrix $M \in \mathbb{M}_n(\mathbb{Z})$. Then, since the a_i's are not all zero, α is an eigenvalue of M. Therefore, it's a root of the determinant of $|\lambda I - M|$ which is a monic polynomial of degree n over $\mathbb{Z}$, completing the proof. □

Corollary 2.7. Number rings are multiplicative rings.

Proof. It suffices to show that $\mathbb{A}$ is a ring. Given $\alpha, \beta \in \mathbb{A}$, we know that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated. Suppose $\{\alpha_1, \cdots, \alpha_s\}$ generates $\mathbb{Z}[\alpha]$ and $\{\beta_1, \cdots, \beta_r\}$ generates $\mathbb{Z}[\beta]$. Then, $\mathbb{Z}[\alpha, \beta]$ which we can view as $\mathbb{Z}[\alpha][\beta]$ is generated by $\{\alpha_i\beta_j \big| 1 \leq i \leq s, 1 \leq j \leq r\}$. Since it contains $\alpha\beta$ and $\alpha + \beta$, we deduce that they are in $\mathbb{A}$. □

2.3 Trace, Norm, and Discriminant

Our goal for the remaining of the chapter is to study the structure of the number ring. We introduce two important maps that encode important information about elements within a number field.

Definition 2.8. Given number fields $K \subset L$, we define the relative trace and relative norm of $\alpha \in L$ as

$$\begin{aligned} T_K^L : K &\to \mathbb{C} & \qquad N^K : K &\to \mathbb{C} \\ \alpha &\mapsto T_K^L(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) & \qquad \alpha &\mapsto N^K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \end{aligned}$$

where σ_i are the $n = [L : K]$ embeddings of L which fix K point-wise.

Properties 2.9. We note a few remarks and important properties.

(1) Since the embeddings are ring homomorphisms, then the trace and norm inherit their homomorphism properties. Namely, the trace is an additive homomorphism, and the norm is a multiplicative homomorphism. So, for $\alpha, \beta \in L$,

$$T_K^L(\alpha + \beta) = T_K^L(\alpha) + T_K^L(\beta) \quad ; \quad N_K^L(\alpha\beta) = N_K^L(\alpha)N_K^L(\beta)$$

Recalling that the embeddings fix K point-wise, it follows that for $\delta \in K$,

$$T_K^L(\delta) = n\delta \qquad N_K^L(\delta) = \delta^n \qquad T_K^L(\delta\alpha) = \delta T_K^L(\alpha) \qquad N_K^L(\delta\alpha) = \delta^n N_K^L(\alpha)$$

(2) Given $\alpha \in L$ such that $[K[\alpha] : K] = d$. Then, since each embedding of $K[\alpha]$, extends to exactly n/d embeddings of L, we deduce that

$$T_K^L(\alpha) = \frac{n}{d} T_K^{K[\alpha]} \qquad\qquad N_K^L(\alpha) = \left(N_K^{K[\alpha]}\right)^{n/d}$$

Moreover, we know that the images of α under the embeddings of $K[\alpha]$ constitute exactly all its conjugates over K. Then, noting that those conjugates of α are all the roots of its monic minimal polynomial $f \in K[x]$, we deduce that $T_K^{K[\alpha]}$ and $N_K^{K[\alpha]}$ are the second coefficient and the constant term of f respectively.

(3) By the argument above, since $n/d = [L : K[\alpha]] \in \mathbb{Z}$, it follows that $T_K^L(\alpha), N_K^L(\alpha) \in K$. Also, if $\alpha \in \mathbb{A}$, then $f \in \mathbb{Z}[x]$. Therefore, its relative trace and norm are integers.

(4) When we are working with only one number field K over $\mathbb{Q}$, we simply refer to the maps above as the trace and norm. Moreover, for $\alpha \in K$, we assume the

context is clear and denote

$$T(\alpha) = T_{\mathbb{Q}}^{K}(\alpha) \quad ; \quad N(\alpha) = N_{\mathbb{Q}}^{K}(\alpha) \qquad\qquad (\text{both} \in \mathbb{Q})$$

(5) Finally, when we are working with more than two number fields, $K \subset L \subset M$, then for $\alpha \in M$, we have transitivity - meaning

$$T_L^K(T_L^M(\alpha)) = T_K^M(\alpha) \qquad\qquad N_L^K(N_L^M(\alpha)) = N_K^M(\alpha)$$

We admit this without proof.(Jacobson [2], p. 426). It requires composing the embeddings of L fixing K with those of M fixing L in a suitable context, and then verifying that the compositions yield the correct number of distinct embeddings corresponding to those of M over K.

The trace is closely associated with an the discriminant, an essential tool is that defined over n-tuples.

Definition 2.10. Given K of degree n over $\mathbb{Q}$, and $\alpha_1, \cdots, \alpha_n \in K$, we define their discriminant to be the square of the determinant of the matrix whose entries are given by $\sigma_i(\alpha_j)$ (where i indexes the rows and j indexes the columns).

$$\text{disc}(\alpha_1, \cdots, \alpha_j) = |\sigma_i(\alpha_j)|^2 = \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & & \sigma_n(\alpha_n) \end{vmatrix}^2$$

Switching the indexing would yield the same determinant. This allows us to relate the determinant to the trace

$$\text{disc}(\alpha_1, \cdots, \alpha_n) = |\sigma_i(\alpha_j)|\,|\sigma_j(\alpha_i)| = \left|\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right| = |T(\alpha_i\alpha_j)|$$

By similar reasoning to property (3) in 2.9, it follows that the $\operatorname{disc}(\alpha_1, \cdots, \alpha_n) \in \mathbb{Q}$. Moreover, if all $\alpha_i \in \mathbb{A}$, then so are their products. Therefore, all elements of the matrix of traces are integers yielding an integer discriminant.

The relation above also allows us to observe that the discriminant characterizes linear independence, in a fashion similar to the determinant.

Proposition 2.11. $\operatorname{disc}(\alpha_1, \cdots, \alpha_n) = 0$ if and only if $\{\alpha_1, \cdots, \alpha_n\}$ is linearly dependent over $\mathbb{Q}$.

Proof. The backward direction is trivial. Any linear dependence of the $\alpha_i's$ can be translated into linear dependence between the columns since the embeddings are additive homomorphisms. It follows that the determinant is 0.

On the other hand, assume the discriminant is 0. Then, the rows of the trace matrix $[T(\alpha_i\alpha_j)]$ are linearly dependent, so we may write $a_1R_1 + \cdots + a_nR_n = 0$ for rational numbers $a_i \in \mathbb{Q}$ that are not all 0. Then, for $1 \leq j \leq n$, jth component of the sum above can be expressed as

$$0 = \sum_{i=1}^{n} a_i T(\alpha_i \alpha_i) = T\left(\alpha_j \cdot \sum_{i=1}^{n} a_1 \alpha_i\right) = T(\alpha_j \alpha) \qquad \text{where } \alpha = \sum_{i=1}^{n} a_1 \alpha_i$$

Suppose the set $\{\alpha_i\}$ were linearly independent. Then, it forms a basis for K over $\mathbb{Q}$ and $\alpha \neq 0$. It follows that the set $\{\alpha\alpha_i\}$ is also a basis. Therefore, the trace map must be identically 0 since it's additive and 0 on a basis. This is a contradiction since $T(1) = n$. Hence, $\{\alpha_i\}$ must be linearly dependent. □

2.4 The Structure of a Number Ring

In the final section, we will use the discriminant to study the structure of number rings. More precisely, we will prove the following theorem.

Theorem 2.12. Given a number field K of degree n over Q, and R the corresponding number ring $\mathbb{A} \cap K$. Then, R is a free abelian group of rank n.

In other words, we'll show that that R has an *integral basis* over $\mathbb{Z}$ consisting of n elements $\beta_1, \cdots, \beta_n \in R$ such that for every $\alpha \in \mathbb{R}$, there exists unique integers $m_1, \cdots, m_n$ with

$$\alpha = m_1\beta_1 + \cdots + m_n\beta_n$$

Proof. The proof relies on the following key algebraic result. (Jacobson [2], p. 179)

Proposition 2.13 (Nielsen-Schreier Theorem)**.** A subgroup of a free abelian group of rank n is also a free abelian group of rank $m \leq n$

We will construct two free abelian groups A and B of rank n such that $A \subset R \subset B$. Then, since R is an additive group, the proposition above shows that it must be free abelian of rank n - completing the proof.

<u>Construction of A:</u> We will find a basis for K over $\mathbb{Q}$ consisting of algebraic integers. This is straightforward due to the following lemma.

Lemma 2.14. For each $\alpha \in K$, there exists $m \in \mathbb{Z}$ such that $m\alpha \in \mathbb{A}$.

Proof. (of lemma) Since $\alpha \in K$, it has finite degree $k \leq n$ over $\mathbb{Q}$. Then, suppose

$$f = x^k + \frac{a_1}{b_1}x^{k-1} + \cdots + \frac{a_k}{b_k} \qquad a_i \in \mathbb{Z}, b_i \in \mathbb{Z} \setminus 0$$

is the minimal polynomial of α. Letting $b = b_1 b_2 \cdots b_k$ and $c_i = b/b_i \in \mathbb{Z}$, we get

$$\begin{aligned} 0 = f(\alpha) = b^k f(\alpha) &= b^k \alpha^k + b^{k-1}\frac{ba_1}{b_1}\alpha^{k-1} + \cdots + b^k \frac{a_k}{b_k} \\ &= (b\alpha)^k + a_1 c_1 (b\alpha)^{k-1} + \cdots + b^{k-1} c_k a_k = g(b\alpha) \end{aligned}$$

where

$$g(x) = x^k + \sum_{i=1}^{k-1} a_i c_i b^{i-1} x^{k-1} \in \mathbb{Z}[x]$$

Therefore, $b\alpha \in \mathbb{A}$. □

Applying the lemma on a basis for K over $\mathbb{Q}$ yields a new basis $\{\alpha_1, \cdots, \alpha_n\} \subset R$. We take A to be the free group of rank n generated by this basis.

$$A = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n \subset R$$

<u>Construction of B:</u> Take $\{\alpha_1, \cdots, \alpha_n\} \subset R$ a basis for K over $\mathbb{Q}$ like above, and let $d = \mathrm{disc}(\alpha_1, \cdots, \alpha_n)(\neq 0)$. We will show that $R \subset B = \frac{1}{d}A$. Given $\alpha \in R$, we may write

$$\alpha = q_1\alpha_1 + \cdots + q_n\alpha_n \qquad\qquad q_i \in \mathbb{Q}$$

Applying each of the embeddings of K to the equation above yields a system of n equations

$$\sigma_i(\alpha) = q_1\sigma_i(\alpha_1) + \cdots + q_n\sigma_i(\alpha_n) \qquad\qquad 1 \leq i \leq n$$

Using Cramer's rule to solve the system

$$b = [\sigma_i(\alpha)] = [\sigma_i(\alpha_j)][q_j] = M[q_j]$$

we get that $q_j = |M_j|/|M|$ where M_j is obtained from M by replacing the j-th column by b.

Note that the matrices M and M_j have entries in $\mathbb{A}$, and hence their determinants must also be algebraic integers. Moreover, noting that $|M|^2 = d$, we get that the rational number $m_j \coloneqq dq_j = |M||M_j| \in \mathbb{A}$. Therefore, $m_j \in \mathbb{A}_{\mathbb{Q}} = \mathbb{Z}$. Putting it together, we deduce

$$\alpha = \frac{m_1}{d}\alpha_1 + \cdots + \frac{m_n}{d}\alpha_n \subset \frac{1}{d}A$$

As required, the latter is an abelian group of rank n having basis $\{\alpha_1/d, \cdots, \alpha_n/d\}$.

□

The theorem above shows that R has an integral basis. But, it is not unique. For instance, if $\{\beta_1, \cdots \beta_n\}$ is an integral basis, then so are $\{\beta_1, \cdots, \beta_n + \beta_1\}$ and similar $\mathbb{Z}$-linear combinations. However, it turns out that their discriminants are equal.

Proposition 2.15. If $\{\beta_1, \cdots, \beta_n\}$ and $\{\delta_1, \cdots, \delta_n\}$ are both an integral basis for a number ring R, then $\operatorname{disc}(\beta_1, \cdots, \beta_n) = \operatorname{disc}(\delta_1, \cdots, \delta_n)$.

Proof. For $1 \leq i \leq n$, since $\delta_i \in R$, we may write it as a $\mathbb{Z}$-linear combination of the β's. Therefore, we have

$$\begin{pmatrix} \delta_1 \\ \vdots \\ \delta_n \end{pmatrix} = M \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

for some integer square matrix M. Applying each of the n embeddings $\{\sigma_j\}$ to the n equations above yields

$$[\sigma_j(\delta_i)] = \begin{pmatrix} \sigma_1(\delta_1) & \cdots & \sigma_n(\delta_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\delta_n) & \cdots & \sigma_n(\delta_n) \end{pmatrix} = M \begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_n(\beta_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \cdots & \sigma_n(\beta_n) \end{pmatrix} = [\sigma_j(\beta_i)]$$

Then, taking the square of their determinants, we obtain

$$\mathrm{disc}(\beta_1, \cdots, \beta_n) = |M|^2 \mathrm{disc}(\delta_1, \cdots, \delta_n)$$

Applying the same process in reverse, expressing the β's in terms of the δ's, results in an analogous equation for some different integer matrix N.

$$\mathrm{disc}(\delta_1, \cdots, \delta_n) = |N|^2 \mathrm{disc}(\beta_1, \cdots, \beta_n) = |N|^2|M|^2 \mathrm{disc}(\delta_1, \cdots, \delta_n)$$

Since M, N have entries in $\mathbb{Z}$, then $|N|, |M|$ are both positive integers with $|N|^2|M|^2 = 1$. It follows that $|N| = |M| = 1$ which completes our proof. □

The proposition above shows that the discriminant is actually an invariant of the number ring R. We denote it by $\mathrm{disc}(K)$ or $\mathrm{disc}(R)$ where $R = \mathbb{A}_K$.

We conclude by computing the discriminant of number rings associated with the real quadratic fields we defined at the beginning of the chapter.

Proposition 2.16. For squarefree $d > 0$, $K = \mathbb{Q}[\sqrt{d}]$,

$$\mathrm{disc}(\mathbb{A}_K) = \begin{cases} 4d & d \equiv 2, 3 \mod 4 \\ d & d \equiv 1 \mod 4 \end{cases}$$

Note that the proposition is true for all $d \in \mathbb{Z}$, but we will be working mainly with the case of real quadratic fields.

Proof. The minimal polynomial of $\alpha = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ is $x^2 - 2ax + (a^2 - db^2)$. For α to be an integer, we must have

$$\begin{cases} r = 2a \in \mathbb{Z} \\ a^2 - db^2 = \frac{r^2}{4} - db^2 \in \mathbb{Z} \Leftrightarrow r^2 - 4db^2 \equiv 0 \mod 4 \end{cases}$$

If r is even ($a \in \mathbb{Z}$), then $db^2 \in \mathbb{Z}$, which implies $b \in \mathbb{Z}$ since d is squarefree. Otherwise, if r is odd ($a \in \mathbb{Z}/2$), then $4b^2d \equiv 1 \mod 4$, so $2b$ must also be an odd integer, and hence $d \equiv 1 \mod 4$. Putting it together, we get

$$\mathbb{A}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \mod 4 \end{cases}$$

It follows that an integral basis for $\mathbb{A}_K$ would be

$$\begin{cases} \{1, \sqrt{d}\} & d \equiv 2,3 \mod 4 \\ \{1, \frac{1+\sqrt{d}}{2}\} & d \equiv 1 \mod 4 \end{cases}$$

Then, noting that the 2 embeddings of K aregiven by

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d} \qquad\qquad \sigma_1(a + b\sqrt{d}) = a - b\sqrt{d}$$

We deduce that

$$\operatorname{disc}(\mathbb{A}_K) = \begin{cases} \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d & d \equiv 2,3 \mod 4 \\ \\ \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = (-\sqrt{d})^2 = d & d \equiv 1 \mod 4 \end{cases}$$

□

Chapter 3

Ideal Class Group and Prime Decomposition

The simplest examples of number rings are $\mathbb{Z}$ and $\mathbb{Z}[i]$. Both of those rings are unique factorization domains. Each element can be uniquely expressed as a product of irreducibles (elements which can only be factored further via units). In general, as seen in the introduction, this is not true of all number rings. However, all number rings do admit unique factorization into prime ideals.

In this chapter, we will define ideal multiplication and the ideal class group. We'll then show that number rings are so-called Dedekind domains which admit factorization into prime ideals. Finally, we'll explore the splitting of primes, and develop tools which we use to show that the ideal class group is finite.

3.1 Ideal Class Group and Dedekind Domains

Let R be a domain, given ideals $I, J \subset R$ we define their product

$$IJ = \left\{ \sum_{k=1}^{n} i_k j_k \quad \middle| \quad i_k \in I, j_k \in J, k \in \mathbb{N} \right\}$$

It is easy to see that IJ is an ideal. For $\alpha \in R$, we denote by $(\alpha) = \alpha R$ the principal ideal generated by α. We also define an equivalence relation on the set of ideals of R given by

$$I \sim J \text{ iff } \alpha I = \beta J \text{ for some non-zero } \alpha, \beta \in R$$

It is clear that this is a well-defied equivalence relation on the set of ideals. We call the equivalence classes ideal classes and denote them by $[I]$. Moreover, it is easy to see that all principal ideals $(\alpha) = \alpha R = \alpha(1)$ are equivalent to the identity. Hence, the set of all ideals classes, $\mathcal{C}$, is a monoid whose identity element is the class of all principal ideals, [1].

As we shall see, when working with number rings, the monoid $\mathcal{C}$ is in fact a group. We will prove this for more general settings, known as Dedekind domains, which include number rings. Then, we will prove that ideal multiplication does in fact lead to unique factorization into prime ideals - which we recall are ideals I such that $ab \in I$ only if at least one of a or $b \in I$.

Definition 3.1. A *Dedekind domain* R is an integral domain satisfying

i. Every ideal in R is finitely generated. Equivalently, R is *Noetherian:* every ascending chain of ideals eventually becomes stationary.

ii. Every non-zero prime ideal is a maximal ideal : an ideal that is not contained in any other ideals besides R itself.

iii. Let K be the field of fractions of $R = \{\alpha/\beta \,|\alpha, \beta \in R,\ \beta \neq 0\}$ Then, we require that R be *integrally closed* in K: $\alpha/\beta \in K$ is a root of a monic $f \in R[x]$ only if $\alpha/\beta \in R$.

We verify that number rings are Dedekind domains.

Theorem 3.2. Given a number field K such that $[K : \mathbb{Q}] = n$, then the corresponding number ring $R = \mathbb{A} \cap K$ is a Dedekind domain.

Proof. i. We have already seen in theorem 2.12 that R is a free abelian group of rank n. Then, an ideal $I \subset R$ is an additive subgroup of R. So, it follows by proposition 2.13 that I is free abelian group of rank $\leq n$. Therefore, it's finitely generated. In fact, for any non-zero $\alpha \in I, (\alpha) \subset I$ has rank n, so I has rank exactly n.

ii. We claim that R/I is finite for any ideal I. Fix a non-zero $\alpha \in I$, then $m = N^K(\alpha)$ is a non-zero integer by (3) in 2.9. We know that $m = \alpha \cdot \beta$ where β is the product of all conjugates of α. So, $\beta = m/\alpha \in R$, and therefore $m \in (\alpha) \subset I$. Therefore, $|R/I| \subset |R/(m)|$ which is finite of order m^n (it looks like $\mathbb{Z}\alpha_1/m\mathbb{Z} \times \cdots \times \mathbb{Z}\alpha_n/m\mathbb{Z}$ for some generators $\alpha_1, \cdots, \alpha_n$ which is a product of cyclic groups of order m).

If I is a prime ideal, it follows that R/I is an integral domain. But, finite integral domains are fields. Therefore, I is a maximal ideal since R/I is a field.

iii. Assume $\alpha \in \mathbb{C}$ is the root of a monic polynomial $f = x^n + a_1x^{n-1} + \cdots + a_n \in R[x]$. For $1 \leq i \leq n$, we know that $a_i \in \mathbb{A}$, then let d_i be the degree of f_i, the minimal polynomial of a_i. Consider the set

$$H = \left\{\alpha^m \cdot a_1^{m_1} \cdots a_n^{m_n} \middle| 0 \leq m < n, 0 \leq m_i < d_i\right\}$$

We claim that H generates $G = \mathbb{Z}[a_1, \cdots, a_n, \alpha]$. Given an element $a_1^{c_1} \cdots a_n^{c_n}\alpha^c \in G$, then if $c \geq n$ or $c_i \geq d_i$, we may use the linear combination induced by the minimal polynomials f and f_i to express our element as a linear combination of elements of with smaller exponents. Eventually, this becomes a linear combination of elements of H. It follows that G has a finitely generated additive subgroup. And clearly, $\alpha G \subset G$, therefore $\alpha \in \mathbb{A}$ by proposition 2.6. Applying this to any α in the field of fractions of R proves that R is integrally closed.

□

We admit the following lemma concerning Dedekind domains. (Marcus [1], pg. 40)

Lemma 3.3. Let A be a proper ideal in R. Then, there exists $\gamma \in K \setminus R$ such that $\gamma A \subset R$.

Theorem 3.4. If R is a Dedekind domain, then the set of its ideal classes $\mathcal{C}$ is a group, which we call the ideal class group.

Proof. We only need to prove that every class $[I]$ has an inverse. Therefore, it suffices to find an ideal J such that IJ is principal ($\in [1]$). Fix a non-zero $\alpha \in I$ and consider

$$J = \{\beta \in R \big| \beta I \subset (\alpha)\}$$

J is an ideal, and $\alpha \in J$ ensures that J is non-zero. By definition, $IJ \subset (\alpha)$. We want to prove the reverse inclusion. To that end, we construct $A = \frac{1}{\alpha} IJ$. It is clear that A is an ideal. Moreover, $J \subset A$ since I contains α, so every $\beta \in J$ can be expressed as $\frac{1}{\alpha}\alpha\beta \in A$.

Assume $A \neq R$, then we may apply the lemma above to obtain $\gamma \in K \setminus R$ such that $\gamma A \subset R$. Then, for every $\beta \in J$, we have

$$\begin{cases} \gamma\beta \in \gamma J \subset \gamma A \subset R \\ \frac{\gamma\beta}{\alpha} I = \gamma \frac{1}{\alpha}\beta I \subset \gamma A \subset R \implies \gamma\beta I \subset (\alpha) \end{cases} \implies \gamma\beta \in J$$

This shows that $\gamma J \subset J$. Then, recalling that J is finitely generated since R is a

Dedekind domain, we may fix a set of generators of $J, \{\beta_1, \cdots, \beta_n\}$. So, we get

$$\gamma \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = M \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

where $M \in M_n(R)$. It follows that γ is an eigenvalue of M whose determinant is a monic polynomial $R[x]$. This is a contradiction since R is integrally closed and $\gamma \notin R$. Therefore, $A = R$ which implies $IJ = (\alpha)$ as desired. □

The result above allows us to establish three key properties of ideals that we shall use to prove unique factorization.

Corollary 3.5. Given ideals A, B, C in a Dedekind domain R, then

(a) $AB = BC \implies B = C$

(b) $A \big| B \Leftrightarrow B \subset A$

(c) Every proper ideal is contained in some maximal ideal $\neq R$.

Proof. (a) By the theorem , there exists an ideal J such that $AJ = (\alpha)$ for some α. Then, multiplying by J yields $(\alpha)B = (\alpha)C$ which is the same as $\alpha B = \alpha C$. Recalling that Dedekind domains are integral domains, it follows that $B = C$.

(b) We define $A\big|B$ to mean that $B = AC$ for some ideal C. Since $AC \subset A$ it follows that $B \subset A$. On the other hand, assume that $B \subset A$, then choose an ideal J such that $AJ = (\alpha)$. Consider the ideal $C = \frac{1}{\alpha}JB \subset \frac{1}{\alpha}JA \subset R$. We have $AC = \frac{1}{\alpha}AJB = \frac{1}{\alpha}(\alpha)B = B$, so $A\big|B$.

(c) Let I be a proper ideal. If I is not maximal, then $I \subsetneq I_1 \subsetneq R$. Iterating, we get an ascending chain of ideals which must become stationary since R is Noetherian.

□

We can now prove

Theorem 3.6. In a Dedekind domain R, every proper ideal is uniquely representable as a product of prime ideals.

Proof. **Existence:**

First, we prove that such a representation exists. Let $S = \bigcup_{\alpha \in A} I_\alpha$, be the set containing proper ideals which can not be written as a product of prime ideals. We want to show S is empty.

If S were not empty, then it must have a maximal element M that is not contained in any other element of S. Otherwise, we may construct a strictly ascending chain of ideals which is not possible in Dedekind domains.

Then, by (C) above, M is contained in some maximal ideal $P \neq R$. Hence, since maximal ideals are prime, we deduce that $M = IP$ for some ideal I by (b) above. Then, $M \subsetneq I$ (if $M = I$, then $M = RM = PM \implies R = P$ by (a) above). Therefore, $I \notin S$ since M is maximal. But this leads to a contradiction since it implies that I factors into a product of primes, and $M = PI$ would factor as well.

Uniqueness:

Suppose $P_1 \cdots P_s = Q_1 \cdots Q_r$ where the P_i, Q_i are primes. Then, $Q_1 \cdots Q_s \subset P_1$ by (2) above. If none of the Q_i were contained in P, then choosing $a_i \in Q_i \setminus P$ for each i would yield a product $a_1 \cdots a_s \in P$ whose factors are all not in P. This contradicts the fact that P is prime. So, asume $Q_1 \subset P_1$ without loss of generality. Then, since prime ideals are maximal in Dedekind domains, we conclude that $Q_1 = P_1$. Using (1) above, we may cancel them to get $P_2 \cdots P_s = Q_2 \cdots Q_r$. Proceeding as such, we deduce that $r = s$, and that the factors are identical. □

3.2 Splitting of Primes

From hereon, we use primes to refer to prime ideals. Primes in $\mathbb{Z}$ may not be prime in larger number rings. For example, $(2) = (2, 1+\sqrt{-5})^2$ in $\mathbb{Z}[\sqrt{-5}]$. We say $(2) \subset \mathbb{Z}$ splits into the square of the prime ideal $(2, 1+\sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$ lying over (2).

Given number fields $K \subset L$, and their corresponding number rings $R = \mathbb{A}_K \subset S = \mathbb{A}_L$, we will study how the ideal generated by primes P in S splits in S.

Definition 3.7. Let P be a prime of R, and Q a prime of S. Then, Q lies over P or P lies under Q if any of the following equivalent conditions hold.

$$Q \mid PS \overset{\text{by } 3.5}{\iff} PS \subset Q \overset{Q \text{ ideal in } S}{\iff} P \subset Q \iff Q \cap R = P \overset{\mathbb{A} \cap Q = Q}{\iff} Q \cap K = P$$

The third implication holds since P, being prime, is maximal. It is contained in $Q \cap R \neq R$ since $1 \notin Q$. Therefore, $Q \cap R = P$. The equivalence of conditoins allows us to easily prove the following.

Proposition 3.8. Every prime P of R lies under at least one prime Q of S. On the other hand, every prime Q of S lies over a unique prime P of R.

Proof. For the first part, it suffices to show that $PS \neq S$. It will follow that PS has at least one prime divisor Q which lies over P. By lemma 3.3, since P is a proper ideal in R, there exists $\gamma \in K \setminus R$ such that $\gamma P \subset R$. If $1 \in PS$, then $\gamma = \gamma 1 \in \gamma PS \subset RS = S$ is a contradiction since $\gamma \notin \mathbb{A}$. Therefore, $1 \notin PS$, so $PS \neq S$.

The second statement is equivalent to showing that $Q \cap R$ is prime in R. Suppose $a, b \in R$ such that $ab \in P$. Then, $ab \in Q$ so it follows that either a or $b \in Q$ since Q is prime. Therefore, either a or $b \in R$. Moreover, P is proper since Q is proper ($1 \notin Q$). Finally, P is non-zero. Fix a non-zero element $a \in Q$, then by property 2.9 $0 \neq N_K^L(a) \in R \subset S$ since $a \in \mathbb{A}$. Then, $N_K^L(a) = ab$ where b is the product of the conjugates of a, and $b = N_K^L(a)/a \in S$ since § is a ring. It follows that $N_K^L(a) \subset aS \cap K \subset QS \cap K = P$. □

We will introduce two important numbers which we associate with primes and their splitting. Given a pair of primes P, Q with Q lying over P, we know that $Q^e | PS$ for some $e \geq 1$. We call the highest power of Q dividing PS the *ramification index* of Q over P, and denote it $e(Q|P)$. If $e(Q|P) > 1$, we say that P ramifies in L.

Also, since P, Q are maximal, then the quotient rings R/P and S/Q are fields. These are called the residue fields associated with P and Q. We know by statement (ii) in theorem 3.2 that they're finite. The inclusion $R \hookrightarrow S/Q$ has kernel $R \cap Q = P$. Therefore, we obtain an injective embedding $R/P \hookrightarrow S/Q$ which allows us to view R/P as a subfield of S/Q, or equivalently S/Q as a finite extension of R/P. We denote the degree of this extension by $f(Q|P) = \log_{|R/P|}|S/Q|$ and call it the *inertial degree* of Q over P. We have the following important theorem relating the degree $n = [L : K]$ with the inertial degrees and ramification indices of primes lying over primes in L. More precisely,

Theorem 3.9. Let P be a prime in R , and denote by $Q_1, \cdots Q_r$ the primes in S lying over P. Then,

$$\sum_{i=1}^{r} e_i f_i = n \text{ where } e_i = e(Q_i|P),\ f_i = f(Q_i|P)$$

For an ideal $I \subset R$, we denote the size of the residue field $|R/I|$ by $\big|\big|I\big|\big|$. The result follows from studying the multiplicativity of those indices. Specifically, we have the following proposition.

Proposition 3.10. (Marcus [1], p. 46) Taking R, S as before,

i. For ideals I, J in R, $\big|\big|IJ\big|\big| = \big|\big|I\big|\big| \cdot \big|\big|J\big|\big|$

ii. For the S-ideal IS, $\big|S/IS\big| = \big|\big|IS\big|\big| = \big|\big|I\big|\big|^n = \big|R/I\big|^n$

iii. For a principal ideal $(\alpha) \subset R$, $\big|\big|(\alpha)\big|\big| = \big|N_{\mathbb{Q}}^{K}(\alpha)\big|$

The theorem follows immediately. We know that $PS = \prod_{i=1}^{r} Q_i^{e_i}$. So,

$$\big|\big|P\big|\big|^n \overset{\text{by } ii.}{=} \big|\big|PS\big|\big| \overset{\text{by } i.}{=} \prod_{i=1}^{r} \big|\big|Q_i\big|\big|^{e_i} \overset{\text{def of } f_i}{=} \prod_{i=1}^{r} \left(\big|\big|P\big|\big|^{f_i}\right)^{e_i} \implies \sum_{i=1}^{r} e_i f_i = n$$

3.3 Splitting in Real Quadratic Fields

We will formulate four key propositions which will be of use later when working strictly with real quadratic fields. First, we will admit the following theorem from Marcus [1] p. 50.

Theorem 3.11. Let p be a prime in $\mathbb{Z}$ that ramifies in a number ring R, then $p \mid \operatorname{disc}(R)$.

Given a quadratic field $\mathbb{Q}[\sqrt{d}]$ where $d > 0$ squarefree and its associated number ring R, we can now determine exactly how primes $p \in \mathbb{Z}$ split in R .

Proposition 3.12. We tackle three separate cases.

i. If $p \mid d$, then $pR = (p, \sqrt{d})^2$.

ii. If $2 \nmid d$, then

$$2R = \begin{cases} (2, 1+\sqrt{d})^2 & \text{if } d = 3 \mod 4 \\ \left(2, \frac{1+\sqrt{d}}{2}\right)\left(2, \frac{1-\sqrt{d}}{2}\right) & \text{if } d = 1 \mod 8 \\ \text{prime} & \text{if } d = 5 \mod 8 \end{cases}$$

iii. If $p \nmid d$ and p is odd, then

$$pR = \begin{cases} (p, n+\sqrt{d})(p, n-\sqrt{d}) & \text{if } d = n^2 \mod p \\ \text{prime} & \text{otherwise} \end{cases}$$

Proof. We will only prove ii. since the others follow by identical arguments.

<u>Suppose $d = 3 \mod 4$</u>. Proceeding as above, $(2, 1+\sqrt{d})^2 = (4, 2+2\sqrt{d}, 1+d+2\sqrt{d})$. This is contained in $2R$ since 2 divides all factors (d is odd). On the other hand, the reverse inclusion follows since

$$2 + 2\sqrt{d} - (1 + d + 2\sqrt{d}) = d - 1 \implies \gcd(d-1, 4) = 2 \in (2, 1+\sqrt{d})^2$$

<u>Suppose $d = 1 \mod 8$</u>. By proposition 2.16, we have $R = \mathbb{Z}[(1+\sqrt{d})/2]$ since $d = 1$ mod 4. It's clear that

$$\left(2, \frac{1+\sqrt{d}}{2}\right)\left(2, \frac{1-\sqrt{d}}{2}\right) = \left(4, 1-\sqrt{d}, 1+\sqrt{d}, \frac{1-d}{4}\right) \subset 2R$$

The other inclusion follows since $2 = 1 - \sqrt{d} + 1 + \sqrt{d}$. Finally, note the factors are distinct since by 3.11 above, and proposition 2.16, we deduce that 2 does not ramify in R.

<u>Suppose $d = 5 \mod 8$</u>. Then, we also have $R = \mathbb{Z}[(1+\sqrt{d})/2]$ since $d = 1 \mod 4$. Consider the polynomial $f(x) = x^2 + x + \frac{1-d}{4} \in \mathbb{Z}[x]$ and note that $f((1+\sqrt{d})/2) = 0$. Assume P is a prime lying over 2. Then, f has a root in R/P since it has a root in R. But $[f]_2(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ has no roots. Therefore, $R/P \ncong \mathbb{Z}_2$. It follows that $f(P|p) \neq 1$. So, by theorem 3.9, we must have $f(P|p) = 2$. Therefore, pR is prime. (If $pR = P_1P_2$, then $2 = e_1f_1 + e_2f_2 \geq 4$ is a contradiction.) Note that for statement iii., a similar argument where we consider $x^2 - d$ yields the desired result. □

We have the following immediate corollary due to proposition 2.16.

Corollary 3.13. For a prime $p \in \mathbb{Z}$, p ramifies in $R = \mathbb{A}_{\mathbb{Q}[\sqrt{d}]}$ iff $p \mid \operatorname{disc}(R)$.

We briefly recall *Galois Groups* before proceeding to our second proposition. Given number fields $K \subset L$. We say, that L is normal over K iff L is closed under taking conjugates over K. Equivalently, every embedding of L that fixes K point-wise is an automorphism of L. We define the *Galois Group* of L over K, $\operatorname{Gal}(L/K)$, to be the group of automorphisms of L which fix K point-wise.

We will work in the special context of cyclotomic fields since every quadratic field is contained in a cyclotomic field . Let K be a subfield of $\mathbb{Q}[\omega], \omega = e^{2\pi i/m}$. We can identify $\mathbb{Z}_m^*$ with the Galois Group $G = \operatorname{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ by mapping a to the embedding $\omega \mapsto \omega^a$ (Washington [3] pg. 11) . Let H be the subgroup of $\mathbb{Z}_m^*$ that fixes K pointwise. Since $G = \mathbb{Z}_m^*$ is abelian, then H is normal in G. For a prime $p \nmid m$, let f_p denote the order of $[p]$ in G/H. Then, we have the following result.

Lemma 3.14. For any prime $P \subset K$ lying over p, $f(P|p) = f_p$.

Proof. This is an immediate corollary of Marcus [1] Theorem 33 p . 78. □

Proposition 3.15. Suppose K is a quadratic field with $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\omega]$. Then, with notation as above, for prime $p \nmid m$, if p is odd,

$$\overline{p} \in H \iff d = a^2 \mod p \text{ for some } a$$

Otherwise, for $p = 2$,

$$\overline{p} \in H \iff d = 1 \mod 8$$

where $\overline{p}$ represents the congruence class of $p \mod m$.

Proof. By 3.14, it is clear that $\overline{p} \in H$ is equivalent to having $f_p = 1$. The result then follows by immediately by proposition 3.12. □

3.4 The Class Number

Earlier in the chapter, we proved that the ideal classes of a number ring do indeed form a group. We will conclude the chapter by showing that this group is finite. Given a number field K of degree n over $\mathbb{Q}$ and its associated number ring $R = \mathbb{A}_K$, we start by introducing an embedding of the number ring into $\mathbb{R}^n$, which we will repeatedly use throughout the next chapters.

Let $\sigma_1, \ldots, \sigma_r$ and $\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s}$ denote the real and complex embeddings of K respectively. Thus, $r + 2s = [K : Q] = n$. Then, we can obtain an embedding ϕ of K in $\mathbb{R}^n$ defined by

$$\phi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathcal{R}\tau_1(\alpha), \mathcal{I}\tau_1(\alpha), \ldots, \mathcal{R}\tau_s(\alpha), \mathcal{I}\tau_s(\alpha))$$

where $\mathcal{R}$ and $\mathcal{I}$ denote the real and imaginary parts of the complex embeddings respectively. We have the following theorem.

Theorem 3.16. The embedding ϕ above sends R onto an n-dimensional lattice, $\wedge_R$. A fundamental parallelotope for this lattice has volume $\frac{1}{2^s}\sqrt{|\mathrm{disc}(R)|}$.

An n-dimensional lattice is defined as the $\mathbb{Z}$-span of an $\mathbb{R}$-basis for $\mathbb{R}^n$. For a basis $\{v_1, \ldots, v_n\}$, we define the corresponding fundamental parallelotope of the lattice as

$$\left\{ \sum_{i=1}^{n} a_i v_i \mid 0 \leq a_i < 1 \right\}$$

Proof. By 2.12, we may fix an integral basis $\alpha_1, \ldots, \alpha_n$ for R. We know that $R = \bigoplus_{i=1}^n \alpha_i \mathbb{Z}$, and clearly from the definition ϕ is an additive homomorphism. Therefore, $\wedge_R = \bigoplus_{i=1}^n \phi(\alpha_i)\mathbb{Z}$. We want to show that the images $\phi(\alpha_i)$ are linearly independent over $\mathbb{R}$.

Recall that the volume of a fundamental parallelotope for an n-dimensional lattice is the absolute value of the determinant of the matrix formed by a basis. Therefore, computing the determinant of the $n \times n$ matrix $A = (a_{ij})$ defined by $a_{ij} = (\phi(\alpha_i))_j$ will simultaneously verify the linear independence of the $\phi(\alpha_i)$'s and prove the remaining clause in the theorem.

By applying elementary column operations on A, we get

$$\begin{vmatrix} & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \cdots & \sigma_r(\alpha_i) & \mathcal{R}\tau_1(\alpha_i) & \mathcal{I}\tau_1(\alpha_i) & \cdots & \mathcal{R}\tau_s(\alpha_i) & \mathcal{I}\tau_s(\alpha_i) \\ & \vdots & \vdots & \vdots & & \vdots & \vdots \end{vmatrix}^2$$

$$\text{For } 1 \leq j \leq s \qquad \Big\downarrow {\scriptstyle \substack{C_{r+2j-1} \to C_{r+2j-1} - i \cdot C_{r+2j} \\ C_{r+2J} \to -C_{r+2j} + \frac{1}{2} \cdot C_{r+2j-1}}}$$

$$\begin{vmatrix} & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \cdots & \sigma_r(\alpha_i) & \tau_1(\alpha_i) & \frac{1}{2}\,\overline{\tau_1}(\alpha_i) & \cdots & \tau_s(\alpha_i) & \frac{1}{2}\,\overline{\tau_s}(\alpha_i) \\ & \vdots & \vdots & \vdots & & \vdots & \vdots \end{vmatrix}^2 = \frac{1}{2^{s+1}} |\mathrm{disc}(R)|$$

It follows that

$$\mathrm{Vol}\left(\mathbb{R}^N / \wedge_R\right) = \left| \sqrt{\frac{1}{2^{s+1}} |\mathrm{disc}(R)|} \right| = \frac{1}{2^s} \sqrt{|\mathrm{disc}(R)|}$$

We denote it by $\mathrm{Vol}\left(\mathbb{R}^N / \wedge_R\right)$ since we know that the discriminant is invariant of the choice of basis, so this volume is an invariant of $\wedge_R$.

□

We will use this embedding to prove the following theorem.

Theorem 3.17. For every non-zero ideal I in R, there exists a non-zero $\alpha \in I$ such that

$$\left|N^K(\alpha)\right| \leq \lambda \|I\| \qquad \text{where} \qquad \lambda = \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}(R)|}$$

Proof. Let $\wedge_I$ denote the image of I under ϕ. Since we know $|R/I|$ is finite, we deduce that that $\wedge_R/\wedge_I$ is a finite group and subsequently that $\wedge_I$ is an n-dimensional sublattice of $\wedge_R$. It follows by the structure theorem for finitely generated abelian groups that $\wedge_R/\wedge_I$ is a product of at most n cyclic groups whose orders we denote $c_1, \cdots, c_n$ such that $c_i \mid c_{i+1}$. Choosing appropriately, we may get $\{v_1, \ldots, v_n\}$ a basis for $\wedge_R$ such that $\{c_1v_1, \cdots, c_nv_n\}$ is a basis for $\wedge_I$. It follows that

$$\operatorname{Vol}(\mathbb{R}^n/\wedge_I) = c_1 \cdots c_n \operatorname{Vol}(\mathbb{R}^n/\wedge_R) = \frac{1}{2^s}\sqrt{|\operatorname{disc}(R)|}\big|\big|I\big|\big|$$

We will use this in tandem with Minkowski's theorem in order to find the desired $\alpha \in I$. Define $N : \mathbb{R}^n \to \mathbb{R}$ by

$$N(x) = x_1 \cdots x_r(x_{r+1}^2 + x_{r+2}^2) \cdots (x_{r+2s-1}^2 + x_{r+2s}^2)$$

and note that $N(\phi(\alpha)) = N^K(\alpha)$ for $\alpha \in R$. Consider the set

$$A = \left\{x \in \mathbb{R}^n \middle| |x_i| \leq 1, (x_{r+2j-1}^2 + x_{r+2j}^2) \leq 1 \text{ for } 1 \leq i \leq r, 1 \leq j \leq s\right\}$$

Clearly A is convex, closed under taking opposites, and $|N(a)| \leq 1$ for $a \in A$. Then, Minkowski's theorem (Marcus [1] p. 97) guarantees that $\wedge_I$ contains a point $a \in A$ with

$$|N(a)| \leq \frac{2^n}{\operatorname{Vol}(A)} \cdot \operatorname{Vol}(\mathbb{R}^n/\wedge_I)$$

Taking $\alpha = \phi^{-1}(a)$ and noting that $\operatorname{Vol}(A) = 2^r\pi^s$ proves the theorem. □

Corollary 3.18. The ideal class group of a number ring R is finite.

Proof. Given an ideal class C, fix an ideal I belonging to C^{-1} and obtain an $\alpha \in I$ as in the theorem above. By unique factorization, since $(\alpha) \subset I$, we must have $(\alpha) = IJ$ for some $J \in C$. Then, using proposition 3.10, we get

$$\left|N^K(\alpha)\right| = \|I\| \cdot \|J\| \leq \alpha \|I\| \Longrightarrow \|J\| \leq \alpha$$

So, every ideal class must contain an ideal J with $\left|\left|J\right|\right| \leq \lambda$. But, there can only be finitely many J since this bound clearly permits only finitely prime factorizations also by proposition 3.10. □

We denote the cardinality of the class group by h, the class number. In what remains, we develop a formula to calculate h via studying the behavior of functions associated to the number field.

Chapter 4

Distribution of Ideals

In order to study the class number of a ring, we will need a fundamental result concerning the distribution of ideals within classes. More precisely, given a number field K of degree n and its associated number ring R, let $F(\mathcal{C}, t)$ denote the ideals in a fixed class $\mathcal{C}$ of R with $\big|\big|I\big|\big| = \big|R/I\big| \leq t$. Then, we are going to prove

Theorem 4.1. $F(\mathcal{C}, t) = \kappa t + O(t^{1-1/n})$ for some constant κ.

The main approach of the proof is to translate the problem into different contexts that facilitate the counting process. We start off with the following proposition.

Proposition 4.2. Fix an ideal class C and an ideal J in C^{-1}. Then, every ideal I in C with $||I|| \leq t$ corresponds uniquely to a principal ideal $(\alpha) \subset J$ with $||\alpha|| \leq t||J||$

Proof. IJ must be principal since it belongs to $\mathcal{C}\mathcal{C}^{-1} = [(1)]$. Then, I corresponds to $IJ = (\alpha)$ and $||\alpha|| = ||I|| \cdot ||J|| \leq t||J||$. On the other hand, given a principal ideal $(\alpha) \subset J$ with $||\alpha|| \leq t||J||$, we know that $(\alpha) = IJ$ for some I. It follows that $I \in \mathcal{C}^{-1}$ and $||I|| \leq t$.

□

We have now simplified the problem into counting principal ideals $(\alpha) \subset J$, a fixed ideal in $\mathcal{C}$, with $\big|\big|(\alpha)\big|\big| = \big|N^K(\alpha)\big| \le t\big|\big|J\big|\big|$. In essence, we're counting elements $\alpha \in J$ whose norm is bounded by $t\big|\big|J\big|\big|$. The delicate part of this process is accounting for associates - elements that only differ by a unit. They generate the same principal ideal so we want to avoid double counting. In order to resolve this issue, we must first understand how those associates are spread out through understanding the structure of the unit group.

We will first prove the theorem for the real quadratic case where the structure of the unit group U makes it feasible to visually tackle our problem.

4.1 Real Quadratic Case

In what follows, $K = Q[\sqrt{m}]$ for squarefree $m \in \mathbb{Z}, R$ is the associated number ring, and U is its group of units. For simplicity, we assume $m = 2, 3 \mod 4$ so $R = \mathbb{A}_{\mathbb{Q}[\sqrt{m}]} = \mathbb{Z}[\sqrt{m}]$.

Theorem 4.3. There exists a **fundamental unit** $u \in R$ such that

$$U = \{\pm u^k \big| k \in \mathbb{Z}\}$$

We will require the following proposition concerning certain subgroups in $\mathbb{R}^m$.

Proposition 4.4. Let G be a subgroup of $\mathbb{R}^m$ such that every bounded subset is finite. Then, G is a lattice.

Proof. Let $\wedge = \mathbb{Z}\text{-span}\{v_1, \cdots, v_d\}$ be a lattice of maximal dimension contained in G, (possibly just 0). Then, G is contained in the subspace generated by $\wedge$. Otherwise, there would exist a $v \in G \setminus \mathbb{R}\text{-span}\{v_1, \cdots, v_d\}$. Then, the lattice given by $\mathbb{Z}\text{-span}\{v, v_1, \cdots, v_d\} \subset G$ contradicts the maximality of $\wedge$.

Fix a *fundamental parallelotope* F for $\wedge$ defined as

$$F = \left\{ \sum_{i=1}^{n} a_i v_i \Big| a_i \in [0,1) \right\}$$

Clearly, F is bounded. Moreover, by subtracting integer multiples of the basis, every element $v \in G$ can be translated into F via elements of $\wedge$. Hence, $\big|G/\wedge\big| \leq \big|G \cap F\big|$ which is finite by assumption. It is not difficult to see that $G/\wedge$ is in fact a finite group with the binary operation

$$[a]_\wedge + [b]_\wedge = [a+b]_\wedge \quad \text{(we denote } [a]_\wedge = a + \wedge\text{)}$$

Taking r to be the least common multiple of the orders of elements in $G/\wedge$, we deduce that $rG = [0]_\wedge \subset \wedge$. This implies rG is a free abelian group of rank $\leq d$ by 2.13. Since $r \neq 0$, it follows G must be a free abelian group with the same rank as rG. Then, $rG \subset \wedge \subset G$ and hence rank $G = d$.

Finally, we admit the stacked bases theorem (equivalent to expressing a basis for $\wedge$ in terms of G and applying the normal form from Jacobson [2] pg. 181). It asserts that we may choose a $\mathbb{Z}$-basis for G, $\{a_1, \cdots, a_d\}$ such that $\{c_1 a_1, \cdots, c_d a_d\}$ is a basis for $\wedge$ for some integers $c_1, \cdots, c_d$. Then, $\wedge$ being a lattice ensures that $\{a_1, \cdots, a_d\}$ are $\mathbb{R}$-independent, which in turn implies G is a lattice. □

We now proceed with the proof of the unit theorem.

Proof. We recall the natural embedding of R into the lattice $\wedge_R \subset \mathbb{R}^2$ that maps an element to its conjugates.

$$\begin{aligned} \phi : U \subset R \to \quad & \wedge_R \\ a + b\sqrt{m} \mapsto & \left(a + b\sqrt{m}, a - b\sqrt{m}\right) \end{aligned}$$

We restrict the mapping above to the unit group $U \subset R$ and compose it with a logarithmic mapping, $\mathcal{L}$, in order to encode the multiplicative structure of our unit group into an additive lattice structure. We naturally define $\mathcal{L}$ component-wise by

$$\begin{aligned} \mathcal{L} : \mathbb{R}^* \times \mathbb{R}^* &\to \mathbb{R}^2 \\ (z, w) &\to (\log|z|, \log|w|) \end{aligned}$$

We refer to the composition as $\log = \mathcal{L} \circ \ \phi$.

$$\begin{array}{ccccc} \log : \ U \subset R \setminus \{0\} & \overset{\phi}{\to} & \wedge_R \setminus \{0\} & \overset{\mathcal{L}}{\to} & \{x + y = 0\} \subset \mathbb{R}^2 \\ \alpha = a + b\sqrt{m} & \mapsto & \left(a + b\sqrt{m}, a - b\sqrt{m}\right) & \mapsto & \left(\log\left|a + b\sqrt{m}\right|, \log\left|a - b\sqrt{m}\right|\right) \end{array}$$

Note that for α, β in U, $\log\alpha\beta = \log\ \alpha + \log\beta$. It follows that, for $\alpha \in U$, the coordinate sum of $\log\ \alpha = \log|N^K(\alpha)| = 0$. Therefore, $\log : U \to \{x + y = 0\}$ is a group homomorphism.

In addition, note that if $|\log\alpha| \leq M$, then each of its coordinates must be less than M, therefore $|\alpha| \in (e^{-M}, e^{M})$. Since bounded subsets of a lattice are finite, we deduce that bounded subsets of $\log(U)$ are finite since they have a bounded (and hence finite) pre-image. Therefore, by 4.4, $\log(U)$ is a lattice in $\mathbb{R}^2$ which we will denote by $\wedge_U$ from hereon.

In conclusion, $\log(U)$ is an additive one-dimensional lattice on the line $x = -y$. Therefore, it has two opposite minimal norm elements. We choose the one with the positive x-value, and denote it $log(u)$. Hence, U is multiplicatively generated by u, the **fundamental unit**, which is the smalllest unit > 1.

□

Proof of theorem 4.1 for real quadratic fields. Recall that we were interested in the structure of the unit group in order to count principal ideals via the sets of associates that generate them. If we view the unit group U to be acting on R via multiplication, then those associates belong to the orbit of some unit u. In other words, our principal ideals are actually in bijection with the orbits of the unit group U acting on elements of R by multiplication.

So, our problem boils down to finding a subset $S \subset R$ of orbit representatives for U, then counting the elements of $J \cap S$ whose norm is bounded by $t\big|\big|J\big|\big|$. To simplify our task, we will actually find a set S' of representatives for $V = \{u^k\}$ and account for the opposites that will be represented twice in our coset.

In order to benefit from the additive structure of our ideal J, we again exploit the geometric embedding from earlier. J maps isomorphically onto a lattice $\wedge_J \subset \mathbb{R}^2$. Similarly, the group V maps isomorphically onto a subgroup V'. So, we will find a set of orbit representatives of $V' \subset (\mathbb{R}^*)^2$, and our norm N^K in R translates into

$$\begin{aligned} N : (\mathbb{R}^*)^2 &\to \mathbb{R} \\ (x_1, x_2) &\mapsto x_1 x_2 \end{aligned}$$

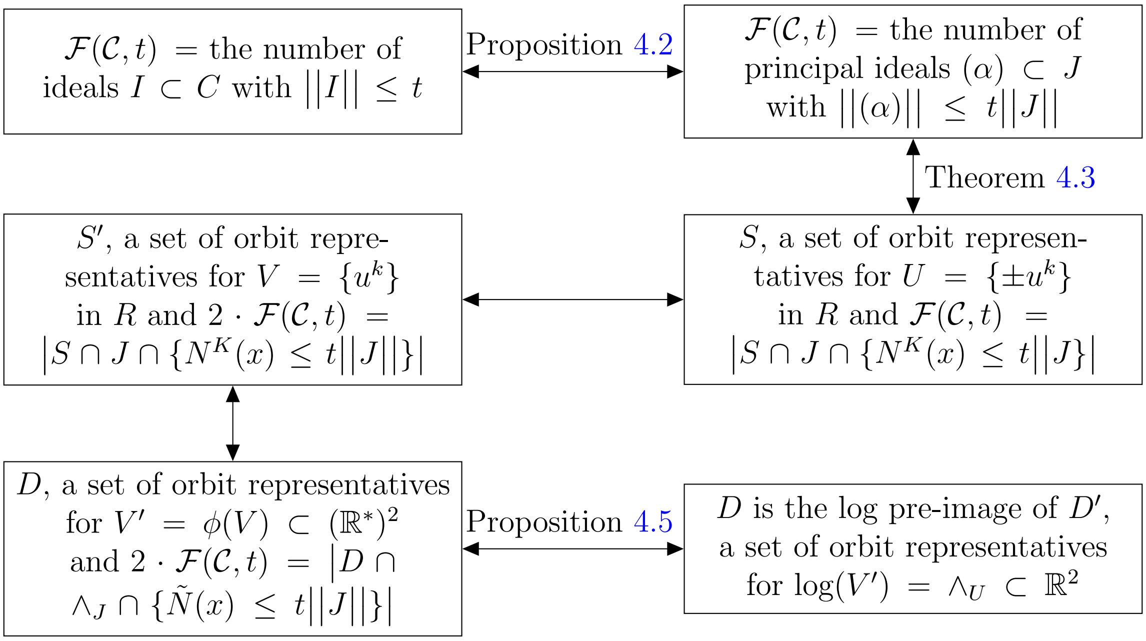
since the norm is just the product of the two embeddings.

The structure of $\wedge_R$ does not encode the special nature of our units, and hence is less convenient for constructing a set of coset representatives. So, we will again resort to the log mapping from earlier.

$$\begin{array}{llll} \log: & U \subset R\setminus\{0\} \xrightarrow{\phi} & \wedge_R \setminus \{0\} & \xrightarrow{\mathcal{L}} \{x+y=0\} \subset \mathbb{R}^2 \\ & \alpha = a + b\sqrt{m} \mapsto & \left(a+b\sqrt{m}, a-b\sqrt{m}\right) & \mapsto \left(\log\left|a+b\sqrt{m}\right|, \log\left|a-b\sqrt{m}\right|\right) \end{array}$$

It is clear from the definition that ker(log)$= \{\pm 1\}$. Then, by the fundamental homomorphism theorem, $U/\{\pm 1\} \cong \log(U) = \wedge_U \subset \mathbb{R}^2$. Recalling that $U = \pm V$, we deduce that $\log|_V$ is an isomorphism. It follows that $\mathcal{L} : V' \subset (\mathbb{R}^*)^2 \to \wedge_U)$ is an isomorphism. In which case, $\log(V) = \mathcal{L}(\phi(V)) = \mathcal{L}(V') = \wedge_U$. Then, we claim that our desired subset of orbit representatives is $D = \mathcal{L}^{-1}(D')$, where D' is a set of orbit representatives for $\wedge_U \subset \mathbb{R}^2$.

To summarize, our task has been transformed as follows



$\mathcal{F}(\mathcal{C}, t)$ = the number of ideals $I \subset C$ with $||I|| \leq t$

Proposition 4.2

$\mathcal{F}(\mathcal{C}, t)$ = the number of principal ideals $(\alpha) \subset J$ with $||(\alpha)|| \leq t||J||$

Theorem 4.3

S', a set of orbit representatives for $V = \{u^k\}$ in R and $2 \cdot \mathcal{F}(\mathcal{C}, t) = |S \cap J \cap \{N^K(x) \leq t||J||\}|$

S, a set of orbit representatives for $U = \{\pm u^k\}$ in R and $\mathcal{F}(\mathcal{C}, t) = |S \cap J \cap \{N^K(x) \leq t||J\}|$

D, a set of orbit representatives for $V' = \phi(V) \subset (\mathbb{R}^*)^2$ and $2 \cdot \mathcal{F}(\mathcal{C}, t) = |D \cap \wedge_J \cap \{\tilde{N}(x) \leq t||J||\}|$

Proposition 4.5

D is the log pre-image of D', a set of orbit representatives for $\log(V') = \wedge_U \subset \mathbb{R}^2$

Figure 4.1: Summary of approach

The final assertion follows from the following proposition which we apply to $G = (\mathbb{R}^*)^2$ and the map $\mathcal{L}$.

Proposition 4.5. Given a homomorphism of abelian groups, $f : G \to G'$, and a subgroup S of G that is isomorphic to its image S' in G', then the pre-image of a set of coset representatives for S' is a set of coset representatives for S.

Proof. Let D' denote a set of coset representatives for S', and let $D = f^{-1}(D')$. Then, for $g \in G$, we know that $f(g) \sim a$ for some $a \in D'.Hence, f(g) = a + s'$ for some $s' \in S'$. But, $f(S) \cong S'$, so there exists a unique s such that $f(s) = s'$. Therefore, $a = f(g) - f(s) = f(g - s)$ from which it follows that $g - s \in D$, and $g \sim g - s$. So, every element in G has an orbit representative in D.

To show this representative is unique, assume $d_1, d_2 \in D$ satisfy $d_1 \sim d_2$. Then, $d_1 = d_2 + s$ for some $s \in S$. So, $f(d_1) = f(d_2) + f(s)$ and $f(d_1) \sim f(d_2)$. But, this implies $f(d_1) = f(d_2)$ since they are both in D' which is a set of coset representatives. Therefore, $f(s) = 0$, and hence $s = 0$, since $f|_S$ is an isomorphism. Hence, $d_1 = d_2$. We have shown that every element of G has a unique representative in D. Therefore, D is a set of coset representatives of S in G.

□

We may apply the proposition to $\mathcal{L}$ since the orbits of the subgroups by multiplication are essentially cosets. Fix a fundamental parallelotope F of $\wedge_U$. Then, $F = \{c\log(u) \big| 0 \leq c < 1\}$ is the line segment from the origin to the image of the fundamental unit u. Crossing said segment with the perpendicular line in the direction of $\mathbf{v} = (1,1)$ will yield a set of coset representatives D' for $\wedge_U \in \mathbb{R}^2$. Then,

$$D = \mathcal{L}^{-1}(D') = \mathcal{L}^{-1}(F + \mathbb{R}v) = \{x \in (R^*)^2 \big| \mathcal{L}(x) \in F + \mathbb{R}(1,1)\}$$

So, all that is left is to show that

$$\Big| D \cap \wedge_J \{|N(x)| \leq t \cdot ||J||\Big| = O(t)$$

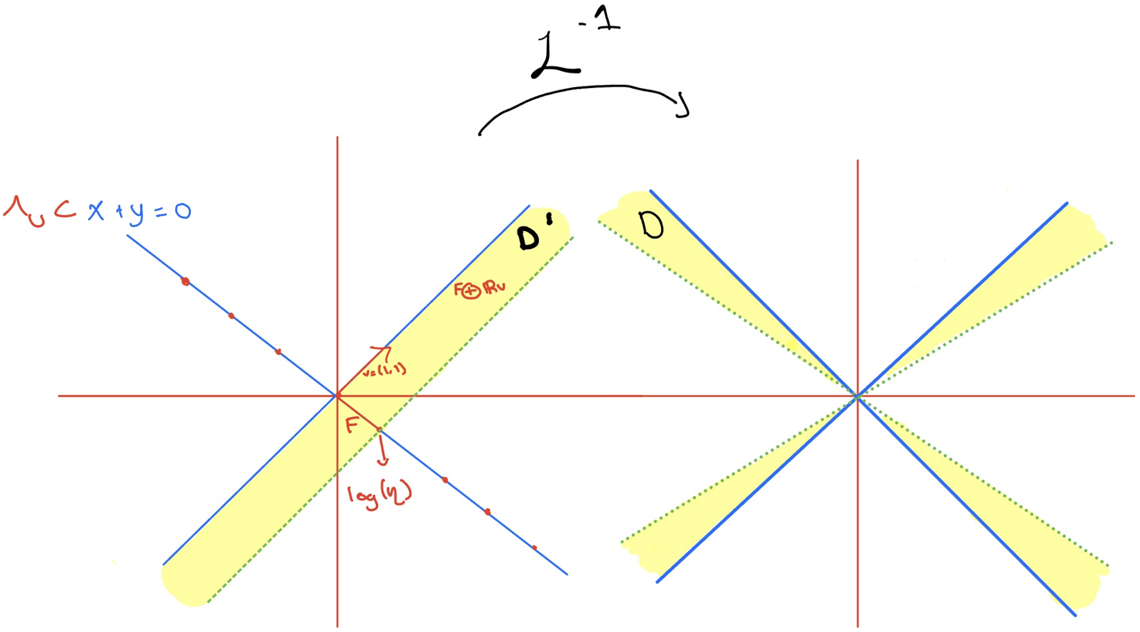


Figure 4.2: $D = \mathcal{L}^{-1}(D')$

Note that D is homogenous since $D = aD$ for every non-zero real number a. Indeed, if $x = (x_1, x_2) \in D$,

$$\mathcal{L}(x) = f + c(1,1) \quad , f \in F, c \in \mathbb{R}$$

$$\implies \mathcal{L}(ax) = \log(|ax_1|, |ax_2|) = (\log(|a|), \log(|a|)) + \mathcal{L}(x) = f + (c + \log|a|)(1,1)$$

Then, letting $D_a = D \cap \{|N(x)| \leq a\}$, it follows that $D_a = \sqrt{a}D_1$. We may now benefit from the following proposition that describes how bounded subsets interact with lattices in $\mathbb{R}^2$.

Proposition 4.6. Given a lattice $\wedge$ in $\mathbb{R}^2$ and a bounded subset B of $\mathbb{R}^2$ such that its boundary ∂B is piecewise-smooth, then for $a \in \mathbb{R}$

$$\big| \wedge \cap aB \big| = a^2 \frac{\text{vol}(B)}{\text{vol}(\mathbb{R}^2/\wedge)} + O(a)$$

Proof. We claim that we may take $\wedge = \mathbb{Z}^2$ without loss of generality. We know that

$\wedge$ maps to $\mathbb{Z}^2$ through a bounded linear transformation T that preserves smoothness, and scales all volumes by an equal factor. Hence, letting $D = T(B)$

$$\left|\mathbb{Z}^2 \cap aD\right| = \left|\wedge \cap aB\right| \quad ; \quad \frac{\text{vol}(B)}{\text{vol}(\mathbb{R}^2/\wedge)} = \frac{\text{vol}(T(B))}{\text{vol}(\mathbb{R}^2/T(\wedge))} = \frac{\text{vol}(D)}{\text{vol}(\mathbb{R}^2/\mathbb{Z}^2)} = \text{vol}(D)$$

The key idea is that both the number of lattice points in aD and its volume can be approximated by dividing the region into small cubes. Then, the difference will amount to no more than the cubes on the boundary which we'll show can be nicely bounded by a linear multiple of a. Divide the grid into 1×1 cubes centered at $\mathbb{Z}^2$ as shown in the images of an example set $D, 2D$ below. (Note the more refined grid on the right representing $2D$).

Each cube has volume 1 and so letting $I(aD)$ denote the number of cubes inside

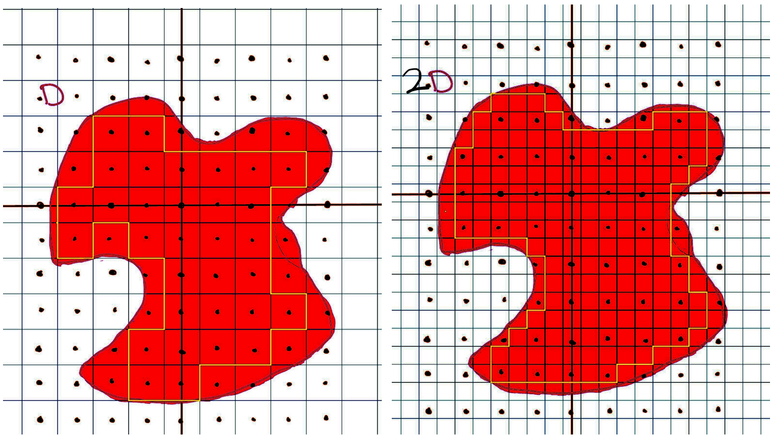


Figure 4.3: Using grids to measure volume and lattice points

aD and ∂aD denote the number of cubes intersecting the boundary, we have

$$\text{vol}(aD) - I(aD) \leq \partial(aD) \quad ; \quad |\mathbb{Z}^2 \cap aD| - I(aD) \leq \partial(aD)$$

Combining the two, we get that

$$\left||\mathbb{Z}^2 \cap aD| - \text{vol}(aD)\right| \leq 2\partial(aD)$$

Therefore, it remains to show that $\partial(aD)$ is $O(a)$. The boundary of D is piecewise smooth. So, it's the union of finitely many smooth segments, and it suffices to show that for a smooth segment, $f([0,1])$, $\partial(af([0,1])) = O(a)$. Consider the example below where we closely analyze the top-right chunk of D from above.

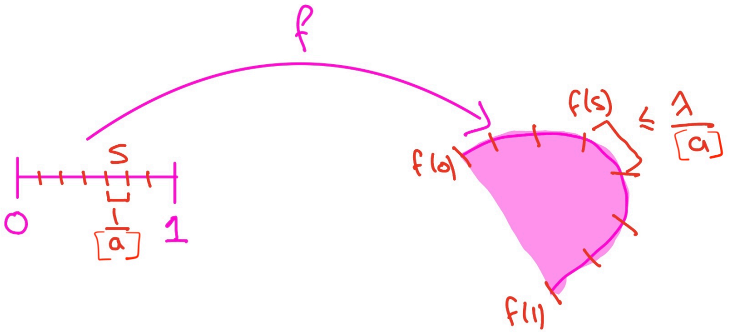


Figure 4.4: Studying how $[0,1]$ behaves under f when scaled

For any $a > 1$, divide $[0,1]$ into $[a]$ small cubes S of size $1/[a]$. f is smooth, so it has continuous partial derivatives. Moreover, each of its partial derivatives are bounded on $[0,1]$ since it's a compact set. By applying the Mean Value Theorem on each of the two components, we have for $x_1, x_2 \in S \subset [0,1]$,

$$f(x_1) - f(x_2) = (x_1 - x_2)\left(\frac{\partial f}{\partial x}(c_1), \frac{\partial f}{\partial x}(c_2)\right) \text{for some } c_1, c_2 \in [x_1, x_2]$$

It follows that $f(S)$ has diameter at most $\lambda/[a]$ for some λ. Then, the diameter of $af(S)$ is at most $a\lambda/[a] \leq 2\lambda$. Zoom into $af(S)$, and construct a circle of radius 2λ around any point. Clearly $af(S)$ is contained within this circle. Moreover, this circle intersects at most $(2\text{diam}(f(s)+2)^2 \leq (4\lambda+2)^2$ of our 1×1 cubes from above. Finally, noting that we have $[a]$ small cubes, we get that the smooth segment $af([0,1])$ intersects at most $[a](4\lambda+2)^2$ cubes which is $O(a)$. Since, $\partial(aD)$ consists of finitely many piecewise smooth segments, this shows that $\partial(aD)$ is $O(a)$, completing our proof.

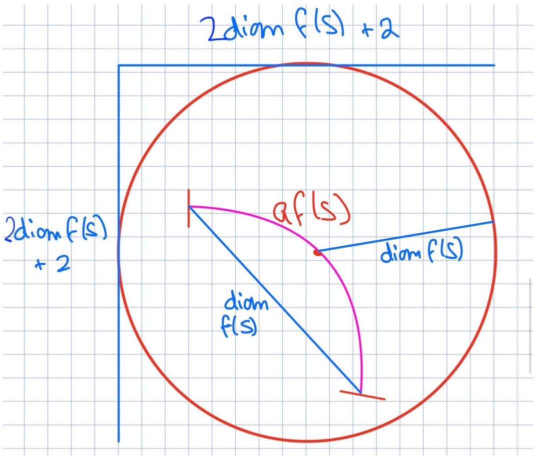


Figure 4.5: Bounding $af(S)$

□

Applying our proposition with $\wedge = \wedge_J$, and $B = D_{t||J||}$ and recalling that

$$\mathrm{vol}(\mathbb{R}^2/\wedge_J) = \mathrm{vol}(\wedge_R/\wedge_J\,| \cdot \mathrm{vol}(\mathbb{R}^2/\wedge_R) = \big|R/J\big|\sqrt{\mathrm{disc}(R)} = \big||J|\big|\sqrt{\mathrm{disc}(R)}$$

we get

$$\Big|\wedge_J \cap D_{t||J||}\Big| = \Big|\wedge_J \cap \sqrt{t||J||}D_1\Big| = t||J|| \cdot \frac{\mathrm{vol}(D_1)}{||J||\sqrt{\mathrm{disc}(R)}} + O\left(\sqrt{t||J||}\right)$$

$$= \frac{\mathrm{vol}(D_1)}{\sqrt{\mathrm{disc}(R)}}t + O(t^{1/2})$$

Summing it all together,

$$\mathcal{F}(\mathcal{C}, t) = \frac{1}{2}\Big|\wedge_J \cap D_{t||J||}\Big| = \kappa t + O(t^{1/2}) \qquad \text{where } \kappa = \frac{\mathrm{vol}(D_1)}{2\sqrt{\mathrm{disc}(R)}}$$

completing the proof. □

Proposition 4.7. $\kappa = \dfrac{2\mathrm{log}(u)}{\sqrt{\mathrm{disc}(R)}}$

Proof. The result follows immediately if we can show that $\mathrm{vol}(D_1) = 4\log(u)$. Recall that u is the smallest fundamental unit greater than 1. Assume its conjugate $|\overline{u}| < u$. The, our initial region D' was defined as the region between the lines

$$y = x \quad \text{and} \quad y = x + \log\left|\frac{u}{\overline{u}}\right|$$

Then, taking the inverse of the log mapping, we get that D is defined as the region between

$$|y| = |x| \quad \text{and} \quad |y| = \left|\frac{u}{\overline{u}}\, x\right|$$

Then, D_1 is the portion of D bounded by $|N(x)| = |xy| = 1$. Finally, we show that the volume of A below is $\log(u)$ which completes our proof since D_1 consists of four copies of A.

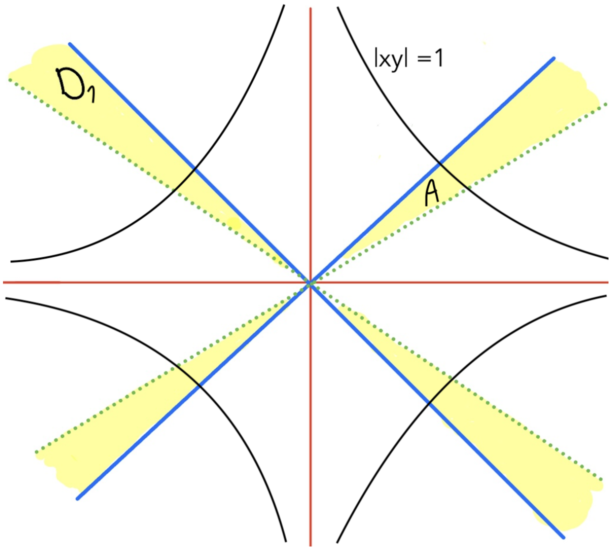


Figure 4.6: $\mathrm{Vol}(D_1) = 4\mathrm{Vol}(A)$

$$\begin{aligned}
\mathrm{vol}(A) &= \int_0^{\sqrt{|\frac{\overline{u}}{u}|}} \left(\left|\frac{u}{\overline{u}}\right| - 1\right) x\, dx + \int_{\sqrt{|\frac{\overline{u}}{u}|}}^{1} \left(\frac{1}{x} - x\right)\, dx \\
&= \frac{1}{2} - \frac{\sqrt{|\frac{\overline{u}}{u}|}}{2} + -\frac{1}{2} - \log\left(\sqrt{\left|\frac{\overline{u}}{u}\right|}\right) + \frac{\sqrt{|\frac{\overline{u}}{u}|}}{2} \\
&= -\frac{1}{2}\log\left(\frac{\overline{u}}{u}\right) = \log(u)
\end{aligned}$$

where the final equality follows since $\overline{u}/u = N(u)/u^2 = 1/u^2$.

□

4.2 General Case

In general, a similar procedure holds for any number ring. Some of our tools will have to be adjusted to a more general context and may require more technical work, but the underlying trajectory is unchanged. In what follows, given any number field K of degree n over $\mathbb{Q}$ and the associated number ring R, we let r and $2s$ denote the number of real and complex embeddings of K, where $r + 2s = n$. We will again need to understand the structure of the group of units.

Theorem 4.8. (Unit Theorem) Let U denote the group of units, and W denote the group consisting of the roots of 1. Then, U is the direct product $W \times V$ where V is a free abelian group of rank $r + s - 1$.

Note that in the case of the real quadratic fields, $r + s - 1 = 1$ and W consists only of ± 1, which coincides with our earlier result. In general, rather than having solely one fundamental unit, we have a fundamental system of units $u_1, \cdots, u_{r+s-1}$ which generates V. In other words,

$$V = \{u_1^{k_1} \cdots u_{r+s-1}^{k_{r+s-1}} | k_i \in \mathbb{Z}\}$$

Proof. The proof idea is similar to the quadratic case, but some steps need to be adjusted to the new context. Letting $\sigma_1, \cdots, \sigma_r, \tau_1, \cdots \tau_s$ denote the real and complex embeddings of K, we can construct the embedding of K into $\mathbb{R}^n$ via

$$\begin{aligned} \phi : K &\to \mathbb{R}^n \\ \alpha &\mapsto \Big(\sigma_1(\alpha), \cdots, \sigma_r(\alpha), \Re\tau_1(\alpha), \Im\tau_1(\alpha) \cdots \Re\tau_s(\alpha), \Im\tau_s(\alpha)\Big) \end{aligned}$$

We know from earlier that the restriction of this embedding to R sends it to a lattice $\wedge_R$. Then, we again define the log sequence of mappings below in order to encode the multiplicative nature of U into the additive nature of lattices.

$$\log : U \subset R \setminus \{0\} \overset{\phi}{\to} \wedge_R \setminus \{0\} \subset \mathbb{R}^n \overset{\mathcal{L}}{\to} \wedge_U \subset H = \{z_1 + \cdots + z_{r+s} = 0\} \subset \mathbb{R}^{r+s}$$

where the definition of $\mathcal{L}$ is adjusted to become

$$\begin{aligned} \mathcal{L} : (\mathbb{R}^*)^n &\to \mathbb{R}^{r+s} \\ (x_1, \cdots, x_r, y_1, \cdots, y_{2s}) &\mapsto \big(\log|x_1|, \cdots, \log|x_r|, \log(y_1^2 + y_2^2), \cdots\big) \end{aligned}$$

Note that this does indeed function like the log mapping in the previous section:

i. $\mathcal{L}$ is well-defined on $\wedge_R$ since all the conjugates of α are non-zero. Therefore, their norms are strictly positive.

ii. For $\alpha \in U$, the field norm of U is ± 1, hence the coordinate sum of $\log(\alpha)$ is given by

$$\begin{aligned} &\log|\sigma_1(\alpha)| + \cdots + \log|\sigma_r(\alpha)| + \log(|\tau_{r+1}(\alpha)|^2) + \cdots + \log(|\tau_s(\alpha)|^2) \\ &= \log\big|\sigma_1(\alpha) \cdots \sigma_r(\alpha)\tau_{r+1}(\alpha)\overline{\tau}_{r+1}(\alpha) \cdots \tau_s(\alpha)\overline{\tau}_s(\alpha)\big| = \log|N^K(\alpha)| = 0 \end{aligned}$$

Thus U does indeed map into the hypersurface H.

iii. For $\alpha, \beta \in \wedge_R \setminus \{0\}$, $\log(\alpha\beta) = \log(\alpha) + \log(\beta)$ since the embeddings are multiplicative so

$$|\sigma_i(\alpha\beta)| = |\sigma_i(\alpha)\sigma_i(\beta)| = |\sigma_i(\alpha)| \cdot |\sigma_i(\beta)|$$

Therefore, $\log(\alpha\beta)_i = \log(\alpha)_i + \log(\beta)_i$.

iv. The previous two remarks show that log: $U \to H$ is in fact a group homomorphism from the multiplicative group U to the additive group H. Moreover, note that for any $\omega \in W$, $\omega^n = 1 \implies n\log(\omega) = 0$. Therefore, $W \subset \text{Ker}(\log)$.

v. Given a bounded subset B in $\mathbb{R}^{r+s}$ such that $|x| \leq M$ for all $x \in B$, then every element in $\mathcal{L}^{-1}(B)$ must have coordinates bounded above by e^M. Therefore, $\mathcal{L}^{-1}(B) \subset [-e^M, e^M]^n \bigcap \wedge_R \subset \mathbb{R}^n$. Hence, $\mathcal{L}^{-1}(B)$ is finite since bounded subsets of a lattice are finite.

vi. The property above shows that the Ker(log) is a finite subgroup (ϕ is an isomorphism). So, for every element of the kernel ω has finite order which implies $\omega^k = 1$ for some k. Therefore, W is in fact the kernel. Alternatively, we could have observed that for any root of 1, its minimal polynomial must be a cyclotomic polynomial of order $d|n$ of which there are finitely many. In either case, we can conclude that W is a subgroup of the group of $|W|$-th roots of unity which is cyclic, therefore W is also cyclic.

vii. Also note that a bounded subset of $\log(U)$ must be finite since its pre-image is finite. Therefore, by lemma 4.4 we deduce that U is a lattice, which we denote $\wedge_U$ as above.

$\wedge_U = \log\ (U)$ is a free abelian group of rank $d \leq r + s - 1$. Thus, we fix a $\mathbb{Z}$-basis for it denoted by $\log(u_1), \cdots \log(u_d)$, and let V be the subgroup of U generated by

$u_1, \cdots, u_d$. Then, for every element $\alpha \in U$, we may express

$$\log(\alpha) = k_1 \log(u_1) + \cdots + k_d \log(u_d) = \log(u_1^{k_1} \cdots u_d^{k_d}) \quad , c_i \in \mathbb{Z}$$

Hence, $\alpha = \omega \cdot u_1^{k_1} \cdots u_d^{k_d}$ for some $\omega \in \text{Ker log} = W$. Therefore, $U = W \times V$. All that remains is to show that $\log(U)$ has rank $r+s-1$ by generating $r+s-1$ units whose log images are linearly independent over $\mathbb{R}$. We admit the following lemma.

Lemma 4.9. There exists a unit u such that $\log(u)_1$ is positive and all other coordinates of $\log(u)$ are negative. (Marcus [1] pg. 145)

Applying the lemma above allows us to generate special units $u_1, \cdots, u_{r+s}$ such that all coordinates of $\log(u_i)$ are negative except the i-th which is necessarily positive since the coordinate sum of $\log(u_i)$ is 0. Then, take the square matrix

$$M = \begin{pmatrix} \log(u_1) \\ \hline \log(u_2) \\ \hline \vdots \\ \hline \log(u_{r+s}) \end{pmatrix} = (c_1 | c_2 | \cdots | c_{r+s})$$

We note that the sum of the columns $\sum_i c_i$ is 0 so M can have rank at most $r+s-1$. Assume the first $r+s-1$ columns are linearly dependent, and without loss of generality that c_1 has the largest coefficient in a relation of linear dependence. Then, after normalizing, we can write $c_1 + t_2 c_2 + \cdots + t_{r+s-1} c_{r+s-1} = 0$ where $t_i \leq 1$, are not all 0. Considering the first row in this equation and recalling that $\log(u_1) = (\log(u_1)_1, \cdots \log(u_1)_{r+s})$ has coordinate sum 0 and is only non-negative in its first coordinate, we get a contradiction.

$$\begin{aligned} 0 = \log(u_1)_1 + \sum_{j=2}^{r+s-1} t_j \log(u_1)_j &= |\log(u_1)_1| - \sum_{j=2}^{r+s-1} t_j |\log(u_1)_j| \\ &\geq |\log(u_1)_1| - \sum_{j=2}^{r+s-1} |\log(u_1)_j| \quad (\text{since } t_j \leq 1) \\ &> |\log(u_1)_1| - \sum_{j=2}^{r+s} |\log(u_1)_j| = \sum_{j=1}^{r+s} \log(u_1)_j = 0 \end{aligned}$$

Therefore, M has rank $r+s-1$, and as a result V is of rank $r+s-1$. □

As in the quadratic case, our goal of counting ideals in a certain class $\mathcal{C}$ that are bounded by t can be rephrased in a different context. It is equivalent to finding a subset of orbit representatives for $U \subset R$, and then counting the elements of J in this subset whose norm is bounded by $t||J||$. Again, it is easier to simplify the structure of U by working with a subset of orbit representatives for V and accounting for the $|W|$ factor in the final tally.

We can view $\wedge_R$ as a subset of $(\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$ in order to benefit from their multiplicative group structure. Then, we can adjust our earlier log mapping accordingly to preserve it.

$$V \subset R \setminus \{0\} \overset{\phi}{\hookrightarrow} V' \subset (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \qquad \overset{\mathcal{L}}{\hookrightarrow} \wedge_U \subset H = \{z_1 + \cdots + z_{r+s} = 0\} \subset \mathbb{R}^{r+s}$$

$$\alpha \mapsto \Big(\sigma_1(\alpha), \cdots, \tau_1(\alpha), \cdots\Big) \mapsto \Big(\log|\sigma_1(\alpha)|, \cdots, 2\log|\tau_1(\alpha)|, \cdots\Big)$$

We know from the earlier proof that the this is in fact an isomorphism since the generators of V map to the $\mathbb{Z}$-basis of $\wedge_U$. Therefore, a set of orbit representatives for the elements of the group V acting on R through multiplication maps isomorphically to a set of orbit representatives for the subgroup V', a fundamental domain D for V'. And using the fact that J maps isomorphically to $\wedge_J$, we can undergo our counting process in $(\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$ instead.

In this scenario, our task has become counting the lattice elements of $\wedge_J$ inside D whose "equivalent" norm obeys $N(x) \leq t||J||$. More precisely, $N(x)$ is the same map on $\mathbb{R}^n$ from above but adjusted to our new viewpoint of $(\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$. So,

$$N(x_1, \cdots, x_r, z_1, \cdots, z_s) = x_1 \cdots x_s |z_1|^2 \cdots |z_s|^2$$

We recall our two lemmas from the quadratic case.

Lemma 4.10 (A)**.** Given a homomorphism of abelian groups, $f : G \to G'$, and a subgroup S of G that is isomorphic to its image S' in G', then the pre-image of a set of coset representatives for S' is a set of coset representatives for S.

Lemma 4.11 (B)**.** Given a lattice $\wedge$ in $\mathbb{R}^n$ and a bounded subset D of $\mathbb{R}^n$ such that its boundary ∂B is piecewise-smooth, then for $a \in \mathbb{R}$

$$\big| \wedge \cap aB \big| = a^n \frac{\text{vol}(B)}{\text{vol}(\mathbb{R}^n/\wedge)} + O(a^{n-1})$$

The proof of Lemma B is exactly identical to the earlier proof, but with the dimensions properly adjusted.

Applying Lemma A to

$$f = \mathcal{L} : S = V' \subset G = (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \to S' = \wedge_U \subset G' = \mathbb{R}^{r+s}$$

we see that it it suffices to find a set of orbit representatives D' for $\wedge_U \subset H \subset \mathbb{R}^{r+s}$, and $D = f^{-1}(D')$ will be our desired set. Fix a fundamental parallelotope F for $\wedge_U$, then as in the quadratic case, we can take D' to be the sum of F and $\mathbb{R}v$ for a vector $v \notin H$. Then,

$$D = \log^{-1}(F \oplus \mathbb{R}v) = \big\{x \in (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \big| \log(x) \in F \oplus \mathbb{R}v\big\}$$

In order to preserve the homogeneity of D as in the quadratic case, we may take

$$v = (1, \overset{r \text{ times}}{\cdots}, 1, 2, \overset{s \text{ times}}{\cdots}, 2)$$

Then, we get that for any $x \in D$,and non-zero $a \in \mathbb{R}$,

$\log(ax) = \log(a) + \log(x) = \log|a|v + f + cv = f + (\log|a| + c)v$ for some $f \in F, c \in V$

which shows that D is homogenous. Taking $D_a = D \bigcap \{|N(x)| \leq a\}$, if we are able to apply Lemma B with $B = D_1$ and use the same line of reasoning as earlier, we deduce that

$$\begin{aligned} |W| \cdot \mathcal{F}(\mathcal{C}, t) &= \left| \wedge_J \bigcap D_{t||J||} \right| = \left| \wedge_J \bigcap \sqrt[n]{(t||J||)} D_1 \right| \\ &= \frac{\text{vol}(D_1)||J||}{\text{vol}(\mathbb{R}^n/\wedge_J)} t + O((t||J||)^{(n-1)/n}) = \frac{\text{vol}(D_1)||J||}{\text{vol}(\mathbb{R}^n/\wedge_R)} t + O(t^{1-1/n}) \end{aligned}$$

which proves our theorem with

$$\kappa = \frac{2^s \mathrm{vol}(D_1)}{|W|\sqrt{|\mathrm{disc}(R)|}}$$

Therefore, the final step is verifying that the boundary of D_1 is indeed Lipschitz-parametrizable, and then calculating its volume.

We recall that

$$D_1 = \left\{x \in (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \middle| \log(x) \in F \oplus \mathbb{R}v \text{ and } |N(x)| \leq 1\right\}$$

where F is a fundamental parallelotope for $\wedge_U$ and $v = (1, \overset{r \text{ times}}{\cdots}, 1, 2, \overset{s \text{ times}}{\cdots}, 2)$. We simplify D_1 in two respects. First, note that for $x \in D_1$, we have

$$\log(x) = (\log|x_1|, \cdots,\ \log|x_r|, 2\ \log|z_1|, \cdots, 2\ \log|z_s|) = f + av \quad \text{for } f \in F, a \in V$$

Then, by the homomorphism properties of the log, we may express the coordinate sum of $\log(x)$ as

$$\sum_{i=1}^{r} \log|x_i| + \sum_{j=1}^{s} 2\log|z_j| = \log\left(|x_1|\cdots|x_r| \cdot |z_1|^2 \cdots |z_s|^2\right) = \log(|N(x)|) \leq 0$$

where the inequality follows since $|N(x)| \leq 1$. On the other hand, this is equal to the coordinate sum of $f + a$ which is $(r + 2s)a$ since $f \in \wedge_U \subset H$ has coordinate sum 0. Therefore, $a \leq 0$. So, D_1 can be more precisely described as

$$D_1 = \left\{x \in (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \middle| \log(x) \in F \oplus (-\infty, 0]v \text{ and } |N(x)| \leq 1\right\}$$

Our next simplification follows from noting that our log mapping is even with respect to the real coordinates $x_1, \cdots, x_r$ since it does not depend on their signs. So, we may express D_1 as the union of 2^r identical regions, where each element $\gamma = (\gamma_1, \cdots, \gamma_r) \in \{-1, 1\}^r$ corresponds to

$$D_\gamma = D_1 \bigcap \{\gamma_i x_i \leq 0 \big| i = 1, \cdots, r\}$$

Note also that the regions D_γ are disjoint since the conjugates of a non-zero element $x \in R \setminus \{0\}$ must be non-zero. Therefore, it suffices to show that one of D_γ is Lipschitz-parametrizable and the volume of D_1 would be 2^r vol (D_γ). We take $\gamma = (1, \cdots, 1)$ for simplicity and denote the region D_1^+. We will now proceed to parametrize its boundary by first parametrizing all of D_1^+ by a half-open cube in $\mathbb{R}^n$, and then letting the parametrization extend to the boundary. We fix a $\mathbb{Z}$-basis $\{v_1, \cdots, v_{r+s-1}\}$ for $\wedge_U \subset \mathbb{R}^{r+s}$, so the fundamental parallelotope F can be described by

$$F = \left\{ \sum_{k=1}^{r+s-1} t_k v_k \big| 0 \leq t_k < 1 \right\}$$

For every k, we write $v_k = (v_k^1, \cdots, v_k^{r+s})$. Then, using polar coordinates, any $x = (x_1, \cdots, x_r, \rho_1 e^{i\theta_1}, \cdots, \rho_s e^{i\theta_s}) \in D_1^+$ where $\theta_j \in (0, 2\pi]$ can be described by the equations

$$\begin{aligned}
\log(x_1) &= \sum_{k=1}^{r+s-1} t_k v_k^1 + a \\
&\vdots \\
\log(x_r) &= \sum_{k=1}^{r+s-1} t_k v_k^r + a \\
\log(2\rho_1) &= \sum_{k=1}^{r+s-1} t_k v_k^{r+1} + 2a \\
&\vdots \\
\log(2\rho_s) &= \sum_{k=1}^{r+s-1} t_k v_k^{r+s} + 2a
\end{aligned}$$

where $t_k \in [0,1)$ for $1 \leq k \leq r+s-1$ and $a \leq 0$.

Let $t_{r+s} = e^a \in (0,1]$ and $t_{r+s+j} = \theta_j/2\pi \in (0,1]$ for $j = 1, \cdots, s$. Then, exponentiating the equations above yields a parametrization of D_1^+ given by the restriction of f to $[0,1)^{r+s-1} \times (0,1]^{s+1}$, where

$$\begin{array}{rcccl} f: & [0,1]^n & \overset{f_1}{\to} & \mathbb{R}^n & \overset{f_2}{\to} \mathbb{R}^r \times \mathbb{C}^s \\ & (t_1, \cdots, t_{r+2s}) & \mapsto & (g_1, \cdots, g_n) & \to (g_1, \cdots, g_r, g_{r+1}e^{ig_{r+s+1}}, \cdots) \end{array}$$

and

$$g_j = \begin{cases} t_{r+s} \exp\left(\sum_{k=1}^{r+s-1} t_k v_k^j\right) & 1 \leq j \leq r \\ t_{r+s} \exp\left(\frac{1}{2}\sum_{k=1}^{r+s-1} t_k v_k^j\right) & r < j \leq r+s \\ 2\pi t_j & r+s < j \leq n \end{cases}$$

Then, the Jacobian $(\partial g_j/\partial t_k)$ of f_1 above is given by

$$J = \left(\begin{array}{cccccccccc} v_1^1 g_1 & \cdots & v_1^r g_r & \frac{1}{2}v_1^{r+1} g_{r+1} & \cdots & \frac{1}{2}v_1^{r+s} g_{r+s} & & & & \\ \vdots & & \vdots & \vdots & & \vdots & & \mathbf{0} & & \\ v_{r+s-1}^1 g_1 & \cdots & v_{r+s-1}^r g_r & \frac{1}{2}v_{r+s-1}^{r+1} g_{r+1} & \cdots & \frac{1}{2}v_{r+s-1}^{r+s} g_{r+s} & & & & \\ & & & & & & & & & \\ g_1/t_{r+s} & \cdots & g_r/t_{r+s} & g_{r+1}/t_{r+s} & \cdots & \cdots g_{r+s}/t_{r+s} & & & & \\ & & & & & & 2\pi & & & \\ & & & & & & & 2\pi & & \\ & & & \mathbf{0} & & & & & \ddots & \\ & & & & & & & & & 2\pi \end{array}\right)$$

We note the following.

i. All the partial derivatives are continuous, and therefore f_1 is smooth.

Moreover, polar transformations are smooth by the same reasoning since their components $(x\cos(y), ix\cos(y))$ have continuous derivatives. Then, f_2 is smooth and therefore f as a whole is smooth in each of its components.

ii. We claim that f is an open map since both f_1 and f_2 are open. The log and exponential functions map open intervals to open intervals on the real-line, and the polar transformation maps a product of open intervals in $\mathbb{R}^2$ to a sector of a circle in $\mathbb{C}$. Therefore, recalling that the product of open intervals is a basis for the product topology on $\mathbb{R}^n$, we may deduce that f_2 as well as the maps below are open.

$$\begin{aligned} &h : (x_1, \cdots, x_n) \to (x_1, \cdots, x_{r+s-1}, \log(x_{r+s}), x_{r+s+1}, \cdots, x_n) \\ &g : (x_1, \cdots, x_n) \to (e^{x_1}, \cdots, e^{x_r}, \frac{1}{2}e^{x_{r+1}}, \cdots, 1/2e^{x_{r+s}}, 2\pi x_{r+s+1}, \cdots, 2\pi x_n) \end{aligned}$$

Then, it's clear that f_1 can be written as the composition $h \circ M \circ g$, where M is the linear transformation given by

$$\begin{pmatrix} v_1 & \\ \ldots & 0 \\ v_{r+s-1} & \\ v & \\ & \\ 0 & 1 \end{pmatrix}$$

We know that the rows are linearly independent, so M is clearly invertible and thus open. Therefore, f is open.

iii. Note that $f([0,1]^n) = \overline{D_1}^+$ since the f is compact so the image must be a compact set containing D_1^+. On the other hand, we know that the half open cube $[0,1)^{r+s-1} \times (0,1]^{s+1}$ is dense in $[0,1]^n$ and maps to D_1. Therefore, D_1 is dense in the image, from which the statement follows. Since f is open, we conclude that the boundary of the n-cube is mapped onto a set containing the boundary $B = \partial D_1$. The boundary of the n-cube consists of $2n(n-1)$ cubes. It follows by $(i.)$ that the boundary B is piecewise smooth. So, we may apply Lemma B as claimed.

Note that for $j \leq r+s$ column j is multiplied by g_j, and row $r+s$ is divided by t_{r+s}. So, using basic properties of determinants and multiplying the s columns $r+1$ through $r+s$ by 2 , we may express

$$\det(J) = \frac{(2\pi)^s g_1 \cdots g_{r+s}}{t_{r+s}} \cdot \frac{n}{2^s} \begin{vmatrix} v_1 \\ \vdots \\ v_{r+s-1} \\ \\ \frac{1}{n} v \end{vmatrix} = \frac{\pi^s f_1 \cdots g_{r+s}}{t_{r+s}} \cdot n \cdot \operatorname{reg}(R)$$

where the middle determinant is called the regulator of R and expressed as $\operatorname{reg}(R)$.This allows us to nicely compute the volume of D_1^+. Using the formula for change of polar coordinates, we have

$$\operatorname{vol}(D_1^+) = \int_{D_1^+} \mathrm{d}x_1 \cdots \mathrm{d}x_r \rho_1 \mathrm{d}\rho_1 \mathrm{d}\theta_1 \cdots \rho_s \mathrm{d}\rho_s \mathrm{d}\theta_s$$

Then, using the map f_1 from above and the determinant of the Jacobian, this becomes

$$\mathrm{vol}(D_1^+) = n\pi^s \cdot \mathrm{reg}(R) \int_{[0,1]^n} \frac{f_1 \cdots f_r f_{r+1}^2 \cdots f_{r+s}^2}{t_{r+s}} \mathrm{d}t_1 \cdots \mathrm{d}t_n$$

Finally, note that by definition of the functions g_i,

$$g_1 \cdots g_r g_{r+1}^2 \cdots g_{r+s}^2 = t_{r+s}^n \cdot \exp\left(\sum_{j=1}^{r+s} \sum_{k=1}^{r+s-1} t_k v_k^j\right) = t_{r+s}^n \cdot \exp\left(\sum_{k=1}^{r+s-1} t_k \sum_{j=1}^{r+s} v_k^j\right)$$

The innermost sum is 0 for all k since the vectors v_k have coordinate sum 0. Then, putting it all together ,

$$\mathrm{vol}(D_1^+) = \pi^s \mathrm{reg}(R) \cdot n \int_0^1 t_{r+s}^{n-1} \mathrm{d}t_{r+s} \cdot \int_{[0,1]^{n-1}} \mathrm{d}t_1 \cdots \mathrm{d}t_{r+s-1} \mathrm{d}t_{r+s+1} \cdots \mathrm{d}t_n = \pi^s \mathrm{reg}(R)$$

Thus, we have proved theorem 4.1, and also proved that

$$\kappa = \frac{2^{r+s}\pi^s \mathrm{Reg}(R)}{|W|\sqrt{|\mathrm{disc}(R)|}}$$

Chapter 5

Class Number Formula

In this final chapter, we will use the result on the distribution of ideals to define and study the Dedekind Zeta function of a number field K. We will express the class number h in terms of this function, and compute a simplified form for h in the case of quadratic fields.

5.1 Dedekind Zeta Functions

The Dedekind Zeta Function of a number field K is defined as

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{j_n}{n_s} \qquad \Re(s) > 1$$

where j_n is the number of ideals in $R = \mathbb{A} \cap K$ with $\big|\big|I\big|\big| = n$. This function is well-defined and analytic on the half-plane $\Re(s) > 1$ due to the following convergence proposition.

Proposition 5.1. Given the Dirichlet Series

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad a_n, s \in \mathbb{C}$$

such that $\left|\sum_{n=1}^{t} a_n\right| = O(t^r)$, then f converges and is analytic on the half-plane $\Re s > r$.

Proof. See Serre [4] p. 66. □

By theorem 4.1, we know that $\sum_{n=1}^{t} j_n = \mathcal{F}(t) \sim h\kappa t$. Then, applying the proposition to our Zeta functions establishes their convergence on the half-plane $x > 1$. When $K = \mathbb{Z}$, $j_n = 1$ since there is exactly one ideal of size n in $\mathbb{Z}$. In the case, we get the Riemann Zeta function

$$\zeta_(s) := \zeta_{\mathbb{Z}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

We will extend ζ_K to a meromorphic function on the half-plane $x > 1 - [K : \mathbb{Q}]$. To do so, we will first need to extend ζ. We do so by considering the two series

$$f(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots \quad ; \quad g(s) = 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + \cdots$$

It is clear that f, g converge to analytic functions for $x > 0$ by 5.1. Moreover, for $x > 1$, by absolute convergence, we may write

$$f(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} - 2\sum_{n=1}^{\infty} \frac{1}{(2n)^s} = (1 - 2^{1-s})\zeta(s)$$

$$g(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} - 3\sum_{n=1}^{\infty} \frac{1}{(3n)^s} = (1 - 3^{1-s})\zeta(s)$$

This allows us to extend ζ to a meromorphic function on $x > 0$ in two different ways.

$$\zeta(s) = \frac{f(s)}{1 - 2^{1-s}} \quad ; \quad \zeta(s) = \frac{g(s)}{1 - 3^{1-s}}$$

f is analytic on the half-plane $x > 0$, so the only possible poles of $f(s)/(1 - 2^{1-s})$

are the simple poles at the points where

$$2^{1-s} = 1 \implies e^{(1-s)\log(2)} = 1 \implies s := s_k = 1 + \frac{2k\pi i}{\log(2)} \quad ; \quad k \in \mathbb{Z}$$

However, it turns out that for $k \neq 0, f(s_k) = 0$ cancelling out the simple pole of the denominator. This can be observed by noting that the only possible poles of $g(s)/(1 - 3^{1-s})$ lie at $t_k = 1 + \frac{2k\pi i}{\log(3)}$ which only coincide with s_k for $k = 0$. ($\log(2)/\log(3)$ is irrational). Hence, for $k \neq 0$,

$$\lim_{\substack{x \to 1^+ \\ s = x + \frac{2k\pi i}{\log(2)}}} \frac{g(s)}{1 - 3^{1-s}} = \zeta(s) = \lim_{\substack{x \to 1^+ \\ s = x + \frac{2k\pi i}{\log(2)}}} \frac{f(s)}{1 - 2^{1-s}}$$

which implies that $f(s)/(1 - 2^{1-s})$ has no poles except at $s = 1$ since $f(1) = \log(1/2) \neq 0$. We take this as the extension of ζ and use it to extend ζ_K. For $x > 1$, by absolute convergence, we have

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{j_n - h\kappa + h\kappa}{n^s} = \sum_{n=1}^{\infty} \frac{j_n - h\kappa}{n^s} + h\kappa\zeta(s)$$

By theorem **??** and proposition 5.1, the Dirichlet series converges to an analytic function on the half-plane $x > 1 - \frac{1}{[K;\mathbb{Q}]}$. Combining this with the extension of ζ leads to our desired extension of ζ_K on $x > 1 - \frac{1}{[K;\mathbb{Q}]}$, which is analytic everywhere except at $s = 1$.

Our goal is to find an equation for h, the class number of our field. Rearranging the above, we may write

$$h\kappa = \frac{\zeta_K(s)}{\kappa\zeta(s)} - \frac{\sum_{n=1}^{\infty} \frac{j_n - h\kappa}{n^s}}{\zeta(s)}$$

The Dirichlet series converges in the half-plane $x > 1 - \dfrac{1}{[K:\mathbb{Q}]}$, specifically at $s = 1$. Meanwhile, ζ has a simple pole at $s = 1$. Therefore, taking the limit as $s \to 1^+$, we deduce that

$$h = \lim_{s \to 1^+} \frac{\zeta_K(s)}{\kappa \zeta(s)}$$

Note from the definition that the residue of ζ at $s = 1$, $\mathrm{Res}(\zeta, 1) = 1$. Therefore, combining this with the value of κ obtained in theorem **??**, we get the class number formula in its most general form

$$h = \frac{|W|\sqrt{|\mathrm{disc}(R)|}}{2^{r+s}\pi^s \mathrm{Reg}(R)} \cdot \lim_{s \to 1^+} (s-1)\zeta_K(s)$$

In what remains, we will obtain a formula for h assuming K is an abelian extension of $\mathbb{Q}$. Equivalently, by the Kronecker-Weber theorem [1], K is contained in some cyclotomic field $\mathbb{Q}[\omega], \omega = e^{2\pi i/m}$. In order to benefit from this structure of K, we will first need to define explore characters of finite abelian groups.

5.2 Characters of Finite Abelian Groups

Let G be a finite abelian group. Then , we define

Definition 5.2. A *character* of G is a homomorphism $\chi : G \to \mathbb{C}^*$, the non-zero complex numbers.

The simplest example of a character is the principal character $\chi_0 = 1$. It acts like the identity element since the characters of G form a group under multiplication, which we denote by $\hat{G}$, with $\chi^{-1} = 1/\chi$. In fact,

Proposition 5.3. $G \cong \hat{G}$

Proof. We will first prove the proposition for finite cyclic groups. Suppose $G = \langle a \rangle$ is cyclic of order n. Then, since χ is a homomorphism, $\chi(a)^n = \chi(a^n) = \chi(e) = 1$.

Therefore, $\chi(a)$ is an nth roof of unity. On the other hand, every nth root of unity ω defines a character of G by $\chi(a) = \omega$. Therefore, $\hat{G}$ is also cyclic of order n since it's isomorphic to the group of nth roots of unity.

In order to prove the general case, we need to show that given any two finite abelian groups G, H, the map $\psi : \hat{G} \times \hat{H} \to \widehat{G \times H}$ defined by $\psi(\chi_1, \chi_2)(g \cdot h) = \chi_1(g)\chi_2(h)$ is an isomorphism. It is easy to check that ψ is an injective homomorphism. Moreover, given a character $\chi \in \widehat{G \times H}$, define $\chi_1(g) = \chi(g \cdot e_H), \chi_2(h) = \chi(e_g \cdot h)$ which belong to $\hat{G}$ and $\hat{H}$ respectively. Then, $\psi(\chi_1, \chi_2)(gh) = \chi_1(g)\chi_2(h) = \chi(ge_H)\chi(e_G h) = \chi(gh)$. Therefore, ψ is surjective.

Summing it up, given any finite abelian group G, we may write $G = G_1 \times \cdots \times G_n$ by the fundamental theorem of finite abelian groups (Jacobson [2] p. 188). Then, $\hat{G} \cong \hat{G}_1 \times \cdots \hat{G}_n \cong G_1 \times \cdots \times G_n = G$.

□

We have simultaneously proved the following important proposition.

Properties 5.4. Suppose G is cyclic of order n, and write $G = \langle a \rangle$. Then, $\hat{G} = \left\{ \chi_k(a^m) = e^{2\pi i k m/n} \middle| 0 \leq k \leq n-1 \right\}$.

Corollary 5.5. Suppose G is cyclic of order n. Then,

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} n & ; \quad g = e \\ 0 & ; \quad g \neq e \end{cases} \quad ; \quad \sum_{g \in G} \chi(g) = \begin{cases} n & ; \quad \chi = \chi_0 \\ 0 & ; \quad \chi \neq \chi_0 \end{cases}$$

Proof. For $g = a^m$, let $d = \gcd(m, n)$ and $f = n/d = |\langle g \rangle|$ be the order of g. Consider the evaluation map $\epsilon : \hat{G} \to \mathbb{C}$ given by $\epsilon(\chi) = \chi(g)$. It is clear that the kernel of ϵ consists of characters which map g to 1. Therefore, it is in bijection with the character group $\widehat{G/\langle g \rangle}$. By 5.3, this has order $|G|/f$. Therefore, the image must consist of all the f-roots of 1. Hence, the first sum would consist of d copies of the f-th roots of unity. Those roots sum up to the trace of the polynomial $x^f - 1$ which is the opposite of the $(f-1)$th coefficient. This is 0 except for the case when $f = 1$, in which case the trace is 1 and the sum is $d = n$.

Similarly, for χ_k, letting $d = \gcd(k, n)$, the first sum would consist of d copies of the n/d-th roots of unity. Those roots sum up to the trace of $x^{n/d} - 1$ which is 0 whenever $d < n$. □

For reasons that will soon become clear, we are interested in a special family of characters, known as *Dirichlet characters.* Let $\mathbb{T}$ denote the unit circle $\{|z| = 1\} \subset \mathbb{C}$.

Definition 5.6. A *Dirichlet character* mod m is a homomorphism $\chi : \mathbb{Z}_m^* \to \mathbb{T}$. Every character mod m has a natural extension to the natural numbers which we also denote by χ, defined as

$$\chi(n) = \begin{cases} \chi([n]_m) = \chi(\overline{n}) & \gcd(m,n) = 1 \\ 0 & \gcd(m,n) = 1 \end{cases}$$

We are now ready to define L-series which we will use to compute ζ_K in a more efficient manner.

5.3 Computing ζ_K in terms of L-series

Definition 5.7. An L-series is a Dirichlet series whose coefficients correspond to characters. We write

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

where $s \in \mathbb{C}$ and χ is a character mod m.

It is clear by proposition 5.1 as well as corollary 5.5 that $L(s,\chi)$ converges on the half-plane $x > 1$ since $\sum_{n=1}^{t} \chi(n) \leq t$. We will need the following lemma concerning "Euler Products" from Marcus [1] p.133.

Lemma 5.8. Let $a_1, a_2 \cdots \in \mathbb{C}$ such that $|a_i| < 1$ and the $\sum_{i=1}^{\infty} |a_i|$ converges. Then,

$$\prod_{i=1}^{\infty} \frac{1}{1-a_i} = 1 + \sum_{j=1}^{\infty} \sum_{(r_1,\cdots,r_j)} a_1^{r_1} \cdots a_j^{r_j}$$

where the second sum is taken over all $(r_1, \cdots, r_j) \in \mathbb{N}_0^{j-1} \times \mathbb{N}$.

Recalling that χ is multiplicative and applying the lemma with the set $\{\chi(p)/p^s \mid p \text{ prime}\}$, we may write

$$L(s,\chi) = \prod_{p \text{ prime}} \frac{1}{1 - \frac{\chi(p)}{p^s}} = \prod_{p \nmid m} \frac{1}{1 - \frac{\chi(p)}{p^s}} \tag{5.3.1}$$

where the latter equality follows since $\chi(p) = 0$ whenever $(p,m) > 1$. Recall that we are interested in refining our class number formula for the case where K is a finite abelian extension. We admit the Kronecker-Weber theorem (Washington [3] p. 319) which asserts that this is equivalent to $K \subseteq \mathbb{Q}[\omega], \omega = e^{2\pi i/m}$ for some m. We assume without loss of generality that every prime $p \mid m$ is ramified in K. If $p \mid m$ is not ramified, then we have $K \subset \mathbb{Q}[\tilde{\omega}], \tilde{\omega} = e^{2\pi i/m'}$ where $m' = m/p^k$ and p^k is the highest power of p dividing m.

Then, the Galois group of K, $G = Gal(K/\mathbb{Q})$ is a quotient group of $Gal(\mathbb{Q}[\omega]/\mathbb{Q})$. We know that the latter is identified with $\mathbb{Z}_m^*$ by mapping $a \in \mathbb{Z}_m^*$ to the embedding $\omega \to \omega^a$. Therefore, G can be identified with a a subgroup of $\mathbb{Z}_m^*$, i.e. there exists a surjective homomorphism $\phi : \mathbb{Z}_m^* \to G$. Then, we can view characters of G as characters mod m by composing them with ϕ. So, we consider $\hat{G}$ to be a subgroup of $\widehat{\mathbb{Z}_m^*}$.

We will prove the following theorem.

Theorem 5.9.

$$h = \frac{1}{\kappa}\prod_{p|m}\left(1-\frac{1}{p^s}\right)\left(1-\frac{1}{p^{f_p s}}\right)^{-r_p}\prod_{\substack{\chi\in\hat{G}\\ \chi\neq 1}} L(1,\chi)$$

where r_p is the number of primes in $R = \mathbb{A}_K$ lying over p and f_p is the inertial degree of those primes.

Proof. Recall that by definition

$$\zeta_K(s) = \sum_{n=1}^{\infty}\frac{j_n}{n^s}$$

where j_n is the number of ideals of size n. Since this is absolutely convergent for $x > 1$, then we can rewrite this as

$$\zeta_K(s) = \sum_{n=1}^{\infty}\sum_{||I||=n}\frac{1}{\big|\big|I\big|\big|^s} = \sum_{I\neq 0}\frac{1}{\big|\big|I\big|\big|^s} \text{ for } x > 1$$

By unique factorization into prime ideals, and the fact that $\big|\big|\cdot\big|\big|$ is multiplicative, we may apply lemma 5.8 to the set $\{1/||P|| \mid P \text{ prime in } R\}$ to get

$$\zeta_K(s) = \sum_P\left(1+\frac{1}{||P||^s}+\frac{1}{||P||^{2s}}+\cdots\right) = \sum_P\frac{1}{1-\frac{1}{||P||^s}}$$

For $p\in\mathbb{Z}$, and P lying over p, we have $\big|\big|P\big|\big| = p^{f(P|p)}$. However, since the extension is Galois, then $f(P|p)$ is constant for all P. So , we denote it by f_p. Therefore, for $x > 1$, we can write

$$\zeta_K(s) = \prod_p\left(\frac{1}{1-\frac{1}{p^{f_p s}}}\right)^{r_p}$$

As discussed earlier, characters of $G = \text{Gal}(K/\mathbb{Q})$ can be viewed as characters mod m. Subsequently, $\hat{G}$ is a subgroup of $\widehat{\mathbb{Z}_m^*}$.

Fix a $p \nmid m$, and consider $\{\chi(p) \mid \chi \in \hat{G}\}$. Under the canonical homomorphism $\psi : \mathbb{Z}_m^* \to G$ that maps a to the embedding $\omega \to \omega^a$, $\chi(p)$ runs through the f-th roots of 1 where $f = |\langle \psi(p) \rangle|$ is the order of $\psi(p)$ in G. By proposition, **??** $f = f_p$, from which it follows that $\{\chi(p) \mid \chi \in \hat{G}\}$ is exactly $|G|/f_p$ copies of the f_pth roots of 1. However, since p is unramified, then $e(P|p) = 1$ for all P lying over p. It follows that $|G|/f_p = n/f_p = r_p$ the number of primes lying over p. Combining this with the fact that

$$x^{f_p} - c^{f_p} = \prod_{\omega^{f_p}=1} (x - \omega c) \implies 1 - \frac{1}{p^{f_p s}} = \prod_{\omega^{f_p}=1} \left(1 - \frac{\omega}{p^{f_p s}}\right)$$

we deduce that

$$\prod_{\chi \in \hat{G}} \left(1 - \frac{\chi(p)}{p^s}\right) = \prod_{\omega^{f_p}=1} \left(1 - \frac{\omega}{p^{f_p s}}\right)^{r_p} = \left(\frac{1}{1 - \frac{1}{p^{f_p s}}}\right)^{r_p}$$

It follows by equation 5.3.1 that for $x > 1$, using absolute convergence

$$\prod_{\chi \in \hat{G}} L(s, \chi) = \prod_{\chi \in \hat{G}} \prod_{p \nmid m} \left(1 - \frac{\chi(p)}{p^s}\right) = \prod_{p \nmid m} \prod_{\chi \in \hat{G}} \left(1 - \frac{\chi(p)}{p^s}\right) = \prod_{p \nmid m} \left(\frac{1}{1 - \frac{1}{p^{f_p s}}}\right)^{r_p}$$

We may also use equation 5.3.1 in addition to lemma 5.8 to conclude that for $\chi = 1$,

$$L(s, 1) = \prod_{p \nmid m} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p | m} \left(1 - \frac{1}{p^s}\right) = \zeta(s) \prod_{p | m} \left(1 - \frac{1}{p^s}\right)$$

Combining the above, we get

$$\begin{aligned}\zeta_K(s) &= \prod_{p|m} \left(\frac{1}{1 - \frac{1}{p^{f_p s}}}\right)^{r_p} \prod_{p \nmid m} \left(\frac{1}{1 - \frac{1}{p^{f_p s}}}\right)^{r_p} = \prod_{p|m} \left(\frac{1}{1 - \frac{1}{p^{f_p s}}}\right)^{r_p} \prod_{\chi \in \hat{G}} L(s, \chi) \\ &= \prod_{p|m} \left(\frac{1}{1 - \frac{1}{p^{f_p s}}}\right)^{r_p} \prod_{\substack{\chi \in \hat{G} \\ \chi \neq 1}} L(s, \chi) \cdot L(s, 1)\end{aligned}$$

Therefore,

$$\frac{\zeta_K(s)}{\zeta(s)} = \prod_{p|m}\left(\frac{1}{1-\frac{1}{p^{f_p s}}}\right)^{r_p}\left(1-\frac{1}{p^s}\right)\prod_{\substack{\chi\in\hat{G}\\ \chi\neq 1}} L(s,\chi)$$

Since $\chi \neq 1$, then it follows by 5.5 that $\sum_{n=1}^{t}\chi(n) \leq m$. Therefore, $L(1,\chi)$ converges for $x > 0$. Then, taking $s = 1$ proves the theorem. □

Proposition 5.10. Let $\mathcal{X}$ be a non-trivial character $\mod m$. Then,

$$L(1,\chi) = -\frac{1}{m}\sum_{k=1}^{m-1}\tau_k(\chi)\text{log}(1-w^{-k})$$

where $\omega = e^{2\pi i/m}$ and $\tau_k(\chi) = \sum_{a\in\mathbb{Z}_m^*}\chi(a)w^{ak}$ and we take the principal branch of $\log(z)$ for $z \in \mathbb{C}$.

Proof. By definition, for s in the half-plane $x > 1$,

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

If two indices m, n are equal mod m, i.e. $\overline{n} = \overline{m} = a$, then $\chi(n) = \chi(m) = \chi(a)$. So, recalling that $\chi(a) = 0$ when $(a, m) > 1$, we write

$$L(s,\chi) = \sum_{a=1}^{m-1}\chi(a)\sum_{\substack{\overline{n}=a\\ n\geq 1}}\frac{1}{n^s} = \sum_{a\in\mathbb{Z}_m^*}\chi(a)\sum_{\substack{\overline{n}=a\\ n\geq 1}}\frac{1}{n^s} \tag{1}$$

Given $a \in \mathbb{Z}_m^*$, consider the function

$$\Omega_a(n) = \frac{1}{m}\sum_{k=0}^{m-1}\omega^{(a-n)k}$$

When $\overline{n} = a$, $(a-n) = dm$ for some $d \in \mathbb{Z}$. Therefore,

$$\Omega_a(n) = \frac{1}{m}\sum_{k=0}^{m-1} \omega^{(a-n)k} = \frac{1}{m}\sum_{k=0}^{m-1} e^{2\pi idk} = \frac{1}{m}\sum_{k=0}^{m-1} 1 = 1$$

Otherwise $(a-n, m) = d < m$, so letting G be the group of m/d-th roots of unity, we may write by 5.5

$$\Omega_a(n) = \frac{d}{m}\sum_{\chi \in G} \chi(g) \text{ for some } g \neq e$$

It follows that

$$\Omega_a(n) = \begin{cases} 1 & \overline{n} = a \\ 0 & \overline{n} \neq a \end{cases} \implies \sum_{\substack{\overline{n}=a \\ n \geq 1}} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{\Omega_a(n)}{n^s}$$

Substituting in (1), we get

$$L(s,\chi) = \sum_{a \in \mathbb{Z}_m^*} \chi(a) \sum_{n=1}^{\infty} \frac{\Omega_a(n)}{n^s} = \frac{1}{m}\sum_{a \in \mathbb{Z}_m^*} \chi(a) \sum_{n=1}^{\infty} \frac{\sum_{k=0}^{m-1} \omega^{(a-n)k}}{n^s} \tag{2}$$

The infinite series is absolutely convergent for $x > 1$ since its numerator is bounded. So, we may interchange the order of summation to get

$$L(s,\chi) = \frac{1}{m}\sum_{a \in \mathbb{Z}_m^*} \chi(a) \sum_{k=0}^{m-1}\sum_{n.=1}^{\infty} \frac{\omega^{(a-n)k}}{n^s} = \frac{1}{m}\sum_{k=0}^{m-1} \left(\sum_{a \in \mathbb{Z}_m^*} \chi(a)\omega^{ak} \right) \sum_{n=1}^{\infty} \frac{\omega^{-nk}}{n^s}$$

Note that $\tau_0(\chi) = \sum_{a \in \mathbb{Z}_m^*} \chi(a) = 0$ by 5.5. We need to consider the Dirichlet series

$$\sum_{n=1}^{\infty} \frac{\omega^{-nk}}{n^s} = \sum_{n=1}^{\infty} \frac{(\omega^{-k})^n}{n^s}$$

for $1 \leq k \leq m-1$. As before, we have $\sum_{n=1}^{t} \omega^{-nk} \leq m$ is bounded for all t. Then, the series converges for $x > 0$. Therefore, we can now substitute $s = 1$, and use the power series representation

$$\log(1-z) = -\sum_{n=1}^{\infty} \frac{z^n}{n} \quad ; \quad |z| < 1,$$

to deduce that for $x > 1$,

$$L(s,\chi) = -\frac{1}{m} \sum_{k=1}^{m-1} \tau_k(x) \log(1-\omega^{-k})$$

□

We will conclude by using primitive characters to further simplify our expression for $L(1,\chi)$, and finally computing a simplified form in the real quadratic case.

Definition 5.11. Suppose χ' is character mod d such that $d|m$, and we have

$$\chi([p]_m) = \begin{cases} \chi'([p]_d) & \text{if } (p,m) = 1 \\ 0 & \text{if } (p,m) \neq= 1 \end{cases}.$$

Then, we say χ' *induces* χ. If χ is only induced by itself, we call χ a *primitive character* mod m.

It is clear by the definition of $L(1,\chi)$ that if χ' induces χ,

$$L(1,\chi) = \prod_{\substack{p|m \\ p\nmid d}} \left(1 - \frac{\chi'(p)}{p}\right) L(1,\chi')$$

We will admit the following important proposition concerning primitive characters.

Proposition 5.12. Let χ be a primitive character mod m. Then, $|\tau(\chi)| = \sqrt{m}$ and

$$\tau_k(\chi) = \begin{cases} \overline{\chi}(k)\tau(\chi) & \text{if } (k,m) = 1 \\ 0 & \text{if } (k,m) \neq 1 \end{cases}$$

Proof. See Marcus [1] pg. 141. □

We say a character χ is even if $\chi(1) = \chi(-1)$. Since we are only interested in the norm of $|L(1,\chi)|$ for our purposes, then we may now use the propositions above to prove the following.

Theorem 5.13. Let χ be an even primitive character mod m, then

$$|L(1,\chi)| = \frac{2}{\sqrt{m}} \Bigg| \sum_{\substack{k \in \mathbb{Z}_m^* \\ k < m/2}} \chi(k) \, \log\left(\sin\,\frac{k\pi}{m}\right)\Bigg|$$

Proof. Applying proposition 5.12 to 5.10, we get

$$\begin{aligned} L(1,\chi) &= -\frac{1}{m} \sum_{k \in \mathbb{Z}_m^*} \tau(\chi)\overline{\chi(k)}\log(1-\omega^{-k}) \\ &= -\frac{\tau(\chi)}{m} \sum_{k \in \mathbb{Z}_m^*} \overline{\chi(-k)}\log(1-\omega^{k}) \quad \text{(Letting } k = -k) \end{aligned}$$

Since χ is even and multiplicative, then $\overline{\chi(-k)} = \overline{\chi(k)\chi(-1)} = \overline{\chi(k)}$. Using Euler's formula and double angle identities, we have the following equality

$$\begin{aligned} 1 - e^{2\pi ik/m} &= 1 - \cos(2\pi k/m) - i\sin(2\pi ik/m) \\ &= 2\sin^2(\pi k/m) - 2i\sin(\pi k/m)\cos(\pi k/m) \\ &= -2i\sin(\pi k/m)\Big(\cos(\pi k/m) + \sin(\pi k/m)\Big) \\ &= 2e^{i(\pi k/m - \pi/2)}\sin(\pi k/m) \end{aligned}$$

It follows that

$$\log(1-\omega^k) = \log(2) + \log\left(\sin\frac{k\pi}{m}\right) + \left(\frac{k}{m} - \frac{1}{2}\right)\pi i$$

Substituting back into $L(1,\chi)$, and noting that $k \in \mathbb{Z}_m^* \Leftrightarrow m-k \in Z_m^*$

$$\begin{aligned}
|L(1,\chi)| &= \left|\frac{\tau(\chi)}{m}\right| \cdot \left| \left(\log(2) - \frac{\pi i}{2}\right) \overbrace{\sum_{k\in\mathbb{Z}_m^*} \chi(k)}^{=0} + \sum_{k\in\mathbb{Z}_m^*} \left(\frac{k}{m}\overline{\chi(k)} + \log\,\sin\frac{k\pi}{m}\overline{\chi(k)}\right)\right| \\
&= \left|\frac{\tau(\chi)}{m}\right| \cdot \left| \sum_{\substack{k\in\mathbb{Z}_m^* \\ k<m/2}} \overbrace{\chi(k)}^{=\chi(m-k)} \left(k + m - k + \log\,\sin\frac{k\pi}{m} + \log\, \underbrace{\sin\frac{(m-k)\pi}{m}}_{\substack{=\sin(\pi-k/m) \\ =\sin(k/m)}}\right)\right| \\
&= \underbrace{\frac{2}{\sqrt{m}}}_{by 5.12} \left| \sum_{\substack{k\in\mathbb{Z}_m^* \\ k<m/2}} \chi(k)\, \log\left(\sin\,\frac{k\pi}{m}\right)\right| \qquad \left(m \cdot \sum_{k\in\mathbb{Z}_m^*} \chi(k) = 0\right)
\end{aligned}$$

□

We will conclude by using the above expression for $L(1,\chi)$ to compute the number of ideal classes in the case of real quadratic fields.

Given a quadratic field $K = \mathbb{Q}[\sqrt{d}]$ with $d > 0$ squarefree, and its associated number ring $R = \mathbb{A} \cap K$, we note the following.

i. $K \subset \mathbb{Q}[\omega]$ where $\omega = e^{2\pi i/m}$. This can be shown explicitly by computing that for prime p, $\text{disc}(\mathbb{A} \cap \mathbb{Q}[e^{2/\pi i/p}]) = \pm p^{p-2}$. Then, by the properties of the discriminant, it will follow that the $p-th$ cyclotomic field contains either $\sqrt{p}$ or $\sqrt{-p}$. Finally, since we know by 2.16 that $m = |d|$ or $m = 4|d|$; then an argument which involves factorizing d into primes yields the desired inclusion. (See Marcus [1] p. 29)

ii. By proposition 3.13, p is ramified in K iff $p \mid m$.

iii. $\mathrm{Gal}(K/\mathbb{Q})$ consists of the embeddings $\sqrt{d} \mapsto \pm\sqrt{d}$. Thus, there is only one non-trivial character mod m, χ. Recall that $\chi : \mathbb{Z}_m^* \to \{\pm 1\}$ since $\mathrm{Gal}(K/\mathbb{Q})$ has order 2. For $p \in \mathbb{Z}_m^*$, it corresponds to the embedding $\omega \mapsto \omega^p$. Then, $\chi(p)$ is the order of this embedding in $\mathrm{Gal}(K/\mathbb{Q})$. It follows by proposition 3.15 that for odd p,

$$\chi(p) = \left(\frac{d}{p}\right) := \begin{cases} 1 & \text{if } d \text{ is a square} \mod p \\ -1 & \text{otherwise} \end{cases}$$

And if m is odd ($d = 1 \mod 4$), then $\chi(2) = 1$ iff $d = 1 \mod 8$. By extending multiplicatively, $\chi(n)$ is defined for all positive integers n which are relatively prime to m. So, for odd numbers, χ coincides with the so-called Jacobi symbol. It then becomes clear that χ is a character mod m since we know that the Jacobi symbol satisfies

$$\left(\frac{d}{n}\right) = \left(\frac{[d]_n}{n}\right)$$

Finally, it is well-known that χ is primitive and even for $d > 0$ (see Apostol [5] chapter 9).

Then, applying theorem 5.13, we get our desired result

Theorem 5.14. Let $R = \mathbb{A}_{\mathbb{Q}[\sqrt{d}]}$ with $d > 0$ squarefree, and let $m = |\mathrm{disc}(R)|$. Then, the number of ideal classes in R is expressed as

$$h = \frac{1}{\log(u)} \left| \sum_{\substack{k \in \mathbb{Z}_m^* \\ k < m/2}} \chi(k) \log\left(\sin \frac{k\pi}{m}\right) \right|$$

where u denotes the fundamental unit of R.

References

[1] D. Marcus, *Number Fields* (Graduate Texts in Mathematics). Springer, 1977, ISBN: 9780387902791.

[2] N. Jacobson, *Basic Alegbra I*. Dover, 1974, ISBN: 9780486471891.

[3] L. Washington, *Introduction to Cyclotomic Fields* (Graduate Texts in Mathematics). Springer, 1997, ISBN: 9780387947624.

[4] J.-P. Serre, *A Course in Arithmetic* (Graduate Texts in Mathematics). Springer, 1978, ISBN: 9781468498844.

[5] T. Apostol, *Introduction to Analytic Number Theory* (Undergraduate Texts in Mathematics). Springer, 1976, ISBN: 0387901639.