Representation of Numbers by Decomposable Forms

Gustav Lindberg

May 25, 2019

LUNDS UNIVERSITET
Naturvetenskapliga fakulteten

A form is a sum of expressions of the type $ax_1^{k_1} \cdots x_m^{k_m}$, where a is a given number and $x_1, \ldots, x_m$ are unknowns, and the sum of the exponents $k_1 + \cdots + k_m$ is the same for each term. For example, $x^3 + 3xyz + 7xz^2$ is a form where x, y and z are the unknowns. In this thesis, we will study equations where a form should be equal to an integer, for example $x^3 + 3xyz + 7xz^2 = 5$.

Abstract

In this thesis, we will study the structure of equations of the type $F(x_1, \ldots, x_m) = a$, where F is an irreducible decomposable form, $x_1, \ldots, x_m$ are unknown integers and a is a given integer. We will see that the form F can be written as the norm of some unknown μ, which is an element of a finite extension of $\mathbb{Q}$ and which has a one-to-one correspondence with the unknowns $x_1, \ldots, x_m$.

Contents

1 Introduction **1**
1.1 Forms . . . 1

2 Algebraic Structures **1**
2.1 Groups, Rings and Fields . . . 1
2.2 Algebraic Extensions . . . 2

3 Conjugates and Norms **4**
3.1 Homomorphisms and Conjugates . . . 4
3.2 Real and Complex Conjugates . . . 4
3.3 Norms . . . 5
3.4 Decomposable Forms and Norms . . . 6

4 Group Theory **7**
4.1 Equivalence Classes and Generalized Congruences . . . 8
4.2 Factor Groups . . . 8
4.3 Finite Groups . . . 9

5 Geometric Methods **10**
5.1 Modules . . . 10
5.2 Geometric Representations . . . 11
5.3 Lattices . . . 13
5.4 Logarithmic Representations . . . 15

6 Units **16**
6.1 Orders and Units . . . 17
6.2 Associate Elements . . . 17
6.3 Geometric Representation of Units . . . 18
6.4 Volumes of Fundamental Parallelepipeds . . . 19
6.5 Dirichlet's Theorem . . . 23

7 The Structure of the Set of Solutions to $N(\mu) = a$ **24**
7.1 Algebraic Number Fields with Odd Dimension . . . 24
7.2 Algebraic Number Fields with Even Dimension . . . 25
7.3 The Structure of the Set of Solutions to $N(\mu) = a$ . . . 26

8 References **27**

1 Introduction

Consider the equation

$$x^2 - 2y^2 = 7 \tag{1.0.1}$$

where x and y are unknown integers. The main purpose of this thesis is to find the structure of the set of solutions to this kind of equation (note that this is not the same thing as how to compute these solutions in practice).

In this thesis, most results and proofs are from [1]. Some definitions and results about algebraic structures and group theory are from [2], and definitions 2.2 to 2.6 are from [3]. Definition 2.1 is from [4], Definition 3.2 is from [5] and Definition 6.17 is from [6].

The first step to finding the structure of the set of solutions to equation (1.0.1) would be to factorize it. However, this equation can't be factorized over the set of rational numbers $\mathbb{Q}$. In order to solve this, we will need to introduce an extension of $\mathbb{Q}$ also containing $\sqrt{2}$. We will later see that such an extension can be denoted $\mathbb{Q}[\sqrt{2}]$. In $\mathbb{Q}[\sqrt{2}]$, equation (1.0.1) can be factorized as

$$(x + y\sqrt{2})(x - y\sqrt{2}) = 7. \tag{1.0.2}$$

In order to define extensions such as $\mathbb{Q}[\sqrt{2}]$ formally, we will need to define algebraic structures such as groups, rings and fields. Once we will have the necessary definitions, we will study the structure of these extensions of $\mathbb{Q}$ in order to be able to prove Theorem 7.6, which will give us the structure of the set of solutions to these kinds of equations.

1.1 Forms

The first thing to do is to clearly define what kinds of equations we're interested in. To do this, we need the following definition:

Definition 1.1. A **form** $F(x_1, \ldots, x_m)$ of degree $n \in \mathbb{N}$ over $\mathbb{Q}$ is a sum of expressions of the type $ax_1^{k_1} \cdots x_m^{k_m}$ where $a \in \mathbb{Q}$, $k_1, \ldots, k_m \in \mathbb{N}$ and $k_1 + \cdots + k_m = n$.

In this thesis, we're interested in equations of the type

$$F(x_1, \ldots, x_m) = a \tag{1.1.1}$$

where F is a form over $\mathbb{Q}$, $x_1, \ldots, x_m \in \mathbb{Z}$ are unknown integers and $a \in \mathbb{Z}$ is a given integer.

In the example in equation (1.0.1), $F(x, y) = x^2 - 2y^2$, and $a = 7$.

We will also require that the form F is decomposable, which means that it can be factorized over some extension of $\mathbb{Q}$, and that it's irreducible, which means that it can't be factorized over $\mathbb{Q}$. As we will prove in Theorem 3.18, all two-variable forms are decomposable over some extension of $\mathbb{Q}$.

2 Algebraic Structures

In order to formally define extensions of $\mathbb{Q}$ and other concepts that we will need, we need to define basic algebraic structures such as groups, rings and fields. Once we have defined these concepts, we will prove some basic theorems related to extensions of $\mathbb{Q}$.

2.1 Groups, Rings and Fields

Definition 2.1. A set G with an operation $* : G^2 \to G$ is called a **group** if the following conditions are satisfied for all $a, b, c \in G$:

1. Associativity: $(a * b) * c = a * (b * c)$
2. Existence of neutral element: $\exists e \in G$ such that $e * a = a * e = a$ (if $*$ is an addition the neutral element is usually denoted 0 and if $*$ is a multiplication the neutral element is usually denoted 1)

3. Existence of inverse element: $\exists a^{-1}$ such that $a * a^{-1} = a^{-1} * a = e$ (if $*$ is an addition the inverse element of a is usually denoted $-a$)

The operation $*$ is called the group law of G. If $*$ is an addition G is called an additive group and if $*$ is a multiplication G is called a multiplicative group. Additive groups are usually commutative, which means that $a + b = b + a \ \forall a, b \in G$.

Definition 2.2. An additive group R with an addition $+ : R^2 \to R$ and a multiplication $\cdot : R^2 \to R$ is called a **ring** if the following conditions are satisfied for all $a, b, c \in R$:

1. Associativity of addition: $a + (b + c) = (a + b) + c$
2. Commutativity of addition: $a + b = b + a$
3. Existence of neutral element for addition: $\exists 0 \in R$ such that $a + 0 = a$
4. Existence of additive inverse: $\exists -a$ such that $a + (-a) = 0$
5. Associativity of multiplication $a(bc) = (ab)c$
6. Distributivity: $(a + b)c = ac + bc$ and $a(b + c) = ab + ac$

Definition 2.3. A ring R is **commutative** if $ab = ba \ \forall a, b \in R$.

Definition 2.4. An element $1 \in R$ is called a **unity** if $a \cdot 1 = 1 \cdot a = a \ \forall a \in R$. It's easy to prove that if a unity exists, it is unique.

Definition 2.5. Let R be a ring with unity 1. Then an element $a \in R$ is **invertible** if $\exists a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Definition 2.6. A ring F is called a **field** if it is commutative, has a non-zero unity and all non-zero elements of F are invertible.

Definition 2.7. If F and G are fields and $F \subseteq G$, then F is called a **subfield** of G and G is called an **extension** of F.

Example 2.8. $\mathbb{C}$ is an extension of $\mathbb{R}$ and $\mathbb{R}$ is an extension of $\mathbb{Q}$.

2.2 Algebraic Extensions

Definition 2.9. Let K be a field, k be a subfield of K, and $\alpha \in K$. Then α is **algebraic** over k if $\exists n \in \mathbb{N}$ and $\exists a_0, \ldots, a_n \in k$ such that $a_n \neq 0$ and $p(\alpha) = 0$ where $p(x) = a_n x^n + \cdots + a_1 x + a_0$. The monic polynomial p over k of the lowest degree such that this holds is called the **minimal polynomial** of α.

Example 2.10. $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because $\sqrt{2}^2 - 2 = 0$. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $p(x) = x^2 - 2$.

Definition 2.11. Let K be a field, k be a subfield of K, and $\alpha \in K$. We denote $k[\alpha] \subseteq K$ the ring such that $z \in k[\alpha] \iff \exists n \in \mathbb{N}$ and $\exists a_0, \ldots, a_n \in k$ such that $a_n\alpha^n + \cdots + a_1\alpha + a_0 = z$.
By setting $n = 0$ and letting a_0 vary, we can get any element in k, so $k \subseteq k[\alpha]$.

Example 2.12. $\mathbb{Q}[\sqrt{2}] = \{z \in \mathbb{R}; z = x + y\sqrt{2}, x, y \in \mathbb{Q}\}$ since $\sqrt{2}^2 = 2 \in \mathbb{Q}$ so all powers of $\sqrt{2}$ are of that form, so all linear combinations of powers of $\sqrt{2}$ are also of that form.

Example 2.13. $\mathbb{C} = \mathbb{R}[i]$ because for the same reason as above, all elements in $\mathbb{R}[i]$ are of the form $x + yi$, and we know that all complex numbers are also of that form.

Theorem 2.14. *If K is a field, k is a subfield of K and $\alpha \in K$ is algebraic over k, then $k[\alpha]$ is a field.*

Proof. $k \subseteq k[\alpha]$ and k is a field so k contains a unity so so does $k[\alpha]$, and $k[\alpha] \subseteq K$ and K is commutative so so is $k[\alpha]$, so all we need to prove is that every non-zero element in $k[\alpha]$ is invertible. Let $p(x)$ be the minimal polynomial of α over k, and let $f(x)$ be a polynomial over k such that $f(\alpha) \neq 0$. Then p and f are relatively prime (if they wouldn't $f(\alpha)$ would be 0 since $p(\alpha) = 0$), so there exist polynomials $g(x)$ and $h(x)$ such that

$$g(x)p(x) + h(x)f(x) = 1. \tag{2.14.1}$$

If we plug in $x = \alpha$, equation (2.14.1) becomes

$$h(\alpha)f(\alpha) = 1. \tag{2.14.2}$$

$k[\alpha]$ is defined as all the elements that are of the form $f(\alpha)$ for some polynomial f, and since f in equation (2.14.2) is an arbitrary polynomial as long as $f(\alpha) \neq 0$, so for any non-zero element z in $k[\alpha]$, we can choose f such that $f(\alpha) = z$, and then $h(\alpha)z = 1$, so z is invertible. □

If k is a field and K is an extension of k, then K can be seen as a vector space over k with dimension n. If n is finite, K is an n-dimensional extension of k, and if $n = \infty$, K is an infinite-dimensional extension of k. We denote this dimension n as $[K : k]$.

Example 2.15. $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ because since $\mathbb{Q}[\sqrt{2}] = \{z \in \mathbb{R}; z = x + y\sqrt{2}, x, y \in \mathbb{Q}\}$, 1 and $\sqrt{2}$ can be seen as basis vectors for $\mathbb{Q}[\sqrt{2}]$.

Example 2.16. $[\mathbb{Q}[e] : \mathbb{Q}] = \infty$ because all powers of e are linearly independent, so all numbers $e^n, n \in \mathbb{N}$ can be seen as basis vectors for $\mathbb{Q}[e]$ and there are infinitely many of them.

Definition 2.17. Let K be an extension of k. If $[K : k] = \infty$, K is called an **infinite extension** of k, and if $[K : k]$ is finite, K is called a **finite extension** of k. A finite extension of $\mathbb{Q}$ is called an **algebraic number field**.

Theorem 2.18. *If k is a field and α is algebraic over k, then $k[\alpha]$ is a finite extension of k, and the dimension of $k[\alpha]$ over k is equal to the degree of the minimal polynomial of α.*

Proof. Let $p(x)$ be the minimal polynomial of α over k, and let n be the degree of p. Then by the definition of the minimal polynomial, $p(\alpha) = 0$. Therefore, $1, \alpha, \ldots, \alpha^n$ are linearly dependent. By Theorem 2.14 $k[\alpha]$ is a field, so α^n can be written as a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$, so $[k[\alpha] : k] \leq n$ is finite. Suppose for a contradiction that $[k[\alpha] : k] < n$. Then $1, \alpha, \ldots, \alpha^{n-1}$ would be linearly dependent, so there would exist a non-zero polynomial $q(x)$ of degree strictly less than to n such that $q(\alpha) = 0$. This is a contradiction since p (which is of degree exactly n) was defined as the polynomial of lowest degree such that $p(\alpha) = 0$. Therefore, $[k[\alpha] : k] = n$. □

Definition 2.19. Let k be a field and f be a polynomial of degree n in k. Then K is a **splitting field** of f if f can be factorized into linear terms in K, that is $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ for $c \in k, \alpha_1, \ldots, \alpha_n \in K$, and if $K = k[\alpha_1, \ldots, \alpha_n]$.

Example 2.20. $\mathbb{Q}[\sqrt{2}]$ is the splitting field of $x^2 - 2$ in $\mathbb{Q}$.

Definition 2.21. Let K be a finite n-dimensional extension of k, and let $\alpha \in K$. Let $A \in k^{n\times n}$ be the transformation matrix of the mapping $\xi \mapsto \alpha\xi$ with respect to any basis for K where $\xi \in K$ is seen as a vector over k. Then the **characteristic polynomial** of α is defined as $\phi_\alpha(\lambda) = \det(\lambda I - A)$ where I is the identity matrix, and the **trace** of α is defined as the trace of A, $\mathrm{tr}(\alpha) = \mathrm{tr}(A)$.

Lemma 2.22. *Let K be a finite n-dimensional extension of k, and let $\alpha \in K$. Then the characteristic polynomial of α is a power of the minimal polynomial of α.*

Proof. Let $p(x) = x^m + c_1x^{m-1} + \cdots + c_m$ be the minimal polynomial of α. By the proof of Theorem 2.18, $1, \alpha, \ldots, \alpha^{m-1}$ form a basis for $k[\alpha]$ over k. Let $\theta_1, \ldots, \theta_s$ be a basis for K over $k[\alpha]$. Then we can take

$$\theta_1, \alpha\theta_1, \ldots, \alpha^{m-1}\theta_1, \ldots, \theta_s, \alpha\theta_s, \ldots, \alpha^{m-1}\theta_s$$

as a basis for K over k. Then the matrix for the linear transformation $\xi \mapsto \alpha\xi$ in this basis where $\xi \in K$ is the following matrix, which is a block-diagonal matrix with s blocks.

$$\begin{pmatrix}
0 & 1 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \cdots & 0 & 0 & \cdots & 0 \\
0 & 0 & \cdots & 1 & \cdots & 0 & 0 & \cdots & 0 \\
-c_m & -c_{m-1} & \cdots & -c_1 & \cdots & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & \cdots & 0 & 1 & \cdots & 0 \\
0 & 0 & \cdots & 0 & \cdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 1 \\
0 & 0 & \cdots & 0 & \cdots & -c_m & -c_{m-1} & \cdots & -c_1
\end{pmatrix}$$

By definition, the characteristic polynomial of α is the characteristic polynomial of this matrix. By doing some basic linear algebra, we get that that characteristic polynomial is equal to $p(x)^s$, which proves the theorem. □

Corollary 2.23. *Let K be a finite n-dimensional extension of $\mathbb{Q}$, and let $\alpha \in K$. Then the minimal polynomial of α divides the characteristic polynomial of α.*

3 Conjugates and Norms

Conjugate functions and norms are very important concepts for studying the structure of the set of solutions to equation (1.1.1). As we will see in Theorem 3.24, equation (1.1.1) can be rewritten using norms, which will simplify our calculations in the remaining part of this thesis.

3.1 Homomorphisms and Conjugates

Definition 3.1. Let A and B be rings. Then a function $f : A \to B$ is called a **homomorphism** if the following conditions are satisfied for all $a, b \in A$:

1. $f(a + b) = f(a) + f(b)$
2. $f(ab) = f(a)f(b)$
3. If 1 is a unity in A, then $f(1)$ is a unity in B.

Definition 3.2. A **monomorphism** is an injective homomorphism.

Definition 3.3. An **isomorphism** is a bijective homomorphism.

Definition 3.4. Let $k \subset \mathbb{C}$ be a field, and let K be a finite extension of k. Then a monomorphism σ from K to $\mathbb{C}$ is called a **conjugate function** if $\sigma(a) = a \ \forall a \in k$. Note that the identity map is always a conjugate function.

Theorem 3.5. *Let k be a field, and let K be a finite extension of k, let σ be a conjugate function from K to $\mathbb{C}$, and let $\alpha \in K$ be algebraic over k. Then $\sigma(\alpha)$ is a root of the minimal polynomial of α.*

Proof. Let $p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ be the minimal polynomial of α. Since σ is a conjugate function in K, it's a homomorphism from K to $\mathbb{C}$ and it's the identity map over k. Therefore for any $x \in k$

$$\begin{aligned}\sigma(p(x)) &= \sigma((x - \alpha_1) \cdots (x - \alpha_n)) \\ &= \sigma(x - \alpha_1) \cdots \sigma(x - \alpha_n) \\ &= (\sigma(x) - \sigma(\alpha_1)) \cdots (\sigma(x) - \sigma(\alpha_n)) \\ &= (x - \sigma(\alpha_1)) \cdots (x - \sigma(\alpha_n)).\end{aligned}$$

Since p is a polynomial over k, we also have that $p(x) \in k$ if $x \in k$, so therefore $\sigma(p(x)) = p(x)$ $\forall x \in k$. This means that the two polynomials $p(x)$ and $\sigma(p(x))$ have the same roots, so $\{\alpha_1, \ldots, \alpha_n\} = \{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$ in some order. Since α is a root of p, $\alpha = \alpha_j$ for some j, so $\sigma(\alpha) \in \{\alpha_1, \ldots, \alpha_n\}$, so $\sigma(\alpha)$ is a root of p. □

Theorem 3.6. *If k is a field and K is an n-dimensional extension of k, then there are exactly n conjugate functions in K.*

Example 3.7. Let $k = \mathbb{R}$ and $K = \mathbb{C}$. Then the two conjugate functions are $f(z) = z$ and $g(z) = \bar{z}$. Since $f(z) = z$ is a trivial conjugate, we usually think of $g(z) = \bar{z}$ as the complex conjugate.

3.2 Real and Complex Conjugates

Definition 3.8. Let K be a finite extension of $\mathbb{Q}$, and let σ be a conjugate function of K. If $\sigma(x) \in \mathbb{R}$ $\forall x \in K$, σ is called **real**, otherwise σ is called **complex**.

Example 3.9. Let $K = \mathbb{Q}[\sqrt[3]{2}]$. Then $\sigma_1(x) : \mathbb{Q}[\sqrt[3]{2}] \to \mathbb{Q}[\sqrt[3]{2}]$ defined by $\sigma_1(x) = x$ is a real conjugate and $\sigma_2(x) : \mathbb{Q}[\sqrt[3]{2}] \to \mathbb{Q}\left[\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\sqrt[3]{2}\right]$ defined by

$$\sigma_2(x + y\sqrt[3]{2} + z\sqrt[3]{4}) = x + y\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\sqrt[3]{2} + z\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\sqrt[3]{4}$$

is a complex conjugate.

Theorem 3.10. *The number of complex conjugates of a given finite extension of $\mathbb{Q}$ is even.*

Proof. If σ is a conjugate, $\bar{\sigma}$ is also a conjugate because the function $z \mapsto \bar{z}$ is a monomorphism and $\bar{q} = q$ $\forall q \in \mathbb{Q}$. Therefore if $\sigma \neq \bar{\sigma}$, the conjugates come in pairs, so the only way there could be an odd number of complex conjugates is if there exists a complex conjugate σ such that $\sigma = \bar{\sigma}$. But if $\sigma = \bar{\sigma}$, that means that $\sigma(\alpha) = \overline{\sigma(\alpha)}$ $\forall \alpha \in K$, which means that $\sigma(\alpha) \in \mathbb{R}$ $\forall \alpha \in K$, which means that σ is real. □

The number of real conjugates of K to a subset of $\mathbb{C}$ will be denoted s and half the number of complex conjugates will be denoted t (note that t is an integer because of Theorem 3.10). The number $s + t - 1$ will be denoted as r (this number has some special properties as we will see later).

Theorem 3.11. *Let K be a finite extension of $\mathbb{Q}$ with dimension n, and let s and t be defined as above. Then $n = s + 2t$.*

Proof. There are n conjugates over K, of which s are real and $2t$ are complex. All conjugates are either real or complex, so therefore the total number of conjugates n equals the sum of the number of real conjugates and the number of complex conjugates $s + 2t$, so $n = s + 2t$. □

3.3 Norms

Definition 3.12. Let k be a field, K be a finite extension of k, $\sigma_1, \ldots, \sigma_n$ be the conjugate functions in K, and α be an element in K. Then the **norm** of α is defined as $N(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha)$.

Theorem 3.13. *Let K be a finite extension of k with dimension n and let $a \in k$. Then $N(a) = a^n$.*

Proof. Let $\sigma_1, \ldots, \sigma_n$ be the conjugate functions of K. Since $a \in k$, by the definition of a conjugate function $\sigma_j(a) = a$ $\forall j \in \{1, \ldots, n\}$. Therefore,

$$\begin{aligned} N(a) &= \sigma_1(a) \cdots \sigma_n(a) \\ &= a \cdots a \\ &= a^n. \end{aligned}$$

□

Corollary 3.14. $N(1) = 1$

Theorem 3.15. $N(\alpha\beta) = N(\alpha)N(\beta)$ $\forall \alpha, \beta \in K$.

Proof. By the definition of a conjugate function, each conjugate function is a homomorphism, so by point 2 in the definition of a homomorphism they're multiplicative. Therefore

$$\begin{aligned} N(\alpha\beta) &= \sigma_1(\alpha\beta) \cdots \sigma_n(\alpha\beta) \\ &= \sigma_1(\alpha)\sigma_1(\beta) \cdots \sigma_n(\alpha)\sigma_n(\beta) \\ &= \sigma_1(\alpha) \cdots \sigma_n(\alpha)\sigma_1(\beta) \cdots \sigma_n(\beta) \\ &= N(\alpha)N(\beta). \end{aligned}$$

□

Theorem 3.16. *Let K be a finite n-dimensional extension of k, and let $\alpha \in K$. Then $N(\alpha) = (-1)^n \phi_\alpha(0)$, where ϕ_α is the characteristic polynomial of α.*

3.4 Decomposable Forms and Norms

Definition 3.17. A form $F(x_1, \ldots, x_m)$ over a field k is called **decomposable** if it can be factorized as a product of linear factors in an algebraic extension of k.

Theorem 3.18. *Let $F(x, y) = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_0 y^n$ be a two-variable form over $\mathbb{Q}$ and let $g(t) = a_n t^n + \cdots + a_0$ be a polynomial with the same coefficients as F. Then F is decomposable.*

Proof. Let K be the splitting field of g. By the definition of the splitting field, $g(t) = c(t-\alpha_1)\cdots(t-\alpha_n)$ for $c, \alpha_1, \ldots, \alpha_n \in K$. If we take $t = \frac{x}{y}$, we get $g(\frac{x}{y}) = c(\frac{x}{y} - \alpha_1)\cdots(\frac{x}{y} - \alpha_n)$. By multiplying by y^n on both sides, we get:

$$\begin{aligned} F(x,y) &= a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_0 y^n \\ &= y^n \left(a_n \left(\frac{x}{y}\right)^n + a_{n-1} \left(\frac{x}{y}\right)^{n-1} + \cdots + a_0 \right) \\ &= y^n g\left(\frac{x}{y}\right) \\ &= c y^n \left(\frac{x}{y} - \alpha_1\right) \cdots \left(\frac{x}{y} - \alpha_n\right) \\ &= c(x - y\alpha_1) \cdots (x - y\alpha_n). \end{aligned}$$

Therefore, F can be factorized as a product of linear factors in the splitting field of g which is a finite extension of $\mathbb{Q}$, so F is decomposable over $\mathbb{Q}$. □

Definition 3.19. A form F is called **reducible** over a ring k if there exist non-constant forms G and H over k such that $F = GH$. If this is not the case, F is called **irreducible**.

Example 3.20. The form $x^2 - 2y^2$ is irreducible over $\mathbb{Q}$ since it can't be written as a non-trivial product of two other forms over $\mathbb{Q}$. It is however decomposable since it can be factorized into linear factors over $\mathbb{Q}[\sqrt{2}]$.

Definition 3.21. Two forms over $\mathbb{Q}$ of the same degree are called **integrally equivalent** if they can be obtained from each other by a linear change of variables with integer coefficients.

Lemma 3.22. *Any form of degree n is integrally equivalent to a form in which the coefficient of the term x_1^n is non-zero.*

Lemma 3.23. *Let $\mu_2, \ldots, \mu_m$ be algebraic over $\mathbb{Q}$ and let $K = \mathbb{Q}[\mu_2, \ldots, \mu_m]$. Then the form $F(x_1, \ldots, x_m) = N(x_1 + x_2\mu_2 + \cdots + x_m\mu_m)$ is irreducible over $\mathbb{Q}$.*

Proof. Assume for a contradiction that

$$F = GH \tag{3.23.1}$$

where G and H are non-constant forms over $\mathbb{Q}$, and let $\sigma_1, \ldots, \sigma_n$ be the conjugate functions of K, where σ_1 is the identity map. Let $L_j = x_1 + x_2\sigma_j(\mu_2) + \cdots + x_m\sigma_j(\mu_m)$ for $j \in \{1, \ldots, n\}$. We know by assumption that

$$\begin{aligned} F(x_1, \ldots, x_m) &= N(x_1 + x_2\mu_2 + \cdots + x_m\mu_m) \\ &= \sigma_1(x_1 + x_2\mu_2 + \cdots + x_m\mu_m) \cdots \sigma_n(x_1 + x_2\mu_2 + \cdots + x_m\mu_m) \\ &= (x_1 + x_2\sigma_1(\mu_2) + \cdots + x_m\sigma_1(\mu_m)) \cdots (x_1 + x_2\sigma_n(\mu_2) + \cdots + x_m\sigma_n(\mu_m)) \\ &= L_1 \cdots L_n. \end{aligned} \tag{3.23.2}$$

Therefore each L_j divides F. Since factorization in polynomial rings is unique, each L_j must divide either G or H. Let $L_1 = x_1 + x_2\mu_2 + \cdots + x_m\mu_m$. By what we just proved, L_1 divides either G or H. Since G and H are interchangeable, we can assume without loss of generality that L_1 divides G. Therefore, there exists a form M_1 such that

$$G = L_1 M_1. \tag{3.23.3}$$

By taking the image of σ_j on both sides of equation (3.23.3) for an arbitrary conjugate function σ_j, we get $\sigma_j(G) = L_j\sigma_j(M_1)$. Since G is a form over $\mathbb{Q}$, $\sigma_j(G) = G$. By defining M_j as $\sigma_j(M_1)$, we get:

$$G = L_j M_j.$$

Therefore, each L_j divides G. Since the σ_j's are distinct and the μ_k's are linearly independent over $\mathbb{Q}$, the forms L_j are pairwise distinct. Since each L_j divides G, this means that their product $L_1 \cdots L_n$ divides G. By equation (3.23.2), $L_1 \cdots L_n = F$, so F divides G. By combining this with equation (3.23.1), we get that H is constant, which concludes the proof. □

Theorem 3.24. *Let F be an irreducible decomposable form over $\mathbb{Q}$ of degree n. Then the problem from equation* (1.1.1)

$$F(x_1, \ldots, x_m) = a^* \tag{3.24.1}$$

where $a^* \in \mathbb{Z}$ can be written as

$$N(\mu) = a \tag{3.24.2}$$

where $a \in \mathbb{Q}$, $\mu \in K$ is unknown and where K is some finite extension of $\mathbb{Q}$.

Proof. By Lemma 3.22, we can assume that the coefficient of x_1^n is non-zero (otherwise we just do a change of variables and get an equation which is equivalent to the original equation). Because of this and since F is decomposable, we can factorize F as:

$$F = c(x_1 + \beta_{1,2}x_2 + \cdots + \beta_{1,m}x_m) \cdots (x_1 + \beta_{n,2}x_2 + \cdots + \beta_{n,m}x_m) \tag{3.24.3}$$

where $c \in \mathbb{Q}$ the $\beta_{j,k}$'s are algebraic over $\mathbb{Q}$. Let $\mu_j = \beta_{1,j}$ for $j \in \{2, \ldots, m\}$ and consider $K = \mathbb{Q}[\mu_2, \ldots, \mu_m]$. By Lemma 3.23, the form

$$F^* = N(x_1 + x_2\mu_2 + \cdots + x_m\mu_m) \tag{3.24.4}$$

is irreducible. Let $L_1, \ldots, L_n$ be defined as in the proof of Lemma 3.23, and in particular

$$L_1 = x_1 + x_2\mu_2 + \cdots + x_m\mu_m.$$

L_1 divides both F and F^*, so there exists a form M_1 such that

$$F = L_1 M_1.$$

By using exactly the same reasoning on F as we did on G in the proof of Lemma 3.23, we get that F^* divides F. By assumption, F is irreducible, so therefore

$$F = cF^* \tag{3.24.5}$$

where $c \in \mathbb{Q}$ is a constant. If we let $\mu = x_1 + x_2\mu_2 + \cdots + x_m\mu_m$ and combine equations (3.24.4) and (3.24.5), we get:

$$\begin{aligned} F = a^* &= cN(\mu) \\ \iff N(\mu) &= a \end{aligned}$$

where a is defined as $a = \frac{a^*}{c}$.
Since $1, \mu_2, \ldots, \mu_m$ are linearly independent over $\mathbb{Q}$, there is a one-to-one correspondence between the unknown μ in equation (3.24.2) and the unknowns $x_1, \ldots, x_m$ in equation (1.1.1). □

Example 3.25. The problem in equation (1.0.1) can be written as $N(\mu) = 7$, where $\mu \in \mathbb{Q}[\sqrt{2}]$ is unknown. Here $\mu = x + y\sqrt{2}$.

From now on we will work with equation (3.24.2) instead of equation (1.1.1), since Theorem 7.6 (which is the main theorem of this thesis) is easier to formulate and to prove if the problem involves equation (3.24.2).

4 Group Theory

In order to prove some theorems later on in this thesis, we will need several definitions and theorems related to group theory, such as factor groups and theorems related to finite groups.

4.1 Equivalence Classes and Generalized Congruences

Definition 4.1. A relation $\sim$ on a set A is said to be an **equivalence relation** if the following conditions are satisfied for all $a, b, c \in A$:

1. Reflexivity: $a \sim a$
2. Symmetry: $a \sim b \iff b \sim a$
3. Transitivity: $a \sim b$ and $b \sim c \implies a \sim c$

Definition 4.2. Let $\sim$ be an equivalence relation on a set A, and let $x \in A$. We define the **equivalence class** of x to be $[x] = \{y \in A; x \sim y\}$. An element $y \in [x]$ is called a representative for $[x]$.

In the remaining part of this section, we will suppose that all groups are additive unless stated otherwise in order to simplify the notation. However, the same theory works for any commutative group with group law $*$ by replacing $x + y$ by $x * y$, $x - y$ by $x * y^{-1}$ and 0 by the neutral element.

Definition 4.3. Let G be a group and H be a subgroup of G. Two elements of $x, y \in G$ are said to be **congruent** mod H if $x - y \in H$. This is denoted $x \equiv y \pmod{H}$.

Example 4.4. If $G = \mathbb{Z}$ and $H = n\mathbb{Z}$ where $n \in \mathbb{N}^*$, then $x \equiv y \pmod{n\mathbb{Z}}$ if $n|(x - y)$. This congruence is the one that is commonly used in number theory and is commonly denoted $x \equiv y \pmod{n}$.

Theorem 4.5. *Let G be a group, let H be a subgroup of G, and let $a, b, c, d \in G$. Then $a \equiv b \pmod{H}$ and $c \equiv d \pmod{H} \implies a + c \equiv b + d \pmod{H}$.*

Proof. We know that $a - b \in H$ and $c - d \in H$. Since H is a group, $(a - b) + (c - d) = (a + c) - (b + d) \in H$, so $a + c \equiv b + d \pmod{H}$. □

Theorem 4.6. *Let G be a group and let H be a subgroup of G. Then the relation of congruence mod H is an equivalence relation.*

Proof. For any $a, b, c \in G$:

1. Reflexivity: $a - a = 0$. Since H is a group $0 \in H$ so $a \equiv a \pmod{H}$.
2. Symmetry: Suppose $a \equiv b \pmod{H}$. Then $a - b \in H$. Since H is a group and $a - b \in H$, $-(a - b) \in H$. $-(a - b) = b - a$, so $b \equiv a \pmod{H}$.
3. Transitivity: Suppose $a \equiv b \pmod{H}$ and $b \equiv c \pmod{H}$. Then $a - b \in H$ and $b - c \in H$. Since H is a group, this means that $(a - b) + (b - c) \in H$. $(a - b) + (b - c) = a - c$, so $a \equiv c \pmod{H}$.

□

4.2 Factor Groups

Definition 4.7. Let G be a group and let H be a subgroup of G. Then the **factor group** of G and H is defined by $G/H = \{[x]; x \in G\}$ where $[x]$ is the equivalence class of the congruence relation mod H.

Example 4.8. If $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$ where $n \in \mathbb{N}^*$, then $\mathbb{Z}/5\mathbb{Z}$ is $\mathbb{Z}_5$.

Theorem 4.9. *Let G be a group, let H be a subgroup of G and let G/H be their factor group. Then for $x, y \in G$ the addition $+ : (G/H)^2 \to G/H$ defined as $[x] + [y] = [x + y]$ is well-defined.*

Proof. Let $[x], [y] \in G/H$, let $x_1, x_2 \in G$ be representatives for $[x]$ and let $y_1, y_2 \in G$ be representatives for $[y]$. We know that $x_1 \equiv x_2 \pmod{H}$ since they're in the same equivalence class and $y_1 \equiv y_2 \pmod{H}$ for the same reason. Therefore $x_1 + y_1 \equiv x_2 + y_2 \pmod{H}$, so no matter which representatives of $[x]$ and $[y]$ we choose their sum is in the same equivalence class, so the addition over G/H is well-defined. □

Theorem 4.10. *G/H with the addition defined as in Theorem 4.9 is a group.*

Proof. First, we need to prove that the addition is closed over G/H. If $[x], [y] \in G/H$, $[x + y] \in G/H$ because if x is a representative of $[x]$ and y is a representative of y, then $x + y$ has an equivalence class which also is in G/H, so the addition is closed over G/H. We also need to prove that the three conditions in the definition of a group are satisfied. For this, let $[a], [b], [c] \in G/H$ and let $a, b, c \in G$ be their representatives:

1. Associativity: $([a]+[b])+[c]=[a+b]+[c]=[a+b+c]=[a]+[b+c]=[a]+([b]+[c])$
2. Existence of neutral element: Let 0 be the neutral element in G. Then $[a]+[0]=[a+0]=[a]$, so $[0]$ is a neutral element in G/H.
3. Existence of inverse element: Let $-a$ be the inverse of a. Then $[a]+[-a]=[a-a]=[0]$ and $[0]$ is the neutral element, so $[-a]$ is the inverse of $[a]$.

□

4.3 Finite Groups

Definition 4.11. A finite group G is said to be **cyclic** if $\exists a \in G$ such that $\forall x \in G\ \exists n \in \mathbb{N}$ such that $x = na$.

Definition 4.12. Let G be a finite group and let $a \in G$. Then the **order** of a is defined as the smallest strictly positive integer $n \in \mathbb{N}^*$ such that $na = 0$.

Theorem 4.13. *Let G be a finite group with n elements. Then the number of elements of any subgroup $H \subseteq G$ divides the number of elements in G.*

Proof. Consider all the elements $a_1, \ldots, a_n \in G$, and consider the congruence classes $[a_j] \bmod H$ as defined above. Let $x \in [a_j] \cap [a_k]$. Then $a_j \equiv x \equiv a_k \pmod{H}$, so $[a_j] = [a_k]$, so all the $[a_j]$'s are either equal or pairwise disjoint. Also, since any element in G is an a_j, the $[a_j]$'s cover G entirely. Now we want to prove that all the $[a_j]$'s contain equally many elements. To do so, consider two of these congruence classes $[a_j]$ and $[a_k]$. The function $f(x) = a_k - a_j + x$ has a well-defined inverse function $f^{-1}(y) = a_j - a_k + y$ so it's a bijection and if $x \in [a_j]$ then $x \equiv a_j \pmod{H}$ so $f(x) = a_k - a_j + x \equiv a_k - a_j + a_j = a_k \pmod{H}$, so it maps any element of $[a_j]$ onto an element of $[a_k]$. Therefore f is a bijection from $[a_j]$ to $[a_k]$, so $[a_j]$ and $[a_k]$ must have the same number of elements, call this number m. Since the $[a_j]$'s cover G and are pairwise disjoint, $n = lm$ where l is the number of distinct classes $[a_j]$, so $m|n$. Since $H = [0]$, H is itself one of the $[a_j]$'s, so H has m elements, which proves the theorem. □

Theorem 4.14. *Let G be a finite group and let $a \in G$. Then the order of a divides the number of elements in G.*

Proof. Let n be the number of elements in G and let m be the order of a. Consider the set $H = \{x \in G; \exists j \in \mathbb{N}, x = ja\}$. H contains m elements because for $j \geq m$, if $j = qm + r$ where $0 \leq r < m$, $ja = (qm + r)a = qma + ra = 0 + ra = ra$. $ja + ka = (j + k)a \in H$, so addition is closed on H. It's obvious that addition is associative on H since it's associative on G and $H \subseteq G$. $0 \in H$ because $0 = ma$. Any element $ja \in H$ has an inverse element in H because $ja + (m - j)a = ma = 0$, and $(m - j)a \in H$ for $j \leq m$, and any element in H is of the form ja where $j \leq m$. Therefore H satisfies all the conditions for being a group, so H is a subgroup of G. H has m elements so by Theorem 4.13, $m|n$. Since m is the order of a, this proves the theorem. □

Lemma 4.15. *Let G be a finite multiplicative group. Then if G contains at least one element with order m and at least one element with order n, it contains at least one element whose order is the least common multiple of m and n.*

Proof. Let $x, y \in G$, let m be the order of x and let n be the order of y. Let $p_1, \ldots, p_k$ be the prime numbers that are part of the prime factorization of either m or n (if $m = n = 1$, let $k = 1$ and p_1 be any prime number). Then

$$m = p_1^{s_1} \cdots p_k^{s_k}$$
$$n = p_1^{t_1} \cdots p_k^{t_k}$$

for some $s_1, \ldots, s_k, t_1, \ldots, t_k \in \mathbb{N}$ (the s_j's and t_j's are allowed to be 0). Let

$$u_j = \begin{cases} s_j \text{ if } s_j \geq t_j \\ 0 \text{ otherwise} \end{cases}$$

$$v_j = \begin{cases} t_j \text{ if } s_j < t_j \\ 0 \text{ otherwise} \end{cases}$$

Let $m_0 = p_1^{u_1} \cdots p_k^{u_k}$, $n_0 = p_1^{v_1} \cdots p_k^{v_k}$, $m_1 = \frac{m}{m_0}$ and $n_1 = \frac{n}{n_0}$. Then $\gcd(m_0, n_0) = 1$. x^{m_1} has order m_0, y^{n_1} has order n_0, and $x^{m_1}y^{n_1}$ has order $m_0 n_0$, where $m_0 n_0$ is the least common multiple of m and n. Therefore, if G contains elements with order m and n, it contains at least one element whose order is the least common multiple of m and n. □

Theorem 4.16. *Let F be a field and let G be a finite multiplicative subgroup of the multiplicative group F^*. Then G is always cyclic.*

Proof. Let g be the number of elements in G and let m be the maximum of the orders of elements in G. Since the order n of an element a is defined as the smallest $n \in \mathbb{N}^*$ such that $a^n = 1$, no order can be greater than g because by Dirichlet's box principle, there exist $j, k \in \{1, \ldots, g+1\}$ such that $a^j = a^k$ with $j < k$, so then $a^{k-j} = 1$ where $k - j \leq g$, so the order of a is less than or equal to g. Therefore $m \leq g$. Also, the order of any element in G divides m because if it wouldn't, there would be an order n of an element in G such that the least common multiple of m and n is strictly greater than m, but since m and n are orders of elements in G, by Lemma 4.15, so is their least common multiple, and no order is greater than m, which would be a contradiction. So since the order of any element $a \in G$ divides m, $a^m = 1 \iff a^m - 1 = 0$, so any element in G is a root to the polynomial $x^m - 1$, so this polynomial has g roots. This polynomial can't have more than m roots, so $g \leq m$. But we also have that $g \geq m$, so $g = m$. If a is the element with order $m = g$, a^k takes g distinct values for $k \in \{1, \ldots, g\}$, so any element $x \in G$ is of the form $x = a^k$, so by definition this means that G is cyclic. □

5 Geometric Methods

5.1 Modules

Definition 5.1. Let K be an algebraic number field of dimension n and let $\mu_1, \ldots, \mu_m \in K$. Then the set M of integral linear combinations $c_1\mu_1 + \cdots + c_m\mu_m$ where $c_1, \ldots, c_m \in \mathbb{Z}$ is called a **module** in K. Such a module is denoted $M = \{\mu_1, \ldots, \mu_m\}$. The numbers $\mu_1, \ldots, \mu_m$ are called the **generators** of the module M.

Definition 5.2. Let K be a finite extension of $\mathbb{Q}$ with dimension n. Modules with n linearly independent elements over $\mathbb{Q}$ are called **full** modules, and other modules are called **non-full**.

Definition 5.3. Let K be an algebraic number field, let $M = \{\mu_1, \ldots, \mu_m\}$ and let $\alpha \in K$. Then αM denotes the module $\{\alpha\mu_1, \ldots, \alpha\mu_m\}$.

Theorem 5.4. *Any module $M = \{\mu_1, \ldots, \mu_m\}$ is an additive group.*

Proof. Associativity holds for any elements in K, so it obviously also holds for any elements in $M \subseteq K$. So we need to prove that $0 \in M$, that $\alpha \in M \implies -\alpha \in M$ and that M is closed under addition.
$0 = 0\mu_1 + \cdots + 0\mu_m$ so $0 \in M$.
If $\alpha \in M$, then $\exists c_1, \ldots, c_m \in \mathbb{Z}$ such that $\alpha = c_1\mu_1 + \cdots + c_m\mu_m$. If $c_1, \ldots, c_m \in \mathbb{Z}$, then $-c_1, \ldots, -c_m \in \mathbb{Z}$, so $-\alpha = -c_1\mu_1 + \cdots + -c_m\mu_m \in M$.
Suppose $\alpha = c_1\mu_1 + \cdots + c_m\mu_m \in M$ and $\beta = d_1\mu_1 + \cdots + d_m\mu_m \in M$, with $c_1, \ldots, c_m, d_1, \ldots, d_m \in \mathbb{Z}$. Then $(c_1 + d_1), \ldots, (c_m + d_m) \in \mathbb{Z}$, so $\alpha + \beta = (c_1 + d_1)\mu_1 + \cdots + (c_m + d_m)\mu_m \in M$. □

Corollary 5.5. *If M is a module, then $-M = M$.*

Definition 5.6. Two modules M_1 and M_2 are **similar** if $\exists \alpha \in K^*$ such that $M_1 = \alpha M_2$.

Definition 5.7. Let M be a module over K. Then $\alpha \in K$ is called a **coefficient** of M if $\alpha M \subseteq M$, or equivalently, $\forall \xi \in M$, $\alpha\xi \in M$.

Theorem 5.8. *The set of coefficients D_M of a given module $M = \{\mu_1, \ldots, \mu_m\}$ forms a ring with unity. This ring is called the ring of coefficients of M.*

Proof. Associativity, commutativity and distributivity hold for any elements in K, so they obviously also hold for any elements in $D_M \subseteq K$. So to prove that D_M is a ring, we only need to prove that D_M is closed under addition and multiplication, that $0, 1 \in D_M$ and that if $\alpha \in D_M$, $-\alpha \in D_M$.
To prove that $0 \in D_M$, we need to prove that 0 is a coefficient of M, that is $\forall \xi \in M$, $0\xi = 0 \in M$, which is true.
It's obvious that $1 \in D_M$ since $1M = M \subseteq M$.

Now let $\alpha \in D_M$. Then $\alpha M \subseteq M$, so $-\alpha M = (-\alpha)(-M) = \alpha M \subseteq M$, so $-\alpha \in D_M$.
Now let $\alpha, \beta \in D_M$. We want to prove that $\alpha + \beta \in D_M$ and $\alpha\beta \in D_M$. $\forall \xi \in M$, $\alpha\xi \in M$ and $\beta\xi \in M$. Since M is an additive group, $(\alpha + \beta)\xi = \alpha\xi + \beta\xi \in M$, so D_M is closed under addition. Since $\beta \in D_M$, $\beta\xi \in M$, so let $\xi_1 = \beta\xi \in M$. Then $(\alpha\beta)\xi = \alpha(\beta\xi) = \alpha\xi_1 \in M$ since $\alpha \in D_M$ and $\xi_1 \in M$. Therefore, $\alpha\beta \in D_M$ so D_M is closed under multiplication. □

5.2 Geometric Representations

Definition 5.9. We denote $L^{s,t}$ the set of all vectors $\vec{x} = (x_1, \ldots, x_s, x_{s+1}, \ldots, x_{s+t})$ where $x_1, \ldots, x_s \in \mathbb{R}$ and $x_{s+1}, \ldots, x_{s+t} \in \mathbb{C}$ (these can also be real but they don't have to be). We define addition and multiplication over $L^{s,t}$ componentwise.

$L^{s,t}$ can be seen as a vector space over $\mathbb{R}$ with basis vectors $\vec{e_1}, \ldots, \vec{e_s}, \vec{e_{s+1}}, i\vec{e_{s+1}}, \ldots, \vec{e_{s+t}}, i\vec{e_{s+t}}$ where $\vec{e_j}$ is the vector in $\mathbb{R}^{s+t}$ with a 1 in the jth position and zeros everywhere else. This vector space is of dimension $n = s + 2t$ because that's how many basis vectors there are. In this vector space, $\vec{x} = (x_1, \ldots, x_s, x_{s+1}, \ldots, x_{s+t})$ has coordinates $(x_1, \ldots, x_s, \mathrm{Re}(x_{s+1}), \mathrm{Im}(x_{s+1}), \ldots, \mathrm{Re}(x_{s+t}), \mathrm{Im}(x_{s+t}))$. Therefore $L^{s,t}$ can be seen as $\mathbb{R}^{s+2t}$.

Definition 5.10. Let $\vec{x} \in L^{s,t}$. We define the **norm** of $\vec{x}$ to be $N(\vec{x}) = x_1 \cdots x_s |x_{s+1}|^2 \cdots |x_{s+t}|^2$.

Theorem 5.11. *Let $\vec{x}, \vec{y} \in L^{s,t}$. Then $N(\vec{x}\vec{y}) = N(\vec{x})N(\vec{y})$ where $\vec{x}\vec{y}$ is the componentwise multiplication.*

Proof.

$$\begin{aligned} N(\vec{x}\vec{y}) &= x_1 y_1 \cdots x_s y_s |x_{s+1} y_{s+1}|^2 \cdots |x_{s+t} y_{s+t}|^2 \\ &= x_1 \cdots x_s |x_{s+1}|^2 \cdots |x_{s+t}|^2 y_1 \cdots y_s |y_{s+1}|^2 \cdots |y_{s+t}|^2 \\ &= N(\vec{x})N(\vec{y}) \end{aligned}$$

□

Theorem 5.12. *Let $\vec{a} \in L^{s,t}$. Then $N(\vec{a}) = \det(A)$ where A is the matrix of the linear transformation $f(\vec{x}) = \vec{a}\vec{x}$ where $\vec{a}\vec{x}$ is the componentwise multiplication.*

Proof. Let $b_j = \mathrm{Re}(a_{s+j})$, $c_j = \mathrm{Im}(a_{s+j})$, $y_j = \mathrm{Re}(x_{s+j})$ and $z_j = \mathrm{Im}(x_{s+j})$ for $j \in \{1, \ldots, t\}$, and consider $\vec{a}$ and $\vec{x}$ to be vectors in $\mathbb{R}^{s+2t}$ as defined above. Then in order to get the matrix A, we calculate the product $\vec{a}\vec{x}$ (this product is the componentwise product over $L^{s,t}$, not over $\mathbb{R}^{s+2t}$). The first s components are the same over $L^{s,t}$ and over $\mathbb{R}^{s+2t}$ so they're easy. For the other components, we multiply them together in $L^{s,t}$ and take their real and imaginary parts to get their coordinates in $\mathbb{R}^{s+2t}$:

$$\begin{aligned} A\vec{x} &= f(\vec{x}) \\ &= \vec{a}\vec{x} \\ &= (a_1 x_1, \ldots, a_s x_s, \mathrm{Re}(a_{s+1}x_{s+1}), \mathrm{Im}(a_{s+1}x_{s+1}), \ldots, \mathrm{Re}(a_{s+t}x_{s+t}), \mathrm{Im}(a_{s+t}x_{s+t})) \\ &= (a_1 x_1, \ldots, a_s x_s, \mathrm{Re}((b_1 + ic_1)(y_1 + iz_1)), \ldots, \mathrm{Im}((b_t + ic_t)(y_t + iz_t))) \\ &= (a_1 x_1, \ldots, a_s x_s, b_1 y_1 - c_1 z_1, c_1 y_1 + b_1 z_1, \ldots, b_t y_t - c_t z_t, c_t y_t + b_t z_t) \\ &= \begin{pmatrix} a_1 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & a_s & 0 & 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & b_1 & -c_1 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & c_1 & b_1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & b_t & -c_t \\ 0 & \cdots & 0 & 0 & 0 & \cdots & c_t & b_t \end{pmatrix} \vec{x} \end{aligned}$$

Now we have the matrix A, so we need to calculate its determinant:

$$\begin{aligned}
\det(A) &= \det \begin{pmatrix}
a_1 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\
\vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & \cdots & a_s & 0 & 0 & \cdots & 0 & 0 \\
0 & \cdots & 0 & b_1 & -c_1 & \cdots & 0 & 0 \\
0 & \cdots & 0 & c_1 & b_1 & \cdots & 0 & 0 \\
\vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & \cdots & 0 & 0 & 0 & \cdots & b_t & -c_t \\
0 & \cdots & 0 & 0 & 0 & \cdots & c_t & b_t
\end{pmatrix} \\
&= a_1 \cdots a_s \det \begin{pmatrix} b_1 & -c_1 \\ c_1 & b_1 \end{pmatrix} \cdots \det \begin{pmatrix} b_t & -c_t \\ c_t & b_t \end{pmatrix} \\
&= a_1 \cdots a_s (b_1^2 + c_1^2) \cdots (b_t^2 + c_t^2) \\
&= a_1 \cdots a_s |a_{s+1}|^2 \cdots |a_{s+t}|^2 \\
&= N(\vec{a})
\end{aligned}$$

□

Definition 5.13. Let K be a finite extension of $\mathbb{Q}$ and let $\alpha \in K$. Let $\sigma_1, \ldots, \sigma_s$ be the real conjugates over K and let $\sigma_{s+1}, \overline{\sigma_{s+1}}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+t}}$ be the complex conjugates over K. Then we define the **geometric representation** of α denoted as $x(\alpha) \in L^{s,t}$ by $x(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha))$.

Example 5.14. Let $K = \mathbb{Q}[\sqrt{2}]$ and let $\alpha = 1 + \sqrt{2}$. The conjugates over K are $\sigma_1(z) = z$ and $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$, so $s = 2$ and $t = 0$. So the geometric representation of $\alpha = 1 + \sqrt{2}$ is $x(\alpha) = (1 + \sqrt{2}, 1 - \sqrt{2})$.

Example 5.15. Let $K = \mathbb{Q}[i\sqrt{2}]$ and let $\alpha = 1 + i\sqrt{2}$. The conjugates over K are $\sigma_1(z) = z$ and $\sigma_2(z) = \bar{z}$, so $s = 0$ and $t = 1$. So the geometric representation of $\alpha = 1 + i\sqrt{2}$ is $x(\alpha) = 1 + i\sqrt{2}$.

Lemma 5.16. *The mapping $\alpha \mapsto x(\alpha)$ from K to $L^{s,t}$ of an element onto its geometric representation is injective.*

Proof. Let $\alpha, \beta \in K$ and suppose that $\alpha \neq \beta$. Since each σ_j is a conjugate and therefore a monomorphism, it is injective, so $\sigma_j(\alpha) \neq \sigma_j(\beta)$, which means that $x(\alpha) \neq x(\beta)$, so the mapping is injective. □

Remark: This mapping is not bijective since K has the same set cardinality as $\mathbb{Q}^n$ which is countable and $L^{s,t}$ has the same set cardinality as $\mathbb{R}^n$ which is not countable, so there can't be any bijection from one to the other. Therefore there exist points in $L^{s,t}$ that are not geometric representations of any element in K.

Theorem 5.17. *The mapping $\alpha \mapsto x(\alpha)$ of an element onto its geometric representation is a monomorphism from K into $L^{s,t}$.*

Proof. By Lemma 5.16, we know that this mapping is injective from K to $L^{s,t}$, so all we need to prove is that it's a homomorphism from K to $L^{s,t}$. This means that we need to prove that it satisfies the three conditions from the definition of a homomorphism: $x(\alpha + \beta) = x(\alpha) + x(\beta)$, $x(\alpha\beta) = x(\alpha)x(\beta)$ and $x(1)$ is a unity in $L^{s,t}$. Since all σ_j's are homomorphisms, these three conditions hold componentwise and since addition and multiplication over $L^{s,t}$ are defined componentwise they hold for the mapping into $L^{s,t}$. □

Theorem 5.18. *Let $\alpha \in K$ and let $x(\alpha) \in L^{s,t}$ be its geometric representation. Then $N(\alpha) = N(x(\alpha))$ where $N(\alpha)$ is the norm over K and $N(x(\alpha))$ is the norm over $L^{s,t}$.*

Proof. $N(\alpha)$ is by definition the product of the conjugates of α. If we divide these conjugates up into real and complex conjugates as above, we get:

$$\begin{aligned}
N(\alpha) &= \sigma_1(\alpha) \cdots \sigma_s(\alpha) \sigma_{s+1}(\alpha) \overline{\sigma_{s+1}(\alpha)} \cdots \sigma_{s+t}(\alpha) \overline{\sigma_{s+t}(\alpha)} \\
&= \sigma_1(\alpha) \cdots \sigma_s(\alpha) |\sigma_{s+1}(\alpha)|^2 \cdots |\sigma_{s+t}(\alpha)|^2 \\
&= x_1 \cdots x_s |x_{s+1}|^2 \cdots |x_{s+t}|^2 \\
&= N(x(\alpha)).
\end{aligned}$$

□

5.3 Lattices

Definition 5.19. Let $\vec{e_1}, \ldots, \vec{e_m}$ be linearly independent vectors in $\mathbb{R}^n$. Then the set of integral linear combinations $a_1\vec{e_1} + \cdots + a_m\vec{e_m}$, $a_1, \ldots, a_m \in \mathbb{Z}$ is called an m-dimensional **lattice** in $\mathbb{R}^n$. If $m = n$, the lattice is called **full**, otherwise it's called **non-full**. $\vec{e_1}, \ldots, \vec{e_m}$ is called a **basis** of the lattice. The basis of a certain lattice is not unique.

Theorem 5.20. *Let K be a finite extension of $\mathbb{Q}$ of dimension n and let $M = \{\mu_1, \ldots, \mu_n\}$ be a full module in K. Then the set of geometric representations of elements of M in $\mathbb{R}^n$ is a full lattice with basis $x(\mu_1), \ldots, x(\mu_n)$.*

Proof. By Theorem 5.17, the mapping of an element of K onto its geometric representation is a monomorphism, so we have

$$x(c_1\mu_1 + \cdots + c_n\mu_n) = c_1x(\mu_1) + \cdots + c_nx(\mu_n) \tag{5.20.1}$$

for $c_1, \ldots, c_n \in \mathbb{Z}$. By the definition of a module, M is the set of elements $c_1\mu_1 + \cdots + c_n\mu_n$, so the set of geometric representations of the elements of M is the set of elements of the form $x(c_1\mu_1 + \cdots + c_n\mu_n)$, $c_1, \ldots, c_n \in \mathbb{Z}$. So each geometric representation of an element of M equals an integral linear combination of $x(\mu_1), \ldots, x(\mu_n)$, and each integral linear combination of these vectors equals the geometric representation of an element in M, which concludes the proof. □

Definition 5.21. Let $r > 0$. Then the **ball** $U(r) \subset \mathbb{R}^n$ of radius r is the set of vectors $\vec{x} \in \mathbb{R}^n$ such that $||\vec{x}|| < r$, where $||\vec{x}||$ is the standard 2-norm.

Definition 5.22. A set $S \subseteq \mathbb{R}^n$ is called **discrete** if $\forall r > 0$, $S \cap U(r)$ only contains finitely many elements.

Theorem 5.23. *Any lattice is discrete.*

Proof. Any non-full lattice is a subset of a full lattice, so if the theorem holds for any full lattice it holds for any lattice, so we only need to consider full lattices. Let M be a full lattice, and let $\vec{e_1}, \ldots, \vec{e_n}$ be a basis for M. Consider the system of linear equations

$$\begin{cases} \vec{x} \cdot \vec{e_2} = 0 \\ \vdots \\ \vec{x} \cdot \vec{e_n} = 0 \end{cases}$$

where $\vec{x} \cdot \vec{e_j}$ is the standard euclidean scalar product. This system is underdetermined and homogeneous, so there are infinitely many solutions, so there exists a non-zero solution $\vec{x_0}$. If we add the condition $\vec{x} \cdot \vec{e_1} = 0$, we get n equations and n unknowns, so the only solution would be the zero vector, so $\vec{x_0}$ isn't a solution to $\vec{x} \cdot \vec{e_1} = 0$ (since it is a solution to the other equations), so $\vec{x_0} \cdot \vec{e_1} \neq 0$ so we can divide by $\vec{x_0} \cdot \vec{e_1}$. Consider the vector $\vec{f_1} = \frac{\vec{x_0}}{\vec{x_0} \cdot \vec{e_1}}$. We have $\vec{f_1} \cdot \vec{e_1} = 1$ and $\vec{f_1} \cdot \vec{e_j} = 0$ for $j \neq 1$. Similarly, for any integer $k \leq n$, we can find a vector $\vec{f_k}$ such that $\vec{f_k} \cdot \vec{e_k} = 1$ and $\vec{f_k} \cdot \vec{e_j} = 0$ for $j \neq k$.
Now let $r > 0$ and let $\vec{z} = a_1\vec{e_1} + \cdots + a_n\vec{e_n} \in M \cap U(r)$, $a_1, \ldots, a_n \in \mathbb{Z}$, and consider $\vec{z} \cdot \vec{f_k}$:

$$\begin{aligned} \vec{z} \cdot \vec{f_k} &= (a_1\vec{e_1} + \cdots + a_n\vec{e_n}) \cdot \vec{f_k} \\ &= a_1\vec{e_1} \cdot \vec{f_k} + \cdots + a_n\vec{e_n} \cdot \vec{f_k} \\ &= a_k\vec{e_k} \cdot \vec{f_k} \\ &= a_k. \end{aligned}$$

By using this together with the Cauchy-Schwartz inequality we get:

$$\begin{aligned} |a_k| &= |\vec{z} \cdot \vec{f_k}| \\ &\leq ||\vec{z}||||\vec{f_k}|| \\ &< r||\vec{f_k}||. \end{aligned}$$

Since $r||\vec{f_k}||$ doesn't depend on $\vec{z}$ or any a_j, this means that with a given r there are only finitely many ways to choose each a_k since $a_k \in \mathbb{Z}$ and $|a_k| < r||\vec{f_k}||$, so there are only finitely many ways to choose a vector $\vec{z}$ in the set $M \cap U(r)$, which concludes the proof. □

Definition 5.24. Let M be a lattice with basis $\vec{e_1}, \ldots, \vec{e_m}$. Then the set of vectors of the form $b_1\vec{e_1} + \cdots + b_m\vec{e_m}$ where $0 \leq b_j < 1$ is called a **fundamental parallelepiped** of M. Fundamental parallelepipeds of a lattice are not unique, they depend on the choice of basis.

Theorem 5.25. *Let M be a full lattice in $\mathbb{R}^n$ and let T be a fundamental parallelepiped of M. Then the sets $T_z = T + \vec{z}$ where $\vec{z}$ runs through all elements of M are disjoint and fill the entire space $\mathbb{R}^n$.*

Proof. Let $\vec{e_1}, \ldots, \vec{e_n}$ be the basis of M used to construct T. We need to prove that any vector $\vec{x} \in \mathbb{R}^n$ belongs to exactly one T_z. Let $\vec{x} = x_1\vec{e_1} + \cdots + x_n\vec{e_n}$ be an arbitrary vector in $\mathbb{R}^n$. Let $a_k = \lfloor x_k \rfloor$ be the integer part of x_k and let $b_k = x_k - a_k$ be the fractional part of x_k. Let $\vec{z} = a_1\vec{e_1} + \cdots + a_n\vec{e_n} \in M$ and let $\vec{u} = b_1\vec{e_1} + \cdots + b_n\vec{e_n} \in T$. Since $\vec{x} = \vec{z} + \vec{u}$, $x \in T_z$, so each $\vec{x}$ lies in at least one T_z. Suppose $\exists \vec{z'} \in M$ such that $\vec{x}$ also lies in $T_{z'}$, and let $\vec{u'} = \vec{x} - \vec{z'}$. Then we have $\vec{u} + \vec{z} = \vec{x} = \vec{u'} + \vec{z'}$ and $\vec{u'} \in T$. The only way to get this is if $\vec{z} = \vec{z'}$, which concludes the proof. □

Theorem 5.26. *For any $r > 0$, there are only a finite number of sets T_z such that $T_z \cap U(r) \neq \emptyset$.*

Proof. Let $\vec{e_1}, \ldots, \vec{e_n}$ be the basis of M used to construct T. If $T_z \cap U(r) \neq \emptyset$, there exists at least one element $\vec{x}$ in $T_z \cap U(r)$, which means that T_z contains at least one element $\vec{x}$ such that $||\vec{x}|| < r$. Let $\vec{u} = \vec{x} - \vec{z} = b_1\vec{e_1} + \cdots + b_n\vec{e_n}$. Since $\vec{u} \in T$, $|b_j| < 1 \ \forall j \leq n$, so by the triangle inequality:

$$\begin{aligned} ||\vec{z}|| &= ||\vec{u} - \vec{x}|| \\ &= ||b_1\vec{e_1} + \cdots + b_n\vec{e_n} + \vec{x}|| \\ &\leq |b_1|||\vec{e_1}|| + \cdots + |b_n|||\vec{e_n}|| + ||\vec{x}|| \\ &< ||\vec{e_1}|| + \cdots + ||\vec{e_n}|| + r. \end{aligned}$$

$||\vec{e_1}|| + \cdots + ||\vec{e_n}|| + r$ doesn't depend on $\vec{x}$ or $\vec{z}$, so $\vec{z} \in U(||\vec{e_1}|| + \cdots + ||\vec{e_n}|| + r)$. There are only finitely many such $\vec{z}$ which concludes the proof. □

Definition 5.27. An additive group G is called **finitely generated** if there exist finitely many elements $x_1, \ldots, x_m \in G$ such that any $x \in G$ can be written as $x = c_1x_1 + \cdots + c_mx_m$ where $c_1, \ldots, c_m \in \mathbb{Z}$. $x_1, \ldots, x_m$ are called **generators** of G.

Lemma 5.28. *Let M be a finitely generated additive group without elements of finite order and with m generators, and let N be a subgroup of M. Then N has a finite basis with $l \leq m$ elements.*

Proof. Let $x_1, \ldots, x_m$ be a basis for M. We will prove by induction on m that N has a basis of the type

$$\begin{aligned} \eta_1 &= c_{1,1}x_1 + \cdots + c_{1,l}x_l + \cdots + c_{1,m}x_m \\ &\cdots \\ \eta_l &= c_{l,l}x_l + \cdots + c_{l,m}x_m. \end{aligned}$$

If $m = 0$, then $M = N = \{0\}$, so then N has a zero-dimensional basis so the theorem holds for $m = 0$. Now let $m \geq 1$ and assume the theorem holds for $m-1$. If $N = \{0\}$, then N has a zero-dimensional basis and we're done, so we can assume that N contains at least one non-zero element α. Since $\alpha \in N \subseteq M$, α can be written as

$$\alpha = c_1x_1 + \cdots + c_mx_m$$

where $c_1, \ldots, c_m \in \mathbb{Z}$. Since we assumed that $\alpha \neq 0$, at least one of the c_j's is non-zero. By reordering the basis, we can assume that $c_1 \neq 0$. Let

$$\eta_1 = c_{1,1}x_1 + \cdots + c_{1,m}x_m$$

be the element in N such that $c_{1,1} > 0$ is smallest. Let $c_1 = c_{1,1}q_1 + r_1$ where $q_1 \in \mathbb{Z}$ and $0 \leq r_1 < c_{1,1}$. We have that

$$\alpha - q_1\eta_1 = r_1x_1 + r_2x_2 + \cdots + r_mx_m \tag{5.28.1}$$

for some $r_2, \ldots, r_m$. Since $\alpha, \eta_1 \in N$, $\alpha - q_1\eta_1 \in N$. By the definition of η_1, there is no element in N such that the coefficient of x_1 is strictly between 0 and $c_{1,1}$, and since $0 \leq r_1 < c_{1,1}$, this means that $r_1 = 0$, so $c_{1,1}$ divides c_1.

Let M_0 be the group generated by $x_2, \ldots, x_m$. $N \cap M_0$ is a subgroup of M_0, so by the induction hypothesis, $N \cap M_0$ has a basis of the type

$$\begin{aligned} \eta_2 &= c_{2,2}x_2 + \cdots + c_{2,l}x_l + \cdots + c_{2,m}x_m \\ &\cdots \\ \eta_l &= c_{l,l}x_l + \cdots + c_{l,m}x_m. \end{aligned}$$

Since we proved that $r_1 = 0$, equation (5.28.1) becomes

$$\alpha - q_1\eta_1 = r_2x_2 + \cdots + r_mx_m.$$

Therefore, $\alpha - q_1\eta_1 \in M_0 \cap N$, so by the induction hypothesis, $\exists q_2, \ldots, q_m \in \mathbb{Z}$ such that

$$\begin{aligned} &\alpha - q_1\eta_1 = q_2\eta_2 + \cdots + q_m\eta_m \\ \iff &\alpha = q_1\eta_1 + q_2\eta_2 + \cdots + q_m\eta_m. \end{aligned}$$

Since α was an arbitrary non-zero element of N and $\eta_1, \ldots, \eta_m$ don't depend on α, any $\alpha \in N^*$ is an integral linear combination of $\eta_1, \ldots, \eta_m$. Also, it's trivial that 0 is an integral linear combination of $\eta_1, \ldots, \eta_m$, so any $\alpha \in N$ is an integral linear combination of $\eta_1, \ldots, \eta_m$. Therefore, $\eta_1, \ldots, \eta_m$ form a basis for N, which concludes the proof. □

Theorem 5.29. *Any discrete additive group $M \subset \mathbb{R}^n$ is a lattice.*

Proof. Let G be the smallest linear subspace of $\mathbb{R}^n$ which contains M, let m be the dimension of G and let $\vec{e_1}, \ldots, \vec{e_m}$ be elements of M which form a basis for G. Let M_0 be the lattice spanned by $\vec{e_1}, \ldots, \vec{e_m}$. Since M is an additive group containing $\vec{e_1}, \ldots, \vec{e_m}$, any integral linear combination of these vectors is also in M, so $M_0 \subseteq M$.
Let T be the fundamental parallelepiped of M_0. Then by Theorem 5.25, $\forall \vec{x} \in \mathbb{R}^n$, $\exists \vec{u} \in T, \vec{z} \in M_0$ such that $\vec{x} = \vec{u} + \vec{z}$. Since $\vec{z} \in M_0 \subseteq M$, if $\vec{x} \in M$, then $\vec{u} \in M$ since $\vec{x} = \vec{u} + \vec{z}$ and M is an additive group. We also know that $\vec{u} \in T$ so $||\vec{u}|| \leq r$ where $r = ||\vec{e_1}|| + \cdots + ||\vec{e_m}||$, so $\vec{u} \in M \cap U(r)$. Since M is discrete, there are only finitely many such $\vec{u}$'s. This means that for a given $\vec{z} \in M_0$, we can only find finitely many $\vec{x} \in M$ so the factor group M/M_0 is finite.
Let j be the number of elements in M/M_0. By Theorem 4.14, the order of any element in M/M_0 divides j, which means that any element in M/M_0 multiplied by j is the zero element in M/M_0. Let $\vec{x}$ be any element in M and let $[\vec{x}]$ be the congruence class of $\vec{x}$ mod M_0. Then $[j\vec{x}] = j[\vec{x}] = [\vec{0}]$ since $[\vec{x}] \in M/M_0$ and j times any element in M/M_0 is $[\vec{0}]$. This means that $j\vec{x}$ and $\vec{0}$ are in the same congruence class, so $j\vec{x} \equiv \vec{0} \pmod{M_0}$, so $j\vec{x} = j\vec{x} - \vec{0} \in M_0$. This means that $j\vec{x}$ is an integral linear combination of $\vec{e_1}, \ldots, \vec{e_m}$, so $\vec{x}$ is an integral linear combination of $\frac{\vec{e_1}}{j}, \ldots, \frac{\vec{e_m}}{j}$, so M is a subgroup of the lattice with basis $\frac{\vec{e_1}}{j}, \ldots, \frac{\vec{e_m}}{j}$, so by Lemma 5.28 M has a basis $\vec{f_1}, \ldots, \vec{f_l}$ where $l \leq m$. But M contains m linearly independent vectors $\vec{e_1}, \ldots, \vec{e_m}$ so the dimension of M is exactly m, so M is a lattice. □

5.4 Logarithmic Representations

Definition 5.30. Let K be a finite extension of $\mathbb{Q}$, let s be the number of real conjugates from K to $\mathbb{C}$ and let $2t$ be the number of complex conjugates from K to $\mathbb{C}$, and let $\vec{x} \in L^{s,t}$ such that $x_j \neq 0 \ \forall j \leq s + t$. Then the **logarithmic representation** of $\vec{x}$ in $\mathbb{R}^{s+t}$ is defined as $l(\vec{x}) = (\ln|x_1|, \ldots, \ln|x_s|, \ln|x_{s+1}^2|, \ldots, \ln|x_{s+t}^2|)$.

Theorem 5.31. *Let $\vec{x}, \vec{y} \in L^{s,t}$ with all their components non-zero. Then $l(\vec{x}\vec{y}) = l(\vec{x}) + l(\vec{y})$. This means that the mapping $\vec{x} \mapsto l(\vec{x})$ is a homomorphism from the multiplicative group of vectors in $L^{s,t}$ with non-zero components to the additive group $\mathbb{R}^{s+t}$.*

Proof.

$$\begin{aligned} l(\vec{x}\vec{y}) &= l(x_1y_1, \ldots, x_{s+t}y_{s+t}) \\ &= (\ln|x_1y_1|, \ldots, \ln|x_sy_s|, \ln|(x_{s+1}y_{s+1})^2|, \ldots, \ln|(x_{s+t}y_{s+t})^2|) \\ &= (\ln|x_1y_1|, \ldots, \ln|x_sy_s|, \ln|x_{s+1}^2y_{s+1}^2|, \ldots, \ln|x_{s+t}^2y_{s+t}^2|) \\ &= (\ln|x_1| + \ln|y_1|, \ldots, \ln|x_s| + \ln|y_s|, \ln|x_{s+1}^2| + \ln|y_{s+1}^2|, \ldots, \ln|x_{s+t}^2| + \ln|y_{s+t}^2|) \\ &= (\ln|x_1|, \ldots, \ln|x_s|, \ln|x_{s+1}^2|, \ldots, \ln|x_{s+t}^2|) + (\ln|y_1|, \ldots, \ln|y_s|, \ln|y_{s+1}^2|, \ldots, \ln|y_{s+t}^2|) \\ &= l(\vec{x}) + l(\vec{y}) \end{aligned}$$

□

Theorem 5.32. *Let $\vec{x} \in L^{s,t}$ with norm $N(\vec{x}) \neq 0$. Then $\sum_{k=1}^{s+t} l_k(\vec{x}) = \ln|N(\vec{x})|$.*

Proof.

$$\begin{aligned}\sum_{k=1}^{s+t} l_k(\vec{x}) &= \ln|x_1| + \cdots + \ln|x_s| + \ln|x_{s+1}^2| + \cdots + \ln|x_{s+t}^2| \\ &= \ln(|x_1|\cdots|x_s||x_{s+1}^2|\cdots|x_{s+t}^2|) \\ &= \ln|x_1\cdots x_s|x_{s+t}^2|\cdots|x_{s+t}^2|| \\ &= \ln|N(\vec{x})|\end{aligned}$$

□

Definition 5.33. Let $\alpha \in K^*$ and let $x(\alpha)$ be the geometric representation of α. Then the **logarithmic representation** of α is defined as $l(\alpha) = l(x(\alpha))$.

Theorem 5.34. *Let $\alpha, \beta \in K^*$. Then $l(\alpha\beta) = l(\alpha) + l(\beta)$.*

Proof.

$$\begin{aligned}l(\alpha\beta) &= l(x(\alpha\beta)) \\ &= l(x(\alpha)x(\beta)) \\ &= l(x(\alpha)) + l(x(\beta)) \\ &= l(\alpha) + l(\beta)\end{aligned}$$

□

Theorem 5.35. *Let $\alpha \in K^*$ and let α^{-1} be the multiplicative inverse of α. Then $l(\alpha^{-1}) = -l(\alpha)$.*

Proof.

$$\begin{aligned}l(\alpha^{-1}) &= l(\alpha^{-1}) + l(\alpha) - l(\alpha) \\ &= l(\alpha^{-1}\alpha) - l(\alpha) \\ &= l(1) - l(\alpha) \\ &= l(x(1)) - l(\alpha) \\ &= l(1,\ldots,1) - l(\alpha) \\ &= (\ln|1|,\ldots,\ln|1|,\ln|1^2|,\ldots,\ln|1^2|) - l(\alpha) \\ &= \vec{0} - l(\alpha) \\ &= -l(\alpha)\end{aligned}$$

□

Corollary 5.36. $l(1) = \vec{0}$

Theorem 5.37. *Let $\alpha \in K^*$. Then $\sum_{k=1}^{s+t} l_k(\alpha) = \ln|N(\alpha)|$.*

Proof.

$$\sum_{k=1}^{s+t} l_k(\alpha) = \sum_{k=1}^{s+t} l_k(x(\alpha)) = \ln|N(x(\alpha))| = \ln|N(\alpha)|$$

□

6 Units

By studying the structure of the set of elements with norm ± 1, it will be relatively easy to study the set of solutions to equation (3.24.2). As we will prove in theorem Theorem 6.5, units are elements with norm equal to ± 1, which is why units are important in the main theorem of this thesis.

6.1 Orders and Units

Definition 6.1. A full module $D \subset K$ which is a ring containing the number 1 is called an **order** of K (not to be confused with the order of an element of a group in Definition 4.12).

Definition 6.2. Let K be a finite extension of $\mathbb{Q}$, and let D be an order of K. Then an element $\varepsilon \in D$ is called a **unit** of D if $\varepsilon^{-1} \in D$ (not to be confused with unity in Definition 2.4).

Lemma 6.3. *Let K be a finite extension of $\mathbb{Q}$, and let D be an order of K. Then if $\alpha \in D$, then its characteristic polynomial has integer coefficients.*

Proof. By definition, D is a ring, so if $e_1, \ldots, e_n$ is a basis for D, $\alpha e_1, \ldots, \alpha e_n$ are all in D. Since $e_1, \ldots, e_n$ is a basis for D and D is a module, each of the numbers $\alpha e_1, \ldots, \alpha e_n$ are integral linear combinations of $e_1, \ldots, e_n$. Therefore the transformation matrix for this linear transformation only contains integers, so its characteristic polynomial which is also the characteristic polynomial of α has integer coefficients. □

Corollary 6.4. *Let K be a finite extension of $\mathbb{Q}$, and let D be an order of K. Then if $\alpha \in D$, $N(\alpha) \in \mathbb{Z}$.*

Proof. By Theorem 3.16, $N(\alpha)$ is plus or minus the characteristic polynomial of α evaluated at 0. By Lemma 6.3, the coefficients of the characteristic polynomial are integers, so the characteristic polynomial of α evaluated at 0 is an integer. □

Theorem 6.5. *Let K be a finite extension of $\mathbb{Q}$, and let D be an order of K. Then a number $\varepsilon \in D$ is a unit of D if and only if $N(\varepsilon) = \pm 1$.*

Proof. $\implies$: Let ε be a unit of D. Then $\exists \varepsilon^{-1} \in D$ such that $\varepsilon\varepsilon^{-1} = 1$. This means that

$$\begin{aligned} N(\varepsilon)N(\varepsilon^{-1}) &= N(\varepsilon\varepsilon^{-1}) \\ &= N(1) \\ &= 1. \end{aligned}$$

Since $\varepsilon, \varepsilon^{-1} \in D$, $N(\varepsilon), N(\varepsilon^{-1}) \in \mathbb{Z}$, and therefore $N(\varepsilon) = \pm 1$.

$\impliedby$: Let $\alpha \in D$ such that $N(\alpha) = \pm 1$. Consider the characteristic polynomial of α

$$\phi_\alpha(\lambda) = \lambda^n + c_{n-1}\lambda^{n-1} + \cdots + c_0.$$

By Theorem 3.16, $c_0 = (-1)^n N(\alpha)$. By Lemma 6.3, $c_0, \ldots, c_{n-1} \in \mathbb{Z}$. By Corollary 2.23 the minimal polynomial of α divides the characteristic polynomial of α, so $\phi_\alpha(\alpha) = 0$, so $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha = (-1)^{n+1}N(\alpha)$. By dividing by $(-1)^{n+1}\alpha$ on both sides, we get that $\frac{N(\alpha)}{\alpha}$ is an integral linear combination of powers of α, and therefore $\frac{N(\alpha)}{\alpha} \in D$. Since $N(\alpha) = \pm 1$, $\frac{1}{\alpha} \in D$, so by definition α is a unit of D. □

6.2 Associate Elements

Definition 6.6. Two elements in D are called **associate** if they divide each other in D.

Lemma 6.7. *All elements of an order D with a given norm are in one of only finitely many associate classes. By associate class we mean the equivalence class with respect to the equivalence relation of two elements being associate (proving that being associate is an equivalence relation is trivial).*

Proof. Let $w_1, \ldots, w_n$ be a basis for D and let $\alpha, \beta \in D$ such that $|N(\alpha)| = |N(\beta)|$ and $\alpha \equiv \beta \pmod{c}$ where $c = |N(\alpha)| = |N(\beta)|$. It's clear that for any $\alpha_0 \in D$ there exists a unique $x = x_1w_1 + \cdots + x_nw_n \in D$ where $0 \leq x_j < c \ \forall j \in \{1, \ldots, n\}$ such that $\alpha_0 \equiv x \pmod{c}$. Therefore D contains c^n congruence classes mod c. Since $\alpha \equiv \beta \pmod{c}$, $\exists \gamma \in D$ such that $\alpha - \beta = c\gamma$. By dividing by β on each side and since $c = |N(\beta)|$, we get:

$$\begin{aligned} &\alpha - \beta = c\gamma \\ \iff &\frac{\alpha}{\beta} - 1 = \frac{c}{\beta}\gamma = \frac{|N(\beta)|}{\beta}\gamma. \end{aligned}$$

From the proof of Theorem 6.5, we know that $\frac{|N(\beta)|}{\beta} \in D$. Also, $\gamma \in D$ and $1 \in D$, so $\frac{\alpha}{\beta} \in D$, which means that β divides α in D. Similarly, we get that α divides β in D, so α and β are associate. Since the elements with norm of a given absolute value c must belong to one of the c^n congruence classes and all such elements in a congruence class belong to the same associate class, they must belong to one of no more than c^n associate classes, which proves the theorem. □

Lemma 6.8. *If two elements $\alpha, \beta \in D$ are associate, then the absolute values of their norms are equal.*

Proof. Let $\gamma_1, \gamma_2 \in D$ such that $\alpha = \gamma_1\beta$ and $\beta = \gamma_2\alpha$. Then $N(\alpha) = N(\gamma_1)N(\beta)$ and $N(\beta) = N(\gamma_2)N(\alpha)$. Since $\gamma_1, \gamma_2 \in D$, $N(\gamma_1), N(\gamma_2) \in \mathbb{Z}$, so this means that $N(\alpha)$ and $N(\beta)$ divide each other in $\mathbb{Z}$. Two integers divide each other if and only if their absolute values are equal, which proves the theorem. □

Corollary 6.9. *If two elements $\alpha, \beta \in D$ are associate, then there exists a unit $\varepsilon \in D$ such that $\alpha = \varepsilon\beta$.*

Proof. Since α and β divide each other in D, $\exists\gamma \in D$ such that $\alpha = \gamma\beta$. Since the norm is multiplicative, $N(\alpha) = N(\gamma)N(\beta)$, and by Lemma 6.8, $N(\alpha) = \pm N(\beta)$, so $N(\gamma) = \pm 1$, so by Theorem 6.5 γ is a unit. □

6.3 Geometric Representation of Units

Lemma 6.10. *Let K be a finite extension of $\mathbb{Q}$, let D be an arbitrary order of K and let W be the set of units ε of D with logarithmic representation $l(\varepsilon) = \vec{0}$. Then W is a cyclic multiplicative group with a finite and even number of elements.*

Proof. First we prove that W is a multiplicative group. It's obvious that multiplication is associative over W since it's associative over K. If $\alpha, \beta \in W$, $l(\alpha) = l(\beta) = \vec{0}$, so

$$\begin{aligned} l(\alpha\beta) &= l(\alpha) + l(\beta) \\ &= \vec{0} + \vec{0} \\ &= \vec{0} \\ \implies \alpha\beta &\in W \end{aligned}$$

so W is closed under multiplication. We know that $l(1) = \vec{0}$, so $1 \in W$. If $\alpha \in W$, then $l(\alpha^{-1}) = -l(\alpha) = -\vec{0} = \vec{0}$, so $\alpha^{-1} \in W$. Therefore all conditions for W being a multiplicative group are satisfied, so W is a multiplicative group.
Now we want to prove that the number of elements in W is finite:

$$\begin{aligned} \alpha \in W &\iff l(\alpha) = \vec{0} \\ &\iff \ln|x_k(\alpha)| = 0 \ \forall k \in \{1, \dots, s+t\} \\ &\iff |x_k(\alpha)| = 1 \ \forall k \in \{1, \dots, s+t\} \\ &\iff ||x(\alpha)|| = \sqrt{s+t}. \end{aligned}$$

Therefore the norm of $x(\alpha)$ is bounded. Since $\alpha \in W \subseteq D$ and D is a module, the set of geometric representations $x(\alpha)$ of elements $\alpha \in W$ is a subset of a lattice, and is therefore discrete by Theorem 5.23. Since $x(\alpha)$ is bounded and is in a discrete set, there are only finitely many possible values $x(\alpha)$. Since the mapping $\alpha \mapsto x(\alpha)$ is injective, this means that there are only finitely many $\alpha \in W$.
Since W is a finite multiplicative subgroup of the field K, by Theorem 4.16, W is cyclic.
The multiplicative group $\{1, -1\}$ is a subgroup of W and has two elements, so the number of elements in the subgroup $\{1, -1\}$ divides the number of elements in W, so by Theorem 4.13 the number of elements in W is even. □

Lemma 6.11. *Let K be a finite extension of $\mathbb{Q}$, and let D be an order of K. Then an element $\varepsilon \in D$ has logarithmic representation 0 if and only if it is a root of 1, that is $\exists j \in \mathbb{N}^*$ such that $\varepsilon^j = 1$.*

Proof. Let W be defined as in Lemma 6.10.
$\implies$: Since W is a finite multiplicative group, it immediately follows that if $\varepsilon \in W$ then $\exists j \in \mathbb{N}^*$ such that $\varepsilon^j = 1$.

$\impliedby$: Suppose for a contradiction that $\varepsilon^j = 1$ and $\varepsilon \notin W$, that is $l(\varepsilon) \neq \vec{0}$. That means that for some $k \in \{1, \dots, s+t\}$, $\ln|x_k(\varepsilon)| \neq 0$ (if $k \leq s$ this is obvious and if $k > s$, we get $\ln|x_k(\varepsilon)^2| \neq 0 \iff 2\ln|x_k(\varepsilon)| \neq 0 \iff \ln|x_k(\varepsilon)| \neq 0$). Since $\varepsilon^j = 1$, $x_k(\varepsilon^j) = 1$ so $\ln|x_k(\varepsilon^j)| = 0$. $x_k(\varepsilon^j) = \sigma_k(\varepsilon^j)$ and since σ_k is a conjugate function, it's a homomorphism so $\sigma_k(\varepsilon^j) = \sigma_k(\varepsilon)^j$. Therefore,

$$\begin{aligned} 0 = \ln|x_k(\varepsilon^j)| = \ln|x_k(\varepsilon)^j| &= j\ln|x_k(\varepsilon)| \\ \iff \ln|x_k(\varepsilon)| &= 0. \end{aligned}$$

But we chose k specifically such that $\ln|x_k(\varepsilon)| \neq 0$, which is a contradiction, which proves the theorem. □

Lemma 6.12. *Let $E \subset \mathbb{R}^{s+t}$ be the set of points $l(\varepsilon)$ such that ε is a unit of the order D (not necessarily in W). Then E is a lattice of dimension less than or equal to $s+t-1$.*

Proof. Consider the numbers ε such that $||l(\varepsilon)|| < r$ for some fixed $r > 0$. Then $\forall k \in \{1, \dots, s+t\}$, $l_k(\varepsilon) \leq |l_k(\varepsilon)| \leq ||l(\varepsilon)|| < r$. By taking the exponential on both sides, we get that $|x_j(\varepsilon)| < e^r$ for $j \in \{1, \dots, s\}$ and $|x_k(\varepsilon)|^2 < e^r$ for $k \in \{s+1, \dots, s+t\}$. Therefore the set of $x(\varepsilon)$ such that $||l(\varepsilon)|| < r$ is bounded. We also know from previous theorems that the set of geometric representations $x(\alpha)$ where $\alpha \in K$ is discrete, so the set of $x(\varepsilon)$ is also discrete. Since the set of $x(\varepsilon)$ such that $||l(\varepsilon)|| < r$ is both discrete and bounded, there are only finitely many such $x(\varepsilon)$, and since the mapping $\varepsilon \mapsto x(\varepsilon)$ is injective, there are also only finitely many ε such that $||l(\varepsilon)|| < r$, which means that there are only finitely many such $l(\varepsilon)$, which means that the set E of $l(\varepsilon)$'s is discrete. Also, $\vec{0} = l(1) \in E$, $-l(\varepsilon) = l(\varepsilon^{-1}) \in E$ (since $(\varepsilon^{-1})^{-1} = \varepsilon \in D$ so ε^{-1} is also a unit of D) and if $l(\varepsilon_1)$ and $l(\varepsilon_2)$ are in D, then $l(\varepsilon_1)+l(\varepsilon_2) = l(\varepsilon_1\varepsilon_2) \in E$ since $(\varepsilon_1\varepsilon_2)^{-1} = \varepsilon_1^{-1}\varepsilon_2^{-1} \in D$ so $\varepsilon_1\varepsilon_2$ is a unit. Therefore E is a subgroup of the additive group $\mathbb{R}^{s+t}$, and we also proved that E is discrete, so by Theorem 5.29 E is a lattice.
Since ε is a unit of D, $N(\varepsilon) = \pm 1$, so $l_1(\varepsilon) + \cdots + l_{s+t}(\varepsilon) = \ln|N(\varepsilon)| = 0$, so $E \subset L$ where L is the hyperplane in $\mathbb{R}^{s+t}$ given by the equation $\lambda_1 + \cdots + \lambda_{s+t} = 0$. The dimension of L is $s+t-1$, so the dimension of E must be less than or equal to $s+t-1$. □

Theorem 6.13. *Let D be defined as above. Then for some $r \leq s+t-1$, $\exists \varepsilon_1, \dots, \varepsilon_r$ units of D such that any unit ε of D can be written as $\varepsilon = \zeta\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$ for a unique choice of $\zeta, a_1, \dots, a_r$ where $\zeta \in D$ is a root of 1 and $a_1, \dots, a_r \in \mathbb{Z}$.*

Proof. Let $E \subset \mathbb{R}^{s,t}$ be the set of points $l(\varepsilon)$ such that ε is a unit of D and let $r \leq s+t-1$ be the dimension of the lattice E and let $l(\varepsilon_1), \dots, l(\varepsilon_r)$ be a basis for E. Then for any $l(\varepsilon) \in E$,

$$l(\varepsilon) = a_1 l(\varepsilon_1) + \cdots + a_r l(\varepsilon_r) \tag{6.13.1}$$

for a unique choice of $a_1, \dots, a_r \in \mathbb{Z}$. Let

$$\zeta = \varepsilon\varepsilon_1^{-a_1} \cdots \varepsilon_r^{-a_r}. \tag{6.13.2}$$

Then $l(\zeta) = l(\varepsilon) - (a_1 l(\varepsilon_1) + \cdots + a_r l(\varepsilon_r)) = l(\varepsilon) - l(\varepsilon) = \vec{0}$, so by Lemma 6.11 ζ is a root of 1. By rearranging equation (6.13.2), we get:

$$\begin{aligned} &\zeta = \varepsilon\varepsilon_1^{-a_1} \cdots \varepsilon_r^{-a_r} \\ \iff &\varepsilon = \zeta\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}. \end{aligned} \tag{6.13.3}$$

So all we have left to prove is that $\zeta, a_1, \dots, a_r$ are unique. Suppose there are $\tilde{\zeta}, b_1, \dots, b_r$ such that

$$\varepsilon = \tilde{\zeta}\varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r} \tag{6.13.4}$$

where $b_1, \dots, b_r \in \mathbb{Z}$ and $\tilde{\zeta}$ is a root of 1. By assumption, $\tilde{\zeta}$ is a root of 1, so by Lemma 6.11, $l(\tilde{\zeta}) = 0$. Therefore, by taking the logarithmic representation on both sides of equation (6.13.4), we get:

$$l(\varepsilon) = b_1 l(\varepsilon_1) + \cdots + b_r l(\varepsilon_r).$$

Therefore, $b_1, \dots, b_r$ are the coordinates of $l(\varepsilon)$ in E with respect to the basis $l(\varepsilon_1), \dots, l(\varepsilon_r)$. But according to equation (6.13.1), these coordinates are $a_1, \dots, a_r$, so $b_j = a_j$ for $j \in \{1, \dots, r\}$.
Now we just need to prove that $\zeta = \tilde{\zeta}$. Since $b_j = a_j$, by replacing each b_j by the corresponding a_j in equation (6.13.4), we get equation (6.13.3) but with $\tilde{\zeta}$ instead of ζ. Since equations (6.13.3) and (6.13.2) are equivalent, we can replace ζ by $\tilde{\zeta}$ in equation (6.13.2). By doing so, we get $\tilde{\zeta} = \varepsilon\varepsilon_1^{-a_1} \cdots \varepsilon_r^{-a_r}$. But $\varepsilon\varepsilon_1^{-a_1} \cdots \varepsilon_r^{-a_r}$ is the definition of ζ, so $\tilde{\zeta} = \zeta$, which concludes the proof. □

6.4 Volumes of Fundamental Parallelepipeds

Definition 6.14. Let $X \subseteq \mathbb{R}^n$ be measurable. Then the **volume** of X is defined as

$$v(X) = \int \cdots \int_X 1 dx_1 \cdots dx_n.$$

This volume can be finite or infinite.

Theorem 6.15. *The following properties of the volume can be easily proved using properties of integrals:*

1. *If $X \subseteq X'$, then $v(X) \leq v(X')$.*
2. *If $v(X \cap X') = 0$, then $v(X \cup X') = v(X) + v(X')$.*
3. *If $\vec{z} \in \mathbb{R}^n$, then $v(X + \vec{z}) = v(X)$.*
4. *If $a \in \mathbb{R}$, then $v(aX) = a^n v(X)$.*

Lemma 6.16. *Let $M \subset \mathbb{R}^n$ be a lattice, let T be a fundamental parallelepiped of M and let $\vec{e_1}, \ldots, \vec{e_n}$ be the basis of M used to construct T. Then the volume of T is given by:*

$$v(T) = |\det \begin{pmatrix} | & & | \\ \vec{e_1} & \cdots & \vec{e_n} \\ | & & | \end{pmatrix}|$$

Proof. Consider the change of variables to $x'_1, \ldots, x'_n$ where $x_j = \sum_{k=1}^{n} (\vec{e_k})_j x'_k$. The Jacobian of this transformation is the determinant that we want to prove is equal to the $v(T)$. Since $\vec{e_1}, \ldots, \vec{e_n}$ are linearly independent, $d \neq 0$. The image of T by this transformation is $[0,1]^n$. Therefore by applying this change of variables to the integral in the definition of $v(T)$, we get:

$$\begin{aligned} v(T) &= \int \cdots \int_T 1 dx_1 \cdots dx_n \\ &= \int \cdots \int_{[0,1]^n} |\det \begin{pmatrix} | & & | \\ \vec{e_1} & \cdots & \vec{e_n} \\ | & & | \end{pmatrix}| dx'_1 \cdots dx'_n \\ &= |\det \begin{pmatrix} | & & | \\ \vec{e_1} & \cdots & \vec{e_n} \\ | & & | \end{pmatrix}| \int_0^1 \cdots \int_0^1 1 dx'_1 \cdots dx'_n \\ &= |\det \begin{pmatrix} | & & | \\ \vec{e_1} & \cdots & \vec{e_n} \\ | & & | \end{pmatrix}| \end{aligned}$$

□

Definition 6.17. Let K be an n-dimensional finite extension of $\mathbb{Q}$, and let $M \subset K$ be a full module with basis $\alpha_1, \ldots, \alpha_n$, and let $\sigma_1, \ldots, \sigma_n$ be the conjugates over K. Then the **discriminant** Δ_M of the module M is defined as:

$$\Delta_M = \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}^2$$

Lemma 6.18. *Let K be a finite extension of $\mathbb{Q}$ with dimension $n = s + 2t$ and let $M \subset K$ be a full module with discriminant Δ_M, and let $L \in \mathbb{R}^n$ be the lattice containing the geometric representations of the elements of M. Then the volume of any fundamental parallelepiped of L is equal to $2^{-t}\sqrt{\Delta_M}$.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a basis for M. Then their geometric representations $x(\alpha_1), \ldots, x(\alpha_n)$ form a basis for L. Therefore if T is the fundamental parallelepiped of L with basis $x(\alpha_1), \ldots, x(\alpha_n)$, we have:

$$\begin{aligned} v(T) &= \left|\det \begin{pmatrix} | & & | \\ x(\alpha_1) & \cdots & x(\alpha_n) \\ | & & | \end{pmatrix}\right| \\ &= \left|\det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \cdots & \sigma_s(\alpha_n) \\ \mathrm{Re}(\sigma_{s+1}(\alpha_1)) & \cdots & \mathrm{Re}(\sigma_{s+1}(\alpha_n)) \\ \mathrm{Im}(\sigma_{s+1}(\alpha_1)) & \cdots & \mathrm{Im}(\sigma_{s+1}(\alpha_n)) \\ \vdots & \ddots & \vdots \\ \mathrm{Re}(\sigma_{s+t}(\alpha_1)) & \cdots & \mathrm{Re}(\sigma_{s+t}(\alpha_n)) \\ \mathrm{Im}(\sigma_{s+t}(\alpha_1)) & \cdots & \mathrm{Im}(\sigma_{s+t}(\alpha_n)) \end{pmatrix}\right| \end{aligned}$$

$$
\begin{aligned}
&= \left| \left(\frac{i}{2}\cdot -2i\right)^t \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \cdots & \sigma_s(\alpha_n) \\ \mathrm{Re}(\sigma_{s+1}(\alpha_1)) & \cdots & \mathrm{Re}(\sigma_{s+1}(\alpha_n)) \\ \mathrm{Im}(\sigma_{s+1}(\alpha_1)) & \cdots & \mathrm{Im}(\sigma_{s+1}(\alpha_n)) \\ \vdots & \ddots & \vdots \\ \mathrm{Re}(\sigma_{s+t}(\alpha_1)) & \cdots & \mathrm{Re}(\sigma_{s+t}(\alpha_n)) \\ \mathrm{Im}(\sigma_{s+t}(\alpha_1)) & \cdots & \mathrm{Im}(\sigma_{s+t}(\alpha_n)) \end{pmatrix} \right| \\
&= \left| \left(\frac{i}{2}\right)^t \right| \left| \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \cdots & \sigma_s(\alpha_n) \\ \mathrm{Re}(\sigma_{s+1}(\alpha_1)) & \cdots & \mathrm{Re}(\sigma_{s+1}(\alpha_n)) \\ -2i\mathrm{Im}(\sigma_{s+1}(\alpha_1)) & \cdots & -2i\mathrm{Im}(\sigma_{s+1}(\alpha_n)) \\ \vdots & \ddots & \vdots \\ \mathrm{Re}(\sigma_{s+t}(\alpha_1)) & \cdots & \mathrm{Re}(\sigma_{s+t}(\alpha_n)) \\ -2i\mathrm{Im}(\sigma_{s+t}(\alpha_1)) & \cdots & -2i\mathrm{Im}(\sigma_{s+t}(\alpha_n)) \end{pmatrix} \right| \\
&= \left| \frac{i}{2} \right|^t \left| \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \cdots & \sigma_s(\alpha_n) \\ \mathrm{Re}(\sigma_{s+1}(\alpha_1)) + i\mathrm{Im}(\sigma_{s+1}(\alpha_1)) & \cdots & \mathrm{Re}(\sigma_{s+1}(\alpha_n)) + i\mathrm{Im}(\sigma_{s+1}(\alpha_n)) \\ -2i\mathrm{Im}(\sigma_{s+1}(\alpha_1)) & \cdots & -2i\mathrm{Im}(\sigma_{s+1}(\alpha_n)) \\ \vdots & \ddots & \vdots \\ \mathrm{Re}(\sigma_{s+t}(\alpha_1)) + i\mathrm{Im}(\sigma_{s+t}(\alpha_1)) & \cdots & \mathrm{Re}(\sigma_{s+t}(\alpha_n)) + i\mathrm{Im}(\sigma_{s+t}(\alpha_n)) \\ -2i\mathrm{Im}(\sigma_{s+t}(\alpha_1)) & \cdots & -2i\mathrm{Im}(\sigma_{s+t}(\alpha_n)) \end{pmatrix} \right| \\
&= \left(\frac{1}{2}\right)^t \left| \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \cdots & \sigma_s(\alpha_n) \\ \sigma_{s+1}(\alpha_1) & \cdots & \sigma_{s+1}(\alpha_n) \\ -2i\mathrm{Im}(\sigma_{s+1}(\alpha_1)) & \cdots & -2i\mathrm{Im}(\sigma_{s+1}(\alpha_n)) \\ \vdots & \ddots & \vdots \\ \sigma_{s+t}(\alpha_1) & \cdots & \sigma_{s+t}(\alpha_n) \\ -2i\mathrm{Im}(\sigma_{s+t}(\alpha_1)) & \cdots & -2i\mathrm{Im}(\sigma_{s+t}(\alpha_n)) \end{pmatrix} \right| \\
&= 2^{-t} \left| \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \cdots & \sigma_s(\alpha_n) \\ \sigma_{s+1}(\alpha_1) & \cdots & \sigma_{s+1}(\alpha_n) \\ \sigma_{s+1}(\alpha_1) - 2i\mathrm{Im}(\sigma_{s+1}(\alpha_1)) & \cdots & \sigma_{s+1}(\alpha_n) - 2i\mathrm{Im}(\sigma_{s+1}(\alpha_n)) \\ \vdots & \ddots & \vdots \\ \sigma_{s+t}(\alpha_1) & \cdots & \sigma_{s+t}(\alpha_n) \\ \sigma_{s+t}(\alpha_1) - 2i\mathrm{Im}(\sigma_{s+t}(\alpha_1)) & \cdots & \sigma_{s+t}(\alpha_n) - 2i\mathrm{Im}(\sigma_{s+t}(\alpha_n)) \end{pmatrix} \right| \\
&= 2^{-t} \left| \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \cdots & \sigma_s(\alpha_n) \\ \dfrac{\sigma_{s+1}(\alpha_1)}{\sigma_{s+1}(\alpha_1)} & \cdots & \dfrac{\sigma_{s+1}(\alpha_n)}{\sigma_{s+1}(\alpha_n)} \\ \vdots & \ddots & \vdots \\ \dfrac{\sigma_{s+t}(\alpha_1)}{\sigma_{s+t}(\alpha_1)} & \cdots & \dfrac{\sigma_{s+t}(\alpha_n)}{\sigma_{s+t}(\alpha_n)} \end{pmatrix} \right| \\
&= 2^{-t}\sqrt{\Delta_M}
\end{aligned}
$$

□

Corollary 6.19. *The volume of a fundamental parallelepiped T of M depends only on M itself, not on the choice of T.*

Definition 6.20. A set $X \subseteq \mathbb{R}^n$ is called **centrally symmetric** if $\forall \vec{x} \in X$, $-\vec{x} \in X$.

Definition 6.21. A set $X \subseteq \mathbb{R}^n$ is called **convex** if the line segment between any two points in X is contained entirely in X.

Lemma 6.22. *Let $M \subset \mathbb{R}^n$ be a full lattice, and let v be the volume of a fundamental parallelepiped of M. Let $X \subset \mathbb{R}^n$ be bounded, centrally symmetric, convex and have a volume $v(X) > 2^n v$. Then X contains at least one non-zero point of M.*

Proof. Let $Y \subset \mathbb{R}^n$ be bounded, and let T be a fundamental parallelepiped of M. By Theorem 5.25, the sets $T - \vec{z}$ where $\vec{z} \in M$ are pairwise disjoint and cover the entire space $\mathbb{R}^n$, so $Y = \bigcup_{\vec{z} \in M} (Y \cap (T - \vec{z}))$. Since $v(Y \cap (T - \vec{z})) = v((Y + \vec{z}) \cap T)$, we get:

$$v(Y) = \sum_{\vec{z} \in M} v((Y + \vec{z}) \cap T).$$

If the sets $Y + \vec{z}$ are all non-intersecting for $\vec{z} \in M$, the sets $(Y + \vec{z}) \cap T$ are also pairwise non-intersecting. Since all the sets $(Y + \vec{z}) \cap T$ are contained in T, if the sets $(Y + \vec{z}) \cap T$ are pairwise non-intersecting, we get that $\sum_{\vec{z} \in M} v((Y + \vec{z}) \cap T) \leq v(T)$, so therefore $v(Y) \leq v(T)$.
Consider the set $\frac{1}{2}X = \{\vec{x} \in \mathbb{R}^n; 2\vec{x} \in X\}$. Then by part 4 of Theorem 6.15, $v(\frac{1}{2}X) = 2^{-n} v(X)$. By assumption, this is strictly greater than v. If all sets $\frac{1}{2}X + \vec{z}$ where $\vec{z} \in M$ were non-intersecting, then by what we proved above, $v(X) \leq v(T) = v$. This is not the case, so for $\vec{z_1}, \vec{z_2} \in M$, $\vec{z_1} \neq \vec{z_2}$, $\frac{1}{2}X + \vec{z_1}$ and $\frac{1}{2}X + \vec{z_2}$ have a common point:

$$\begin{aligned} &\frac{1}{2}\vec{x_1} + \vec{z_1} = \frac{1}{2}\vec{x_2} + \vec{z_2} \\ \iff\ &\vec{z_1} - \vec{z_2} = \frac{1}{2}\vec{x_2} - \frac{1}{2}\vec{x_1}. \end{aligned}$$

Since X is centrally symmetric, $-\vec{x_1} \in X$, and since X is convex, the middle of the line segment between $\vec{x_2}$ and $-\vec{x_1}$, $\frac{1}{2}\vec{x_2} + \frac{1}{2}(-\vec{x_1})$, is in X. We just proved that this point is equal to $\vec{z_1} - \vec{z_2} \in M$ where $\vec{z_1} \neq \vec{z_2}$, so M and X have a common non-zero point, which proves the theorem. □

Lemma 6.23. *Let v be defined as above, and let $Y \subseteq \mathbb{R}^n$ be such that $\bigcup_{\vec{z} \in M} Y + \vec{z} = \mathbb{R}^n$. Then $v(Y) \geq v$.*

Proof. Let T be a fundamental parallelepiped of M. Since the sets $Y + \vec{z}$ completely fill $\mathbb{R}^n$, the sets $(Y + \vec{z}) \cap T$ completely fill T. Therefore, by using the formula for $v(Y)$ used in the proof of Lemma 6.22, we get:

$$\begin{aligned} v(Y) &= \sum_{\vec{z} \in M} v((Y + \vec{z}) \cap T) \\ &\geq v(T) \\ &= v. \end{aligned}$$

□

Lemma 6.24. *Let M be a full lattice in $\mathbb{R}^n$, let v be the volume of a fundamental parallelepiped in M, and let $c_1, \ldots, c_{s+t} \in \mathbb{R}_+$ such that $\prod_{j=1}^{s+t} c_j > \left(\frac{4}{\pi}\right)^t v$.*
Then $\exists \vec{x} = (x_1, \ldots, x_s, y_{s+1}, z_{s+1}, \ldots, y_{s+t}, z_{s+t}) \in M \backslash \{\vec{0}\}$ such that $|x_j| < c_j$ $\forall j \in \{1, \ldots, s\}$ and $y_k^2 + z_k^2 < c_k$ $\forall k \in \{s+1, \ldots, s+t\}$.

Proof. Let X be the set of vectors $\vec{x} = (x_1, \ldots, x_s, y_{s+1}, z_{s+1}, \ldots, y_{s+t}, z_{s+t})$ such that $|x_j| < c_j$ $\forall j \in \{1, \ldots, s\}$ and $y_k^2 + z_k^2 < c_k$ $\forall k \in \{s+1, \ldots, s+t\}$. It's clear that X is convex and centrally

symmetric. We calculate the volume of X:

$$\begin{aligned}
v(X) &= \int \cdots \int_X 1 dx_1 \cdots dx_s dy_{s+1} dz_{s+1} \cdots dy_{s+t} dz_{s+t} \\
&= \int_{-c_1}^{c_1} dx_1 \cdots \int_{-c_s}^{c_s} dx_s \int \int_{y_{s+1}^2 + z_{s+1}^2 < c_{s+1}} dy_{s+1} dz_{s+1} \cdots \int \int_{y_{s+t}^2 + z_{s+t}^2 < c_{s+t}} dy_{s+t} dz_{s+t} \\
&= 2c_1 \cdots 2c_s \pi c_{s+1} \cdots \pi c_{s+t} \\
&= 2^s \pi^t \prod_{j=1}^{s+t} c_j \\
&> 2^s \pi^t \left(\frac{4}{\pi} \right)^t v \\
&= 2^s 2^{2t} v \\
&= 2^n v.
\end{aligned}$$

So we can apply Lemma 6.22, which says that X contains at least one non-zero point of M, which proves the theorem. □

6.5 Dirichlet's Theorem

Lemma 6.25. *Let L be a vector space, and let $M \subset L$ be a lattice. Then M is a full lattice in L if and only if there exists a bounded set $U \subset L$ such that $\forall \vec{x} \in L$, $\exists \vec{u} \in U, \vec{z} \in M$ such that $\vec{x} = \vec{u} + \vec{z}$.*

Proof. $\implies$: If M is full, we can take U to be a fundamental parallelepiped of M. Then by Theorem 5.25 this theorem holds.
$\impliedby$: Suppose that M is not full and let U be an arbitrary bounded set in L. Since U is bounded, $\exists r \in \mathbb{R}$ such that $||\vec{u}|| \leq r \ \forall \vec{u} \in U$. Let L' be the vector space generated by the vectors in M. Since M is not a full lattice, $L' \subset L$ (they're not equal), so there are vectors in L of any length that are orthogonal to L'. In particular, $\exists \vec{y} \in L$ orthogonal to L' such that $||\vec{y}|| > r$. Suppose for a contradiction that $\exists \vec{z} \in M, \vec{u} \in U$ such that $\vec{y} = \vec{u} + \vec{z}$. Since $\vec{y} \cdot \vec{z} = 0$, $||\vec{y}||^2 = \vec{y} \cdot \vec{y} = \vec{y} \cdot \vec{u} \leq ||\vec{y}||||\vec{u}|| \leq r||\vec{y}|| \iff ||\vec{y}|| \leq r$, which is a contradiction, which proves the theorem. □

Theorem 6.26. *(Dirichlet's Theorem) Let K be a finite extension of $\mathbb{Q}$ of dimension $n = s + 2t$ and let D be an order of K. Then for $r = s + t - 1$, $\exists \varepsilon_1, \ldots, \varepsilon_r$ units of D such that any unit of D ε can be written as $\varepsilon = \zeta \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$ for a unique choice of $\zeta, a_1, \ldots, a_r$ where $\zeta \in D$ and $\zeta^m = 1$ for some $m \in \mathbb{N}^*$ and $a_1, \ldots, a_r \in \mathbb{Z}$. $\varepsilon_1, \ldots, \varepsilon_r$ are called fundamental units of D.*

Proof. By Theorem 6.13, the theorem is true for some $r \leq s + t - 1$, so we just need to prove that $r = s + t - 1$. Let $E \subset \mathbb{R}^{s+t}$ be the lattice containing the logarithmic representations of the units of D, and let $L \subset \mathbb{R}^{s+t}$ be the vector space consisting of vectors $(\lambda_1, \ldots, \lambda_{s+t})$ such that $\lambda_1 + \cdots + \lambda_{s+t} = 0$. All we need to prove is that E is a full lattice in L.
Let $\vec{\lambda} = (\lambda_1, \ldots, \lambda_{s+t})$ be an arbitrary vector in L. Then if $\vec{x} = (e^{\lambda_1}, \ldots, e^{\lambda_s}, e^{\frac{\lambda_{s+1}}{2}}, \ldots, e^{\frac{\lambda_{s+t}}{2}}) \in L^{s,t}$, then $l(\vec{x}) = \vec{\lambda}$, so any vector in L is the logarithmic representation of some vector $\vec{x} \in L^{s,t}$. By Theorem 5.32, $\sum_{k=1}^{s+t} l_k(\vec{x}) = \ln |N(\vec{x})|$, so $l(\vec{x}) \in L$ if and only if $N(\vec{x}) = \pm 1$.
Let $S = \{\vec{x} \in L^{s,t}; N(\vec{x}) = \pm 1\}$, and let X_0 be an arbitrary bounded subset of S. Then $\exists c > 0$ such that $\forall \vec{x} = (x_1, \ldots, x_{s+t}) \in X_0$, $|x_j| < c \ \forall j \in \{1, \ldots, s\}$ and $|x_k|^2 < c \ \forall k \in \{s+1, \ldots, s+t\}$, so $l_k(\vec{x}) < \ln(c)$ $\forall k \in \{1, \ldots, s+t\}$, so $l(X_0)$ is bounded. Since the norm is multiplicative, if $\vec{x}$ is an arbitrary vector in S, then $\forall \vec{y} \in S$, $\vec{x}\vec{y} \in S$ since $N(\vec{x}\vec{y}) = N(\vec{x})N(\vec{y}) = \pm 1 \cdot \pm 1 = \pm 1$, so therefore

$$X_0 \vec{x} \subseteq S. \tag{6.26.1}$$

If ε is a unit of D and $x(\varepsilon)$ is its geometric representation, $N(x(\varepsilon)) = N(\varepsilon) = \pm 1$, so $x(\varepsilon) \in S$, so by equation (6.26.1), $X_0 x(\varepsilon) \subseteq S$.
Let $\vec{y}$ be an arbitrary vector in S and let $M \subset L^{s,t}$ be the lattice containing the geometric representations of the numbers in the order D. Consider the linear transformation from $L^{s,t}$ to itself given by $\vec{x} \mapsto \vec{y}\vec{x}$ where $\vec{y}\vec{x}$ is the componentwise multiplication. The determinant of the matrix of this transformation is

$$N(\vec{y}) = \pm 1 \tag{6.26.2}$$

so the volumes of the fundamental parallelepipeds of M and $\vec{y}M$ are equal. Let v be this volume. Let $c_1, \ldots, c_{s+t} > 0$ such that $c_1 \cdots c_{s+t} > \left(\frac{4}{\pi}\right)^t v$ and let

$$X = \{\vec{x} \in L^{s,t}; |x_1| < c_1, \ldots, |x_s| < c_s, |x_{s+1}|^2 < c_{s+1}, \ldots, |x_{s+t}| < c_{s+t}\}. \tag{6.26.3}$$

By Lemma 6.24, $\exists \vec{x} = \vec{y}x(\alpha) \in X \backslash \{\vec{0}\}$ such that $\alpha \in D \backslash \{0\}$. Let $q = c_1 \cdots c_{s+t}$. By using the fact from equation (6.26.2) that $N(\vec{y}) = \pm 1$ and the fact from equation (6.26.3) that $|N(\vec{x})| < c_1 \cdots c_{s+t} = q$, we get

$$\begin{aligned} |N(\alpha)| &= |N(\vec{y})N(\alpha)| \\ &= |N(\vec{x})| \\ &< q. \end{aligned}$$

By Corollary 6.4, since $\alpha \in D$, $N(\alpha) \in \mathbb{Z}$. Since $N(\alpha) \in \mathbb{Z}$ and $|N(\alpha)| < q$, there are only finitely many numbers that $N(\alpha)$ can be equal to. By Lemma 6.7, for each of these possible norms, there are only finitely many non-associate elements α. Let $\alpha_1, \ldots, \alpha_m \in D \backslash \{\vec{0}\}$ be pairwise non-associate such that any element in $D \backslash \{\vec{0}\}$ with a norm whose absolute value is less than q is associate with one of the α_j's. In particular, α is associate with one of the α_j's, so by Corollary 6.9, $\alpha_j = \alpha\varepsilon$ where ε is a unit in D. So we get:

$$\begin{aligned} \vec{y} &= \vec{y}x(1) \\ &= \vec{y}x(\alpha\alpha^{-1}) \\ &= \vec{y}x(\alpha\alpha_j^{-1}\varepsilon) \\ &= \vec{y}x(\alpha)x(\alpha_j^{-1})x(\varepsilon) \\ &= \vec{x}x(\alpha_j^{-1})x(\varepsilon). \end{aligned} \tag{6.26.4}$$

Let $X_0 = S \cap \left(\bigcup_{j=1}^m Xx(\alpha_j^{-1})\right)$. Since X is bounded, each set $Xx(\alpha_j^{-1})$ is bounded so X_0 is bounded. S, X and the α_j's don't depend on $\vec{y}$ and are completely determined by D, so so is X_0. $\vec{y} \in S$, $x(\varepsilon) \in S$, so by equation (6.26.4), $xx(\alpha_j^{-1}) \in S$. Since $x \in X$, this means that $xx(\alpha_j^{-1}) \in X_0$. So any arbitrary $\vec{y}$ belongs to $X_0x(\varepsilon)$, so the $X_0x(\epsilon)$'s cover S, which by Lemma 6.25 proves the theorem. □

7 The Structure of the Set of Solutions to $N(\mu) = a$

Theorem 6.26 gives us the structure of the set of units of an order D, that is the set of elements with norm ± 1. By using this, we can get the structure of the set of units with norm 1 (and not -1), and from that we will be able to get the structure of the set of elements μ with an arbitrary norm a, which due to Theorem 3.24 will give us the structure of the set of solutions to equation (1.1.1).

7.1 Algebraic Number Fields with Odd Dimension

Lemma 7.1. *Let K be a finite extension of $\mathbb{Q}$ with $s > 0$. Then the only roots of 1 in K are 1 and -1.*

Proof. Let σ be a conjugate function from K into $\mathbb{R}$ (since $s > 0$, there exists such a function). Suppose for a contradiction that $\exists \varepsilon \neq \pm 1$ such that $\varepsilon^m = 1$ for some $m \in \mathbb{N}^*$. Since σ is a real conjugate function, all its images are in $\mathbb{R}$, and in particular, $\sigma(\varepsilon) \in \mathbb{R}$. Also, if $m \in \mathbb{N}^*$ such that $\varepsilon^m = 1$, then since σ is a homomorphism and is therefore multiplicative,

$$\begin{aligned} (\sigma(\varepsilon))^m &= \sigma(\varepsilon^m) \\ &= \sigma(1) \\ &= 1. \end{aligned}$$

Therefore, $\sigma(\varepsilon) \in \mathbb{R}$ is a root of 1. The only real roots of 1 are ± 1, so $\sigma(\varepsilon) = \pm 1$. Obviously, $\sigma(1) = 1$, and since σ is injective and $\varepsilon \neq 1$, $\sigma(\varepsilon)$ can't be 1, so $\sigma(\varepsilon) = -1$. But -1 is also a root of 1 which is not equal to 1, so by the same argument, we can prove that $\sigma(-1) = -1$. Since σ is injective, this implies that $\varepsilon = -1$, but we assumed that not to be the case, which concludes the proof. □

Corollary 7.2. *Let K be a finite extension with odd dimension n. Then the only roots of 1 in K are 1 and -1.*

Proof. Since $n = s + 2t$ is odd and $2t$ is even, s is odd. Therefore s can't be 0, so Lemma 7.1 applies. □

Lemma 7.3. *Let K be a finite extension of $\mathbb{Q}$ with odd dimension n, and let D be an order of K. Then D has a set of fundamental units $\eta_1, \ldots, \eta_r$ with norm 1 such that any unit ε with norm 1 can be written as*

$$\varepsilon = \eta_1^{a_1} \cdots \eta_r^{a_r} \tag{7.3.1}$$

for a unique choice of $a_1, \ldots, a_r \in \mathbb{Z}$.

Proof. By Theorem 6.26, any unit ε of D can be written as

$$\varepsilon = \zeta \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} \tag{7.3.2}$$

for a unique choice of $a_1, \ldots, a_r$, where ζ is a root of 1. In particular, this holds if $N(\varepsilon) = 1$. Let $\eta_j = N(\varepsilon_j)\varepsilon_j \ \forall j \in \{1, \ldots, r\}$. Then

$$\begin{aligned} N(\eta_j) &= N(N(\varepsilon_j)\varepsilon_j) \\ &= N(\varepsilon_j)^n N(\varepsilon_j) \\ &= N(\varepsilon_j)^{n+1} \\ &= (\pm 1)^{n+1} \\ &= 1. \end{aligned}$$

This holds because n is odd, so $(\pm 1)^{n+1} = 1$. Since $N(\varepsilon_j) = \pm 1$, $\frac{1}{N(\varepsilon_j)} = N(\varepsilon_j)$. Therefore, equation (7.3.2) can be written as:

$$\varepsilon = \zeta N(\varepsilon_1)^{a_1} \cdots N(\varepsilon_r)^{a_r} \eta_1^{a_1} \cdots \eta_r^{a_r}. \tag{7.3.3}$$

By assumption, $N(\varepsilon) = 1$ and we know that $N(\eta_j) = 1 \ \forall j \in \{1, \ldots, r\}$, so by taking the norm on both sides of equation (7.3.3), we get:

$$N(\zeta) N(\varepsilon_1)^{a_1} \cdots N(\varepsilon_r)^{a_r} = 1. \tag{7.3.4}$$

Since n is odd, by Corollary 7.2, $\zeta = \pm 1$. If $\zeta = 1$, then it's obvious that $N(\zeta) = 1$. If $\zeta = -1$ and $\sigma_1, \ldots, \sigma_n$, then by Theorem 3.13, $N(-1) = (-1)^n$. Since n is odd, this is -1. Therefore, $N(\zeta) = \zeta$. By replacing $N(\zeta)$ by ζ in equation (7.3.4) and plugging that into equation (7.3.3), we get equation (7.3.1), which concludes the proof. □

7.2 Algebraic Number Fields with Even Dimension

Lemma 7.4. *Let K be a finite extension of $\mathbb{Q}$ with even dimension n. Then if ζ is a root of 1, $N(\zeta) = 1$.*

Proof. The theorem is obvious for $\zeta = 1$. If $\zeta = -1$ and $\sigma_1, \ldots, \sigma_n$ are the conjugate functions of K, then $N(-1) = \sigma_1(-1) \cdots \sigma_n(-1) = (-1)^n$. Since n is even, this is 1, so the theorem also holds for -1.
If $s > 0$, then by Lemma 7.1, the only roots of 1 are ± 1, and then we're done. So the only remaining case is if $s = 0$.
If $s = 0$, then all conjugate functions of K are complex, so they're divided into pairs σ and $\overline{\sigma}$. Then for any root ζ of 1,

$$\begin{aligned} N(\zeta) &= \sigma_1(\zeta)\overline{\sigma_1(\zeta)} \cdots \sigma_t(\zeta)\overline{\sigma_t(\zeta)} \\ &= |\sigma_1(\zeta)|^2 \cdots |\sigma_t(\zeta)|^2 \\ &= 1 \cdots 1 \\ &= 1. \end{aligned}$$

□

Lemma 7.5. *Let K be a finite extension of $\mathbb{Q}$ with even dimension n, and let D be an order of K. Then D has a set of fundamental units $\eta_1, \ldots, \eta_r$ with norm 1 such that any unit ε with norm 1 can be written as*

$$\varepsilon = \zeta \eta_1^{a_1} \cdots \eta_r^{a_r} \tag{7.5.1}$$

where ζ is a root of 1, for a unique choice of $\zeta, a_1, \ldots, a_r$.

Proof. By Theorem 6.26, any unit ε of D can be written as

$$\varepsilon = \zeta \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r} \tag{7.5.2}$$

for a unique choice of $b_1, \ldots, b_r$, where ζ is a root of 1.
We can reorder the ε_j's such that $N(\varepsilon_1) = \cdots = N(\varepsilon_k) = 1$ and $N(\varepsilon_{k+1}) = \cdots = N(\varepsilon_r) = -1$. Let $\eta_j = \varepsilon_j$ for $j \in \{1, \ldots, k\}$, $\eta_j = \varepsilon_j \varepsilon_r$ for $j \in \{k+1, \ldots, r\}$ (note that $\eta_r = \varepsilon_r^2$). Then if $j \leq k$, $N(\eta_j) = N(\varepsilon_j) = 1$ and if $j > k$,

$$\begin{aligned} N(\eta_j) &= N(\varepsilon_j \varepsilon_r) \\ &= N(\varepsilon_j) N(\varepsilon_r) \\ &= (-1) \cdot (-1) \\ &= 1. \end{aligned}$$

Let $a_j = b_j$ for $j \in \{1, \ldots, r-1\}$ and $a = b_r - b_{r-1} - \cdots - b_{k+1}$. Then equation (7.5.2) becomes:

$$\begin{aligned} \varepsilon &= \zeta \varepsilon_1^{b_1} \cdots \varepsilon_k^{b_k} \varepsilon_{k+1}^{b_{k+1}} \cdots \varepsilon_{r-1}^{b_{r-1}} \varepsilon_r^{b_r} \\ &= \zeta \varepsilon_1^{a_1} \cdots \varepsilon_k^{a_k} \varepsilon_{k+1}^{a_{k+1}} \cdots \varepsilon_{r-1}^{a_{r-1}} \varepsilon_r^{a} \varepsilon_r^{a_{k+1}} \cdots \varepsilon_r^{a_{r-1}} \\ &= \zeta \varepsilon_1^{a_1} \cdots \varepsilon_k^{a_k} (\varepsilon_r \varepsilon_{k+1})^{a_{k+1}} \cdots (\varepsilon_r \varepsilon_{r-1})^{a_{r-1}} \varepsilon_r^{a} \\ &= \zeta \eta_1^{a_1} \cdots \eta_{r-1}^{a_{r-1}} \varepsilon_r^{a}. \end{aligned} \tag{7.5.3}$$

By Lemma 7.4, $N(\zeta) = 1$, and therefore if $N(\varepsilon) = 1$, by taking the norm on both sides of equation (7.5.3), we get:

$$\begin{aligned} 1 &= N(\varepsilon) \\ &= N\left(\zeta \eta_1^{a_1} \cdots \eta_{r-1}^{a_{r-1}} \varepsilon_r^{a}\right) \\ &= N(\zeta) N(\eta_1)^{a_1} \cdots N(\eta_{r-1})^{a_{r-1}} N(\varepsilon)^{a} \\ &= 1 \cdot 1 \cdots 1 \cdot (-1)^{a} \\ &= (-1)^{a}. \end{aligned}$$

So since $N(\varepsilon) = 1$, a is even, so there exists $a_r \in \mathbb{Z}$ such that $a = 2a_r$. Therefore,

$$\begin{aligned} \varepsilon_r^{a} &= \varepsilon_r^{2a_r} \\ &= \left(\varepsilon_r^2\right)^{a_r} \\ &= \eta_r^{a_r}. \end{aligned}$$

By plugging this into equation (7.5.3), we get equation (7.5.1), which concludes the proof. □

7.3 The Structure of the Set of Solutions to $N(\mu) = a$

Theorem 7.6. *Let K be a finite extension of $\mathbb{Q}$ of degree $n = s + 2t$, let $r = s + t - 1$ and let M be a full module in K with coefficient ring D, and let $a \in \mathbb{Z}^*$. Then there exist units $\eta_1, \ldots, \eta_r$ of D with norm 1, and there exists a finite, possibly empty set of numbers $\mu_1, \ldots, \mu_k$ each with norm a such that every solution $\mu \in M$ to the equation $N(\mu) = a$ can be written uniquely as*

$$\mu = \mu_j \eta_1^{a_1} \cdots \eta_r^{a_r} \text{ for } n \text{ odd} \tag{7.6.1}$$

$$\mu = \mu_j \zeta \eta_1^{a_1} \cdots \eta_r^{a_r} \text{ for } n \text{ even} \tag{7.6.2}$$

where $j \in \{1, \ldots, k\}$, ζ is a root of 1, and $a_1, \ldots, a_r \in \mathbb{Z}$.

Proof. By Lemma 6.7, there are only finitely many associate classes that contain elements with norm a. Let $\mu_1, \ldots, \mu_k$ be representatives of these associate classes, where each μ_j belongs to a different associate class. If $N(\mu) = a$, then μ is associate with exactly one μ_j. Let $\varepsilon = \frac{\mu}{\mu_j}$. Then $N(\varepsilon) = 1$, which by Lemma 7.3 proves the theorem for odd n and by Lemma 7.5 proves the theorem for even n. □

8 References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York and London (1966)
[2] S. Lang, *Algebra*, Second Edition, Addison-Wesley Publishing Company, California (1984)
[3] K. G. Andersson, *Finite Fields and Error-Correcting Codes*, Lund University (2015)
[4] https://en.wikipedia.org/wiki/Group_(mathematics)
[5] https://en.wikipedia.org/wiki/Monomorphism
[6] https://en.wikipedia.org/wiki/Discriminant_of_an_algebraic_number_field