THE STRUCTURE OF UNIT GROUPS

DANIEL KLINE

Abstract. Since the time of ancient Greece and India, Pell's equation, $a^2 - db^2 = 1$, has been studied and its solutions sought after. These solutions are significant, because they correspond to the units of the rings $\mathbb{Z}[\sqrt{d}]$. Along with prime numbers, units are vital in understanding the structure and especially the factorization within different rings. Dirichlect's Unit Theorem establishes the structure of the units of a number field as a finite abelian group. In addition to describing the nature of units, Dirichlect's Unit Theorem represents the interconnectedness of geometry (namely Minkowski's Theorem), algebra, and number theory.

Contents

1. Units of $\mathbb{Z}[\sqrt{d}]$

Definition 1.1. Given a ring R, $u \in R$ is a *unit* if there exists $v \in R$ such that $u \cdot v = 1$. We denote the set of units of a ring R as R^*.

Example 1.2. Consider the ring $\mathbb{Z}$. It is easy to check that $\mathbb{Z}^* = \{\pm 1\}$.

Units are not generally as obvious as in the case of $\mathbb{Z}$. Throughout this section, we will consider the rings of the form $\mathbb{Z}[\sqrt{d}]$ where d is a square-free integer. We define $\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$. For identifying units of rings in this form, we will rely on the useful property that the norm of a unit, which we will define below, is equal to ± 1. First, we will define what it means to be a conjugate and then the concept of a norm on $\mathbb{Z}[\sqrt{d}]$.

Definition 1.3. Let $\alpha \in \mathbb{Z}[\sqrt{d}]$. This means that α is of the form $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$. Then, we denote the conjugate of α as $\overline{\alpha}$, where $\overline{\alpha} = a - b\sqrt{d}$.

Date: August 29, 2014.

Definition 1.4. For the rings $R = \mathbb{Z}[\sqrt{d}]$, where d is a square-free integer, the *norm* of $\alpha \in R$ is defined as $N(\alpha) = \alpha \cdot \overline{\alpha} \in \mathbb{Z}$.

Example 1.5. For example, for all $z \in \mathbb{Z}$, $z = \overline{z}$. Therefore, the norm of $z \in \mathbb{Z}$ is $N_{\mathbb{Z}}(z) = z^2$. As observed above, the norms of the units of $\mathbb{Z}$ are equal to ± 1. It is clear that the norm in this case cannot be -1 for any $z \in \mathbb{Z}$, so we consider the elements whose norms are 1. We see that ± 1 are units since $N_{\mathbb{Z}}(\pm 1) = (\pm 1)^2 = 1$. Also, note that for all $z' \in \mathbb{Z}$ such that $z' \neq \pm 1$, z' is not a unit and $N_{\mathbb{Z}}(z') \neq \pm 1$. In this case, not only do the units of $\mathbb{Z}$ have a norm of 1 but also the non-units of $\mathbb{Z}$ do not have a norm of ± 1. This is a special case of the fact that the norm of an element $\alpha \in \mathbb{Z}[\sqrt{d}]$ is ± 1 if and only if α is a unit of $\mathbb{Z}[\sqrt{d}]$. We will prove this below, but first we need to show that the norm on $\mathbb{Z}[\sqrt{d}]$ is multiplicative.

Lemma 1.6. *The norm on $\mathbb{Z}[\sqrt{d}]$ is multiplicative.*

Proof. $N(\alpha \cdot \beta) = \alpha \cdot \beta \cdot \overline{\alpha \cdot \beta} = \alpha \cdot \beta \cdot \overline{\alpha} \cdot \overline{\beta} = \alpha \cdot \overline{\alpha} \cdot \beta \cdot \overline{\beta} = N(\alpha) \cdot N(\beta)$ □

Proposition 1.7. *Let $\alpha \in \mathbb{Z}[\sqrt{d}]$. Then, $N(\alpha) = \pm 1 \iff \alpha$ is a unit of $\mathbb{Z}[\sqrt{d}]$.*

Proof.

($\Longrightarrow$) This direction is clear from the definitions.

($\Longleftarrow$) Suppose that α is a unit. Then, there exists $\alpha^{-1} \in \mathbb{Z}[\sqrt{d}]$ such that $\alpha \cdot \alpha^{-1} = 1$. Now, we take the norm on both sides to get $N(\alpha \cdot \alpha^{-1}) = N(1)$. As seen in 1.5, $N(1) = 1$ and by 1.6, $N(\alpha \cdot \alpha^{-1}) = N(\alpha) \cdot N(\alpha^{-1})$. Therefore, $1 = N(\alpha) \cdot N(\alpha^{-1})$. By 1.5, the only values of $N(\alpha)$ that makes this statement true is $N(\alpha) = \pm 1$.

□

Now, we look more explicitly at the norm of the rings $\mathbb{Z}[\sqrt{d}]$. Suppose that $\alpha \in \mathbb{Z}[\sqrt{d}]$. Then, α is of the form $\alpha = a + b\sqrt{d}$, where $a, b \in \mathbb{Z}$. Note that $\overline{\alpha} = a - b\sqrt{d}$. Therefore, $N(\alpha) = \alpha \cdot \overline{\alpha} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$. Then, we can find the units of the ring $\mathbb{Z}[\sqrt{d}]$ by setting $N(\alpha) = \pm 1$. This equation for finding units, $\pm 1 = a^2 - db^2$, is commonly referred to as Pell's equation. We now look at two examples below to see the differing behavior of Pell's equation for $d < 0$ and $d > 0$.

Example 1.8. First, consider an example in which $d < 0$. For instance, consider the ring $\mathbb{Z}[i]$, where $d = -1$. The units of this ring then are those elements of the form $a + bi$ which satisfy $\pm 1 = a^2 + b^2$. It is clear that either $a = \pm 1$ and $b = 0$ or $a = 0$ and $b = \pm 1$. Therefore, the set of units in this case is $\{\pm 1, \pm i\}$. Similarly, for any square-free integer $d < -1$, the set of units of $\mathbb{Z}[\sqrt{d}]$ is $\{\pm 1\}$.

Example 1.9. Now, we will consider an example in which $d > 0$. To find the units of the ring $\mathbb{Z}[\sqrt{2}]$, we again use Pell's equation, which in this case, looks like $a^2 - 2b^2 = \pm 1$. We quickly see that ± 1 is a solution. With a little effort, we can find other units, such as $1 + \sqrt{2}$ and $3 + 2\sqrt{2}$. We will soon see that there are an infinite number of units of the ring $\mathbb{Z}[\sqrt{2}]$, which each have the form $\pm(1 + \sqrt{2})^m$ for $m \in \mathbb{Z}$. This agree with the units we have already found as $1 = (1 + \sqrt{2})^0$, $1 + \sqrt{2} = (1 + \sqrt{2})^1$, and $3 + 2\sqrt{2} = (1 + \sqrt{2})^2$.

Now, we will use the concept of the fundamental unit to describe the behavior of the units of the ring $\mathbb{Z}[\sqrt{2}]$ as well as others.

Definition 1.10. A *fundamental unit* u is a unit of infinite order such that every unit is of the form ζu^m, where ζ is a root of unity and $m \in \mathbb{Z}$.

For all rings of the form $\mathbb{Z}[\sqrt{d}]$, there exists a fundamental unit. Ireland [3] provides a theorem to find the fundamental units in these cases, which we will use to identify $1+\sqrt{2}$ as the fundamental unit of the ring $\mathbb{Z}[\sqrt{2}]$. First, we need a proposition.

Later, we will define a notion of the ring of algebraic integers for finite-dimensional field extensions of $\mathbb{Q}$. For quadratic field extensions, though, we know what the set of algebraic integers looks like.

Proposition 1.11. *For $d \in \mathbb{N}$ and d square-free, the set of algebraic integers $\mathcal{O}$ of $\mathbb{Q}(\sqrt{d})$ is either the set $\mathbb{Z}[\sqrt{d}]$ when $d \not\equiv 1 \mod 4$ or the set $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ when $d \equiv 1 \mod 4$.*

Theorem 1.12. *Let $d \in \mathbb{N}$ such that d is square free. Consider the set $\mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$. Let $\mathcal{O}$ be the ring of algebraic integers of $\mathbb{Q}(\sqrt{d})$. There exists a fundamental unit $u \in \mathcal{O}$, such that $u > 1$ and all the units of $\mathcal{O}$ are in the form of $\pm u^m$, where $m \in \mathbb{Z}$.*

We will prove the above theorem in section 7, but for now, we will assume the theorem in order to show that $1+\sqrt{2}$ must be the fundamental unit of $\mathbb{Z}[\sqrt{2}]$.

Example 1.13. By the previous result, there exists a fundamental unit, which without loss of generality is > 1, of $\mathbb{Z}[\sqrt{2}]$. First, we will show that the fundamental unit must be of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{N}$. Assume by contradiction that $u = \pm(a - b\sqrt{2}) > 1$, where $a, b \in \mathbb{N}$. Then, by induction, for all $m \in \mathbb{N}$, u^m is of the form $\pm(x - y\sqrt{2})$, where $x, y \in \mathbb{N}$. Also, for all $n < 0$, $u^n \leq 1$. However, we know that $1 + \sqrt{2} > 1$ is a unit of $\mathbb{Z}[\sqrt{2}]$. Since $1 + \sqrt{2}$ is clearly not plus or minus an integer power of $\pm(a - b\sqrt{2})$, then the fundamental unit cannot be of this form. Also, note that for the fundamental unit, $a, b \neq 0$, because the only only units in this case would be ± 1, which cannot be the fundamental unit as we have seen other units such as $1 + \sqrt{2}$. Therefore, the fundamental unit must be of the form $u = a + b\sqrt{2}$, where $a, b \in \mathbb{N}$. Thus, because $1 + \sqrt{2}$ is the unit of this form that is closest to 1, $1 + \sqrt{2}$ must be the fundamental unit of $\mathbb{Z}[\sqrt{2}]$.

The above reasoning fails to say anything about the unit group of other rings. For this reason, we will prove Dirichlet's Unit Theorem so as to build up an answer to the structure of unit groups in general as well as prove 1.12.

2. Minkowski's Theorem in the Plane

To provide an intuition for Minkowski's Theorem, we will first show this theorem for the specific case of the integer lattice in $\mathbb{R}^2$. We will follow the proof provided by Hardy [1]. In the next section, we will rigorously define a lattice, but for now, we will only consider the integer lattice $\mathbb{Z}^2 \subset \mathbb{R}^2$.

Lemma 2.1. *Let R_0 be an open region containing 0 and $R_p = R_0 + p$, where $p \in Z^2$. If for all distinct $q, r \in Z^2$, $R_q \cap R_r = \emptyset$, then the area of R_0 is less than or equal to 1.*

Proof. Let C_0 be the set of points on the boundary of R_0. Then, define $m = \max_{c \in C_0}(|N(c)|)$. In other words, m is the largest distance from 0 over all points in

C_0. Now, for $n \in \mathbb{N}$, we look at the regions R_p such that $|N(p)| \leq 2n^2$. Consider the square N formed by the points $(n, \pm n), (-n, \pm n) \in \mathbb{Z}^2$. Then, we look at the regions R_p such that p is in or on the boundary of N. Define Δ as the area of R_0. By the hypothesis, none of the R_p's intersect each other, so the area of all regions situated around points in or on the boundary of N is given by $(2n+1)^2\Delta$. Furthermore, $(2n+1)^2\Delta$ is clearly contained in the square $(2n+2m)^2$ so that:

$$(2n+1)^2\Delta \leq (2n+2m)^2$$

Then, by dividing both sides by $(2n+1)^2$:

$$\Delta \leq \frac{(2n+2m)^2}{(2n+1)^2}$$

Thus, as $n \to \infty$, we see that $\Delta \leq 1$. □

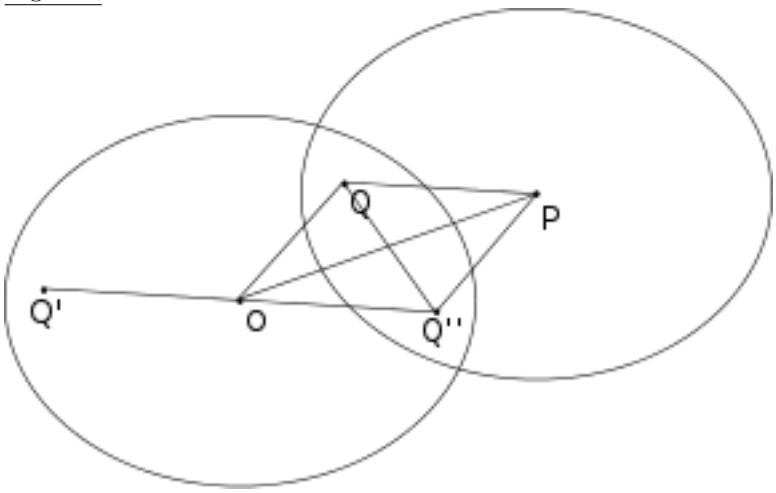
Definition 2.2. A region R is *convex* if for all $p, q \in R$, the line connecting p and q that lies in R.

Definition 2.3. A region R is *centrally symmetric* or *symmetric about* 0 if for all $x \in R$, $-x \in R$.

Theorem 2.4. *If a convex region R is symmetrical about 0 and has area greater than 4, then there exists $p \in R$ such that $p \in \mathbb{Z}^2 \setminus \{(0,0)\}$.*

Proof. Contract the region R linearly about 0 to get the region R_0 which has half the linear dimensions of R. The area of R_0 is greater than 1, and by the contrapositive of 2.1, there exists a congruent, similarly situated region, R_p, around some point $P \in \mathbb{Z}^2 \setminus \{(0,0)\}$ such that $R_0 \cap R_p \neq \emptyset$. Refer to figure 1 below. Let Q be a point in the intersection. Then, there exists $Q' \in R_0$ such that the segment OQ' is congruent and parallel to PQ. Because R_0 is symmetric, there exists the point $Q'' \in R_0$, where Q'' is the point resulting from reflecting Q' about 0. This creates the parallelogram $OQPQ''$, with diagonals QQ'' and OP that bisect each other. Since R_0 is convex and $Q, Q'' \in R_0$, then QQ'' lies within R_0. Therefore, the point B at which QQ'' bisects OP lies within R_0, which implies that OB lies within R_0. Therefore, since R_0 has linear dimensions that are half of R, then the line OP lies in R. Thus, there exists a point $P \in \mathbb{Z}^2 \setminus \{(0,0)\}$ in R. □

Figure 1



3. Minkowski's Theorem in General

Before we give a proof of the general form of Minkowski's Theorem, we will follow Neukirch [4] to establish a definition of a lattice as well as to recall some important properties about lattices.

Definition 3.1. Let V be an n-dimensional $\mathbb{R}$ vector space. A *lattice* Γ is a subgroup of V of the form $\Gamma = \mathbb{Z}v_1 + ... + \mathbb{Z}v_m$, where $m \leq n$ and $v_1, ..., v_m$ are linearly independent vectors of V.

Definition 3.2. A set A is discrete if for all $a \in A$ there exists a neighborhood around a that contains no other points of A.

Proposition 3.3. *A subgroup $\Gamma \subset V$ is a lattice if and only if Γ is discrete.*

Definition 3.4. For an n-dimensional vector space V, a lattice $\Gamma = \mathbb{Z}v_1 + ... + \mathbb{Z}v_m$ is *complete* if $m = n$.

Proposition 3.5. *A lattice $\Gamma \subset V$ is complete if and only if there exists a bounded subset $M \subset V$ such that $V \subset \bigcup_{\gamma \in \Gamma} M + \gamma$.*

Definition 3.6. A *euclidean vector space* V is equipped with an inner product, which gives us the concept of volume.

Definition 3.7. Let V be a euclidean vector space with dimension n. Then, for the linearly independent vectors $v_1, ..., v_m$, we define the *fundamental mesh* as $\phi = \{x_1v_1 + ... + x_mv_m \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$. If $v_1, ..., v_m$ spans the lattice Γ, then ϕ is the fundamental mesh of Γ.

Proposition 3.8. *If ϕ_1 and ϕ_2 are both fundamental meshes of Γ, then $vol(\phi_1) = vol(\phi_2)$.*

Theorem 3.9. *Let V be an n-dimensional euclidean vector space, Γ be a complete lattice in V, and ϕ be a fundamental mesh of Γ. If $X \subset V$ is centrally symmetric and convex and*

$$vol(X) > 2^n vol(\phi)$$

then $X \cap \Gamma \setminus \{0\} \neq \emptyset$.

Proof. First, we will show that there exists distinct $\gamma_1, \gamma_2 \in \Gamma$ such that $(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset$. Assume by contradiction that for all distinct $\gamma_1, \gamma_2 \in \Gamma$, $(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) = \emptyset$. This implies that for all $\gamma \in \Gamma \setminus \{0\}$, $\phi \cap (\frac{1}{2}X + \gamma) = \emptyset$. Therefore,

$$vol(\phi) \geq \sum_{\gamma \in \Gamma} vol(\phi \cap (\frac{1}{2}X + \gamma))$$

Since volume is conserved under translation,

$$vol(\phi) \geq \sum_{\gamma \in \Gamma} vol((\phi - \gamma) \cap \frac{1}{2}X)$$

Because Γ is complete, then $\frac{1}{2}X \subset V \subset \bigcup_{\gamma \in \Gamma} \phi + \gamma$ and more importantly, $\frac{1}{2}X \subset V \subset \bigcup_{\gamma \in \Gamma} \phi - \gamma$. This implies that $\sum_{\gamma \in \Gamma} vol((\phi - \gamma) \cap \frac{1}{2}X) = vol(\frac{1}{2}X)$ and,

$$vol(\phi) \geq vol(\frac{1}{2}X) = \frac{1}{2^n} vol(X)$$

This contradicts the hypothesis that $vol(X) > 2^n vol(\phi)$, and therefore, there exists distinct $\gamma_1, \gamma_2 \in \Gamma$ such that $(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset$. Now, we can take a point in the intersection where there exists $x_1, x_2 \in X$ such that

$$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$$

Let $\gamma = \gamma_1 - \gamma_2 = \frac{1}{2}(x_1 - x_2)$. Because Γ is a subgroup and therefore closed under linear combinations, then $\gamma \in \Gamma$. Since X is centrally symmetric, $-x_2 \in X$, and since X is convex, the chord connecting x_1 and $-x_2$ lies inside X. Therefore, the midpoint of this chord, $\frac{1}{2}(x_1 - x_2)$, is in X. Thus, $\gamma \in X$, and $X \cap \Gamma \setminus \{0\} \neq \emptyset$. □

4. Basic Properties of Number Fields

To understand number fields, we first need to introduce the concepts of an algebraic number and the minimal polynomial of an algebraic number.

Definition 4.1. $\alpha \in \mathbb{C}$ is an *algebraic number* if there exists $f(x) \in \mathbb{Q}[x] \setminus \{0\}$ such that $f(\alpha) = 0$.

Definition 4.2. Let α be an algebraic number. The *minimal polynomial* $m_\alpha(x) \in \mathbb{Q}[x]$ is the unique monic polynomial with root α and smallest degree among other polynomials with rational coefficients and α as a root.

Before we show that such a polynomial exists and is unique, we need the following lemma.

Lemma 4.3. *$\mathbb{Q}[x]$ is a PID.*

Proof. It is clear that (0) and $\mathbb{Q}[x]$ are principal ideals. So consider a non-zero ideal J such that $J \neq \mathbb{Q}[x]$. If there exists a constant function $c \in J$, then since $\mathbb{Q}$ is a field, there would also exist $c^{-1} \in J$ which contradicts the fact that $J \neq \mathbb{Q}[x]$. So, the degree of all polynomials in J is greater than or equal to 1. Because the possible degree of polynomials in J has a lower bound of 1, we can find a non-zero polynomial $d \in J$ with the smallest degree $n \geq 1$. Now, let $f \in J$. By the euclidean division algorithm on $\mathbb{Q}[x]$, there exists $q, r \in \mathbb{Q}[x]$ such that $f = qd + r$, where $\deg r < n$. This implies that $r = f - qd \in J$. Therefore, as to not contradict the fact that d is a non-zero polynomial in J with smallest degree, $r = 0$. So, $f = qd$ and $J = (d)$. Thus, $\mathbb{Q}[x]$ is a PID. □

Proposition 4.4. *$m_\alpha(x)$ exists and is unique.*

Proof. Let $I \subset \mathbb{Q}[x]$ be the ideal of all polynomials with rational coefficients and α as a root. Because $\mathbb{Q}[x]$ is a PID, there exists a monic and therefore unique polynomial $m_\alpha(x)$ that generates I. For $m_\alpha(x)$ to generate this ideal, it must be the smallest degree polynomial with rational coefficients and root α. Thus, $m_\alpha(x)$ is the minimal polynomial and it is unique. □

Proposition 4.5.
Let us establish some basic properties of $m_\alpha(x)$:

(i) *$m_\alpha(x)$ is irreducible.*
(ii) *If $f(x) \in \mathbb{Q}[x]$ has the root α, then $m_\alpha(x) \mid f(x)$. We then call $m_\alpha(x)$ a minimal polynomial of α.*
(iii) *m_α has no repeated roots.*

Proof.

(i) Suppose that $m_\alpha(x)$ is reducible with degree m. Then, there exists $g(x), h(x) \in \mathbb{Q}[x]$ with $1 \leq \deg g(x), \deg h(x) < m$ such that $m_\alpha(x) = g(x)h(x)$. Since α is a root of $m_\alpha(x)$, then $0 = m_\alpha(\alpha) = g(\alpha)h(\alpha)$. This implies that either $g(\alpha) = 0$ or $h(\alpha) = 0$. However, both $g(x)$ and $h(x)$ have smaller degrees than $m_\alpha(x)$, which contradicts the fact that m_α is the smallest degree polynomial with the root α. Thus, $m_\alpha(x)$ is irreducible.

(ii) By the Euclidean Division algorithm on $\mathbb{Q}[x]$, there exists $q(x), r(x) \in \mathbb{Q}[x]$, such that $f(x) = q(x)m_\alpha(x) + r(x)$, where $\deg r(x) < \deg m_\alpha(x)$. After plugging in α, $f(\alpha) = q(\alpha)m_\alpha(\alpha) + r(\alpha) \implies 0 = q(\alpha) \cdot 0 + r(\alpha) = r(\alpha)$. If $r(x) \neq 0$, then this implies that there exists a polynomial with the root α and smaller degree than $m_\alpha(x)$, which is a contradiction. Therefore, $r(x) = 0$, and thus, $m_\alpha(x) \mid f(x)$.

(iii) Assume by contradiction that $m_\alpha(x)$ has a repeated root $\beta \in \mathbb{C}$, where β may be equal to α. So, the minimal polynomial for α must also be the minimal polynomial for β, or in other words, $m_\alpha(x) = m_\beta(x)$. Then, there exists $q(x) \in \mathbb{C}[x]$ such that $m_\beta(x) = (x - \beta)^2 q(x)$. Now, consider the derivative of the minimal polynomial $m'_\beta(x) = 2(x - \beta)q(x) - (x - \beta)^2 q'(x)$. Since $m_\beta(x) \in \mathbb{Q}[x]$, then its derivative $m'_\beta(x) \in \mathbb{Q}[x]$. Also, $m'_\beta(x)$ clearly has a smaller degree than $m_\beta(x)$. Therefore, there exists a rational polynomial of smaller degree than m_β with the root β, which contradicts 4.2. Thus, $m_\alpha(x)$ has no repeated roots.

□

Now that we have defined algebraic numbers and minimal polynomials, we can look at number fields and their relationship with algebraic numbers.

Definition 4.6. A *number field* is a finite-dimensional field extension of $\mathbb{Q}$.

Lemma 4.7. *Let K be an n-dimensional number field. For all $x \in K$, x is an algebraic number.*

Proof. Let $x \in K$. Consider the elements $x^0, ..., x^n$. Because K has dimension n, $x^0, ..., x^n$ must be linearly dependent over $\mathbb{Q}$. In other words, there exists $\alpha_0, ..., \alpha_n \in \mathbb{Q}$ where at least one $\alpha_i \neq 0$ such that $\alpha_n x^n + ... + \alpha_0 = 0$. Thus, by 4.1, x is algebraic. □

Example 4.8. Let α be an algebraic number. As an abstract example of a number field, we define $\mathbb{Q}(\alpha)$ as the smallest field that contains $\mathbb{Q}$ and α. We will see in 4.14 that such a field exists and is finite-dimensional. Therefore, $\mathbb{Q}(\alpha)$ is a number field.

Example 4.9. As a more specific example of a number field, consider the set of Gaussian rationals: $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. $\mathbb{Q}(i)$ is clearly a field extension of $\mathbb{Q}$. Now, we need to find a finite basis for $\mathbb{Q}(i)$. Consider the vectors $1, i$. They are linearly independent and $\text{span}(1, i) = \mathbb{Q}(i)$. Therefore, $1, i$ provides a basis for $\mathbb{Q}(i)$, and $\mathbb{Q}(i)$ is two-dimensional.

Now, we will establish some important properties of the dimension of a number field. Let K be a number field such that $\mathbb{Q} \subset K \subset \mathbb{C}$. We define the symbol $[K : \mathbb{Q}]$ as the dimension as a vector space with coefficients in $\mathbb{Q}$ of the number field K.

For instance, K is finite-dimensional, so $[K : \mathbb{Q}] < \infty$. To continue talking about the dimension of number fields, we need a useful theorem.

Theorem 4.10 (Primitive Element Theorem)**.** *For a number field K, there exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.*

Next, we will show that the number of embeddings of K into $\mathbb{C}$ is equal to $[K : \mathbb{Q}]$. First, we show that the number of embedding of K is equal to the degree of the minimal polynomial.

Lemma 4.11. *A number field $K = \mathbb{Q}(\alpha)$ has precisely deg$(m_\alpha(x))$ embeddings into $\mathbb{C}$.*

Proof. Let σ be an embedding of K into $\mathbb{C}$, so that $\sigma : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$. This means that $\alpha \mapsto \sigma(\alpha)$. Now, consider the minimal polynomial $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in \mathbb{Q}[x]$, where $\mathbb{Q}[x]$ is the set of polynomials with rational coefficients. By the fundamental theorem of algebra, $m_\alpha(x)$ has exactly n roots counted with multiplicity, and by 4.5, $m_\alpha(x)$ has n distinct roots. Because embeddings are linear, $m_\alpha(\sigma(\alpha)) = \sigma(m_\alpha(\alpha)) = \sigma(0) = 0$. So, $\sigma(\alpha)$ is also a root of $f(x)$. Since α must be mapped to another root of $m_\alpha(x)$, then there must be $n = \deg(m_\alpha(x))$ embeddings. □

Now, we want to show that $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/m_\alpha\mathbb{Q}$. We will show this isomorphism by proving that there exists an injective, surjective mapping $\overline{\phi}$: $Q[x]/m_\alpha\mathbb{Q} \to Q(\alpha)$.

Proposition 4.12. *There exists an injective map from $\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x]$ to $K = \mathbb{Q}(\alpha)$.*

Proof. First, we will define the map $\phi : \mathbb{Q}[x] \to \mathbb{Q}(\alpha)$. Constant functions in $\mathbb{Q}[x]$ will be mapped to themselves in $Q(\alpha)$. So, if $q \in \mathbb{Q}$, then we define $\phi : q \mapsto q$. The rest of the functions in $\mathbb{Q}[x]$ are mapped to analogous functions in $\mathbb{Q}(\alpha)$. In other words, $\phi : x \mapsto \alpha$, or similarly, for the rational polynomial $f(x) \in \mathbb{Q}[x]$, $\phi : f(x) \mapsto f(\alpha)$. So, because $m_\alpha(\alpha) = 0$, then $m_\alpha(x) \mapsto 0$. Then, the $\ker\phi = \{m_\alpha(x)\mathbb{Q}[x]\}$ Therefore, we can define the map $\overline{\phi} : \mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x] \to Q(\alpha)$, where for some $q \in Q[x]$, $\overline{\phi}(q + m_\alpha(x)\mathbb{Q}[x]) = \phi(q)$ $\overline{\phi}$ has the kernel $\{0\}$ and thus, $\overline{\phi}$ is an injective map. □

Before we show that $\overline{\phi}$ is surjective, we require a lemma.

Lemma 4.13. *If $m(x) \in \mathbb{Q}[x]$ is irreducible, then $\mathbb{Q}[x]/m(x)\mathbb{Q}[x]$ is a field.*

Proof. Because $\mathbb{Q}[x]$ is a PID and $m(x)$ is irreducible, the principal $(m(x))$ is maximal. There is a bijection from the ideals of $\mathbb{Q}/m(x)\mathbb{Q}[x]$ and the ideals of $\mathbb{Q}[x]$ that contain $m(x)$. Since $m(x)$ is irreducible, there are only two ideals of $\mathbb{Q}[x]$ which contain $m(x)$ (the ideals (1) and $(m(x))$). Therefore, $\mathbb{Q}/m(x)\mathbb{Q}[x]$ has two ideals and $\mathbb{Q}/m(x)$ is a field. □

We can now show that $\overline{\phi}$ is surjective.

Proposition 4.14. *The injective function $\overline{\phi}$: $\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x] \to Q(\alpha)$ is surjective.*

Proof. Because $\overline{\phi}$ is a ring homomorphism, if its domain is a field, then its image is also a field. By 4.13, $\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x]$ is a field so $\overline{\phi}(\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x])$ is also a field. Recall that $\mathbb{Q}(\alpha)$ is the smallest field that contains both $\mathbb{Q}$ and α. Therefore, the image of $\overline{\phi}$ must be $Q(\alpha)$. Thus, $\overline{\phi}$ is surjective and along with 4.12, this shows that $\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x] \cong \mathbb{Q}(\alpha)$. □

Now that we have shown that $\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x] \cong \mathbb{Q}(\alpha)$, we can show that $[K\colon \mathbb{Q}]$ is equal to the degree of $m_\alpha(x)$. To do this, we will show that $1 \mod m_\alpha(x), x \mod m_\alpha(x), ..., \alpha^{n-1} \mod m_\alpha(x)$ forms a basis of $\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x]$.

Proposition 4.15. *$1 \mod m_\alpha(x), x \mod m_\alpha(x), ..., x^{n-1} \mod m_\alpha(x)$ forms a basis of $\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x]$.*

Proof. $1 \mod m_\alpha(x), x \mod m_\alpha(x), ..., x^{n-1} \mod m_\alpha(x)$ are clearly linearly independent, so it is sufficient to show that they span $\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x]$. Let $f(x) \in \mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x]$. Since $\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x]$ is a field, it is a Euclidean Domain. Then, there exists $q(x), r(x) \in \mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x]$ such that $f(x) = q(x)m_\alpha(x) + r(x)$, where $\deg r(x) < \deg m_\alpha(x) = n$. Therefore, $f(x) \equiv r(x) \mod m_\alpha(x)$, which implies that $f(x) \in$span$(1 \mod m_\alpha(x), x \mod m_\alpha(x), ..., x^{n-1} \mod m_\alpha(x))$. Thus, $1 \mod m_\alpha(x), x \mod m_\alpha(x), ..., x^{n-1} \mod m_\alpha(x)$ forms a basis of $\mathbb{Q}[x]/m_\alpha(x)\mathbb{Q}[x]$. □

Therefore, $[K\colon \mathbb{Q}] = n = \deg m_\alpha(x)$. Since there are no repeated roots of $m_\alpha(x)$, then n is also the number of embeddings of K into $\mathbb{C}$. Thus, $[K\colon \mathbb{Q}]$ is equal to the number of embeddings of K into $\mathbb{C}$.

Finally, we define the norm on a number field.

Definition 4.16. Let $K = \mathbb{Q}(\alpha)$, where α is an algebraic number, and let γ be an algebraic number in K. Then, we consider the minimal polynomial $m_\gamma(x) \in \mathbb{Q}[x]$ and its roots $\beta_1, ..., \beta_k$ for some $k \in \mathbb{N}$. Note that for some $1 \leq i \leq k$, $\gamma = \beta_i$. We can now define

$$N_{K/\mathbb{Q}}(\gamma) = (\prod_{i=1}^{k} \beta_i)^{[K\colon \mathbb{Q}(\gamma)]}$$

5. Algebraic Integers

We will very briefly define an algebraic integer and recall some basic properties of algebraic integers .

Definition 5.1. An *algebraic integer* α is the root of a monic polynomial in $\mathbb{Z}[x]$.

Example 5.2. Any root of unity is an algebraic integer. Let u be a root of unity. Then, there exists $n \in \mathbb{Z}$ such that $u^n = 1$. Consider the polynomial $x^n - 1 \in \mathbb{Z}[x]$. Clearly, u is a root of this polynomial, so u is an algebraic integer.

We now state a theorem about algebraic integers that Neukirch proves [4].

Theorem 5.3. *Let $\mathcal{O}$ be the set of algebraic integers of K. Then, $\mathcal{O}$ is a subring of K.*

Finally, we recall an important statement about the norm of an algebraic integer.

Theorem 5.4. *Let δ be an algebraic integer. Then, $N_{K/\mathbb{Q}}(\delta) \in \mathbb{Z}$. Moreover, the minimal polynomial of an algebraic integer has integer coefficients.*

6. Real and Imaginary Embeddings

We will follow Conrad [2] for a proof of Dirichlet's Unit Theorem. First, we will establish some definitions. Let K be a number field with dimension n. Then, by what was shown above, the number of embeddings of K into $\mathbb{C}$ is also n. We will now make a distinction between real embeddings (those whose image is in $\mathbb{R}$) and complex embeddings (those whose image is not in $\mathbb{R}$). Let r_1 be the number of K's real embeddings and $2r_2$ be the number of K's complex embeddings. Let us quickly explain why there are $2r_2$ complex embeddings. Recall that an embedding of $K = \mathbb{Q}(\alpha)$ maps α to a root of the minimal polynomial $m_\alpha(x)$. So, if α maps to a complex root β, then there is another embedding that maps α to the complex conjugate of β. Therefore, complex embeddings of K must come in conjugate pairs. Now, let $\sigma_1, ..., \sigma_{r_1}$ be the real embeddings of K and let $\sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, ..., \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}$ be the conjugate pairs of complex embeddings of K. We also define the vector space $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ and note that $\dim_{\mathbb{R}} V = n$.

Definition 6.1. The *Euclidean Embedding* is defined as $\theta_K \colon K \to V$, where for $\gamma \in K$,

$$\theta_K(\gamma) = (\sigma_1(\gamma), ..., \sigma_{r_1}(\gamma), \sigma_{r_1+1}(\gamma), ..., \sigma_{r_1+r_2}(\gamma))$$

Definition 6.2. We define $N \colon V \to \mathbb{R}$, where for $x_1, ..., x_{r_1} \in \mathbb{R}$ and $z_1, ..., z_{r^2} \in \mathbb{C}$,

$$N(x_1, ..., x_{r_1}, z_1, ..., z_{r^2}) = x_1 \cdots x_{r_1} z_1 \overline{z}_1 \cdots z_{r_2} \overline{z}_{r_2}$$

Remark 6.3. Note that for all $\alpha \in K$, $N_{K/\mathbb{Q}}(\alpha) = N(\theta(\alpha))$.

Proposition 6.4. *The norm defined in 4.16 is equivalent to that of 6.2 when the norm is restricted to the euclidean embedding.*

Proof. We claim that the norm of γ is given by the product of the roots of the minimal polynomial $m_\gamma(x)$. The roots of the minimal polynomial are also the possible embeddings of γ. There could be non-distinct embeddings of γ, and in fact, each embedding is repeated $[K \colon \mathbb{Q}(\gamma)]$ times. Then, taking the product of the embeddings of γ is equivalent to taking the product of the roots of the minimal polynomial $m_\gamma(x)$ raised to the power of $[K \colon \mathbb{Q}(\gamma)]$. Therefore, this definition of the norm in 4.16 is equivalent to that of 6.2. □

Definition 6.5. Let $V^* = (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2}$. Then, we define the set

$$G = \{v \in V^* \mid |N(v)| = 1\}$$

Definition 6.6. We define

$$U = \theta_K(\mathcal{O}^*) = G \cap \theta_K(\mathcal{O})$$

7. Dirichlet's Unit Theorem

Before we begin the proof, we need the Integral Bases Theorem [4], a restatement of the norm N in geometric terms, and a few lemmas.

Theorem 7.1 (Integral Bases Theorem)**.** *Let K be a number field and $\mathcal{O}$ the set of algebraic integers of K. Then, there exists a set of algebraic integers $\{\alpha_1, ..., \alpha_n\}$ whose $\mathbb{Z}$-span is $\mathcal{O}$ and whose $\mathbb{Q}$-span is K.*

Remark 7.2. Let $v \in V^*$ so that multiplication of V by v forms a linear map that is a matrix with determinant $N(v)$. Then, we can view $|N(v)|$ as the scaling factor of a finite volume in V. In other words, let $R \subset V$ be a finite volume. Then, the volume of vR is equal to the volume of R multiplied by $|N(v)|$.

Lemma 7.3. *For all $a \in \mathcal{O} \setminus \{0\}$, $[\mathcal{O}\colon (a)] = |N_{K/\mathbb{Q}}(a)|$*

Proof. By 7.1, there exists algebraic integers $v_1, ..., v_n$ that form a basis of $\mathcal{O}$, where $n = [K\colon \mathbb{Q}]$. Consider the parallelepiped formed by the basis vectors $v_1, ..., v_n$. Since $v_1, ..., v_n$ form a basis of $\mathcal{O}$, then this parallelepiped does not contain any algebraic integers except on its vertices. Now, consider the parallelepiped formed by $av_1, ..., av_n$, where $a \in \mathcal{O} \setminus \{0\}$. The number of algebraic integers that this parallelepiped contains equals the cardinality of $\mathcal{O}/a\mathcal{O}$ and is determined by the determinant of the linear transformation given by multiplication by a. As seen in 7.2, the determinant of this linear transformation is $|N_{K/\mathbb{Q}}(a)|$. Therefore, $[\mathcal{O}\colon (a)] = |N_{K/\mathbb{Q}}(a)|$. □

Lemma 7.4. *For every $M \in \mathbb{N}$, there are finitely many $a \in \mathcal{O}$, up to multiplication by a unit of $\mathcal{O}$, such that $|N_{K/\mathbb{Q}}(a)| = M$.*

Proof. Suppose $|N_{K/\mathbb{Q}}(a)| = M$, where $a \in \mathcal{O}$ and $M \in \mathbb{N}$. Since $a \in \mathcal{O}$, $(a) \subset \mathcal{O}$, and by 4.16, $a|M$, which implies $M\mathcal{O} \subset (a) \subset \mathcal{O}$. Also, by 7.3, $[\mathcal{O}\colon (a)] = M$, and therefore, $\mathcal{O}/M\mathcal{O}$ is finite. Then, there are finitely many principal ideals between $M\mathcal{O}$ and $\mathcal{O}$, which will be denoted as $(a_1), ..., (a_k)$, where $k \in \mathbb{N}$ and $(a) = (a_i)$ for some $1 \leq i \leq k$. Thus, for any $a \in \mathcal{O}$ that satisfies $|N_{K/\mathbb{Q}}(a)| = M$, a is a unit multiple of some a_i. □

Lemma 7.5. *The group G/U is compact in the quotient topology.*

Proof. We need to find a compact subset of G that represents all of the cosets of G/U. To do this, we will start by considering a compact, convex, centrally symmetric region $C \subset V$ such that $\mathrm{vol}(C) > 2^n \mathrm{vol}(\theta_K(\mathcal{O}))$. By $\mathrm{vol}(\theta_K(\mathcal{O}))$, we mean the volume of the fundamental mesh of the lattice $\theta_K(\mathcal{O})$. Now, for $g \in G$, consider gC. Because multiplication by g is a linear map, as described in 7.2, gC is also compact, convex, and centrally symmetric. Note that $g^{-1} \in G$, so consider the set $g^{-1}C$. Since $g^{-1} \in G$, then $|N(g^{-1})| = 1$ and $\mathrm{vol}(g^{-1}C) = \mathrm{vol}(C)$. Then, by Minkowski's Theorem,

$$g^{-1}C \cap \theta_K(\mathcal{O}) \setminus \{0\} \neq \emptyset$$

Let $a \neq 0$ be in this intersection. By 6.3, and because N is multiplicative, $|N_{K/\mathbb{Q}}(a)| = |N(a)| \in |N(g^{-1}C)| = |N(C)|$. Since C is compact and therefore bounded, then $|N(C)|$ is also bounded in $\mathbb{R}$. Consider the set $P = |N(C)| \cap |N(\theta_K(\mathcal{O}))|$. Since $|N(C)|$ is bounded and $|N(\theta_K(\mathcal{O}))| \subset \mathbb{Z}$ by 4.16, P is a finite set. Because $|N_{K/\mathbb{Q}}(a)| \in P$, it is in a finite set. By 7.4, there exists finitely many $a_1, ..., a_k \in \theta_K(\mathcal{O})$ such that every $g^{-1}C$ meets some $a_i\theta_K(\mathcal{O}^*) = a_iU$. By multiplying both $g^{-1}C$ and a_iU by ga_i^{-1}, we see that every gU meets some $a_i^{-1}C$. Therefore, the quotient group G/U is represented by $G \cap \bigcup_{i=1}^{k} a_i^{-1}C$. Now, we will show that $G \cap \bigcup_{i=1}^{k} a_i^{-1}C$ is compact. Because C is compact, every $a_i^{-1}C$ is compact.

Therefore, the union $\bigcup_{i=1}^{k} a_i^{-1}C$ is compact. It is then sufficient to show that G is closed. Consider the continuous map $v \mapsto N(v)$. Under this continuous map, the image of G is $\{1\}$, which is closed. Therefore, G is also closed and the intersection $G \cap \bigcup_{i=1}^{k} a_i^{-1}C$ is compact in G. Now, we can construct a continuous, surjective map from $G \cap \bigcup_{i=1}^{k} a_i^{-1}C \to G/U$. Because $G \cap \bigcup_{i=1}^{k} a_i^{-1}C$ is compact and the map is continuous, then G/U is compact in the quotient topology. □

Theorem 7.6. *Let K be a number field with r_1 real embeddings and $2r_2$ complex embeddings (the 2 comes from pairs of complex conjugate embeddings). Define $r = r_1 + r_2 - 1$. Then, for the set of algebraic integers $\mathcal{O}$ in K, $\mathcal{O}$ contains multiplicatively independent units $\epsilon_1, ..., \epsilon_r$ of infinite order where for all $o \in \mathcal{O}^*$, there exists a root of unity $\zeta \in \mathcal{O}$ and integers $m_1, ..., m_r \in \mathbb{Z}$ such that*

$$o = \zeta \epsilon_1^{m_1} \cdots \epsilon_r^{m_r}$$

Proof. For all $v \in V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, v is in the form of $v = (x_1, ..., x_{r_1}, z_{r_1+1}, ..., z_{r_1+r_2})$. Now, we define the logarithmic mapping $L\colon V^* \to \mathbb{R}^{r_1+r_2}$ such that

$$L(v) = (\log|x_1|, ..., \log|x_{r_1}|, 2\log|z_{r_1+1}|, ..., 2\log|z_{r_1+r_2}|)$$

where the coefficients of 2 comes from the pairs of complex conjugate embeddings. Recall that $G = \{v \in V \mid |N(v)| = 1\}$. Define the set $H \subset \mathbb{R}^{r_1+r_2}$ such that $H = \{(y_1, ..., y_{r_1+r_2}) \mid \sum_i y_i = 0\}$. If $g \in G$, then $L(g) \in H$, and likewise, if $h \in H$, then $h \in L(G)$. So, $L(G) = H$, which implies that $\dim(L(G)) = r_1 + r_2 - 1$ over $\mathbb{R}$. To complete the proof, we look at the set $L(U)$. First, we look at the kernel of L restricted to U, which we denote $\ker L|_U$. It is clear to see that $\ker L = \{\pm 1\}^{r_1} \times (S^1)^{r_2}$, where S^1 is the set of points on the unit circle in $\mathbb{R}^2$. Moreover, $\ker L$ is compact because the sets $\{\pm 1\}$ and S^1 are compact. The roots of unity of U are in $\ker L$, so we want to show that these are the only elements of U in $\ker L$. First, recall that $U = \theta_K(\mathcal{O}) \cap G$. By 7.1, $\mathcal{O}$ is a lattice and therefore discrete. So, U is also discrete. Also, G is closed, so since U is a discrete subset of a closed set, U is also closed. Because U is discrete and closed, $\ker L|_U \subset U$ is discrete and closed. Since $\ker L|_U$ is a closed subset of the compact set $\{\pm 1\}^{r_1} \times (S^1)^{r_2}$, $\ker L|_U$ is compact. Since $\ker L|_U$ is compact and discrete, it is finite. Because $\ker L|_U$ is a finite subgroup of U, it can only contain roots of unity, and because $\ker L|_U$ is a finite subgroup of K^*, the elements of $\ker L|_U$ form a cyclic group.

Now, we will look at the image $L(U)$ in $L(G)$. We want to show that $L(U)$ is discrete in $L(G)$, or in other words, there are only finitely many elements of $L(U)$ in any bounded region of $\mathbb{R}^{r_1+r_2}$. To show this, consider the bounded region $B = \{(y_1, ..., y_{r_1+r_2}) \mid |y_i| < b\}$, where $b \in \mathbb{R}$. Let $u \in U = \theta_K(\mathcal{O}^*)$ such that $L(u) \in B$. Let $\alpha \in K$ such that $u = \theta_K(\alpha)$, where α is the set of original coordinates of u. The real embeddings of the original coordinates of u are bounded above by e^b, and the complex embeddings of the original coordinates of u are bounded above by $e^{\frac{b}{2}}$. In other words, if we define $u = (x_1, ..., x_{r_1}, z_{r_1+1}, ..., z_{r_1+r_2})$, then $x_1, ..., x_{r_1} \leq e^b$ and $z_{r_1+1}, ..., z_{r_1+r_2} \leq e^{\frac{b}{2}}$. Then, there is an upper bound, related to b, on the coefficients of the polynomial $\prod_\sigma T - \sigma(\alpha) \in \mathbb{Z}[T]$. Because α is an algebraic

integer and the aforementioned polynomial is a power of the minimal polynomial of α, then it must have integer coefficients. Because there is an upper bound on the coefficients of all such integer polynomials, then there are finitely many such polynomials. Since u is a root of such a polynomial, then there are finitely many u such that $L(u) \in B$. Therefore, $L(U)$ is discrete.

Since $L\colon G \to L(G)$ is continuous and surjective, then the map $L'\colon G/U \to L(G)/L(U)$ is also continuous and surjective where both quotient groups get the quotient topology. By 7.5, G/U is compact, and since L' is continuous, then $L(G)/L(U)$ is also compact. Now, since $L(U)$ is discrete in $L(G)$ and $L(G) \cong \mathbb{R}^{r_1+r_2-1}$, $L(U) \cong \mathbb{Z}^{r'}$, where $r' \leq r_1 + r_2 - 1$. For a Euclidean space, such as $L(G)$, modulo a discrete subgroup, such as $L(U)$, to be compact, as $L(G)/L(U)$ is, the subgroup must have the same rank as the dimension of the space. Therefore, $L(U) \cong \mathbb{Z}^{r_1+r_2-1}$. Since $\mathbb{Z}^{r_1+r_2-1}$ forms a lattice in $\mathbb{R}^{r_1+r_2-1}$, $L(U)$ forms a lattice in $L(G)$.

Let $r = r_1+r_2-1$ and $\epsilon_1, ..., \epsilon_r$ be elements in $\mathcal{O}^*$ such that $\theta_K(\epsilon_1), ..., \theta_K(\epsilon_r) \in U$ form a $\mathbb{Z}$ basis for $L(U)$. Now we will show that $\epsilon_1, ..., \epsilon_r$ are multiplicatively independent. Suppose $p_1, ..., p_r \in \mathbb{Z}$ such that $\epsilon_1^{p_1} \cdots \epsilon_r^{p_r} = 1$. Then, $L(\epsilon_1^{p_1} \cdots \epsilon_r^{p_r}) = p_1L(\epsilon_1)+...+p_rL(\epsilon_r) = L(1) = 0$. Because $L(\epsilon_1), ..., L(\epsilon_r)$ are linearly independent, $p_1 = ... = p_r = 0$, and $\epsilon_1, ..., \epsilon_r$ are multiplicatively independent. Finally, consider $\epsilon \in \mathcal{O}^*$. Because $\epsilon_1, ..., \epsilon_r$ provide a $\mathbb{Z}$ basis of $L(U)$, $L(\epsilon) = m_1L(\epsilon_1)+...+m_rL(\epsilon_r)$, where $m_1, ..., m_r \in \mathbb{Z}$. This implies that $L(\epsilon) = L(\epsilon_1^{m_1} \cdots \epsilon_r^{m_r})$. Therefore, $\epsilon = \zeta\epsilon_1^{m_1} \cdots \epsilon_r^{m_r}$, where $\zeta \in \ker K|_U$. □

Now, we have an understanding of unit groups in general, we can use Dirichlet's Unit Theorem to prove 1.12.

Theorem 7.7. *Let $d \in \mathbb{N}$ such that d is square free. Consider the set $\mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$ Let $\mathcal{O}$ be the ring of algebraic integers of $\mathbb{Q}(\sqrt{d})$. There exists a fundamental unit $u \in \mathcal{O}$, such that $u > 1$ and all the units of $\mathcal{O}$ are in the form of $\pm u^m$, where $m \in \mathbb{Z}$.*

Proof. We will split this proof into the cases $d > 0$ and $d < 0$.

(a) Suppose $d > 0$. Then, the minimal polynomial for $\sqrt{d}$, which is $x^2 - d$, has two real roots: $\pm\sqrt{d}$. Therefore, there are two embeddings of $\mathbb{Q}(\sqrt{d})$ into $\mathbb{C}$ and both of them are real. Using notation of Dirichlet's Unit Theorem, because there are two real embeddings and zero complex embeddings, $r = 1$. Let $\mathcal{O}$ be the set of algebraic integers of $\mathbb{Q}(\sqrt{d})$ (this is only equal to $\mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \mod 4$). Then, by Dirichlet's Unit Theorem, there exists one unit $\epsilon \in \mathcal{O}^*$ such that for all $o \in \mathcal{O}^*$, $o = \pm\epsilon^m$, where $m \in \mathbb{Z}$. Notice that $\mathcal{O} \subset \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$ because $\sqrt{d} \in \mathbb{R}$ in this case. Therefore, the only roots of unity in $\mathcal{O}$ are ± 1.

(b) Now, suppose $d < 0$. Then, the minimal polynomial for $\sqrt{d}$ has one pair of complex conjugate roots: $\pm\sqrt{d}$. There is only one pair of complex conjugate embeddings of $\mathbb{Q}(\sqrt{d})$ into $\mathbb{C}$, so $r = 0$. Let $\mathcal{O}$ be the set of algebraic integers of $\mathbb{Q}(\sqrt{d})$. Then, by Dirichlet's Unit Theorem, for all $o \in \mathcal{O}^*$, there exists a root of unity $\zeta \in \mathcal{O}$ such that $o = \zeta$. There exists a smallest root of unity ζ^*, where the smallest is defined as the root that is raised to the largest power to equal 1 (i.e. $e^{\frac{2\pi i}{3}}$ is the smallest third root of unity, because to

equal 1, it must be raised to the third power). Because every root of unity is some power of ζ^*, then for all $o \in \mathcal{O}^*$, $o = \pm\zeta^m$, where $m \in \mathbb{Z}$

□

Finally, we will consider two examples in which we apply Dirichlet's Unit Theorem.

Example 7.8. First, we will consider the number field $\mathbb{Q}(\sqrt{2})$. Because $2 \not\equiv 1 \mod 4$, the set of algebraic integers of $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$. As shown in 1.11, the units of $\mathbb{Z}[\sqrt{2}]$ are of the form $\pm(1+\sqrt{2})^m$, where $m \in \mathbb{Z}$. This agrees with Dirichlet's Unit Theorem as $1+\sqrt{2}$ is an algebraic integer of infinite order, since $|1+\sqrt{2}| \neq 1$. Every unit of $\mathbb{Z}[\sqrt{2}]$ is an integer power of $1+\sqrt{2}$ up to multiplication by ± 1.

Example 7.9. The next example we will consider is the number field $\mathbb{Q}(\sqrt{-3})$. Because $3 \equiv 1 \mod 4$, we know that the set of algebraic integers of $\mathbb{Q}(\sqrt{-3})$ is $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. The algebraic integers of $\mathbb{Q}(\sqrt{-3})$ contains the sixth roots of unity. Because these are roots of unity, they are also units. The norm on $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, $N(\frac{a+b\sqrt{-3}}{2}) = \frac{a^2+3b^2}{4}$, clearly shows that the aforementioned elements are the only units. Then, in accordance with Dirichlet's Unit Theorem, the units of $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ take the form of a root of unity.

Acknowledgments. It is a pleasure to thank my mentor, Jesse Silliman, for his guidance and patience. My understanding of Section 4 as well as many of the other algebra concepts comes directly from him.

References

[1] G. H. Hardy and E. M. Wright. An Introduction to the Theory of Numbers. Oxford University Press. 1975.
[2] Keith Conrad. Dirichlet's Unit Theorem. http://www.math.uconn.edu/∼kconrad/blurbs/grad numthy/unittheorem.pdf
[3] Kenneth Ireland and Michael Rosen. A Classical Introduction to Modern Number Theory. Springer Science+Business Media. 1982.
[4] Jürgen Neukirch. Algebraic Number Theory. Springer. 1999.