MATH 377 Project: Dirichlet Unit Theorem

Jun Kai Liao

McGill University, Mathematics and Statistics, Burnside Hall, 805 Sherbrooke Street West, Montreal, H3A 0B9, Quebec, Canada.

E-mail: jun.k.liao@mail.mcgill.com;

Abstract

I tried not to be.

1 Introduction

Algebraic number theory is a branch of mathematics that studies the properties of algebraic numbers, which are complex numbers that are solutions of polynomial equations with rational coefficients. In the late 19th century, mathematicians were interested in understanding the structure of the units of number fields, which are elements of the field that have a multiplicative inverse also in the same field. In particular, they were interested in finding the generators of the unit group and determining their structure.

In 1846, Peter Gustav Lejeune Dirichlet proved the Dirichlet Unit Theorem, which provided a way to calculate the rank of the unit group of a number field. This result was a significant breakthrough in algebraic number theory, as it provided a method to understand the structure of the units of a number field.

The Dirichlet Unit Theorem is a fundamental result in algebraic number theory, which provides a deep insight into the structure of the units of a number field. It asserts that the group of units of an algebraic number field of degree n is a finitely generated abelian group of rank $n - 1$.

2 Preliminary Results

Theorem 1 (Dirichlet Unit Theorem)**.** *Let K be a number field with r_1 real embedding and r_2 pairs of complex conjugate embeddings. The unit group of an order $\mathcal{O}$ is isomorphic to $G \times \mathbb{Z}^{r_1+r_2-1}$ where G is the finite cyclic group of roots of unity of $\mathcal{O}$.*

The proof of the theorem is quite involved and requires multiple steps. We start by introducing the necessary tools and techniques and then combine them into the final theorem. The main idea is to embed the ring we are interested in into a vector space G over $\mathbb{Q}$, and study the units in this space. In particular, we can embed this vector space in a logarithmic space such that the units maps to a hyperplane $L(G)$ of dimension $r_1 + r_2 - 1$. The goal is to show that the units span a full rank lattice in this hyperplane. This is done by showing G/U is compact, where U correspond to the embedding of the units. It can be done by finding a bounded set of representative for gU, which implies G/U is compact. The compactness transfers to the logarithmic space, which forces $L(U)$ to be full rank in $L(G)$.

Definition 1. An **algebraic number field** K is an extension of $\mathbb{Q}$ of finite degree, that is, K is a finite degree vector space over $\mathbb{Q}$.

Let K be a number field of degree n over $\mathbb{Q}$. Each $x \in K$ acts as a linear map $m_x : K \to K$ induced by multiplication, e.i., $m_x(y) = xy$.

Definition 2. [1, § 2] Let A_x be the matrix representing m_x in some basis for K. The **norm** of x is

$$\mathrm{N}(x) = \det A_x.$$

Definition 3. [1, § 2] The **characteristic polynomial** of x is the characteristic polynomial of A_x

$$\chi_{A_x} = \det(XI - A_x).$$

Proposition 1. *The norm and the characteristic polynomial are independent of the choice of basis.*

Proof. Let A be the matrix representing m_x in the basis b_1 and P the change of basis matrix from b_1 to b_2. By the change of basis formula, $P^{-1}AP$ represents m_x in the basis b_2. Now

$$\begin{aligned}
\chi_A &= \det(XI - A) \\
&= \det(XI - A)\det(P^{-1}P) \\
&= \det(P^{-1}(XI - A)P) \\
&= \det(P^{-1}XIP - P^{-1}AP) \\
&= \det(XI - P^{-1}AP) \\
&= \chi_{P^{-1}AP}.
\end{aligned}$$

The characteristic polynomial is invariant under change of basis hence independent of the choice. The norm is just the determinant of a matrix representing a linear map in a vector space hence clearly independent of the choice of the basis. □

Definition 4. [2, § 1] The **ring of integers** of an algebraic number field K is the ring of all algebraic integers contained in K. It is denoted $\mathcal{O}_K$.

Definition 5. [2, § 1] An **order** of an algebraic number field K is a subring $\mathcal{O} \subseteq \mathcal{O}_K$ which is also a $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.

Proposition 2. *Let $\mathcal{O}$ be an order of K. Then $x \in \mathcal{O}$ is a unit if and only if* $\mathrm{N}(x) = \pm 1$.

Proof. [1, § 2] If x is a unit, $\mathrm{N}(1) = \mathrm{N}(xx^{-1}) = \mathrm{N}(x)\,\mathrm{N}(x^{-1})$. Conversely, let $\mathrm{N}(x) = \pm 1$, then the characteristic polynomial of x has the form

$$X^n + a_{n-1}X^{n-1} + \ldots + a_1 X \pm 1$$

with $a_i \in \mathbb{Z}$. Let A be the matrix representing x in some basis. Since $A : \mathcal{O} \to M_n(\mathbb{Z})$ is an injective ring homomorphism, $\chi(A_x) = 0 \in M_n(\mathbb{Z})$ implies $\chi(x) = 0 \in \mathcal{O}$. Therefore,

$$x\left(x^{n-1} + a_{n-1} + \ldots + a_2 x + a_1\right) = \mp 1.$$

□

Definition 6. An **embedding** of K in $\mathbb{C}$, is a injective homomorphism $\sigma : K \to \mathbb{C}$. If $\sigma(K) \subseteq \mathbb{R}$, we say σ is a real embedding, otherwise σ is a complex embedding.

Theorem 2 (Primitive Element Theorem)**.** *Every algebraic number field K is isomorphic to $\mathbb{Q}[\alpha]$ for some $\alpha \in K$.*

Proof. The proof of this theorem is beyond the scope of this paper but can be found in Milne [3, § 5] □

Proposition 3. *If K has degree n over $\mathbb{Q}$, K has exactly n embedding.*

Proof. By the Primitive Element Theorem, there exist $\alpha \in K$ such that $K = \mathbb{Q}[\alpha]$. We can write

$$K \cong \mathbb{Q}[X]/\langle P \rangle$$

where P is the minimal polynomial of α. Since P is a polynomial of degree n, P has n district roots $\rho_1, \rho_2, \ldots \rho_n \in \mathbb{C}$. Then for each i we can define $\sigma_i : K \hookrightarrow \mathbb{C}$ induced by $\alpha \mapsto \rho_i$. There are no others since $\sigma_i(\alpha)$ must be a root of P is $\mathbb{C}$. □

Example 1. The ring $\mathbb{Q}[\sqrt{2}]$ has primitive element $\sqrt{2}$, with minimal polynomial $P(X) = X^2 - 1$, and roots $\sqrt{2}$ and $-\sqrt{2}$. Therefore, there exist two embedding σ_1

and σ_2, with $\sigma_1(\sqrt{2}) = \sqrt{2}$ and $\sigma_2(\sqrt{2}) = -\sqrt{2}$. Notice that both are real embedding since $\sigma_i(K) \subset \mathbb{R}$.

Definition 7. If K has r_1 real embeddings $\sigma_1, \dots, \sigma_{r_1}$ and $2r_2$ complex embeddings $\sigma_{r_1+1}, \overline{\sigma}_{r_1}, \dots, \sigma_{r_1+2r_2}, \overline{\sigma}_{r_1+r_2}$, we define the **canonical embedding** $\theta_K : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = V$ as

$$\theta_k(x) = (\sigma_1(x), \dots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \dots, \sigma_{r_1+r_2}(x)) .$$

Definition 8. Let $\mathcal{N} : V \to \mathbb{R}$ be the map

$$\mathcal{N}(x_1, \dots, x_{r_1}, x_{r_1+1} \dots, x_{r_1+r_2}) = \sigma_1(x) \dots \sigma_{r_1}(x)|\sigma_{r_1+1}(x)|^2 \dots |\sigma_{r_1+r_2}(x)|^2.$$

Example 2. For an element of $K = \mathbb{Q}[\sqrt{2}i]$, $\mathcal{N}$ behave just like the norm. We have $\mathcal{N}(\theta_K(1+\sqrt{2}i) = (1-\sqrt{2}i)(1+\sqrt{2}i) = 3$. Consider the basis $v_1 = 1$, $v_2 = \sqrt{2}i$. Then

$$A_x = \begin{pmatrix} 1 & -2 \\ 1 & 1 \end{pmatrix}$$

hence $\mathrm{N}(x) = 3 = \mathcal{N}(\theta_K(1+\sqrt{2}i))$.

Proposition 4. *For all $x \in K$, $\chi_x = \prod_{i=1}^{n}(X - \sigma_i(x))$.*

Proof. [4, § 3] Let $K = \mathbb{Q}[\alpha]$ and consider the matrix A_α in the basis $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$. Since α has a minimal polynomial of the form $f_\alpha = X^n + a_{n-1}X^{n-1} + \dots + a_0$, A_α will look like

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}.$$

Now

$$\chi_\alpha = \det \begin{pmatrix} X & 0 & \dots & 0 & a_0 \\ -1 & X & \dots & 0 & a_1 \\ 0 & -1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & X + a_{n-1} \end{pmatrix} = \sum_{i=0}^{n} a_i X^i$$

can be easily computed using Leibniz formula. Hence $\chi_\alpha = f_\alpha = \prod_{i=1}^{n}(X - \sigma_i(\alpha))$. Since all embeddings are distinct, A_α is diagonalizable hence there exist some P

invertible such that

$$M_\alpha = P \begin{pmatrix} \sigma_1(\alpha) & 0 & \dots & 0 \\ 0 & \sigma_2(\alpha) & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_n(\alpha) \end{pmatrix} P^{-1}.$$

Any $x \in K$ can be expressed as $g(\alpha)$ for some $g \in \mathbb{Q}[X]$. The map $m : K \to M_n(\mathbb{C})$ is a ring homomorphism hence

$$\begin{aligned} M_x = g(M_\alpha) &= P \begin{pmatrix} g(\sigma_1(\alpha)) & 0 & \dots & 0 \\ 0 & g(\sigma_2(\alpha)) & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & g(\sigma_n(\alpha)) \end{pmatrix} P^{-1} \\ &= P \begin{pmatrix} \sigma_1(g(\alpha)) & 0 & \dots & 0 \\ 0 & \sigma_2(g(\alpha)) & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_n(g(\alpha)) \end{pmatrix} P^{-1} \\ &= P \begin{pmatrix} \sigma_1(x) & 0 & \dots & 0 \\ 0 & \sigma_2(x) & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_n(x) \end{pmatrix} P^{-1}. \end{aligned}$$

Therefore, for all $x \in K$ $\chi_x = \prod_{i=1}^n (X - \sigma_i(x))$ □

Proposition 5. *For all $x \in K$, $\mathcal{N}(x) = \mathrm{N}(x)$.*

Proof. By Proposition 4, $\chi_x = \prod_{i=1}^n (x - \sigma_i(x))$. Since $\mathrm{N}(x)$ is just the constant term of χ_x, clearly $\mathrm{N}(x) = \prod_{i=1}^n \sigma_i(x)$. □

Recall $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is the vector space in which $\theta_K(K)$ lives. We equip V of the natural topology of the Euclidean space, with all subsets of V assumed to have the subspace topology. In particular, we will be interested in the subsets $V^\times = (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$. Let

$$G = \{v \in V^\times : |\mathcal{N}(v)| = 1\}.$$

This is a closed subgroup of $V^\times$ since $G = f^{-1}(\{1\})$ where $f : V \to \mathbb{R}$ is the continuous map $f(v) = |\mathcal{N}(v)|$.

Let

$$U = \theta_K\left(\mathcal{O}^\times\right) = G \cap \theta_K(\mathcal{O})$$

be the image of the units of $\mathcal{O}$. Clearly $U \subset G$ since $\mathcal{O}^\times = \{\alpha \in \mathcal{O} : |\,\mathrm{N}(\alpha)| = 1\}$ and U is discrete in G.

Definition 9. Let $e_1, \ldots, e_n \in \mathbb{R}^n$ form a basis for $\mathbb{R}^n$ as a vector space over $\mathbb{R}$. The e_i also form a basis for the free $\mathbb{Z}$-module of rank n, namely

$$H = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_n.$$

The **fundamental domain** of H is

$$T = \{x \in \mathbb{R}^n : x = \sum_{i=1}^{n} a_i e_i, 0 \leq a_i < 1\}.$$

Let μ be a Lebesgue measure, the volume $\mu(T)$ is denoted $\mathrm{V}(H)$. Every point in $\mathbb{R}^n$ is congruent modulo H to a unique point in T.

Example 3. For $H = \mathbb{Z}(1,2) + \mathbb{Z}(1,-1)$, T is a parallelogram and $\mathrm{V}(H) = 3$.

Proposition 6. *If S is a Lebesgue measurable subset of $\mathbb{R}^n$ with $\mu(S) > \mathrm{V}(H)$, there exist distinct points $x, y \in S$ such that $x - y \in H$.*

Proof. [1, § 5] The sets $S \cap (h + T)$, $h \in H$ are pairwise disjoints and form a cover for S. We can express the volume of S as

$$\mu(S) = \sum_{h \in H} \mu(S \cap (h + T)).$$

Notice that for each i, $\mu(S \cap (h_i + T)) = \mu((-h_i + S) \cap T)$, but the $(-h_i + S) \cap T$ might no longer be disjoint. We will show that they are not. Assume for contradiction that all $(-h_i + S) \cap T$ are pairwise disjoints. Then

$$\mathrm{V}(H) = \mu(T) \geq \sum_{h \in H} (-h + S) \cap T = \mu(S),$$

which contradicts the assumption that $\mu(S) > \mathrm{V}(T)$. Therefore, there exist h_1 and h_2 such that $((-h_1 + S) \cap T) \cap ((-h_2 + S) \cap T) \neq \emptyset$. This means there exist $x, y \in S$ such that $-h_1 + x = -h_2 + y$, i.e., $x - y = h_1 - h_2 \in H$. □

Theorem 3 (Minkowski's Convex Body Theorem)**.** *Let H be a lattice in $\mathbb{R}^n$, and S a Lebesgue measurable subset of $\mathbb{R}^n$ that is symmetric about the origin and convex. If*

$$\mu(S) > 2^n \operatorname{V}(H),$$

then $S \cap (H \setminus \{0\} \neq \emptyset)$

Proof. [1, § 5] Let $S' = \frac{1}{2}S$. Then $\mu(S') = 2^{-n}\mu(S) > \operatorname{V}(H)$ by hypothesis, so there exist distinct elements, $y, z \in S'$ such that $y - z \in H$. Notice $y - z = \frac{1}{2}(2y + (-2z))$, a convex combination of $2y, -2z \in S$. Therefore, $y - z \in S \cap (H \setminus \{0\})$. □

Proposition 7. *For all $\alpha \in \mathcal{O}$, $[\mathcal{O} : \langle\alpha\rangle] = |\operatorname{N}(\alpha)|$.*

Proof. [5, § 3] Since $\mathcal{O}$ is a n dimensional lattice, $\mathcal{O} \cong \theta_K(\mathcal{O})$ is full rank in V. Clearly

$$[\theta_K(\mathcal{O}) : \langle\theta_K(a)\rangle] = [\mathcal{O} : \langle a\rangle] = \operatorname{N}(a).$$

□

Proposition 8. *For all positive integer N, there exist $\alpha_1, \ldots, \alpha_k \in \mathcal{O}$ such that $|\operatorname{N}(\alpha_i)| = N$ up to multiplication by an unit.*

Proof. [5, § 3] If $|\operatorname{N}(\alpha)| = N$, then $[\mathcal{O} : \langle\alpha\rangle] = N$ by Proposition 7, so $N\mathcal{O} \subset \langle\alpha\rangle$. Since $\mathcal{O}/N\mathcal{O}$ is finite, there are only finitely many principal ideals between $N\mathcal{O}$ and $\mathcal{O}$. □

Proposition 9. *The group G/U is compact with respect to the quotient topology.*

Proof. [5, § 3] We find a compact subset S of G that represent all cosets in G/U. Notice that for a Lebesgue measurable region $R \subset V$ with measure $\mu(R) < \infty$, and $v \in V$ which acts on the space, the measure of vR is $|\operatorname{N}(v)|\ \mu(R)$. In particular, for $v \in G$, $\mu(vR) = \mu(R)$ since $\operatorname{N}(v) = 1$. If R is compact, vR also is since continuous functions map compact sets to compact sets. Fix a compact, convex centrally symmetric region $C \subset V$ with $\mu(C) > 2^n \operatorname{V}(\theta_K(\mathcal{O}))$ and consider $g^{-1}C$ with $g \in G$. Clearly $g^{-1}C$ is compact, centrally symmetric, and convex. We can apply Minkowski's convex body theorem to $g^{-1}C$ for the lattice $\theta_K(\mathcal{O}) \subset V$ to get

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

Let $a \in g^{-1}C \cap (\mathcal{O} \setminus \{0\}) \neq \emptyset^{-1}$. Then $|\operatorname{N}(a)|$ must take a value in $\{|\operatorname{N}(gx)| : x \in g^{-1}C\} = \{|\operatorname{N}(x)| : x \in C\}$, which is bounded since C is compact. Notice $|\operatorname{N}(x)|$ must be a integer, hence $|\operatorname{N}(x)|$ can take a finite amount of values. Using Proposition 8, there is a finite set $\{a_1, \ldots, a_m\}$ of nonzero elements of $\mathcal{O}$ such that $g^{-1}C$ intersect some $a_i\mathcal{O}^\times = a_iU$, which implies each gU intersects some $a_i^{-1}C$. The quotient group

G/U can be represented by $G \cap \bigcup_{i=1}^{m} a_i^{-1}C$. The union $\bigcup_{i=1}^{m} a_i^{-1}C$ is compact since each $a_i^{-1}C$ is compact. Since G is closed, the intersect is compact in G. Therefore, G/U has a compact set of representative in G, so G/U is compact in the quotient topology. □

Let $L : V^{\times} \to \mathbb{R}^{r_1+r_2}$ be the logarithmic map

$$L(x_1, \ldots, z_{r_1+r_2}) = (\ldots, \log|x_i|, \ldots, 2\log|z_j|, \ldots),$$

so that $\log \mathcal{N}(x) = \sum_{i=1}^{r_1+r_2} L(x)_i$. This map is a continuous group homomorphism and sends each $g \in G$ in the hyperplane

$$H = \{(x_1, \ldots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} : \sum_{i=1}^{r_1+r_2} x_i = 0\}.$$

Clearly $L(G) = H$, so $L(G)$ has dimension $r_1 + r_2 - 1$ over R.

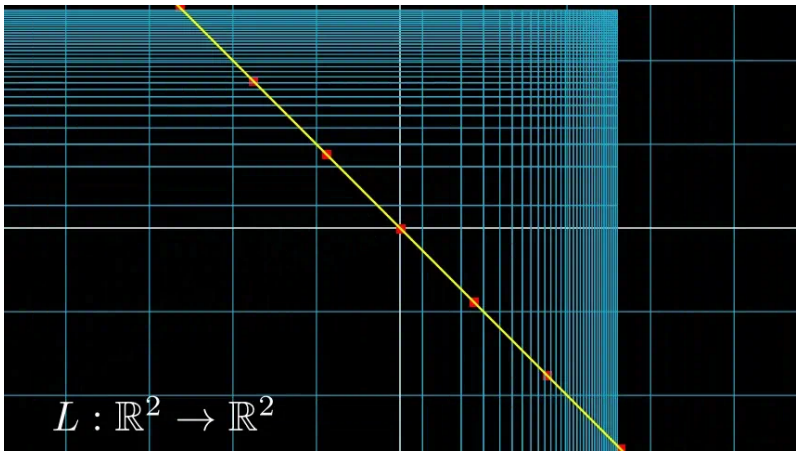

Fig. 1 Embedding of G in the logarithmic space where $K = \mathbb{Q}[\sqrt{3}]$. Full animation [6]: https://youtu.be/2i-mMF7sFN0).

3 Dirichlet Unit Theorem

Recall Dirichlet Unit Theorem 1:

Theorem 4 (Dirichlet Unit Theorem)**.** *Let K be a number field with r_1 real embedding and r_2 pairs of complex conjugate embeddings. The unit group of an order $\mathcal{O}$ is isomorphic to $G \times \mathbb{Z}^{r_1+r_2-1}$ where G is the finite cyclic group of roots of unity of $\mathcal{O}$.*

We need to show that $L(U)$ span a full lattice in the hyperplane $L(G)$ and the kernel of L restricted to U is the root of unity in U.

Proposition 10. *Let H be a finite subgroup of $K^\times$. Then H consists of roots of unity and is cyclic.*

Proof. [1, § 6] Let z be an element of H such that the order of z is the LCM of the order of all elements of H. Let n be the order of z. Then $y^n = 1$ for all $y \in H$ so H consists of roots of unity. Since the polynomial $X^n - 1$ has at most n distinct roots, we have $|H| \leq n$. But the order of z is n hence $1, z^1, z^2, \ldots, z^{n-1}$ are distinct elements. Therefore, H is only composed of roots of unity and is cyclic. □

Proposition 11. *The kernel of L restricted to U is the roots of unity of U.*

Proof. [5, § 3] If ζ is a root of unity, clearly $L(\zeta) = 0$ so we only need to check that nothing else is in the kernel. Since U is discrete, U is closed in $V^\times$. Now notice $\ker L|_U$ is a subset of $\{\pm 1\}^{r_1} \times (S^1)^{r_2}$, which is bounded, $\ker L|_U$ is compact and discrete, so finite. By Proposition 10, a finite subgroup of U can only contain the roots of unity. Therefore, $\ker L|_U$ is exactly the root of unity. □

Proposition 12. *If L is a lattice in $\mathbb{R}^n$, then $\mathbb{R}^n/L$ is compact in the quotient topology implies L is full rank.*

Proof. [5, § 3] Assume L is not full rank so $L = \operatorname{span}\{\alpha_1, \ldots \alpha_m\}$ with $m < n$. Take $x \in \mathbb{R}^n \setminus \operatorname{span}\{\alpha_1, \ldots, \alpha_m\}$ and consider $\pi : \mathbb{R}^n \to \mathbb{R}^n/L$ which maps $x \mapsto xL$. Notice π is injective on $\mathbb{R}x$, hence $\mathbb{R}^n/L$ is not compact. Therefore, $\mathbb{R}^n/L$ is compact implies L is full rank in $\mathbb{R}^n$. □

Proposition 13. *The image $L(U)$ span $r_1 + r_2 - 1$ dimension in the hyperplane $L(G)$.*

Proof. [5, § 3] We start by showing $L(U)$ is a discrete subgroup of $L(G)$. Consider the region

$$R = \{(x_1, \ldots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} : |x_i \leq b\}.$$

Let $L(u) \in R$ for some $u \in U$. The real embeddings of u have absolute value at most e^b and the complex embeddings of u have absolute values at most $e^{b/2}$. Since the characteristic polynomial of u is $\prod(X - \sigma_i(u)) \in \mathbb{Z}[X]$, this puts a bound on the coefficients of the characteristic polynomial, which implies there are finitely many such polynomial. Since u must be a root of such polynomial, there are finitely many choices for u, so $L(U)$ is discrete. Since $L : G \to L(G)$ is a continuous and surjective group homomorphism, the induced map $G/U \to L(G)/L(U)$ is also continuous and surjective with respect to the quotient topology. By Proposition 9, G/U is compact so $L(G)/L(U)$ is also compact. Since $L(U)$ is a discrete subgroup of $L(G) \cong \mathbb{R}^{r_1+r_2-1}$,

$L(U)$. By Proposition 12, $L(U)$ must be full rank. Therefore, $L(U)$ span $r_1 + r_2 - 1$ dimensions. □

Proof of Dirichlet Unit Theorem. [5, § 3] Let $\varepsilon_1, \ldots, \varepsilon_r$ be elements of $\mathcal{O}^\times$ such $\theta_K(\varepsilon_i)$ form a $\mathbb{Z}$ basis for $L(U)$. For any $\varepsilon \in \mathcal{O}^\times$, $L(\varepsilon) = m_1 L(\varepsilon_1) + \ldots + m_r L(\varepsilon_r)$ so $L(\varepsilon) = L(\varepsilon_1^{m_1} \ldots \varepsilon_r^{m_r})$. Since $\ker(L|_U)$ is the image of the roots of unity of $\mathcal{O}^\times$, $\varepsilon = \zeta \varepsilon_1^{m_1} \ldots \varepsilon_r^{m_r}$ for some root of unity ζ. Therefore, $\mathcal{O}^\times \cong G \times \mathbb{Z}^{r_1+r_2-1}$ where G is the group of roots of unity in $\mathcal{O}$. □

References

[1] Ash, R.B.: A Course In Algebraic Number Theory, (2003)

[2] Nielsen, P.: An Introduction to Orders of Number Fields, (2002)

[3] Milne, J.S.: Fields and Galois Theory. Kea Books, Ann Arbor, MI (2022)

[4] Bouyer, F.: Algebraic Number Theory Notes, (2011)

[5] Conrad, K.: Dirichlet's Unit Theorem

[6] The Manim Community Developers: Manim – Mathematical Animation Framework. https://www.manim.community/