On the S-Euclidean minimum of an ideal class

Kevin J. McGown
Department of Mathematics and Statistics
California State University, Chico
400 West First Street
Chico, California, 95929, USA
E-mail: kmcgown@csuchico.edu

Abstract

We show that the S-Euclidean minimum of an ideal class is a rational number, generalizing a result of Cerri. In the proof, we actually obtain a slight refinement of this and give some corollaries which explain the relationship of our results with Lenstra's notion of a norm-Euclidean ideal class and the conjecture of Barnes and Swinnerton-Dyer on quadratic forms. In particular, we resolve a conjecture of Lenstra except when the S-units have rank one. The proof is self-contained but uses ideas from ergodic theory and topological dynamics, particularly those of Berend.

1 Introduction

Let K be a number field of degree $n = r_1+2r_2$. Let S be a finite set of primes containing the infinite primes S_∞. Let $\mathcal{O}_S$ denote the S-integers of K, let $\mathcal{U}_S$ denote the S-units of K, and let N_S denote the S-norm map.[1] Recall that we define $\mathcal{O}_S = \{\xi \in K \mid v(\xi) \geq 0 \text{ for all } v \notin S\}$ and $\mathcal{U}_S = \mathcal{O}_S^\times$; additionally, the S-norm of a number $\xi \in K$ is defined as $N_S(\xi) = \prod_{v\in S} |\xi|_v$ and the S-norm of an ideal $\mathfrak{a} \subseteq \mathcal{O}_S$ is defined as $N_S(\mathfrak{a}) = |\mathcal{O}_S/\mathfrak{a}|$. This setting is a standard one in algebraic number theory (one possible reference is [12]).

2010 *Mathematics Subject Classification*: Primary 11H50, 13F07, 2D40; Secondary 11R04, 11H55, 54H20.

Key words and phrases: Euclidean ring, Euclidean ideal, Euclidean minimum, Conjecture of Barnes and Swinnerton-Dyer.

[1] In cases where "S" is dropped from the notation this will mean we are using $S = S_\infty$.

For an ideal $\mathfrak{a} \subseteq \mathcal{O}_S$ and an element $\xi \in K$, we define

$$m_{\mathfrak{a}}^S(\xi) = \frac{1}{N_S(\mathfrak{a})} \inf_{\gamma \in \mathfrak{a}} N_S(\xi - \gamma),$$

and we set

$$M_{\mathfrak{a}}^S = \sup_{\xi \in K} m_{\mathfrak{a}}^S(\xi).$$

Notice that $m_{\mathfrak{a}}^S(\xi)$ depends upon the ideal $\mathfrak{a}$, but that $M_{\mathfrak{a}}^S$ only depends upon the ideal class $[\mathfrak{a}]$; this follows easily from the fact $\mathfrak{a} = \gamma\mathfrak{b}$ implies $m_{\mathfrak{a}}(\xi) = m_{\mathfrak{b}}(\xi\gamma^{-1})$ for nonzero $\gamma \in K$. We call $M_{\mathfrak{a}}^S$ the S-Euclidean minimum of the ideal class $[\mathfrak{a}]$.

One easily verifies that $m_{\mathfrak{a}}^S(\xi) \in \mathbb{Q}$ for all $\xi \in K$ since the infimum is being taken over a discrete subset of $\mathbb{Q}$.[2] However, it is not by any means clear whether $M_{\mathfrak{a}}^S$ is rational or not. When $K = \mathbb{Q}(\sqrt{d})$, $d > 0$, and $S = S_\infty$, the statement $M_{\mathfrak{a}}^S \in \mathbb{Q}$ is equivalent to a classical conjecture of Barnes and Swinnerton-Dyer, which is still unresolved. Our aim is to prove the following:

Theorem 1. *If $\#S \geq 3$, then $M_{\mathfrak{a}}^S \in \mathbb{Q}$.*

Cerri proved (see [9]) that $M_{\mathfrak{a}}^S \in \mathbb{Q}$ when $S = S_\infty$, $\#S \geq 3$, and $\mathfrak{a} = \mathcal{O}$; our theorem generalizes his result to the S-integral setting. As we will discuss in §3, the quantity $M_{\mathfrak{a}}^S$ is important in the study of norm-Euclidean ideal classes. *A priori*, it is possible that there are norm-Euclidean ideal classes with $M_{\mathfrak{a}}^S = 1$. However, our results lead to:

Corollary 1. *If $\#S \geq 3$, then an ideal class $[\mathfrak{a}]$ of $\mathcal{O}_S$ is norm-Euclidean if and only if $M_{\mathfrak{a}}^S < 1$.*

A result closely related to the previous one (see Corollary 3) resolves a conjecture of Lenstra except when $\mathcal{U}_S$ (modulo torsion) has rank one. In §4 we discuss the relationship of the quantity $M_{\mathfrak{a}}^S$ with the conjecture of Barnes and Swinnerton-Dyer. In the case of $K = \mathbb{Q}(\sqrt{d})$, $d > 0$ one has $\#S_\infty = 2$ and hence our result gives the following:

Corollary 2. *"The conjecture of Barnes and Swinnerton–Dyer holds for fundamental discriminants if we invert a single prime."*

Strictly speaking, the previous two corollaries will follow from a slight refinement of Theorem 1 which we describe after introducing the requisite notation (see Theorem 2).

[2]Given $\xi \in K$ there exists $d \in \mathbb{Z}^+$ such that $d\xi \in \mathcal{O}$ and hence $\{N_S(\xi - \gamma)\}_{\gamma \in \mathfrak{a}}$ is contained in $N_S(d)^{-1}\mathbb{Z}$.

2 Main idea and setup

From the definition one sees that $m_{\mathfrak{a}}^S$ can be viewed as a function $K \to \mathbb{R}_{\geq 0}$ as well as a function $K/\mathfrak{a} \to \mathbb{R}_{\geq 0}$. As there should be no confusion, we will denote both of these functions by $m_{\mathfrak{a}}^S$.

The S-units $\mathcal{U}_S$ act on $K/\mathfrak{a}$ by multiplication and the function $m_{\mathfrak{a}}^S : K/\mathfrak{a} \to \mathbb{R}_{\geq 0}$ is invariant under this action. The main idea is to embed $K/\mathfrak{a}$ into a compact metric group $\mathbb{T}$ where $\mathcal{U}_S$ still acts and $m_{\mathfrak{a}}^S$ extends naturally to an upper semi-continuous function on $\mathbb{T}$. In this setting we will be able to study the action of the units from the point of view of ergodic theory and topological dynamics.

We embed K diagonally into the product of its completions at the primes in S. We will write $K \subseteq \prod_{v \in S} K_v =: \overline{K}_S$. The function $N_S : K \to \mathbb{R}_{\geq 0}$ extends to a continuous function $N_S : \overline{K}_S \to \mathbb{R}_{\geq 0}$, and this allows us to define $m_{\mathfrak{a}}^S(\xi)$ for any $\xi \in \overline{K}_S$. It follows that $m_{\mathfrak{a}}^S : K \to \mathbb{R}_{\geq 0}$ extends to an upper semi-continuous function $m_{\mathfrak{a}}^S : \overline{K}_S \to \mathbb{R}_{\geq 0}$.[3]

Finally, we define

$$\overline{M}_{\mathfrak{a}}^S := \sup_{\xi \in \overline{K}_S} m_{\mathfrak{a}}^S(\xi)\,.$$

We call $\overline{M}_{\mathfrak{a}}^S$ the S-inhomogeneous minimum of the ideal class $[\mathfrak{a}]$.

The embedding $K \subseteq \overline{K}_S$ induces an embedding $K/\mathfrak{a} \subseteq \overline{K}_S/\mathfrak{a} =: \mathbb{T}$, and $m_{\mathfrak{a}}^S$ induces an upper semi-continuous function $m_{\mathfrak{a}}^S : \mathbb{T} \to \mathbb{R}_{\geq 0}$. Since $\mathbb{T}$ is compact, this tells us that there exists $\xi_0 \in \overline{K}_S$ such that $m_{\mathfrak{a}}^S(\xi_0) = \overline{M}_{\mathfrak{a}}^S$. If we can show that there exists an element $\xi_0 \in K$ such that $m_{\mathfrak{a}}^S(\xi_0) = \overline{M}_{\mathfrak{a}}^S$, then it would follow that $M_{\mathfrak{a}}^S = \overline{M}_{\mathfrak{a}}^S \in \mathbb{Q}$. Indeed, we will prove the following result from which Theorem 1 follows.

Theorem 2. *Suppose $\#S \geq 3$. Then there exists an element $\xi_0 \in K$ such that $m_{\mathfrak{a}}^S(\xi_0) = \overline{M}_{\mathfrak{a}}^S$.*

Although many aspects of the proof of Theorem 2 are motivated by ideas in topological dynamics and ergodic theory (particularly those of Berend), our account will be largely self-contained. In fact, except for a couple small lemmas, the only outside results we appeal to are standard theorems in number theory. However, we should mention that much has been gleaned from studying the papers [10, 2, 3, 4, 9].

[3] Given a metric space X, a function $f : X \to \mathbb{R}$ is called upper semi-continuous if $\limsup_{x \to x_0} f(x) \leq f(x_0)$ for every $x_0 \in X$. Clearly, the infimum of a family of continuous (and hence upper semi-continuous) functions is upper semi-continuous; from this general fact it follows immediately that $m_{\mathfrak{a}}^S$ is upper semi-continuous.

Before proceeding to the proof of Theorem 2, we will discuss some applications.

3 Euclidean Ideal Classes

Lenstra introduced the following definition: We call an ideal class $[\mathfrak{a}]$ of $\mathcal{O}_S$ norm-Euclidean if for every $\xi \in K$ there exists $\gamma \in \mathfrak{a}$ such that $N_S(\xi - \gamma) < N_S(\mathfrak{a})$. (Recall that our norms are defined to be positive.) Notice that if we take $\mathfrak{a} = (1)$, then this reduces to the usual definition of the ring $\mathcal{O}_S$ being norm-Euclidean. One important fact is that if an ideal class $[\mathfrak{a}]$ is norm-Euclidean, then it generates the class group of $\mathcal{O}_S$; in particular, the existence of a norm-Euclidean ideal class implies that the class group is cyclic. (See [14] for more details.)

It is clear that $M_{\mathfrak{a}}^S < 1$ implies that $[\mathfrak{a}]$ is norm-Euclidean, and that $M_{\mathfrak{a}}^S > 1$ implies that $[\mathfrak{a}]$ is not norm-Euclidean. In the case $M_{\mathfrak{a}}^S = 1$, one cannot draw any immediate conclusion. However, in light of Theorem 2, provided $\#S \geq 3$, the condition $M_{\mathfrak{a}}^S = 1$ always implies that $[\mathfrak{a}]$ is not norm-Euclidean; indeed, in this case, Theorem 2 implies that there exists $\xi_0 \in K$ such that $N_S(\xi_0 - \gamma) \geq N_S(\mathfrak{a})$ for all $\gamma \in \mathfrak{a}$. This establishes Corollary 1.

Define the open neighborhoods $V_t := \{\xi \in \overline{K}_S \mid N_S(\xi) < t\}$. Lenstra points out that $[\mathfrak{a}]$ is norm-Euclidean if and only if $K \subseteq \mathfrak{a} + V_{N_S(\mathfrak{a})}$. We quote [14] (using our notation): "It seems that in all cases in which this condition is known to be satisfied we actually have $\overline{K}_S = \mathfrak{a} + V_{N_S(\mathfrak{a})}$. It is unknown whether both properties are in fact equivalent."[4] We completely answer this question when $\#S \geq 3$ (in the number field case) with the following:

Corollary 3. *Suppose $\#S \geq 3$. Then we have $K \subseteq \mathfrak{a} + V_{N_S(\mathfrak{a})}$ if and only if $\overline{K}_S = \mathfrak{a} + V_{N_S(\mathfrak{a})}$.*

Proof. One direction of the result is obvious. To prove the other direction, suppose $K \subseteq \mathfrak{a} + V_{N_S(\mathfrak{a})}$; in other words, $[\mathfrak{a}]$ is norm-Euclidean. In light of Theorem 2 and Corollary 1 we see that $\overline{M}_{\mathfrak{a}}^S = M_{\mathfrak{a}}^S < 1$. It follows that for every $\xi \in \overline{K}_S$ there exists $\gamma \in \mathfrak{a}$ such that $N_S(\xi - \gamma) < N_S(\mathfrak{a})$; this proves $\overline{K}_S \subseteq \mathfrak{a} + V_{N_S(\mathfrak{a})}$. □

[4] He then goes on to state the only known result in this direction. It is not important to us here as it pertains to the case where $\#S \leq 2$.

In light of the discussion in [15], we now immediately obtain the following additional result:

Corollary 4. *The question of whether* $[\mathfrak{a}]$ *is norm-Euclidean is decidable when* $\#S \geq 3$.

In the situation where $S = S_\infty$, $\mathfrak{a} = \mathcal{O}$, the analog of Corollary 4 was established in [9] by Cerri. This result was further extended in [16] by Shapira and Wang.[5] Readers interested in reading more regarding the Euclidean algorithm in number fields should consult the excellent expository article [13].

4 The Conjecture of Barnes and Swinnerton-Dyer

Let $f(x, y) = ax^2+bxy+cy^2$ with $a, b, c \in \mathbb{Z}$ be a binary quadratic form with discriminant $\Delta = b^2 - 4ac > 0$. For ease of exposition, we will henceforth write *form* to mean *binary quadratic form*. For a form f and a point $P \in \mathbb{Q}^2$, we define

$$m_f(P) = \inf_{Q\in\mathbb{Z}^2} |f(P - Q)|,$$

and we set

$$M_f = \sup_{P\in\mathbb{Q}^2} m_f(P), \quad \overline{M}_f = \sup_{P\in\mathbb{R}^2} m_f(P).$$

Since $M_{\lambda f} = |\lambda| M_f$ and $\overline{M}_{\lambda f} = |\lambda| \overline{M}_f$ for all $\lambda \in \mathbb{Z}$, we will only consider forms where $\gcd(a, b, c) = 1$, which are known as primitive forms. Barnes and Swinnerton-Dyer conjecture (see [1]) that there exists a point $P_0 \in \mathbb{Q}^2$ such that $m_f(P_0) = M_f = \overline{M}_f$; in particular, $M_f \in \mathbb{Q}$.[6]

Fix a fundamental discriminant $\Delta > 0$. Let $K = \mathbb{Q}(\sqrt{\Delta})$ be the real quadratic field of discriminant Δ having ring of integers $\mathcal{O}$. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ with $\mathbb{Z}$-basis $\{\alpha_1, \alpha_2\}$. We can associate to $\mathfrak{a}$ the form of discriminant Δ given by

$$\frac{1}{N(\mathfrak{a})}(\alpha_1 x + \alpha_2 y)(\overline{\alpha}_1 x + \overline{\alpha}_2 y).$$

In fact, every primitive form of discriminant Δ arises in this way.[7] See [6]

[5] In particular, they give a bound on the computational complexity of $M_{\mathcal{O}}^{S_\infty}$ in terms of the degree, discriminant, and regulator of K, provided $\#S \geq 3$ and K is not a CM-field.

[6] They also conjecture that the minimum is so-called attained and isolated, but we will ignore this part of the conjecture for the purposes of this investigation.

[7] One can extend the correspondence to include forms with non-fundamental discriminants by considering orders other than the full ring of integers, but in this paper we are content to restrict ourselves to forms with fundamental discriminants.

for a classical treatment of this correspondence or [5] for a more modern treatment.

The conjecture of Barnes and Swinnerton-Dyer (as stated above) for fundamental discriminants is equivalent to the statement: Given an ideal class $[\mathfrak{a}]$ in a real quadratic field K, there exists $\xi_0 \in K$ such that $m_{\mathfrak{a}}^{S_\infty}(\xi_0) = \overline{M}_{\mathfrak{a}}^{S_\infty}$. Although we cannot prove this statement, since $\#S_\infty = 2$ in the case where $K = \mathbb{Q}(\sqrt{d})$, $d > 0$, we can prove the analogous statement when $S = S_\infty \cup \{\mathfrak{p}\}$ where $\mathfrak{p}$ is any (finite) prime of K. This follows from Theorem 2 and is the content of Corollary 2.

5 Preliminary Results

In this section we give a brief justification for the facts claimed in §2 and derive a couple other basic results. The hurried reader who is willing to refer back to this section as necessary may skip to §6.

Observe that $\overline{K}_S$ is a locally compact abelian group. It is also a complete metric space with metric $d(\alpha, \beta) = \max_{v \in S} |\alpha_v - \beta_v|_v$. The fact that $N_S(\xi) = \prod_{v \in S} |\xi_v|_v$ is continuous on $\overline{K}_S$ follows immediately from the fact that each $|\cdot|_v : K_v \to \mathbb{R}$ is continuous.

To show that $\mathcal{O}_S$ is discrete in $\overline{K}_S$, it suffices to show that $\{0\}$ is open in the subspace topology on $\mathcal{O}_S$. The set $V = \{\alpha \in \overline{K}_S \mid N_S(\alpha) < 1\}$ is open in $\overline{K}_S$ since N_S is continuous, and, moreover, $V \cap \mathcal{O}_S = \{0\}$. Since $\mathcal{O}_S$ is discrete in $\overline{K}_S$, so is $\mathfrak{a}$. It now follows from generalities that $\mathbb{T}$ is a locally compact Hausdorff space. In fact, one can show that the metric on $\overline{K}_S$ induces a metric on $\mathbb{T}$ in the usual manner.

The only fact that remains to be justified is that $\mathbb{T}$ is compact. For this, we will need the following standard result from algebraic number theory (see, for example, [8]).

Strong Approximation Theorem. *Suppose we are given a finite set of primes T, elements $\alpha_v \in K_v$ for each $v \in T$, and a prime $w \notin T$. Then for each $\varepsilon > 0$, there exists a number $\beta \in K$ such that $|\alpha_v - \beta|_v < \varepsilon$ for all $v \in T$ and $|\beta|_v \leq 1$ for all $v \notin T$ with $v \neq w$.*

We mention in passing that applying the previous result with $T = S$ tells us that K is dense in $\overline{K}_S$, which explains the notation. In what follows we write S_0 for the finite primes in S so that $S = S_\infty \cup S_0$.

Lemma 5.1. *Let $(\alpha_v)_{v \in S} \in \overline{K}_S$. Then there exists $\gamma \in \mathfrak{a}$ such that $v(\alpha_v - \gamma) \geq 0$ for all $v \in S_0$.*

Proof. By the Strong Approximation Theorem, there exists $\gamma \in K$ such that $v(\alpha_v - \gamma) \geq 0$ for all $v \in S_0$, $v(\gamma) \geq v(\mathfrak{a} \cap \mathcal{O})$ for all finite v dividing $\mathfrak{a} \cap \mathcal{O}$, and $v(\gamma) \geq 0$ for all other v. This is possible since $\mathfrak{a} \cap \mathcal{O}$ is not divisible by any primes in S. One checks that this choice of γ works. □

Lemma 5.2. *Let $\mathcal{F}$ be a fundamental domain for $\overline{K}_{S_\infty}/(\mathfrak{a} \cap \mathcal{O})$. (Note that $\overline{K}_{S_\infty} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is the usual Minkowski space and $\mathfrak{a} \cap \mathcal{O}$ is an ideal of $\mathcal{O}$.) Each element of $\mathbb{T}$ has a unique representative in $\mathcal{F} \times \prod_{v \in S_0} \mathcal{O}_v$.*

Proof. Let $(\alpha_v) \in \overline{K}_S$. Using Lemma 5.1, choose $\gamma \in \mathfrak{a}$ such that $v(\alpha_v - \gamma) \geq 0$ for all $v \in S_0$. Choose $a \in \mathcal{O} \cap \mathfrak{a}$ such that $(\alpha_v - \gamma - a)_{v \in S_\infty} \in \mathcal{F}$. Then $\alpha_v - \gamma - a \in \mathcal{O}_v$ for all $v \in S_0$. Set $\beta_v = \alpha_v - \gamma - a \in \mathcal{F} \times \prod_{v \in S_0} \mathcal{O}_v$. Then $(\alpha_v) - (\beta_v) = \gamma + a \in \mathfrak{a}$.

Now we show uniqueness. Suppose $(\alpha_v) = (\beta_v) + \delta$ for some $\delta \in \mathfrak{a}$ with $(\alpha_v), (\beta_v) \in \mathcal{F} \times \prod_{v \in S_0} \mathcal{O}_v$. Then $v(\delta) \geq 0$ for all $v \in S_0$ which implies $\delta \in \mathcal{O} \cap \mathfrak{a}$. Since $(\alpha_v)_{v \in S_\infty}, (\beta_v)_{v \in S_\infty} \in \mathcal{F}$ and $\delta \in \mathcal{O} \cap \mathfrak{a}$, we have $(\alpha_v)_{v \in S_\infty} = (\beta_v)_{v \in S_\infty}$ which implies $\delta = 0$. □

Lemma 5.3. *$\mathbb{T}$ is compact.*

Proof. By the previous lemma, $\mathbb{T}$ is the image under the natural projection of the compact set $\overline{\mathcal{F}} \times \prod_{v \in S_0} \mathcal{O}_v$. □

We conclude this section with another simple result that is a consequence of Strong Approximation which will prove useful in the sequel. For each $w \in S$, we can view K_w as a subset of $\overline{K}_S$ by sending the element $x \in K_w$ to the vector $\xi \in \overline{K}_S$ where $\xi_w = x$ and $\xi_v = 0$ for $v \neq w$; that is, the image of K_w in $\overline{K}_S$ is zero outside the w-component.

Lemma 5.4. *For each $w \in S$, we have $K_w + \mathfrak{a}$ is dense in $\overline{K}_S$. In particular, there are no proper closed subgroups of $\overline{K}_S$ containing both K_w and $\mathfrak{a}$.* [8]

Proof. Let $\xi = (\xi_v)_{v \in S} \in \overline{K}_S$. Fix $\varepsilon > 0$. Using Strong Approximation, choose $\gamma \in K$ such that $|\gamma - \xi_v|_v < \varepsilon$ for all $v \in S$ with $v \neq w$, $|\gamma|_v < \varepsilon$ for all finite v dividing $\mathfrak{a} \cap \mathcal{O}$, and $|\gamma|_v \leq 1$ for all $v \notin S$. When $\varepsilon > 0$ is small enough, this implies $\gamma \in \mathfrak{a}$. Additionally, $\xi - \gamma = (\xi_v - \gamma)_{v \in S}$ is ε-close to $\beta := \xi_w - \gamma \in K_w \subseteq \overline{K}_S$. It follows that ξ is ε-close to $\beta + \gamma \in K_w + \mathfrak{a}$. Since $\varepsilon > 0$ was arbitrary, there are points in $K_w + \mathfrak{a}$ arbitrarily close to ξ. □

[8] Keep in mind that K_w is embedded into one component and $\mathfrak{a}$ is embedded diagonally.

6 Outline of the Proof

Given an element $\xi \in \overline{K}_S$, we will write $[\xi]$ for the class of ξ in $\mathbb{T}$; namely, $[\xi] = \pi(\xi)$ where $\pi : \overline{K}_S \to \mathbb{T}$ is the natural projection map. We begin with two lemmas concerning the orbit structure of the action of $\mathcal{U}_S$ on $\mathbb{T}$.

Lemma 6.1. *For $\xi \in \overline{K}_S$, the following are equivalent:*

1. $\xi \in K$
2. $[\xi] \in \mathbb{T}_{tors}$
3. $\mathrm{Orb}([\xi])$ *is finite*
4. $[\xi]$ *is an isolated point of* $\overline{\mathrm{Orb}([\xi])}$

Proof. First we show (1) $\Rightarrow$ (2) $\Rightarrow$ (3). If $\xi \in K$, there exists $n \in \mathbb{Z}^+$ such that $n\xi \in \mathfrak{a}$ and hence $[\xi] \in \mathbb{T}_{\mathrm{tors}}$. In this case $u\xi \in (1/n)\mathfrak{a}$ for all $u \in \mathcal{U}_S$ and therefore $\mathrm{Orb}([\xi]) \subseteq \pi((1/n)\mathfrak{a})$, which is a finite subgroup of $K/\mathfrak{a}$.

Now we show (3) $\Rightarrow$ (1). Suppose $u[\xi] = u'[\xi]$ in $\mathbb{T}$ with $u \neq u' \in \mathcal{U}_S$. Then there exists $\alpha \in \mathfrak{a}$ such that $u\xi = u'\xi + \alpha$ in $\overline{K}_S$. It follows that $u\xi_v = u'\xi_v + \alpha$ in K_v for all $v \in S$. We conclude that $\xi_v = \alpha/(u - u') \in K$ for all v and therefore $\xi \in K$.

Now we show (3) $\Leftrightarrow$ (4). For convenience of notation let $A = \overline{\mathrm{Orb}([\xi])}$. The set A is a closed subset of $\mathbb{T}$ and therefore compact (see Lemma 5.3). It is now easy to see that for $\xi \in \overline{K}_S$ one has: $[\xi]$ is isolated in A iff $\mathrm{Orb}([\xi])$ is discrete in A iff $\mathrm{Orb}([\xi])$ is finite. □

Lemma 6.2. *Let $\xi \in \overline{K}_S \setminus K$. Then the map $\mathcal{U}_S \to \mathrm{Orb}([\xi])$ given by $u \mapsto u[\xi]$ is a bijection.*

Proof. This follows immediately from the proof of (3) $\Rightarrow$ (1) in the previous lemma. □

The next lemma is easily deduced, but essential. It constitutes the natural generalization of an important observation of Cerri. In fact, we employ the group $\mathbb{T} = \overline{K}_S/\mathfrak{a}$ precisely so that the following result will go through in our setting:

Lemma 6.3. *The set $\{[\xi] \in \mathbb{T} \mid m_{\mathfrak{a}}^S(\xi) = \overline{M}_{\mathfrak{a}}^S\}$ is a nonempty closed $\mathcal{U}_S$-invariant subset of $\mathbb{T}$.*

Proof. This follows from the fact that $m_{\mathfrak{a}}^S$ is a $\mathcal{U}_S$-invariant, upper semi-continuous function defined on the compact set $\mathbb{T}$. □

Theorem 3. *Suppose $\#S \geq 3$. Then every nonempty closed $\mathcal{U}_S$-invariant subset of $\mathbb{T}$ contains torsion elements.*

If we can prove Theorem 3, then Theorems 2 and 1 immediately follow in light of Lemmas 6.1 and 6.3. The proof requires the next three propositions whose proofs we postpone until Sections 8, 9, and 10 respectively.

Definition. We refer to a nonempty $\mathcal{U}_S$-invariant closed subset of $\mathbb{T}$ which is minimal with respect to set inclusion as a $\mathcal{U}_S$-minimal set.

Observe that by Zorn's Lemma, every nonempty $\mathcal{U}_S$-invariant closed subset of $\mathbb{T}$ contains a $\mathcal{U}_S$-minimal set.

Proposition 1. *Let M be $\mathcal{U}_S$-minimal subset of $\mathbb{T}$. Then $M - M$ is a proper subset of $\mathbb{T}$.*

Recall that a CM-field is a totally complex quadratic extension of a totally real field. Let K^+ denote the maximal totally real subfield of K. In the case where K is a CM-field we have $[K : K^+] = 2$.

Proposition 2. *Suppose K is not a CM-field or S contains a finite prime that splits in K/K^+. Let N be a closed $\mathcal{U}_S$-invariant subset of $\mathbb{T}$ that contains 0 as a non-isolated point. If $\#S \geq 3$, then $N = \mathbb{T}$.*

Proposition 3. *If Theorem 3 holds except in the case where K is a CM-field and distinct primes in S lie over distinct primes in K^+, then it holds in all cases.*

Proof of Theorem 3. Let M be a $\mathcal{U}_S$-minimal subset of $\mathbb{T}$. Moreover, assume that M contains no torsion elements. Then $N = M - M$ is a closed $\mathcal{U}_S$-invariant subset of $\mathbb{T}$.

We show that N contains 0 as a non-isolated point. Pick $[\xi] \in M$. Then $M = \overline{\mathrm{Orb}([\xi])}$. By Lemma 6.1, $[\xi]$ must be non-isolated and therefore there is a sequence $u_n \in \mathcal{U}_S$ with the u_n distinct and $u_n[\xi] \to [\xi]$. Without loss of generality, we may assume that $u_n \neq 1$ for all n. Now observe that $u_n[\xi] - [\xi]$ is a sequence of nonzero points in N converging to 0.

By Proposition 3 it suffices to prove the theorem in the situation where Proposition 2 applies. We invoke Proposition 2 and conclude that $N = \mathbb{T}$. This contradicts Proposition 1. Thus M contains torsion elements. □

7 Character Theory and Ergodicity

Before turning to the proofs of Propositions 1,2,3, we need a few lemmas which are consequences of the study of the character theory of $\overline{K}_S$ and $\mathbb{T}$. We have tried to assume a minimal amount of background, giving the appropriate definitions and stating the necessary facts, but some familiarity with the duality theory of locally compact abelian groups (and local fields in particular) will be helpful in this section.

Let G be a locally compact abelian group. A (unitary) character of G is a continuous group homomorphism $\chi : G \to S^1$. (We will always view S^1 as the unit circle inside $\mathbb{C}$.) The Pontryagin dual of G, denoted by $G^\vee$, is the (abelian) multiplicative group consisting of all the characters of G. It is locally compact when endowed with the topology of uniform convergence on compact sets.

We are interested in the characters of $\mathbb{T}$. However, since any character of $\mathbb{T}$ may be viewed as a character of $\overline{K}_S$ that is trivial on $\mathfrak{a}$, we will first consider characters of $\overline{K}_S$. (Note that another way to view the previous sentence is that we have an injection $\mathbb{T}^\vee \hookrightarrow \overline{K}_S^\vee$.) The group $\overline{K}_S$ is self-dual since it is a product of local fields. We now construct an explicit nontrivial character of $\overline{K}_S$ that will facilitate subsequent arguments.

7.1 Constructing a character of $\overline{K}_S$

For each $v \in S$, one can define a nontrivial local character $\phi_v : K_v \to S^1$ in a natural way. If v is real, we set $\phi_v(x) = e^{2\pi i x}$, and if v is complex, we set $\phi_v(z) = e^{2\pi i(z+\overline{z})}$. In the case where v is a finite prime, we define $\phi_v(\alpha)$ to be the exponential of $2\pi i$ times the the "polar part" of $\mathrm{Tr}_{K_v/\mathbb{Q}_p}(\alpha)$.[9] Then $\psi = \prod_{v\in S} \phi_v$ is a non-trivial character of $\overline{K}_S$ and we have the explicit isomorphism $\overline{K}_S \to \overline{K}_S^\vee$ given by $\xi \mapsto \psi_\xi$; here $\psi_\xi(\eta) = \psi(\xi\eta)$.

Since $\mathcal{O}_S$ is a proper closed subgroup of $\overline{K}_S$ there is a nonzero character ϕ of $\overline{K}_S$ that is trivial on $\mathcal{O}_S$. By duality, $\phi = \psi_\rho$ for some $\rho \in \overline{K}_S$. Therefore

$$\phi(\xi) = \prod_{v\in S} \phi_v(\rho_v \xi_v)\,. \tag{1}$$

As before we have an explicit isomorphism $\overline{K}_S \to \overline{K}_S^\vee$ given by $\xi \mapsto \phi_\xi$ where $\phi_\xi(\eta) = \phi(\xi\eta)$. To completely justify this, one should check that $\rho_v \neq 0$ for all $v \in S$. Suppose it were the case that $\rho_w = 0$ for some w. Then

[9] Here p is the rational prime lying under v, and the polar part of an element of $\mathbb{Q}_p$ is the element of $\mathbb{Q}/\mathbb{Z}$ defined by the (non-unique) decomposition $\mathbb{Q}_p = \mathbb{Z}[1/p] + \mathbb{Z}_p$.

we would have that $\ker \phi$ contains both K_w and $\mathcal{O}_S$ which implies that ϕ is the trivial character (by an application Lemma 5.4 with $\mathfrak{a} = \mathcal{O}_S$), a clear contradiction. We will not need to determine the ρ_v; it will be enough to know that they are all nonzero.

For the remainder of the paper, ϕ will refer to this particular fixed character of $\overline{K}_S$. Likewise, the notations ϕ_ξ and ϕ_v will refer to the characters constructed here. Notice that ϕ depends upon the number field K and set of primes S, but it does not depend upon the choice of $\mathfrak{a}$.

7.2 The dual of $\mathbb{T}$

Definition. Given a subset $E \subseteq \overline{K}_S$, we define its complement:

$$E^\perp = \{\xi \in \overline{K}_S \mid \phi(\xi E) = 1\}.$$

It is an easy exercise to show that if E is a subgroup (or $\mathcal{O}_S$-submodule) of $\overline{K}_S$, then so is $E^\perp$.

Lemma 7.1. *The map $\mathfrak{a}^\perp \to \mathbb{T}^\vee$ given by $\alpha \mapsto \phi_\alpha$ is an isomorphism of topological groups.*

Proof. Every character of $\mathbb{T}$ may be viewed as a character of $\overline{K}_S$ that is trivial on $\mathfrak{a}$. Every character of $\overline{K}_S$ is of the form ϕ_ξ for some $\xi \in \overline{K}_S$. Finally, a character ϕ_ξ is trivial on $\mathfrak{a}$ if and only if $\xi \in \mathfrak{a}^\perp$. □

To make the previous result useful, one would like a better description of $\mathfrak{a}^\perp$.

Lemma 7.2. *If $\mathfrak{b}$ is a fractional ideal of $\mathcal{O}_S$, then so is $\mathfrak{b}^\perp$. Moreover $\mathfrak{b}^\perp = \mathfrak{b}^{-1}\mathcal{O}_S^\perp$.* [10]

Proof. Since $\phi(\mathcal{O}_S) = 1$ we have $\mathcal{O}_S \subseteq \mathcal{O}_S^\perp$. We show that $\mathcal{O}_S^\perp/\mathcal{O}_S$ is finite. First, since $\mathcal{O}_S^\perp$ is dual to the compact group $\overline{K}_S/\mathcal{O}_S$ (by the previous lemma) we know that $\mathcal{O}_S^\perp$ is discrete. It follows that $\mathcal{O}_S^\perp/\mathcal{O}_S$ is a discrete subspace of the compact space $\overline{K}_S/\mathcal{O}_S$ and therefore finite. If we set $d = |\mathcal{O}_S^\perp/\mathcal{O}_S|$, then this gives $d\mathcal{O}_S^\perp \subseteq \mathcal{O}_S$ and therefore $\mathcal{O}_S^\perp$ is contained in K. In light of previous comments, it now follows easily that $\mathcal{O}_S^\perp$ is a fractional ideal of $\mathcal{O}_S$. Finally, given that $\mathfrak{b}$ and $\mathcal{O}_S^\perp$ are fractional ideals, it is easy to show that $\mathfrak{b}^\perp = \mathfrak{b}^{-1}\mathcal{O}_S^\perp$. □

[10] Here $\mathcal{O}_S^\perp$ plays the role of the inverse different $\mathfrak{D}^{-1}$. In particular, when $S = S_\infty$ one can take $\phi = \prod_{v \in S} \phi_v$ and we have $\mathcal{O}_S^\perp = \mathfrak{D}^{-1}$.

7.3 The action of the units is ergodic

Definition. Let G be a compact topological group with normalized Haar measure μ. An automorphism $\sigma : G \to G$ is ergodic if $\sigma(E) = E$ implies $\mu(E) = 0$ or $\mu(E) = 1$ for every measurable set E.

Lemma 7.3 (Halmos)**.** *A (continuous) automorphism of a compact abelian group G is ergodic if and only if the induced automorphism on the character group $G^\vee$ has no finite orbits (other than the trivial one).*

Proof. The proof is a one page argument using Pontryagin duality and Fourier series. See [11] for the details. □

Lemma 7.4. *If $u \in \mathcal{U}_S$ is not a root of unity, then the automorphism of $\mathbb{T}$ given by $[\xi] \mapsto u[\xi]$ is ergodic.*

Proof. We will use Lemma 7.3. Since any character of $\mathbb{T}$ may be viewed as a character of $\overline{K}_S$ that is trivial on $\mathfrak{a}$, we will consider characters of $\overline{K}_S$. One checks that the action of multiplication by $\mathcal{U}_S$ induces the action $u\phi_\xi = \phi_{u\xi}$ on $\overline{K}_S^\vee$.

Now let n denote a nonzero integer. Using duality, we have $u^n\phi_\xi = \phi_\xi \Rightarrow \phi_{u^n\xi} = \phi_\xi \Rightarrow u^n\xi = \xi \Rightarrow (u^n - 1)\xi = 0 \Rightarrow u^n = 1$ or $\xi = 0$. By hypothesis, u is not a root of unity. Hence the only solution to $u^n\chi = \chi$ is when χ is the trivial character. □

7.4 Convergence of subgroups

Definition. Let G be a locally compact abelian group. For a subgroup H of G, we define the annihilator of H in $G^\vee$ to be

$$A(G^\vee, H) = \{\chi \in G^\vee \mid \chi(H) = 1\}.$$

Lemma 7.5 (Berend)**.** *Let G be a compact abelian metric group. A sequence G_n of closed subgroups of G satisfies $G_n \to G$ in the Hausdorff metric if and only if for every nonzero $\chi \in G^\vee$ we have $\chi \notin A(G^\vee, G_n)$ for sufficiently large n.*

Proof. The proof is half a page and uses the Haar measure and integral on the groups involved. See [2] for the details. □

Lemma 7.6. *Suppose L is a subgroup of $\overline{K}_S$. Let $u \in \mathcal{U}_S$. If $u^n\overline{\pi(L)} \not\to \mathbb{T}$, then there exists nonzero $\alpha \in K$ and an increasing sequence $n_k \in \mathbb{Z}^+$ such that $\phi(u^{n_k}\alpha L) = 1$ for all k.* [11]

[11] Actually α lies in the fractional ideal $\mathfrak{a}^\perp$, but we won't need this.

Proof. Suppose $u^n\overline{\pi(L)} \not\to \mathbb{T}$. Then Lemma 7.5 says that there exists a nonzero $\chi \in \mathbb{T}^\vee$ and an increasing sequence $n_k \in \mathbb{Z}^+$ such that $\chi(u^{n_k}\overline{\pi(L)}) = 1$ for all k. Viewing χ as a character on $\overline{K}_S$ and using duality (Lemma 7.1), we know there exists a nonzero $\alpha \in \mathfrak{a}^\perp$ so that $\chi([\xi]) = \phi_\alpha(\xi) = \phi(\alpha\xi)$ for all $\xi \in \overline{K}_S$. This leads to $\phi(u^{n_k}\alpha L) = 1$ for all k. □

8 Proof of Proposition 1

Lemma 8.1. *Let U be a finite index subgroup of $\mathcal{U}_S$, and Λ be a closed U-invariant subset of $\mathbb{T}$ with nonempty interior. If $\#S \geq 2$, then $\Lambda = \mathbb{T}$.*

Proof. First observe that Λ has nonzero measure because it has nonempty interior. The group U is of finite index in $\mathcal{U}_S$ and therefore $\operatorname{rank}(U) = \operatorname{rank}(\mathcal{U}_S) = \#S - 1 \geq 1$, which implies that U contains a unit which is not a root of unity. Now Lemma 7.4 implies that Λ is dense in $\mathbb{T}$, giving the result. □

In order to prove the proposition, we first give a construction and a lemma. For the remainder of this section, let M be a $\mathcal{U}_S$-minimal subset of $\mathbb{T}$. It suffices to show that $M - M = \mathbb{T}$ implies $M = \mathbb{T}$, as clearly $\mathbb{T}$ is not $\mathcal{U}_S$-minimal. Hence we assume that $M - M = \mathbb{T}$. We will write ξ, η for an element of $\overline{K_S}$ as well as the corresponding element of $\mathbb{T}$; that is, we will drop the brackets from the expressions $[\xi]$,$[\eta]$.

Construction. Define $U^{(n)} = (\mathcal{U}_S)^{n!}$ so that $U^{(n)} \subseteq (\mathcal{U}_S)^n$ and $\mathcal{U}_S = U^{(1)} \supseteq U^{(2)} \supseteq U^{(3)} \supseteq \dots$; choose a sequence of subsets $M = M^{(1)} \supseteq M^{(2)} \supseteq \dots$ so that $M^{(k)}$ is $U^{(k)}$-minimal. Finally, define the set $M^\infty = \cap_k M^{(k)}$; observe that M^∞ is closed and nonempty since $\mathbb{T}$ is compact.

Lemma 8.2. *Given $\xi \in K$, we have $\xi + \eta \in M$ for all $\eta \in M^\infty$.*

Proof. Let $\xi \in K$. First we show that there exists $\eta' \in M^\infty$ so that $\xi + \eta' \in M$. Since $\operatorname{Orb}(\xi)$ is finite, there exists $N \in \mathbb{Z}^+$ such that $(\mathcal{U}_S)^N\xi = \{\xi\}$ and hence $U^{(N)}\xi = \{\xi\}$. For ease of notation, set $U' = U^{(N)}$ and $M' = M^{(N)}$. Since U' has finite index in $\mathcal{U}_S$, we have $\mathcal{U}_S/U' = \{a_1U', a_2U', \dots, a_\ell U'\}$ for $a_k \in \mathcal{U}_S$ with $a_1 = 1$.

We define the closed sets $\Lambda_i = M - a_iM'$ for $i = 1, \dots, \ell$. We observe $\cup_{i=1}^\ell a_iM' = M$ as the former set is closed and $\mathcal{U}_S$-invariant and clearly contained in the latter set. Since $M - M = \mathbb{T}$ by hypothesis, this leads to $\cup_{i=1}^\ell \Lambda_i = \mathbb{T}$. It is now easy to see that Λ_j must have nonempty interior for some j. Since Λ_j is closed and U'-invariant, Lemma 8.1 gives $\Lambda_j = \mathbb{T}$.

It follows that there exists $\eta \in a_j M'$ such that $a_j\xi + \eta \in M$ and therefore $\xi + a_j^{-1}\eta = a_j^{-1}(a_j\xi + \eta) \in M$. It is plain that $\eta' := a_j^{-1}\eta \in M'$. We have shown that there exists $\eta' \in M'$ such that $\xi + \eta' \in M$. Now observe that $U'(\xi + \eta') \subseteq M$, and since $\overline{U'\eta'} = M'$ and $U'\xi = \{\xi\}$, we have $\xi + \eta \in M$ for all $\eta \in M'$. □

Proof of Proposition 1. Fix $\eta \in M^\infty$. We will show that $M - \eta = \mathbb{T}$ from which $M = \mathbb{T}$ immediately follows. Since K is dense in $\mathbb{T}$, it suffices to show that $K \subseteq M - \eta$. Let $\xi \in K$ be arbitrary. The previous lemma says that $\xi + \eta \in M$. The result follows. □

9 Proof of Proposition 2.

The following standard result in algebraic number theory will be helpful. If one was forced to attach names to it, the following might be called the Dirichlet–Minkowski–Hasse–Chevalley Unit Theorem.

S-Unit Theorem. *For every $w \in S$ there exists $\varepsilon \in \mathcal{U}_S$ such that $|\varepsilon|_v < 1$ for all $v \in S$ with $v \neq w$. Moreover, choosing ε_w as above for each $w \in S$ yields a set $\{\varepsilon_w\}_{w\in S}$ which, after any one element is discarded, forms an independent set of units (modulo torsion) and generates a finite index subgroup of $\mathcal{U}_S$; in particular* $\operatorname{rank}(\mathcal{U}_S) = \#S - 1$.

The following lemma allows us to locate points that "live in a single component".

Lemma 9.1. *Suppose $\#S \geq 2$. Let N be a closed $\mathcal{U}_S$-invariant subset of $\overline{K}_S$ that contains 0 as a non-isolated point. For each $w \in S$, the set $N \cap K_w$ contains a nonzero point.*

Proof. By hypothesis, there is a sequence $\xi_n \in N$, $\xi_n \neq 0$, with $\xi_n \to 0$. We will write $\xi_n = (\xi_{n,v})_{v\in S}$. By the S-Unit Theorem there exists a unit $u \in \mathcal{U}_S$ such that $|u|_v < 1$ for all $v \neq w$, and hence $C := |u|_w > 1$. Define

$$\mathcal{A} = \left\{(\alpha_v)_{v\in S} \in \overline{K}_S : |\alpha_w|_w \geq 1\,,\ |\alpha_v|_v \leq C\ \ \forall v \in S\right\}\,.$$

For all sufficiently large m we have $|\xi_{m,v}|_v \leq 1$ for all $v \in S$ and hence there exists a $j_m \in \mathbb{Z}^+$ such that $u^{j_m}\xi_m \in \mathcal{A}$. Since $\mathcal{A}$ is compact there is a limit point η of this sequence; $\eta \in \mathcal{A}$ and hence $\eta \neq 0$. Since N is $\mathcal{U}_S$-invariant and closed we have $\eta \in N$. Finally, for all $v \neq w$ we have $|u|_v < 1$ which implies $|u^{j_m}\xi_{m,v}|_v \to 0$ and hence $\eta \in K_w$. □

9.1 K has a real embedding

Given what we have shown up to this point, it is now quite easy to establish Proposition 2 in the case where K has a real embedding. This makes use of the following fact:

Lemma 9.2. *Suppose $K \subseteq \mathbb{R}$ is a number field. If $\mathrm{rank}(\mathcal{U}_S) \geq 2$, then $\mathcal{U}_S$ is dense in $\mathbb{R}$.*

This result is well-known and not hard to establish, but we prove it here for the sake of completeness and also because it motivates what we do in the general case. We will need the following well-known result in Diophantine approximation (see, for example, [7]).

Kronecker's Theorem. *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$. Then*

$$\{(m\alpha_1, \ldots, m\alpha_n) \mid m \in \mathbb{Z}\}$$

is dense in $\mathbb{R}^n/\mathbb{Z}^n$ iff $1, \alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$.

Lemma 9.2 follows immediately from:

Lemma 9.3. *Let $a, b \in \mathbb{R}^+$. Suppose a and b are multiplicatively independent. Then $\{a^n b^m \mid n, m \in \mathbb{Z}\}$ is dense in $\mathbb{R}^+$.*

Proof. Taking the logarithm to the base a of $a^n b^m$ gives $m + n\alpha$ where $\alpha = \log b / \log a$. Thus it suffices to show that $\{m + n\alpha \mid m, n \in \mathbb{Z}\}$ is dense in $\mathbb{R}$. But since a, b are multiplicatively independent, we know that α is irrational. Thus $\{n\alpha \mid n \in \mathbb{Z}\}$ is dense in $\mathbb{R}/\mathbb{Z}$ by Kronecker's Theorem. The result follows. □

Proof of Proposition 2 when K has a real embedding. Set $\tilde{N} = \pi^{-1}(N)$. Then $\tilde{N}$ is a closed $\mathcal{U}_S$-invariant subset of $\overline{K}_S$ that contains 0 as a non-isolated point. Let w be a real place and apply Lemma 9.1 to $\tilde{N}$. This gives an element $x \in \mathbb{R} = K_w \subseteq \overline{K}_S$ such that $x \in \tilde{N}$, $x \neq 0$. Lemma 9.2 tells us that $\mathcal{U}_S$ is dense in $\mathbb{R}$ and hence $\{ux \mid u \in \mathcal{U}_S\}$ is dense in $\mathbb{R}$; it follows that $\tilde{N}$ contains $\mathbb{R}$. Now Lemma 5.4 gives $\tilde{N} = \overline{K}_S$ and hence $N = \mathbb{T}$. □

At this junction, we point out that we have completely justified Theorem 3, and hence all the results of §1,2,3, in the case where K has a real embedding. In particular, this is enough to establish Corollary 2. However, there is more work to be done to establish our results in the case where K is totally complex. We don't seem to get any additional mileage out of the assumption that all the embeddings are complex, so we will simply work with number fields that have at least one complex embedding.

9.2 K has a complex embedding

We recall the following standard definition.

Definition. We call a number field K a CM-field if either of the two equivalent conditions are satisfied:

1. K is a totally complex quadratic extension of a totally real field.
2. There is a subfield F of K with $\text{rank}(\mathcal{U}_F) = \text{rank}(\mathcal{U}_K)$.

The equivalence of the two definitions follows from Dirichlet's Unit Theorem (or the S-Unit Theorem with $S = S_\infty$). We write K^+ for the maximal totally real subfield of K. In the case where K is a CM-field we have $[K : K^+] = 2$.

Lemma 9.4. *Suppose $K \subseteq \mathbb{C}$ is a number field with $K \not\subseteq \mathbb{R}$. If K is not a CM-field, then there exists $u \in \mathcal{U}$ such that $u^n \notin \mathbb{R}$ for all nonzero $n \in \mathbb{Z}$.*

Proof. Suppose that for every $u \in \mathcal{U}$ there exists $n \in \mathbb{Z}^+$ such that $u^n \in \mathbb{R}$. It follows that there must exists $N \in \mathbb{Z}^+$ such that $\mathcal{U}^N \subseteq \mathbb{R}$. If $K \not\subseteq \mathbb{R}$, this implies $\mathbb{Q}(\mathcal{U}^N) \neq K$ which forces K to be a CM-field. □

Lemma 9.5. *Suppose $K \subseteq \mathbb{C}$ is a number field with $K \not\subseteq \mathbb{R}$. If K is a CM-field and S contains a finite prime that splits in K/K^+, then there exists $u \in \mathcal{U}_S$ such that $u^n \notin \mathbb{R}$ for all nonzero $n \in \mathbb{Z}$.*

Proof. Let $\mathfrak{P}$ be a finite prime in S that splits in K/K^+. Let h denote the class number of K. Then define $u \in \mathcal{O}$ by $(u) = \mathfrak{P}^h$. It is plain that $u \in \mathcal{U}_S$ since $v(u) = 0$ for all $v \notin S$. By way of contradiction, suppose $u^n \in \mathbb{R}$ for some nonzero $n \in \mathbb{Z}$. Then we would have $u^n \in K^+$ and $(u^n) = \mathfrak{P}^{hn}$ in K. Since $\mathfrak{P}$ lies above two distinct primes in K^+, this is impossible. □

In what follows, we will write $[x]$ to denote the floor of x, and write $x = [x] + \{x\}$ so that $\{x\}$ denotes the fractional part of x. We will also use the notation $\|x\| = \inf_{y \in \mathbb{Z}} |x - y|$.

Lemma 9.6. *Suppose $\alpha, \beta \in \mathbb{R}$ and $\alpha \notin \mathbb{Q}$. Then there exists $r, s \in \mathbb{Z}$ with $r > 0$ such that $\{(m\alpha, m\beta) \mid m \in \mathbb{Z}\}$ is dense in $\{(rt, st) \mid t \in \mathbb{R}\}$ when they are both viewed as subsets of $\mathbb{R}^2/\mathbb{Z}^2$.*

Proof. If $\{1, \alpha, \beta\}$ is linearly independent over $\mathbb{Q}$ then the result follows from Kronecker's Theorem (with $n = 2$). Otherwise we have $a\alpha + b\beta + c = 0$ with $a, b, c \in \mathbb{Z}$, not all zero; we must have $b \neq 0$ lest we contradict the fact

that $\alpha \notin \mathbb{Q}$, and, without loss of generality, we may assume that $b > 0$. Pick $t \in \mathbb{R}$ and let $\varepsilon > 0$ be given. Pick $\delta > 0$ so that $|a|\delta, |b|\delta < \varepsilon$. Applying Kronecker's Theorem (with $n = 1$) we may choose $m \in \mathbb{Z}$ so that $\|m\alpha - t\| < \delta$. It follows that $\|mb\alpha - bt\| < |b|\delta < \varepsilon$. Also we have $b\beta = -a\alpha - c$ which implies $mb\beta = -a(m\alpha - t) - at - mc$. Therefore $\|mb\beta + at\| < |a|\delta < \varepsilon$. It follows that $(mb\alpha, mb\beta)$ is ε-close to $(bt, -at)$ in $\mathbb{R}^2/\mathbb{Z}^2$. □

The following result says that in our situation the closure of $\mathcal{U}_S$ contains a nice spiral or concentric circles. It is a little complicated to state, but it plays the same role as Lemma 9.2.

Lemma 9.7. *Suppose $K \subseteq \mathbb{C}$ and $K \not\subseteq \mathbb{R}$. Suppose K is not a CM-field or S contains a finite prime that splits in K/K^+. If $\#S \geq 3$ then either:*

1. $\overline{\mathcal{U}}_S \supseteq \{z^t \mid t \in \mathbb{R}\}$ *where* $z \in \mathbb{C} \setminus \mathbb{R}$, $|z| > 1$
2. $\overline{\mathcal{U}}_S \supseteq \{x^n z^t \mid t \in \mathbb{R}, n \in \mathbb{Z}\}$ *where* $z \in \mathbb{C} \setminus \mathbb{R}$, $|z| = 1$, $x \in \mathbb{R}$, $x > 1$

Proof. First, suppose there exists $u \in \mathcal{U}_S$ with $|u| = 1$ which is not a root of unity. In this case, $\{u^m \mid m \in \mathbb{Z}\}$ is dense in the unit circle. Using the S-Unit Theorem we may choose $v \in \mathcal{U}_S$ with $|v| > 1$. We see that $\{u^m v^n \mid m, n \in \mathbb{Z}\}$ is dense in $\{|v|^n u^t \mid t \in \mathbb{R}, n \in \mathbb{Z}\}$. In this case, conclusion 2 holds with $z = u$ and $x = |v|$. Hence we may assume that no elements of $\mathcal{U}_S$ other than roots of unity are unimodular.

Since $\operatorname{rank}(\mathcal{U}_S) = \#S - 1 \geq 2$, we know that $\mathcal{U}_S$ contains two independent units u and v. Write $u = |u|e^{2\pi i\theta}$ and $v = |v|e^{2\pi i\varphi}$, where $|u|, |v| \neq 1$. Given our hypotheses, we may assume that $\theta \notin \mathbb{Q}$ (see Lemmas 9.4 and 9.5). Without loss of generality, we may assume $|u| > 1$ by replacing u with u^{-1} if necessary.

Set $\alpha = \log|v|/\log|u|$ and $\beta = \varphi - \alpha\theta$. Observe that α is irrational; if it was the case that $\alpha = a/b$, then $u^a v^{-b}$ would be a unimodular unit which is not a root of unity. Choose r, s as in the previous lemma. Set $z = |u|^r e^{2\pi i(r\theta + s)}$. Choose $\delta > 0$ small enough so that $\{rt\} = rt$ for all $t \in [0, \delta]$. Since $\overline{\mathcal{U}}_S$ is a multiplicative group, to prove the lemma it suffices to show that $\overline{\mathcal{U}}_S \supseteq \{z^t \mid 0 < t < \delta\}$.

Fix $t \in (0, \delta)$. We construct sequences n_k and m_k so that $u^{n_k} v^{m_k} \to z^t$. By our choice of r, s, there is a sequence m_k so that $(m_k\alpha, m_k\beta)$ converges to (rt, st) in $\mathbb{R}^2/\mathbb{Z}^2$; it follows that $\{m_k\alpha\} \to \{rt\}$ and that $m_k\beta$ converges to st in $\mathbb{R}/\mathbb{Z}$. Set $n_k = -[m_k\alpha]$ so that $n_k + m_k\alpha \to rt$. It follows that

$|u|^{n_k}|v|^{m_k} \to |u|^{rt}$. Now observe that

$$n_k\theta + m_k\varphi = \{m_k\alpha\}\theta + m_k\beta\,,$$

which converges (modulo 1) to $rt\theta + st$. It follows that

$$u^{n_k}v^{m_k} \to |u|^{rt}e^{2\pi i(r\theta+s)t} = z^t\,.$$

□

Proof of Proposition 2. Set $\tilde{N} = \pi^{-1}(N)$. Then $\tilde{N}$ is a closed $\mathcal{U}_S$-invariant subset of $\overline{K}_S$ that contains 0 as a non-isolated point. Pick a complex place of K and apply Lemma 9.1 to $\tilde{N}$. (Since we have already proved the result when K has a real place, we may certainly assume that K has a complex place.) This gives a nonzero element $a \in \mathbb{C} \subseteq \overline{K}_S$ such that $a \in \tilde{N}$. In what follows, distances between sets and convergence of sets will always be measured using the standard Hausdorff distance.

Claim 1: There exists a sequence of (compact) arcs A_n and line segments L_n which lie in $\mathbb{C} \subseteq \overline{K}_S$ with the following properties:

$$A_n \subseteq \tilde{N}\,,\ d(L_n, A_n) \to 0\,,\ \text{length}(L_n) \to \infty$$

We apply Lemma 9.7 and obtain one of two possible conclusions (see the statement of the lemma). First, we assume that conclusion 1 holds. (When conclusion 2 holds, the proof will be similar.) We have that $\overline{\mathcal{U}}_S$ contains $\{z^t \mid t \in \mathbb{R}\}$ for some $z \in \mathbb{C} \setminus \mathbb{R}$ with $|z| > 1$. Therefore $\tilde{N}$ contains the spiral $\{az^t \mid t \in \mathbb{R}\}$ in $\mathbb{C}$. The arcs A_n we construct will be subarcs of this spiral and are therefore all automatically contained in $\tilde{N}$. Let $\delta_n > 0$ be a sequence of real numbers with $\delta_n \to 0$ to be chosen later. Define the arc:

$$A_n = \{az^t : t \in [n, n+\delta_n]\}\,.$$

Let L_n denote the corresponding line segment which has the same endpoints. Namely,

$$L_n = \left\{az^n\left[1 + \lambda(z^{\delta_n} - 1)\right] : \lambda \in [0,1]\right\}\,.$$

For $\lambda \in [0,1]$ we write $t = n + \delta_n\lambda$ and, using calculus, we obtain:[12]

$$\begin{aligned} A_n(\lambda) - L_n(\lambda) &= az^n\left[(z^{\lambda\delta_n} - 1) - \lambda(z^{\delta_n} - 1)\right] \\ &= az^n\left[\frac{\text{Log}^2 z}{2}\lambda(\lambda-1)\delta_n^2 + O(\delta_n^3)\right] \end{aligned}$$

[12]Log will denote the principal branch of the logarithm.

Thus there are constants $C_1, C_2 > 0$ such that for n sufficiently large, we have:

$$\begin{aligned} d(A_n, L_n) &\leq C_1 |z|^n \delta_n^2 \\ \text{length}(L_n) &= |a||z|^n |z^{\delta_n} - 1| \\ &\geq C_2 |z|^n \delta_n \end{aligned}$$

Choose $\delta_n > 0$ with $|z|^n \delta_n^2 \to 0$ but $|z|^n \delta_n \to \infty$ so that $d(A_n, L_n) \to 0$ and $\text{length}(L_n) \to \infty$. This completes the proof of the claim in this case.

Now we suppose that conclusion 2 of Lemma 9.7 holds, so that $\tilde{N}$ contains $\{ax^n z^t \mid t \in \mathbb{R},\, n \in \mathbb{Z}\}$; here $z \in \mathbb{C} \setminus \mathbb{R}$, $|z| = 1$, $x \in \mathbb{R}$, $x > 1$. This time we use:

$$A_n = \{ax^n z^t : t \in [0, \delta_n]\}$$
$$L_n = \left\{ax^n \left[1 + \lambda(z^{\delta_n} - 1)\right] : \lambda \in [0, 1]\right\}$$

For $\lambda \in [0, 1]$ we write $t = \delta_n \lambda$ and find:

$$A_n(\lambda) - L_n(\lambda) = ax^n \left[(z^{\lambda \delta_n} - 1) - \lambda(z^{\delta_n} - 1)\right]$$

Hence there are constants $C_1, C_2 > 0$ such that for n sufficiently large, we have:

$$d(A_n, L_n) \leq C_1 x^n \delta_n^2\,, \quad \text{length}(L_n) \geq C_2 x^n \delta_n$$

As before we choose δ_n appropriately and the claim follows.

Claim 2: There is a line $L \subseteq \mathbb{C} \subseteq \overline{K}_S$ passing through the origin such that $[\xi] + \pi(L) \subseteq N$ for some $\xi \in \overline{K}_S$.

We can think of each line segment L_n (given by the previous claim) as a triple $(x_n, y_n, z_n) \in \mathbb{C} \times S^1 \times \mathbb{R}^+$ which represents the midpoint, direction, and length of the segment. Namely,

$$L_n = \{x_n + t y_n : -z_n \leq 2t \leq z_n\}\,.$$

(The choice of $y_n \in S^1$ in this representation is not unique, but this won't affect the argument.) By passing to a subsequence, we may assume that $\pi(x_n) \to [\xi]$ for some $[\xi] \in \mathbb{T}$ and $y_n \to y$ for some $y \in S^1$; we have $z_n \to \infty$ by what we have already shown. Therefore, for each $t \in \mathbb{R}$ we have $\pi(x_n + t y_n) \to [\xi] + \pi(ty)$.

Let L denote the line corresponding to the triple $(0, y, \infty)$ which passes through the origin in the direction of y; namely,

$$L = \{t\, y \mid t \in \mathbb{R}\}\,.$$

We show that $[\xi] + \pi(L) \subseteq N$. Let $\eta \in [\xi] + \pi(L)$ be arbitrary and $\varepsilon > 0$ be given. For n sufficiently large, we have

$$d(\eta, N) \leq d(\eta, \pi(A_n)) \leq d(\eta, \pi(L_n)) + d(\pi(L_n), \pi(A_n)) < \varepsilon\,.$$

Since N is closed, we obtain $\eta \in N$. This proves the claim.

Claim 3: There is a unit $u \in \mathcal{U}_S$ such that $u^n\overline{\pi(L)} \to \mathbb{T}$.

Pick $u \in \mathcal{U}_S$ so that $u^n \notin \mathbb{R}$ for all $n \in \mathbb{Z}^+$ (see Lemmas 9.4 and 9.5). By way of contradiction, suppose $u^n\overline{\pi(L)} \not\to \mathbb{T}$. In light of Lemma 7.6 there exists a nonzero $\alpha \in K$ and a strictly increasing sequence of positive integers n_k so that $\phi(u^{n_k}\alpha L) = 1$ for all k. Fix an arbitrary $k \in \mathbb{Z}^+$. We have $\phi(u^{n_k}\alpha t y) = 1$ for all $t \in \mathbb{R}$. Since $y \in \mathbb{C} \subseteq \overline{K}_S$ and the local character is $\phi_w(z) = e^{2\pi i(z+\overline{z})}$ (see Equation 1), this leads to $2\Re(u^{n_k} t y') \in \mathbb{Z}$ for all $t \in \mathbb{R}$ where we define $y' := \rho_w \alpha y \in \mathbb{C} \subseteq \overline{K}_S$. Because $y' \neq 0$, it follows that $\Re(u^{n_k} y') = 0$. Now we see that $u^{n_2 - n_1} \in \mathbb{R}$. This contradiction proves the claim.

By Claim 2 and the fact that N is closed, we have $[\xi] + \overline{\pi(L)} \subseteq N$. By Claim 3, we have $u^n\overline{\pi(L)} \to \mathbb{T}$. Choose a subsequence so that $u^{n_k}[\xi] \to [\eta]$ for some $[\eta] \in \mathbb{T}$. Therefore $u^{n_k}([\xi] + \overline{\pi(L)}) = u^{n_k}[\xi] + u^{n_k}\overline{\pi(L)} \to [\eta] + \mathbb{T}$. Since N is closed and $\mathcal{U}_S$-invariant, we conclude $[\eta] + \mathbb{T} \subseteq N$ which implies $N = \mathbb{T}$. □

10 Proof of Proposition 3

Suppose Theorem 3 holds except in the case where K is a CM-field and distinct primes in S lie over distinct primes in K^+. We will show it holds in the remaining cases.

Let K be a CM-field with totally real subfield K^+. We assume that distinct primes in S lie over distinct primes in K^+. Let S^+ denote the set of all primes in K^+ (including the infinite ones) lying under primes in S. Given our hypotheses, no finite primes of S are split in K/K^+ and $\#S = \#S^+$. For ease of notation, we will write $\mathcal{U}_S = \mathcal{U}_{K,S}$ and $\mathcal{U}_{S^+} = \mathcal{U}_{K^+,S^+}$. Now we proceed to the proof proper.

Proof of Proposition 3. Since $\mathcal{U}_{S^+}$ is contained in $\mathcal{U}_S$, it suffices to prove that every nonempty closed $\mathcal{U}_{S^+}$-invariant subset of $\mathbb{T}$ contains torsion elements.

First we consider what happens locally. Choose $v \in S^+$. By our hypothesis, there is exactly one prime $w \in S$ lying above v. In this case, we

have the inclusion $K_v^+ \subseteq K_w$ (with $[K_w : K_v^+] = 2$) and the isomorphism $K_w/K_v^+ \simeq K_v^+$. (Let $\{1, \theta\}$ be a basis for K/K^+; then $\{1, \theta\}$ is also a basis for K_w/K_v^+ and the aforementioned isomorphism is the one that sends the coset represented by $x + y\theta$ to the element y.) The multiplication action of $\mathcal{U}_{S^+}$ on K_w induces an action on K_v^+ via mapping $K_w \to K_w/K_v^+ \simeq K_v^+$; one checks that this is just the usual multiplication action so that in subsequent arguments we won't be dealing with two different actions.

In light of the inclusions of local fields discussed above, we have an inclusion $\overline{K}_{S^+}^+ \subseteq \overline{K}_S$ and an isomorphism $\overline{K}_S/\overline{K}_{S^+}^+ \simeq \overline{K}_{S^+}^+$. If we define $\mathfrak{a}^+ = \mathfrak{a} \cap K^+$ and $\mathbb{T}^+ = \overline{K}_{S^+}^+/\mathfrak{a}^+$, then this leads to an exact sequence of compact abelian groups:

$$0 \to \mathbb{T}^+ \to \mathbb{T} \to \mathbb{T}/\mathbb{T}^+ \to 0 \tag{2}$$

We have that $\mathcal{U}_{S^+}$ acts on $\mathbb{T}$ and $\mathbb{T}^+$ and this leads to an action of $\mathcal{U}_{S^+}$ on $\mathbb{T}/\mathbb{T}^+$. Moreover, Theorem 3 applies to K^+ and hence every nonempty $\mathcal{U}_{S^+}$-invariant subset of $\mathbb{T}^+$ contains torsion elements. We will show that the same holds for $\mathbb{T}/\mathbb{T}^+$ and hence for $\mathbb{T}$.

The situation is summarized by the following commutative diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathfrak{a}^+ & \longrightarrow & \mathfrak{a} & \longrightarrow & \mathfrak{a}/\mathfrak{a}^+ & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \overline{K}_{S^+}^+ & \longrightarrow & \overline{K}_S & \longrightarrow & \overline{K}_S/\overline{K}_{S^+}^+ & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{T}^+ & \longrightarrow & \mathbb{T} & \longrightarrow & \mathbb{T}/\mathbb{T}^+ & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

The isomorphism $\overline{K}_S/\overline{K}_{S^+}^+ \simeq \overline{K}_{S^+}^+$ carries $\mathfrak{a}/\mathfrak{a}^+$ to a fractional ideal $\mathfrak{b}$ and we obtain the isomorphic exact sequences:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathfrak{a}/\mathfrak{a}^+ & \longrightarrow & \overline{K}_S/\overline{K}_{S^+}^+ & \longrightarrow & \mathbb{T}/\mathbb{T}^+ & \longrightarrow & 0 \\
 & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\
0 & \longrightarrow & \mathfrak{b} & \longrightarrow & \overline{K}_{S^+}^+ & \longrightarrow & \mathbb{T}_*^+ & \longrightarrow & 0
\end{array}$$

In light of previous comments, the induced action of $\mathcal{U}_{S^+}$ on $\mathbb{T}_*^+ = \overline{K}_{S^+}^+/\mathfrak{b}$ is just the usual multiplication action. Here we have written $\mathbb{T}_*^+$ to emphasize

that it is potentially different from $\mathbb{T}^+$ since the quotient is by a different ideal. In any case, Theorem 3 applied to K^+ tells us that every nonempty closed $\mathcal{U}_{S^+}$-invariant subset of $\mathbb{T}_*^+$ contains torsion elements; hence the same holds for $\mathbb{T}/\mathbb{T}^+$.

Finally, we use what we have shown to complete the proof. Reconsidering the exact sequence (2), we note that the desired result holds for both $\mathbb{T}^+$ and $\mathbb{T}/\mathbb{T}^+$. Let N be a nonempty closed $\mathcal{U}_{S^+}$-invariant subset of $\mathbb{T}$. Applying the result for $\mathbb{T}/\mathbb{T}^+$, we have that $\pi(N) \subseteq \mathbb{T}/\mathbb{T}^+$ contains torsion elements which implies[13] that $mN \cap \mathbb{T}^+ \neq \emptyset$ for some $m \in \mathbb{Z}^+$. Since the set $mN \cap \mathbb{T}^+$ has the property in question, we apply the result for $\mathbb{T}^+$ to conclude that $mN \cap \mathbb{T}^+$ contains torsion elements. It follows that N contains torsion elements. □

Acknowledgements

This author would like to thank Hendrik Lenstra for his helpful suggestions and encouragement, and Mary Flahive and Tom Schmidt for many helpful discussions. This research was partially supported by a faculty development summer grant from Ursinus College.

References

[1] E. S. Barnes and H. P. F. Swinnerton-Dyer. The inhomogeneous minima of binary quadratic forms. II. *Acta Math.*, 88:279–316, 1952.

[2] Daniel Berend. Multi-invariant sets on tori. *Trans. Amer. Math. Soc.*, 280(2):509–532, 1983.

[3] Daniel Berend. Minimal sets on tori. *Ergodic Theory Dynam. Systems*, 4(4):499–507, 1984.

[4] Daniel Berend. Multi-invariant sets on compact abelian groups. *Trans. Amer. Math. Soc.*, 286(2):505–535, 1984.

[5] Manjul Bhargava. Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. *Ann. of Math. (2)*, 159(1):217–250, 2004.

[6] Duncan A. Buell. *Binary quadratic forms*. Springer-Verlag, New York, 1989. Classical theory and modern computations.

[13] Here π denotes the projection $\pi : \mathbb{T} \to \mathbb{T}/\mathbb{T}^+$ which is different than the previous usage of this notation.

[7] J. W. S. Cassels. *An introduction to Diophantine approximation*. Cambridge Tracts in Mathematics and Mathematical Physics, No. 45. Cambridge University Press, New York, 1957.

[8] J. W. S. Cassels. Global fields. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 42–84. Thompson, Washington, D.C., 1967.

[9] Jean-Paul Cerri. Inhomogeneous and Euclidean spectra of number fields with unit rank strictly greater than 1. *J. Reine Angew. Math.*, 592:49–62, 2006.

[10] Harry Furstenberg. Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation. *Math. Systems Theory*, 1:1–49, 1967.

[11] Paul R. Halmos. On automorphisms of compact groups. *Bull. Amer. Math. Soc.*, 49:619–624, 1943.

[12] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[13] Franz Lemmermeyer. The Euclidean algorithm in algebraic number fields. *Exposition. Math.*, 13(5):385–416, 1995.

[14] Hendrik W. Lenstra, Jr. Euclidean ideal classes. In *Journées Arithmétiques de Luminy (Colloq. Internat. CNRS, Centre Univ. Luminy, Luminy, 1978)*, volume 61 of *Astérisque*, pages 121–131. Soc. Math. France, Paris, 1979.

[15] Hendrik W. Lenstra, Jr. Euclidean number fields. II. *Math. Intelligencer*, 2(2):73–77, 99–103, 1979/80. Translated from the Dutch by A. J. Van der Poorten.

[16] Uri Shapira and Zhiren Wang. Remarks on Euclidean minima. *J. Number Theory*, 137:93–121, 2014.

Kevin J. McGown

Oregon State University, Corvallis, Oregon, USA

Ursinus College, Collegeville, Pennsylvania, USA

California State University, Chico, USA