EPIsciences

Communications in Mathematics **33** (2025), no. 1, Paper no. 6
DOI: https://doi.org/10.46298/cm.14235

Constructions of well-rounded algebraic lattices over odd prime degree cyclic number fields

Robson de Araujo, Antonio de Andrade, Trajano da Nóbrega Neto, Jéfferson Bastos

Abstract. Algebraic lattices are those obtained from modules in the ring of integers of algebraic number fields through canonical or twisted embeddings. In turn, well-rounded lattices are those with maximal cardinality of linearly independent vectors in its set of minimal vectors. Both classes of lattices have been applied for signal transmission in some channels, such as wiretap channels. Recently, some advances have been made in the search for well-rounded lattices that can be realized as algebraic lattices. Moreover, some works have been published that study algebraic lattices obtained from modules in cyclic number fields of odd prime degree p. In this work, we generalize some results of a recent work of Tran et al. and we provide new constructions of well-rounded algebraic lattices from a certain family of modules in the ring of integers of each of these fields when p is ramified in its extension over the field of rational numbers.

Contents

MSC 2020: 11H06, 11R20.
Keywords: Cyclic number fields, algebraic lattices, well-rounded lattices.
Contact information:
R. R. de Araujo:
Affiliation: Federal Institute of São Paulo, Catanduva, Brazil.
Email: robson.ricardo@ifsp.edu.br
A. A. de Andrade:
Affiliation: São Paulo State University, São José do Rio Preto, Brazil.
Email: antonio.andrade@unesp.br
T. P. da Nóbrega Neto:
Affiliation: São Paulo State University, São José do Rio Preto, Brazil.
Email: trajano.nobrega@unesp.br
J. L. R. Bastos:
Affiliation: São Paulo State University, São José do Rio Preto, Brazil.
Email: jefferson.bastos@unesp.br

1 Introduction

Lattices are discrete additive subgroups of $\mathbb{R}^n$. Recently, they have been considered for applications in different areas, such as coding theory and cryptography [5,6,20]. Algebraic lattices are those obtained as image in the Euclidean space of some $\mathbb{Z}$-module in the ring of integers of an algebraic number field through the canonical embedding or some twisted embedding. In last decades, algebraic lattices have been studied from different perspectives [1,3,9,19].

Explicitly, a lattice $\Lambda \subseteq \mathbb{R}^n$ of rank $k \leq n$ is defined as the $\mathbb{Z}$-module generated by a set $\mathcal{B} = \{u_1, u_2, \ldots, u_k\}$ of k linearly independent vectors in $\mathbb{R}^n$ - this set $\mathcal{B}$ is called a basis of Λ. In this work, we only consider full-rank lattices, which are those having maximal rank $k = n$. If Λ is a full-rank lattice in $\mathbb{R}^n$, then it can be obtained as $\Lambda = \mathbf{M}\mathbb{Z}^n$, where $\mathbf{M}$ is the matrix $n \times n$ whose columns are given by the entries of the vector in a basis of Λ - this matrix is called a generator matrix of Λ. In this case, the volume of Λ is defined by $Vol(\Lambda) = |\det(\mathbf{M})|$ and the minimum norm of Λ is given by $t_\Lambda = \min\{\|\mathbf{u}\|^2 : \mathbf{0} \neq \mathbf{u} \in \Lambda\}$, where $\|.\|$ is the usual Euclidian norm in $\mathbb{R}^n$. The center density of Λ is defined as $\delta(\Lambda) = \rho(\Lambda)^n / Vol(\Lambda)$, where $\rho(\Lambda) = \sqrt{t_\Lambda}/2$ is the largest radius such that it is possible to obtain a sphere packing with centers in the points of the lattice Λ. This parameter $\delta(\Lambda)$ is important because it is related to the classic sphere packing problem [5], since the center density is greater, the spherical packing centered at the points of the lattice is greater.

The set of minimal vectors of a lattice Λ is defined by $S(\Lambda) = \{\mathbf{u} \in \Lambda : \|\mathbf{u}^2\| = t_\Lambda\}$. The lattice Λ is said to be well-rounded if $S(\Lambda)$ generates $\mathbb{R}^n$, that is, if $S(\Lambda)$ contains a subset of n linearly independent vectors (this set can be or not a basis of the lattice). Research on well-rounded lattices has recently been developed due to their important properties and their applications for signal transmission over SISO and MIMO channels [15,16,21].

In particular, studies linking algebraic lattices and well-rounded lattices have been made after the remarkable work of Fukshansky and Petersen in 2012 [14]. In this work, the authors provide well-rounded algebraic lattices via real quadratic fields and prove a necessary and sufficient condition for the algebraic lattice coming from the whole ring of integers of an algebraic number field via the Minkowski embedding be well-rounded. Araujo and Costa [11] obtained (infinitely many) well-rounded lattices from cyclic number

fields of odd prime degree in the unramified case. In the last years, several other articles have been published relating well-rounded and algebraic lattices, such as [7, 8, 13, 26, 27].

Recently, several papers have been published studying algebraic lattices coming from $\mathbb{Z}$-modules in the ring of integers of cyclic number fields of odd prime degree p via the canonical embedding [9, 10, 11, 12, 17, 23], some of them in the perspective of the well-roundedness property. In this context, we need to consider two different cases: when p is unramified and when p in ramified in the extension of the fixed number field over the field of rational numbers. A family with infinitely many well-rounded algebraic lattices was presented in [11]. In turn, some constructions of well-rounded algebraic lattices have been provided in the ramified case in [2].

In this work, we present new constructions of well-rounded algebraic lattices in the ramified case (Section 3.2.2). In Proposition 3.2, we generalize the result of [27, Lemma 2.5], which is related to the construction of well-rounded algebraic lattices in cubic number fields. Using this fact, we provided a way to obtain well-rounded algebraic lattices over $\mathbb{K}$ via the canonical embedding (Corollary 3.3). Moreover, we present a family of modules over $\mathbb{K}$ which realizes well-rounded lattices via the canonical embedding (Subsection 3.2.2) and we give some additional results.

This paper is organized as follows. In Section 2, we present some definitions and basic facts about algebraic lattices (Subsection 2.1) and about odd prime degree cyclic number fields (Subsection 2.2). In Section 3, we present the contributions mentioned in the last paragraph.

2 Preliminaries

In this section we present some definitions and facts related to algebraic lattices (Subsection 2.1) and to odd prime degree cyclic number fields (Subsection 2.2) necessary in the development of this article.

2.1 Algebraic lattices

Let $\mathbb{K}$ be an algebraic number field of degree n and be $\mathcal{O}_{\mathbb{K}}$ its ring of algebraic integers. There are exactly n distinct $\mathbb{Q}$-monomorphisms $\sigma_i : \mathbb{K} \to \mathbb{C}$, for $i = 1, 2, \ldots, n$. A $\mathbb{Q}$-monomorphism σ_i is said to be real if $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$, and imaginary otherwise. A number field $\mathbb{K}$ is said to be totally real if σ_i is real for all $i = 1, 2, \ldots, n$ and totally imaginary if σ_i is imaginary for all $i = 1, 2, \ldots, n$. If $r_1 \geq 0$ denotes the number of indices such that $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, then $n - r_1$ is an even number satisfying $r_1 + 2r_2 = n$. In order to standardize, we denote the $\mathbb{Q}$-monomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_n$ in such a way that $\sigma_1, \ldots, \sigma_{r_1}$ are the real $\mathbb{Q}$-monomorphisms and that $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, for $j = 1, 2, \ldots, r_2$.

The trace of any element $\alpha \in \mathbb{K}$ is defined to be the rational number

$$Tr_{\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

and the discriminant of $\mathbb{K}$ over $\mathbb{Q}$ is given by

$$D(\mathbb{K}) = \det(Tr_{\mathbb{K}}(\alpha_i\alpha_j))_{i,j=1}^{n},$$

where $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is an integral basis of $\mathcal{O}_{\mathbb{K}}$. The canonical embedding $\sigma : \mathbb{K} \to \mathbb{R}^n$ is defined by setting $\sigma(x)$ as

$$(\sigma_1(x), \ldots, \sigma_{r_1}(x), Re(\sigma_{r_1+1}(x)), Im(\sigma_{r_1+1}(x)), \ldots, Re(\sigma_{r_1+r_2}(x)), Im(\sigma_{r_1+r_2}(x))), \quad (1)$$

where $x \in \mathbb{K}$, and $Re(\beta)$ and $Im(\beta)$ denote the real and the imaginary parts of the complex number β, respectively [24].

If $\mathcal{M}$ is a free $\mathbb{Z}$-module of $\mathcal{O}_{\mathbb{K}}$ with rank n, then $\Lambda = \sigma(\mathcal{M})$ is an n-dimensional lattice whose minimum is given by $t_\Lambda = \min\{\|\sigma(x)\|^2 : x \in \mathcal{M},\ x \neq 0\}$, where

$$\|\sigma(x)\|^2 = \begin{cases} Tr_{\mathbb{K}}(x^2) & \text{if } \mathbb{K} \text{ is totally real;} \\ \frac{1}{2}Tr_{\mathbb{K}}(x\overline{x}) & \text{if } \mathbb{K} \text{ is totally complex.} \end{cases}$$

if $\mathbb{K}$ is an Abelian number field. The lattice Λ is called an algebraic lattice. In particular, if $\mathcal{M}$ is an integral ideal of $\mathcal{O}_{\mathbb{K}}$, Λ is called an ideal lattice. The center density of the algebraic lattice $\Lambda = \sigma(\mathcal{M})$ is given by

$$\delta(\Lambda) = \frac{(\sqrt{t_\Lambda}/2)^n}{[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]\sqrt{|D(\mathbb{K})|}} = \frac{t_\Lambda^{n/2}}{2^n[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]\sqrt{|D(\mathbb{K})|}}, \quad (2)$$

where $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]$ denotes the index of $\mathcal{M}$ in $\mathcal{O}_{\mathbb{K}}$ as additive groups [24].

2.2 Odd prime degree cyclic number fields

Let $\mathbb{K}$ be a cyclic number field of prime degree $p > 2$. This means that $\mathbb{K}/\mathbb{Q}$ is an Abelian extension of degree p. Also, $\mathbb{K}$ is a totally real number field. By Kronecker-Weber Theorem, there exists $n > 0$ such that $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity [28, Theorem 14.1]. The smallest n with this property is called the conductor of $\mathbb{K}$. The discriminant of $\mathbb{K}$ is given by $D(\mathbb{K}) = n^{p-1}$ [18]. It is well known (see [25], for example) that:

1. p is unramified in $\mathbb{K}$ if and only if $n = p_1p_2 \ldots p_s$, with $s \geq 1$, or
2. p is ramified in $\mathbb{K}$ if and only if $n = p^2p_1p_2 \ldots p_s$, with $s \geq 0$,

where p_i are distinct prime numbers satisfying $p_i \equiv 1\ (mod\ p)$, for $i = 1, 2, \ldots, s$. Furthermore:

1. if p is unramified in $\mathbb{K}$, then $p\mathcal{O}_{\mathbb{K}} = \mathcal{B}$ and $p_i\mathcal{O}_{\mathbb{K}} = \mathcal{B}_i^p$, or
2. if p is ramified in $\mathbb{K}$, then $p\mathcal{O}_{\mathbb{K}} = \mathcal{B}^p$ and $p_i\mathcal{O}_{\mathbb{K}} = \mathcal{B}_i^p$,

where $\mathcal{B}$ and $\mathcal{B}_i$ are prime ideals in $\mathcal{O}_\mathbb{K}$ such that $\mathcal{B} \cap \mathbb{Z} = p\mathbb{Z}$ and $\mathcal{B}_i \cap \mathbb{Z} = p_i\mathbb{Z}$, for $i = 1, 2, \ldots, s$.

Denote by θ a generator of the cyclic Galois group $Gal(\mathbb{K}/\mathbb{Q})$ and by $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$ the trace of ζ_n in the field extension $\mathbb{Q}(\zeta_n)/\mathbb{K}$. As shown in [4, 10, 12], it is known that:

1. if p is unramified in $\mathbb{K}$, then $\{t, \theta(t), \ldots, \theta^{p-1}(t)\}$ is an integral basis of $\mathbb{K}$ and $Tr_\mathbb{K}(\theta^i(t)) = (-1)^s$, for $i = 0, 1, \ldots, p-1$, and

2. if p is ramified in $\mathbb{K}$, then $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ is an integral basis of $\mathbb{K}$ and also $Tr_\mathbb{K}(\theta^i(t)) = 0$, for $i = 0, 1, \ldots, p-1$.

3 Well-rounded algebraic lattices

Let $\mathbb{K}$ be a cyclic number field of prime degree $p > 2$. Consider the notation adopted in Subsection 2.2. In this section we present some constructions of well-rounded algebraic lattices coming from $\mathbb{Z}$-modules in the ring of integers of $\mathbb{K}$. Firstly, we generalize to p-th degree a result presented in [27] for third degree. We start with a technical lemma:

Lemma 3.1. *Let ζ_p be a primitive p-th root of unity and $\alpha \in \mathcal{O}_\mathbb{K}$. Consider the polynomial $f(x) = \alpha + \theta(\alpha)x + \theta^2(\alpha)x^2 + \ldots + \theta^{p-1}(\alpha)x^{p-1} \in \mathcal{O}_\mathbb{K}[x]$. If $\alpha \in \mathcal{O}_\mathbb{K} \setminus \mathbb{Z}$, then $f(\zeta_p^i) \neq 0$, for all $i = 1, 2, \ldots, p-1$.*

Proof. Let $\phi(x) = 1 + x + x^2 + \ldots + x^{p-1} \in \mathbb{Z}[x]$ be the minimal polynomial of ζ_p. Since $\gcd(p, p-1) = 1$, then $\mathbb{L} = \mathbb{K}[\zeta_p]$ has degree $p(p-1)$, which implies that $\phi(x)$ is irreducible over $\mathbb{K}$. So, supposing that $f(\zeta_p^i) = 0$ for some $i = 1, 2, \ldots, p-1$, then $\phi(x)$ divides $f(x)$ in $\mathbb{K}[x]$ since ζ_p^i is a root of the polynomials $f(x)$ and $\phi(x)$ simultaneously. Thus, since $\phi(x)$ is irreducible in $\mathbb{K}[x]$ and have the same degree of $f(x)$, it follows that $f(x) = \alpha\phi(x)$. This implies that $\theta^j(\alpha) = \alpha$ for all $j = 1, \ldots, p-1$. However, this leads to $\alpha \in \mathbb{Z}$, which is a contradiction. Therefore, $f(\zeta_p^i) \neq 0$, for all $i = 1, 2, \ldots, p-1$. □

The next result extends Lemma 2.5 of [27]:

Proposition 3.2. *Let $\alpha \in \mathcal{O}_\mathbb{K} \setminus \mathbb{Z}$. Then, $Tr_\mathbb{K}(\alpha) \neq 0$ if and only if the set*

$$\{\sigma(\alpha), \sigma(\theta(\alpha)), \ldots, \sigma(\theta^{p-1}(\alpha))\}$$

is a $\mathbb{R}$-linearly independent subset of $\mathbb{R}^p$, where σ is the canonical embedding of $\mathbb{K}$ in $\mathbb{R}^p$.

Proof. Suppose

$$a_0\sigma(\alpha) + a_1\sigma(\theta(\alpha)) + \cdots + a_{p-1}\sigma(\theta^{p-1}(\alpha)) = 0,$$

where $a_0, a_1, \ldots, a_{p-1} \in \mathbb{R}$. Since $\sigma(x) = (x, \theta(x), \ldots, \theta^{p-1}(x))$, where $x \in \mathbb{K}$, it follows that

$$C \cdot \begin{pmatrix} a_0 & a_1 & \ldots & a_{p-1} \end{pmatrix}^T = \begin{pmatrix} 0 & 0 & \cdots & 0 \end{pmatrix}^T$$

where C is the circulant matrix

$$C = \begin{pmatrix} \alpha & \theta(\alpha) & \theta^2(\alpha) & \cdots & \theta^{p-1}(\alpha) \\ \theta^{p-1}(\alpha) & \alpha & \theta(\alpha) & \cdots & \theta^{p-2}(\alpha) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \theta(\alpha) & \theta^2(\alpha) & \theta^3(\alpha) & \cdots & \alpha \end{pmatrix}.$$

It is well-known that the determinant of C is given by $\det(C) = \prod_{i=0}^{p-1} f(\zeta_p^i)$, where

$$f(\zeta_p^i) = \alpha + \theta(\alpha)\zeta_p^i + \theta^2(\alpha)\zeta_p^{2i} + \cdots + \theta^{p-1}(\alpha)\zeta_p^{(p-1)i},$$

for $i = 0, 1, \ldots, p-1$, and ζ_p is a primitive p-th root of unity. So, $\det(C) \neq 0$ if and only if $f(\zeta_p^i) \neq 0$, for all $i = 0, 1, \ldots, p-1$. From Lemma 3.1, it follows that $f(\zeta_p^i) \neq 0$, for $i = 1, 2, \ldots, p-1$. Thus, $\det(C) \neq 0$ if and only if $f(1) = Tr_{\mathbb{K}}(\alpha) \neq 0$. Therefore, $B = \{\sigma(\alpha), \sigma(\theta(\alpha)), \ldots, \sigma(\theta^{p-1}(\alpha))\}$ is $\mathbb{R}$-linearly independent subset of $\mathbb{R}^p$ if and only if $Tr_{\mathbb{K}}(\alpha) \neq 0$. □

The following corollary presents the construction of some well-rounded algebraic lattices via some special submodules of $\mathcal{O}_{\mathbb{K}}$:

Corollary 3.3. *Let $\mathcal{M} \subseteq \mathcal{O}_{\mathbb{K}}$ be a $\mathbb{Z}$-module such that $\theta(\mathcal{M}) \subseteq \mathcal{M}$. Let $\alpha \in \mathcal{M} \setminus \mathbb{Z}$ such that $\sigma(\alpha)$ is one of the shortest vectors in the lattice $\Lambda = \sigma(\mathcal{M})$. Then $Tr_{\mathbb{K}}(\alpha) \neq 0$ if and only if $B = \{\sigma(\alpha), \sigma(\theta(\alpha)), \ldots, \sigma(\theta^{p-1}(\alpha))\}$ generates a well-rounded sublattice of Λ of rank p.*

Proof. Firstly, we note that $\|\sigma(\theta^i(\alpha))\| = \lambda_1$ is a constant number for all $i = 0, 1, \ldots, p-1$, because, in this case, the canonical embedding is given by

$$\sigma(x) = (x, \theta(x), \theta^2(x), \ldots, \theta^{p-1}(x)),$$

which leads to the fact that the coordinates of $\sigma(\theta^i(\alpha))$ are a permutation of that of $\sigma(\alpha)$. Since $\theta(\mathcal{M}) \subseteq \mathcal{M}$ by hypothesis, and so $\theta^i(\mathcal{M}) \subseteq \mathcal{M}$ for all $i = 0, 1, \ldots, p-1$, then $L = \langle B \rangle_{\mathbb{Z}}$ generates a sublattice of Λ containing a shortest vector of it. Thus, B is a set having only minimal vectors of L. From this fact and from Proposition 3.2, finally this leads to the fact that $L = \langle B \rangle_{\mathbb{Z}}$ is a well-rounded full-rank sublattice of Λ if and only if $Tr_{\mathbb{K}}(\alpha) \neq 0$. □

We remark that the hypothesis in Corollary 3.3 given by $\theta(\mathcal{M}) \subseteq \mathcal{M}$ happens, for example, if $\mathcal{M} = \mathcal{O}_{\mathbb{K}}$ or if $\mathcal{M} = \mathcal{B}_1\mathcal{B}_2 \ldots \mathcal{B}_s$, since $\theta(\mathcal{B}_i) = \mathcal{B}_j$, for all $i, j = 1, 2, \ldots, s$.

3.1 The unramified case

Now suppose that p is unramified in $\mathbb{K}/\mathbb{Q}$. So the conductor of $\mathbb{K}$ is $n = p_1 p_2 \dots p_s$, for $s \geq 1$. For any $m > 0$ integer number, consider the subset of $\mathcal{O}_\mathbb{K}$ given by

$$\mathcal{M}_m = \{\alpha \in \mathcal{O}_\mathbb{K} : Tr_\mathbb{K}(\alpha) \equiv 0 \pmod{m}\},$$

or, equivalently,

$$\mathcal{M}_m = \left\{ \alpha = \sum_{i=0}^{p-1} a_i \theta^i(t) \in \mathcal{O}_\mathbb{K} : a_0, \dots, a_{p-1} \in \mathbb{Z}, \ \sum_{i=1}^{p-1} a_i \equiv 0 \pmod{m} \right\}.$$

As observed in [9], these modules generalize the prime ideals of $\mathcal{O}_\mathbb{K}$ above p_i - in fact, $\mathcal{B}_j = \mathcal{M}_{p_j}$, for $j = 1, 2, \dots, s$. Additionally, in the following proposition we give an explicit characterization of each prime ideal $\mathcal{B}_i$:

Proposition 3.4. $\mathcal{B}_j = p_j \mathbb{Z}t + \sum_{i=1}^{p-1} \mathbb{Z}(\theta^i(t) - t)$.

Proof. Let $\alpha = \sum_{i=0}^{p-1} a_i \theta^i(t) \in \mathcal{O}_\mathbb{K}$. Thus, $\alpha \in \mathcal{B}_j$ if and only if $\sum_{i=0}^{p-1} a_i = p_j k$, for some $k \in \mathbb{Z}$. Thus,

$$\alpha = \sum_{i=0}^{p-1} a_i \theta^i(t) - \sum_{i=0}^{p-1} a_i t + \sum_{i=0}^{p-1} a_i t = t \sum_{i=0}^{p-1} a_i + \sum_{i=0}^{p-1} a_i (\theta^i(t) - t) = p_j k t + \sum_{i=1}^{p-1} a_i (\theta^i(t) - t).$$

Therefore, $\alpha \in \mathcal{B}_j$ if and only if $\alpha \in p_j \mathbb{Z}t + \sum_{i=1}^{p-1} \mathbb{Z}(\theta^i(t) - t)$. □

Furthermore, about the family of $\mathbb{Z}$-modules $\mathcal{M}_m$, from [9, 11], it follows that:

1. $\mathcal{M}_m$ is a $\mathbb{Z}$-module of index m and rank p in $\mathcal{O}_\mathbb{K}$;
2. If $m \equiv 1 \pmod{p}$, the lattice $\sigma(\mathcal{M}_m)$ is well-rounded if and only if
$$\sqrt{\frac{n}{p+1}} \leq m \leq \sqrt{n(p+1)};$$
3. An element $\alpha \in \mathcal{O}_\mathbb{K}$ belongs to $\mathcal{B}_1 \mathcal{B}_2 \dots \mathcal{B}_s$ if and only if $Tr_\mathbb{K}(\alpha) \equiv 0 \pmod{n}$;
4. $\mathcal{M}_m$ is an ideal of $\mathcal{O}_\mathbb{K}$ if and only if $m | n$.

We emphasize the second point mentioned above, which states that $\sigma(\mathcal{M}_m)$ is well-rounded under certain conditions on m and p. Next, we explore the well-roundedness property of a similar family of $\mathbb{Z}$-modules in the case where p is ramified in $\mathbb{K}/\mathbb{Q}$.

3.2 The ramified case

In this section, our objective is to construct well-rounded algebraic lattices in the ramified case via $\mathbb{Z}$-submodules of $\mathcal{O}_{\mathbb{K}}$ with similar characterization of that presented in the unramified case (Subsection 3.1). Suppose that p is ramified in the extension $\mathbb{K}/\mathbb{Q}$, that is, $p\mathcal{O}_{\mathbb{K}} = \mathcal{B}^p$. In this case, the conductor of $\mathbb{K}$ is $n = p^2 p_1 p_2 \dots p_s$, for $s \geq 0$. We first give a characterization of the prime ideal above p using the norm function $N_{\mathbb{L}/\mathbb{K}}$ in the extension $\mathbb{L} = \mathbb{Q}(\zeta_{p^2})$ over $\mathbb{K}$, i.e., $n = p^2$:

Proposition 3.5. *If the conductor of $\mathbb{K}$ is $n = p^2$, then*

$$p\mathcal{O}_{\mathbb{K}} = \mathcal{B}^p,$$

where $\mathcal{B} = \langle N_{\mathbb{L}/\mathbb{K}}(1-\zeta_n)\rangle$.

Proof. In this case, it is well-known that $p\mathcal{O}_{\mathbb{L}} = \mathcal{B}_{\mathbb{L}}^{p(p-1)}$, where $\mathcal{B}_{\mathbb{L}} = (1-\zeta_n)\mathcal{O}_{\mathbb{L}}$ [22, (10.1) Lemma]. Let $\lambda = N_{\mathbb{L}/\mathbb{K}}(1-\zeta_n) = \prod_{j=1}^{p-1}(1-\zeta_n^{rjp})$, where r is a generator of the cyclic group $(\mathbb{Z}/p^2\mathbb{Z})^*$ of the inversible elements of $\mathbb{Z}/p^2\mathbb{Z}$. Since $1-\zeta_n$ is a conjugate of $1-\zeta_n^{rjp}$, for some $j = 1, 2, \dots, p-1$, it follows that $(1-\zeta_n)\mathcal{O}_{\mathbb{L}} = (1-\zeta_n^{rjp})\mathcal{O}_{\mathbb{L}}$. So,

$$\prod_{j=1}^{p-1}(1-\zeta_n^{rjp})\mathcal{O}_{\mathbb{L}} = (1-\zeta_n)^{p-1}\mathcal{O}_{\mathbb{L}},$$

and so $\lambda\mathcal{O}_{\mathbb{L}} = (1-\zeta_n^{rjp})\mathcal{O}_{\mathbb{L}}$. Thus, $\lambda\mathcal{O}_{\mathbb{L}} = \mathcal{B}_{\mathbb{L}}^{p-1} = \mathcal{B}\mathcal{O}_{\mathbb{L}}$. Therefore, $\lambda\mathcal{O}_{\mathbb{L}} = \mathcal{B}\mathcal{O}_{\mathbb{L}}$, that is, $\mathcal{B} = \langle\lambda\rangle = \langle N_{\mathbb{L}/\mathbb{K}}(1-\zeta_n)\rangle$, which proves the result. □

In the following, we present a family of $\mathbb{Z}$-submodules of $\mathcal{O}_{\mathbb{K}}$ initially studied in [9]. For any positive integers $m, c \in \mathbb{Z}$ such that $0 \leq c < m$, consider the set

$$\mathcal{M}_{m,c} = \left\{ \sum_{i=0}^{p-1} a_i\theta^i(t) \in \mathcal{O}_{\mathbb{K}} \ : \ a_0 + c\sum_{i=1}^{p-1} a_i \equiv 0 \pmod{m} \right\}$$

(where the coefficients a_i are integer numbers). From [9], it follows that

1. $\mathcal{M}_{m,c} = \left\{ \alpha \in \mathcal{O}_{\mathbb{K}} \ : \ Tr_{\mathbb{K}}\left(\frac{1}{p}\alpha - \frac{pc}{n}\alpha t\right) \equiv 0 (mod\ m) \right\}$;
2. $S = \{m, c-\theta(t), c-\theta^2(t), \dots, c-\theta^{p-1}(t)\}$ is a $\mathbb{Z}$-basis of $\mathcal{M}_{m,c}$;
3. $\mathcal{M}_{m,c}$ has rank p;
4. $\mathcal{O}_{\mathbb{K}}/\mathcal{M}_{m,c} \cong \mathbb{Z}/p\mathbb{Z}$;
5. $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}_{m,c}] = m$;
6. If $i \in \{1, \dots, p-1\}$, then $\mathcal{B}_i = \mathcal{M}_{p_i,0}$ and $\mathcal{B} = \mathcal{M}_{p,\ell}$ for some $\ell \in \{0, \dots, p-1\}$ such that $t - l \in \mathcal{B}$;

7. If $\alpha = a_0 m + a_1(c - \theta(t)) + \cdots + a_{p-1}(c - \theta^{p-1}(t)) \in \mathcal{M}_{m,c}$, with $a_i \in \mathbb{Z}$, for $i \in \{0, \ldots, p-1\}$, then

$$Tr_{\mathbb{K}}(\alpha^2) = p\left(\left(a_0 m + c\sum_{i=1}^{p-1} a_i\right)^2 + u\left(p\sum_{i=1}^{p-1} a_i^2 - \left(\sum_{i=1}^{p-1} a_i\right)^2\right)\right), \tag{3}$$

where $u = n/p^2$.

In this work, we specifically focus on the submodule $\mathcal{M}_m \subseteq \mathcal{O}_{\mathbb{K}}$ for any rational integer $m > 1$:

$$\mathcal{M}_m := \{\alpha \in \mathcal{O}_{\mathbb{K}} : Tr_{\mathbb{K}}(\alpha) \equiv 0 \pmod{m}\}.$$

We observe that

1. $\mathcal{M}_m = \mathcal{M}_{m,0}$ if and only if $p \nmid m$;
2. $\mathcal{M}_m = \mathcal{M}_{m/p,0}$ if and only if $p \mid m$.

Lemma 3.6. *$\mathcal{M}_m$ is an ideal of $\mathcal{O}_{\mathbb{K}}$ if and only if $m \mid n$.*

Proof. If $\alpha = a_0 + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathcal{M}_m$ (with $a_0, a_1, \ldots, a_{p-1} \in \mathbb{Z}$), then $Tr_{\mathbb{K}}(\alpha) \equiv 0 \pmod{m}$. From [10, Theorem 3.1], it follows that

$$Tr_{\mathbb{K}}(\theta^i(t)\theta^j(t)) = Tr_{\mathbb{K}}(t\theta^{i-j}(t)) = \begin{cases} \frac{n(p-1)}{p} & \text{if } i = j \\ -\frac{n}{p} & \text{if } i \neq j, \end{cases} \tag{4}$$

for $i, j = 0, 1, \ldots, p-1$. Thus,

$$Tr_{\mathbb{K}}(\alpha\theta^k(t)) = (a_1 + \cdots + a_{p-1})\left(\frac{-n}{p}\right) + a_k n,$$

for $k = 1, \ldots, p-1$. If $m \mid n$, then $Tr_{\mathbb{K}}(\alpha\theta^k(t)) \equiv 0 \pmod{m}$, for $k = 1, \ldots, p-1$. Thus, $\alpha\theta^k(t) \in \mathcal{M}_m$, for $k = 1, \ldots, p-1$. Since the set $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ is an integral basis of $\mathbb{K}$, it follows that $\mathcal{M}_m$ is an ideal. Reciprocally, $Tr_{\mathbb{K}}(\theta(t) - \theta^2(t)) = 0$, and, therefore, $\theta(t) - \theta^2(t) \in \mathcal{M}_m$. Since $\theta(t) \in \mathcal{O}_{\mathbb{K}}$ and $\mathcal{M}_m$ is an ideal, it follows that $\theta(t)(\theta(t) - \theta^2(t)) \in \mathcal{M}_m$. From Equation (4), it follows that

$$Tr_{\mathbb{K}}(\theta(t)(\theta(t) - \theta^2(t))) = Tr_{\mathbb{K}}(t^2) - Tr_{\mathbb{K}}(t\theta(t)) = n \equiv 0 \pmod{m},$$

that is, $m \mid n$. □

Lemma 3.7. *The index $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}_m]$ is m.*

Proof. Let $\alpha \in \mathcal{O}_{\mathbb{K}}$ and $[\alpha]$ denote the coset of M_m in $\mathcal{O}_{\mathbb{K}}$ containing α. The proof is completed by showing that the cosets $[0], [1], [2], \ldots, [(m-1)]$ partition $\mathcal{O}_{\mathbb{K}}$. Indeed, let $0 \leq i \leq j \leq m-1$. Then $[i] = [j]$ if and only if $[(i-j)] = [0]$, that is, $i - j \equiv 0$

(mod m), whence $i = j$ and the cosets $[0], [1], [2], \ldots, [(m-1)]$ are distinct. Finally, let $\alpha = a_0 + \sum_{i=1}^{p-1} a_i \theta^i(t) \in \mathcal{O}_{\mathbb{K}}$ (with $a_0, a_1, \ldots, a_{p-1}$ integer numbers). We can write

$$\alpha = a_0 + \sum_{i=1}^{p-1} a_i \theta^i(t) = a_0 + m \sum_{i=1}^{p-1} a_i + \sum_{i=1}^{p-1} a_i (\theta^i(t) - m).$$

Since $m \sum_{i=1}^{p-1} a_i + \sum_{i=1}^{p-1} a_i (\theta^i(t) - m) \in \mathcal{M}_m$, it follows that $\alpha \equiv a_0 \pmod{\mathcal{M}_m}$. By writing $a_0 = ms + r$ with $0 \leq r < m$, it follows that $[\alpha] = [r]$, that is, $\alpha \in [r]$, which proves the result. □

Lemma 3.8. *The rank of $\mathcal{M}_m$ is p.*

Proof. If $p \mid m$, then $\{m/p, m - \theta(t), \ldots, m - \theta^{p-1}(t)\}$ is a $\mathbb{Z}$-basis of $\mathcal{M}_m$. If $p \nmid m$, then $\{m, m - \theta(t), \ldots, m - \theta^{p-1}(t)\}$ is a $\mathbb{Z}$-basis of $\mathcal{M}_m$. Therefore, in both cases, the rank is p. □

3.2.1 Case $p \mid m$.

Suppose that p is a divisor of m. As pointed in Lemma 3.8, the submodule $\mathcal{M}_m$ of $\mathcal{O}_{\mathbb{K}}$ has basis $\{m/p, m - \theta(t), \ldots, m - \theta^{p-1}(t)\}$. In the next proposition, we calculate the trace form associated to $\mathcal{M}_m$ in relation with this basis:

Proposition 3.9. *If $\alpha = a_0 \frac{m}{p} + \sum_{i=1}^{p-1} a_i (m - \theta^i(t)) \in \mathcal{M}_m$, for some integer $a_0, a_1, \ldots, a_{p-1}$, then*

$$Tr_{\mathbb{K}}(\alpha^2) = p \left(\left(\frac{a_0 m}{p} + m \sum_{i=1}^{p-1} a_i \right)^2 + u \left(p \sum_{i=1}^{p-1} a_i^2 - \left(\sum_{i=1}^{p-1} a_i \right)^2 \right) \right) \tag{5}$$

where $u = n/p^2$.

Proof. Developing the expression of α^2, we have the following:

$$\begin{aligned}
\alpha^2 &= \tfrac{a_0^2 m^2}{p^2} + 2\tfrac{a_0 m}{p} \textstyle\sum_{i=1}^{p-1} a_i (m - \theta^i(t)) + \left(\sum_{i=1}^{p-1} a_i (m - \theta^i(t)) \right)^2 \\
&= \frac{a_0^2 m^2}{p^2} + 2\frac{a_0 m}{p} \sum_{i=1}^{p-1} a_i (m - \theta^i(t)) + \sum_{i=1}^{p-1} a_i^2 (m - \theta^i(t))^2 \\
&\quad +2 \sum_{1 \leq i < j \leq p-1} a_i a_j (m - \theta^i(t))(m - \theta^j(t)) \\
&= \frac{a_0^2 m^2}{p^2} + \frac{2a_0 m}{p} \sum_{i=1}^{p-1} a_i (m - \theta^i(t)) + \sum_{i=1}^{p-1} a_i^2 (m^2 - 2m\theta^i(t) + \theta^i(t)\theta^i(t)) \\
&\quad +2 \sum_{1 \leq i < j \leq p-1} a_i a_j (m^2 - m\theta^i(t) - m\theta^j(t) + \theta^i(t)\theta^j(t)).
\end{aligned}$$

Thus, the trace form is given by

$$\begin{aligned} Tr_{\mathbb{K}}(\alpha^2) &= \frac{a_0^2m^2}{p^2}Tr_{\mathbb{K}}(1) + 2\frac{a_0m}{p}\sum_{i=1}^{p-1} a_i Tr_{\mathbb{K}}(m-\theta^i(t)) \\ &\quad + \sum_{i=1}^{p-1} a_i^2 Tr_{\mathbb{K}}(m^2 - 2m\theta^i(t) + \theta^i(t)\theta^i(t)) \\ &\quad + 2\sum_{1\le i<j\le p-1} a_i a_j Tr_{\mathbb{K}}(m^2 - m\theta^i(t) - m\theta^j(t) + \theta^i(t)\theta^j(t)). \end{aligned}$$

Since $Tr_{\mathbb{K}}(1) = p$ and $Tr_{\mathbb{K}}(\theta^i(t)) = 0$, for $i = 1, 2, \ldots, p-1$, it follows from Equation (4) that

$$\begin{aligned} Tr_{\mathbb{K}}(\alpha^2) &= p\left(\frac{a_0^2m^2}{p^2}\right) + 2pm\frac{a_0m}{p}\sum_{i=1}^{p-1} a_i + \sum_{i=1}^{p-1} a_i^2\left(pm^2 + \frac{n(p-1)}{p}\right) \\ &\quad + 2\sum_{1\le i<j\le p-1} a_i a_j\left(pm^2 - \frac{n}{p}\right) \end{aligned}$$

and so

$$Tr_{\mathbb{K}}(\alpha^2) = p\left(\frac{a_0^2m^2}{p^2} + \frac{2a_0m^2}{p}\sum_{i=1}^{p-1} a_i + \sum_{i=1}^{p-1} a_i^2(m^2 + u(p-1)) + 2\sum_{1\le i<j\le p-1} a_i a_j(m^2-u)\right).$$

From this and since $\sum_{i=1}^{p-1} a_i^2 + 2\sum_{1\le i<j\le p-1} a_i a_j = \left(\sum_{i=1}^{p-1} a_i\right)^2$, it follows that

$$Tr_{\mathbb{K}}(\alpha^2) = p\left(\frac{(a_0m)^2}{p^2} + \frac{2a_0m^2}{p}\sum_{i=1}^{p-1} a_i + (m^2-u)\left(\sum_{i=1}^{p-1} a_i\right)^2 + up\sum_{i=1}^{p-1} a_i^2\right).$$

Finally, since

$$\left(\frac{a_0}{p} + \sum_{i=1}^{p-1} a_i\right)^2 = \frac{a_0^2}{p^2} + 2\frac{a_0}{p}\sum_{i=1}^{p-1} a_i + \left(\sum_{i=1}^{p-1} a_i\right)^2,$$

then

$$Tr_{\mathbb{K}}(\alpha^2) = p\left(\left(\frac{a_0m}{p} + m\sum_{i=1}^{p-1} a_i\right)^2 - u\left(\sum_{i=1}^{p-1} a_i\right)^2 + up\sum_{i=1}^{p-1} a_i^2\right),$$

that is,

$$Tr_{\mathbb{K}}(\alpha^2) = p\left(\left(\frac{a_0m}{p} + m\sum_{i=1}^{p-1} a_i\right)^2 + u\left(p\sum_{i=1}^{p-1} a_i^2 - \left(\sum_{i=1}^{p-1} a_i\right)^2\right)\right),$$

which proves the result. □

In order to calculate the minimum norm of the lattice $\Lambda_m = \sigma(\mathcal{M}_m)$, we will now compute the minimum of $Tr_{\mathbb{K}}(\alpha^2)$, for $0 \neq \alpha \in \mathcal{M}_m$, considering the Equation (5). For this purpose, consider the quadratic form $Q_1 : \mathbb{Z} \times \mathbb{Z}^{p-1} \to \mathbb{Z}$ given by

$$Q_1(a_0, (a_1, \ldots, a_{p-1})) = \left(\frac{a_0 m}{p} + m \sum_{i=1}^{p-1} a_i \right)^2$$

and the quadratic form $Q_2 : \mathbb{Z}^{p-1} \to \mathbb{Z}$ given by

$$Q_2(a_1, \ldots, a_{p-1}) = p \sum_{i=1}^{p-1} a_i^2 - \left(\sum_{i=1}^{p-1} a_i \right)^2.$$

So, Proposition 3.9 provides

$$Tr_{\mathbb{K}}(\alpha^2) = pQ_1(a_0, (a_1, \ldots, a_{p-1})) + uQ_2(a_1, \ldots, a_{p-1}), \tag{6}$$

for each $\alpha = a_0(m/p) + a_1(m - \theta(t)) + \cdots + a_{p-1}(m - \theta^{p-1}(t)) \in \mathcal{M}_m$, with $a_i \in \mathbb{Z}$, for $i = 0, 1, \ldots, p-1$.

Proposition 3.10. $\min\limits_{0 \neq \alpha \in \mathcal{M}_m} Tr_{\mathbb{K}}(\alpha^2) = \min\left\{ \frac{m^2}{p}, up(p-1) \right\}$.

Proof. From [9, Corollary 11], $Q_2(a_1, \ldots, a_{p-1}) = 0$ if and only if $a_1 = \ldots = a_{p-1} = 0$. Thus, from Equation (6), the minimum of $Tr_{\mathbb{K}}(\alpha^2)$ is m^2/p, since the minimum of Q_1 with this condition is equal to m^2/p^2, which is achieved only by setting $a_0 = \pm 1$. If $Q_2(a_1, \ldots, a_{p-1}) > 0$, from [9, Corollary 11], the minimum of Q_2 is $p-1$, which is achieved by the vectors $\pm(1, \ldots, 1)$ and by the permutations of $\pm(1, 0, \ldots, 0)$. In this case, the minimum of Q_1 is zero, which is achieved only for $a_0 = 0$, and, thus, from Equation (6) it follows that the minimum of $Tr_{\mathbb{K}}(\alpha^2)$ is $up(p-1)$. Therefore, the minimum of $Tr_{\mathbb{K}}(\alpha^2)$ for $0 \neq \alpha \in M_m$ is $\min\{m^2/p, up(p-1)\}$. □

As shown in the proof of Proposition 3.10, the value m^2/p is achieved for $\alpha = \pm m$ and the value $up(p-1)$ is achieved for $\alpha = \pm(m - \theta^i(t))$, with $i = 1, 2, \ldots, p-1$, and $\alpha = \pm \sum_{i=1}^{p-1}(m - \theta^i(t))$. Furthermore, Proposition 3.10 and Equation (2) provides that the center density of the algebraic lattice $\Lambda_m = \sigma(\mathcal{M}_m)$ is given by

$$\delta(\Lambda_m) = \frac{(\min\{m^2/p, up(p-1)\})^{p/2}}{2^p n^{\frac{p-1}{2}} m},$$

where $\Lambda_m = \sigma(\mathcal{M}_m)$.

3.2.2 Case: $p \nmid m$

Suppose that p is not a divisor of m. As shown in the proof of Lemma 3.8, the submodule $\mathcal{M}_m$ of $\mathcal{O}_{\mathbb{K}}$ has basis $\{m, m-\theta(t), \ldots, m-\theta^{p-1}(t)\}$. Let

$$\alpha = a_0 m + \sum_{i=1}^{p-1} a_i (m - \theta^i(t)) \in \mathcal{M}_m,$$

with $a_0, a_1, \ldots, a_{p-1} \in \mathbb{Z}$. From [9, Proposition 8], it follows that

$$Tr_{\mathbb{K}}(\alpha^2) = p\left[m^2\left(a_0 + \sum_{i=1}^{p-1} a_i\right)^2 + u\left[p\sum_{i=1}^{p-1} a_i^2 - \left(\sum_{i=1}^{p-1} a_i\right)^2\right]\right], \tag{7}$$

where $u = n/p^2$. From [9, Theorem 12], it follows that

$$\min_{0\neq\alpha\in\mathcal{M}_{m,0}} Tr_{\mathbb{K}}(\alpha^2) = \min\{pm^2,\ up(p-1)\}.$$

Furthermore, the center density of the algebraic lattice $\Lambda_m = \sigma(\mathcal{M}_m)$ is given by

$$\delta(\Lambda_m) = \frac{(\min\{pm^2, up(p-1)\})^{p/2}}{2^p n^{\frac{p-1}{2}} m},$$

where $\Lambda_m = \sigma(\mathcal{M}_m)$.

Observe that, in general, Λ_m is not a well-rounded lattice. However, consider the its submodule

$$\mathcal{M} = \{a_0(m-t) + a_1(m-\theta(t)) + \cdots + a_{p-1}(m-\theta^{p-1}(t)) :\ a_0, a_1, \ldots, a_{p-1} \in \mathbb{Z}\}.$$

The module $\mathcal{M}$ has rank p and $\mathcal{M} \subsetneq \mathcal{M}_m$, since $m \in \mathcal{M}_m$ and $m \notin \mathcal{M}$.

In the following, we compute the trace of α^2, for all α in this $\mathbb{Z}$-submodule:

Proposition 3.11. *If $\alpha = a_0(m-t) + a_1(m-\theta(t)) + \cdots + a_{p-1}(m-\theta^{p-1}(t)) \in \mathcal{M}$, with $a_0, a_1, \ldots, a_{p-1} \in \mathbb{Z}$, then*

$$Tr_{\mathbb{K}}(\alpha^2) = p\left(up\sum_{i=0}^{p-1} a_i^2 + (m^2-u)\left(\sum_{i=0}^{p-1} a_i\right)^2\right). \tag{8}$$

Proof. The expression of α^2 is given by

$$\begin{aligned}
\alpha^2 &= \sum_{i=0}^{p-1} a_i^2 (m-\theta^i(t))^2 + 2\sum_{0\le i<j\le p-1} a_i a_j (m-\theta^i(t))(m-\theta^j(t)) \\
&= \sum_{i=0}^{p-1} a_i^2 (m^2 - 2m\theta^i(t) + \theta^i(t)\theta^i(t)) \\
&\quad +2\sum_{0\le i<j\le p-1} a_i a_j (m^2 - m\theta^i(t) - m\theta^j(t) + \theta^i(t)\theta^j(t)).
\end{aligned}$$

Thus,

$$\begin{aligned} Tr_{\mathbb{K}}(\alpha^2) &= \sum_{i=0}^{p-1} a_i^2 Tr_{\mathbb{K}}(m^2 - 2m\theta^i(t) + \theta^i(t)\theta^i(t)) \\ &\quad +2 \sum_{0\leq i<j\leq p-1} a_i a_j Tr_{\mathbb{K}}(m^2 - m\theta^i(t) - m\theta^j(t) + \theta^i(t)\theta^j(t)). \end{aligned}$$

Since $Tr_{\mathbb{K}}(\theta^i(t)) = 0$, for $i = 0, 1, \ldots, p-1$, then

$$Tr_{\mathbb{K}}(\alpha^2) = \sum_{i=0}^{p-1} a_i^2 (Tr_{\mathbb{K}}(m^2) + Tr_{\mathbb{K}}(\theta^i(t)\theta^i(t))) + 2 \sum_{0\leq i<j\leq p-1} a_i a_j (Tr_{\mathbb{K}}(m^2) + Tr_{\mathbb{K}}(\theta^i(t)\theta^j(t))).$$

Also, $Tr_{\mathbb{K}}(\theta^i(t)^2) = Tr_{\mathbb{K}}(t^2)$ and $Tr_{\mathbb{K}}(\theta^i(t)\theta^j(t)) = Tr_{\mathbb{K}}(t\theta^{j-i}(t))$ for $j > i$. So,

$$Tr_{\mathbb{K}}(\alpha^2) = \sum_{i=0}^{p-1} a_i^2 (Tr_{\mathbb{K}}(m^2) + Tr_{\mathbb{K}}(t^2)) + 2 \sum_{0\leq i<j\leq p-1} a_i a_j (Tr_{\mathbb{K}}(m^2) + Tr_{\mathbb{K}}(t\theta^{j-i}(t)).$$

From Equation (4), it follows that

$$\begin{aligned} Tr_{\mathbb{K}}(\alpha^2) &= \sum_{i=0}^{p-1} a_i^2 \left(m^2 p + \frac{n(p-1)}{p} \right) + 2 \sum_{0\leq i<j\leq p-1} a_i a_j \left(m^2 p + \frac{-n}{p} \right) \\ &= \left(m^2 p + \frac{n(p-1)}{p} \right) \sum_{i=0}^{p-1} a_i^2 + 2 \left(m^2 p - \frac{n}{p} \right) \sum_{0\leq i<\leq p-1} a_i a_j \\ &= p \left(\left(m^2 + u(p-1) \right) \sum_{i=0}^{p-1} a_i^2 + 2(m^2 - u) \sum_{0\leq i<j\leq p-1} a_i a_j \right). \end{aligned}$$

Since $\left(\sum_{i=0}^{p-1} a_i \right)^2 = \sum_{i=0}^{p-1} a_i^2 + 2 \sum_{0\leq i<j\leq p-1} a_i a_j$, denoting $u = n/p^2$, we have that

$$Tr_{\mathbb{K}}(\alpha^2) = p \left(up \sum_{i=0}^{p-1} a_i^2 + (m^2 - u) \left(\sum_{i=1}^{p-1} a_i \right)^2 \right),$$

which proves the result. □

Equation (8) can be rewritten as

$$Tr_{\mathbb{K}}(\alpha^2) = p \left(uQ_1(a_0, a_1, \ldots, a_{p-1}) + m^2 Q_2(a_0, a_1, \ldots, a_{p-1}) \right),$$

where $Q_1 : \mathbb{Z}^p \to \mathbb{Z}$ and $Q_2 : \mathbb{Z}^p \to \mathbb{Z}$ are the quadratic forms defined by

$$Q_1(a_0, a_1, \ldots, a_{p-1}) = p \sum_{i=0}^{p-1} a_i^2 - \left(\sum_{i=0}^{p-1} a_i \right)^2$$

and

$$Q_2(a_0, a_1, \ldots, a_{p-1}) = \left(\sum_{i=0}^{p-1} a_i \right)^2.$$

The minimum of the trace form $Tr_{\mathbb{K}}(\alpha^2)$ is given below:

Proposition 3.12. $\min_{0 \neq \alpha \in \mathcal{M}} Tr_{\mathbb{K}}(\alpha^2) = p(u(p-1) + m^2)$.

Proof. Proposition 3.11 provides

$$Tr_{\mathbb{K}}(\alpha^2) = p\left(upQ_1(a_0, a_1, \ldots, a_{p-1}) + m^2 Q_2(a_0, a_1, \ldots, a_{p-1})\right),$$

for each

$$\alpha = a_0(m-t) + a_1(m-\theta(t)) + \cdots + a_{p-1}(m-\theta^{p-1}(t)) \in \mathcal{M},$$

with $a_0, a_1, \ldots, a_{p-1} \in \mathbb{Z}$. From [9, Corollary 11], the minimum of the quadratic form $Q_1(a_0, a_1, \ldots, a_{p-1})$ is $p-1$, which is achieved by the permutations of vectors $\pm(0, 1, 1, \ldots, 1)$ and by the permutations of $\pm(1, 0, \ldots, 0)$. In turn, the minimum of the quadratic form $Q_2(a_0, a_1, \ldots, a_{p-1})$ is 1, which is achieved by the permutations of $\pm(1, 0, \ldots, 0)$. This proves the proposition. □

By Proposition 3.12 and Equation (2), we have that the center density of the algebraic lattice $\Lambda_m = \sigma(\mathcal{M})$ is equal to

$$\delta(\Lambda_m) = \frac{(p(u(p-1) + m^2))^{p/2}}{2^p n^{\frac{p-1}{2}} m}.$$

Proposition 3.13. *$\sigma(\mathcal{M})$ is a well-rounded lattice with a minimal basis*

$$\{m - t,\ m - \theta(t),\ \ldots,\ m - \theta^{p-1}(t)\}.$$

Proof. For $i = 0, 1, \ldots, p-1$, it follows from Equation (4) that

$$\begin{aligned} Tr_{\mathbb{K}}(m - \theta^i(t))^2 &= Tr_{\mathbb{K}}(m^2) - 2mTr_{\mathbb{K}}(\theta^i(t)) + Tr_{\mathbb{K}}(t^2) \\ &= pm^2 + (n(p-1))/p = p(u(p-1) + m^2), \end{aligned}$$

which proves the result. □

Acknowledgments

The authors thank the reviewers for their valuable suggestions and the funding received from CNPq under Grant No. 405842/2023-6, from CAPES-PRINT-UNESP and from FAPESP 2022/02303-0.

References

[1] A. A. Andrade, A. J. Ferrari, C. W. O. Benedito, and S. I. R. Costa. Constructions of algebraic lattices. *Computational & Applied Mathematics*, 29:493–505, 2010.

[2] J. L. R. Bastos, R. R. de Araujo, T. P. da Nobrega Neto, and A. A. de Andrade. Algebraic lattices coming from $\mathbb{Z}$-modules generalizing ramified prime ideals in odd prime degree cyclic number fields. 2025. To appear in Advances in Geometry.

[3] E. Bayer-Fluckiger. Lattices and number fields. *Contemporary Mathematics*, 241:69–84, 1999.

[4] J. Carmelo Interlando, T. Pires da Nóbrega Neto, T. M. Rodrigues, and J. O. D. Lopes. A note on the integral trace form in cyclotomic fields. *Journal of Algebra and its Applications*, 14(04):1550045, 2015.

[5] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290. Springer Science & Business Media, 2013.

[6] S. I. Costa, F. Oggier, A. Campello, J.-C. Belfiore, and E. Viterbo. *Lattices applied to coding for reliable and secure communications*. Springer, 2017.

[7] M. T. Damir and D. Karpuk. Well-rounded twists of ideal lattices from real quadratic fields. *Journal of Number Theory*, 196:168–196, 2019.

[8] M. T. Damir and G. Mantilla-Soler. Bases of minimal vectors in tame lattices. *arXiv preprint arXiv:2006.16794*, 2020.

[9] A. A. de Andrade, R. R. de Araujo, T. P. da Nobrega Neto, and J. L. R. Bastos. Algebraic lattices coming from $\mathbb{Z}$-modules generalizing ramified prime ideals in odd prime degree cyclic number fields. *Applicable Algebra in Engineering, Communication and Computing*, pages 1–20, 2024.

[10] R. R. de Araujo, A. C. M. M. Chagas, A. A. de Andrade, and T. P. da Nobrega Neto. Trace form associated to cyclic number fields of ramified odd prime degree. *Journal of Algebra and Its Applications*, 19(04):2050080, 2020.

[11] R. R. de Araujo and S. I. R. Costa. Well-rounded algebraic lattices in odd prime dimension. *Archiv der Mathematik*, 112(2):139–148, 2019.

[12] E. L. De Oliveira, J. C. Interlando, T. P. Da Nobrega Neto, and J. O. D. Lopes. The integral trace form of cyclic extensions of odd prime degree. *The Rocky Mountain Journal of Mathematics*, 47(4):1075–1088, 2017.

[13] L. Fukshansky, G. Henshaw, P. Liao, M. Prince, X. Sun, and S. Whitehead. On well-rounded ideal lattices II. *International Journal of Number Theory*, 9(01):139–154, 2013.

[14] L. Fukshansky and K. Petersen. On well-rounded ideal lattices. *International Journal of Number Theory*, 8(01):189–206, 2012.

[15] O. W. Gnilke, A. Barreal, A. Karrila, H. T. N. Tran, D. A. Karpuk, and C. Hollanti. Well-rounded lattices for coset coding in mimo wiretap channels. In *2016 26th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 289–294. IEEE, 2016.

[16] O. W. Gnilke, H. T. N. Tran, A. Karrila, and C. Hollanti. Well-rounded lattices for reliability and security in rayleigh fading siso channels. In *2016 IEEE Information Theory Workshop (ITW)*, pages 359–363. IEEE, 2016.

[17] J. C. Interlando, A. A. de Andrade, B. G. Malaxechebarría, and R. R. de Araujo. Fully-diverse lattices from ramified cyclic extensions of prime degree. *International Journal of Applied Mathematics*, 33(6):1009, 2020.

[18] J. C. Interlando, J. O. D. Lopes, and T. P. D. N. NETO. The discriminant of abelian number fields. *Journal of Algebra and its Applications*, 5(01):35–41, 2006.

[19] G. C. Jorge, A. J. Ferrari, and S. I. Costa. Rotated D_n-lattices. *Journal of Number Theory*, 132(11):2397–2406, 2012.

[20] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29*, pages 1–23. Springer, 2010.

[21] J. Martinet. *Perfect lattices in Euclidean spaces*, volume 327. Springer Science & Business Media, 2013.

[22] J. Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[23] J. V. L. Nunes, J. C. Interlando, T. P. d. N. Neto, and J. O. D. Lopes. New p-dimensional lattices from cyclic extensions. *Journal of Algebra and Its Applications*, 16(10):1750186, 2017.

[24] P. Samuel. *Algebraic Theory of Numbers: Translated from the French by Allan J. Silberger*. Courier Corporation, 2013.

[25] B. K. Spearman and K. S. Williams. The discriminant of a cyclic field of odd prime degree. *The Rocky Mountain Journal of Mathematics*, pages 1101–1122, 2003.

[26] A. Srinivasan. A complete classification of well-rounded real quadratic ideal lattices. *Journal of Number Theory*, 207:349–355, 2020.

[27] D. T. Tran, N. H. Le, and H. T. Tran. Well-rounded ideal lattices of cyclic cubic and quartic fields. *Communications in Mathematics*, 31(2): 209–250, 2023.

[28] L. C. Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science & Business Media, 2012.

Received: September 10, 2024
Accepted for publication: March 14, 2025
Communicated by: Lenny Fukshansky