J. Algebra Comb. Discrete Appl.
13(2) • 179–186

Received: 2 September 2024
Accepted: 20 September 2025

Journal of Algebra Combinatorics Discrete Structures and Applications

Some constructions of unimodular lattices via totally real subfields of the p-th cyclotomic field*

Research Article

Antonio A. de Andrade**, Grasiele C. Jorge***

Abstract: Algebraic number theory has recently attracted significant interest due to its role in algebraic lattice theory and in the design of codes for applications in coding theory. Algebraic lattices have been useful in information theory, where the problem of constructing lattices over number fields with full diversity and maximal minimum product distance has been investigated, since these parameters are directly related to error probabilities over Rayleigh fading channels. In this paper, we present a family of full diversity rotated unimodular lattices constructed via totally real subfields of the cyclotomic fields $\mathbb{Q}(\zeta_p)$, with p an odd prime. A closed-form expression for the minimum product distance is derived.

2020 MSC: 11H06, 11H71, 11R18, 11R80

Keywords: Rotated lattices, Ideal lattices, Full diversity lattices

1. Introduction

A finite extension $\mathbb{K}$ of $\mathbb{Q}$ is called a number field, and the degree of the extension $\mathbb{Q} \subseteq \mathbb{K}$ is denoted by $[\mathbb{K} : \mathbb{Q}] = n$. In this case, there are n $\mathbb{Q}$-embeddings $\sigma_i : \mathbb{K} \to \mathbb{C}$. The Galois group of the extension $\mathbb{Q} \subseteq \mathbb{K}$, denoted by $Gal(\mathbb{K}/\mathbb{Q})$, is the group of $\mathbb{Q}$-automorphisms $\sigma : \mathbb{K} \to \mathbb{K}$. The ring of algebraic integers of $\mathbb{K}$ is defined as $\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} \mid$ there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0\}$, and it is a free $\mathbb{Z}$-module of rank n. The determination of the ring of integers has long been a subject of study and is closely linked to lattice theory. The norm and trace of an element $\alpha \in \mathbb{K}$ are defined as $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$ and

* This work was supported by CNPq 405842/2023-6, Fapesp 2022/02303-0 and Capes Print Unesp.
** Antonio A. de Andrade; São Paulo State University (UNESP), Institute of Biosciences, Humanities and Exact Sciences, São José do Rio Preto, Brazil (antonio.andrade@unesp.br).
*** Grasiele C. Jorge (Corresponding Author); Federal University of São Paulo (UNIFESP), Institute of Science and Technology, São José dos Campos, Brazil (grasiele.jorge@unifesp.br).

$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$, respectively. The discriminant of $\mathbb{K}$ is defined as $D_{\mathbb{K}} = \det\left(Tr_{\mathbb{K}/\mathbb{Q}}(\alpha_i\alpha_j)\right)_{i,j=1}^{n}$ $= \left(\det(\sigma_j(\alpha_i))_{i,j=1}^{n}\right)^2$, where $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_{\mathbb{K}}$.

It can be shown that every nonzero fractional ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module of rank n. The norm of a free $\mathbb{Z}$-module $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ of rank n is defined by $N_{\mathbb{K}}(\mathcal{I}) = \#(\mathcal{O}_{\mathbb{K}}/\mathcal{I})$. If $\mathcal{I}$ is a principal ideal, with $\mathcal{I} = \alpha\mathcal{O}_{\mathbb{K}}$ for some $\alpha \in \mathcal{O}_{\mathbb{K}}$, then $N_{\mathbb{K}}(\mathcal{I}) = |N_{\mathbb{K}/\mathbb{Q}}(\alpha)|$ [15].

A *lattice* Λ is a nonzero discrete additive subgroup of the n-dimensional Euclidean space $\mathbb{R}^n$. Equivalently, $\Lambda \subset \mathbb{R}^n$ is a lattice if and only if there exists a set $B = \{u_1, u_2, \ldots, u_m\}$ of linearly independent vectors in $\mathbb{R}^n$ such that

$$\Lambda = \left\{ \sum_{i=1}^{m} a_i u_i;\ a_i \in \mathbb{Z},\ i = 1, 2, \ldots, m \right\}.$$

The set B is called a *basis* for Λ. In this work we only consider full rank lattices, that is, lattices $\Lambda \subset \mathbb{R}^n$ with rank $m = n$. A matrix $M = (u_{i,j})_{i,j=1}^{n}$ whose rows are the vectors $u_1, \ldots, u_n$ is said to be a *generator matrix* for Λ, and the matrix $G = MM^t$ is called the *Gram matrix* associated with M. The *determinant* of Λ is defined by $\det(\Lambda) = \det(G)$, which is invariant under change of basis [8]. A lattice Λ has *diversity* $k \leq n$ if k is the largest integer such that every nonzero vector $y \in \Lambda$ has at least k nonzero coordinates. In particular, when $k = n$, the lattice is said to have full diversity. Given a full rank lattice $\Lambda \subseteq \mathbb{R}^n$ with full diversity, its *minimum product distance* [3] is defined as

$$d_{p,\min}(\Lambda) = \inf \left\{ \prod_{i=1}^{n} |y_i| \;\middle|\; y = (y_1, y_2, \ldots, y_n) \in \Lambda,\ y \neq 0 \right\}.$$

Proposition 1.1. *[3] If $\mathbb{K}$ is a totally real number field and $\mathcal{I} \subset \mathbb{K}$ is a free $\mathbb{Z}$-module of rank n, then $\Lambda = \sigma_\alpha(\mathcal{I})$ is a full diversity lattice and the minimum product distance of Λ is given by $d_{p,\min}(\Lambda) = \sqrt{N_{\mathbb{K}/\mathbb{Q}}(\alpha)}\ \min_{0\neq y\in\mathcal{I}} \left|N_{\mathbb{K}/\mathbb{Q}}(y)\right|$. If $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ is a principal ideal, then $d_{p,\min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{|D_{\mathbb{K}}|}}$.*

One of the most fruitful ways to construct lattices is via number fields. The connection between their geometric and algebraic natures was first observed by Minkowski. Specifically, in this work we consider a totally real number field $\mathbb{K}$ of degree n, together with its n distinct $\mathbb{Q}$-embeddings $\sigma_i : \mathbb{K} \to \mathbb{R}$ for $i = 1, 2, \ldots, n$.

The embedding

$$\begin{aligned} \sigma_\alpha : \mathbb{K} &\longrightarrow \mathbb{R}^n \\ x &\longmapsto \left(\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_n}\sigma_n(x)\right), \end{aligned}$$

where $\alpha \in \mathbb{K}$ is such that $\alpha_i = \sigma_i(\alpha) > 0$ for all $i = 1, \ldots, n$, is an injective homomorphism, called a *twisted embedding* [4, 5].

Proposition 1.2. *[3] If $\mathcal{I} \subset \mathbb{K}$ is a free $\mathbb{Z}$-module of rank n with $\mathbb{Z}$-basis $\{w_1, \ldots, w_n\}$, then the image $\Lambda = \sigma_\alpha(\mathcal{I})$ is a lattice in $\mathbb{R}^n$ with basis $\{\sigma_\alpha(w_1), \ldots, \sigma_\alpha(w_n)\}$. Moreover, $G = \left(Tr_{\mathbb{K}/\mathbb{Q}}(\alpha w_i w_j)\right)_{i,j=1}^{n}$ is a Gram matrix for Λ.*

This association between number fields and lattices in $\mathbb{R}^n$, called algebraic lattices, allows us to derive certain lattice parameters that are usually difficult to calculate for general lattices, such as the minimum product distance and the packing density.

If $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ is a $\mathbb{Z}$-module of rank n with $\mathbb{Z}$-basis $\{w_1, \ldots, w_n\}$, then the lattice $\sigma_\alpha(\mathcal{I})$ has generator matrix $M = M_1 D$, where

$$M_1 = \begin{pmatrix} \sigma_1(w_1) & \sigma_2(w_1) & \cdots & \sigma_n(w_1) \\ \sigma_1(w_2) & \sigma_2(w_2) & \cdots & \sigma_n(w_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(w_n) & \sigma_2(w_n) & \cdots & \sigma_n(w_n) \end{pmatrix}$$

and

$$D = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & 0 & \cdots & 0 \\ 0 & \sqrt{\sigma_2(\alpha)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sqrt{\sigma_n(\alpha)} \end{pmatrix}.$$

The purpose of this paper is to present a method for constructing a family of full diversity rotated unimodular lattices arising from totally real subfields of the cyclotomic fields $\mathbb{Q}(\zeta_p)$, where p is an odd prime. Section 2 presents basic results on p-th cyclotomic fields. Section 3 contains the main contributions, namely the construction of unimodular lattices. Section 4 concludes with a discussion of the results.

2. Basic resuts of p-th cyclotomic fields

Let p be an odd prime, and let $\mathbb{L} = \mathbb{Q}(\zeta_p)$ be the p-th cyclotomic field, where ζ_p is a primitive p-th root of unity. The extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p)$ is cyclic, and its Galois group is isomorphic to $\mathbb{Z}_p^* = \langle \overline{r} \rangle$, i.e., $Gal(\mathbb{L}/\mathbb{Q}) = \langle \sigma_r \rangle = \{\sigma_r, \sigma_{r^2}, \ldots, \sigma_{r^{p-1}}\}$, where $\sigma_{r^i}(\zeta_p) = \zeta_p^{r^i}$ for all $i = 1, 2, \ldots, p-1$.

From the Galois correspondence theorem, it follows that the subfields of $\mathbb{Q}(\zeta_p)$ are precisely the fixed fields $\mathbb{K} = \mathbb{Q}(\zeta_p)_H = \{\alpha \in \mathbb{Q}(\zeta_p) : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$ by subgroups H of $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Furthermore, the totally real subfields of $\mathbb{Q}(\zeta_p)$ are the fixed fields corresponding to subgroups $H \subseteq Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ such that the complex conjugation is contained in H. The following diagram illustrates the correspondence between intermediate fields of $\mathbb{Q} \subset \mathbb{L}$ and subgroups of its Galois group:

$$\begin{array}{ccc} \mathbb{Q}(\zeta_p) & \longleftarrow & \{0\} \\ | & & | \\ \mathbb{K} & \longleftarrow & H \\ | & & | \\ \mathbb{Q} & \longleftarrow & G \end{array}$$

Furthermore, the ring of algebraic integers of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-2}\zeta_p^{p-2} : a_0, a_1, \ldots, a_{p-2} \in \mathbb{Z}\}$.

We end this section with the following proposition, which characterizes the subfields of $\mathbb{Q}(\zeta_p)$. This result is extremely important for the lattice constructions presented in the next section.

Proposition 2.1. *[14] Let $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$ be a number field such that $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = m$ and $[\mathbb{K} : \mathbb{Q}] = n$. If $\theta = Tr_{\mathbb{Q}(\zeta_p):\mathbb{K}}(\zeta_p)$, then*

1. $\mathbb{K} = \mathbb{Q}(\theta)$;
2. $\{\sigma_r(\theta), \sigma_{r^2}(\theta), \ldots, \sigma_{r^n}(\theta)\}$ *is an integral basis for* $\mathcal{O}_{\mathbb{K}}$;
3. $Gal(\mathbb{K}/\mathbb{Q}) = \langle \sigma_r \rangle = \{\sigma_r, \sigma_{r^2}, \ldots, \sigma_{r^n}\}$;
4. *The discriminant of the extension* $\mathbb{Q} \subseteq \mathbb{K}$ *is* $D_{\mathbb{K}} = p^{n-1}$;
5. $Gal(\mathbb{L}/\mathbb{K}) = \langle \sigma_r^n \rangle = \{\sigma_{r^n}, \sigma_{r^{2n}}, \ldots, \sigma_{r^{mn}}\}$.

3. Construction of unimodular lattices

Constructions of algebraic lattices have been proposed in several papers, for example, [1–7, 9–11, 14]. Lattices constructed from totally real number fields have full diversity, which makes them attractive for

use on Rayleigh fading channels. Furthermore, results in the literature indicate that signal constellations based on algebraic lattices offer a good trade-off between bit labelling and constellation shaping, since they are only slightly worse in terms of shaping gain yet are usually easier to label. In [3], the authors showed that if $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is the maximal totally real subfield of $\mathbb{Q}(\zeta_p)$, p prime, and $\alpha = (1-\zeta_p)(1-\zeta_p^{-1})$, then the lattice $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ is a rotated $\mathbb{Z}^{\frac{p-1}{2}}$-lattice. In this case, the Gram matrix G associated with the $\mathbb{Z}$-basis $\{e_1, \ldots, e_n\}$, where $e_i = \zeta_p^i + \zeta_p^{-i}$ for all $i = 1, 2, \ldots, p-1$, of $\mathcal{O}_\mathbb{K}$ is given by

$$G = \begin{pmatrix} 2 & -1 & 0 & \ldots & \ldots & 0 \\ -1 & 2 & -1 & \ldots & \vdots & \vdots \\ 0 & -1 & 2 & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & & -1 & 0 \\ \vdots & \vdots & \vdots & -1 & 2 & -1 \\ 0 & \ldots & \ldots & 0 & -1 & 1 \end{pmatrix}. \tag{1}$$

Furthermore, $TGT^t = I_n$, where

$$T = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & 1 & \ldots & 1 \\ 0 & 0 & 1 & \ldots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}, \tag{2}$$

T^t denotes the transpose of the matrix T and I_n is the identity matrix of order n.

Proposition 3.1. *[4] If $\mathcal{I} \subseteq \mathcal{O}_\mathbb{K}$ is a nonzero free $\mathbb{Z}$-module of rank n, then* $\det(\sigma_\alpha(\mathcal{I})) = N_\mathbb{K}(\mathcal{I})^2 N_{\mathbb{K}/\mathbb{Q}}(\alpha) D_\mathbb{K}$.

From now on, let $\mathbb{K} \subseteq \mathbb{L} = \mathbb{Q}(\zeta_p)$ be a totally real number field. From Proposition 3.1, a necessary condition for constructing a rotated unimodular lattice scaled by $\sqrt{c}$, with $c \in \mathbb{Z}$, via a free $\mathbb{Z}$-module $\mathcal{I} \subseteq \mathcal{O}_\mathbb{K}$, is the existence of an element α such that $\sigma(\alpha) \geq 0$ for all $\sigma \in Gal(\mathbb{K}/\mathbb{Q})$ and

$$c^n = N_{\mathbb{K}/\mathbb{Q}}(\alpha)\, N_\mathbb{K}(\mathcal{I})^2\, D_\mathbb{K}. \tag{3}$$

Taking $\mathcal{I} = \mathcal{O}_\mathbb{K}$ and $c = p$, a necessary condition for constructing a rotated unimodular lattice $\frac{1}{\sqrt{c}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ is the existence of a totally positive element $\alpha \in \mathcal{O}_\mathbb{K}$ such that $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = p$. In the following proposition, we present an element α such that $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = p$.

Proposition 3.2. *If $\alpha = N_{\mathbb{L}/\mathbb{K}}(1-\zeta_p)$, then $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = p$.*

Proof. The p-th cyclotomic polynomial is $\Phi_p(x) = 1+x+x^2+\cdots+x^{p-1} = (x-\zeta_p)(x-\zeta_p^2)\cdots(x-\zeta_p^{p-1})$. Hence, $N_{\mathbb{L}/\mathbb{Q}}(1-\zeta_p) = \prod_{i=1}^{p-1}(1-\zeta_p^i) = \Phi_p(1) = p$. Finally,

$$p = N_{\mathbb{L}/\mathbb{Q}}(1-\zeta_p) = N_{\mathbb{K}/\mathbb{Q}}\big(N_{\mathbb{L}/\mathbb{K}}(1-\zeta_p)\big) = N_{\mathbb{K}/\mathbb{Q}}(\alpha),$$

which proves the result. □

Since $\mathbb{K}$ is totally real, it follows that m is even, and the complex conjugation lies in $Gal(\mathbb{L}/\mathbb{K})$. In the next result, we show that the lattice $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ is in fact unimodular.

Proposition 3.3. *Let $[\mathbb{K} : \mathbb{Q}] = n$ and $Gal(\mathbb{L}/\mathbb{Q}) = \langle\sigma_r\rangle$ for some $r \in \mathbb{N}$. If α is defined as in Proposition 3.2, then the lattice $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ is a rotated unimodular lattice.*

Proof. Let $\theta = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_p)$. From Proposition 2.1, a $\mathbb{Z}$-basis of $\mathcal{O}_{\mathbb{K}}$ is given by $\{\sigma_r(\theta), \ldots, \sigma_{r^n}(\theta)\}$. A Gram matrix associated with $\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ is $G = (g_{ij})_{i,j=1}^n$, where

$$g_{ij} = Tr_{\mathbb{K}/\mathbb{Q}}\big(\alpha\, \sigma_{r^i}(\theta)\, \sigma_{r^j}(\theta)\big) = \sum_{k=1}^{n} \sigma_{r^k}\big(\alpha\, \sigma_{r^i}(\theta)\, \sigma_{r^j}(\theta)\big).$$

From Proposition 3.2, $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = p$. Therefore, $\alpha\mathcal{O}_{\mathbb{K}}$ is a prime ideal of $\mathcal{O}_{\mathbb{K}}$. Furthermore, $\alpha\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$. Hence, $p\mathcal{O}_{\mathbb{K}} = (\alpha\mathcal{O}_{\mathbb{K}})^n$. Since $\sigma_{r^k}(\alpha\mathcal{O}_{\mathbb{K}})$ lies over $p\mathcal{O}_{\mathbb{K}}$ for all $k = 1, \ldots, n$, it follows that $\sigma_{r^k}(\alpha\mathcal{O}_{\mathbb{K}}) = \alpha\mathcal{O}_{\mathbb{K}}$. Hence,

$$Tr_{\mathbb{K}/\mathbb{Q}}\big(\alpha\, \sigma_{r^i}(\theta)\, \sigma_{r^j}(\theta)\big) \in \alpha\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z} \quad \text{and} \quad \frac{1}{p}\, Tr_{\mathbb{K}/\mathbb{Q}}\big(\alpha\, \sigma_{r^i}(\theta)\, \sigma_{r^j}(\theta)\big) \in \mathbb{Z}.$$

Since $\det\big(\sigma_\alpha(\mathcal{O}_{\mathbb{K}})\big) = p^n$, it follows that $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ is a unimodular lattice. □

Proposition 3.4. *If $\alpha = N_{\mathbb{L}/\mathbb{K}}(1 - \zeta_p)$, then $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha) = p$.*

Proof. Using properties of the trace and [3], we obtain

$$p = Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_p) = Tr_{\mathbb{K}/\mathbb{Q}}\big(Tr_{\mathbb{L}/\mathbb{K}}(\zeta_p)\big) = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha),$$

which proves the result. □

Corollary 3.5. *The lattice $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ is an odd unimodular lattice with minimum Euclidean norm 1.*

Proof. Since $1 \in \mathcal{O}_{\mathbb{K}}$, it follows that $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha)$ corresponds to the squared Euclidean norm of the vector $\sigma_\alpha(1)$. □

Remark 3.6. *In some special cases, we can characterize these lattices without using Gram matrices. It is known that the only odd unimodular lattices in dimensions $n \leq 8$ are rotated $\mathbb{Z}^n$-lattices [8]. Therefore, if $[\mathbb{K} : \mathbb{Q}] \leq 8$, then the unimodular lattices in Proposition 3.3 are rotated $\mathbb{Z}^n$-lattices.*

According to Remark 3.6, the unimodular lattices obtained up to dimension 8 are rotated $\mathbb{Z}^n$-lattices. In the following examples, we present constructions of odd unimodular lattices in specific dimensions, using the LLL lattice basis reduction algorithm [12] in *Mathematica* to find a change-of-basis matrix. In what follows, we set $e_i = \zeta_p^i + \zeta_p^{-i}$ for all $i = 1, 2, \ldots, p-1$.

Example 3.7. *Let $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{73})$ be a totally real number field with $[\mathbb{K} : \mathbb{Q}] = 9$ and $Gal(\mathbb{Q}(\zeta_{73})/\mathbb{Q}) = \langle\sigma_5\rangle$. We have $\mathbb{K} = \mathbb{Q}(\theta)$, where $\theta = e_1 + e_{10} + e_{22} + e_{27}$, and let $\alpha = (2 - e_1)(2 - e_{10})(2 - e_{22})(2 - e_{27})$. A Gram matrix G for $\frac{1}{\sqrt{73}}\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$, associated with the $\mathbb{Z}$-basis $\{e_5 + e_{23} + e_{36} + e_{11},\ e_{25} + e_{31} + e_{34} + e_{18}, e_{21} + e_9 + e_{24} + e_{17}, e_{32} + e_{28} + e_{26} + e_{12}, e_{14} + e_6 + e_{16} + e_{13}, e_3 + e_{30} + e_7 + e_8, e_{15} + e_4 + e_{35} + e_{33}, e_2 + e_{20} + e_{29} + e_{19}, e_{10} + e_{27} + e_1 + e_{22}\}$ of $\mathcal{O}_{\mathbb{K}}$, is given by*

$$\begin{pmatrix}
36 & -9 & 14 & -19 & -20 & 6 & 0 & 2 & -2 \\
-9 & 10 & 5 & -3 & 1 & 2 & 0 & -10 & 2 \\
14 & 5 & 24 & -18 & -16 & 9 & 1 & -15 & -2 \\
-19 & -3 & -18 & 20 & 15 & -8 & 0 & 10 & -1 \\
-20 & 1 & -16 & 15 & 16 & -6 & 0 & 5 & 1 \\
6 & 2 & 9 & -8 & -6 & 4 & 0 & -6 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & -1 \\
2 & -10 & -15 & 10 & 5 & -6 & -1 & 16 & 0 \\
-2 & 2 & -2 & -1 & 1 & 0 & -1 & 0 & 3
\end{pmatrix}$$

Considering the change-of-basis matrix

$$T = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & -1 & -1 & 0 & -1 & -2 & -1 & -2 & 0 \\ 1 & 1 & 2 & 1 & 2 & 0 & 0 & 1 & 1 \\ 0 & -1 & 0 & 0 & 0 & -1 & 0 & -1 & 1 \\ 2 & 2 & 3 & 2 & 3 & 1 & 1 & 2 & 2 \\ -1 & -2 & -1 & -2 & -1 & -4 & -2 & -2 & -1 \\ -3 & -5 & -5 & -4 & -5 & -6 & -4 & -6 & -3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 4 & 6 & 4 & 5 & 3 & 3 & 5 & 4 \end{pmatrix}$$

we have $TGT^t = I_9$. *Therefore, the lattice* $\frac{1}{\sqrt{73}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ *is a rotated* $\mathbb{Z}^9$*-lattice.*

Example 3.8. *Let* $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{41})$ *be a totally real number field with* $[\mathbb{K} : \mathbb{Q}] = 10$ *and* $Gal(\mathbb{Q}(\zeta_{41})/\mathbb{Q}) = \langle\sigma_6\rangle$. *Thus* $\mathbb{K} = \mathbb{Q}(\theta)$, *where* $\theta = e_1 + e_9$, *and let* $\alpha = (2 - e_1)(2 - e_9)$. *A Gram matrix* G *for* $\frac{1}{\sqrt{41}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$, *associated with the* $\mathbb{Z}$*-basis* $\{e_6 + e_{13}, e_5 + e_4, e_{11} + e_{17}, e_{16} + e_{20}, e_{14} + e_3, e_2 + e_{18}, e_{12} + e_{15}, e_{10} + e_8, e_{19} + e_7, e_9 + e_1\}$ *of* $\mathcal{O}_\mathbb{K}$, *is given by*

$$\begin{pmatrix} 4 & -1 & 0 & 1 & -1 & 1 & -2 & 0 & -2 & 0 \\ -1 & 1 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 4 & -1 & 1 & -2 & -2 & -2 & 1 & 1 \\ 1 & 0 & -1 & 2 & 0 & 0 & -1 & 1 & -2 & 0 \\ -1 & -1 & 1 & 0 & 4 & -2 & -2 & 0 & 1 & 0 \\ 1 & 0 & -2 & 0 & -2 & 4 & 1 & 2 & -2 & -2 \\ -2 & 1 & -2 & -1 & -2 & 1 & 4 & 0 & 1 & 0 \\ 0 & 0 & -2 & 1 & 0 & 2 & 0 & 4 & -2 & -4 \\ -2 & 0 & 1 & -2 & 1 & -2 & 1 & -2 & 4 & 1 \\ 0 & 0 & 1 & 0 & 0 & -2 & 0 & -4 & 1 & 6 \end{pmatrix}.$$

Consider the change-of-basis matrix

$$T = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 2 & 1 & 1 & 1 & 0 & 1 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & -1 & 0 \\ 0 & 1 & -1 & -2 & 0 & -1 & -1 & 0 & -1 & 0 \\ 2 & 1 & 2 & 2 & 1 & 1 & 2 & 2 & 2 & 1 \\ -2 & -1 & -3 & -4 & -2 & -2 & -3 & -2 & -3 & -1 \\ 2 & 1 & 3 & 3 & 2 & 2 & 3 & 2 & 2 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{pmatrix}$$

so that $TGT^t = I_{10}$. *Therefore, the lattice* $\frac{1}{\sqrt{41}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ *is a rotated* $\mathbb{Z}^{10}$*-lattice.*

Since $\mathcal{O}_\mathbb{K}$ is a principal ideal and $D_\mathbb{K} = p^{n-1}$, from [3] it follows that the minimum product distance of $\Lambda = \frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ is given by

$$d_{p,\min}(\Lambda) = \frac{1}{\sqrt{D_\mathbb{K}}} = \frac{1}{p^{\frac{n-1}{2}}}.$$

Thus, for a fixed dimension n, the greatest minimum product distance is obtained when p is the smallest prime such that n divides $(p-1)/2$.

The family of full diversity rotated unimodular lattices obtained in Proposition 3.3 has the same packing density as $\mathbb{Z}^n$, which is $\Delta\left(\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})\right) = \frac{\rho^n \operatorname{vol}(B(1))}{(\det\Lambda)^{1/2}} = \frac{\operatorname{vol}(B(1))}{2^n}$. However, the fact that the

lattices $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ are unimodular and have the same packing density as $\mathbb{Z}^n$ is not sufficient to guarantee that they are rotated $\mathbb{Z}^n$-lattices. In [3], the authors showed that for $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $\alpha = 2 - e_1$, the lattices $\frac{1}{\sqrt{p}}\sigma_\alpha(\mathcal{O}_\mathbb{K})$ are indeed rotated $\mathbb{Z}^{\frac{p-1}{2}}$-lattices. In our more general setting, we do not observe a pattern in the Gram matrices obtained using the $\mathbb{Z}$-basis of $\mathcal{O}_\mathbb{K}$ from Proposition 2.1, as illustrated in Examples 3.7 and 3.8.

4. Conclusion

Lattices have been studied in various areas, particularly in information theory and cryptography [7, 13]. In [1, 2, 6, 11], the authors presented families of full diversity rotated $\mathbb{Z}^n$-lattices based on algebraic number theory. Based on these constructions, a technique was introduced to construct families of full diversity rotated unimodular lattices via subfields $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p+\zeta_p^{-1})$, where p is an odd prime. These lattices are geometric images of the ring of integers of $\mathbb{K}$. Performance in terms of minimum product distance is given by an explicit formula in terms of the discriminant. Furthermore, based on Examples 3.7 and 3.8, we believe that the unimodular lattices in Proposition 3.3 are rotated $\mathbb{Z}^n$-lattices for all $n \in \mathbb{N}^*$, which remains an open problem; in particular, one needs to find a suitable $\mathbb{Z}$-basis for $\mathcal{O}_\mathbb{K}$ with respect to which the Gram matrix is the identity.

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(3) (2010) 1–13.

[2] A. A. Andrade, C. Alves and T. B. Carlos, Rotated lattices via the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$. Int. J. Appl. Math. 19(3) (2006) 321–331.

[3] E. Bayer-Fluckiger, F. Oggier and E. Viterbo, New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel, IEEE Transactions on Information Theory 50(4) (2004) 702–714.

[4] E. Bayer-Fluckiger, Lattices and number fields, Contemp. Math. 241 (1999) 69–84.

[5] E. Bayer-Fluckiger, Ideal lattices, Proceedings of the Conference Number Theory and Diophantine Geometry, Zurich 1999 Cambridge Univ. Press (2002) 168–184.

[6] E. Bayer-Fluckiger, F. Oggier and E. Viterbo. Algebraic lattice constellations: bounds on performance, IEEE Transactions on Information Theory 52(1) (2006) 319–327.

[7] J. Boutros, E. Viterbo, C. Rastello and J-C. Belfiore, Good lattice constellations for both Rayleigh fading and Gaussian channels, IEEE Transactions on Information Theory 42(2) (1996) 502–517.

[8] J. H. Conway and N.J.A. Sloane, Sphere packings, lattices and groups, New York Springer-Verlag (1988).

[9] A. J. Ferrari, A. A. Andrade, R. R. Araujo and J. C. Interlando, Trace forms of certain subfields of cyclotomic fields and applications, Journal of Algebra Combinatorics Discrete Structures and Applications 7(2) (2020) 141–160.

[10] A. J. Ferrari, G. C. Jorge and A. A. Andrade, Rotated D_n-lattices in dimensions power of 3, Journal of Algebra Combinatorics Discrete Structures and Applications 8(3) (2021) 151–160.

[11] A. J. Ferrari, A. A. Andrade, J. C. Interlando and C. A. Severo, Characterization of Totally Real Subfields of 2-Power Cyclotomic Fields and Applications to Signal Set Design, Journal of Algebra Combinatorics Discrete Structures and Applications 11(2) (2024) 73–81.

[12] A. K. Lenstra, H.W. Lenstra and L. Lovasz, Factoring polynomials with rational coefficients, Mathematische Annalen 261 (1982) 515–534.

[13] D. Micciancio and O. Regev, Lattice-based Cryptography, In: Bernstein, D.J., Buchmann, J., Dah-

men, E. (eds) Post-Quantum Cryptography, Springer Berlin Heidelberg (2009).
[14] E. L. Oliveira, Lattice constructions via odd degree cyclic extensions, Master Degree, Ibilce - Unesp, São José do Rio Preto - SP 2011 (in portuguese).
[15] P. Samuel. Algebraic theory of numbers, Paris Hermann 1970.