

Trace forms of certain subfields of cyclotomic fields and applications*

Research Article

Agnaldo José Ferrari, Antonio Aparecido de Andrade, Robson Ricardo de Araujo, José Carmelo Interlando

Abstract: In this work, we present a explicit trace forms for maximal real subfields of cyclotomic fields as tools for constructing algebraic lattices in Euclidean space with optimal center density. We also obtain a closed formula for the Gram matrix of algebraic lattices obtained from these subfields. The obtained lattices are rotated versions of the lattices Λ_9, Λ_{10} and Λ_{11} and they are images of \mathbb{Z} -submodules of rings of integers under the twisted homomorphism, and these constructions, as algebraic lattices, are new in the literature. We also obtain algebraic lattices in odd dimensions up to 7 over real subfields, calculate their minimum product distance and compare with those known in literatura, since lattices constructed over real subfields have full diversity.

2010 MSC: 11H06, 11H31, 11R80, 97N70

Keywords: Cyclotomic fields, Algebraic lattices, Twisted homomorphism, Signal design

1. Introduction

Lattices have been considered in different areas, especially in coding theory and more recently in cryptography. Algebraic lattices are lattices obtained via the ring of integers of a number field and they have been studied in several papers and from different points of view [1–7, 10–13, 15, 16, 18].

* This work was supported by Fapesp 2013/25977-7 and CNPq 429346/2018-2.

Agnaldo José Ferrari; Department of Mathematics, School of Sciences, São Paulo State University (Unesp), Bauru-SP, Brazil (email: agnaldo.ferrari@unesp.br).

Antonio Aparecido de Andrade (Corresponding Author); Department of Mathematics, Institute of Biosciences, Humanities and Exact Sciences (Ibilce), São Paulo State University (Unesp), São José do Rio Preto-SP, Brazil (email: antonio.andrade@unesp.br).

Robson Ricardo de Araujo; São Paulo Federal Institute at Cubatão, São Paulo, Brazil (email: dearaujorobison-ricardo@gmail.com).

José Carmelo Interlando; Department of Mathematics & Statistics, San Diego University, San Diego, California, USA (email: interlan@sdsu.edu).

The classical sphere packing problem is to determine how densely a large number of identical spheres can be packed together in the Euclidean space. The packing density of a lattice Λ is the proportion of the space covered by the non-overlapping spheres of maximum radius centered at the points of Λ . The densest known lattice packings in dimensions 1 through 8 and 24 are also the optimal ones, see [12, p. 12] for $n = 1, 2, \dots, 8$, and [11] for $n = 24$. Those lattice packings are unique. For all other dimensions, it is not known whether the current records are optimal.

A lattice Λ has diversity equal to k if k is the maximum number such that any non-zero vector $y \in \Lambda$ has at least k non-zero coordinates. Given an n -dimensional lattice $\Lambda \subseteq \mathbb{R}^n$ of full diversity, the minimum product distance of Λ is defined as $d_{p,min}(\Lambda) = \min\{\prod_{i=1}^n |y_i|; y = (y_1, y_2, \dots, y_n) \in \Lambda, y \neq 0\}$. Usually the problem of finding good signal constellations for a Gaussian channel is associated with the search for lattices with high packing density, see [12, Chapter 3]. On the other hand, for a Rayleigh fading channel, the efficiency of the signal constellation, measured by the error probability in the transmission, is strongly related to the lattice diversity and its minimum product distance, see [10, Section III]. For this purpose the lattice parameters we consider here are packing density, diversity, and minimum product distance.

The approach in this work, following [2, 3] is the use of algebraic number theory to construct lattices which have good performance on both channels. For general lattices the packing density and the minimum product distance are usually hard to estimate [17]. Those parameters can be calculated in certain cases of lattices associated to number fields through algebraic properties. In [4–6] some families of rotated \mathbb{Z}^n -lattices of full diversity and high minimum product distance are studied for transmission over Rayleigh fading channels. In [13] some families of rotated \mathbb{Z}^n -lattices of full diversity in dimensions power of 3 are studied and lower bounds for the minimum product distances of such construction are also presented. In [7] the lattices A_{p-1} , p prime, E_6 , E_8 , K_{12} and Λ_{24} were realized as full diversity ideal lattices via some subfields of cyclotomic fields. In this work we construct the lattices D_3 , E_5 , E_7 , Λ_9 , Λ_{10} and Λ_{11} , calculate (or estimate) their minimum product distance and compare the obtained values with those known in literature, mainly \mathbb{Z}^n -lattices given in [5, 18].

In [14, Theorem 1] a trace form for cyclotomic fields $\mathbb{Q}(\zeta_n)$ via the Minkowski homomorphism is derived. In this work, we generalize the result for the maximal real subfields $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ via the twisted homomorphism. In [6, Proposition 4.1(a)] and [8] the Gram matrix of the algebraic lattice constructed via the Minkowski homomorphism over $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is determined, but in this work we use a different approach. In this work, we generalize the result to the case $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ considering the twisted homomorphism. Trace forms are used to calculate the packing radius of algebraic lattices. As an application, we present constructions of algebraic lattices with optimal center density in dimensions 3, 5, 7, 9, 10 and 11.

The paper is organized as follows. In Sections 2, we collect some results on number fields and algebraic lattices. In Section 3, we present a explicit trace form for the maximal real subfields via the twisted homomorphism. We also present a closed formula of Gram matrix for the lattice $\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$, where $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. In Section 4, we construct algebraic lattices in Euclidean space with optimal center density in dimensions 3, 5, 7, 9, 10 and 11 and calculate (estimate) their minimum product distance. Finally, in Section 5, we draw our conclusions.

2. Background on number fields and algebraic lattices

If \mathbb{L} is a number field of degree n , that is, a field that is a finite degree extension of \mathbb{Q} , then $\mathbb{L} = \mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{C}$ is a root of a monic irreducible polynomial $p(x) \in \mathbb{Z}[x]$. The n distinct roots of $p(x)$, namely, $\alpha_1, \alpha_2, \dots, \alpha_n$, are the conjugates of α . If $\sigma : \mathbb{L} \rightarrow \mathbb{C}$ is a \mathbb{Q} -homomorphism, then $\sigma(\alpha) = \alpha_i$ for some $i = 1, 2, \dots, n$. Furthermore, there are exactly n \mathbb{Q} -homomorphisms σ_i , for $i = 1, 2, \dots, n$, of \mathbb{L} in \mathbb{C} , where r_1 are real monomorphisms and $2r_2$ are complex monomorphisms with $n = r_1 + 2r_2$.

An element $\alpha \in \mathbb{L}$ is called an algebraic integer if there is a monic polynomial $f(x)$ with integer coefficients such that $f(\alpha) = 0$. The set

$$\mathcal{O}_{\mathbb{L}} = \{\alpha \in \mathbb{L} : \alpha \text{ is an algebraic integer}\}$$

is a ring, called *ring of algebraic integers* of \mathbb{L} [20, 21]. It can be shown that $\mathcal{O}_{\mathbb{L}}$, as a \mathbb{Z} -module, has a basis $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ over \mathbb{Z} , called *integral basis*, where n is the degree of \mathbb{L} . In other words, every element $\alpha \in \mathcal{O}_{\mathbb{L}}$ can be uniquely written as

$$\alpha = \sum_{i=1}^n a_i \alpha_i,$$

where $a_i \in \mathbb{Z}$ for all $i = 1, 2, \dots, n$.

The *trace* and the *norm* of an element $\alpha \in \mathbb{L}$ over \mathbb{Q} are defined as the rational numbers

$$Tr_{\mathbb{L}/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha) \text{ and } N_{\mathbb{L}/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha).$$

If $\alpha \in \mathcal{O}_{\mathbb{L}}$, then $Tr_{\mathbb{L}/\mathbb{Q}}(\alpha)$ and $N_{\mathbb{L}/\mathbb{Q}}(\alpha)$ are algebraic integers. The *discriminant* of \mathbb{L} over \mathbb{Q} is defined by

$$d_{\mathbb{L}} = d(\alpha_1, \alpha_2, \dots, \alpha_n) = \det_{1 \leq i, j \leq n} (\sigma_i(\alpha_j))^2,$$

where $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is an integral basis of \mathbb{L} .

A lattice Λ is a discrete additive subgroup of \mathbb{R}^n considered as the standard real vector space, that is, $\Lambda \subseteq \mathbb{R}^n$ is a lattice if there are linearly independent vectors $\alpha_1, \alpha_2, \dots, \alpha_m \in \mathbb{R}^n$ such that

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

The classical sphere packing problem is to find out how densely a large number of identical spheres can be packed together in the Euclidean space. The *packing density*, $\Delta(\Lambda)$, of a lattice Λ is the proportion of the space \mathbb{R}^n covered by the non-overlapping spheres of maximum radius centered at the points of Λ . The densest possible lattice packings have only be determined in dimensions 1 to 8 and 24 [12, p. 12]. It is also known that these densest lattice packings are unique.

Let $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ be a set of linearly independent vectors in \mathbb{R}^n and $\Lambda = \{\sum_{i=1}^m a_i \alpha_i; a_i \in \mathbb{Z}\}$ a lattice. The set $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ is called a *basis* for Λ . A matrix M whose rows are these vectors is said to be a *generator matrix* for Λ whereas $G = MM^t = ((\alpha_i, \alpha_j))_{i,j=1}^m$ is called the *Gram matrix* of Λ . The *determinant* of Λ , denoted by $\det \Lambda$, is equal to $\det G$ and it is an invariant under change of basis. The *volume* of Λ is equal to $\sqrt{\det(\Lambda)}$. The *packing density* of Λ is the proportion occupied by the spheres centered in the points of the lattice and having radius $\min\{\|x - y\|; x, y \in \Lambda, x \neq y\}/2$ relative to the entire space \mathbb{R}^n . If $\Delta(\Lambda)$ is the packing density of Λ , then $\delta(\Lambda) = \Delta(\Lambda)/V_n$ is the *center density* of the lattice, where V_n is the volume of an n -dimensional sphere of radius 1 [12, p. 9].

Let $\alpha \in \mathbb{L}$ such that $\alpha_i = \sigma_i(\alpha) > 0$ for all $i = 1, \dots, n$. If $\Re(x)$ and $\Im(x)$ denote, respectively, the real part and the imaginary part of x , the homomorphism $\sigma_{\alpha} : \mathbb{L} \rightarrow \mathbb{R}^n$ defined by

$$\sigma_{\alpha}(x) = (\sqrt{\alpha_1} \sigma_1(x), \dots, \sqrt{\alpha_{r_1}} \sigma_{r_1}(x), \dots, \sqrt{\alpha_{r_1+r_2}} \Re(\sigma_{r_1+r_2}(x)), \sqrt{\alpha_{r_1+r_2}} \Im(\sigma_{r_1+r_2}(x))),$$

for every $x \in \mathbb{L}$, is called *twisted homomorphism* [2, 3]. When $\alpha = 1$ the twisted homomorphism is the *Minkowski homomorphism*. If \mathcal{M} is a \mathbb{Z} -module in \mathbb{L} of rank n with \mathbb{Z} -basis $\{w_1, w_2, \dots, w_n\}$, then the set $\Lambda = \sigma_{\alpha}(\mathcal{M})$ is a complete lattice in \mathbb{R}^n with basis $\{\sigma_{\alpha}(w_1), \sigma_{\alpha}(w_2), \dots, \sigma_{\alpha}(w_n)\}$. If \mathbb{L} is a totally real number field then $G = (Tr_{\mathbb{L}/\mathbb{Q}}(\alpha w_i w_j))_{i,j=1}^n$ is a Gram matrix for $\sigma_{\alpha}(\mathcal{M})$. From [2], $\det(\Lambda) = [\mathcal{O}_{\mathbb{K}} : \mathcal{M}]^2 N_{\mathbb{L}/\mathbb{Q}}(\alpha) |d_{\mathbb{L}}|$, so the center density of Λ is given by

$$\delta(\Lambda) = \frac{\rho^n}{\sqrt{\det(\Lambda)}} = \frac{t^{n/2}}{2^n [\mathcal{O}_{\mathbb{L}} : \mathcal{M}] \sqrt{N_{\mathbb{L}/\mathbb{Q}}(\alpha) |d_{\mathbb{L}}|}},$$

where $d_{\mathbb{L}}$ denotes the discriminant of the number field \mathbb{L} , $[\mathcal{O}_{\mathbb{L}} : \mathcal{M}]$ denotes the index of \mathcal{M} and

$$t = \min \{Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x^2) : x \in \mathcal{M}, x \neq 0\}.$$

If \mathcal{M} is a \mathbb{Z} -module in \mathbb{L} of rank m , $m < n$, with \mathbb{Z} -basis $\{w_1, w_2, \dots, w_m\}$, then the set $\Lambda = \sigma_{\alpha}(\mathcal{M})$ is a lattice of rank m in \mathbb{R}^n with basis $\{\sigma_{\alpha}(w_1), \sigma_{\alpha}(w_2), \dots, \sigma_{\alpha}(w_m)\}$ and $Q = (Tr_{\mathbb{L}/\mathbb{Q}}(\alpha w_i w_j))_{i,j=1}^m$ is a Gram matrix for $\sigma_{\alpha}(\mathcal{M})$. The center density of Λ is given by

$$\delta(\Lambda) = \begin{cases} \frac{t^{m/2}}{2^m \sqrt{\det(Q)}}, & \text{if } \mathbb{L} \text{ is totally real.} \\ \frac{t^{m/2}}{2^{3m/2} \sqrt{\det(Q)}}, & \text{if } \mathbb{L} \text{ is totally complex.} \end{cases} \tag{1}$$

If \mathbb{K} is a totally real field number with $[\mathbb{K} : \mathbb{Q}] = n$ and $\mathcal{M} \subseteq \mathbb{K}$ a free \mathbb{Z} -module of rank n , then the minimum product distance of $\Lambda = \sigma_{\alpha}(\mathcal{M})$ is defined as

$$d_{p,min}(\Lambda) = \sqrt{N_{\mathbb{K}/\mathbb{Q}}(\alpha)} \min_{0 \neq y \in \mathcal{M}} |N_{\mathbb{K}/\mathbb{Q}}(y)|. \tag{2}$$

In particular, by [5], if $\mathcal{M} \subseteq \mathbb{K}$ is a principal ideal then

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{|d_{\mathbb{K}}|}}. \tag{3}$$

The relative minimum product distance of Λ , denoted by $d_{p,rel}(\Lambda)$, is the minimum product distance of a scaled version of Λ with unitary minimum norm vector. Thus, if Λ_1 is a scaled version of Λ of dimension n with scale factor \sqrt{k} , i. e., $\Lambda_1 = \sqrt{k}\Lambda$ and the minimum norm of Λ is μ , then the relative minimum product distance of Λ_1 is given by

$$d_{p,rel}(\Lambda_1) = \left(\frac{1}{\sqrt{k}\mu}\right)^n d_{p,min}(\Lambda_1). \tag{4}$$

3. Trace forms for cyclotomic fields

In this section, we present explicit trace forms for maximal real subfield $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ via twisted homomorphism. We also present a closed formula of Gram matrix for the lattice $\sigma_{\alpha}(\mathcal{O}_{\mathbb{K}})$. A related result, through a different approach, can be found in [6] and [8], where the authors use abelian fields of odd prime power conductor.

A cyclotomic field is a number field \mathbb{L} such that $\mathbb{L} = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n -th root of unity. It can be shown that $[\mathbb{L} : \mathbb{Q}] = \varphi(n)$, where φ is the Euler function, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_n]$ is the ring of algebraic integers of $\mathbb{Z}[\zeta_n]$, $\{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{\varphi(n)-1}\}$ is an integral basis of \mathbb{L} . Let $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ be the maximal real subfield of a cyclotomic field $\mathbb{Q}(\zeta_n)$. In this case, $[\mathbb{K} : \mathbb{Q}] = \varphi(n)/2$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ and $\{1, \zeta_n + \zeta_n^{-1}, \zeta_n^2 + \zeta_n^{-2}, \dots, \zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{-\frac{\varphi(n)}{2}+1}\}$ is an integral basis of $\mathcal{O}_{\mathbb{K}}$. [21].

Lemma 3.1. [14] Let j, n be integers. If $\gcd(j, n) = d$, then

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) = \frac{\varphi(n)}{\varphi(n/d)} Tr_{\mathbb{Q}(\zeta_{n/d})/\mathbb{Q}}(\zeta_{n/d}^{j/d}).$$

Lemma 3.2. [14] If j, a_i are integers, $a_i \geq 1$ and p_i is a prime number such that $\gcd(j, p_i^{a_i}) = 1$, then

$$Tr_{\mathbb{Q}(\zeta_{p_i^{a_i}})/\mathbb{Q}}(\zeta_{p_i^{a_i}}^j) = \begin{cases} -1, & \text{if } a_i = 1. \\ 0, & \text{if } a_i > 1. \end{cases}$$

Lemma 3.3. [14] Let $n = p_1^{a_1} \cdots p_s^{a_s}$, where $a_k \geq 1$, for $k = 1, \dots, s$. If j is a prime number and $\gcd(j, n) = d$, then

$$\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) = \frac{\varphi(n)}{\varphi(n/d)} \mu(n/d),$$

where μ is the Moebius function.

Lemma 3.4. Let $n = p_1^{a_1} \cdots p_s^{a_s}$, where $a_j \geq 1$, for $j = 1, \dots, s$. If i is an integer such that $i < \varphi(n)$ and $d = \gcd(i, n)$, then

$$\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) \neq 0 \Leftrightarrow d = (n/P)t_k \text{ and } i = (n/P)k,$$

where $P = p_1 \cdots p_s$, $t_k = \gcd(k, P)$ and $k = 0, 1, 2, \dots, \varphi(P) - 1$.

Proof. If $d = (n/P)t_k$, where $t_k = \gcd(k, P)$, then the values that t_k can assume are 1 and $p_{\alpha_1} \cdots p_{\alpha_t}$, where $1 \leq \alpha_r \leq s$, for $r = 1, 2, \dots, t$ and $\alpha_r \neq \alpha_l$ if $r \neq l$ and $1 \leq t < s$. So, $d = p_1^{a_1-1} \cdots p_s^{a_s-1}$ or $d = p_1^{a_1-1} \cdots p_{\alpha_1}^{a_{\alpha_1}} \cdots p_{\alpha_t}^{a_{\alpha_t}} \cdots p_s^{a_s-1}$. Thus, $n/d = p_1 \cdots p_s$ or $n/d = p_1 \cdots p_{\alpha_1-1} p_{\alpha_1+1} \cdots p_{\alpha_t-1} p_{\alpha_t+1} \cdots p_s$, and therefore, $\mu(n/d) = \pm 1 \neq 0$. But, from Lemma 3.3, it follows that

$$\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) = \frac{\varphi(n)}{\varphi(n/d)} \mu(n/d) \neq 0.$$

Now, if $i = (n/P)k$, then $\gcd(i, n) = d$, for $k = 0, 1, 2, \dots, \varphi(P) - 1$. In fact, if $\gcd(i, n) = d'$, then $\gcd((n/P)k, n) = d'$. Thus, $\gcd(((n/P)k)/(n/P)n/(n/P)) = d'/(n/P)$, that is, $t_k = \gcd(k, P) = (P/n)d'$. So, $d' = (n/P)t_k = d$ and $k = 0, 1, 2, \dots, \varphi(P) - 1$. From the Euler function, it follows that

$$\begin{aligned} \frac{\varphi(n)}{\varphi(P)} &= \frac{\varphi(p_1^{a_1} \cdots p_s^{a_s})}{\varphi(p_1 \cdots p_s)} = \frac{\varphi(p_1^{a_1}) \cdots \varphi(p_s^{a_s})}{\varphi(p_1) \cdots \varphi(p_s)} = \frac{[p_1^{a_1-1}(p_1-1)] \cdots [p_s^{a_s-1}(p_s-1)]}{(p_1-1) \cdots (p_s-1)} \\ &= p_1^{a_1-1} \cdots p_s^{a_s-1} = \frac{n}{P}. \end{aligned}$$

Thus, if $k \geq \varphi(P)$, then $i = (n/P)k = ((\varphi(n))/(\varphi(P)))k \geq ((\varphi(n))/(\varphi(P)))\varphi(P) = \varphi(n)$, which is a contradiction. Therefore, $k = 0, 1, 2, \dots, \varphi(P) - 1$. Furthermore, $d = (n/P)t_k$ if and only if $i = (n/P)k$. Reciprocally, suppose that $\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) \neq 0$ com $d \neq (n/P)t_k$. Thus, n/d is not square free. So, from definition of Euler function, it follows that $\mu(n/d) = 0$, and therefore, $\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) = 0$, which is a contradiction. \square

Lemma 3.5. Let $n = p_1^{a_1} \cdots p_s^{a_s}$, where $a_r \geq 1$, for $r = 1, \dots, s$. If i and j are integers such that $i, j < \varphi(n)$ and $d = \gcd(i - j, n)$, then

$$\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{i-j}) \neq 0 \Leftrightarrow d = (n/P)t_k \text{ and } |i - j| = (n/P)k,$$

where $P = p_1 \cdots p_s$, $t_k = \gcd(k, P)$ and $k = 0, 1, 2, \dots, \varphi(P) - 1$.

Proof. It is enough to observe that $\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{i-j}) = \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{j-i})$, $\gcd(i - j, n) = \gcd(j - i, n)$ and as $i, j < \varphi(n)$ then $|i - j| < \varphi(n)$. Therefore, by Lemma 3.4, it follow the result. \square

Lemma 3.6. Let $n = p_1^{a_1} \cdots p_s^{a_s}$, where $a_r \geq 1$, for $r = 1, \dots, s$. If i and j are integers such that $i, j < \varphi(n)$ and $d = \gcd(i + j, n)$, then

$$\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{i+j}) \neq 0 \Leftrightarrow d = (n/P)t_k \text{ and } i + j = (n/P)k,$$

where $P = p_1 \cdots p_s$, $t_k = \gcd(k, P)$ and $k = 0, 1, \dots, 2\varphi(P) - 2$ if $n = P$ and $k = 0, 1, \dots, 2\varphi(P) - 1$, otherwise.

Proof. For $n = P$, if $k \geq 2\varphi(P) - 1$, then $i + j = (n/P)k = k \geq 2\varphi(P) - 1 = 2\varphi(n) - 1$, which is a contradiction, since $i, j \leq \varphi(n) - 1$ implies $i + j \leq 2\varphi(n) - 2$. Thus, $k = 0, 1, \dots, 2\varphi(P) - 2$. For $n > P$, if $k \leq 2\varphi(P) - 1$, then $i + j = (n/P)k \leq (\varphi(n)/\varphi(P))(2\varphi(P) - 1) = 2\varphi(n) - (n/P) < 2\varphi(n) - 1$. So, $i + j \leq 2\varphi(n) - 2$. If $k \geq 2\varphi(P)$, then $i + j = (n/P)k \geq (\varphi(n)/\varphi(P))2\varphi(P) = 2\varphi(n)$, which is a contradiction, since $i + j \leq 2\varphi(n) - 2$. Therefore, $k = 0, 1, \dots, 2\varphi(P) - 1$. \square

Lemma 3.7. Let $n = p_1^{a_1} \cdots p_s^{a_s}$, where $a_r \geq 1$, for $r = 1, 2, \dots, s$. If i and j are integers such $i, j \leq \varphi(n)/2 - 1$ and $d = \gcd(i + 2j, n)$, then

$$\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{i+2j}) \neq 0 \Leftrightarrow d = (n/P)t_k \text{ and } i + 2j = (n/P)k,$$

where $P = p_1 \cdots p_s$, $t_k = \gcd(k, P)$ and $k = 0, 1, \dots, \lfloor 3\varphi(P)/2 - 3P/n \rfloor$, where $\lfloor y \rfloor$ is the greater integer less than or equal to y .

Proof. If $k > 3\varphi(P)/2 - 3P/n$, then $i + 2j = (n/P)k > (n/P)(3\varphi(P)/2 - 3P/n) = 3\varphi(n)/2 - 3$, which is a contradiction, since $i, j \leq \varphi(n)/2 - 1$ implies $i + 2j \leq 3\varphi(n)/2 - 3$. Thus, $k = 0, 1, \dots, \lfloor 3\varphi(P)/2 - 3P/n \rfloor$. \square

Lemma 3.8. Let $n = p_1^{a_1} \cdots p_s^{a_s}$, where $a_r \geq 1$, for $r = 1, 2, \dots, s$. If i and j are integers such $i, j \leq \varphi(n)/2 - 1$ and $d = \gcd(-i + 2j, n)$, then

$$\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{-i+2j}) \neq 0 \Leftrightarrow d = (n/P)t_k \text{ and } |-i + 2j| = (n/P)k,$$

where $P = p_1 \cdots p_s$, $t_k = \gcd(k, P)$ and $k = 0, 1, 2, \dots, \lfloor \varphi(P) - 3P/n \rfloor$.

Proof. It is enough to observe that $\text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{-i+2j}) = \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{i-2j})$, $\gcd(-i + 2j, n) = \gcd(i - 2j, n)$. If $k > \varphi(P) - 3P/n$, then $|-i + 2j| = (n/P)k > (n/P)(\varphi(P) - 3P/n) = \varphi(n) - 3$, which is a contradiction, since $i, j \leq \varphi(n)/2 - 1$ implies $|-i + 2j| \leq \varphi(n) - 3$. Thus, $k = 0, 1, \dots, \lfloor \varphi(P) - 3P/n \rfloor$. \square

Proposition 3.9. Let $\mathbb{L} = \mathbb{Q}(\zeta_n)$ and $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ be its maximal real subfield, where $n = p_1^{a_1} \cdots p_s^{a_s}$, with $a_j \geq 1$, for $j = 1, 2, \dots, s$, $m = \varphi(n)$. Let $\alpha = \alpha_0 + \alpha_1(\zeta_n + \zeta_n^{-1}) + \alpha_2(\zeta_n^2 + \zeta_n^{-2}) + \cdots + \alpha_{m/2-1}(\zeta_n^{m/2-1} + \zeta_n^{-m/2+1})$ be a totally positive element of $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, i. e., $\sigma_i(\alpha) > 0$, for all $i = 1, 2, \dots, m/2$, where σ_i are the $m/2$ distinct \mathbb{Q} -homomorphisms from \mathbb{K} to \mathbb{C} . If $x = a_0 + a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \cdots +$

$a_{\frac{m}{2}-1}(\zeta_n^{m/2-1} + \zeta_n^{-m/2+1})$ is an element of $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, then

$$\begin{aligned}
 \text{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha x^2) = & \frac{n}{P} \left(\frac{\varphi(P)}{2} \alpha_0 a_0^2 + \alpha_0 \sum_{\substack{k=l_1 \\ \frac{n}{P} k: \text{even}}}^{u_1} a_{\frac{n}{P}k}^2 \rho(t_k) + 2\alpha_0 a_0 \sum_{k=l_2}^{u_2} a_{\frac{n}{P}k} \rho(t_k) + 2\alpha_0 \sum_{k=l_3}^{u_3} B_{\frac{n}{P}k} \rho(t_k) \right. \\
 & + \varphi(P) \alpha_0 \sum_{j=1}^{m/2-1} a_j^2 + 2\alpha_0 \sum_{k=l_2}^{u_4} A_{\frac{n}{P}k} \rho(t_k) + a_0^2 \sum_{k=l_2}^{u_2} \alpha_{\frac{n}{P}k} \rho(t_k) + \sum_{\substack{n \neq i+2j = \frac{n}{P}k \\ l_3 \leq k \leq u_5 \\ 1 \leq i \leq \frac{m}{2}-1 \\ 1 \leq j \leq \frac{m}{2}-1}} \alpha_i a_j^2 \rho(t_k) \\
 & + \varphi(P) \sum_{\substack{2 \\ 1 \leq i+2j=n \\ 1 \leq i \leq \frac{m}{2}-1 \\ 1 \leq j \leq \frac{m}{2}-1}} \alpha_i a_j^2 + \sum_{\substack{0 \leq |-i+2j| = \frac{n}{P}k \\ 0 \leq k \leq u_3 \\ 1 \leq i \leq m/2-1 \\ 1 \leq j \leq m/2-1}} \alpha_i a_j^2 \rho(t_k) + 2a_0 \sum_{\substack{i+j = \frac{n}{P}k \\ l_1 \leq k \leq u_1 \\ 1 \leq i \leq m/2-1 \\ 1 \leq j \leq m/2-1}} \alpha_i a_j \rho(t_k) \\
 & + 2a_0 \sum_{\substack{0 \leq |i-j| = \frac{n}{P}k \\ 0 \leq k \leq u_4 \\ 1 \leq i \leq m/2-1 \\ 1 \leq j \leq m/2-1}} \alpha_i a_j \rho(t_k) + 2 \sum_{\substack{n \neq i+j = \frac{n}{P}k \\ l_4 \leq k \leq u_7 \\ 1 \leq i \leq m/2-1 \\ 3 \leq j \leq m-3}} \alpha_i B_j \rho(t_k) + 2\varphi(P) \sum_{\substack{i+j=n \\ 1 \leq i \leq m/2-1 \\ 3 \leq j \leq m-3}} \alpha_i B_j \\
 & + 2 \sum_{\substack{0 \leq |i-j| = \frac{n}{P}k \\ 0 \leq k \leq u_8 \\ 1 \leq i \leq m/2-1 \\ 3 \leq j \leq m-3}} \alpha_i B_j \rho(t_k) + 2 \sum_{k=l_2}^{u_2} \sum_{j=1}^{m/2-1} \alpha_{\frac{n}{P}k} a_j^2 \rho(t_k) + 2 \sum_{\substack{i+j = \frac{n}{P}k \\ l_1 \leq k \leq u_3 \\ 1 \leq i \leq m/2-1 \\ 1 \leq j \leq \frac{m}{2}-2}} \alpha_i A_j \rho(t_k) \\
 & \left. + 2 \sum_{\substack{0 \leq |i-j| = \frac{n}{P}k \\ 0 \leq k \leq u_4 \\ 1 \leq i \leq m/2-1 \\ 1 \leq j \leq \frac{m}{2}-2}} \alpha_i A_j \rho(t_k) \right).
 \end{aligned}$$

where $P = p_1 \cdots p_s$, $t_k = \gcd(k, P)$, $\lceil y \rceil$ is the smaller integer greater than or equal to y , $\lfloor y \rfloor$ is the greater integer less than or equal to y , $l_1 = \lceil 2P/n \rceil$, $l_2 = \lceil P/n \rceil$, $l_3 = \lceil 3P/n \rceil$, $l_4 = \lceil 4P/n \rceil$, $u_1 = \lfloor \varphi(P) - 2P/n \rfloor$, $u_2 = \lfloor \varphi(P)/2 - P/n \rfloor$, $u_3 = \lfloor \varphi(P) - 3P/n \rfloor$, $u_4 = \lfloor \varphi(P)/2 - 2P/n \rfloor$, $u_5 = \lfloor 3\varphi(P)/2 - 3P/n \rfloor$, $u_6 = \lfloor (m-2)/4 \rfloor$, $u_7 = \lfloor 3\varphi(P)/2 - 4P/n \rfloor$, $u_8 = \lfloor \varphi(P) - 4P/n \rfloor$, $\rho(t_k) = \mu(\frac{P}{t_k})\varphi(t_k)$ with μ the Mobius function and φ the Euler function, $A_j = a_1 a_{j+1} + a_2 a_{j+2} + \cdots + a_{\frac{m}{2}-1-j} a_{m/2-1}$, $B_j = \sum_{\substack{k \geq 1 \\ k < j - k \leq m/2-1}} a_k a_{j-k}$,

and any sum of the trace form must be disregarded if the lower bound of k is greater than the upper bound.

Proof. Let $x = a_0 + a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \cdots + a_{m/2-1}(\zeta_n^{m/2-1} + \zeta_n^{-m/2+1})$ be an element of $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, with $a_i \in \mathbb{Z}$, for $i = 0, 1, 2, \dots, m/2 - 1$. Thus,

$$\begin{aligned}
 x^2 &= (a_0 + a_1 \zeta_n + a_1 \zeta_n^{-1} + \cdots + a_{m/2-1} \zeta_n^{m/2-1} + a_{m/2-1} \zeta_n^{-m/2+1})^2 = \left(\sum_{j=0}^{m/2-1} a_j \zeta_n^j + \sum_{j=1}^{m/2-1} a_j \zeta_n^{-j} \right)^2 \\
 &= \left(\sum_{j=0}^{m/2-1} a_j \zeta_n^j \right)^2 + \left(\sum_{j=1}^{m/2-1} a_j \zeta_n^{-j} \right)^2 + 2 \left(\sum_{j=0}^{m/2-1} a_j \zeta_n^j \right) \left(\sum_{j=1}^{m/2-1} a_j \zeta_n^{-j} \right) = \\
 &= \sum_{j=0}^{m/2-1} a_j^2 \zeta_n^{2j} + 2 \sum_{0 \leq i < j \leq m/2-1} a_i a_j \zeta_n^{i+j} + \sum_{j=1}^{m/2-1} a_j^2 \zeta_n^{-2j} + 2 \sum_{1 \leq i < j \leq m/2-1} a_i a_j \zeta_n^{-i-j}
 \end{aligned}$$

$$\begin{aligned}
 &+ 2 \left(\sum_{j=0}^{m/2-1} a_j \zeta_n^j \right) \left(\sum_{j=1}^{m/2-1} a_j \zeta_n^{-j} \right) = \\
 = &a_0^2 + \sum_{j=1}^{m/2-1} a_j^2 (\zeta_n^{2j} + \zeta_n^{-2j}) + 2 \sum_{j=1}^{m/2-1} a_0 a_j (\zeta_n^j + \zeta_n^{-j}) + 2 \sum_{j=3}^{m-3} B_j (\zeta_n^j + \zeta_n^{-j}) + 2 \sum_{j=1}^{m/2-1} a_j^2 \\
 &+ 2 \sum_{j=1}^{m/2-2} A_j (\zeta_n^j + \zeta_n^{-j}),
 \end{aligned}$$

where $A_j = a_1 a_{j+1} + a_2 a_{j+2} + \dots + a_{m/2-1-j} a_{m/2-1}$ and $B_j = \sum_{\substack{k \geq 1 \\ k < j - k \leq m/2-1}} a_k a_{j-k}$. Now, let $\alpha = \alpha_0 + \alpha_1(\zeta_n + \zeta_n^{-1}) + \alpha_2(\zeta_n^2 + \zeta_n^{-2}) + \dots + \alpha_{m/2-1}(\zeta_n^{m/2-1} + \zeta_n^{-m/2+1})$ be a totally positive element of $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, with $\alpha_i \in \mathbb{Z}$, for $i = 0, 1, 2, \dots, m/2 - 1$. Thus,

$$\begin{aligned}
 \alpha x^2 &= \left(\alpha_0 + \sum_{i=1}^{m/2-1} \alpha_i (\zeta_n^i + \zeta_n^{-i}) \right) \left(a_0^2 + \sum_{j=1}^{m/2-1} a_j^2 (\zeta_n^{2j} + \zeta_n^{-2j}) + 2 \sum_{j=1}^{m/2-1} a_0 a_j (\zeta_n^j + \zeta_n^{-j}) \right. \\
 &\quad \left. + 2 \sum_{j=3}^{m-3} B_j (\zeta_n^j + \zeta_n^{-j}) + 2 \sum_{j=1}^{m/2-1} a_j^2 + 2 \sum_{j=1}^{m/2-2} A_j (\zeta_n^j + \zeta_n^{-j}) \right) = \\
 = &\alpha_0 a_0^2 + \alpha_0 \sum_{j=1}^{m/2-1} a_j^2 (\zeta_n^{2j} + \zeta_n^{-2j}) + 2\alpha_0 a_0 \sum_{j=1}^{m/2-1} a_j (\zeta_n^j + \zeta_n^{-j}) + 2\alpha_0 \sum_{j=3}^{m-3} B_j (\zeta_n^j + \zeta_n^{-j}) \\
 &+ 2\alpha_0 \sum_{j=1}^{m/2-1} a_j^2 + 2\alpha_0 \sum_{j=1}^{m/2-2} A_j (\zeta_n^j + \zeta_n^{-j}) + a_0^2 \sum_{i=1}^{m/2-1} \alpha_i (\zeta_n^i + \zeta_n^{-i}) \\
 &+ \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j^2 (\zeta_n^{i+2j} + \zeta_n^{-i-2j}) + \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j^2 (\zeta_n^{-i+2j} + \zeta_n^{i-2j}) \\
 &+ 2a_0 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j (\zeta_n^{i+j} + \zeta_n^{-i-j}) + 2a_0 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j (\zeta_n^{i-j} + \zeta_n^{-i+j}) \\
 &+ 2 \sum_{i=1}^{m/2-1} \sum_{j=3}^{m-3} \alpha_i B_j (\zeta_n^{i+j} + \zeta_n^{-i-j}) + 2 \sum_{i=1}^{m/2-1} \sum_{j=3}^{m-3} \alpha_i B_j (\zeta_n^{i-j} + \zeta_n^{-i+j}) \\
 &+ 2 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j^2 (\zeta_n^i + \zeta_n^{-i}) + 2 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-2} \alpha_i A_j (\zeta_n^{i+j} + \zeta_n^{-i-j}) \\
 &+ 2 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-2} \alpha_i A_j (\zeta_n^{i-j} + \zeta_n^{-i+j}).
 \end{aligned}$$

Since ζ_n^k and ζ_n^{-k} are conjugates, it follows that they have the same trace, i. e., $Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^k + \zeta_n^{-k}) = 2Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^k)$ and as $Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x^2) = [\mathbb{L} : \mathbb{K}] Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x^2)$, it follows that

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x^2) = \frac{1}{2} Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x^2).$$

Thus,

$$\begin{aligned}
 \text{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha x^2) &= \frac{1}{2} \text{Tr}_{\mathbb{L}/\mathbb{Q}} \left(\alpha_0 a_0^2 + \alpha_0 \sum_{j=1}^{m/2-1} a_j^2 (\zeta_n^{2j} + \zeta_n^{-2j}) + 2\alpha_0 a_0 \sum_{j=1}^{m/2-1} a_j (\zeta_n^j + \zeta_n^{-j}) \right. \\
 &\quad + 2\alpha_0 \sum_{j=3}^{m-3} B_j (\zeta_n^j + \zeta_n^{-j}) + 2\alpha_0 \sum_{j=1}^{m/2-1} a_j^2 + 2\alpha_0 \sum_{j=1}^{m/2-2} A_j (\zeta_n^j + \zeta_n^{-j}) \\
 &\quad + a_0^2 \sum_{i=1}^{m/2-1} \alpha_i (\zeta_n^i + \zeta_n^{-i}) + \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j^2 (\zeta_n^{i+2j} + \zeta_n^{-i-2j}) \\
 &\quad + \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j^2 (\zeta_n^{-i+2j} + \zeta_n^{i-2j}) + 2a_0 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j (\zeta_n^{i+j} + \zeta_n^{-i-j}) \\
 &\quad + 2a_0 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j (\zeta_n^{i-j} + \zeta_n^{-i+j}) + 2 \sum_{i=1}^{m/2-1} \sum_{j=3}^{m-3} \alpha_i B_j (\zeta_n^{i+j} + \zeta_n^{-i-j}) \\
 &\quad + 2 \sum_{i=1}^{m/2-1} \sum_{j=3}^{m-3} \alpha_i B_j (\zeta_n^{i-j} + \zeta_n^{-i+j}) + 2 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j^2 (\zeta_n^i + \zeta_n^{-i}) \\
 &\quad \left. + 2 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-2} \alpha_i A_j (\zeta_n^{i+j} + \zeta_n^{-i-j}) + 2 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-2} \alpha_i A_j (\zeta_n^{i-j} + \zeta_n^{-i+j}) \right) \\
 &= \frac{m}{2} \alpha_0 a_0^2 + \alpha_0 \sum_{j=1}^{m/2-1} a_j^2 \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{2j}) + 2\alpha_0 a_0 \sum_{j=1}^{m/2-1} a_j \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^j) \\
 &\quad + 2\alpha_0 \sum_{j=3}^{m-3} B_j \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^j) + m\alpha_0 \sum_{j=1}^{m/2-1} a_j^2 + 2\alpha_0 \sum_{j=1}^{m/2-2} A_j \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^j) \\
 &\quad + a_0^2 \sum_{j=1}^{m/2-1} \alpha_j \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^j) + \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j^2 \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i+2j}) \\
 &\quad + \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j^2 \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{-i+2j}) + 2a_0 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i+j}) \\
 &\quad + 2a_0 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i-j}) + 2 \sum_{i=1}^{m/2-1} \sum_{j=3}^{m-3} \alpha_i B_j \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i+j}) \\
 &\quad + 2 \sum_{i=1}^{m/2-1} \sum_{j=3}^{m-3} \alpha_i B_j \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i-j}) + 2 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j^2 \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^i) \\
 &\quad + 2 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-2} \alpha_i A_j \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i+j}) + 2 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-2} \alpha_i A_j \text{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i-j}).
 \end{aligned}$$

From Lemmas 3.3 to 3.8, it follows that

$$\begin{aligned}
 \sum_{j=1}^{m/2-1} a_j^2 Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{2j}) &= \sum_{\substack{k=l_1 \\ \frac{P}{2}k:\text{even}}}^{u_1} a_{\frac{n}{2}k}^2 \rho(t_k), \quad \sum_{j=1}^{m/2-1} a_j Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^j) = \sum_{k=l_2}^{u_2} a_{\frac{n}{2}k} \rho(t_k), \\
 \sum_{j=3}^{m-3} B_j Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^j) &= \sum_{k=l_3}^{u_3} B_{\frac{n}{2}k} \rho(t_k), \quad \sum_{j=1}^{m/2-2} A_j Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^j) = \sum_{k=l_2}^{u_4} A_{\frac{n}{2}k} \rho(t_k), \\
 \sum_{j=1}^{m/2-1} \alpha_j Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^j) &= \sum_{k=l_2}^{u_2} \alpha_{\frac{n}{2}k} \rho(t_k), \\
 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j^2 Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i+2j}) &= \sum_{\substack{n \neq i+2j = \frac{n}{2}k \\ l_3 \leq k \leq u_5 \\ 1 \leq i \leq m/2-1 \\ 1 \leq j \leq m/2-1}} \sum_{i=1}^2 \sum_{j=1}^2 \alpha_i a_j^2 \rho(t_k) + \sum_{\substack{i+2j=n \\ 1 \leq i \leq m/2-1 \\ 1 \leq j \leq m/2-1}} \sum_{i=1}^2 \sum_{j=1}^2 \alpha_i a_j^2, \\
 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j^2 Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{-i+2j}) &= \sum_{\substack{0 \leq |-i+2j| = \frac{n}{2}k \\ 0 \leq k \leq u_3 \\ 1 \leq i \leq m/2-1 \\ 1 \leq j \leq m/2-1}} \alpha_i a_j^2 \rho(t_k), \\
 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i+j}) &= \sum_{\substack{i+j = \frac{n}{2}k \\ l_1 \leq k \leq u_1 \\ 1 \leq i \leq m/2-1 \\ 1 \leq j \leq m/2-1}} \alpha_i a_j \rho(t_k), \\
 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i-j}) &= \sum_{\substack{0 \leq |i-j| = \frac{n}{2}k \\ 0 \leq k \leq u_4 \\ 1 \leq i \leq m/2-1 \\ 1 \leq j \leq m/2-1}} \alpha_i a_j \rho(t_k), \\
 \sum_{i=1}^{m/2-1} \sum_{j=3}^{m-3} \alpha_i B_j Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i+j}) &= \sum_{\substack{n \neq i+j = \frac{n}{2}k \\ l_4 \leq k \leq u_7 \\ 1 \leq i \leq m/2-1 \\ 3 \leq j \leq m-3}} \sum_{i=1}^2 \alpha_i B_j \rho(t_k) + \varphi(P) \sum_{\substack{i+j=n \\ 1 \leq i \leq m/2-1 \\ 3 \leq j \leq m-3}} \sum_{i=1}^2 \alpha_i B_j, \\
 \sum_{i=1}^{m/2-1} \sum_{j=3}^{m-3} \alpha_i B_j Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i-j}) &= \sum_{\substack{0 \leq |i-j| = \frac{n}{2}k \\ 0 \leq k \leq u_8 \\ 1 \leq i \leq m/2-1 \\ 3 \leq j \leq m-3}} \alpha_i B_j \rho(t_k), \\
 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-1} \alpha_i a_j^2 Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^i) &= \sum_{k=l_2}^{u_2} \sum_{j=1}^{m/2-1} \alpha_{\frac{n}{2}k} a_j^2 \rho(t_k), \\
 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-2} \alpha_i A_j Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i+j}) &= \sum_{\substack{i+j = \frac{n}{2}k \\ l_1 \leq k \leq u_3 \\ 1 \leq i \leq m/2-1 \\ 1 \leq j \leq \frac{m}{2}-2}} \sum_{i=1}^2 \alpha_i A_j \rho(t_k), \\
 \sum_{i=1}^{m/2-1} \sum_{j=1}^{m/2-2} \alpha_i A_j Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^{i-j}) &= \sum_{\substack{0 \leq |i-j| = \frac{n}{2}k \\ 0 \leq k \leq u_4 \\ 1 \leq i \leq m/2-1 \\ 1 \leq j \leq \frac{m}{2}-2}} \alpha_i A_j \rho(t_k),
 \end{aligned}$$

where $l_1 = \lceil \frac{2P}{n} \rceil$, $l_2 = \lceil \frac{P}{n} \rceil$, $l_3 = \lceil \frac{3P}{n} \rceil$, $l_4 = \lceil \frac{4P}{n} \rceil$, $u_1 = \lfloor \varphi(P) - \frac{2P}{n} \rfloor$, $u_2 = \lfloor \frac{\varphi(P)}{2} - \frac{P}{n} \rfloor$,

$u_3 = \lfloor \varphi(P) - \frac{3P}{n} \rfloor$, $u_4 = \lfloor \frac{\varphi(P)}{2} - \frac{2P}{n} \rfloor$, $u_5 = \lfloor \frac{3\varphi(P)}{2} - \frac{3P}{n} \rfloor$, $u_6 = \lfloor \frac{m-2}{4} \rfloor$, $u_7 = \lfloor \frac{3\varphi(P)}{2} - \frac{4P}{n} \rfloor$, $u_8 = \lfloor \varphi(P) - \frac{4P}{n} \rfloor$, $\rho(t_k) = \mu(\frac{P}{t_k})\varphi(t_k)$ with μ the Mobius function and φ the Euler function. Therefore, the result follows. \square

As a corollary of the last theorem, we present an explicit Gram matrix of a lattice via the maximal real subfield of $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, when the \mathbb{Z} -module is the ring $\mathcal{O}_{\mathbb{K}}$.

Corollary 3.10. *Let be $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, $e_0 = 1$ and $e_j = \zeta_n^j + \zeta_n^{-j}$ for $j = 1, 2, \dots, m/2 - 1$, where $n = p_1^{a_1} \dots p_s^{a_s}$, $m = \varphi(n)$ and $\alpha = \alpha_0 + \alpha_1(\zeta_n + \zeta_n^{-1}) + \alpha_2(\zeta_n^2 + \zeta_n^{-2}) + \dots + \alpha_{m/2-1}(\zeta_n^{m/2-1} + \zeta_n^{-m/2+1})$ is a totally positive element of $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, i. e., $\sigma_i(\alpha) > 0$, for all $i = 1, 2, \dots, m/2$, where σ_i are the $m/2$ distinct \mathbb{Q} -homomorphisms from \mathbb{K} to \mathbb{C} . A Gram matrix for the lattice $\Lambda = \sigma_{\alpha}(\mathcal{O}_{\mathbb{K}})$ is given by $G = (Tr_{\mathbb{K}/\mathbb{Q}}(\alpha e_i e_j))_{i,j=0}^{m/2-1}$, where*

$$(a) \quad Tr_{\mathbb{K}/\mathbb{Q}}(\alpha e_0 e_0) = \frac{m\alpha_0}{2} + \frac{n}{P} \sum_{k=l_1}^{u_1} \alpha_{\frac{nk}{P}} \rho(t_k),$$

(b) For $j \geq 1$,

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha e_0 e_j) = \frac{\varphi(n)}{\varphi(n/d_1)} \mu(n/d_1) \alpha_0 + \frac{n}{P} \sum_{\substack{r+j=\frac{nk}{P} \\ l_2 \leq k \leq u_2 \\ 1 \leq r \leq m/2-1}} \alpha_r \rho(t_k) + \frac{n}{P} \sum_{\substack{|r-j|=\frac{nk}{P} \\ 0 \leq k \leq u_3 \\ 1 \leq r \leq m/2-1}} \alpha_r \rho(t_k),$$

(c) For $i, j \geq 1$,

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha e_i e_j) = \frac{\varphi(n)}{\varphi(n/d_2)} \mu(n/d_2) \alpha_0 + \frac{\varphi(n)}{\varphi(n/d_3)} \mu(n/d_3) \alpha_0 + \frac{n}{P} \sum_{\substack{r+i+j=\frac{nk}{P} \\ l_3 \leq k \leq u_4 \\ 1 \leq r \leq m/2-1}} \alpha_r \rho(t_k) \\ + \frac{n}{P} \sum_{\substack{|r-(i+j)|=\frac{nk}{P} \\ 0 \leq k \leq u_5 \\ 1 \leq r \leq m/2-1}} \alpha_r \rho(t_k) + \frac{n}{P} \sum_{\substack{|r+(i-j)|=\frac{nk}{P} \\ 0 \leq k \leq u_5 \\ 1 \leq r \leq m/2-1}} \alpha_r \rho(t_k) + \frac{n}{P} \sum_{\substack{|r+(j-i)|=\frac{nk}{P} \\ 0 \leq k \leq u_5 \\ 1 \leq r \leq m/2-1}} \alpha_r \rho(t_k),$$

where $P = p_1 \dots p_s$, $t_k = \gcd(k, P)$, $\lceil y \rceil$ is the smaller integer greater than or equal to y , $\lfloor y \rfloor$ is the greater integer less than or equal to y , $l_1 = \lceil P/n \rceil$, $l_2 = \lceil 2P/n \rceil$, $l_3 = \lceil 3P/n \rceil$, $u_1 = \lfloor \varphi(P)/2 - P/n \rfloor$, $u_2 = \lfloor \varphi(P) - 2P/n \rfloor$, $u_3 = \lfloor \varphi(P)/2 \rfloor$, $u_4 = \lfloor 3\varphi(P)/2 - 3P/n \rfloor$, $u_5 = \lfloor \varphi(P) - 3P/n \rfloor$, $d_1 = \gcd(j, n)$, $d_2 = \gcd(i + j, n)$, $d_3 = \gcd(i - j, n)$, $\rho(t_k) = \mu(\frac{P}{t_k})\varphi(t_k)$ with μ the Mobius function and φ the Euler function, and any sum must be disregarded if the lower bound of k is greater than the upper bound.

Proof. From Lemmas 3 to 6 and following the same steps of the proof of the Proposition 3.9, the result follows. \square

The next proposition, stated and proved in [19, Corollary 2.3], will be used in the next section. Before recalling it, we need a few assumptions. Let \mathbb{L}/\mathbb{Q} be a Galois extension of prime degree p such that p is unramified in $\mathcal{O}_{\mathbb{L}}$, the ring of integers of \mathbb{L} . Denote the conductor of \mathbb{L} by n , that is, n is the smallest positive integer such that $\mathbb{L} \subseteq \mathbb{Q}(\zeta_n)$. Then $\{\sigma^{(i)}(\theta)\}_{i=0}^{p-1}$ is an integral basis for \mathbb{L} where $\theta = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{L}}(\zeta_n)$ and σ is any generator of $\text{Gal}(\mathbb{L}/\mathbb{Q})$.

Proposition 3.11. *Let $x = \sum_{i=0}^{p-1} a_i \sigma^{(i)}(\theta)$ be any element in $\mathcal{O}_{\mathbb{L}}$. Then*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x^2) = n \sum_{i=0}^{p-1} a_i^2 - \frac{n-1}{p} \left(\sum_{i=0}^{p-1} a_i \right)^2.$$

4. Constructions of algebraic lattices

In this section, we construct algebraic lattices in Euclidean space with optimal center density in dimensions 9, 10 and 11 which are rotated versions of the lattices Λ_9, Λ_{10} and Λ_{11} via twisted embeddings applied to \mathbb{Z} -modules of the ring of integers of a number field \mathbb{K} . We believe these constructions, as algebraic lattices, are new in the literature. Constructions of rotated D_3, D_5 and E_7 -lattices via ideals and free \mathbb{Z} -modules that are not ideals are also presented. The same lattices are also constructed in [15, 16], through a different approach, where the authors construct these lattices by shifting ideal lattices constructed over cyclotomic fields via ideal or module in the maximal totally real subfields of cyclotomic fields.

4.1. Construction of the D_3 -lattice

If $\mathbb{K} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, then $[\mathbb{K} : \mathbb{Q}] = 3$ and $d_{\mathbb{K}} = 3^4$. If $\alpha = 1$, then α is a totally positive element of $\mathbb{Z}[\zeta_9 + \zeta_9^{-1}]$ and $N(\alpha) = 1$. If \mathcal{M} is a submodule of $\mathcal{O}_{\mathbb{K}}$ generated by $\{2 + e_1 + e_2, -e_1 + e_2, 2 - e_2\}$, where $e_j = \zeta_9^j + \zeta_9^{-j}$, for $j = 1, 2$, then \mathcal{M} is a submodule of $\mathcal{O}_{\mathbb{K}}$ of index 6 and

$$\delta(\sigma_{\alpha}(\mathcal{M})) = \frac{t^{n/2}}{2^n [\mathcal{O}_{\mathbb{L}} : \mathcal{M}] \sqrt{N(\alpha) |d_{\mathbb{K}}|}} = \frac{18^{3/2}}{2^3 6 \sqrt{|3^4|}} = \frac{1}{4\sqrt{2}},$$

i.e., with the same center density of the lattice D_3 . The norm equation $|N_{\mathbb{K}/\mathbb{Q}}(y)| = 2$ has no solution in $\mathcal{O}_{\mathbb{K}}$ [9], however $|N_{\mathbb{K}/\mathbb{Q}}(y)| = 3$ when $y = 2 - e_2 \in \mathcal{M}$. Thus, $\min_{0 \neq y \in \mathcal{M}} |N_{\mathbb{K}/\mathbb{Q}}(y)| = 3$. and the minimum norm in D_3 is $\mu = 2$. As $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = 1$ and $\sigma_{\alpha}(\mathcal{M})$ is a scaled version of D_3 with scale factor $\sqrt{9}$, from Equation (4), it follows that

$$d_{p,rel}(\sigma_{\alpha}(\mathcal{M})) = \left(\frac{1}{\sqrt{18}}\right)^3 \sqrt{1} \times 3 = 0.03928,$$

and therefore,

$$\sqrt[3]{d_{p,rel}(\sigma_{\alpha}(\mathcal{M}))} = 0.33994.$$

4.2. Construction of the D_5 -lattice

If $\mathbb{K} = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$, then $[\mathbb{K} : \mathbb{Q}] = 5$ and $d_{\mathbb{K}} = 11^4$. If $\alpha = 2 - e_1$, where $e_1 = \zeta_{11} + \zeta_{11}^{-1}$, then α is a totally positive element of $\mathbb{Z}[\zeta_{11} + \zeta_{11}^{-1}]$ and $N(\alpha) = 11$. If \mathcal{M} is a submodule of $\mathcal{O}_{\mathbb{K}}$ generated by $\{2 + e_1, -e_1, -e_2, -e_3, -e_4\}$, where $e_j = \zeta_{11}^j + \zeta_{11}^{-j}$, for $j = 1, 2, 3, 4$, then $\sigma_{\alpha}(\mathcal{M})$ is a lattice of rank 5 and

$$\delta(\sigma_{\alpha}(\mathcal{M})) = \frac{t^{n/2}}{2^n [\mathcal{O}_{\mathbb{L}} : \mathcal{M}] \sqrt{N(\alpha) |d_{\mathbb{K}}|}} = \frac{22^{5/2}}{2^6 \sqrt{11^5}} = \frac{1}{8\sqrt{2}},$$

i.e., with the same center density of the lattice D_5 . In this case, $\min_{0 \neq y \in \mathcal{M}} |N_{\mathbb{K}/\mathbb{Q}}(y)| = 1$, because $N_{\mathbb{K}/\mathbb{Q}}(y) = 1$, where $y = 2 + e_1 \in \mathcal{M}$. The minimum norm in D_5 is $\mu = 2$. As $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = 11$ and $\sigma_{\alpha}(\mathcal{M})$ is a scaled version of D_5 with scale factor $\sqrt{11}$, by Equation (4), it follows that

$$d_{p,rel}(\sigma_{\alpha}(\mathcal{M})) = \left(\frac{1}{\sqrt{22}}\right)^5 \sqrt{11} \cdot 1 = 0.00146,$$

and therefore,

$$\sqrt[5]{d_{p,rel}(\sigma_\alpha(\mathcal{M}))} = 0.27097.$$

4.3. Construction of the E_7 -lattice

If \mathbb{K} is a subfield of $\mathbb{L} = \mathbb{Q}(\zeta_{29})$ such that $[\mathbb{K} : \mathbb{Q}] = 7$ and $\langle \sigma \rangle = Gal(\mathbb{K}/\mathbb{Q})$, where $\sigma : \zeta_{29} \mapsto \zeta_{29}^7$, then $\mathbb{K} = \mathbb{Q}(\theta)$, where

$$\theta = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_{29}) = \zeta_{29} + \zeta_{29}^{-1} + \zeta_{29}^{12} + \zeta_{29}^{-12}.$$

If

$$\begin{aligned} \alpha &= N_{\mathbb{L}/\mathbb{K}}(1 - \zeta_{29}) = \prod_{i \in \{1, -1, 12, -12\}} (1 - \zeta_{29}^i) = \\ &= -(6\theta + 4\sigma(\theta) + 4\sigma^2(\theta) + 4\sigma^3(\theta) + 4\sigma^4(\theta) + 3\sigma^5(\theta) + 4\sigma^6(\theta)), \end{aligned}$$

then

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha) = N_{\mathbb{K}/\mathbb{Q}}(\alpha) = 29.$$

If

$$\mathcal{M} = \{a_0\theta + a_1\sigma(\theta) + \dots + a_6\sigma^6(\theta) \in \mathcal{O}_{\mathbb{K}}; a_j \equiv 0 \pmod{2}, \text{ for } j = 0, 1, 2, 4\},$$

then \mathcal{M} is a \mathbb{Z} -submodule of $\mathcal{O}_{\mathbb{K}}$ and \mathcal{M} is not an ideal of $\mathcal{O}_{\mathbb{K}}$, because for $x = \sigma(\theta) \in \mathcal{O}_{\mathbb{K}}$ and $y = \sigma^3(\theta) \in \mathcal{M}$ it follows that $xy = -3\theta - 2\sigma(\theta) - 4\sigma^2(\theta) - 2\sigma^3(\theta) - 3\sigma^4(\theta) - 3\sigma^5(\theta) - 4\sigma^6(\theta) \notin \mathcal{M}$. Since $d_{\mathbb{K}} = 29^6$, it follows that

$$\delta(\sigma_\alpha(\mathcal{M})) = \frac{t^{n/2}}{2^n [\mathcal{O}_{\mathbb{K}} : \mathcal{M}] \sqrt{N(\alpha) |d_{\mathbb{K}}|}} = \frac{(2^2 \cdot 29)^{7/2}}{2^7 \cdot 16 \sqrt{29} |29^6|} = \frac{1}{16},$$

i.e., with the same center density of the lattice E_7 . As E_7 is the only lattice with such center density in \mathbb{R}^7 , it follows that $\sigma_\alpha(\mathcal{M})$ is a rotated version of E_7 . In this case, $\min_{0 \neq y \in \mathcal{M}} |N_{\mathbb{K}/\mathbb{Q}}(y)| = 1$, since for $y = -2\theta - 2\sigma^2(\theta) + \sigma^3(\theta) - \sigma^6(\theta) \in \mathcal{M}$, $N_{\mathbb{K}/\mathbb{Q}}(y) = 1$. Now, the minimum norm in E_7 is $\mu = 2$. As $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = 29$ and $\sigma_\alpha(\mathcal{M})$ is a scaled version of E_7 with scale factor $\sqrt{58}$, by Equation (4), it follows that

$$d_{p,rel}(\sigma_\alpha(\mathcal{M})) = \left(\frac{1}{\sqrt{116}}\right)^7 \sqrt{29} \cdot 1 = 3.203 \times 10^{-7},$$

and consequently,

$$\sqrt[7]{d_{p,rel}(\sigma_\alpha(\mathcal{M}))} = 0.11809.$$

4.4. Construction of the Λ_9 and Λ_{10} -lattice

Let \mathbb{K} be a number field such that $\mathbb{K} = \mathbb{Q}(\zeta_{180} + \zeta_{180}^{-1})$. In this case, $[\mathbb{K} : \mathbb{Q}] = 24$, taking $e_0 = 1$ and $e_j = \zeta_{180}^j + \zeta_{180}^{-j}$, for $j = 1, 2, \dots, 23$, we have that $\{1, e_1, e_2, \dots, e_{22}, e_{23}\}$ is a basis of \mathbb{K} . Let $\alpha = 165 + 129e_2 + 153e_4 + 120e_6 + 119e_8 + 105e_{10} + 67e_{12} + 82e_{14} + 25e_{16} + 49e_{18} + 3e_{20} + 17e_{22}$ be a

totally positive element of $\mathbb{Z}[\zeta_{180} + \zeta_{180}^{-1}]$ and let \mathcal{M}_1 be a submodule of $\mathcal{O}_{\mathbb{K}}$ generated by the linearly independent vectors $\{w_1, w_2, \dots, w_{10}\}$, where $w = Mv, w = (w_1, w_2, \dots, w_{10})^T, v = (1, e_1, e_2, \dots, e_{23})^T$ and the matrix M is given by

$$M = \begin{pmatrix} 8 & -24 & 8 & 8 & 0 & 8 & 16 & -16 & 24 & 0 & -16 & 0 & 8 & -24 & 16 & 8 & -32 & 32 & -8 & 8 & -8 & 0 & -24 & 8 \\ 8 & -16 & -8 & 24 & -16 & 0 & 8 & -72 & 8 & 24 & -16 & 64 & 8 & -56 & 16 & 8 & -16 & 40 & -8 & -48 & 16 & 8 & 8 & 32 \\ -8 & -16 & 8 & 24 & 16 & 16 & -8 & -8 & -8 & 24 & 16 & 16 & -8 & -40 & -16 & -8 & 16 & 24 & 8 & -16 & -16 & -24 & -8 & 0 \\ 0 & -16 & -8 & 24 & 0 & 8 & 8 & -40 & 0 & 24 & 8 & 40 & 8 & -48 & -8 & 0 & 0 & 32 & -24 & -32 & 0 & -8 & 16 & 16 \\ -8 & 48 & 0 & -32 & 16 & -8 & 0 & 96 & -8 & -16 & 24 & -56 & 0 & 88 & -16 & -24 & 8 & -88 & -16 & 32 & -16 & -16 & 8 & -48 \\ -16 & -8 & -8 & 24 & 16 & 16 & -16 & 0 & -32 & 32 & 40 & 24 & -8 & -32 & -32 & -16 & 40 & 8 & -8 & -24 & -8 & -32 & 32 & -8 \\ -56 & -16 & -16 & 16 & 56 & 8 & -56 & -24 & -96 & 16 & 128 & 24 & -32 & -32 & -104 & 0 & 136 & 24 & -8 & -16 & -40 & -8 & 80 & 8 \\ 0 & 8 & -16 & 0 & -16 & 8 & -8 & 40 & -16 & 8 & 0 & -16 & 0 & 16 & 0 & -16 & 16 & -24 & 0 & 8 & 24 & -24 & 32 & -24 \\ 24 & 48 & 16 & -52 & -8 & 8 & 24 & 84 & 44 & -36 & -32 & -48 & 12 & 88 & 24 & -20 & -56 & -72 & 0 & 40 & -8 & 0 & -48 & -36 \\ -16 & 52 & 0 & -60 & 8 & -4 & -24 & 104 & -16 & -36 & 20 & -56 & -12 & 96 & -12 & -28 & 28 & -80 & 48 & 0 & 4 & -8 & 20 & -44 \end{pmatrix}.$$

In this case, $\sigma_\alpha(\mathcal{M}_1)$ is a lattice of rank 10 in \mathbb{R}^{24} and for all $x \in \mathcal{M}_1$ we have that $\sigma_\alpha(x) = \gamma TA$, where $\gamma = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10})$,

$$T = 4 \begin{pmatrix} 2 & -6 & 8 & 2 & 0 & 2 & 4 & -4 & 6 & 0 & -4 & 0 & 2 & -6 & 4 & 2 & -8 & 8 & -2 & 2 & -2 & 0 & -6 & 2 \\ 2 & -4 & -2 & 6 & -4 & 0 & 2 & -18 & 2 & 6 & -4 & 16 & 2 & -14 & 4 & 2 & -4 & 10 & -2 & -12 & 4 & 2 & 2 & 8 \\ -2 & -4 & 2 & 6 & 4 & 4 & -2 & -2 & -2 & 6 & 4 & 4 & -2 & -10 & -4 & -2 & 4 & 6 & 2 & -4 & -4 & -6 & -2 & 0 \\ 0 & -4 & -2 & 6 & 0 & 2 & 2 & -10 & 0 & 6 & 2 & 10 & 2 & -12 & 0 & 0 & -2 & 8 & -6 & -8 & 0 & -2 & 4 & 4 \\ -2 & 12 & 0 & -8 & 4 & -2 & 0 & 24 & -2 & -4 & 6 & -14 & 0 & 22 & -4 & -6 & 2 & -22 & -4 & 8 & -4 & -4 & 2 & -12 \\ -4 & -2 & -2 & 6 & 4 & 4 & -4 & 0 & -8 & 8 & 10 & 6 & -2 & -8 & -8 & -4 & 10 & 2 & -2 & -6 & -2 & -8 & 8 & -2 \\ -14 & -4 & -4 & 4 & 14 & 2 & -14 & -6 & -24 & 4 & 32 & 6 & -8 & -8 & -26 & 0 & 34 & 6 & -2 & -4 & -10 & -2 & 20 & 2 \\ 0 & 2 & -4 & 0 & -4 & 2 & -2 & 10 & -4 & 2 & 0 & -4 & 0 & 4 & 0 & -4 & 4 & -6 & 0 & 2 & 6 & -6 & 8 & -6 \\ 6 & 12 & 4 & -13 & -2 & -2 & 6 & 21 & 11 & -9 & -8 & -12 & 3 & 22 & 6 & -5 & -14 & -18 & 0 & 10 & -2 & 0 & -12 & -9 \\ -4 & 13 & 0 & -15 & 2 & -1 & -6 & 26 & -4 & -9 & 5 & -14 & -3 & 24 & -3 & -7 & 7 & -20 & 0 & 12 & 1 & -2 & 5 & -11 \end{pmatrix}$$

and

$$A = \begin{pmatrix} \sqrt{\sigma_1(\alpha)}\sigma_1(1) & \cdots & \sqrt{\sigma_{24}(\alpha)}\sigma_{24}(1) \\ \sqrt{\sigma_1(\alpha)}\sigma_1(e_1) & \cdots & \sqrt{\sigma_{24}(\alpha)}\sigma_{24}(e_1) \\ \vdots & \ddots & \vdots \\ \sqrt{\sigma_1(\alpha)}\sigma_1(e_{23}) & \cdots & \sqrt{\sigma_{24}(\alpha)}\sigma_{24}(e_{23}) \end{pmatrix},$$

where A is a generator matrix of lattice $\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$, since $\{1, e_1, e_2, \dots, e_{22}, e_{23}\}$ is a \mathbb{Z} -basis for $\mathcal{O}_{\mathbb{K}}$. We have that $B_1 = TA$ is a generator matrix for $\sigma_\alpha(\mathcal{M}_1)$, and as B_1 has rank 10, it follows that the lattice $\sigma_\alpha(\mathcal{M}_1)$ has rank 10. A Gram matrix for the lattice $\sigma_\alpha(\mathcal{M}_1)$ is $Q = TGT^t$, where $G = (Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e_i e_j))_{i,j=0}^{23}$ is a

Gram matrix for the lattice $\sigma_\alpha(\mathcal{O}_\mathbb{K})$. From Proposition 3.10, it follows that the matrix G is given by

$$90 \begin{pmatrix} 47 & 0 & 68 & 0 & 89 & 0 & 72 & 0 & 80 & 0 & 76 & 0 & 69 & 0 & 76 & 0 & 62 & 0 & 71 & 0 & 55 & 0 & 64 & 0 \\ 0 & 162 & 0 & 157 & 0 & 161 & 0 & 152 & 0 & 156 & 0 & 145 & 0 & 145 & 0 & 138 & 0 & 133 & 0 & 126 & 0 & 119 & 0 & 112 \\ 68 & 0 & 183 & 0 & 140 & 0 & 169 & 0 & 148 & 0 & 149 & 0 & 152 & 0 & 131 & 0 & 147 & 0 & 117 & 0 & 135 & 0 & 103 & 0 \\ 0 & 157 & 0 & 166 & 0 & 148 & 0 & 165 & 0 & 141 & 0 & 156 & 0 & 138 & 0 & 140 & 0 & 131 & 0 & 126 & 0 & 119 & 0 & 111 \\ 89 & 0 & 140 & 0 & 174 & 0 & 144 & 0 & 158 & 0 & 148 & 0 & 142 & 0 & 147 & 0 & 124 & 0 & 140 & 0 & 110 & 0 & 127 & 0 \\ 0 & 161 & 0 & 148 & 0 & 170 & 0 & 137 & 0 & 165 & 0 & 134 & 0 & 151 & 0 & 131 & 0 & 133 & 0 & 124 & 0 & 118 & 0 & 109 \\ 72 & 0 & 169 & 0 & 144 & 0 & 163 & 0 & 144 & 0 & 151 & 0 & 143 & 0 & 135 & 0 & 140 & 0 & 117 & 0 & 132 & 0 & 100 & 0 \\ 0 & 152 & 0 & 165 & 0 & 137 & 0 & 170 & 0 & 130 & 0 & 160 & 0 & 127 & 0 & 144 & 0 & 124 & 0 & 125 & 0 & 114 & 0 & 109 \\ 80 & 0 & 148 & 0 & 158 & 0 & 144 & 0 & 156 & 0 & 139 & 0 & 144 & 0 & 136 & 0 & 128 & 0 & 132 & 0 & 107 & 0 & 123 & 0 \\ 0 & 156 & 0 & 141 & 0 & 165 & 0 & 130 & 0 & 165 & 0 & 123 & 0 & 153 & 0 & 120 & 0 & 136 & 0 & 114 & 0 & 116 & 0 & 106 \\ 76 & 0 & 149 & 0 & 148 & 0 & 151 & 0 & 139 & 0 & 149 & 0 & 132 & 0 & 137 & 0 & 128 & 0 & 118 & 0 & 123 & 0 & 99 & 0 \\ 0 & 145 & 0 & 156 & 0 & 134 & 0 & 160 & 0 & 123 & 0 & 158 & 0 & 116 & 0 & 145 & 0 & 110 & 0 & 127 & 0 & 106 & 0 & 102 \\ 69 & 0 & 152 & 0 & 142 & 0 & 143 & 0 & 144 & 0 & 132 & 0 & 142 & 0 & 124 & 0 & 127 & 0 & 119 & 0 & 110 & 0 & 109 & 0 \\ 0 & 145 & 0 & 138 & 0 & 151 & 0 & 127 & 0 & 153 & 0 & 116 & 0 & 150 & 0 & 106 & 0 & 136 & 0 & 102 & 0 & 113 & 0 & 100 \\ 76 & 0 & 131 & 0 & 147 & 0 & 135 & 0 & 136 & 0 & 137 & 0 & 124 & 0 & 132 & 0 & 115 & 0 & 119 & 0 & 105 & 0 & 104 & 0 \\ 0 & 138 & 0 & 140 & 0 & 131 & 0 & 144 & 0 & 120 & 0 & 145 & 0 & 106 & 0 & 141 & 0 & 98 & 0 & 122 & 0 & 96 & 0 & 96 \\ 62 & 0 & 147 & 0 & 124 & 0 & 140 & 0 & 128 & 0 & 128 & 0 & 127 & 0 & 115 & 0 & 124 & 0 & 101 & 0 & 113 & 0 & 88 & 0 \\ 0 & 133 & 0 & 131 & 0 & 133 & 0 & 124 & 0 & 136 & 0 & 110 & 0 & 136 & 0 & 98 & 0 & 127 & 0 & 92 & 0 & 105 & 0 & 93 \\ 71 & 0 & 117 & 0 & 140 & 0 & 117 & 0 & 132 & 0 & 118 & 0 & 119 & 0 & 119 & 0 & 101 & 0 & 118 & 0 & 84 & 0 & 110 & 0 \\ 0 & 126 & 0 & 126 & 0 & 124 & 0 & 125 & 0 & 114 & 0 & 127 & 0 & 102 & 0 & 122 & 0 & 92 & 0 & 110 & 0 & 89 & 0 & 87 \\ 55 & 0 & 135 & 0 & 110 & 0 & 132 & 0 & 107 & 0 & 123 & 0 & 110 & 0 & 105 & 0 & 113 & 0 & 84 & 0 & 115 & 0 & 66 & 0 \\ 0 & 119 & 0 & 119 & 0 & 118 & 0 & 114 & 0 & 116 & 0 & 106 & 0 & 113 & 0 & 96 & 0 & 105 & 0 & 89 & 0 & 92 & 0 & 82 \\ 64 & 0 & 103 & 0 & 127 & 0 & 100 & 0 & 123 & 0 & 99 & 0 & 109 & 0 & 104 & 0 & 88 & 0 & 110 & 0 & 66 & 0 & 108 & 0 \\ 0 & 112 & 0 & 111 & 0 & 109 & 0 & 109 & 0 & 106 & 0 & 102 & 0 & 100 & 0 & 96 & 0 & 93 & 0 & 87 & 0 & 82 & 0 & 80 \end{pmatrix},$$

and consequently,

$$Q = TGT^t = 5760 \begin{pmatrix} 4 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 4 & -2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 4 & 2 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 4 & 2 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 2 & 2 & 4 & 2 & 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 4 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 4 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 4 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 2 & 4 & 0 \end{pmatrix},$$

such that $\det(Q) = 2^{78}3^{21}5^{10}$. By Proposition 3.9, the trace form of $x \in \mathcal{M}_1$ is given by

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x^2) &= 23040a_1^2 - 23040a_1a_2 + 23040a_2^2 - 23040a_2a_3 + 23040a_3^2 + 23040a_2a_4 + 23040a_4^2 \\ &+ 11520a_{10}a_5 + 23040a_4a_5 + 23040a_5^2 + 23040a_{10}a_6 + 23040a_3a_6 + 23040a_4a_6 + 23040a_5a_6 \\ &+ 23040a_6^2 + 23040a_{10}a_7 + 23040a_6a_7 + 23040a_7^2 + 23040a_{10}a_8 + 23040a_6a_8 + 23040a_7a_8 \\ &+ 23040a_8^2 + 23040a_{10}a_9 + 23040a_5a_9 + 11520a_6a_9 + 23040a_9^2 + 23040a_{10}^2. \end{aligned}$$

Thus, $t = \min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x^2); x \in \mathcal{M}_1, x \neq 0\} = 23040$ with $a_1 = 1$ and $a_j = 0$, for $j \neq 1$. By Equation (1) it follows that the center density of lattice $\sigma_\alpha(\mathcal{M}_1)$ is given by

$$\delta(\sigma_\alpha(\mathcal{M}_1)) = \frac{t^{m/2}}{2^m \sqrt{\det(Q)}} = \frac{(23040)^{10/2}}{2^{10} \sqrt{2^{78}3^{21}5^{10}}} = \frac{1}{16\sqrt{3}}.$$

Therefore, $\sigma_\alpha(\mathcal{M}_1)$ is a lattice of rank 10 with the same center density of Λ_{10} . As $\frac{1}{5760}Q$ is a standard Gram matrix of Λ_{10} [12], it follows that $\frac{1}{\sqrt{5760}}\sigma_\alpha(\mathcal{M}_1)$ is a rotated version of Λ_{10} . Using a computer,

we observed that $\min_{0 \neq y \in \mathcal{M}} |N_{\mathbb{K}/\mathbb{Q}}(y)| \leq 4.13 \times 10^{20}$. Now, the minimum norm in Λ_{10} is $\mu = 4$. As $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = 8.3 \times 10^9$ and $\sigma_\alpha(\mathcal{M})$ is a scaled version of Λ_{10} with scale factor $\sqrt{5760}$, by Equation (4)

$$d_{p,rel}(\sigma_\alpha(\mathcal{M})) \leq \left(\frac{1}{\sqrt{23040}}\right)^{24} \sqrt{8.3 \times 10^9} \times 4.13 \times 10^{20} = 1.68 \times 10^{-27},$$

and consequently,

$$\sqrt[10]{d_{p,rel}(\sigma_\alpha(\mathcal{M}))} \leq 0.00210.$$

Now, let \mathcal{M}_2 be a submodule of $\mathcal{O}_{\mathbb{K}}$ generated by the linearly independent vectors $\{w_1, w_2, \dots, w_9\}$, following the same steps as the construction of Λ_{10} , it follows that

$$T = 4 \begin{pmatrix} 2 & -6 & 8 & 2 & 0 & 2 & 4 & -4 & 6 & 0 & -4 & 0 & 2 & -6 & 4 & 2 & -8 & 8 & -2 & 2 & -2 & 0 & -6 & 2 \\ 2 & -4 & -2 & 6 & -4 & 0 & 2 & -18 & 2 & 6 & -4 & 16 & 2 & -14 & 4 & 2 & -4 & 10 & -2 & -12 & 4 & 2 & 2 & 8 \\ -2 & -4 & 2 & 6 & 4 & 4 & -2 & -2 & -2 & 6 & 4 & 4 & -2 & -10 & -4 & -2 & 4 & 6 & 2 & -4 & -4 & -6 & -2 & 0 \\ 0 & -4 & -2 & 6 & 0 & 2 & 2 & -10 & 0 & 6 & 2 & 10 & 2 & -12 & 0 & 0 & -2 & 8 & -6 & -8 & 0 & -2 & 4 & 4 \\ -2 & 12 & 0 & -8 & 4 & -2 & 0 & 24 & -2 & -4 & 6 & -14 & 0 & 22 & -4 & -6 & 2 & -22 & -4 & 8 & -4 & -4 & 2 & -12 \\ -4 & -2 & -2 & 6 & 4 & 4 & -4 & 0 & -8 & 8 & 10 & 6 & -2 & -8 & -8 & -4 & 10 & 2 & -2 & -6 & -2 & -8 & 8 & -2 \\ -14 & -4 & -4 & 4 & 14 & 2 & -14 & -6 & -24 & 4 & 32 & 6 & -8 & -8 & -26 & 0 & 34 & 6 & -2 & -4 & -10 & -2 & 20 & 2 \\ 0 & 2 & -4 & 0 & -4 & 2 & -2 & 10 & -4 & 2 & 0 & -4 & 0 & 4 & 0 & -4 & 4 & -6 & 0 & 2 & 6 & -6 & 8 & -6 \\ 6 & 12 & 4 & -13 & -2 & -2 & 6 & 21 & 11 & -9 & -8 & -12 & 3 & 22 & 6 & -5 & -14 & -18 & 0 & 10 & -2 & 0 & -12 & -9 \end{pmatrix},$$

and consequently a Gram matrix for the lattice $\sigma_\alpha(\mathcal{M}_2)$ is given by

$$Q = TGT^t = 5760 \begin{pmatrix} 4 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 4 & -2 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 4 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 4 & 2 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 4 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 2 & 4 & 2 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 4 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 4 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 4 \end{pmatrix},$$

such that $\det(Q) = 2^{72}3^{18}5^9$. By Proposition 3.9 the trace form of $x \in \mathcal{M}_2$ is given by

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x^2) &= 23040a_1^2 - 23040a_1a_2 + 23040a_2^2 - 23040a_2a_3 + 23040a_3^2 + 23040a_2a_4 + 23040a_4^2 \\ &\quad + 23040a_4a_5 + 23040a_5^2 + 23040a_3a_6 + 23040a_4a_6 + 23040a_5a_6 + 23040a_6^2 + 23040a_6a_7 \\ &\quad + 23040a_7^2 + 23040a_6a_8 + 23040a_7a_8 + 23040a_8^2 + 23040a_5a_9 + 11520a_6a_9 + 23040a_9^2. \end{aligned}$$

Thus, $t = \min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x^2); x \in \mathcal{M}_2, x \neq 0\} = 23040$ with $a_1 = 1$ and $a_j = 0$, for $j \neq 1$. By Equation (1) it follows that the center density of lattice $\sigma_\alpha(\mathcal{M}_2)$ is given by

$$\delta(\sigma_\alpha(\mathcal{M}_2)) = \frac{t^{m/2}}{2^m \sqrt{\det(Q)}} = \frac{(23040)^{9/2}}{2^9 \sqrt{2^{72}3^{18}5^9}} = \frac{1}{16\sqrt{2}}.$$

Therefore, $\sigma_\alpha(\mathcal{M}_2)$ is a lattice of rank 9 with the same center density of Λ_9 . As $\frac{1}{5760}Q$ is a standard Gram matrix of Λ_9 [12], it follows that $\frac{1}{\sqrt{5760}}\sigma_\alpha(\mathcal{M}_2)$ is a rotated version of Λ_9 . Using a computer, we observed

that $\min_{0 \neq y \in \mathcal{M}} |N_{\mathbb{K}/\mathbb{Q}}(y)| \leq 2.28 \times 10^{21}$. Now, the minimum norm in Λ_9 is $\mu = 4$. As $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = 8.3 \times 10^9$ and $\sigma_\alpha(\mathcal{M})$ is a scaled version of Λ_9 with scale factor $\sqrt{5760}$, by Equation (4)

$$d_{p,rel}(\sigma_\alpha(\mathcal{M})) \leq \left(\frac{1}{\sqrt{23040}}\right)^{24} \sqrt{8.3 \times 10^9} \times 2.28 \times 10^{21} = 9.29 \times 10^{-27},$$

and consequently,

$$\sqrt[9]{d_{p,rel}(\sigma_\alpha(\mathcal{M}))} \leq 0.00128.$$

4.5. Construction of the Λ_{11} -lattice

Let $\mathbb{L} = \mathbb{Q}(\zeta_{23})$, \mathbb{K} the subfield of \mathbb{L} such that $[\mathbb{K} : \mathbb{Q}] = 11$, and $\langle \sigma \rangle = Gal(\mathbb{K}/\mathbb{Q})$, where $\sigma : \zeta_{23} \mapsto \zeta_{23}^2$. Then $\mathbb{K} = \mathbb{Q}(\theta)$ where $\theta = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_{23}) = \zeta_{23} + \zeta_{23}^{-1}$. A \mathbb{Z} -basis for $\mathcal{O}_{\mathbb{K}}$, the ring of integers of \mathbb{K} , is $\{\sigma^i(\theta)\}_{i=0}^{10}$. By Proposition 3.11, the trace form of \mathbb{K} is given by

$$Tr_{\mathbb{K}/\mathbb{Q}}(x^2) = 23(a_0^2 + a_1^2 + \dots + a_{10}^2) - 2(a_0 + a_1 + \dots + a_{10})^2,$$

where $x = a_0\theta + a_1\sigma(\theta) + \dots + a_{10}\sigma^{10}(\theta)$. Let

$$\gamma = N_{\mathbb{L}/\mathbb{K}}(1 - \zeta_{23}) = (1 - \zeta_{23})(1 - \zeta_{23}^{-1}) = -\theta - 2\sum_{i=0}^{10} \sigma^i(\theta).$$

It follows that

$$Tr_{\mathbb{K}/\mathbb{Q}}(\gamma) = N_{\mathbb{K}/\mathbb{Q}}(\gamma) = 23.$$

Furthermore, let

$$\epsilon = 6\sum_{i=0}^{10} \sigma^i(\theta) + 4\sigma^6(\theta) + \sigma^7(\theta)$$

be a unit in $\mathcal{O}_{\mathbb{K}}$. The element $\alpha = \epsilon\gamma$ is totally positive and $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = 23$. Let Λ_0 denote the lattice $\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$, where $\sigma_\alpha : \mathbb{K} \rightarrow \mathbb{R}^{11}$ is the twisted homomorphism given by $\sigma_\alpha(x) = (\sqrt{\sigma^0(\alpha)}\sigma^0(x), \sqrt{\sigma^1(\alpha)}\sigma^1(x), \dots, \sqrt{\sigma^{10}(\alpha)}\sigma^{10}(x))$ and \mathcal{M} be the \mathbb{Z} -submodule of $\mathcal{O}_{\mathbb{K}}$ defined by

$$\mathcal{M} = \{a_0\theta + a_1\sigma(\theta) + \dots + a_{10}\sigma^{10}(\theta) \in \mathcal{O}_{\mathbb{K}}; a_j \equiv 0 \pmod{2}, \text{ for } j = 2, 4, 6, 8, 10\},$$

then the Gram matrix of $\sigma_\alpha(\mathcal{M})$ is given by

$$G = 23 \begin{pmatrix} 4 & -2 & 0 & 2 & -2 & -2 & 0 & 2 & 0 & 0 & -2 \\ -2 & 4 & 0 & -1 & 4 & 0 & 0 & -1 & -4 & -1 & 2 \\ 0 & 0 & 12 & 0 & 0 & -2 & 0 & 4 & -8 & -2 & -4 \\ 2 & -1 & 0 & 4 & -6 & -2 & -2 & 0 & 0 & 2 & 0 \\ -2 & 4 & 0 & -6 & 24 & 0 & 0 & 0 & -4 & -6 & 0 \\ -2 & 0 & -2 & -2 & 0 & 4 & 4 & -2 & 0 & -1 & 0 \\ 0 & 0 & 0 & -2 & 0 & 4 & 12 & -2 & -4 & -4 & 0 \\ 2 & -1 & 4 & 0 & 0 & -2 & -2 & 4 & -2 & 0 & -4 \\ 0 & -4 & -8 & 0 & -4 & 0 & -4 & -2 & 16 & 4 & 4 \\ 0 & -1 & -2 & 2 & -6 & -1 & -4 & 0 & 4 & 4 & 0 \\ -2 & 2 & -4 & 0 & 0 & 0 & 0 & -4 & 4 & 0 & 8 \end{pmatrix}.$$

We have that $t = \min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x^2) : x \in \mathcal{M}, x \neq 0\} = 2^2 \times 23$, with $a_0 = 1, a_1 = a_2 = \dots = a_{10} = 0$ and $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}] = 32$. Since $d_{\mathbb{K}} = 23^{10}$, the center density of the lattice $\sigma_{\alpha}(\mathcal{M})$ is given by

$$\delta(\sigma_{\alpha}(\mathcal{M})) = \frac{t^{n/2}}{2^n [\mathcal{O}_{\mathbb{K}} : \mathcal{M}] \sqrt{N(\alpha) |d_{\mathbb{K}}|}} = \frac{(2^2 \cdot 23)^{11/2}}{2^{11} \times 32 \sqrt{23 |23^{10}|}} = \frac{1}{32},$$

i.e., the same as that of the Λ_{11}^{\max} lattice [12, Chapter 6, Section 4]. The above lattice is a rotated version of Λ_{11}^{\max} . Indeed, $G' = \frac{1}{23} U G U^t$, where

$$G' = \begin{pmatrix} 4 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 4 & -2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 4 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 4 & 2 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 4 & 2 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 4 & 2 & 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 4 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 4 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 4 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 2 & 4 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 4 \end{pmatrix}$$

is a Gram matrix of Λ_{11}^{\max} and

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

is an element of $GL(11, \mathbb{Z})$. Thus, $\min_{0 \neq y \in \mathcal{M}} |N_{\mathbb{K}/\mathbb{Q}}(y)| = 1$, since for $y = -\theta \in \mathcal{M}$, $N_{\mathbb{K}/\mathbb{Q}}(y) = 1$. Now, the minimum norm in Λ_{11} is $\mu = 4$. As $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = 23$ and $\sigma_{\alpha}(\mathcal{M})$ is a scaled version of Λ_{11} with scale factor $\sqrt{23}$, by Equation (4)

$$d_{p,rel}(\sigma_{\alpha}(\mathcal{M})) = \left(\frac{1}{\sqrt{92}}\right)^{11} \sqrt{23} \cdot 1 = 7.58 \times 10^{-11},$$

and consequently,

$$\sqrt[11]{d_{p,rel}(\sigma_{\alpha}(\mathcal{M}))} = 0.12022.$$

5. Conclusions

In this section, we assess the performance of the lattices presented in this paper in terms of center density and relative minimum product distance. These parameters are associated with the efficiency in signal transmission over Gaussian and Rayleigh fading channels, respectively. Table 1 shows a comparison between the best known relative product distance of rotated \mathbb{Z}^n -lattices, obtained via cyclotomic, cyclic and mixed constructions [5] and via Kruskemper method [18] (First column), the densest lattices Λ_0

(D_3 , D_5 and E_7) obtained in [15, 16] (Second column), and the densest lattices Λ_n ($\Lambda_3 = D_3$, $\Lambda_5 = D_5$, $\Lambda_7 = E_7$ and $\Lambda_{12} = K_{12}$) from our construction (Third column). The center density δ of these lattices are also displayed.

For the lattice D_3 the minimum product distance 0.36964 presented in [16, Table 3] is higher than that from our construction, while for dimension 5 our construction yields the same value. In dimension 7 (see [15, Remark 4.13]) the authors obtained a lower bound on the minimum product distance whereas for our construction the bound holds. For dimensions 9 and 10, we constructed the lattices Λ_9 and Λ_{10} with an upper bound for their minimum product distance. Although the bounds are not very high, the lattices in those two dimensions and in dimension 11 are new and are not known in the literature (as algebraic lattices). In particular, the value that we obtained in dimension 11 is half of the one obtained for \mathbb{Z}^n (cyclotomic and cyclic constructions in [5]).

A broader question to be investigated is whether algebraic constructions of lattices, mainly in dimensions 9, 10 and 11, as the ones approached here, can provide greater relative minimum product distance for rotated densest lattices.

It is noticed that the relative minimum product distances $d_{p,rel}(\Lambda_n)$ of the rotated lattices obtained in the present paper are smaller than the relative minimum product distances $d_{p,rel}(\mathbb{Z}^n)$ of rotated \mathbb{Z}^n -lattices constructed for the Rayleigh channels in [5, 18]. Nevertheless, if the goal is to construct lattices which have good performance on both Gaussian and Rayleigh channels, we may assert that taking into account the trade-off center density versus product distance, there are some advantages in considering the rotated Λ_n -lattices instead of rotated \mathbb{Z}^n -lattices.

Table 1. Relative minimum product distance versus center density (from [5, 15, 16, 18] and the results presented here)

n	$\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}$	$\sqrt[n]{d_{p,rel}(\Lambda_0)}$	$\sqrt[n]{d_{p,rel}(\Lambda_n)}$	$\delta(\mathbb{Z}^n)$	$\delta(\Lambda)$
3	0.52275	0.36964	0.33994	0.12500	0.17677
5	0.38321	0.27097	0.27097	0.03125	0.08838
7	0.30080	≥ 0.11809	0.11809	0.00781	0.06250
9	0.27018	-	≤ 0.00128	0.00195	0.04419
10	0.25627	-	≤ 0.00210	0.00097	0.03608
11	0.24045	-	0.12022	0.00048	0.03125

References

- [1] A. A. Andrade, A. J. Ferrari, C. W. O. Benedito, Constructions of algebraic lattices, *Comput. Appl. Math.* 29(3) (2010) 1–13.
- [2] E. Bayer–Fluckiger, Ideal lattices, *Proceedings of the conference Number Theory and Diophantine Geometry* (2002) 168–184.
- [3] E. Bayer–Fluckiger, Lattices and number fields, *Contemp. Math.* 241 (1999) 69–84.
- [4] E. Bayer–Fluckiger, Upper bounds for Euclidean minima of algebraic number fields, *J. Number Theory* 121(2) (2006) 305–323.
- [5] E. Bayer–Fluckiger, F. Oggier, E. Viterbo, New algebraic constructions of rotated \mathbb{Z}^n -lattice constellations for the Rayleigh fading channel, *IEEE Trans. Inform. Theory* 50(4) (2004) 702–714.

- [6] E. Bayer–Fluckiger, G. Nebe, On the Euclidian minimum of some real number fields, *Journal de Théorie des Nombres de Bordeaux* 17(2) (2005) 437–454.
- [7] E. Bayer–Fluckiger, I. Suarez, Ideal lattices over totally real number fields and Euclidean minima, *Arch. Math.* 86 (2006) 217–225.
- [8] E. Bayer–Fluckiger, P. Maciak, Upper bounds for Euclidean minimal for abelian number fields of odd prime conductor, *Math. Ann.* 357 (2013) 1071–1089.
- [9] W. Bosma, J. Cannon, C. Playoust, The magma algebra system. I. The user language, *J. Symbolic Comput.* 24 (1997) 235–265.
- [10] J. Boutros, E. Viterbo, C. Rastello, J. C. Belfiori, Good lattice constellations for both Rayleigh fading and Gaussian channels, *IEEE Trans. Inform. Theory* 42(2) (1996) 502–518.
- [11] H. Cohn, A. Kumar, Optimality and uniqueness of the Leech lattice among lattices, *Ann. of Math.* 170(3) (2009) 1003–1050.
- [12] J. H. Conway, N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer–Verlag, New York 1998.
- [13] A. J. Ferrari, A. A. Andrade, Constructions of rotated lattice constellations in dimensions power of 3, *J. Algebra Appl.* 17(09) (2017) 1850175.
- [14] J. C. Interlando, T. P. N. Neto, T. M. Rodrigues, J. O. D. Lopes, A note on the integral trace form in cyclotomic fields, *J. Algebra Appl.* 14(04) (2015) 1550045.
- [15] G. C. Jorge, A. A. Andrade, S. I. R. Costa, J. E. Strapasson, Algebraic constructions of densest lattices, *J. Algebra* 429 (2015) 218–235.
- [16] G. C. Jorge, A. J. Ferrari, S. I. R. Costa, Rotated D_n -lattices, *J. Number Theory* 132(11) (2012) 2397–2406.
- [17] D. Micciancio, S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, in *Kluwer Internat. Ser. Engrg. Comput. Sci.*, Kluwer Academic Publishers 671 2002.
- [18] F. Oggier, E. Bayer–Fluckiger, Best rotated cubic lattice constellations for the Rayleigh fading channel, in *Proceedings of IEEE International Symposium on Information Theory* (2003).
- [19] E. L. Oliveira, J. C. Interlando, T. P. N. Neto, J. O. D. Lopes, The integral trace form of cyclic extensions of odd prime degree, *Rocky Mountain J. Math.* 47(4) (2017) 1075–1088.
- [20] P. Samuel, *Algebraic Theory of Numbers*, Hermann, 1982.
- [21] L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1995.