UFSM

CIÊNCIA e NATURA

ISSN 2179-460X
OPEN ACCESS

Ci. e Nat., Santa Maria, v. 46, e85207, 2024 • https://doi.org/10.5902/2179460X85207
Submitted: 09/26/2023 • Approved: 09/09/2024 • Published: 13/12/2024

Mathematics

Trace form via cyclotomic fields

Forma traço via corpos ciclotômicos

Antonio Aparecido de Andrade [I], **Agnaldo José Ferrari** [I]

[I]Universidade Estadual Paulista, São José do Rio Preto, SP, Brazil
[II]Universidade Estadual Paulista, Bauru, SP, Brazil

ABSTRACT

Let $n \geq 3$ be an integer, ζ_n a primitive nth root of unity, and $\mathbb{K}$ the cyclotomic field $\mathbb{Q}(\zeta_n)$. In this paper, we present an explicit description of the integral trace form $Tr_{\mathbb{K}}(\alpha x\overline{x})$, where $\alpha, x \in \mathbb{K}$ and $\overline{x}$ is the complex conjugate of x. Furthermore, we present constructions of algebraic lattices via the twisted canonical homomorphism with optimal center density in dimensions 2, 4, 6, 8 and 12, which are rotated versions of the lattices Λ_n, for $n = 2, 4, 6, 8$ and K_{12}.

Keywords: Trace form; Algebraic lattice; Cyclotomic field

RESUMO

Sejam $n \geq 3$ um número inteiro, ζ_n uma n-ésima raiz primitiva da unidade e $\mathbb{K}$ o corpo ciclotômico $\mathbb{Q}(\zeta_n)$. Neste trabalho, apresentamos uma descrição explícita da forma traço $Tr_{\mathbb{K}}(\alpha x\overline{x})$, onde $\alpha, x \in \mathbb{K}$ e $\overline{x}$ é o conjugado complexo de x. Além disso, apresentamos construções de reticulados algébricos via o homomorfismo canônico torcido com densidade central ótima nas dimensões 2, 4, 6, 8 e 12, que são versões rotacionadas dos reticulados Λ_n, para $n = 2, 4, 6, 8$ e K_{12}.

Palavras-chave: Forma traço; Reticulado algébrico; Corpos ciclotômicos

1 INTRODUCTION

A *lattice* Λ of rank full is a discrete additive subgroup of $\mathbb{R}^n$, that is, Λ is a lattice if there are linearly independent vectors $v_1, v_2, \ldots, v_n \in \mathbb{R}^n$ such that

$$\Lambda = \{\sum_{i=1}^{n} a_i v_i : \text{ with } a_i \in \mathbb{Z}, \text{ for } i = 1, 2, \ldots, n\}.$$

The set $B = \{v_1, v_2, \ldots, v_n\}$ is called a *basis* for the lattice Λ, the matrix

$$M = \begin{pmatrix} v_{11} & v_{1,2} & \cdots & v_{1,n} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n,1} & v_{n,2} & \cdots & v_{n,n} \end{pmatrix},$$

whose $v_i = (v_{j,1}, v_{j,2}, \ldots, v_{j,n})$, for $j = 1, 2, \ldots, n$, is said a *generator matrix* for Λ. The *volume* of the lattice Λ is defined as the module of the determinant of the matrix M and denoted by $Vol(\Lambda) = |\det(M)|$.

Lattices have been considered in different applied areas, especially in coding/modulation theory and more recently in cryptography. Algebraic lattices are those obtained via algebraic number fields. In digital communications, the lattice parameters of interest are their sphere packing density and minimum product distance. The higher those two parameters are, the more attractive the lattice becomes to be used for data transmission over Gaussian and fading channels. The classical sphere packing problem is to determine the density of a large quantity of identical spheres can be packed together in the Euclidean space, i.e, determine the proportion occupied by the spheres centered in the points of a lattice Λ and having radius $\rho(\Lambda) = \min\{||x - y||;\ x, y \in \Lambda,\ x \neq y\}/2$ relative to the entire space $\mathbb{R}^n$. So, if $\mathcal{B}(\rho(\Lambda))$ is the sphere with center in the origin and radius $\rho(\Lambda)$, the *packing density* of Λ is defined by

$$\Delta(\Lambda) = \frac{Vol(\mathcal{B}(\rho(\Lambda)))}{Vol(\Lambda)} = Vol(\mathcal{B}(1))\rho(\Lambda)^n \frac{1}{Vol(\Lambda)},$$

where $\delta(\Lambda) = \rho(\Lambda)^n / Vol(\Lambda)$ is called the *center density* of the lattice Λ. The densest possible lattice packings have only be determined in dimensions 1 to 8 and 24 and it is

also known that these densest lattice packings are unique. The formula to calculate the volume of an n-dimensional sphere with a radius 1 can be found in the work of Conway and Sloane (1998).

The integral trace form associated to an algebraic number field $\mathbb{K}$ is an integral quadratic form and appears in the study of lattices associated to algebraic number fields. Considering $\mathbb{K}$ an algebraic number field of degree n, $\sigma_1, \sigma_2, \ldots, \sigma_n$ the $\mathbb{Q}$-monomorphisms of $\mathbb{K}$ in $\mathbb{C}$ and $\alpha \in \mathcal{O}_{\mathbb{K}}$ is such that $\sigma_i(\alpha) > 0$, for $i = 1, 2, \ldots, n$, and $\sigma_\alpha : \mathbb{K} \to \mathbb{C}$ is the twisted canonical homomorphism, then $\sigma_\alpha(\mathcal{M})$ is an n-dimensional lattice, where $\mathcal{M}$ is a $\mathbb{Z}$-module of $\mathbb{K}$. The minimum norm $|\sigma_\alpha(x)|^2$, where $x \in \mathcal{M}$, is given by the work of Conway and Sloane (1998).

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

The integral trace form over algebraic number fields has been studied due to its application in the calculation of the packing radius of lattices generated from $\mathbb{Z}$-modules contained in $\mathcal{O}_{\mathbb{K}}$. In Interlando et al. (2015), the authors presented the integral trace form $Tr_{\mathbb{K}}(x\overline{x})$, where $\mathbb{K} = \mathbb{Q}(\zeta_n)$ with $n \geq 3$. In Ferrari et al. (2020), the authors presented the integral trace form $Tr_{\mathbb{K}}(\alpha x \overline{x})$, where $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ with $n \geq 3$. In this paper, we present an explicit construction of the trace form $Tr_{\mathbb{K}}(\alpha x \overline{x})$, where $\mathbb{K} = \mathbb{Q}(\zeta_n)$ with $n \geq 3$, for cyclotomic fields as tools for constructing algebraic lattices in Euclidean space with optimal center density via the twisted canonical homomorphism, where these algebraic lattices are obtained via ideals of a ring of algebraic integers.

2 BASIC RESULTS FROM TRACE FORM

An algebraic number field $\mathbb{K}$ is an extension of $\mathbb{Q}$ of finite degree n, that is, $[\mathbb{K} : \mathbb{Q}] = n$. In this case, $\mathbb{K} = \mathbb{Q}(\theta)$, where $\theta \in \mathbb{C}$ is a root of a monic irreducible polynomial $p(x) \in \mathbb{Q}[x]$ and n is the degree of $p(x)$. The n distinct roots of $p(x)$, namely, $\theta_1, \theta_2, \ldots, \theta_n$, are the conjugates of θ. If $\sigma : \mathbb{K} \to \mathbb{C}$ is a $\mathbb{Q}$-homomorphism, then $\sigma(\theta) = \theta_i$, for some $i = 1, 2, \ldots, n$. Furthermore, there are exactly n $\mathbb{Q}$-homomorphisms σ_i, for $i = 1, 2, \ldots, n$, of $\mathbb{K}$ in $\mathbb{C}$.

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

$\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} : \alpha$ is an algebraic integer$\}$ is a ring, called ring of algebraic integers of $\mathbb{K}$ and $\mathcal{O}_{\mathbb{K}}$, as a $\mathbb{Z}$-module, has a basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ over $\mathbb{Z}$, called integral basis, where n is the degree of $\mathbb{K}$.

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

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

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

$$\mathcal{D}(\mathbb{K}) = \mathcal{D}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det_{1 \leq i,j \leq n} (Tr_{\mathbb{K}}(\alpha_i \alpha_j)) = \det_{1 \leq i,j \leq n} (\sigma_i(\alpha_j))^2,$$

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

An algebraic number field $\mathbb{K}$ is said to be cyclotomic if $\mathbb{K} = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity. In this case, $[\mathbb{K} : \mathbb{Q}] = \phi(n)$, where ϕ is the Euler's totient function, the ring of algebraic integers of $\mathbb{L}$ is given by $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n]$ and $\{1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{\phi(n)-1}\}$ is an integral basis for $\mathbb{K}$, where $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, with $\alpha_k \geq 1$, for $k = 1, 2, \ldots, s$.

Definition 1: The function

$$\mu(n) = \begin{cases} (-1)^s, & \text{if } \alpha_k = 1, \text{ for all } k. \\ 1, & \text{if } n = 1. \\ 0, & \text{if } \alpha_k > 1, \text{ for some } k. \end{cases}$$

is called Möbius function.

Now, we present some results that will be very useful for the development of the trace form $Tr_{\mathbb{K}}(\alpha x \overline{x})$, where $\alpha, x \in \mathcal{O}_{\mathbb{K}}$. Since ζ_n^k and ζ_n^{-k} are conjugates, for $k = 1, 2, \ldots, \phi(n)-1$, it follows that $Tr_{\mathbb{K}}(\zeta_n^k) = Tr_{\mathbb{K}}(\zeta_n^{-k})$, and therefore, $Tr_{\mathbb{K}}(\zeta_n^k + \zeta_n^{-k}) = 2Tr_{\mathbb{K}}(\zeta_n^k)$. If k is a positive integer such that $\gcd(k, n) = d_k$, from Lemma 3.3 of Interlando et al.

(2015), it follows that

$$()Tr_{\mathbb{K}}(\zeta_n^k) = \frac{\mu(n/d_k)}{\phi(n/d_k)}\phi(n). \tag{1}$$

If k is an integer such that $k < \phi(n)$ and $d_k = \gcd(k, n)$, from Lemma 3.4 of Interlando et al. (2015), it follows that

$$Tr_{\mathbb{K}}(\zeta_n^k) \neq 0 \iff d_k = (n/P)t_j \text{ and } k = (n/P)j, \tag{2}$$

where $P = p_1p_2 \dots p_s$, $t_j = \gcd(j, P)$ for $j = 0, 1, 2, \dots, \phi(P) - 1$. From Lemma 3.5 of Interlando et al. (2015), if i and j are integers such that $i, j < \phi(n)$ and $d_{i-j} = \gcd(i - j, n)$, then

$$Tr_{\mathbb{K}}(\zeta_n^{i-j}) \neq 0 \iff d_{i-j} = (n/P)t_k \text{ and } |i - j| = (n/P)k, \tag{3}$$

where $P = p_1p_2 \dots p_s$, $t_k = \gcd(k, P)$ for $k = 0, 1, 2, \dots, \phi(P) - 1$. From Lemma 3.6 of Interlando et al. (2015), if i and j are integers such that $i, j < \phi(n)$ and $d_{i+j} = \gcd(i + j, n)$, then

$$Tr_{\mathbb{K}}(\zeta_n^{i+j}) \neq 0 \iff d_{i+j} = (n/P)t_k \text{ and } i + j = (n/P)k, \tag{4}$$

where $P = p_1p_2 \dots p_s$, $t_k = \gcd(k, P)$ for $k = 0, 1, 2, \dots, 2\phi(P) - 2$, if $n = P$ and $k = 0, 1, 2, \dots, 2\phi(P) - 1$, if $n \neq P$

3 TRACE FORM FOR CYCLOTOMIC FIELDS

In this section, we present an explicit trace form for $\mathbb{K} = \mathbb{Q}(\zeta_n)$, where we consider the same notations as in the previous section.

Proposition 1: If $\alpha = a_0 + a_1\zeta_n + \cdots + a_{\phi(n)-1}\zeta_n^{\phi(n)-1} \in \mathcal{O}_{\mathbb{K}}$, then

$$Tr_{\mathbb{K}}(\alpha) = \frac{n}{P}\left(\phi(P)a_0 + \sum_{k=1}^{\phi(P)-1} a_{\frac{n}{P}k}\mu\left(\frac{P}{t_k}\right)\phi(t_k)\right).$$

Proof. If $\alpha = a_0 + a_1\zeta_n + \cdots + a_{\phi(n)-1}\zeta_n^{\phi(n)-1} \in \mathcal{O}_{\mathbb{K}}$, then

$$\begin{aligned} Tr_{\mathbb{K}}(\alpha) &= Tr_{\mathbb{K}}(a_0 + a_1\zeta_n + \cdots + a_{\phi(n)-1}\zeta_n^{\phi(n)-1}) \\ &= a_0 Tr_{\mathbb{K}}(1) + a_1 Tr_{\mathbb{K}}(\zeta_n) + \cdots + a_{\phi(n)-1} Tr_{\mathbb{K}}(\zeta_n^{\phi(n)-1}). \end{aligned}$$

From Equation (1), it follows that

$$Tr_{\mathbb{K}}(\alpha) = \phi(n)a_0 + \sum_{k=1}^{\phi(n)-1} a_k \frac{\mu(n/d_k)}{\phi(n/d_k)}\phi(n)$$

and from Equation (2), it follows that

$$Tr_{\mathbb{K}}(\alpha) = \phi(n)a_0 + \sum_{k=1}^{\phi(P)-1} a_{\frac{n}{P}k}\mu\left(\frac{P}{t_k}\right)\frac{1}{\phi(\frac{P}{t_k})}\phi(n).$$

Since $\gcd(P/t_k, t_k) = 1$, it follows that $\phi(P) = \phi((P/t_k)t_k) = \phi(P/t_k)\phi(t_k)$, that is, $\phi(P/t_k) = \phi(P)/\phi(t_k)$. Since $\phi(n) = (n/P)\phi(P)$, it follows that

$$\begin{aligned} Tr_{\mathbb{K}}(\alpha) &= \frac{n}{P}\phi(P)a_0 + \sum_{k=1}^{\phi(P)-1} a_{\frac{n}{P}k}\mu\left(\frac{P}{t_k}\right)\frac{\phi(t_k)}{\phi(P)}\frac{n}{P}\phi(P) \\ &= \frac{n}{P}\left(\phi(P)a_0 + \sum_{k=1}^{\phi(P)-1} a_{\frac{n}{P}k}\mu\left(\frac{P}{t_k}\right)\phi(t_k)\right), \end{aligned}$$

which proves the result.

Corolarry 1: If $n = 2^r$, where $r \geq 2$, then $Tr_{\mathbb{K}}(\alpha) = \phi(n)a_0$.

Proof: If $n = 2^r$, where $r \geq 2$, then $d_k = 1$ if 2 does not appear in the decomposition of k or $d_k = 2^q$ if 2 appears in the factorization of k, where $q < r - 1$. Thus, $\mu(2^r/d_k) = 0$, and therefore, $Tr_{\mathbb{K}}(\zeta_n^k) = 0$, for $k = 1, 2, \ldots, \phi(n) - 1$. Therefore, $Tr_{\mathbb{K}}(\alpha) = \phi(n)a_0$.

Theorem 1: If $\alpha = a_0 + a_1\zeta_n + \cdots + a_{\phi(n)-1}\zeta_n^{\phi(n)-1} \in \mathcal{O}_{\mathbb{K}}$ and

$x = b_0 + b_1\zeta_n + \cdots + b_{\phi(n)-1}\zeta_n^{\phi(n)-1} \in \mathcal{O}_{\mathbb{K}}$, then

$$\begin{aligned} Tr_{\mathbb{K}}(\alpha x\overline{x}) &= \frac{n}{P}\left(\phi(P)a_0 + \sum_{k=1}^{\phi(P)-1} a_{\frac{n}{P}k}\mu\left(\frac{P}{t_k}\right)\phi(t_k)\right)\sum_{i=0}^{\phi(n)-1} b_i^2 \\ &\quad +2a_0\sum_{k=1}^{\phi(P)-1} B_{\frac{n}{P}k}\frac{\mu(\frac{P}{t_k})}{\phi(\frac{P}{t_k})}\phi(n) + \sum_{\substack{i+j=\frac{nk}{P}\\ l\le k\le r\\ 1\le i,j\le\phi(n)-1}} a_iB_j\frac{\mu(\frac{P}{t_k})}{\phi(\frac{P}{t_k})}\phi(n) \\ &\quad + \sum_{\substack{0\le|i-j|=\frac{nk}{P}\\ 0\le k\le s\\ 1\le i,j\le\phi(n)-1}} a_iB_j\frac{\mu(\frac{P}{t_k})}{\phi(\frac{P}{t_k})}\phi(n), \end{aligned}$$

where $l = \left\lceil\frac{2P}{n}\right\rceil$, $r = \left\lfloor\phi(P) - \frac{2P}{n}\right\rfloor$, $s = \left\lfloor\frac{\phi(P)}{2} - \frac{2P}{n}\right\rfloor$ and $B_i = b_0b_i + b_1b_{i+1} + \ldots + b_{\phi(n)-1-i}b_{\phi(n)-1}$, for $i = 1, 2, \cdots, \phi(n)-1$

Proof: If $x = b_0 + b_1\zeta_n + \ldots + b_{\phi(n)-1}\zeta_n^{\phi(n)-1} \in \mathcal{O}_{\mathbb{K}}$, then $\overline{x} = b_0 + b_1\zeta_n^{-1} + \ldots + b_{\phi(n)-1}\zeta_n^{-\phi(n)+1}$, and therefore,

$$x\overline{x} = \sum_{i=0}^{\phi(n)-1} b_i^2 + \sum_{i=1}^{\phi(n)-1} B_i\beta_i,$$

where $B_i = b_0b_i + b_1b_{i+1} + \ldots + b_{\phi(n)-1-i}b_{\phi(n)-1}$ and $\beta_i = \zeta_n^i + \zeta_n^{-i}$, for $i = 1, 2, \cdots, \phi(n)-1$. If $\alpha = a_0 + a_1\zeta_n + \cdots + a_{\phi(n)-1}\zeta_n^{\phi(n)-1} \in \mathcal{O}_{\mathbb{K}}$, then

$$\begin{aligned} \alpha x\overline{x} &= \alpha\sum_{i=0}^{\phi(n)-1} b_i^2 + \alpha\sum_{i=1}^{\phi(n)-1} B_i\beta_i \\ &= \alpha\sum_{i=0}^{\phi(n)-1} b_i^2 + (a_0 + a_1\zeta_n + \ldots + a_{\phi(n)-1}\zeta_n^{\phi(n)-1})\sum_{i=1}^{\phi(n)-1} B_i(\zeta_n^i + \zeta_n^{-i}) \\ &= \alpha\sum_{i=0}^{\phi(n)-1} b_i^2 + a_0\sum_{i=1}^{\phi(n)-1} B_i(\zeta_n^i + \zeta_n^{-i}) + a_1\sum_{i=1}^{\phi(n)-1} B_i(\zeta_n^{i+1} + \zeta_n^{-i+1}) \\ &\quad +a_2\sum_{i=1}^{\phi(n)-1} B_i(\zeta_n^{i+2} + \zeta_n^{-i+2}) + \cdots + a_{\phi(n)-1}\sum_{i=1}^{\phi(n)-1} B_i(\zeta_n^{i+\phi(n)-1} + \zeta_n^{-i+\phi(n)-1}), \end{aligned}$$

and therefore,

$$\begin{aligned} Tr_{\mathbb{K}}(\alpha x\overline{x}) &= Tr_{\mathbb{K}}(\alpha)\sum_{i=0}^{\phi(n)-1} b_i^2 + a_0\sum_{i=1}^{\phi(n)-1} B_i Tr_{\mathbb{K}}(\zeta_n^i+\zeta_n^{-i}) + a_1\sum_{i=1}^{\phi(n)-1} B_i Tr_{\mathbb{K}}(\zeta_n^{i+1}+\zeta_n^{-i+1}) \\ &\quad + a_2\sum_{i=1}^{\phi(n)-1} B_i Tr_{\mathbb{K}}(\zeta_n^{i+2}+\zeta_n^{-i+2}) + \cdots \\ &\quad + a_{\phi(n)-1}\sum_{i=1}^{\phi(n)-1} B_i Tr_{\mathbb{K}}(\zeta_n^{i+\phi(n)-1}+\zeta_n^{-i+\phi(n)-1}). \end{aligned}$$

Since $Tr_{\mathbb{K}}(\zeta_n^k) = Tr_{\mathbb{K}}(\zeta_n^{-k})$, for $k = 0, 1, 2, \ldots, \phi(n)-1$, it follows that

$$\begin{aligned} Tr_{\mathbb{K}}(\alpha x\overline{x}) &= Tr_{\mathbb{K}}(\alpha)\sum_{i=0}^{\phi(n)-1} b_i^2 + 2a_0\sum_{i=1}^{\phi(n)-1} B_i Tr_{\mathbb{K}}(\zeta_n^i) + a_1\sum_{i=1}^{\phi(n)-1} B_i(Tr_{\mathbb{K}}(\zeta_n^{i+1}) + Tr_{\mathbb{K}}(\zeta_n^{i-1})) \\ &\quad + a_2\sum_{i=1}^{\phi(n)-1} B_i(Tr_{\mathbb{K}}(\zeta_n^{i+2}) + Tr_{\mathbb{K}}(\zeta_n^{i-2})) + \cdots \\ &\quad + a_{\phi(n)-1}\sum_{i=1}^{\phi(n)-1} B_i(Tr_{\mathbb{K}}(\zeta_n^{i+\phi(n)-1}) + Tr_{\mathbb{K}}(\zeta_n^{i-\phi(n)+1})). \end{aligned}$$

Therefore,

$$\begin{aligned} Tr_{\mathbb{K}}(\alpha x\overline{x}) &= Tr_{\mathbb{K}}(\alpha)\sum_{i=0}^{\phi(n)-1} b_i^2 + 2a_0\sum_{i=1}^{\phi(n)-1} B_i Tr_{\mathbb{K}}(\zeta_n^i) \\ &\quad + \sum_{i=1}^{\phi(n)-1}\sum_{j=1}^{\phi(n)-1} a_i B_j Tr_{\mathbb{K}}(\zeta_n^{i+j}) + \sum_{i=1}^{\phi(n)-1}\sum_{j=1}^{\phi(n)-1} a_i B_j Tr_{\mathbb{K}}(\zeta_n^{i-j}) \end{aligned}$$

From Equations (1) and (2), it follows that

$$\sum_{i=1}^{\phi(n)-1} B_i Tr_{\mathbb{K}}(\zeta_n^i) = \sum_{i=1}^{\phi(n)-1} B_i\frac{\mu(n/d_i)}{\phi(n/d_i)}\phi(n) = \sum_{k=1}^{\phi(P)-1} B_{\frac{n}{P}k}\frac{\mu(\frac{P}{t_k})}{\phi(\frac{P}{t_k})}\phi(n),$$

where $t_k = \gcd(k, P)$. From Equations (3) and (4), it follows that

$$\sum_{i=1}^{\phi(n)-1}\sum_{j=1}^{\phi(n)-1} a_i B_j Tr_{\mathbb{K}}(\zeta_n^{i-j}) = \sum_{\substack{0\le|i-j|=\frac{nk}{P}\\ 0\le k\le s\\ 1\le i,j\le\phi(n)-1}} a_i B_j\frac{\mu(\frac{P}{t_k})}{\phi(\frac{P}{t_k})}\phi(n),$$

where $t_k = \gcd(k, P)$, $s = \left\lfloor \frac{\phi(P)}{2} - \frac{2P}{n} \right\rfloor$, and

$$\sum_{i=1}^{\phi(n)-1} \sum_{j=1}^{\phi(n)-1} a_i B_j Tr_{\mathbb{K}}(\zeta_n^{i+j}) = \sum_{\substack{i+j=\frac{nk}{P} \\ l \leq k \leq r \\ 1 \leq i,j \leq \phi(n)-1}} a_i B_j \frac{\mu(\frac{P}{t_k})}{\phi(\frac{P}{t_k})} \phi(n),$$

where $t_k = \gcd(k, P)$, $l = \left\lceil \frac{2P}{n} \right\rceil$ and $r = \left\lfloor \phi(P) - \frac{2P}{n} \right\rfloor$. which proves the theorem.

Corollary 2: If $n = 2^r$, where $r \geq 2$, then

$$Tr_{\mathbb{K}}(\alpha x \overline{x}) = \phi(n) \left(a_0 \sum_{i=0}^{\phi(n)-1} b_i^2 - \sum_{i=1}^{\phi(n)-1} a_i B_{m-i} + \sum_{i=1}^{m-1} a_i B_i \right).$$

Proof: From Equation (1), it follows that $Tr_{\mathbb{K}}(\zeta_n^{\phi(n)}) = -\phi(n)$ and $Tr_{\mathbb{K}}(\zeta_n^{\phi(n)+j}) = 0$, for $j = 1, 2, \ldots, m-1$. From Theorem 1, it follows the result.

4 CONSTRUCTION OF ALGEBRAIC LATTICE VIA THE TWISTED HOMORPHISM

Let $\mathbb{K}$ be an algebraic number field of degree n and $\mathcal{O}_{\mathbb{K}}$ be the ring of algebraic integers of $\mathbb{K}$. Let $\sigma_j : \mathbb{K} \to \mathbb{C}$ be the n distinct monomorphisms of $\mathbb{K}$. If $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$, say that σ_j is real, otherwise, σ_j is called imaginary. If all the monomorphisms are reals, $\mathbb{K}$ is called a totally real field and if all the monomorphisms are imaginary, $\mathbb{K}$ is called a totally complex field. If $\varphi : \mathbb{C} \to \mathbb{C}$ is the complex conjugation, then for all $j = 1, 2, \ldots, n$, it follows that $\varphi \circ \sigma_j = \sigma_k$, for some $k = 1, 2, \ldots, n$, and that $\sigma_j = \sigma_k$ if and only if $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$. Hence if r_1 is the number of indices such that $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$, we can ordered the monomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_n$ of such manner that $\sigma_1, \sigma_2, \ldots, \sigma_{r_1}$ are the real monomorphisms and that $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, for $j = 1, 2, \ldots, r_2$. Hence $n - r_1$ is an even number and it can be write as $r_1 + 2r_2 = n$.

Denote $\Re(x)$ and $\Im(x)$, respectively, the real and imaginary parts of $x \in \mathbb{R}$. The twisted canonical homomorphism $\sigma_\alpha : \mathbb{K} \to \mathbb{R}^n$ is defined by

$$\begin{aligned} \sigma_\alpha(x) \;=\; & (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \Re(\sqrt{\alpha_{r_1+1}}\sigma_{r_1+1}(x)), \Im(\sqrt{\alpha_{r_1+1}}\sigma_{r_1+1}(x)), \ldots, \\ & \Re(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x)), \Im(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x))), \end{aligned}$$

for all $\alpha, x \in \mathbb{R}$, $\sigma_j(\alpha) \in \mathbb{R}$ and $\alpha_j = \sigma_j(\alpha) > 0$, for $j = 1, 2, \ldots, r_1 + r_2$. If $\mathcal{M}$ is a $\mathbb{Z}$-module of $\mathbb{K}$ of rank n, the set $\Lambda = \sigma_\alpha(\mathcal{M})$ is an n-dimensional lattice in $\mathbb{R}^n$. If either $r_1 = 0$ or $r_2 = 0$, from Proposition 3.3 of Andrade et al. (2010), the center density of Λ is given by

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

where $\mathcal{D}(\mathbb{K})$ denotes the discriminant of $\mathbb{K}$, $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]$ denotes the index of $\mathcal{M}$ in $\mathcal{O}_{\mathbb{K}}$, and

$$t_\alpha = c_k \cdot \min \{Tr_{\mathbb{K}}(\alpha x \overline{x}) \ : \ x \in \mathcal{M}, x \neq 0\}$$

with $c_k = 1$ or 2^{-1} according to whether $r_2 = 0$ or $r_1 = 0$, respectively. The quantity $2^n \sqrt{N_{\mathbb{K}}(\alpha)|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]$, is equal to the volume of $\sigma_\alpha(\mathcal{M})$.

Next we present some examples of algebraic lattices with optimal center density, where a table of lattices with optimal center density can be found in the work of Conway and Sloane (1998).

Example 1: If $\mathbb{K} = \mathbb{Q}(\zeta_6)$, where ζ_6 is a primitive 6-th root of unity, $\alpha = 3$ and $\mathcal{M} = (1 + 2\zeta_6)\mathcal{O}_{\mathbb{K}}$ is an ideal of $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_6]$, then $[\mathbb{K} : \mathbb{Q}] = 2$, $\mathcal{D}(\mathbb{K}) = -3$, $N_{\mathbb{K}}(\alpha) = 9$ and $N_{\mathbb{K}}(\mathcal{M}) = 7$. If $x \in \mathcal{M}$, then $x = (a_0 + a_1\zeta_6)(1 + 2\zeta_6)$, with $a_0, a_1 \in \mathbb{Z}$, and thus $Tr_{\mathbb{K}}(\alpha x \overline{x}) = 42(a_0^2 + a_0a_1 + a_1^2)$. Therefore, $t_\alpha = min\{Tr_{\mathbb{K}}(\alpha x \overline{x}) : x \in \mathcal{M}, x \neq 0\} = 42$, with $a_0 = 1$ and $a_1 = 0$, and the center density of the lattice $\sigma_\alpha(\mathcal{M})$ is given by

$$\delta(\Lambda) = \frac{t_\alpha^{2/2}}{2^2 \sqrt{N_{\mathbb{K}}(\alpha)|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]} = \frac{1}{2\sqrt{3}},$$

which is the optimal center density for this dimension, i.e., with the same center density of the lattice Λ_2.

Example 2: If $\mathbb{K} = \mathbb{Q}(\zeta_8)$, where ζ_8 is a primitive 8-th root of unity, $\alpha = 2 - \zeta_8 + \zeta_8^3$ and $\mathcal{M} = (-12\zeta_8^2 + \zeta_8^3)\mathcal{O}_{\mathbb{K}}$ is an ideal of $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_8]$, then $[\mathbb{K} : \mathbb{Q}] = 4$, $\mathcal{D}(\mathbb{K}) = 256$, $N_{\mathbb{K}}(\alpha) = 4$ and $N_{\mathbb{K}}(\mathcal{M}) = 1$. If $x \in \mathcal{M}$, then $x = (a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3)(-1 + \zeta_8 + \zeta_8^3)$, with $a_0, a_1, a_2, a_3 \in \mathbb{Z}$, and thus $Tr_{\mathbb{K}}(\alpha x \overline{x}) = 8(a_0^2 + a_0a_1 - a_0a_3 + 3a_1^2 + a_1a_2 - 2a_1a_3 + a_2^2 + a_2a_3 + a_3^2)$. Therefore, $t_\alpha = min\{Tr_{\mathbb{K}}(\alpha x \overline{x}) : x \in \mathcal{M}, x \neq 0\} = 8$, with $a_0 = 1$ and $a_1 = a_2 = a_3 = 0$, and the center

density of the lattice $\sigma_\alpha(\mathcal{M})$ is given by

$$\delta(\Lambda) = \frac{t_\alpha^{4/2}}{2^4\sqrt{N_{\mathbb{K}}(\alpha)|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]} = \frac{1}{8},$$

which is the optimal center density for this dimension, i.e., with the same center density of the lattice Λ_4.

Example 3 If $\mathbb{K} = \mathbb{Q}(\zeta_9)$, where ζ_9 is a primitive 9-th root of unity, $\alpha = 5 - 5\zeta_9 + 5\zeta_9^2 - 2\zeta_9^4 + 3\zeta_9^5$ and $\mathcal{M} = (1 - \zeta_9 - \zeta_9^3 + \zeta_9^4)\mathcal{O}_{\mathbb{K}}$ is an ideal of $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_9]$, then $[\mathbb{K} : \mathbb{Q}] = 6$, $\mathcal{D}(\mathbb{K}) = 3^9$, $N_{\mathbb{K}}(\alpha) = 9$ and $N_{\mathbb{K}}(\mathcal{M}) = 81$. If $x \in \mathcal{M}$, then $x = (a_0 + a_1\zeta_9 + a_2\zeta_9^2 + a_3\zeta_9^3 + a_4\zeta_9^4 + a_5\zeta_9^5)(1 - \zeta_9 - \zeta_9^3 + \zeta_9^4)$, with $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}$, and thus $Tr_{\mathbb{K}}(\alpha x\overline{x}) = 177a_0^2 - 243a_0a_1 + 207c_0c_2 - 153a_0a_3 - 24a_0a_4 + 60a_0a_5 + 177a_1^2 - 219a_1a_2 + 231a_1a_3 - 153a_1a_4 - 24a_1a_5 + 147a_2^2 - 231a_2a_3 + 213a_2a_4 - 129a_2a_5 + 165a_3^2 - 249a_3a_4 + 237a_3a_5 + 165a_4^2 - 249a_4a_5 + 165a_5^2$. Therefore, $t_\alpha = min\{Tr_{\mathbb{K}}(\alpha x\overline{x}) : x \in \mathcal{M}, x \neq 0\} = 54$, with $a_0 = a_4 = -1$, $a_1 = a_2 = 0$, $a_3 = -2$ and $a_5 = 1$, and the center density of the lattice $\sigma_\alpha(\mathcal{M})$ is given by

$$\delta(\Lambda) = \frac{t_\alpha^{6/2}}{2^6\sqrt{N_{\mathbb{K}}(\alpha)|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]} = \frac{1}{8\sqrt{3}},$$

which is the optimal center density for this dimension, i.e., with the same center density of the lattice Λ_6.

Example 4: If $\mathbb{K} = \mathbb{Q}(\zeta_{20})$, where ζ_{20} is a primitive 20-th root of unity, $\alpha = 3 - 2\zeta_{20} + \zeta_{20}^3 + \zeta_{20}^4 - \zeta_{20}^5 - \zeta_{20}^6 + \zeta_{20}^7$ and $\mathcal{M} = (1 - 2\zeta_{20} - \zeta_{20}^5 + 2\zeta_{20}^7)\mathcal{O}_{\mathbb{K}}$ is an ideal of $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{20}]$, then $[\mathbb{K} : \mathbb{Q}] = 8$, $\mathcal{D}(\mathbb{K}) = 2^8 5^6$, $N_{\mathbb{K}}(\alpha) = 25$ and $N_{\mathbb{K}}(\mathcal{M}) = 16$. If $x \in \mathcal{M}$, then $x = (c_0 + c_1\zeta_{20} + c_2\zeta_{20}^2 + c_3\zeta_{20}^3 + c_4\zeta_{20}^4 + c_5\zeta_{20}^5 + c_6\zeta_{20}^6 + c_7\zeta_{20}^7)(1 - 2\zeta_{20} - \zeta_{20}^5 + 2\zeta_{20}^7)$, with $c_0, c_1, \ldots, c_7 \in \mathbb{Z}$, and thus $Tr_{\mathbb{K}}(\alpha x\overline{x}) = 240c_0^2 - 360c_0c_1 + 336c_0c_2 - 208c_0c_3 + 104c_0c_4 + 48c_0c_5 - 160c_0c_6 + 272c_0c_7 + 176c_1^2 - 344c_1c_2 + 288c_1c_3 - 144c_1c_4 + 120c_1c_5 + 64c_1c_6 - 160c_1c_7 + 12c_1 + 176c_2^2 - 336c_2c_3 + 288c_2c_4 - 152c_2c_5 + 120c_2c_6 + 48c_2c_7 + 168c_3^2 - 304c_3c_4 + 288c_3c_5 - 144c_3c_6 + 104c_3c_7 - 12c_3 + 168c_4^2 - 336c_4c_5 + 288c_4c_6 - 208c_4c_7 + 176c_5^2 - 344c_5c_6 + 336c_5c_7 - 24c_5 + 176c_6^2 - 360c_6c_7 + 12c_6 + 240c_7^2 - 24c_7$. Therefore, $t_\alpha = min\{Tr_{\mathbb{K}}(\alpha x\overline{x}) : x \in \mathcal{M}, x \neq 0\} = 40$, with $c_0 = c_1 = c_2$, $c_3 = c_7 = 0$,

$c_4 = c_5 = c_6 = 1$, and the center density of the lattice $\sigma_\alpha(\mathcal{M})$ is given by

$$\delta(\Lambda) = \frac{t_\alpha^{8/2}}{2^8\sqrt{N_{\mathbb{K}}(\alpha)|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]} = \frac{1}{16},$$

which is the optimal center density for this dimension, i.e., with the same center density of the lattice Λ_8.

Example 5: If $\mathbb{K} = \mathbb{Q}(\zeta_{20})$, where ζ_{20} is a primitive 20-th root of unity, $\alpha = 3 - 2\zeta_{20} + \zeta_{20}^3 + \zeta_{20}^4 - \zeta_{20}^5 - \zeta_{20}^6 + \zeta_{20}^7$ and $\mathcal{M} = (1 - 2\zeta_{20} - \zeta_{20}^5 + 2\zeta_{20}^7)\mathcal{O}_{\mathbb{K}}$ is an ideal of $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{20}]$, then $[\mathbb{K} : \mathbb{Q}] = 8$, $\mathcal{D}(\mathbb{K}) = 2^8 5^6$, $N_{\mathbb{K}}(\alpha) = 25$ and $N_{\mathbb{K}}(\mathcal{M}) = 16$. If $x \in \mathcal{M}$, then $x = (c_0 + c_1\zeta_{20} + c_2\zeta_{20}^2 + c_3\zeta_{20}^3 + c_4\zeta_{20}^4 + c_5\zeta_{20}^5 + c_6\zeta_{20}^6 + c_7\zeta_{20}^7)(1 - 2\zeta_{20} - \zeta_{20}^5 + 2\zeta_{20}^7)$, with $c_0, c_1, \ldots, c_7 \in \mathbb{Z}$, and thus $Tr_{\mathbb{K}}(\alpha x\overline{x}) = 240c_0^2 - 360c_0c_1 + 336c_0c_2 - 208c_0c_3 + 104c_0c_4 + 48c_0c_5 - 160c_0c_6 + 272c_0c_7 + 176c_1^2 - 344c_1c_2 + 288c_1c_3 - 144c_1c_4 + 120c_1c_5 + 64c_1c_6 - 160c_1c_7 + 12c_1 + 176c_2^2 - 336c_2c_3 + 288c_2c_4 - 152c_2c_5 + 120c_2c_6 + 48c_2c_7 + 168c_3^2 - 304c_3c_4 + 288c_3c_5 - 144c_3c_6 + 104c_3c_7 - 12c_3 + 168c_4^2 - 336c_4c_5 + 288c_4c_6 - 208c_4c_7 + 176c_5^2 - 344c_5c_6 + 336c_5c_7 - 24c_5 + 176c_6^2 - 360c_6c_7 + 12c_6 + 240c_7^2 - 24c_7$. Therefore, $t_\alpha = min\{Tr_{\mathbb{K}}(\alpha x\overline{x}) : x \in \mathcal{M}, x \neq 0\} = 40$, with $c_0 = c_1 = c_2$, $c_3 = c_7 = 0$, $c_4 = c_5 = c_6 = 1$, and the center density of the lattice $\sigma_\alpha(\mathcal{M})$ is given by

$$\delta(\Lambda) = \frac{t_\alpha^{8/2}}{2^8\sqrt{N_{\mathbb{K}}(\alpha)|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]} = \frac{1}{16},$$

which is the optimal center density for this dimension, i.e., with the same center density of the lattice Λ_8.

5 CONCLUSION

In this work, we presented the integral trace form $Tr_{\mathbb{K}}(\alpha x\overline{x})$, with $\alpha, x \in \mathcal{O}_{\mathbb{K}}$, where $\mathbb{K} = \mathbb{Q}(\zeta_n)$ is the nth cyclotomic field. The integral trace form was presented in an explicit manner, amenable to computations. Based on examples which we presented, onde possibility for future work involves minimizing the integral form trace in modules or ideals in order to construct lattices with high center densities.

ACKNOWLEDGMENTS

The authors thank the referees for your careful work and the suggestions that greatly improve the presentation of the paper. This work was supported by Fapesp 2013/25977-7 and Capes Print Unesp.

REFERENCES

Andrade, A. A., Ferrari, A. J., Benedito, C. W. O., and Costa, S. I. R. (2010). Constructions of algebraic lattices. *Computational & Applied Mathematics*, *22*(3), 493-505.

Conway, J. H. and Sloane, N. J. A. (1998). *Sphere packings, latices and groups*. Springer-Verlag, 2nd edition.

Ferrari, A. J., Andrade, A. A., Araujo, R. R., and Interlando, J. C. (2020). Trace form of certain subfields of cyclotomic fields and applications. *Journal of Algebra Combinatorics Discrete Structures and Applications*, *7*(2), 141-160.

Interlando, J. C., Neto, T. P. N., Rodrigues, T. M., and Lopes, J. O. D. (2015). A note on the integral trace form in cyclotomic fields. *Jounal of Algebra and Applications*, *25*(5), 1550045-53.

Author contributions

1 – Antonio Aparecido de Andrade
PhD in Electrial Engineering. Professor at Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, campus São José do Rio Preto.
https://orcid.org/0000-0001-6452-2236 • antonio.andrade@unesp.br
Contribution: Conceptualization – Investigation – Resources – Project Administration – Writing - Original Draft

2 – Agnaldo José Ferrari
PhD in Applied Mathematics at Universidade de Campinas. Professor at Faculdade de Ciências, Universidade Estadual Paulista, Campus Bauru.
https://orcid.org/0000-0002-1422-1416 • agnaldo.ferrari@unesp.br
Contribution: Conceptualization – Formal Analysis – Methodology – Writing - Review & Editing

How to cite this article

Andrade, A. A. de, & Ferrari, A. J. (2024). Trace form via cyclotomic fields. *Ciência e Natura*, Santa Maria, v. 46, e85207, 2024. https://doi.org/10.5902/2179460X85207