Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 11, n. 1, 2025.

Trabalho apresentado no XLIII CNMAC, Centro de Convenções do Armação Resort - Porto de Galinhas - PE, 2024

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Reticulados Ideais Bem-arredondados via Subcorpos Ciclotômicos Maximais Reais de Condutor $4p$, com $p > 2$ Primo

João E. Strapasson[1]
FCA/Unicamp, Limeira, SP
Robson R. de Araujo[2]
IFSP, Catanduva, SP

Resumo. Reticulados são subgrupos aditivos discretos de $\mathbb{R}^n$ frequentemente requisitados na busca de soluções por problemas matemáticos diversos, tais como o do empacotamento esférico, e para aplicações em transmissão e segurança de dados. Em particular, os reticulados bem-arredondados têm sido aplicados na transmissão de sinais em canais Wiretap. Em diversos casos, reticulados podem ser obtidos como imagens de ideais em anéis de inteiros de corpos de números via o mergulho canônico ou algum mergulho torcido - são os chamados reticulados ideais. Em 2012, Fukshansky e Petersen provaram que a imagem do anel de inteiros de um corpo de números K através do mergulho canônico σ_K é um reticulado bem-arredondado se, e somente se, K é ciclotômico. Neste trabalho, provamos que, ao utilizar um certo mergulho torcido σ_α ao invés de σ_K, a imagem do anel de inteiros do subcorpo ciclotômico maximal real $\mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$ através de σ_α é bem-arredondado para qualquer primo ímpar p, em que ζ_{4p} denota a $4p$-ésima raiz primitiva da unidade.

Palavras-chave. Reticulados, Reticulados Bem-arredondados, Reticulados Ideais, Subcorpos Maximais reais, Mergulho Torcido, Canais Wiretap.

1 Introdução

Nas últimas décadas, têm sido frequente o uso de reticulados aplicados a diversos tipos de canais de comunicação para transmissão de sinais, tais como canais gaussianos e Rayleigh com desvanecimento [3]. Recentemente, reticulados têm ganhado ainda mais notoriedade com o avanço dos estudos sobre criptografia pós-quântica, já que são baseados neles os atualmente mais recomendados criptossistemas considerados seguros mesmo sob ataques quânticos - tais como o CRYSTALS-Kyber, como certificou a agência norte-americana de regulamentação NIST [2, 12, 13]. Reticulados podem ser definidos como o conjunto de todas as $\mathbb{Z}$-combinações lineares de $m \leq n$ vetores linearmente independentes em $\mathbb{R}^n$, o que é equivalente a dizer que eles são subgrupos discretos aditivos de $\mathbb{R}^n$. Neste trabalho, consideraremos apenas o caso em que $m = n$, ao que chamamos de reticulados de posto completo.

Diversas vezes, reticulados podem ser obtidos algebricamente como imagens de ideais em anéis de inteiros de corpos de números. Sendo $\mathbb{K}$ um corpo de números de grau n, $\mathcal{O}_\mathbb{K}$ seu anel de inteiros e $\sigma_1, \sigma_2, \ldots, \sigma_n : \mathbb{K} \longrightarrow \mathbb{C}$ os únicos n monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, define-se o mergulho canônico associado a $\mathbb{K}$ como sendo o monomorfismo $\sigma_\mathbb{K} : \mathbb{K} \longrightarrow \mathbb{C}^n$ dado por $\sigma_\mathbb{K}(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x))$. Dessa forma, para qualquer ideal I de $\mathcal{O}_\mathbb{K}$, é fato que $\sigma_\mathbb{K}(I)$ pode ser visto como um reticulado em $\mathbb{R}^n$ de posto completo. De maneira mais geral, sendo $\alpha \in \mathbb{K}$ um número totalmente positivo, isto

[1]strapass@unicamp.br
[2]robson.ricardo@ifsp.edu.br

é, tal que $\alpha_i := \sigma_i(\alpha) > 0$ para todo $i = 1, 2, \ldots, n$, define-se o mergulho torcido $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{C}^n$ por $\sigma_\alpha(x) := \left\langle \left(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_n}\right), \sigma_{\mathbb{K}}(x) \right\rangle$, do que se obtém também que $\sigma_\alpha(I)$ é um reticulado de posto completo em $\mathbb{R}^n$ para qualquer ideal I de $\mathcal{O}_{\mathbb{K}}$. Os reticulados $\sigma_{\mathbb{K}}(I)$ e $\sigma_\alpha(I)$ são chamados de reticulados ideais (ou algébricos). Diversos reticulados notáveis podem ser realizados através de reticulados ideais, o que favorece sua aplicação a canais do tipo Rayleigh com desvanecimento, principalmente quando $\mathbb{K}$ é um corpo totalmente real (isto é, quando $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$ para todo $i = 1, 2, \ldots, n$) [1, 11, 14, 18].

Se $\Lambda \subseteq \mathbb{R}^n$ é um reticulado de posto completo, a menor norma entre as normas de todos os elementos de $\Lambda \setminus \{0\}$ é chamada de norma mínima de Λ e é denotada por λ_1. O conjunto dos vetores de norma mínima em Λ, isto é, dos elementos $v \in \Lambda$ tais que $\|v\| = \lambda_1$, é denotado por $S(\Lambda)$. O reticulado Λ é dito ser bem-arredondado se o conjunto $S(\Lambda)$ gera $\mathbb{R}^n$ (isto é, se existem n vetores de norma mínima linearmente independentes em Λ). Por exemplo, reticulados notáveis, tais como $\mathbb{Z}^n$, A_n, D_n, E_8 e Λ_{24}, são bem-arredondados. Reticulados bem-arredondados têm sido sugeridos como boas alternativas para uso em canais Wiretap, MIMO e SISO [6, 9, 15].

Em [8] foi feito um estudo pioneiro sobre a realização algébrica de reticulados bem-arredondados. Nesse artigo, Fukshansky e Petersen fazem um estudo sobre reticulados ideais obtidos como imagem de anéis de inteiros de corpos de números quadráticos e provam que $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é um reticulado bem-arredondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico (isto é, $\mathbb{K} = \mathbb{Q}(\zeta_n)$, em que ζ_n é uma raiz n-ésima primitiva da unidade). Em trabalhos posteriores, outros reticulados bem-arredondados são construídos através de submódulos de anéis de inteiros de outros corpos de números, tal como em [7]. A partir dessa literatura, uma questão que emerge é a seguinte: dado um corpo de números $\mathbb{K}$ qualquer, é possível garantir a existência de um elemento positivo α tal que o reticulado ideal $\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ é bem-arredondado? Como comentado acima, a partir de [8] pode-se compreender que, se $\mathbb{K}$ é ciclotômico, então a resposta à pergunta acima é positiva (basta usar $\alpha = 1$). Neste trabalho, nosso principal objetivo é mostrar que, se $\mathbb{K}$ é um subcorpo ciclotômico maximal real com condutor $4p$ (em que p é um primo ímpar), isto é, se $\mathbb{K} = \mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$, então existe α totalmente positivo tal que $\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ é bem-arredondado.

2 Preliminares

Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado de posto completo. Chamamos de base de Λ a qualquer conjunto linearmente independente $B = \{u_1, u_2, \ldots, u_n\} \subseteq \Lambda$ tal que $\Lambda = \sum_{i=1}^n \mathbb{Z}u_i$. Dada uma base $B = \{u_1, u_2, \ldots, u_n\}$ de Λ, chamamos de matriz de Gram de Λ à matriz $\mathbf{G} = [\langle u_i, u_j \rangle]_{n \times n}$, em que $\langle ., . \rangle$ denota o produto interno usual em $\mathbb{R}^n$. É fato que o determinante das matrizes de Gram de um reticulado é invariante por mudança de base. Assim, definimos o volume de Λ como sendo $\mathrm{Vol}(\Lambda) := \sqrt{\det(\mathbf{G})}$ (mais detalhes em [4, 5]).

Dois reticulados Λ_1 e Λ_2 são ditos equivalentes se um pode ser obtido do outro a partir de uma reflexão, de uma rotação e de uma dilatação, ao que denotamos por $\Lambda_1 \sim \Lambda_2$. De outra forma, $\Lambda_1 \sim \Lambda_2$ se, e somente se, existem uma constante $c > 0$ e uma matriz unimodular $\mathbf{U}$ tais que $\mathbf{G}_1 = c\mathbf{U}^T\mathbf{G}_2\mathbf{U}$, em que cada $\mathbf{G}_i$ denota uma matriz de Gram de Λ_i e $\mathbf{A}^T$ indica a transposição da matriz $\mathbf{A}$ [5]. A partir da definição de equivalência entre reticulados compreende-se que, se $\Lambda_1 \sim \Lambda_2$ e Λ_1 é um reticulado bem-arredondado, então Λ_2 também é bem-arredondado.

Um corpo de números $\mathbb{K}$ de grau $[\mathbb{K} : \mathbb{Q}] = n$ é um corpo que constitui-se como $\mathbb{Q}$-espaço vetorial de dimensão n. Os elementos de $\mathbb{K}$ que são raízes de um polinômio mônico $p(x) \in \mathbb{Z}[x]$ são chamados de inteiros algébricos e formam um anel $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{K}$ chamado de anel de inteiros de $\mathbb{K}$. É fato que qualquer ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ pode ser escrito como uma $\mathbb{Z}$-combinação linear de n elementos em $\mathcal{O}_{\mathbb{K}}$, os quais formam uma $\mathbb{Z}$-base do ideal. Em particular, uma $\mathbb{Z}$-base do anel de inteiros é chamada de base integral de $\mathbb{K}$. Como descrito na Introdução, existem exatamente n monomorfismos $\sigma_i : \mathbb{K} \longrightarrow \mathbb{C}$, com $i = 1, 2, \ldots, n$. Desses monomorfismos, existem $r_1 \geq 0$ tais

que $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$, aos quais chamamos de monomorfismos reais de $\mathbb{K}$. Os monomorfismos restantes dividem-se em pares conjugados entre si e são chamados de monomorfismos complexos de $\mathbb{K}$. Logo, $n - r_1 = 2r_2$, em que $r_2 \geq 0$. O par (r_1, r_2) é chamado de assinatura de $\mathbb{K}$. Se $\mathbb{K}$ tem assinatura $(r_1, 0)$, dizemos que ele é totalmente real. Se $\mathbb{K}$ tem assinatura $(0, r_2)$, dizemos que ele é totalmente complexo. É fato que, se $\mathbb{K}/\mathbb{Q}$ é uma extensão galoisiana, então $\mathbb{K}$ é totalmente real ou totalmente complexo [16, 17].

Se $\{b_1, b_2, \ldots, b_n\}$ é uma base integral de $\mathbb{K}$, define-se o discriminante desse corpo de números como sendo $\Delta_{\mathbb{K}} = \det\left[\sigma_i(b_j)\right]_{n\times n}^2$ - o qual é invariante por mudança de base integral. Sendo (r_1, r_2) a assinatura de $\mathbb{K}$, reordenemos os n monomorfismos de $\mathbb{K}$ colocando $\sigma_1, \ldots, \sigma_{r_1}$ como sendo os monomorfismos reais, $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r2}$ como sendo monomorfismos complexos não conjugados entre si e $\sigma_{r_1+r_2+1}, \ldots, \sigma_n$ como sendo os restantes. Dessa forma, podemos redefinir o mergulho canônico $\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^n$ da seguinte forma, para qualquer $x \in \mathbb{K}$:

$$\sigma_{\mathbb{K}}(x) := (\sigma_1(x), \ldots, \sigma_{r_1}(x), \mathfrak{Re}(\sigma_{r_1+1}(x)), \mathfrak{Im}(\sigma_{r_1+1}(x)), \ldots, \mathfrak{Re}(\sigma_{r_1+r_2}(x)), \mathfrak{Im}(\sigma_{r_1+r_2}(x))), \quad (1)$$

em que $\mathfrak{Re}(.)$ e $\mathfrak{Im}(.)$ denotam, respectivamente, a parte real e a parte imaginária do número complexo. Assim, é fato que, para qualquer ideal $I \neq \{0\}$ de $\mathcal{O}_{\mathbb{K}}$, o conjunto $\sigma_{\mathbb{K}}(I)$ é um reticulado de posto completo em $\mathbb{R}^n$, ao qual chamamos de reticulado ideal. Tal reticulado tem volume igual a $2^{-r_2}[\mathcal{O}_{\mathbb{K}} : I]\sqrt{|\Delta_{\mathbb{K}}|}$. Além disso, se $\mathbb{K}$ é totalmente real ou totalmente complexo, então $\|\sigma_{\mathbb{K}}(x)\|^2 = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x})$, para qualquer $x \in \mathbb{K}$ ([17]).

Por sua vez, nas notações acima, dado um elemento $\alpha \in \mathbb{K}$ totalmente positivo (isto é, tal que $\alpha_i := \sigma_i(\alpha) > 0$ para todo $i = 1, \ldots, n$), o mergulho torcido $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ pode ser definido como

$$\sigma_\alpha(x) := \left\langle \left(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_{r_1}}, \sqrt{2\alpha_{r_1+1}}, \sqrt{2\alpha_{r_1+1}}, \ldots, \sqrt{2\alpha_{r_1+r_2}}, \sqrt{2\alpha_{r_1+r_2}}\right), \sigma_{\mathbb{K}}(x) \right\rangle. \quad (2)$$

A imagem de qualquer ideal $I \neq \{0\}$ em $\mathcal{O}_{\mathbb{K}}$ é um reticulado de posto completo em $\mathbb{R}^n$, ao qual também chamamos de reticulado ideal. Neste caso, o volume de $\sigma_\alpha(I)$ é ao igual ao produto do volume de $\sigma_{\mathbb{K}}(I)$ pela raiz quadrada da norma algébrica de α na extensão $\mathbb{K}/\mathbb{Q}$. Além disso, se $\mathbb{K}$ é totalmente real ou totalmente complexo, então $\|\sigma_\alpha(x)\|^2 = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha x\overline{x})$, para qualquer $x \in \mathcal{O}_{\mathbb{K}}$. Neste caso, se $\{b_1, b_2, \ldots, b_n\}$ é uma $\mathbb{Z}$-base do ideal I, então uma matriz de Gram de $\sigma_\alpha(I)$ pode ser calculada como $\mathbf{G} = \left[\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha b_i b_j)\right]_{n\times n}$ ([14]).

Sejam $m > 2$ um inteiro qualquer e ζ_m uma raiz m-ésima primitiva da unidade. Denotemos por $\mathbb{L} = \mathbb{Q}(\zeta_m)$ o corpo ciclotômico com índice m, o qual tem grau $\varphi(m)$ (onde φ denota a função totiente de Euler), e por $\mathbb{K} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ o subcorpo maximal real de condutor m, o qual tem grau $\varphi(m)/2$. Tal denominação é adequada porque $\mathbb{K}$ é o maior corpo contido em $\mathbb{L} \cap \mathbb{R}$. São fatos conhecidos, tal como pode ser encontrado em [16], que $\mathbb{K}/\mathbb{Q}$ e $\mathbb{L}/\mathbb{Q}$ são extensões galoisianas e que os anéis de inteiros desses corpos são $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_m]$ e $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_m + \zeta_m^{-1}]$ (a notação $\mathbb{Z}[\theta]$ indica que tal anel tem como $\mathbb{Z}$-base o conjunto $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$, onde n é o grau do corpo). Em [10, Lemma 4] encontra-se demonstrado que, para qualquer $k = 1, 2, \ldots, m-1$,

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_m^k) = \frac{\varphi(m)\mu(m/d)}{\varphi(m/d)}, \quad (3)$$

em que $d = \mathrm{mdc}(m, k)$ e μ denota a função de Möbius.

Consideremos o caso particular em $m = 4p$, onde p é um número primo ímpar, ou seja, $\mathbb{K} = \mathbb{Q}\left(\zeta_{4p} + \zeta_{4p}^{-1}\right)$. Neste caso, o grau de $\mathbb{K}$ é $n = p - 1$. Denotemos $e_0 := 1$ e, para cada $i = 0, 1, \ldots, \varphi(m)/2 - 1$, $e_i := \zeta_m^i + \zeta_m^{-i}$. Os lemas seguintes afirmam que tais e_i são uma base integral de $\mathbb{K}$ e apresentam algumas de suas propriedades:

Lema 2.1. *Nas condições acima,* $\{e_0, e_1, \ldots, e_{p-2}\}$ *é uma base integral de* $\mathbb{K}$. *Dados* $i, j \in \{0, 1, \ldots, p-2\}$, *tal base satisfaz a seguinte propriedade:*

$$e_i e_j = \begin{cases} e_i & j = 0 \\ e_{2i} + 2 & se\ i = j > 0 \\ e_{i-j} + e_{i+j} & se\ i > j > 0 \end{cases}. \tag{4}$$

Demonstração. Primeiramente vamos mostrar as propriedades: i) $e_i e_0 = e_i\, 1 = e_i$; ii) Se $i = j > 0$ temos que $e_i e_i = (\zeta_m^i + \zeta_m^{-i})(\zeta_m^i + \zeta_m^{-i}) = \zeta_m^i \zeta_m^i + \zeta_m^i \zeta_m^{-i} + \zeta_m^{-i} \zeta_m^i + \zeta_m^{-i} \zeta_m^{-i} = \zeta_m^{2i} + \zeta_m^{-2i} + 2 = e_{2i} + 2$; iii) Se $i > j > 0$ temos que $e_i e_j = (\zeta_m^i + \zeta_m^{-i})(\zeta_m^j + \zeta_m^{-j}) = \zeta_m^i \zeta_m^j + \zeta_m^i \zeta_m^{-j} + \zeta_m^{-i} \zeta_m^j + \zeta_m^{-i} \zeta_m^{-j} = \zeta_m^{i+j} + \zeta_m^{-(i+j)} + \zeta_m^{i-j} + \zeta_m^{-(i-j)} = e_{i+j} + e_{i-j}$. Agora vamos mostrar que $\beta' = \{e_i\}_{i=0,\ldots,n-1}$ é base, onde $n = p-1$, e para isso é suficiente mostrar que β' gera o anel de inteiros de $\mathbb{K}$ (a independência linear é trivial). Faremos isso por indução no k-ésimo elemento da base de potências $\beta = \{e_1^i\}_{i=0,\ldots,n-1}$. Vamos mostrar que ele pode ser escrito como combinação linear da base β'. Para $k = 0, 1$ é trivial. Assuma que vale para algum valor k, isto é, $e_1^k = \sum_{i=0}^{k} a_i e_i$, assim $e_1^{k+1} = e_1 e_1^k = e_1 \sum_{i=0}^{k} a_i e_i = a_0 e_1 + a_1 e_1^2 + a_2 e_2 e_1 + \cdots a_k e_k e_1 = a_0 e_1 + a_1(2 + e_2) + a_2(e_1 + e_3) + \cdots a_k(e_{k-1} + e_{k+1}) = \sum_{i=0}^{k+1} b_i e_i$. □

Lema 2.2. *Nas condições acima, sendo* $k \in \{0, 1, \ldots, p-2\}$, *temos:*

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(e_k) = \begin{cases} p-1 & se\ k = 0 \\ 0 & se\ k \equiv 1 \pmod 2 \\ -2 & se\ k \equiv 0 \pmod 4\ e\ k \neq 0 \\ 2 & se\ k \equiv 2 \pmod 4 \end{cases}. \tag{5}$$

Demonstração. Como $e_0 = 1$, então $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(e_0) = [\mathbb{K} : \mathbb{Q}] = p-1$. Se $k > 0$, segue da transitividade do traço e de (3) que

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(e_k) = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\zeta_{4p}^k + \zeta_{4p}^{-k}) = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\zeta_{4p}^k)) = \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(\zeta_{4p}) = \frac{\varphi(4p)\mu(4p/d)}{\varphi(4p/d)}, \tag{6}$$

em que $d = \mathrm{mdc}(4p, k)$. Como $0 < k < p$, então p não divide k. Logo, se $k \equiv 1 \pmod 2$, então $\mathrm{mdc}(4p, k) = 1$. Disso segue que $\mu(4p/\mathrm{mdc}(4p, k)) = \mu(4p) = 0$ e, por (6), $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(e_k) = 0$. Por sua vez, se $k \not\equiv 1 \pmod 2$, então $k \equiv 0 \pmod 4$ (caso I) ou $k \equiv 2 \pmod 4$ (caso II). No caso I, como p não divide k, tem-se $\mathrm{mdc}(4p, k) = p$ e, por (6), então $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(e_k) = 2(p-1)(-1)/(p-1) = -2$. No caso II, ocorre $\mathrm{mdc}(4p, k) = 2p$ e, então, por (6), $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(e_k) = 2(p-1)/(p-1) = 2$. □

3 Resultados Principais

Sejam $\mathbb{K} = \mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$, em que p é um primo ímpar, e $n = p-1$ o grau de $\mathbb{K}$. Consideremos aqui as notações utilizadas na Seção 2. Denotemos $\alpha := 2 + e_1$. Nesta seção, nosso objetivo é mostrar que $\Lambda = \sigma_\alpha(\mathcal{O}_\mathbb{K})$ é equivalente ao reticulado ideal obtido como imagem do anel de inteiros de um corpo ciclotômico através do mergulho canônico, e que, consequentemente, Λ é bem-arredondado.

Consideremos aqui outra base integral $\{v_0, v_1, \ldots, v_{n-1}\}$ para o corpo $\mathbb{K}$, obtida a partir da base $\{e_0, e_1, \ldots, e_{n-1}\}$ por uma matriz de mudança de base triangular unitária:

$$v_i = \sum_{j=0}^{i} (-1)^j e_j, \qquad i = 0, 1, \ldots, p-2. \tag{7}$$

A base definida acima tem propriedades enunciadas no lema a seguir, cuja demonstração será omitida, mas que pode ser feita utilizando as propriedades do Lema 2.1:

Lema 3.1. *Nas condições acima, sendo $\alpha = 2 + e_1$, para cada $i = 0, 1, \ldots, p-2$, temos que*

$$\alpha v_i = \begin{cases} 2 + e_1 & se\ i = 0 \\ (-1)^i (e_i + e_{i+1}) & se\ i \neq 0 \end{cases}. \tag{8}$$

Consequentemente,

$$\alpha v_i v_j = \begin{cases} (-1)^{i-j}(e_{i-j} + e_{i+j+1}) & se\ i > j \\ 2 + e_{2i+1} & se\ i = j \end{cases}. \tag{9}$$

Sendo $\mathbb{L} = \mathbb{Q}(\zeta_p)$ o corpo ciclotômico de índice p, é fato conhecido (como apontado em [4, Seção 7.3]) que

$$\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}}) \sim A_{p-1}^*, \tag{10}$$

em que A_{p-1}^* denota o reticulado dual de $A_{p-1} = \{(x_0, x_1, \ldots, x_{p-1}) \in \mathbb{Z}^m \ : \ x_0 + x_1 + \ldots + x_{p-1} = 0\}$. Também é sabido (como citado em [4, Seção 6.6]) que uma matriz de Gram de A_{p-1}^* é dada por $\mathbf{G} = [a_{ij}]_{(p-1)\times(p-1)}$, em que

$$a_{ij} = \begin{cases} p-1 & se\ i = j \\ -1 & se\ i \neq j \end{cases}. \tag{11}$$

A seguir, considere $w_i := (-1)^{\lfloor \frac{i}{2} \rfloor} v_i$ para cada $i = 0, 1, \ldots, n-1$. Como $\{v_1, v_2, \ldots, v_n\}$ é uma base integral de $\mathbb{K}$, então $\{w_1, w_2, \ldots, w_n\}$ também é.

Teorema 3.1. *Nas notações acima,*

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha w_i w_j) = \begin{cases} 2(p-1) & se\ i = j \\ -2 & se\ i \neq j \end{cases}. \tag{12}$$

Então $\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ é equivalente ao reticulado $\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})$, em que $\mathbb{L} := \mathbb{Q}(\zeta_p)$.

Demonstração. Se $i = j$, segue do Lema 3.1 que $\alpha v_i^2 = 2 + e_{2i+1}$. Disso e do Lema 2.2, concluímos que $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha w_i^2) = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha v_i^2) = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(2) = 2(p-1)$. Se $i \neq j$, o Lema 3.1 implica que $\alpha v_i v_j = (-1)^{j-i}(e_{j-i} + e_{i+j+1})$, ou seja,

$$\alpha w_i w_j = (-1)^{j-i+\lfloor \frac{i}{2} \rfloor + \lfloor \frac{j}{2} \rfloor} (e_{j-i} + e_{i+j+1}). \tag{13}$$

Devido ao Lema 2.2, para obter $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha w_i w_j)$ basta calcular o traço da expressão acima para cada par $(i, j) \in \{0, 1, 2, 3\}$ com $j > i$, tratando $j - i$ e $i + j + 1$ módulo 4 (por exemplo, $\alpha w_1 w_3 = (-1)^3(e_2 + e_1)$ tem traço na extensão $\mathbb{K}/\mathbb{Q}$ igual a $(-1)^3(2+0) = -2$). Em todos esses seis cálculos, verifica-se com o auxílio do Lema 2.2 que $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha w_i w_j) = -2$, como queríamos demonstrar. Portanto, a matriz de Gram do reticulado $\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ é igual a $2\mathbf{G}$, em que $\mathbf{G}$ denota a matriz de Gram do reticulado A_{p-1}^*. Logo, segue de (10) que $\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ é equivalente a $\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})$. □

Exemplo 3.1. *Sejam $\mathbb{K}_1 = \mathbb{Q}\left(\zeta_{4\times 5} + \zeta_{4\times 5}^{-1}\right)$ e $\mathbb{K}_2 = \mathbb{Q}\left(\zeta_{4\times 7} + \zeta_{4\times 7}^{-1}\right)$. Então, para $k = 1, 2$, as matrizes de Gram G_k dos reticulados $\sigma_\alpha(\mathcal{O}_{\mathbb{K}_k})$, com $\alpha = 2 + e_1$, relativas à base $\{w_i\}$ são, respectivamente,*

$$\boldsymbol{G}_1 = 2\begin{pmatrix} 4 & -1 & -1 & -1 \\ -1 & 4 & -1 & -1 \\ -1 & -1 & 4 & -1 \\ -1 & -1 & -1 & 4 \end{pmatrix} \quad e \quad \boldsymbol{G}_2 = 2\begin{pmatrix} 6 & -1 & -1 & -1 & -1 & -1 \\ -1 & 6 & -1 & -1 & -1 & -1 \\ -1 & -1 & 6 & -1 & -1 & -1 \\ -1 & -1 & -1 & 6 & -1 & -1 \\ -1 & -1 & -1 & -1 & 6 & -1 \\ -1 & -1 & -1 & -1 & -1 & 6 \end{pmatrix}. \tag{14}$$

DOI: 10.5540/03.2025.011.01.0471

Corolário 3.1. *O reticulado $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é bem-arredondado.*

Demonstração. Seja $\mathbb{L} = \mathbb{Q}(\zeta_p)$. Sabe-se de [8, Theorem 1.2] que $\sigma_\mathbb{L}(\mathcal{O}_\mathbb{L})$ é um reticulado bem-arredondado, o qual é equivalente ao resultado $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ segundo o Teorema 3.1. Disso segue o resultado. □

4 Considerações Finais

Neste trabalho, mostramos que, para todo primo ímpar p, existe um mergulho torcido σ_α tal que a imagem do anel de inteiros do subcorpo maximal real $\mathbb{Q}(\zeta_{4p}+\zeta_{4p}^{-1})$ através de σ_α consiste em um reticulado ideal bem-arredondado. Para isso, provamos antes que tal reticulado é equivalente ao reticulado ideal obtido através do mergulho canônico como imagem do anel de inteiros do corpo ciclotômico de índice p, que, por sua vez, é equivalente ao conhecido reticulado A_{p-1}^*. Em trabalhos futuros, temos a intenção de generalizar os resultados aqui apresentados para outras famílias de subcorpos ciclotômicos maximais reais e de seguir a investigação sobre a existência de mergulhos torcidos através dos quais imagens de anéis de inteiros de corpos de números são reticulados bem-arredondados.

Agradecimentos

Os autores agradecem à FAPESP, sob os números 2023/07667-2 e 20/09838-0, e ao CNPq Universal 405842/2023-6 pelo suporte financeiro que viabilizou a realização deste trabalho e a participação neste evento.

Referências

[1] E. Bayer-Fluckiger, F. Oggier e E. Viterbo. "New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel". Em: **IEEE Transactions on Information Theory** 50.4 (abr. de 2004), pp. 702–714. ISSN: 0018-9448. DOI: 10.1109/TIT.2004.825045.

[2] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe e D. Stehlé. **CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM**. Cryptology ePrint Archive, Report 2017/634. http://eprint.iacr.org/2017/634. 2017.

[3] J. J. Boutros, E. Viterbo, C. Rastello e J. C. Belfiore. "Good lattice constellations for both Rayleigh fading and Gaussian channels". Em: **IEEE Transactions on Information Theory** 42.2 (mar. de 1996), pp. 502–518. ISSN: 0018-9448. DOI: 10.1109/18.485720.

[4] J. H. Conway e N. J. A. Sloane. **Sphere packings, lattices and groups**. New York, NY, USA: Spring-Verlag, 1998.

[5] S. I. R. Costa, F. Oggier, A. Campello, J. C. Belfiore e E. Viterbo. **Lattices Applied to Coding for Reliable and Secure Communications**. Springer, Cham, 2017. DOI: 10.1007/978-3-319-67882-5.

[6] M. T. Damir, A. Karrila, L. Amoros, O. W. Gnilke, D. Karpuk e C. Hollanti. "Well-rounded lattices: Towards optimal coset codes for Gaussian and fading wiretap channels". Em: **IEEE Transactions on Information Theory** 67.6 (2021), pp. 3645–3663.

[7] R. R. De Araujo e S. I. R. Costa. "Well-rounded algebraic lattices in odd prime dimension". Em: **Arch. Math. 112** (2019), pp. 138–148. DOI: 10.1007/s00013-018-1232-7.

[8] L. Fukshansky e K. Petersen. "On well-rounded ideal lattices". Em: **Int. J. Number Theory** 8 (1) (2012), pp. 189–206. DOI: 10.1142/S179304211250011X.

[9] O. W. Gnilke, A. Barreal, A. Karrila, H. T. Tran, D. Karpuk e C. Hollanti. "Well-Rounded Lattices for Coset Coding in MIMO Wiretap Channels". Em: **IEEE Int. Telecommunication Networks and Applications Conference (ITNAC)** (2016), pp. 289–294. DOI: 10.1109/ATNAC.2016.7878824.

[10] J. C. Interlando, T. P. Da Nóbrega Neto, T. M. Rodrigues e J. O. D. Lopes. "A note on the integral trace form in cyclotomic fields". Em: **Journal of Algebra and Its Applications** 14.04 (2015), p. 1550045. DOI: 10.1142/S0219498815500450. URL: https://doi.org/10.1142/S0219498815500450.

[11] G. C. Jorge, A. A. De Andrade, S. I. R. Costa e J. E. Strapasson. "Algebraic constructions of densest lattices". Em: **Journal of Algebra** 429 (2015), pp. 218–235. ISSN: 0021-8693. DOI: https://doi.org/10.1016/j.jalgebra.2014.12.044. URL: https://www.sciencedirect.com/science/article/pii/S0021869315000526.

[12] D. Micciancio e O. Regev. "Lattice-based Cryptography". Em: **Post-Quantum Cryptography**. Ed. por J. Daniel D. J. Bernstein, J. Buchmann e E. Dahmen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191. ISBN: 978-3-540-88702-7. DOI: 10.1007/978-3-540-88702-7_5. URL: https://doi.org/10.1007/978-3-540-88702-7_5.

[13] National Institute of Standards and Technology - NIST. **Post-Quantum Cryptography - Selected Algorithms 2022**. Online. Acessado em 08/12/2021, https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. 2022.

[14] F. Oggier e E. Viterbo. "Algebraic Number Theory and Code Design for Rayleigh Fading Channels". Em: **Commun. Inf. Theory** 1.3 (dez. de 2004), pp. 333–416. ISSN: 1567-2190. DOI: 10.1561/0100000003. URL: http://dx.doi.org/10.1561/0100000003.

[15] O. W. Oliver, H. T. N. Tran, A. Karilla e C. Hollanti. "Well-Rounded Lattices for Reliability and Security in Rayleigh Fading SISO Channels". Em: **IEEE Information Theory Workshop (ITW)** (2016), pp. 359–363. DOI: 10.1109/ITW.2016.7606856.

[16] P. Ribenboim. **Classical Theory of Algebraic Numbers**. Universitext. Springer New York, 2001. ISBN: 9780387950709.

[17] P. Samuel e A. J. Silberger. **Algebraic Theory of Numbers**. Hermann, Paris, 1970.

[18] J. E. Strapasson, A. J. Ferrari, G. C. Jorge e S. I. R. Costa. "Algebraic constructions of rotated unimodular lattices and direct sum of Barnes–Wall lattices". Em: **Journal of Algebra and Its Applications** 20.03 (2021), p. 2150029. DOI: 10.1142/S0219498821500298. URL: https://doi.org/10.1142/S0219498821500298.

