Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, v. 6, n. 1, 2018.

Trabalho apresentado no XXXVII CNMAC, S.J. dos Campos - SP, 2017.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Reticulados de Posto 3

William Lima da Silva Pinto[1]
Matemática, UNESP, Rio Claro, SP
Carina Alves[2]
Departamento de Matemática, UNESP, Rio Claro, SP

1 Introdução

A teoria dos números algébricos tem desempenhado uma importante contribuição para a construção de códigos e reticulados algébricos. Os reticulados têm sido estudados em vários trabalhos e de diferentes formas. Por exemplo, em [2], Craig mostrou como construir reticulados E_6, E_8, K_{12} e Λ_{24} via corpos ciclotômicos $\mathbb{Q}(\zeta_n)$, para $n = 9$, 20 e 39, respectivamente. Aplicando este método, em [1] foi construído D_4, K_{12} e Λ_{16}, com $n = 8$, 21 e 40. Além das construções citadas, existem outras mais recentes e a maioria delas visa obter reticulados com boa densidade de empacotamento. Neste trabalho, avaliamos a densidade de empacotamento de reticulados no $\mathbb{R}^3$. Para isso, partimos de uma extensão cúbica galoisiana dos racionais que está contida numa extensão p-ciclotômica, p primo.

2 Reticulados e Cúbicas Abelianas

Intuitivamente, um reticulado em $\mathbb{R}^n$ é um conjunto infinito e discreto de pontos do $\mathbb{R}^n$ dispostos de forma regular. Formalmente, se $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ é um conjunto de vetores linearmente independentes em $\mathbb{R}^n$ (tal que $m \leq n$) então o conjunto de pontos

$$\Lambda = \{\mathbf{x} = \sum_{i=1}^{m} \lambda_i \mathbf{v}_i,\ \lambda_i \in \mathbb{Z}\} \tag{1}$$

é chamado um reticulado de posto m, e o conjunto $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ é chamado uma base do reticulado. O conceito de reticulado surgiu a partir do problema de como cobrir o espaço $\mathbb{R}^n$ com esferas de mesmo raio, de forma que quaisquer duas esferas se toquem em apenas um ponto e ocupem a maior parte do espaço possível. A proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas é a densidade de empacotamento de um reticulado.

Constelações de sinais que possuem estrutura de reticulados tem sido usadas em diferentes aplicações como, por exemplo, projetar códigos para canais com desvanecimento do tipo Rayleigh com uma antena e projetar reticulados densos para o canal Gaussiano.

[1]william26535@hotmail.com
[2]carina@rc.unesp.br

Neste contexto, a teoria dos números algébricos torna-se uma importante ferramenta matemática, que permite relacionar corpos de números e o espaço $\mathbb{R}^n$. Fazendo uso da teoria dos números algébricos, estamos interessados em avaliar a densidade de empacotamento de reticulados de posto 3, e portanto vamos considerar cúbicas galoisianas.

Uma extensão K de $\mathbb{Q}$ é dita galoisiana se é normal e separável. Além disso, K é dito abeliano se K é uma extensão galoisiana dos racionais e seu grupo de Galois é abeliano.

Dada uma cúbica galoisiana K, seu grupo de Galois sobre $\mathbb{Q}$ tem grau 3 e assim é abeliano. A partir do Teorema de Kronecker-Weber, K está contido em alguma extensão ciclotômica $\mathbb{Q}(\zeta_n)$, onde n é uma raiz n-ésima primitiva da unidade. Como o grau de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é $\varphi(n)$ onde φ é a função de Euler, segue que se K está contido em algum corpo ciclotômico $\mathbb{Q}(\zeta_n)$, então 3 divide $\varphi(n)$. Veremos que a recíproca desse resultado também é válida, isto é, dado um número inteiro n, se 3 divide $\varphi(n)$ então $\mathbb{Q}(\zeta_n)$ contém uma cúbica.

Visando calcular a densidade de centro de reticulados de posto 3, consideramos primeiramente $n = p$ e assim, $K \subset \mathbb{Q}(\zeta_p)$, p primo, $p \equiv 1 \mod 3$, onde o grau de K sobre $\mathbb{Q}$ é 3. Neste caso, mostramos que a densidade de centro do reticulado obtido a partir do anel dos inteiros de K é

$$\delta(\sigma(\mathcal{O}_K)) = \frac{3\sqrt{3}}{8p}. \tag{2}$$

Posteriormente, consideramos $n = p^r$, $r > 1$ e assim, $K \subset \mathbb{Q}(\zeta_p)$, p primo, $r > 1$ se, e somente se, 3 divide $p - 1$ ou 3 divide p^{r-1}. Analisamos a densidade de centro de reticulados em ambos os casos. Visando calcular a densidade de centro de tais reticulados, apresentamos resultados sobre o discriminante dessas cúbicas e a minimização da função traço, [3].

Agradecimentos

Agradeço à Fundação VUNESP, bolsa de estudos - Convênio UNESP/VUNESP/SEE-SP e à minha orientadora, Profa. Dra. Carina Alves, pela ajuda e incentivo.

Referências

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

[2] M. Craig, Extreme forms and cyclotomy, Mathematika, vol. 25, 44–56, (1978).

[3] T. M. Rodrigues, Cúbicas Galoisianas, Dissertação de Mestrado em Matemática, UNESP, São José do Rio Preto, (2003).

