Revista Eletrônica
Paulista de Matemática

ISSN 2316-9664
Volume 7, dez. 2016
Edição ERMAC

Eliton Mendonça Moro

Universidade Estadual Paulista,
UNESP-São José do Rio Preto
elitonmoro@hotmail.com

Carina Alves

Universidade Estadual Paulista,
UNESP-Rio Claro
carina@rc.unesp.br

**Antonio Aparecido de
Andrade**

Universidade Estadual Paulista,
UNESP-São José do Rio Preto
andrade@ibilce.unesp.br

O reticulado E_8 via o corpo ciclotômico $\mathbb{Q}(\zeta_{20})$

The E_8 -lattice via the cyclotomic field $\mathbb{Q}(\zeta_{20})$

Resumo

Intuitivamente, um reticulado no $\mathbb{R}^n$ é um conjunto infinito de pontos dispostos de forma regular. Dado um reticulado Λ no $\mathbb{R}^n$ e O_K o anel dos inteiros de um corpo de números K , é possível que Λ seja isomorfo a um O_K -reticulado? Motivados por esta questão, neste trabalho apresentamos uma construção do reticulado E_8 como um O_K -reticulado via corpos ciclotômicos. A vantagem de obter reticulados por este método é que podemos identificar os pontos do reticulado no $\mathbb{R}^n$ com os elementos de K . Desta forma, podemos utilizar algumas propriedades do corpo K no estudo de tais reticulados. Os reticulados tem aplicações em diferentes áreas, particularmente em teoria da informação e em criptografia. Constelações de sinais tendo estrutura de reticulados têm sido utilizadas como suporte para transmissão de sinais sobre os canais gaussianos e com desvanecimento do tipo Rayleigh.

Palavras-chave: Reticulado. Teoria dos Números Algébricos. Fatoração de Ideais. Extensão de Corpos.

Abstract

Intuitively, a lattice in $\mathbb{R}^n$ is an infinite set of points arranged regularly. Given a lattice Λ in $\mathbb{R}^n$ and O_K the ring of integers of a number field K , is it possible that Λ is isomorphic to O_K -lattice? Motivated by this question, in this paper we present a construction of the E_8 -lattice as O_K -lattice via a cyclotomic field. The advantage of getting lattice by this method is that we can identify the lattice points in $\mathbb{R}^n$ with the elements of K . In this way, we can use some properties of the field K in the study of such lattices. The lattices has applications in different areas, particularly in information theory and cryptography. Signal constellations having a lattice structure have been used as support for transmitting signals over the Gaussian and Rayleigh fading channels.

Keywords: Lattice. Algebraic Number Theory. Factorization of Ideals. Field Extension.

1 Introdução

Um reticulado Λ é um subgrupo aditivo discreto do $\mathbb{R}^n$. Este conceito 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 no máximo em um ponto e ocupem a maior parte do espaço possível.

Dado um reticulado Λ no $\mathbb{R}^n$ e $O_{\mathbb{K}}$ o anel dos inteiros de um corpo de números $\mathbb{K}$, é possível que Λ seja isomorfo a um $O_{\mathbb{K}}$ -reticulado? Motivados por esta questão, neste trabalho apresentamos uma construção do reticulado E_8 como um $O_{\mathbb{K}}$ -reticulado via $\mathbb{K} = \mathbb{Q}(\zeta_{20})$. O reticulado E_8 é o reticulado de maior densidade de empacotamento em dimensão 8 e é o único reticulado par e unimodular nesta dimensão.

2 Reticulados

Apresentamos aqui o conceito de reticulado no $\mathbb{R}^n$ e alguns de seus parâmetros.

Definição 1. Sejam $\{v_1, v_2, \dots, v_m\}$ vetores linearmente independentes do $\mathbb{R}^n$. O conjunto de pontos

$$\Lambda = \left\{ \mathbf{x} = \sum_{i=1}^m \lambda_i v_i, \lambda_i \in \mathbb{Z} \right\}$$

é chamado reticulado de dimensão m e $\{v_1, v_2, \dots, v_m\}$ é chamado de base do reticulado.

Exemplo 2. O reticulado $\Lambda = \mathbb{Z}^2$ é gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$ com os pontos dispostos conforme a figura abaixo.

Definição 3. Seja $\{v_1, \dots, v_m\}$ uma base de um reticulado. O paralelepípedo formado pelos pontos

$$\lambda_1 v_1 + \dots + \lambda_m v_m, \quad 0 \leq \lambda_i < 1$$

é chamado de paralelepípedo fundamental ou região fundamental do reticulado.

Definição 4. Seja $\{v_1, \dots, v_m\}$ uma base de Λ . Se $v_i = (v_{i1}, \dots, v_{in})$, para $i = 1, \dots, m$, a matriz

$$M = \begin{pmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \dots & v_{mn} \end{pmatrix}$$

é chamada de matriz geradora do reticulado Λ . A matriz $G = MM^t$ é chamada de matriz de Gram do reticulado, onde t denota a transposição.

Assim, os pontos do reticulado são formados por

$$\Lambda = \{\mathbf{x} = \lambda M \mid \lambda \in \mathbb{Z}^m\}.$$

Definição 5. O determinante do reticulado Λ é definido como sendo o determinante da matriz G , ou seja,

$$\det(\Lambda) = \det(G).$$

Um reticulado é dito ter posto máximo se $m = n$, e neste caso M é uma matriz quadrada. Assim,

$$\det(\Lambda) = (\det(M))^2.$$

É importante observar que o mesmo reticulado pode ser representado por mais de uma matriz, e o fato de dois reticulados terem o mesmo determinante não é suficiente para que eles sejam isomorfos.

Definição 6. Um empacotamento esférico, ou simplesmente um empacotamento no $\mathbb{R}^n$, é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$ de forma que a interseção de quaisquer duas esferas tenha no máximo um ponto. Um empacotamento reticulado é um empacotamento em que o conjunto dos centros das esferas formam um reticulado Λ no $\mathbb{R}^n$. Além disso, $\rho = \min\{|\lambda|; \lambda \in \Lambda, \lambda \neq 0\}/2$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ e obter um empacotamento, este raio é então chamado de raio de empacotamento.

Definição 7. Seja Λ um reticulado. A densidade de empacotamento de Λ é definida por

$$\Delta(\Lambda) = \frac{\text{volume da região coberta por uma esfera}}{\text{volume da região fundamental}}.$$

Um dos problemas de empacotamento esférico de um reticulado no $\mathbb{R}^n$ é encontrar o empacotamento com maior densidade de empacotamento. A seguir, daremos exemplos em dimensões 1, 2 e 3.

Exemplo 8. Na dimensão um, temos que os pontos de coordenadas inteiras da reta formam um $\mathbb{Z}$ -reticulado cuja a densidade de empacotamento é a melhor possível dada por $\Delta = 1$. Neste caso, as “esferas” são intervalos como podemos ver na figura abaixo.

Exemplo 9. Na dimensão dois o reticulado hexagonal A_2 (favo de mel) é o de maior densidade, dada por $\Delta = \frac{\pi}{\sqrt{12}} \approx 0,9069$. O empacotamento deste reticulado com base $\beta = \left\{ (1,0), \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \right\}$ é dado por

Exemplo 10. Na dimensão 3 o reticulado conhecido como fcc, (face centered cubic) é o empacotamento com maior densidade, sendo essa $\Delta = \frac{\pi}{\sqrt{18}} \approx 0,7405$.

É conhecido e provado que as densidades de empacotamento dos reticulados $A_1, A_2, D_3, D_4, D_5, E_6, E_7, E_8$ e Λ_{24} , de dimensões 1 a 8 e 24, respectivamente, são ótimas. Para outras dimensões não se sabe as ótimas.

O reticulado E_8 além de possuir a maior densidade de empacotamento é o único reticulado par e unimodular em sua dimensão.

Definição 11. O reticulado E_8 é um reticulado 8-dimensional, definido por:

$$E_8 = \{(x_1, \dots, x_8) \text{ tal que } x_i \in \mathbb{Z} \text{ ou } x_i \in \mathbb{Z} + \frac{1}{2}, \forall i \text{ e } \sum x_i \equiv 0 \pmod{2}\}.$$

A matriz geradora do reticulado E_8 é dada por

$$B = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

seu raio de empacotamento é $\rho = \frac{1}{\sqrt{2}}$ e sua densidade de centro é $\Delta = 0,2537$.

3 Resultados Preliminares

Nesta seção, expomos de modo conciso, resultados necessários para a construção do reticulado E_8 , que será apresentada na Seção 5. Dessa forma, nos limitamos a não demonstrar tais resultados, que podem ser encontrados mais detalhadamente em Samuel (1970).

Definição 12. Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos. Dizemos que $\mathbb{L}$ é uma extensão de $\mathbb{K}$, denotada por $\mathbb{L}|\mathbb{K}$, se $\mathbb{K} \subset \mathbb{L}$.

Definição 13. Dizemos que a extensão $\mathbb{L}$ de $\mathbb{K}$ é extensão algébrica se todo elemento $\alpha \in \mathbb{L}$ for algébrico, isto é, raiz de algum polinômio mônico não-nulo $f(x)$ em $\mathbb{K}[x]$.

Definição 14. O conjunto dos números algébricos de $\mathbb{K}$ sobre $\mathbb{Q}$ é um anel, chamado de anel dos inteiros algébricos de $\mathbb{K}$, e denotado por $O_{\mathbb{K}}$. Além disso, $O_{\mathbb{K}}$ é um $\mathbb{Z}$ -módulo livre de posto $[\mathbb{K} : \mathbb{Q}]$, cuja base é chamada de base integral.

Todo corpo de números $\mathbb{K}$ é da forma $\mathbb{K} = \mathbb{Q}(\theta)$ para algum número algébrico $\theta \in \mathbb{K}$. Assim $\mathbb{K}$ é um $\mathbb{Q}$ -espaço vetorial gerado por potências de θ . Se $\mathbb{K}$ tem grau n então $\{1, \theta, \dots, \theta^{n-1}\}$ é uma base de $\mathbb{K}$ e o grau do polinômio minimal de θ sobre $\mathbb{Q}$ é n e o denotamos por $\min_{\mathbb{Q}} \theta$.

O próximo teorema diz respeito a um homomorfismo entre dois corpos.

Teorema 15. Sejam $\mathbb{K}, \mathbb{L}$, subcorpos de $\mathbb{C}$ onde $\mathbb{L}$ é uma extensão de $\mathbb{K}$ e $[\mathbb{L} : \mathbb{K}] = n < \infty$. Então, existe $\theta \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\theta)$ e existem exatamente n $\mathbb{K}$ -homomorfismos de $\mathbb{L}$ em $\mathbb{C}$, $\sigma_i : \mathbb{L} \rightarrow \mathbb{C}$, $i = 1, \dots, n$, tal que $\sigma_i(\theta) = \theta_i$, onde θ_i são as raízes distintas em $\mathbb{C}$ do polinômio minimal de θ sobre $\mathbb{K}$.

Observação 16. Quando aplicamos σ_i a um elemento arbitrário $x \in \mathbb{L}$, $x = \sum_{k=1}^n a_k \theta^k$, $a_k \in \mathbb{K}$, usando as propriedades dos $\mathbb{K}$ -homomorfismo temos

$$\sigma_i(x) = \sigma_i \left(\sum_{k=1}^n a_k \theta^k \right) = \sum_{k=1}^n \sigma_i(a_k) \sigma_i(\theta)^k = \sum_{k=1}^n a_k \theta_i^k \in \mathbb{C}$$

e temos que a imagem de x sobre σ_i é univocamente identificada por θ_i .

Os elementos $\sigma_1(x), \sigma_2(x), \dots, \sigma_n(x)$ são chamados os $\mathbb{K}$ -conjugados de x e

$$N_{\mathbb{L}|\mathbb{K}}(x) = \prod_{i=1}^n \sigma_i(x), \quad \text{Tr}_{\mathbb{L}|\mathbb{K}}(x) = \sum_{i=1}^n \sigma_i(x)$$

são chamados respectivamente, a norma e o traço de x da extensão $\mathbb{L}$ sobre $\mathbb{K}$.

Fazendo o uso de alguns conceitos expostos anteriormente, apresentamos a definição de discriminante de uma extensão de corpos, que será de grande utilidade para a construção do reticulado E_8 .

Definição 17. Sejam $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $\{\omega_1, \dots, \omega_n\}$ uma base integral de $O_{\mathbb{L}}$. Definimos o discriminante de $\mathbb{L}$ sobre $\mathbb{K}$ como $\text{Disc}(\mathbb{L}|\mathbb{K}) = \det[\sigma_j(\omega_i)]^2$, onde $\det$ denota a função determinante.

Duas famílias importantes de corpos de números é a dos corpos quadráticos e dos corpos ciclotômicos. Nestes corpos é possível caracterizar seu anel de inteiros, base integral, discriminante, entre outros.

Definição 18. Seja $\mathbb{K}$ um corpo. Dizemos que $\mathbb{K}$ é um corpo quadrático se o grau da extensão de $\mathbb{K}$ sobre $\mathbb{Q}$ é igual a 2, ou seja, $[\mathbb{K} : \mathbb{Q}] = 2$.

Observação 19. *Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$ onde d é um inteiro livre de quadradados.*

Dentre os corpos quadráticos e ciclotômicos, a família dos corpos ciclotômicos é a mais utilizada na construção de reticulados algébricos.

Definição 20. *Seja ζ_n uma raiz n -ésima primitiva da unidade, isto é, $\zeta_n^n = 1$ e $\zeta_n^m \neq 1$ para $1 \leq m < n$. Um corpo ciclotômico $\mathbb{K}$ é a menor extensão de $\mathbb{Q}$ contendo ζ_n , isto é, $\mathbb{K} = \mathbb{Q}(\zeta_n)$.*

Definição 21. *Sejam $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos de grau n e $\{\sigma_1, \dots, \sigma_n\}$ os n $\mathbb{K}$ -homomorfismos distintos de $\mathbb{L}$ em $\mathbb{C}$. Dizemos que um homomorfismo σ_i é real se $\sigma_i(\mathbb{L}) \subset \mathbb{R}$. Caso contrário, dizemos que σ_i é imaginário. Além disso, se σ_i for real para todo $i = 1, \dots, n$, dizemos que a extensão $\mathbb{L}|\mathbb{K}$ é totalmente real e, se σ_i for imaginário para todo $i = 1, \dots, n$, dizemos que $\mathbb{L}|\mathbb{K}$ é totalmente imaginária.*

Exemplo 22. *Temos que $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\zeta_3)$ são extensões quadráticas sobre $\mathbb{Q}$, onde $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ é totalmente real e $\mathbb{Q}(\zeta_3)|\mathbb{Q}$ é totalmente imaginária.*

Observação 23. *É possível verificar que se ζ_n é uma raiz n -ésima primitiva da unidade, então*
i) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, onde φ é a função de Euler e $[\cdot : \cdot]$ denota o grau da extensão..
ii) *O anel de inteiros de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Z}$ é $\mathbb{Z}[\zeta_n]$ e uma $\mathbb{Z}$ -base de $\mathbb{Z}[\zeta_n]$ é $\{1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1}\}$.
iii) $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é totalmente real e $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$.*

Teorema 24. *Sejam $n \in \mathbb{N}; n > 2$ e $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n -ésima primitiva da unidade. Se $n = \prod_{j=1}^r p_j^{a_j}$, onde p_j são primos distintos e $a_j \in \mathbb{N}^*$, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

$$\text{Disc}(\mathbb{K}|\mathbb{Q}) = \frac{(-1)^{\frac{\varphi(n)r}{2}} n^{\varphi(n)}}{\prod_{j=1}^r p_j^{\frac{\varphi(n)}{p_j-1}}},$$

onde φ é a função de Euler.

No que segue, apresentamos algumas definições com o intuito de caracterizar um $O_{\mathbb{K}}$ -reticulado.

Definição 25. *Um corpo de números $\mathbb{K}$ é chamado de CM se existe um corpo de números totalmente real $\mathbb{F}$ tal que $\mathbb{K}$ é uma extensão quadrática totalmente imaginária de $\mathbb{F}$.*

Exemplo 26. *O corpo de números $\mathbb{Q}(\sqrt{2}, \zeta_3)$ é um CM-corpo, pois $\mathbb{Q}(\sqrt{2}, \zeta_3)|\mathbb{Q}(\sqrt{2})$ é totalmente imaginária com $[\mathbb{Q}(\sqrt{2}, \zeta_3) : \mathbb{Q}(\sqrt{2})] = 2$ e $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ é totalmente real.*

Definição 27. *Seja $\mathbb{K}$ um corpo de números e $O_{\mathbb{K}}$ o seu anel de inteiros. O conjunto*

$$\mathcal{D}(\mathbb{K}|\mathbb{Q})^{-1} = \{x \in \mathbb{K}; \forall \alpha \in O_{\mathbb{K}}, \text{Tr}_{\mathbb{K}|\mathbb{Q}}(x\alpha) \in \mathbb{Z}\}$$

é um ideal fracionário de $O_{\mathbb{K}}$, chamado de codiferente. O seu ideal inverso $\mathcal{D}(\mathbb{K}|\mathbb{Q})$ é um ideal inteiro de $O_{\mathbb{K}}$, chamado de diferente.

Exemplo 28. Sejam $\mathbb{K} = \mathbb{Q}, \mathbb{L} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados e $d \equiv 2$ ou $3 \pmod{4}$. Sabemos que $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d}; x, y \in \mathbb{Z}\}$ é o anel de inteiros de $\mathbb{L}$ sobre $\mathbb{Z}$. Temos que

$$\mathcal{D}(\mathbb{L}|\mathbb{K})^{-1} = \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}].$$

De fato:

i) Se $x \in \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$, então $x = \frac{1}{2\sqrt{d}}(a + b\sqrt{d}); a, b \in \mathbb{Z}$. Dado $y = c + e\sqrt{d} \in \mathcal{O}_{\mathbb{L}}$,

$$\begin{aligned} \text{Tr}_{\mathbb{L}|\mathbb{K}}(xy) &= \text{Tr}_{\mathbb{L}|\mathbb{K}}\left(\left(\frac{1}{2\sqrt{d}}(a + b\sqrt{d})\right)(c + e\sqrt{d})\right) \\ &= \text{Tr}_{\mathbb{L}|\mathbb{K}}\left(\frac{1}{2\sqrt{d}}ac + \frac{ae}{2} + \frac{bc}{2} + \frac{be\sqrt{d}}{2}\right) \\ &= ae + bc \in \mathbb{Z}. \end{aligned}$$

Assim, $x \in \mathcal{D}(\mathbb{L}|\mathbb{K})^{-1}$. Logo $\frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}] \subset \mathcal{D}(\mathbb{L}|\mathbb{K})^{-1}$.

ii) Se $x = a + b\sqrt{d} \in \mathcal{D}(\mathbb{L}|\mathbb{K})^{-1}$, então $a, b \in \mathbb{Q}, x \in \mathbb{L}$ e $\text{Tr}_{\mathbb{L}|\mathbb{K}}(xy) \in \mathbb{Z}, \forall y \in \mathbb{Z}[\sqrt{d}]$. Tomando $y = 1$,

$$\text{Tr}_{\mathbb{L}|\mathbb{K}}(xy) = \text{Tr}_{\mathbb{L}|\mathbb{K}}(a + b\sqrt{d}) = 2a \in \mathbb{Z}.$$

Assim, $a = \frac{m}{2}; m \in \mathbb{Z}$. Tomando $y = \sqrt{d}$,

$$\text{Tr}_{\mathbb{L}|\mathbb{K}}(xy) = \text{Tr}(a\sqrt{d} + bd) = 2db \in \mathbb{Z}.$$

Assim, $b = \frac{n}{2d}; n \in \mathbb{Z}$. Logo $x = \frac{m}{2} + \frac{n}{2d}\sqrt{d} = \frac{1}{2\sqrt{d}}(n + m\sqrt{d}) \in \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$. Desta forma $\mathcal{D}(\mathbb{L}|\mathbb{K})^{-1} \subset \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$.

Portanto, de (i) e (ii) segue a igualdade $\mathcal{D}(\mathbb{L}|\mathbb{K})^{-1} = \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$.

Proposição 29. Sejam $\mathbb{K}$ um corpo de números totalmente real ou um CM-corpo, $\phi : \mathbb{K} \rightarrow \mathbb{K}$ a conjugação complexa, $\mathbb{F}$ o corpo fixo por ϕ , I um ideal fracionário não nulo de $\mathcal{O}_{\mathbb{K}}$ e $\alpha \in \mathbb{F}$ tal que $\alpha I\phi(I) \subset \mathcal{D}(\mathbb{K}|\mathbb{Q})^{-1}$. Seja

$$\begin{aligned} b_{\alpha} : \quad I \times I &\rightarrow \mathbb{Z} \\ (x, y) &\mapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha x\phi(y)). \end{aligned}$$

Temos que b_{α} está bem definida e é uma forma bilinear simétrica.

Definição 30. Com as mesmas hipóteses da Proposição (29), dizemos que o par (I, b_{α}) é um reticulado ideal ou um $\mathcal{O}_{\mathbb{K}}$ -reticulado.

Definição 31. Dizemos que o reticulado ideal (I, b_{α}) é par se $b_{\alpha}(x, x)$ é um número par para todo $x \in I$, caso contrário, dizemos que é ímpar.

Exemplo 32. Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ e seu anel de inteiros $O_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$. Considere a forma bilinear

$$\begin{aligned} b : \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{2}] &\rightarrow \mathbb{Z} \\ (x, y) &\mapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(xy) \end{aligned}$$

O reticulado ideal $(O_{\mathbb{K}}, b)$ é par, pois para todo $x = a + b\sqrt{2} \in O_{\mathbb{K}}$, temos que $b(x, x) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(xx) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}((a + b\sqrt{2})^2) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(a^2 + 2b^2 + 2ab\sqrt{2}) = 2(a^2 + 2b^2) \in 2\mathbb{Z}$.

4 Teorema de Kummer

Os anéis de Dedekind formam uma classe muito importante de anéis dentro da Álgebra Comutativa. Nestes anéis todo ideal pode ser expresso de forma única, a menos da ordem, como um produto de ideais primos distintos. Nesta seção vamos apresentar alguns resultados sobre fatoração de ideais e o Teorema de Kummer que será utilizado na fatoração dos ideais primos ao longo da construção do reticulado E_8 . Para isso consideremos $\mathcal{A}$ um domínio de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão separável de $\mathbb{K}$ de grau n , $O_{\mathbb{L}}$ o anel dos inteiros de $\mathbb{L}$ sobre $\mathcal{A}$. A demonstração dos resultados apresentados aqui podem ser encontradas em Samuel (1970).

Seja $\mathfrak{p}$ um ideal primo de $\mathcal{A}$. Como $\mathcal{A}$ é um anel de Dedekind, segue que $O_{\mathbb{L}}$ também é um anel de Dedekind e portanto a fatoração de $\mathfrak{p}O_{\mathbb{L}}$ é dada por

$$\mathfrak{p}O_{\mathbb{L}} = \prod_{i=1}^g \mathfrak{q}_i^{e_i}, \quad (1)$$

onde os $\mathfrak{q}_i$'s são ideais primos de $O_{\mathbb{L}}$ e $e_i \in \mathbb{N}$. Nosso objetivo é caracterizar esta decomposição.

Definindo o homomorfismo $\varphi_i : \mathcal{A} \rightarrow O_{\mathbb{L}}/\mathfrak{q}_i$ por $\varphi_i(x) = x + \mathfrak{q}_i$, temos $\ker(\varphi_i) = \mathfrak{p}$ e, então, $\mathcal{A}/\mathfrak{p}$ pode ser identificado com um subanel de $O_{\mathbb{L}}/\mathfrak{q}_i$. Como ambos anéis quocientes são corpos e $O_{\mathbb{L}}$ é um $\mathcal{A}$ -módulo finitamente gerado, então $O_{\mathbb{L}}/\mathfrak{q}_i$ é um espaço vetorial de dimensão finita sobre $\mathcal{A}/\mathfrak{p}$.

Definição 33. Denotamos a dimensão de $O_{\mathbb{L}}/\mathfrak{q}_i$ sobre $\mathcal{A}/\mathfrak{p}$ por f_i denominando-a de grau de inércia de $\mathfrak{q}_i$ sobre $\mathcal{A}$. O índice e_i da equação (1) é chamado de grau de ramificação de $\mathfrak{q}_i$ sobre $\mathcal{A}$.

Definição 34. Seja $\mathfrak{p}$ um ideal primo de $\mathcal{A}$, $\mathfrak{p}O_{\mathbb{L}} = \prod_{i=1}^g \mathfrak{q}_i^{e_i}$ a fatoração de $\mathfrak{p}O_{\mathbb{L}}$ em um produto de ideais primos de $O_{\mathbb{L}}$. Dizemos que o ideal $\mathfrak{p}$ de $\mathcal{A}$ é:

- i) totalmente decomposto em $\mathbb{L}$ (ou em $O_{\mathbb{L}}$), quando $e_i = f_i = 1$, para todo ideal primo $\mathfrak{q}_i$ que está acima de $\mathfrak{p}$.
- ii) inerte em $\mathbb{L}$ (ou em $O_{\mathbb{L}}$), quando $e_i = 1$, e $f_i = n$ para todo ideal primo $\mathfrak{q}_i$ que está acima de $\mathfrak{p}$.
- iii) totalmente ramificado em $\mathbb{L}$ (ou em $O_{\mathbb{L}}$), quando $e_i = n$ e $f_i = 1$, para todo ideal primo $\mathfrak{q}_i$ que está acima de $\mathfrak{p}$.
- iv) ramificado em $\mathbb{L}$ (ou em $O_{\mathbb{L}}$), se existir um ideal primo $\mathfrak{q}_i$ de $O_{\mathbb{L}}$ que está acima de $\mathfrak{p}$ tal que $e_i > 1$ para algum i .

Definição 35. Sejam A um anel e $f(x) = \sum_{i=1}^n a_i x^i \in A[x]$. Denotamos por $\bar{f}(x)$ o polinômio

$\sum_{i=1}^n (a_i + \mathfrak{p})x^i \in (A/\mathfrak{p})[x]$, onde $\mathfrak{p}$ é um ideal primo não nulo de A .

Proposição 36. Sejam $O_{\mathbb{L}}$ o anel de inteiros de $\mathbb{L}$ sobre $\mathcal{A}$ tal que $O_{\mathbb{L}} = \mathcal{A}[\beta]$, para algum $\beta \in \mathbb{L}$ e $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{A}$. Se $f(x) = \min_{\mathbb{K}} \beta$ é o polinômio minimal de β sobre $\mathbb{K}$ e $f_1(x), \dots, f_r(x)$ são polinômios mônicos em $\mathcal{A}[x]$, tal que a fatoração de $f(x)$ em polinômios irredutíveis distintos em $(\mathcal{A}/\mathfrak{p})[x]$ seja dada por

$$\bar{f}(x) = \bar{f}_1^{e_1}(x) \cdots \bar{f}_r^{e_r}(x)$$

então os ideais primos, dois a dois distintos, $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ de $O_{\mathbb{L}}$, que estão acima de $\mathfrak{p}$ satisfazem

$$O_{\mathbb{L}}/\mathfrak{q}_j \cong (\mathcal{A}/\mathfrak{p})[\bar{\beta}_j],$$

onde $\bar{\beta}_j$ é uma raiz de $\bar{f}(x)$. Além disso, $f(\mathfrak{q}_j/\mathfrak{p}) = \text{grau}(f_j)$, para $j = 1, \dots, r$.

Teorema 37. (Kummer) Nas condições da Proposição (36), se $\bar{f}(x) = \bar{f}_1^{e_1}(x) \cdots \bar{f}_r^{e_r}(x)$ é a fatoração de $\bar{f}(x)$ em polinômios irredutíveis em $\mathcal{A}/\mathfrak{p}[x]$, então

$$\begin{aligned} \mathfrak{p}O_{\mathbb{L}} &= \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}, \text{ onde} \\ \mathfrak{q}_j &= \mathfrak{p}O_{\mathbb{L}} + f_j(\beta)O_{\mathbb{L}}, \text{ para } j = 1, \dots, r, \\ e(\mathfrak{q}_j/\mathfrak{p}) &= e_j, \text{ para } j = 1, \dots, r \text{ e} \\ f(\mathfrak{q}_j/\mathfrak{p}) &= \text{grau}(f_j(x)), \text{ para } j = 1, \dots, r. \end{aligned}$$

Exemplo 38. Se $\mathbb{L} = \mathbb{Q}(\sqrt{-17})$, então $O_{\mathbb{L}} = \mathbb{Z}[\sqrt{-17}]$ e $f(x) = x^2 + 17$ é o polinômio minimal de $\sqrt{-17}$ sobre $\mathbb{Q}$. Queremos fatorar os ideais $2O_{\mathbb{L}}$ e $3O_{\mathbb{L}}$ em produto de ideais primos de $O_{\mathbb{L}}$. Para o ideal $2O_{\mathbb{L}}$, como

$$x^2 + 17 \equiv (x+1)^2 \pmod{(\mathbb{Z}/2\mathbb{Z})[x]},$$

segue que

$$\bar{f}_1(x) = x+1, e_1 = 2, \text{ e } \mathfrak{q}_1 = 2O_{\mathbb{L}} + (1 + \sqrt{-17})O_{\mathbb{L}}.$$

Portanto, $2O_{\mathbb{L}} = \mathfrak{q}_1^2$. Para o ideal $3O_{\mathbb{L}}$, como

$$x^2 + 17 \equiv (x+1)(x-1) \pmod{(\mathbb{Z}/3\mathbb{Z})[x]},$$

segue que

$$\begin{aligned} \bar{f}_1(x) &= x+1, \bar{f}_2(x) = x-1, e_1 = e_2 = 1, \\ \mathfrak{q}_1 &= 3O_{\mathbb{L}} + 1(\sqrt{-17})O_{\mathbb{L}} \text{ e } \mathfrak{q}_2 = 3O_{\mathbb{L}} + (1 - \sqrt{-17})O_{\mathbb{L}}. \end{aligned}$$

Portanto, $3O_{\mathbb{L}} = \mathfrak{q}_1\mathfrak{q}_2$.

Os resultados que seguem serão usados para na Seção 5, em que apresentamos a construção do reticulado E_8 .

Definição 39. Sejam $\mathfrak{p}$ um ideal primo de um anel de Dedekind $\mathcal{A}$, $\mathbb{K}$ o corpo de frações de $\mathcal{A}$, e $\mathbb{L}$ uma extensão de $\mathbb{K}$. Para cada ideal primo $\mathfrak{q}$ de $O_{\mathbb{L}}$ satisfazendo $\mathfrak{q} \cap \mathcal{A} = \mathfrak{p}$, o conjunto

$$D_{\mathbb{L}}(\mathfrak{q}/\mathfrak{p}) = \{\sigma \in G; \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

é um subgrupo de $G = \text{Gal}(\mathbb{L}|\mathbb{K})$, chamado de grupo de decomposição de $\mathfrak{q}$ com relação ao ideal $\mathfrak{p}$.

Definição 40. Definimos $O_p(t) = r$, para $p, t \in \mathbb{Z}$ e $r \in \mathbb{Z}_+$ como sendo a ordem de t módulo p , ou seja, r é menor potência de t tal que $t^r \equiv 1 \pmod{p}$.

Proposição 41. Sejam $n = p^k t$, $k \geq 1$ tal que p não divide t , p primo, $\mathbb{L} = \mathbb{Q}(\zeta_n)$, $\mathbb{K} = \mathbb{Q}(\zeta_t)$ e $\bar{\sigma}$ a conjugação complexa. Nestas condições segue que:

- i) Se $\bar{\sigma} \in D_{\mathbb{L}}(p)$, então $\bar{\sigma} \in D_{\mathbb{K}}(p)$.
- ii) Se $\bar{\sigma} \in D_{\mathbb{K}}(p)$, então $O_t(p) \equiv 0 \pmod{2}$.
- iii) Se $O_t(p) \equiv 1 \pmod{2}$, então $\bar{\sigma} \notin D_{\mathbb{L}}(p)$.

Teorema 42. Se $\mathcal{A}$ é um anel de Dedekind, $\mathbb{K}$ seu corpo de frações e $\mathbb{L}$ uma extensão finita de $\mathbb{K}$, então

$$N(\mathcal{D}(\mathbb{L}|\mathbb{K})) = |\text{Disc}(\mathbb{L}|\mathbb{K})|,$$

onde $\text{Disc}(\mathbb{L}|\mathbb{K})$ é o discriminante de $\mathbb{L}$ sobre $\mathbb{K}$ e N é a norma algébrica.

Proposição 43. Sejam $\mathbb{K}$ um corpo de números tal que $\mathbb{K}$ é totalmente real ou um CM-corpo, $O_{\mathbb{K}}$ seu anel de inteiros e $\phi: \mathbb{K} \rightarrow \mathbb{K}$ a sua conjugação complexa. Se existe $\gamma \in O_{\mathbb{K}}$ tal que $\gamma + \phi(\gamma) = 1$, então todo $O_{\mathbb{K}}$ -reticulado é par.

Teorema 44. Seja I um ideal fracionário não nulo de $O_{\mathbb{K}}$. Se (I, b_{α}) é um reticulado ideal, então

$$\det(b_{\alpha}) = N_{\mathbb{K}|\mathbb{Q}}(I)^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha) |\text{Disc}(\mathbb{K}|\mathbb{Q})|.$$

Proposição 45. Se $\mathbb{K}$ é um corpo de números tal que $\mathbb{K}$ é totalmente real ou é uma extensão totalmente imaginária de $\mathbb{F}$, de grau 2, então existe um $O_{\mathbb{K}}$ -reticulado do tipo traço com determinante d se, e somente se, existem ideais I, J de $O_{\mathbb{K}}$ tal que $N(J) = d$ e $\mathcal{D}(\mathbb{K}|\mathbb{Q}) = J I \bar{I}$.

Proposição 46. Se $\mathbb{K}$ é um corpo de números tal que $\mathbb{K}$ é totalmente real ou é uma extensão totalmente imaginária de $\mathbb{F}$, de grau 2, então existe um $O_{\mathbb{K}}$ reticulado unimodular do tipo traço se, e somente se, existe um ideal I de $O_{\mathbb{K}}$ tal que $\mathcal{D}(\mathbb{K}|\mathbb{Q}) = I \bar{I}$.

Proposição 47. Se $n \in \mathbb{N}$ é tal que $n \neq 2m$, para algum $m \in \mathbb{Z}$, m ímpar, então os únicos ideais primos de $\mathbb{Z}$ que se ramificam em $\mathbb{Z}[\zeta_n]$ são da forma $\mathfrak{p} = \langle p \rangle$, onde p é primo e p divide n .

Proposição 48. Seja $\mathcal{D}(\mathbb{L}|\mathbb{K}) = \prod_{i=1}^r \mathfrak{q}_i^{s_i}$, onde $\mathfrak{q}_i$'s são ideais primos de $O_{\mathbb{L}}$ e $s_i \geq 0$ são inteiros.

Para todo $i = 1, \dots, r$, seja $\mathfrak{p}_i = \mathfrak{q}_i \cap \mathcal{A}$. Se $\mathfrak{p}_i O_{\mathbb{L}} = \left(\prod_{j=1}^k \tau_j^{a_j} \right) \mathfrak{q}_i^{e_i}$ é a fatoração de $\mathfrak{p}_i O_{\mathbb{L}}$ em um produto de ideais de $O_{\mathbb{L}}$, então $s_i \geq e_i - 1$, para $i = 1, \dots, n$.

5 O reticulado E_8 via $\mathbb{Q}(\zeta_{20})$

Vamos mostrar que escolhendo adequadamente um ideal fracionário $\mathfrak{I}$ de $\mathbb{Q}(\zeta_{20})$ o reticulado ideal obtido $(\mathfrak{I}, b)$ de dimensão 8 possui a mesma paridade e o mesmo determinante do reticulado E_8 , podendo assim ser identificado com o E_8 .

Para tanto, seja $\mathbb{K} = \mathbb{Q}(\zeta_{20})$ o 20-ésimo corpo ciclotômico. Temos que

$$[\mathbb{K} : \mathbb{Q}] = \varphi(20) = \varphi(2^2 \cdot 5) = \varphi(2^2)\varphi(5) = 1 \cdot 2^1 \cdot 4 \cdot 5^0 = 8.$$

Vamos fatorar o diferente $\mathcal{D}(\mathbb{K}|\mathbb{Q})$. Como 2 e 5 são os únicos primos que dividem 20. Pela Proposição (47), segue que os ideais gerados por 2 e 5, respectivamente, são os únicos ideais primos de $\mathbb{Z}$ que se ramificam em $\mathbb{Z}[\zeta_{20}]$.

Como $\phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1 = \min_{\mathbb{Q}} \zeta_{20}$, segue que $\bar{\phi}_{20}(x) = (\bar{1} + x + x^2 + x^3 + x^4)^2 \pmod{\mathbb{Z}_2[x]}$ e $\bar{\phi}_{20}(x) = (\bar{2} + x)^4(\bar{3} + x)^4 \pmod{\mathbb{Z}_5[x]}$. Assim, pelo Teorema (37),

$$2\mathbb{Z}[\zeta_{20}] = \mathfrak{q}^2, \text{ onde } \mathfrak{q} = \langle 2, 1 + \zeta_{20} + \zeta_{20}^2 + \zeta_{20}^3 + \zeta_{20}^4 \rangle \text{ e}$$

$$5\mathbb{Z}[\zeta_{20}] = \mathfrak{s}^4\mathfrak{r}^4, \text{ onde } \mathfrak{s} = \langle 5, 2 + \zeta_{20} \rangle \text{ e } \mathfrak{r} = \langle 5, 3 + \zeta_{20} \rangle.$$

Assim, os únicos ideais primos de $\mathbb{Z}[\zeta_{20}]$ que se ramificam são $\mathfrak{q}$, $\mathfrak{s}$ e $\mathfrak{r}$, sendo estes os únicos ideais primos de $\mathbb{Z}[\zeta_{20}]$ que dividem o diferente $\mathcal{D}(\mathbb{K}|\mathbb{Q})$. Logo, pela Proposição (48), segue que $\mathcal{D}(\mathbb{K}|\mathbb{Q}) = \mathfrak{q}^q \mathfrak{s}^s \mathfrak{r}^r$, onde $q \geq 1, r, s \geq 3$.

Temos que $2^8 = |N_{\mathbb{K}/\mathbb{Q}}(2)| = N(\mathfrak{q})^2$ e, assim, $N(\mathfrak{q}) = 2^4$. Agora, como $O_4(5) = 1 \equiv 1 \pmod{2}$, pela Proposição (41), segue que $\bar{\mathfrak{r}} \neq \mathfrak{r}$. Logo $\bar{\mathfrak{r}} = \mathfrak{s}$ e, assim, $N(\mathfrak{r}) = N(\mathfrak{s})$. Desta forma,

$$5^7 = |N_{\mathbb{K}/\mathbb{Q}}(5)| = N(\mathfrak{s})^4 N(\mathfrak{r})^4 = N(\mathfrak{s})^8,$$

o que implica que $N(\mathfrak{r}) = N(\mathfrak{s}) = 5$.

Pelo Teorema (42), $N(\mathcal{D}(\mathbb{K}|\mathbb{Q})) = |\text{Disc}(\mathbb{K}|\mathbb{Q})| = 2^8 5^6$. Assim,

$$N(\mathfrak{q})^q N(\mathfrak{r})^r N(\mathfrak{s})^s = 2^8 5^6,$$

o que implica que $q = 2$ e $r = s = 3$. Portanto,

$$\mathcal{D}(\mathbb{K}|\mathbb{Q}) = \mathfrak{q}^2 \mathfrak{r}^3 \mathfrak{s}^3.$$

Como $\bar{\mathfrak{r}} = \mathfrak{s}$ e $\bar{\mathfrak{q}} = \mathfrak{q}$, podemos escrever

$$\mathcal{D}(\mathbb{K}|\mathbb{Q}) = \mathfrak{q}^2 \mathfrak{r}^3 \mathfrak{s}^3 = \mathfrak{q} \mathfrak{r}^3 \overline{\mathfrak{q} \mathfrak{r}^3} = (\mathfrak{q} \mathfrak{r}^3) \overline{(\mathfrak{q} \mathfrak{r}^3)}.$$

Como o diferente se fatora desta forma, pelo Corolário (46), segue que existe um $O_{\mathbb{K}}$ -reticulado unimodular do tipo traço. Seja $\mathfrak{I} = \mathfrak{r}^{-3} \mathfrak{q}^{-1}$. Considere a aplicação:

$$\begin{aligned} b : \mathfrak{I} \times \mathfrak{I} &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(x\bar{y}) \end{aligned}$$

Tomando $\gamma = \zeta_{20}^2 - \zeta_{20}^4 \in \mathbb{Z}[\zeta_{20}]$ e $\zeta_{20} = \zeta$, temos que

$$\begin{aligned}\gamma + \bar{\gamma} &= \zeta^2 - \zeta^4 + \overline{\zeta^2 - \zeta^4} = \zeta^2 - \zeta^4 + \zeta^{18} - \zeta^{16} = \zeta^8 - \zeta^6 + \zeta^4 + 1 - \zeta^4 + \zeta^{18} - \zeta^{16} \\ &= \zeta^8 - \zeta^6 + 1 + \zeta^8 \zeta^{10} - \zeta^6 \zeta^{10} = \zeta^8 - \zeta^6 + 1 - \zeta^8 + \zeta^6 = 1.\end{aligned}$$

Assim, pela Proposição (43), segue que o $O_{\mathbb{K}}$ -reticulado é par. Agora, pelo Teorema (44),

$$\det(b) = N(\mathfrak{I})^2 |Disc(\mathbb{K}|\mathbb{Q})| = (5^{-3}2^{-4})^2 2^8 5^6 = 1.$$

Portanto, $(\mathfrak{I}, b)$ é um $O_{\mathbb{K}}$ -reticulado par e com determinante 1. Como E_8 é o único reticulado unimodular e par em sua dimensão (CONWAY, SLOANE, 1988), concluímos que $(\mathfrak{I}, b)$ é isomorfo ao reticulado E_8 .

6 Considerações Finais

Neste trabalho foi apresentado uma maneira de se construir o reticulado E_8 via corpos ciclotômicos, porém existem outras maneiras de se construir o reticulado E_8 que não abordamos aqui.

Em 1948, Shannon descobriu que alguns problemas na área de códigos possuem propriedades interessantes no que diz respeito à reticulados. Sempre que transmitimos informações, há uma possibilidade da mensagem recebida ser diferente da mensagem enviada. Visando construir bons códigos para recuperar a mensagem enviada ao receptor, usa-se reticulados com boa densidade de empacotamento.

7 Referências

- [1] BAYER-FLUCKIGER, E. Definite unimodular lattices having an automorphism of given characteristic polynomial. **Commentarii Mathematici Helvetici**. v. 59, p. 509-538, 1984.
- [2] BAYER-FLUCKIGER, E. Lattices and number fields. **Contemporary Mathematics**. v. 241, p. 69-84, 1999.
- [3] BOUTROS, J. et al. Good lattice constellations for both Rayleigh fading and Gaussian channels. **IEEE Transactions on Information Theory**, v. 42, n. 2, p. 502-518, 1996.
- [4] CONWAY, J. H.; SLOANE, N. J. A. **Sphere packings, lattices and groups**. New York: Springer-Verlag, 1988.
- [5] SAMUEL, P. **Algebraic theory of numbers**. Paris: Hermann, 1970.
- [6] STEWART, I. N.; TALL, D. O. **Algebraic number theory**. 2. ed. London: Chapman & Hall, 1987.
- [7] SHANNON, C. E. A Mathematical Theory of Communications. **The Bell System Technical Journal**, v. 27, p. 379-423, 623-656, 1948.
- [8] WASHINGTON, L. C. **Introduction to cyclotomic fields**. New York: Springer-Verlag, 1982.