

Novas construções algébricas de reticulados

Antonio Aparecido de Andrade,

Elen Cristina Mazucchi

Depto de Matemática, IBILCE, UNESP,

15054-000, São José do Rio Preto, SP

E-mail: andrade@ibilce.unesp.br, elen_mazucchi@yahoo.com.br

1 Introdução

Os reticulados vem sendo muito utilizados na Teoria das Comunicações. Sinais de constelações tendo estrutura de reticulados são popularmente conhecidos como bons para transmissão com eficiência espectral elevada. Boas constelações de sinais para o canal Rayleigh com desvanecimento são encontradas usando corpos de números algébricos totalmente reais. A eficácia destas constelações encontra-se no seu elevado grau de diversidade, a qual é de fato a maior possível. Reticulados construídos através da imersão canônica de um corpo de números \mathbb{K} totalmente reais possuem diversidade máxima $L = n$, onde n é o grau de \mathbb{K} . Isso nos motiva a investigar reticulados sobre corpos de números totalmente reais. Neste trabalho apresentamos uma construção algébrica de \mathbb{Z}^n -reticulados, com base na teoria de Ideais Reticulados, e pelo do Teorema de Krüskemper, mostramos que todo reticulado inteiro pode ser compreendido como um ideal reticulado.

1.1 Definições básicas

Introduzimos aqui algumas definições utilizadas no decorrer deste trabalho. Considere $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n .

Definição 1 Um elemento $\alpha \in \mathbb{K}$ é chamado inteiro algébrico (ou simplesmente inteiro) sobre \mathbb{Z} se existirem, $a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$. Esta equação é chamada de equação de dependência integral de α .

Exemplo 1 O elemento $\xi_3 = e^{\frac{2\pi i}{3}}$ é inteiro algébrico, pois é raiz do polinômio $x^2 + x + 1$.

Definição 2 Considere os distintos n monomorfismos $\sigma_j : \mathbb{K} \rightarrow \mathbb{C}$. Se $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$, diz-se que σ_j é real, caso contrário, σ_j é dito imaginário. Quando todos os monomorfismos são reais diz-se que \mathbb{K} é um corpo totalmente real e quando os monomorfismos são todos imaginários diz-se que \mathbb{K} é um corpo totalmente imaginário.

Definição 3 Sejam $\sigma_1, \sigma_2, \dots, \sigma_n$, os distintos monomorfismos de \mathbb{K} em \mathbb{C} , e seja $\alpha \in \mathbb{K}$. Defi-

nimos o traço de α por $Tr(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$, a norma

por $N(\alpha) = \det(\sigma_i(\alpha)) = \prod_{i=1}^n \sigma_i(\alpha)$ e o polinômio característico por $m_\alpha(x) = \det(xI - \sigma_i(\alpha)) = x^n - (Tr(\alpha))x^{n-1} + \dots + (-1)^n \det(\alpha)$.

Definição 4 O conjunto $\mathcal{O}_{\mathbb{K}}$ dos elementos de \mathbb{K} que são inteiros sobre \mathbb{Z} é um anel, chamado anel de inteiros de \mathbb{K} .

Definição 5 O anel de inteiros de \mathbb{K} , $\mathcal{O}_{\mathbb{K}}$, é um \mathbb{Z} -módulo livre de posto $n = [\mathbb{K} : \mathbb{Q}]$, cuja base é chamada de base integral de \mathbb{K} (ou de $\mathcal{O}_{\mathbb{K}}$).

Definição 6 Uma ordem \mathcal{D} de \mathbb{K} é um subanel de \mathbb{K} que como um \mathbb{Z} -módulo livre é finitamente gerado e tem posto máximo $n = [\mathbb{K} : \mathbb{Q}]$. Como $\mathcal{O}_{\mathbb{K}}$ é um subanel de \mathbb{K} , também chamamos $\mathcal{O}_{\mathbb{K}}$ de ordem máxima de \mathbb{K} .

Definição 7 Seja $\{w_1, w_2, \dots, w_n\} \subseteq \mathbb{K}$. Definimos o discriminante do conjunto $\{w_1, w_2, \dots, w_n\}$ por $D(w_1, w_2, \dots, w_n) = \det(Tr(w_i w_j))$, para $i, j = 1, \dots, n$. Se $\{w_1, w_2, \dots, w_n\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$, $D_{\mathbb{K}} = D(w_1, w_2, \dots, w_n)$ é chamado de discriminante absoluto de \mathbb{K} .

Definição 8 O grupo quociente $C(\mathbb{K}) = \frac{I(\mathbb{K})}{F(\mathbb{K})}$ é chamado grupo das classes de ideais de \mathbb{K} , onde $I(\mathbb{K})$ é o grupo dos ideais fracionários não nulos de \mathbb{K} , e $F(\mathbb{K})$ é o subgrupo dos ideais fracionários principais de \mathbb{K} . O número $h(\mathbb{K}) = \#C(\mathbb{K})$ é a cardinalidade do grupo das classes de ideais de \mathbb{K} .

Definição 9 Seja M um subconjunto de \mathbb{K} . O conjunto $M^* = \{x \in \mathbb{K} : Tr(xy) \in \mathcal{O}_{\mathbb{K}}, \forall y \in M\}$ é definido como o codiferente de M sobre \mathbb{K} .

Definição 10 Um reticulado Λ é um subconjunto discreto do \mathbb{R}^n gerado por um \mathbb{Z} -módulo livre.

Definição 11 Sejam Λ um reticulado n -dimensional e $x = (x_1, \dots, x_n) \in \Lambda$.

1. A diversidade de x , denotado por $div(x)$, é o número de x_i 's não nulos;

2. A diversidade de Λ é definida por $\text{div}(\Lambda) = \min\{\text{div}(x) \mid x \in \Lambda, x \neq 0\}$.

Definição 12 Seja Λ um reticulado n -dimensional com diversidade $L = n$. Definimos a distância produto de $x = (x_1, x_2, \dots, x_n)$ por $d_p(x) = \prod_{i=1}^n |x_i|$ e a distância produto mínima de Λ por $d_{p,\min}(\Lambda) = \min_{x \in \Lambda} d_p(x), x \neq 0$.

2 Ideal reticulado

Um método para gerar reticulados no \mathbb{R}^n é obtido através do homomorfismo canônico de um corpo. Os reticulados assim gerados dependem diretamente do anel de inteiros do corpo de números.

Sejam $\sigma_1, \dots, \sigma_{r_1}$ os monomorfismos reais e $\sigma_{r_1+1}, \dots, \sigma_{r_1+2r_2}$ os pares de monomorfismos imaginários. Assim, $n = r_1 + 2r_2$ e para cada $x \in \mathbb{K}$, temos que o homomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \rightarrow \mathbb{R}^n$ definido por

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \dots, \sigma_{r_1+2r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2},$$

é um homomorfismo injetivo de anéis, chamado de homomorfismo canônico ou homomorfismo de Minkowski de \mathbb{K} em $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$. Geralmente identificamos $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ com \mathbb{R}^n , e este homomorfismo também pode ser visto como

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \dots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \dots, \Re\sigma_{r_1+2r_2}(x), \Im\sigma_{r_1+2r_2}(x)),$$

onde \Re representa a parte real do número complexo e \Im representa a parte imaginária.

Proposição 1 [3] Seja \mathbb{K} um corpo de números de grau n . Se $M \subseteq \mathbb{K}$ é um \mathbb{Z} -módulo livre de posto n e se $(x_j)_{1 \leq j \leq n}$ é uma \mathbb{Z} -base de M , então $\sigma_{\mathbb{K}}(M)$ é um reticulado no \mathbb{R}^n , com volume

$$\text{Vol}(\sigma_{\mathbb{K}}(M)) = 2^{-r_2} |\det_{1 \leq j, k \leq n} (\sigma_j(x_k))|,$$

onde r_2 é o número de pares de monomorfismos imaginários.

Definição 13 Um ideal reticulado é um reticulado (\mathcal{I}, b) , onde \mathcal{I} é um ideal de $\mathcal{O}_{\mathbb{K}}$, $b : \mathcal{I} \times \mathcal{I} \rightarrow \mathbb{Z}$ é tal que $b(x, y) = \text{Tr}(\alpha xy), \forall x, y \in \mathcal{I}$ e $\alpha \in \mathbb{K}$ é totalmente positivo, isto é, $\sigma_i(\alpha) > 0$, para todo i .

Definição 14 Seja $\{w_1, \dots, w_n\}$ uma \mathbb{Z} -base do ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$. Considere a perturbação da imersão canônica $\sigma_{\alpha} : \mathbb{K} \rightarrow \mathbb{R}^n$ definida como

$$\sigma_{\alpha}(x) = (\sqrt{\alpha_1}\sigma_1(w_1), \dots, \sqrt{\alpha_n}\sigma_n(w_n)),$$

onde $\alpha_i = \sigma_i(\alpha) > 0$, para $i = 1, \dots, n$.

Definição 15 Usando a perturbação da imersão canônica, a matriz geradora M do reticulado $\Lambda = \sigma_{\alpha}(\mathcal{I})$ é dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(w_1) & \sqrt{\alpha_2}\sigma_2(w_1) & \cdots & \sqrt{\alpha_n}\sigma_n(w_1) \\ \sqrt{\alpha_1}\sigma_1(w_2) & \sqrt{\alpha_2}\sigma_2(w_2) & \cdots & \sqrt{\alpha_n}\sigma_n(w_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(w_n) & \sqrt{\alpha_2}\sigma_2(w_n) & \cdots & \sqrt{\alpha_n}\sigma_n(w_n) \end{pmatrix}.$$

Observação 1 De modo análogo, ao homomorfismo canônico, temos que $\sigma_{\alpha}(\mathcal{I})$ é um reticulado.

Proposição 2 [1] O reticulado $\sigma_{\alpha}(\mathcal{I})$ tem diversidade $r_1 + r_2$.

Proposição 3 [1] Um ideal reticulado $\Lambda = (\mathcal{I}, b)$ pode ser imerso no \mathbb{R}^n , com diversidade

- i) n se \mathbb{K} é totalmente real.
- ii) $\frac{n}{2}$ se \mathbb{K} é totalmente complexo.

Pela Proposição 3 a diversidade máxima é atingida quando trabalhamos com corpos de números totalmente reais. Portanto consideraremos de agora em diante $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números totalmente real de grau n .

Teorema 1 [4] Seja \mathbb{K} um corpo de números totalmente real com discriminante $D_{\mathbb{K}}$, \mathcal{D} uma ordem de \mathbb{K} e \mathcal{I} um ideal principal de \mathcal{D} . A distância produto mínima de um ideal reticulado de determinante $\det(\Lambda)$ definido sobre \mathcal{I} é

$$d_{p,\min} = \sqrt{\frac{\det(\Lambda)}{D_{\mathbb{K}} [\mathcal{O}_{\mathbb{K}} : \mathcal{D}]}}.$$

Krüskenper [2] provou que toda forma \mathbb{Z} -bilinear simétrica não degenerada pode se realizar como uma forma traço sobre $\mathbb{Z}[\theta]$, onde θ é um inteiro algébrico. Com base neste resultado, provamos que todo reticulado inteiro pode ser compreendido como um ideal reticulado. Para isso, seja L um \mathbb{Z} -módulo livre finitamente gerado de rank n e seja $b : L \times L \rightarrow \mathbb{Z}$ uma forma bilinear simétrica. Seja $f(x)$ um polinômio mônico irredutível de grau n e $\theta \in \mathbb{C}$ uma raiz de $f(x)$. Então $\frac{\mathbb{Z}[x]}{\langle f(x) \rangle} = \mathbb{Z}[\theta]$, cuja base é $\{1, \theta, \dots, \theta^{n-1}\}$. Seja \mathcal{I} um ideal de $\mathbb{Z}[\theta]$ e \mathcal{I}^* o codiferente de \mathcal{I} .

Teorema 2 [4] Seja (L, b) um reticulado. Então existe um inteiro algébrico θ , um ideal \mathcal{I} de $\mathbb{Z}[\theta]$ e $\alpha \in (\mathcal{I}^2)^* \subseteq \mathbb{Q}(\theta)$ tal que b é isomorfa a

$$\mathcal{I} \times \mathcal{I} \rightarrow \mathbb{Z}$$

$$(x, y) \rightarrow \text{Tr}(\alpha xy).$$

Com base no Teorema 2, fornecemos o algoritmo de construção do reticulado.

1. Primeiramente precisamos encontrar uma matriz simétrica A , com coeficientes em \mathbb{Z} , tal que seu polinômio característico seja irredutível. A pode ser tomada aleatoriamente.

2. Considere

$$v_j = (-1)^{i+j} \Delta_{ij}(A - \theta I_n),$$

isto é, v_j é o j -ésimo cofator em uma dada coluna da matriz $(A - \theta I_n)$, e construa o vetor

$$v_\theta = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}.$$

3. Calcule V e G , onde V é a matriz das coordenadas de v_1, \dots, v_n na base $\{1, \theta, \dots, \theta^{n-1}\}$ e G é a matriz dada por $G = (Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^{i-1}\theta^{j-1}))_{i,j=1}^n$.

4. Calcule o vetor v_θ° tal que

$$v_\theta^\circ = \sum_{i=1}^n m_{ij} \theta^{i-j},$$

onde $(m_{ij})_{i,j=1}^n = G^{-1}(V^t)^{-1}$.

5. Tome $\alpha = \frac{v_i}{v_i}$, para algum $i \in \{1, \dots, n\}$.

6. A matriz geradora do reticulado é dada por

$$\begin{pmatrix} \sqrt{\alpha_1} \sigma_1(v_1) & \cdots & \sqrt{\alpha_n} \sigma_n(v_1) \\ \sqrt{\alpha_1} \sigma_1(v_2) & \cdots & \sqrt{\alpha_n} \sigma_n(v_2) \\ \vdots & \ddots & \vdots \\ \sqrt{\alpha_1} \sigma_1(v_n) & \cdots & \sqrt{\alpha_n} \sigma_n(v_n) \end{pmatrix}.$$

Note que $RR^t = I_n$.

Exemplo 2 Para a dimensão $n = 2$, escolha

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

O polinômio característico de A , é $\chi_A = x^2 - x - 1$, que é irredutível sobre \mathbb{Z} .

Escolhendo $i = 2$ e fazendo os cálculos temos que

$$v_\theta = \begin{pmatrix} -1 \\ 1 - \theta \end{pmatrix}.$$

Logo,

$$V = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \text{ e}$$

$$(V^t)^{-1} = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}.$$

Temos que $Tr(1) = 3$ e pela definição 3, $Tr(\theta) = 1$. O elemento θ é raiz de $x^2 - x - 1$, logo, $\theta^2 = \theta + 1$

e dessa forma, $Tr(\theta^2) = Tr(\theta) + Tr(1) = 1 + 2 = 3$. Assim,

$$G = (Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^{i-1}\theta^{j-1}))_{i,j=1}^2$$

$$G = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix},$$

$$G^{-1} = \begin{pmatrix} \frac{3}{5} & -\frac{1}{5} \\ -\frac{1}{5} & \frac{2}{5} \end{pmatrix} \text{ e}$$

$$G^{-1}(V^t)^{-1} = \begin{pmatrix} -\frac{2}{5} & \frac{1}{5} \\ -\frac{1}{5} & -\frac{1}{5} \end{pmatrix}.$$

Assim,

$$v_j^\circ = \sum_{i=1}^2 m_{ij} \theta^{i-1}, \text{ e portanto,}$$

$$v_\theta^\circ = \begin{pmatrix} -\frac{2}{5} - \frac{1}{5}\theta \\ \frac{1}{5} - \frac{1}{5}\theta \end{pmatrix}.$$

Escolhendo $i = 1$, temos que $\alpha = \frac{v_1}{v_1} = \frac{2}{5} + \frac{1}{5}\theta$. O

conjunto das raízes de χ_A é $\left\{ \frac{1}{2} + \frac{1}{2}\sqrt{5}, \frac{1}{2} - \frac{1}{2}\sqrt{5} \right\}$.

Logo as imersões reais de θ são $\sigma_1(\theta) = 1, 61833989$ e $\sigma_2(\theta) = -0, 61833989$. Assim, a matriz geradora do reticulado é dada por

$$R = \begin{pmatrix} -0, 850686768 & -0, 525672923 \\ -0, 525672923 & 0, 850686768 \end{pmatrix}.$$

Neste caso temos que $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, assim, $D_{\mathbb{K}} = 5$. Como todos ideais de $\mathbb{Q}(\sqrt{5})$ são principais, temos que $h(\mathbb{K}) = 1$ e $[\mathcal{O}_{\mathbb{K}} : \mathcal{D}] = 1$. Logo, a distância produto mínima de Λ é $d_{p,\min}(\Lambda) = \frac{1}{\sqrt{5}}$.

Referências

- [1] E. Bayer-Fluckger, Lattices and number fields, Contemporary Mathematics, vol.241, pp. 69-84, 1999.
- [2] M. Kruskemper, Algebraic construction of bilinear forms over \mathbb{Z} , Pub. Math. de Besancon, Théorie des nombres, 1996/97 - 1997/98.
- [3] I.N.Stewart and D.O.Tall, "Algebraic Number Theory", Chapman & Hall, second edition, 1987.
- [4] E. Viterbo, Best constructions of rotated cubic lattice constellations in small dimension for the Rayleigh fading channel, preprint.