3 - Reticulados

Carina Alves
Antonio Aparecido de Andrade

ALVES, C., and ANDRADE, AA. Reticulados. In: *Reticulados via corpos ciclotômicos* [online]. São Paulo: Editora UNESP, 2014, pp. 107-133. ISBN 978-85-68334-39-3. Available from SciELO Books <http://books.scielo.org>.

3
Reticulados

3.1 Introdução

Os reticulados têm se mostrado bastante úteis em aplicações na Teoria das Comunicações. Intuitivamente, um reticulado no $\mathbb{R}^n$ é um conjunto infinito de pontos dispostos de forma regular.

Neste capítulo apresentamos as definições de reticulado, empacotamento esférico, densidade de empacotamento, densidade de centro e homomorfismo canônico. Através do homomorfismo canônico obtemos um método de gerar reticulados no $\mathbb{R}^n$. Os reticulados obtidos desta maneira dependem diretamente do anel dos inteiros de um corpo de números. O grande desafio é encontrar o anel dos inteiros de qualquer corpo de números, uma vez que são conhecidos apenas o anel dos inteiros dos corpos quadráticos e dos corpos ciclotômicos.

Deste modo, no presente capítulo apresentamos um estudo sobre reticulados no $\mathbb{R}^n$, explicitando alguns reticulados construtivos

conhecidos na literatura via o homomorfismo canônico. Lembramos que os reticulados de maior interesse são aqueles com maior densidade de empacotamento.

3.2 Reticulados

Nesta seção apresentamos o conceito de reticulados enfocando suas principais propriedades.

Definição 3.2.1. *Sejam V um espaço vetorial de dimensão finita n sobre um corpo $\mathbb{K}$, $A \subseteq \mathbb{K}$ um anel e $v_1, \cdots, v_m$ vetores de V linearmente independentes sobre $\mathbb{K}$, com $m \leq n$. Chama-se* **reticulado** *com base $\beta = \{v_1, \cdots, v_m\}$ ao conjunto dos elementos de V da forma*

$$\left\{ x = \sum_{i=1}^{m} a_i v_i, \ \ com\ a_i \in A \right\},$$

que será denotado por H_β.

Nosso interesse maior será nos casos em que $\mathbb{K} = \mathbb{R}$, $A = \mathbb{Z}$, $V = \mathbb{R}^n$ e $m = n$.

Definição 3.2.2. *Seja $H_\beta \subset \mathbb{R}^n$ um reticulado, com $\mathbb{Z}$-base $\beta = \{v_1, \cdots, v_n\}$. O conjunto*

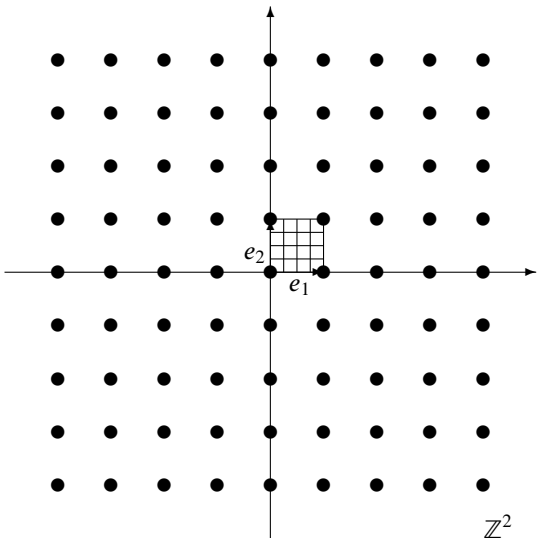
$$P_\beta = \left\{ x \in \mathbb{R}^n \ : \ x = \sum_{i=1}^{n} \lambda_i v_i, \ 0 \leq \lambda_i < 1 \right\},$$

é chamado de **região fundamental** *de H_β com relação a base $\{v_1, \cdots, v_n\}$.*

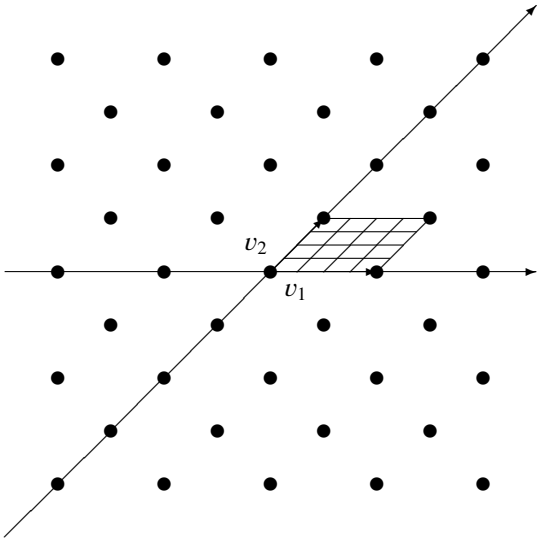
Se H_β é um reticulado com base $\beta = \{v_1, \cdots, v_n\}$ e se $c_1, \cdots, c_n$ são elementos quaisquer de H_β, então $c_i = \sum_{j=1}^{n} a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$.

Temos que uma condição necessária e suficiente para que $\{c_1, \cdots, c_n\}$ seja uma base de H_β é que $\det(a_{ij})$ seja um elemento inversível de $\mathbb{Z}$.

Exemplo 3.2.1. *$H_\beta = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$ com região fundamental descrita na figura abaixo.*



Exemplo 3.2.2. *$H_\beta = \{(a, b) \in \mathbb{Z}^2; a + b \equiv 0 (mod\ 2)\}$ é um reticulado gerado pelos vetores $v_1 = (2, 0)$ e $v_2 = (1, 1)$ com região fundamental descrita pela figura abaixo.*



Definição 3.2.3. *Um subgrupo H do $\mathbb{R}^n$ é* **discreto** *se para qualquer subconjunto compacto $\mathbb{K}$ do $\mathbb{R}^n$, tivermos $H \cap \mathbb{K}$ finito.*

Exemplo 3.2.3. *Um típico exemplo de subconjunto discreto do $\mathbb{R}^n$ é $\mathbb{Z}^n$.*

O próximo teorema nos diz que um reticulado é gerado sobre $\mathbb{Z}$ por uma base do $\mathbb{R}^n$, a qual é então, uma $\mathbb{Z}$-base do reticulado dado.

Teorema 3.2.1. *(*Samuel, 1967, p.53, Teo.1*) Se H é um subgrupo discreto do $\mathbb{R}^n$, então H é gerado como um $\mathbb{Z}$-módulo por r vetores linearmente independentes sobre $\mathbb{R}$, com $r \leq n$.*

Demonstração. Seja $\beta = \{e_1, \cdots, e_r\}$ um conjunto de vetores de H que são linearmente independentes sobre $\mathbb{R}$, onde r é o maior possível com $r \leq n$. Seja o paralelepípedo

$$P_\beta = \left\{ x \in \mathbb{R}^n \,:\, x = \sum_{i=1}^{r} \alpha_i e_i,\ 0 \leq \alpha_i \leq 1 \right\}$$

construído a partir destes vetores. Como P_β é fechado e limitado, segue que P_β é compacto. Assim, $P_\beta \cap H$ é finito pois H é discreto. Se $x \in H$ então pela maximalidade de r, segue que $\{x, e_1, \cdots, e_r\}$ é linearmente dependente. Logo existem $\lambda_i \in \mathbb{R}$, $i = 1, \cdots, r$, não todos nulos, tal que $x = \sum_{i=1}^{r} \lambda_i e_i$. Para cada $j \in \mathbb{N}$, seja

$$x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i \in H, \tag{3.1}$$

onde [k] denota o maior inteiro menor ou igual a k. Assim,

$$x_j = j \sum_{i=1}^{r} \lambda_i e_i - \sum_{i=1}^{r} [j\lambda_i] e_i = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i]) e_i \in P_e \cap H.$$

Dessa forma, se tomarmos $j = 1$ na Equação 3.1 temos que $x_1 = x - \sum_{i=1}^{r} [\lambda_i] e_i$, ou seja, $x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i$. Assim, como $x_1 \in P_e \cap H$ e este é finito, segue que H é finitamente gerado como um $\mathbb{Z}$-módulo. Por outro lado, do fato de $P_e \cap H$ ser finito e $\mathbb{N}$ ser infinito, existem inteiros j e k, tais que $x_j = x_k$. Da Equação (3.1), segue que $x_j = x_k \Longrightarrow jx - \sum_{i=1}^{r} [j\lambda_i] e_i = kx - \sum_{i=1}^{r} [k\lambda_i] e_i \Longrightarrow (j-k)x = \sum_{i=1}^{r} ([j\lambda_i] - [k\lambda_i]) e_i \Longrightarrow (j-k) \sum_{i=1}^{r} \lambda_i e_i = \sum_{i=1}^{r} ([j\lambda_i] - [k\lambda_i]) e_i \Longrightarrow (j-k)\lambda_i = [j\lambda_i] - [k\lambda_i] \Longrightarrow \lambda_i = \dfrac{[j\lambda_i] - [k\lambda_i]}{(j-k)}$, ou seja, $\lambda_i \in \mathbb{Q}$. Assim, H é gerado como um $\mathbb{Z}$-módulo por um número finito de elementos, que são combinações lineares com coeficientes racionais dos $e_i's$. Seja $d \neq 0$ um denominador comum destes coeficientes. Consideremos o conjunto dH. Temos que $dH \subset \sum_{i=1}^{r} \mathbb{Z} e_i$. Daí, pelo Teorema 1.2.1, segue que existe uma base $\{f_1, \cdots, f_r\}$ do $\mathbb{Z}$-módulo $\sum_{i=1}^{r} \mathbb{Z} e_i$ e inteiros α_i, tal que $\{\alpha_1 f_1, \cdots, \alpha_r f_r\}$ gera dH sobre $\mathbb{Z}$. Como o $\mathbb{Z}$-módulo dH tem o mesmo posto de H e como $\sum_{i=1}^{r} \mathbb{Z} e_i \subset H$,

segue que o posto de $dH \geq r$. Pela maximalidade de r decorre que o posto de dH é r e os $\alpha_i's$ são não nulos, pois caso contrário dH não teria posto r. Assim os $f_i's$ são linearmente independentes sobre $\mathbb{R}$, uma vez que $\{e_1, \cdots, e_r\}$ é linearmente independente sobre $\mathbb{R}$. Portanto, dH é gerado por r vetores linearmente independentes sobre $\mathbb{R}$ e consequentemente H também é gerado por r vetores linearmente independentes sobre $\mathbb{R}$. ■

Observação 3.2.1. *Segue do Teorema* 3.2.1 *que um subgrupo discreto do* $\mathbb{R}^n$ *é um reticulado.*

3.3 Empacotamento esférico

A Teoria dos Códigos Corretores de Erros nasceu em 1948, com o famoso trabalho de Shannon (1948), onde foi demonstrado o Teorema da Capacidade do Canal. Em linhas gerais, este resultado diz que para a transmissão de dados abaixo de uma certa taxa C (símbolos por segundo), chamada de capacidade do canal, é possível obter a probabilidade de erro tão pequena quanto se deseja através de códigos corretores de erros eficientes.

A prova do Teorema da Capacidade do Canal implica que no caso de valores altos da relação sinal-ruído (SNR), um código de bloco ótimo para um canal com ruído gaussiano branco (AWGN), limitado em faixa, consiste em um empacotamento denso de sinais dentro de uma esfera, no espaço euclidiano n-dimensional, para n suficientemente grande. Assim, se estabeleceu o vínculo entre empacotamento esférico e Teoria da Informação.

Para cada n, Minkowski provou a existência de reticulados no espaço euclidiano n-dimensional com densidade de empacotamento esférico δ satisfazendo

$$\delta \geq \frac{\zeta(n)}{2^{n-1}},$$

onde ζ é a função zeta de Riemann. Como consequência, obtém-se

$$\frac{1}{n} log_2 \delta \geq -1. \tag{3.2}$$

Depois disto, Leech mostrou como usar códigos corretores de erros para construir empacotamentos esféricos densos no $\mathbb{R}^n$, Conway e Sloane (1999) provaram que reticulados satisfazendo a cota de Minkowski, dada pela Equação (3.2) são equivalentes a códigos atingindo a capacidade do canal.

O problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no espaço Euclidiano n-dimensional de forma que a fração do espaço coberto por essas esferas seja a maior possível. Isto pode ser visto como a versão euclidiana do 18º Problema de Hilbert, proposto em 1900.

Dentre os métodos de geração de reticulados, o homomorfismo de Minkowski apresenta características interessantes. Usando Teoria Algébrica dos Números, Craig (1978) reproduziu o reticulado de Leech Λ_{24} através da representação geométrica de um ideal no anel de inteiros de $\mathbb{Q}(\zeta_{39})$. Com o mesmo método, ainda obteve a família A_n^m em dimensões $n = p - 1$, através de $\mathbb{Q}(\zeta_p)$, onde p é um número primo.

Ao estudar a densidade de empacotamento, um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo manipuláveis.

Para que possamos prosseguir no estudo de reticulados, precisamos da noção de **volume**. O volume no $\mathbb{R}^n$ é bem conhecido e pode ser facilmente transferido para o $\mathbb{R}$-espaço V através do isomorfismo natural entre $\mathbb{R}^n$ e V, e definido por meio de uma base $\{v_1, \ldots, v_n\}$. Além disso, é possível restringir a subconjuntos C de

V que são reuniões finitas da região fundamental, usando apenas as seguintes propriedades de volume:

a) $Vol(x + C) = Vol(C)$, para todo $x \in V$.
b) $Vol(\gamma C) = \gamma^n Vol(C)$, para todo $\gamma \in \mathbb{R},\ \gamma > 0$.
c) Se $C \cap C' = \emptyset$, então $Vol(C \cup C') = Vol(C) + Vol(C')$.

Definição 3.3.1. *Sejam $H \subseteq \mathbb{R}^n$ um reticulado, $\beta = \{v_1, \cdots, v_n\}$ uma base de H e P_β a região fundamental. Se $v_i = (v_{i1}, v_{i2}, \cdots, v_{in})$, para $i = 1, 2, \cdots, n$, definimos o volume da região fundamental P_β, como o módulo do determinante da matriz*

$$B = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix}.$$

Proposição 3.3.1. *(*SAMUEL, 1967, p.55, Lema.1*) O volume da região fundamental $Vol(P_\beta)$ é independente da base β de H.*

Demonstração. Se $f = \{f_1, \ldots, f_n\}$ é uma outra base de H, então, $f_i = \sum_{j=1}^{n} \alpha_{ij} v_j$, com $\alpha_{ij} \in \mathbb{Z}$. Assim, $Vol(P_f) = |\det(\alpha_{ij})| Vol(P_v)$. Como a matriz de mudança de base (α_{ij}) é inversível, segue que $\det(\alpha_{ij}) = \pm 1$. Portanto, $Vol(P_f) = Vol(P_v)$. ■

Definição 3.3.2. *Seja $H_\beta \subseteq \mathbb{R}^n$ um reticulado com base $\beta = \{v_1, v_2, \cdots,$*
$v_n\}$. Definimos o volume do reticulado H_β como $Vol(H_\beta) = Vol(P_\beta)$.

Observamos que, sendo β' uma outra base para H_β, segue que $Vol(H_\beta) = Vol(H_{\beta'})$, pois β e β' diferem pelo produto de uma matriz inversível com entradas inteiras. Dessa forma, faz sentido

definir o volume de H_β como sendo o volume de uma região fundamental.

Definição 3.3.3. **a)** *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 intersecção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*
b) *Um* **empacotamento reticulado** *é um empacotamento em que o conjunto dos centros das esferas formam um reticulado* H_β *de* $\mathbb{R}^n$.
c) *Dado um empacotamento no* $\mathbb{R}^n$, *associado a um reticulado* H_β, *com* $\beta = \{v_1, \cdots, v_n\}$ *uma* $\mathbb{Z}$*-base, definimos a sua* **densidade de empacotamento** *como sendo a proporção do espaço* $\mathbb{R}^n$ *coberta pela união das esferas.*

Estamos interessados no empacotamento associado a um reticulado H_β em que as esferas tenham raio máximo. Para a determinação deste raio, observe que fixado $k > 0$, a intersecção do conjunto compacto $\{x \in \mathbb{R}^n; |x| \leq k\}$ com o reticulado H_β é um conjunto finito, de onde segue que o número $H_{\beta_{min}} = min\{|\lambda|; \lambda \in H_\beta, \lambda \neq 0\}$ está bem definido e $(H_{\beta_{min}})^2$ é chamado de **norma mínima**. Observamos que $\rho = H_{\beta_{min}}/2$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de H_β e obter um empacotamento. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados.

Denotando por $B(\rho)$ a esfera com centro na origem e raio ρ, temos que a **densidade de empacotamento** de H_β é igual a

$$\Delta(H_\beta) = \frac{\text{Volume da região coberta pelas esferas}}{\text{Volume da região fundamental}} = \frac{Vol(B(\rho))}{Vol(H_\beta)} =$$

$$\frac{Vol(B(1))\rho^n}{Vol(H_\beta)}.$$

Portanto, o problema se reduz ao estudo de um outro parâmetro, chamado de **densidade de centro**, que é dado por

$$\delta(H_\beta) = \frac{\rho^n}{Vol(H_\beta)}.$$

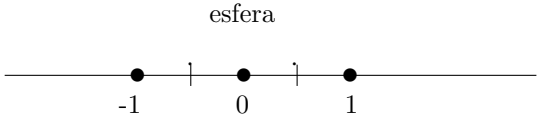
Exemplo 3.3.1. *Se* $H_\beta = \mathbb{Z}^2$ *com base* $(1,0)$ *e* $(0,2)$, *temos que* $\rho = 1/2$, $Vol(B(1)) = \pi.1 = \pi$, *o volume do reticulado é* $Vol(H_\beta) = 1.2 = 2$, *a densidade de empacotamento é*

$$\Delta(H_\beta) = Vol(B(1)).\frac{\rho^2}{Vol(H_\beta)} = \pi\frac{1}{4}.\frac{1}{2} = \frac{\pi}{8}$$

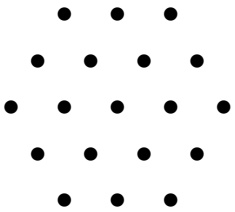
e a densidade de centro é $\delta(H_\beta) = 1/8$.

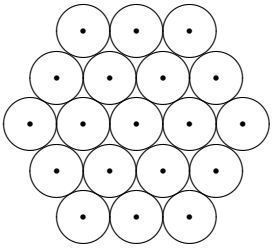
Exemplo 3.3.2. *Seja* $H_\beta = \mathbb{Z}^n$ *um reticulado do* $\mathbb{R}^n$, *gerado pelos vetores* $v_1 = (1,0,\dots,0), v_2 = (0,1,\dots,0), \dots, v_n = (0,0,\dots,1)$. *A forma quadrática* $|v|^2 = x_1^2 + \cdots + x_n^2$ *assume o valor mínimo quando um dos* $x_i = 1$, *para* $i = 1, \cdots, n$ *e os demais nulos. Assim* $|v|^2 = 1$ *e* $\rho = \frac{1}{2}$. *Visto que* $v(H_\beta) = |\det B|$, *e* B *neste caso é a matriz identidade, temos que o* $Vol(H_\beta) = 1$, *e portanto,* $\delta(H_\beta) = \frac{1}{2^n}$.

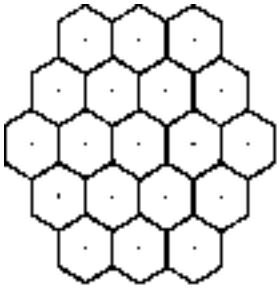
Um dos problemas de empacotamento esférico de um reticulado H_β do $\mathbb{R}^n$ é encontrar um empacotamento com maior densidade. Em dimensão um, temos que os pontos de coordenadas inteiras da reta formam um $\mathbb{Z}$-reticulado cuja a densidade de empacotamento é a melhor possível dada por $\Delta = 1$. Neste caso, as "esferas" são intervalos como podemos ver na figura abaixo.



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







Em dimensão três Gauss mostrou em 1831 que o reticulado fcc, é o empacotamento com maior densidade (pirâmides de laranjas), sendo essa $\Delta = \dfrac{\pi}{\sqrt{18}} \approx 0,7405$.

Já para dimensões $n \geq 4$ conhece-se apenas algumas densidades de determinados empacotamentos, mais ainda não se sabe qual a maior densidade.

3.4 Reticulados importantes e suas propriedades

Nesta seção descreveremos as propriedades de alguns reticulados construtivos importantes conhecidos na literatura.

Definição 3.4.1. *Dizemos que um reticulado é equivalente a outro se este pode ser obtido do outro por rotação ou translação.*

1. **Reticulado cúbico n-dimensional $\mathbb{Z}^n$:** Temos que $\mathbb{Z}^n = \{(x_1, x_2, \ldots, x_n);\ x_i \in \mathbb{Z}\}$ é um reticulado chamado de cúbico. A sua matriz geradora $\boldsymbol{B}$ é a matriz identidade. Assim, $det\mathbb{Z}^n = 1$ e a norma mínima igual a 1, o raio de empacotamento é $\rho = \frac{1}{2}$, sua densidade de empacotamento é $\Delta = V_n 2^{-n}$ e sua densidade de centro é $\delta = 2^{-n}$. Desta forma $\mathbb{Z}$ tem densidade de empacotamento $\Delta = 1$, e as densidades de $\mathbb{Z}^2$, $\mathbb{Z}^3$, $\mathbb{Z}^4$ são $\Delta = \frac{\pi}{4} \approx 0.785$, $\Delta = \frac{\pi}{6} \approx 0.524$ e $\Delta = \frac{\pi^2}{32} \approx 0.308$, respectivamente.

2. **Reticulado n-dimensional A_n:** Para todo $n \geq 1$, $A_n = \{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1};\ x_0 + x_1 + \cdots + x_n = 0\}$ é um reticulado. Por definição, temos que A_n está contido no hiperplano $\sum_i x_i = 0$ no $\mathbb{R}^{n+1}$, possui uma matriz geradora B,

dada por:

$$B = \begin{bmatrix} -1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & -1 & 1 & \cdots & 0 & 0 \\ . & . & . & . & \cdots & . & . \\ 0 & 0 & 0 & 0 & \cdots & -1 & 1 \end{bmatrix},$$

onde $detA_n = det(BB^t) = n + 1$, norma mínima igual a 2, raio de empacotamento $\rho = \frac{1}{\sqrt{2}}$ e densidade de centro $\delta = 2^{-n/2}(n+1)^{-1/2}$.

3. **Reticulado hexagonal:** Temos que $A_1 \simeq \mathbb{Z}$ e que A_2 é equivalente ao reticulado hexagonal. O reticulado hexagonal é gerado pelos vetores $(1, 0)$ e $\left(\frac{-1}{2}, \frac{\sqrt{3}}{2}\right)$, e assim sua matriz geradora é $B = \begin{bmatrix} 1 & 0 \\ \frac{-1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$. Desta forma $detA_2 = \frac{3}{4}$, norma mínima igual a 1, raio de empacotamento $\rho = \frac{1}{2}$, densidade de empacotamento $\Delta = \frac{\pi}{\sqrt{12}} \approx 0,9069$ e densidade de centro $\delta = \frac{1}{\sqrt{12}}$.

4. **Reticulado D_n, para $n \geq 3$:** Temos que $D_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : x_1 + \cdots + x_n \text{ é par}\}$ é um reticulado. Sua matriz geradora é dada por;

$$B = \begin{bmatrix} -1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ . & . & . & \cdots & . & . \\ 0 & 0 & 0 & \cdots & 1 & -1 \end{bmatrix}$$

onde $det D_n = 4$, norma mínima igual a 2, raio de empacotamento $\rho = 1/\sqrt{2}$ e densidade de centro $\delta = 2^{-(n+2)/2}$.

5. **Reticulado face-centered cubic:** Temos que os reticulados A_3 e D_3 são equivalentes ao reticulado fcc. Assim, o fcc consiste de todos os pontos (x, y, z), onde x, y, z são inteiros com soma par. Um matriz geradora de D_3 é dada por;

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

onde $det D_3 = 4$, norma mínima igual a 2, raio de empacotamento $\rho = 1/\sqrt{2}$, densidade $\Delta = \dfrac{\pi}{\sqrt{18}} \approx 0,7305$ e densidade de centro $\delta = 2^{-5/2}$.

• Para D_4, temos $\Delta \approx 0,61685$ e densidade de centro $\delta \approx 0,125$.

• Para D_5, temos $\Delta \approx 0,46526$ e densidade de centro $\delta \approx 0,08839$.

6. **Reticulado 8-dimensional E_8:** Temos que o sistema de coordenadas pares de E_8 consiste dos pontos $\{(x_1, \cdots, x_8) : \forall\, x_i \in \mathbb{Z}$ ou $\forall\, x_i \in \mathbb{Z} + \frac{1}{2}, \sum x_i \equiv 0(mod 2)\}$. O sistema de coordenadas ímpares é obtido mudando o sinal de qualquer

coordenada: os pontos são $\{(x_1, \cdots, x_8) : \forall\, x_i \in \mathbb{Z}$ ou $\forall\, x_i \in \mathbb{Z} + \frac{1}{2}, \sum x_i \equiv 2x_8(mod2)\}$. A matriz geradora de E_8 é dada por

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

detB=1, norma mínima=2, número de vizinhos τ=240, raio de empacotamento $\rho = \frac{1}{\sqrt{2}}$, densidade $\Delta = \frac{\pi^4}{384} \approx 0.2537$ e densidade de centro $\delta = \frac{1}{16}$.

7. **Reticulado 7-dimensional E_7:** Os vetores em E_8 perpendiculares a qualquer vetor minimal $v \in E_8$ formam o reticulado E_7, isto é, $E_7 = \{x \in E_8 : x \cdot v = 0\}$. A matriz geradora de E_7 é dada por

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

detB=2, norma mínima=2, número de vizinhos τ=126, raio de empacotamento $\rho = \frac{1}{\sqrt{2}}$, densidade $\Delta = \frac{\pi^3}{105} \approx 0.2953$ e

densidade de centro $\delta = \frac{1}{16}$.

8. **Reticulado 6-dimensional E_6:** Os vetores em E_8 perpendiculares a qualquer A_2 subreticulado V em E_8 formam o reticulado E_6, isto é, $E_6 = \{x \in E_8 : x \cdot v = 0, \forall v \in V\}$. A matriz geradora de E_6 é dada por

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

detB=3, norma mínima=2, número de vizinhos τ=72, raio de empacotamento $\rho = \frac{1}{\sqrt{2}}$, densidade $\Delta = \frac{\pi^3}{48\sqrt{3}} \approx 0.3729$ e densidade de centro $\delta = \frac{1}{8\sqrt{3}}$.

9. **Reticulado 12-dimensional K_{12}:** Temos que K_{12} é gerado pelos vetores $\frac{1}{\sqrt{2}}(\pm\theta, \pm 1^5)$, onde $\theta = \omega - \overline{\omega} = \sqrt{-3}$ e $\omega = \frac{-1+\sqrt{-3}}{2}$. A matriz geradora de K_{12} é dada por

$$B = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 1 & \omega & \omega & 1 & 0 & 0 \\ \omega & 1 & \omega & 0 & 1 & 0 \\ \omega & \omega & 1 & 0 & 0 & 1 \end{bmatrix},$$

detB=729, norma mínima=4, número de vizinhos τ=756, raio de empacotamento $\rho = 1$, densidade $\Delta = \frac{\pi^6}{19440} \approx 0.04945$ e densidade de centro $\delta = \frac{1}{27}$.

10. **Reticulado 16-dimensional Λ_{16}:** A matriz geradora de Λ_{16} é dada por B=

$$\frac{1}{\sqrt{2}}\begin{bmatrix}
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0\\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0\\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix},$$

detB=256, norma mínima=4, número de vizinhos τ=4320, raio de empacotamento $\rho = 1$, densidade $\Delta = \frac{\pi^8}{16.8!} \approx 0.01471$ e densidade de centro $\delta = \frac{1}{16}$.

11. **Reticulado 24-dimensional Λ_{24}:** Temos que Λ_{24} é gerado pelos vetores da forma $\frac{1}{\sqrt{8}}(\pm 3, \pm 1^{23})$. A matriz geradora de

Λ_{24} é dada por

$$B = \frac{1}{\sqrt{8}}$$

8000	0000	0000	0000	0000	0000
4400	0000	0000	0000	0000	0000
4040	0000	0000	0000	0000	0000
4004	0000	0000	0000	0000	0000
4000	4000	0000	0000	0000	0000
4000	0400	0000	0000	0000	0000
4000	0040	0000	0000	0000	0000
2222	2222	0000	0000	0000	0000
4000	0000	4000	0000	0000	0000
4000	0000	0400	0000	0000	0000
4000	0000	0040	0000	0000	0000
2222	0000	2222	0000	0000	0000
4000	0000	0000	4000	0000	0000
2200	2200	2200	2200	0000	0000
2020	2020	2020	2020	0000	0000
2002	2002	2002	2002	0000	0000
4000	0000	0000	0000	4000	0000
2020	2002	2200	0000	2200	0000
2002	2200	2020	0000	2020	0000
2200	2020	2002	0000	2002	0000
0222	2000	2000	2000	2000	2000
0000	0000	2200	2200	2200	2200
0000	0000	2020	2020	2020	2020
-3111	1111	1111	1111	1111	1111

,

detB=1, norma mínima=2, número de vizinhos τ=196560, raio de empacotamento $\rho = 1$, densidade $\Delta = \frac{\pi^{12}}{12!} \approx 0.001930$ e densidade de centro $\delta = 1$.

3.5 Reticulados via corpos de números

Nesta seção apresentamos o método de Minkowiski, para a geração de reticulados via ideais do anel de inteiros de um corpos de números.

Sejam $\mathbb{K}$ um corpo de números e n seu grau. Temos que existem n monomorfismos distintos $\sigma_j : \mathbb{K} \to \mathbb{C}$, uma vez que o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. 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**. Se $\alpha : \mathbb{C} \to \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \ldots, n$, temos que $\alpha \circ \sigma_j = \sigma_k$, para algum $1 \leq k \leq n$, e que $\sigma_j = \sigma_k$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Assim, usando r_1 para denotar o número de índices, tal que $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, podemos ordenar os monomorfismos $\sigma_1, \ldots, \sigma_n$ de tal modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam os monomorfismos reais e que $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, \ldots, r_2$. Então $n - r_1$ é um número par, assim podemos escrever $r_1 + 2r_2 = n$. Daí, para cada $x \in \mathbb{K}$, temos que o homomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^n$ definido por

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

é um homomorfismo injetivo de anéis, chamado de **homomorfismo canônico** 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 pode também ser visto como

$$\begin{aligned} \sigma_{\mathbb{K}}(x) \quad = \quad & (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \\ & \Im\sigma_{r_1+r_2}(x)), \end{aligned}$$

onde as notações $\mathfrak{R}(x)$ e $\mathfrak{I}(x)$ representam as partes real e imaginária do número complexo x, respectivamente.

Exemplo 3.5.1. *Sejam o corpo quadrático* $\mathbb{K} = \mathbb{Q}(i)$, *onde* $i = \sqrt{-1}$, *e* $\{\sigma_1, \sigma_2\}$ *o grupo dos* $\mathbb{Q}$*-monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$, *onde* σ_1 *é a aplicação identidade e* $\sigma_2(a + bi) = a - bi$, *com* $a, b \in \mathbb{Q}$. *Neste caso,* $r_1 = 0$ *e* $r_2 = 1$. *Para* $x = a + b_i \in \mathbb{K}$, *com* $a, b \in \mathbb{Q}$, *temos* $\sigma_{\mathbb{K}}(x) = (\mathfrak{R}\sigma_1(x), \mathfrak{I}\sigma_1(x)) = (a, b)$.

Exemplo 3.5.2. *Sejam o corpo ciclotômico* $\mathbb{K} = \mathbb{Q}(\zeta_5)$, *onde* $\zeta_5 = e^{\frac{2\pi i}{5}}$ *e* $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ *o grupo dos* $\mathbb{Q}$*-monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$. *Como* $\mathbb{K}$ *é um corpo totalmente complexo, temos que* $r_1 = 0$ *e* $r_2 = 2$. *Os 4 monomorfismos são dados por* $\sigma_1(\zeta_5) = \zeta_5$, $\sigma_2(\zeta_5) = \zeta_5^2$, $\sigma_3(\zeta_5) = \zeta_5^3$, $\sigma_4(\zeta_5) = \zeta_5^4$. *Se* $x = a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3 + e\zeta_5^4 \in \mathbb{K}$, *com* $a, b, c, d, e \in \mathbb{Q}$, *temos que* $\sigma_{\mathbb{K}}(x) = (\mathfrak{R}\sigma_1(x), \mathfrak{I}\sigma_1(x), \mathfrak{R}\sigma_2(x), \mathfrak{I}\sigma_2(x))$.

Uma das aplicações deste homomorfismo é a geração de reticulados no $\mathbb{R}^n$, onde os principais parâmetros podem ser obtidos via teoria algébrica dos números, através de propriedades herdadas de $\mathbb{K}$. Isto pode ser visto de maneira formal nos resultados que seguem.

Proposição 3.5.1. *(*Samuel, 1967, p.56, Prop.1*) 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*

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

onde r_2 *é o número de monomorfismos imaginários.*

Demonstração. Para cada j fixo, as coordenadas de $\sigma_{\mathbb{K}}(x_j)$ com

respeito a base canônica do $\mathbb{R}^n$ são dadas por

$$\sigma_1(x_j), \ldots, \sigma_{r_1}(x_j), \Re\sigma_{r_1+1}(x_j), \Im\sigma_{r_1+1}(x_j), \ldots, \Re\sigma_{r_1+r_2}(x_j), \Im\sigma_{r_1+r_2}(x_j)). \tag{3.3}$$

Agora calculemos o determinante D da matriz que tem a j-ésima coluna dada pela Equação (3.3) fazendo uso das seguintes fórmulas $\Re(z) = \frac{1}{2}(z+\overline{z})$, $\Im(z) = \frac{1}{2i}(z-\overline{z})$ para z em $\mathbb{C}$ e das transformações elementares no determinante, a saber, pela adição da $(r_1 + 2l)$-ésima linha a sua anterior e em seguida pela subtração da $(r_1 + 2l - 1)$-ésima coluna da sua posterior, para $l = 1, \ldots, r_2$. Assim,

$$D = \begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_j) & \ldots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_j) & \ldots & \sigma_{r_1}(x_n) \\ \Re(\sigma_{r_1+1}(x_1)) & \ldots & \Re(\sigma_{r_1+1}(x_j)) & \ldots & \Re(\sigma_{r_1+1}(x_n)) \\ \Im(\sigma_{r_1+1}(x_1)) & \ldots & \Im(\sigma_{r_1+1}(x_j)) & \ldots & \Im(\sigma_{r_1+1}(x_n)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \Re(\sigma_{r_1+r_2}(x_1)) & \ldots & \Re(\sigma_{r_1+r_2}(x_j)) & \ldots & \Re(\sigma_{r_1+r_2}(x_n)) \\ \Im(\sigma_{r_1+r_2}(x_1)) & \ldots & \Im(\sigma_{r_1+r_2}(x_j)) & \ldots & \Im(\sigma_{r_1+r_2}(x_n)) \end{vmatrix} =$$

$$\left(\frac{1}{2i}\right)^{r_2} \begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)} & \ldots & \sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)} & \ldots & \sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)} & \ldots & \sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)} & \ldots & \sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix} =$$

$$\left(\frac{1}{2}\right)^{r_2}\left(\frac{1}{2i}\right)^{r_2}2^{r_2}\begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1)+\overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_n)+\overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1)-\overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_n)-\overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1)+\overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_n)+\overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1)-\overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_n)-\overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix} =$$

$$(-1)^{r_2}\left(\frac{1}{2}\right)^{\frac{r_2}{2}}\left(\frac{1}{2i}\right)^{r_2}2^{r_2}\begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_n) \\ \overline{\sigma_{r_1+1}(x_1)} & \dots & \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) & \dots & \sigma_{r_1+r_2}(x_n) \\ \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix} =$$

$$\left(\frac{1}{2i}\right)^{r_2}\begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_n) \\ \sigma_{r_1+2}(x_1) & \dots & \sigma_{r_1+2}(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+2r_2}(x_1) & \dots & \sigma_{r_1+2r_2}(x_n) \end{vmatrix} = (2i)^{-r_2}\det(\sigma_j(x_k)).$$

Portanto, $D = (2i)^{-r_2}\det(\sigma_j(x_k))$, $j, k = 1, \dots, n$. Como $(x_j)_{1\leq j\leq n}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue da Proposição 1.6.3, que $\det(\sigma_j(x_k)) \neq 0$, e portanto, $D \neq 0$. Assim, os vetores $\sigma_{\mathbb{K}}(x_j)$ do $\mathbb{R}^n$ são linearmente independentes e geram $\sigma_{\mathbb{K}}(M)$, ou seja, $\sigma_{\mathbb{K}}(M)$ é um reticulado do $\mathbb{R}^n$.

Como $\{x_1, \dots, x_n\}$ é uma $\mathbb{Z}$-base de M, segue que $m = \sum_{j=1}^{n} a_j x_j$, $a_j \in \mathbb{Z}$, e portanto, $m \in M$. Assim,

$$\sigma_{\mathbb{K}}(m) = \sum_{j=1}^{n} a_j \sigma_{\mathbb{K}}(x_j),$$

$a_j \in \mathbb{Z}$, ou seja, $\sigma_{\mathbb{K}}(M) = \left\{ \sum_{j=1}^{n} a_j \sigma_{\mathbb{K}}(x_j);\ a_j \in \mathbb{Z} \right\}$. Logo,

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

■

Exemplo 3.5.3. *Tomemos $\mathbb{K} = \mathbb{Q}(\sqrt{3})$, e $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{3}]$ seu anel dos inteiros com $\mathbb{Z}$-base $\{1, \sqrt{3}\}$. Como $\mathbb{K}$ é totalmente real, segue que $r_2 = 0$, e portanto*

$$\begin{aligned} Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) &= \left| \det \begin{pmatrix} \sigma_1(1) & \sigma_1(\sqrt{3}) \\ \sigma_2(1) & \sigma_2(\sqrt{3}) \end{pmatrix} \right| = \left| \det \begin{pmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{pmatrix} \right| \\ &= 2\sqrt{3}. \end{aligned}$$

Assim, a imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathbb{Z}[\sqrt{3}]) \subseteq \mathbb{R}^2$ é um reticulado de posto 2 do $\mathbb{R}^2$, cujo volume é $2\sqrt{3}$.

Exemplo 3.5.4. *Tomemos $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$, e $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ seu anel dos inteiros com $\mathbb{Z}$-base $\left\{1, \frac{1+\sqrt{-7}}{2}\right\}$. Como $\mathbb{K}$ é*

totalmente imaginário, então $r_2 = 1$*, e portanto*

$$Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \frac{1}{2}\left|\det\begin{pmatrix} 1 & \frac{1+\sqrt{-7}}{2} \\ 1 & \frac{1-\sqrt{-7}}{2} \end{pmatrix}\right| = \frac{1}{2}\sqrt{7}.$$

Assim, $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}) \subseteq \mathbb{R}^2$ *é um reticulado de posto 2 de* $\mathbb{R}^2$ *com volume* $\frac{1}{2}\sqrt{7}$*.*

Exemplo 3.5.5. *Tomemos* $\mathbb{K} = \mathbb{Q}(\zeta_3)$*, onde* $\zeta_3 = e^{\frac{2\pi i}{3}}$ *e* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_3]$ *seu anel dos inteiros com* $\mathbb{Z}$*-base* $\{1, \zeta_3\}$*. Como* $\mathbb{K}$ *é totalmente imaginário, segue que* $r_2 = 1$*, e portanto*

$$\begin{aligned} Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) &= \frac{1}{2}\left|\det\begin{pmatrix} 1 & \zeta_3 \\ 1 & \overline{\zeta_3} \end{pmatrix}\right| = \frac{1}{2}\left|-\frac{1}{2} - \frac{i\sqrt{3}}{2} - \left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)\right| \\ &= \frac{1}{2}\sqrt{3}. \end{aligned}$$

A imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathbb{Z}[\sqrt{3}])$ *é um reticulado de posto* 2 *no* $\mathbb{R}^2$*, cujo volume é* $\frac{\sqrt{3}}{2}$*.*

Proposição 3.5.2. *(*Samuel, 1967, p.57, Prop.2*) Seja* $\mathbb{K}$ *um corpo de números de grau* n*. Sejam* $D_{\mathbb{K}}$ *o discriminante absoluto de* $\mathbb{K}$*,* $\mathbb{A}_{\mathbb{K}}$ *o anel dos inteiros de* $\mathbb{K}$ *e* $\mathfrak{a}$ *um ideal não nulo de* $\mathbb{A}_{\mathbb{K}}$*. Então,* $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ *e* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *são reticulados, com respectivos volumes,*

$$Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}} \quad e \quad Vol(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a}),$$

onde r_2 *é o número de monomorfismos imaginários.*

Demonstração. Como $\mathfrak{a}$ e $\mathbb{A}_{\mathbb{K}}$ são $\mathbb{Z}$-módulos livres de posto n, segue da Proposição 3.5.1, que $\sigma_{\mathbb{K}}(\mathfrak{a})$ e $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ são reticulados do $\mathbb{R}^n$ e que $Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = 2^{-r_2}|\det(\sigma_i(x_k))|$, onde $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de $\mathbb{A}_{\mathbb{K}}$ e pela Proposição 1.6.3 temos que $D_{\mathbb{K}} = \det(\sigma_i(x_k))^2$.

Assim, $|D_{\mathbb{K}}|^{\frac{1}{2}} = |\det(\sigma_i(x_k))|$ e portanto $Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}}$. Para a segunda fórmula, temos que $\sigma_{\mathbb{K}}(\mathfrak{a})$ é um subgrupo de $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ de índice $N(\mathfrak{a})$ uma vez que $\mathbb{A}_{\mathbb{K}}/\mathfrak{a}$ é isomorfo a $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})/\sigma_{\mathbb{K}}(\mathfrak{a})$. Além disso, como um domínio fundamental de $\sigma_{\mathbb{K}}(\mathfrak{a})$ é a união disjunta de $N(\mathfrak{a})$ cópias de um domínio fundamental de $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$, segue que

$$Vol(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{a}).$$

■

Chamamos de realização geométrica de um ideal $\mathfrak{a}$ ao reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$. Em consequência das Proposições 3.5.1 e 3.5.2, temos que a densidade de centro destes reticulados é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathfrak{a})))^n}{|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{a})}, \tag{3.4}$$

onde $\rho(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{1}{2}min\{|\sigma_{\mathbb{K}}(x)|,\ x \in \mathfrak{a},\ x \neq 0\}$.

Proposição 3.5.3. *(*Conway; Sloane, 1999, p.225*) Sejam* $\mathbb{K}$ *um corpo de números e* $x \in \mathbb{K}$. *Então*

$$|\sigma_{\mathbb{K}}(x)|^2 = c_{\mathbb{K}}.Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}),$$

onde

$$c_{\mathbb{K}} = \begin{cases} 1, & \text{se } \mathbb{K} \text{ for totalmente real} \\ \frac{1}{2}, & \text{se } \mathbb{K} \text{ for totalmente imaginário.} \end{cases}$$

Demonstração: Suponhamos que $\mathbb{K}$ seja um corpo de grau n de forma que $r_1 + 2r_2 = n$. Como $\sigma_{\mathbb{K}}(x) \in \mathbb{R}^n$, segue que

$$\begin{aligned} |\sigma_{\mathbb{K}}(x)|^2 &= (\sigma_1(x))^2 + \cdots + (\sigma_{r_1}(x))^2 + \Re(\sigma_{r_1+1}(x))^2 + \Im(\sigma_{r_1+1}(x))^2 + \\ &\quad \cdots + \Re(\sigma_{r_1+r_2}(x))^2 + \Im(\sigma_{r_1+r_2}(x))^2. \end{aligned}$$

Observe que $\Re(\sigma_k(x))^2 + \Im(\sigma_k(x))^2 = \sigma_k(x)\overline{\sigma_k(x)} = \sigma_k(x\overline{x})$, para $r_1 + 1 \leq k \leq r_1 + r_2$. Assim,

$$|\sigma_{\mathbb{K}}(x)|^2 = (\sigma_1(x))^2 + \cdots + (\sigma_{r_1}(x))^2 + \sigma_{r_1+1}(x\overline{x}) + \cdots + \sigma_{r_1+r_2}(x\overline{x}).$$

Se $r_1 = 0$, então

$$|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \cdots + \sigma_{r_2}(x\overline{x}) = \sigma_{r_2+1}(x\overline{x}) + \cdots + \sigma_{r_2+r_2}(x\overline{x}),$$

pois sendo $\overline{\sigma}$ a conjugação complexa, temos que $\sigma_{r_2+j}(x\overline{x}) = (\overline{\sigma} \circ \sigma_j)(x\overline{x}) = \sigma_j(x\overline{x})$, para $j = 1, \cdots, r_2$. Logo,

$$2|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \cdots + \sigma_{r_2}(x\overline{x}) + \sigma_{r_2+1}(x\overline{x}) + \cdots + \sigma_{r_2+r_2}(x\overline{x}) = \sum_{i=1}^{n} \sigma_i(x\overline{x}),$$

e como os $\sigma_i(x\overline{x})$ são os conjugados de $x\overline{x}$, segue que

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}).$$

Se $r_2 = 0$, então

$$|\sigma_{\mathbb{K}}(x)|^2 = (\sigma_1(x))^2 + \cdots + (\sigma_{r_1}(x))^2$$

e como $\sigma_i(x) = (\overline{\sigma} \circ \sigma_i)(x) = \sigma_i(\overline{x})$ segue que $\sigma_i(x\overline{x}) = \sigma_i(x)\sigma_i(\overline{x}) = \sigma_i(x)\sigma_i(x) = (\sigma_i(x))^2$ e assim, $|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \cdots + \sigma_{r_1}(x\overline{x})$. Portanto,

$$|\sigma_{\mathbb{K}}(x)|^2 = \sum_{i=1}^{n} \sigma_i(x\overline{x}) = Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}),$$

e isto conclui a demonstração. ■

Observação 3.5.1. *Se $\mathbb{K}$ é um corpo de números e $\mathfrak{a}$ um ideal não nulo de $\mathbb{A}_{\mathbb{K}}$, podemos reescrever o raio de empacotamento do reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$ da seguinte forma:*

$$\rho(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{1}{2} min\{|\sigma_{\mathbb{K}}(x)|,\ x \in \mathfrak{a},\ x \neq 0\} = \frac{1}{2} min\left\{ \sqrt{c_{\mathbb{K}} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})},\ x \in \mathfrak{a},\ x \neq 0 \right\}.$$

Fazendo $t_{\mathfrak{a}} = min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}),\ x \in \mathfrak{a},\ x \neq 0\}$ temos que:

1. *se $\mathbb{K}$ é totalmente real então*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{\left(\frac{\sqrt{t_{\mathfrak{a}}}}{2}\right)^n}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\left(\sqrt{\frac{t_{\mathfrak{a}}}{4}}\right)^n}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\left(\frac{t_{\mathfrak{a}}}{4}\right)^{\frac{n}{2}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})}.$$

2. *se* $\mathbb{K}$ *é totalmente imaginário então*

$$\begin{aligned}\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) &= \frac{2^{\frac{n}{2}}\left(\frac{\sqrt{\frac{1}{2}t_{\mathfrak{a}}}}{2}\right)^n}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\frac{2^{\frac{n}{2}} t_{\mathfrak{a}}^{\frac{n}{2}}}{2^{\frac{3n}{2}}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\frac{t_{\mathfrak{a}}^{\frac{n}{2}}}{2^n}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} \\ &= \frac{\frac{t_{\mathfrak{a}}^{\frac{n}{2}}}{(\sqrt{4})^n}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\frac{t_{\mathfrak{a}}^{\frac{n}{2}}}{4^{\frac{n}{2}}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\left(\frac{t_{\mathfrak{a}}}{4}\right)^{\frac{n}{2}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})}.\end{aligned}$$

Portanto, a densidade de centro é a mesma para ambos os casos.

Exemplo 3.5.6. *Se* $\mathbb{K} = \mathbb{Q}(i)$ *então* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-1}]$ *e* $D_{\mathbb{K}} = -4$. *Se* $x = a + bi \in \mathbb{A}_{\mathbb{K}}$, *então* $x\overline{x} = (a+bi)(a-bi) = a^2 - abi + abi + b^2 = a^2 + b^2$, $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = 2(a^2+b^2)$ *e* $t_{\mathbb{A}} = 2$, *para* $a = 1$ *e* $b = 0$. *Assim*

$$\delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \frac{\left(\frac{2}{4}\right)}{\sqrt{4}} = \frac{\left(\frac{1}{2}\right)}{2} = \frac{1}{4} = 0,25.$$