UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

FABIO DA COSTA RIBEIRO

FAMÍLIAS DE RETICULADOS DE DENSIDADE RECORDE EM DIMENSÕES DOIS E TRÊS

FORTALEZA
2014

FABIO DA COSTA RIBEIRO

FAMÍLIAS DE RETICULADOS DE DENSIDADES RECORDE EM DIMENSÕES DOIS E TRÊS

Dissertação apresentada ao Programa de Pós-graduação em Matemática do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de concentração: Álgebra.

Orientador: Prof. Dr. José Othon Dantas Lopes

FORTALEZA
2014

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Curso de Matemática

R369f Ribeiro, Fábio da Costa
Famílias de reticulados de densidade recorde em dimensões dois e três / Fábio da Costa Ribeiro. – 2014.
55 f. : enc. ; 31 cm

Dissertação (Mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática, Fortaleza, 2014.
Área de Concentração: Álgebra
Orientação: Prof. Dr. José Othon Dantas Lopes

1. Densidade de reticulado. 2. Empacotamento esférico. 3. Corpos de números. I. Título.

CDD 512

FÁBIO DA COSTA RIBEIRO

FAMÍLIAS DE RETICULADOS DE DENSIDADE RECORDE EM DIMENSÕES DOIS E TRÊS

Dissertação apresentada ao Programa de Pós-graduação em Matemática do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática.
Área de concentração: Álgebra.

Aprovado em: 23/05/2014.

BANCA EXAMINADORA

Prof. Dr. José Othon Dantas Lopes (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Trajano Pires da Nobrega Neto
Universidade Estadual Paulista (UNESP)

Prof. Dr. José Carmelo Interlando
San Diego State University (SDSU)

AGRADECIMENTOS

Ao concluir este trabalho, agradeço:

Àquele que tem sido o meu mestre e Senhor, na vida e na profissão, Jesus Cristo.

As muitas mulheres que Deus colocou em minha vida: minhas irmãs Leda, Graça, Lora e Fátima que sempre me apoiaram nos momentos difíceis pelos quais passei; minha querida e amada pastora Raquel e as irmãs de círculo de oração pelas muitas interseções; minha estimada amiga e professora de inglês Wanda que me ajudou a fazer meu abstract; meu colega de Mestrado Diego, pela digitação; minha companheira de estudos Janielly, pela cooperação e incentivo;

Aos professores do departamento, em especial, ao meu orientador, professor Othon, pela orientação e ajuda.

Aos meus colegas de turma.

"As abelhas... em virtude de uma certa intuição geométrica ... sabem que o hexágono é maior do que o quadrado e o triângulo e conterá mais mel com o mesmo gasto de material" (Papus, de Alexandria).

RESUMO

O objetivo deste trabalho é construir exemplos em $\mathbb{R}^2$ e $\mathbb{R}^3$ de reticulados com máxima densidade de centro. O primeiro capítulo é destinado a introduzir os conceitos de reticulado em $\mathbb{R}^n$, o de empacotamento esférico, bem como apresentar algumas propriedades gerais. O segundo capítulo é destinado a construção dos exemplos mencionados acima a partir das raízes de polinômios quadráticos e cúbicos em $\mathbb{Z}[x]$. No apêndice se encontram uma análise do discriminante de um polinômio cúbico e uma demonstração do volume de uma esfera n-dimensional.

Palavras-chave: Densidade de Reticulado. Empacotamento esférico. Corpos de números. Polinômios.

ABSTRACT

The objective of this work is to build example in $\mathbb{R}^2$ and $\mathbb{R}^3$ with lattices with maximum center density. The first chapter is supposed to introduce the concept of lattices in $\mathbb{R}^n$ and spheric packing, as well as present some general properties. The second chapter is done to the construction through the roorts of quatratic polynomials and cubics in $\mathbb{Z}[x]$. In the apendix we find an annalisis of the discriminant of a cubic polynomial and a demonstration of a n-dimentional sphere.

Keywords: Density of lattices. Sphere packing. Numbers field. Polynomials.

SUMÁRIO

1 INTRODUÇÃO

É costume dizer que problemas de teoria dos números são muito fáceis de enunciar e muito difíceis de se resolver. Um exemplo disso é o famoso último teorema de Fermat. Outro exemplo que deve ter tirado o sono de muitos matemáticos é a conjectura de Kepler. Tal conjectura diz que a melhor disposição de esferas com o mínimo de desperdício de espaço é a piramidal. A origem dessa conjectura data de 1611, quando o astrônomo e matemático alemão Johannes Kepler (1571 - 1630), em um ensaio sobre a constituição da matéria, afirmou que uma tal disposição seria a mais justa possível e nenhum outro arranjo teria mais esferas no mesmo contentor. Kepler, no entanto não conseguiu provar tal afirmação. Foi Carl Friedrich Gauss (1777 - 1855) o primeiro a dar uma prova, embora não completa para o problema.

Após três séculos de tentativas de se provar essa afirmação, no Congresso Internacional de Matemática de 1900 em Paris, David Hilbert, o maior matemático de então, o colocou na sua lista dos 23 grandes problemas que deveriam nortear aas pesquisas matemáticas no século XX. A conjectura de Kepler passou a ser o décimo oitavo problema de Hilbert: Qual a maneira mais densa, no espaço, de arrumarmos um número infinito de sólidos iguais de uma dada forma?

Em Agosto de 1998, Thomas Hales, da Universidade de Michingan, anunciou uma prova da veracidade da afirmação de Kepler. O trabalho de Hales envolve uma intensa análise computacional. O veredicto, no entanto, ainda permanece em aberto. O leitor mais interessado pode consultar [5]. O que faremos neste trabalho é darmos exemplos de reticulados, em dimensão dois e três, com densidades máximas.

2 RETICULADOS EM $\mathbb{R}^n$

2.1 Reticulados em $\mathbb{R}^n$

Dados m vetores linearmente independentes $v_1, v_2, \ldots, v_m \in \mathbb{R}^m$, o reticulado gerado por esse vetores é o conjunto

$$H(v_1, \ldots, v_n) = \left\{ \sum_{i=1}^{n} \alpha_i v_i ; \alpha_1 \in \mathbb{Z} \right\}.$$

Diremos ainda que $v_1, \ldots, v_n$ é uma base do reticulado. Quando $m = n$ diremos que $H(v_1, \ldots, v_n)$ é um reticulado completo.

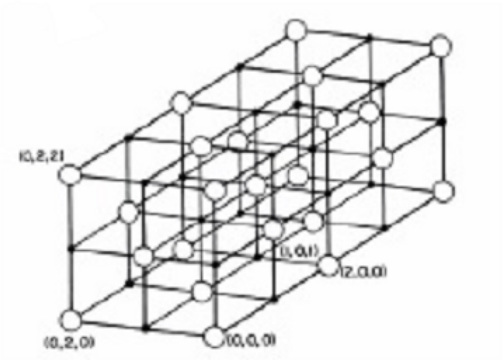
Exemplo 2.1 *Considere $v_1 = 1$. Temos $H(v_1) = \mathbb{Z}$.*

Exemplo 2.2 *Reticulado gerado pela base canônica de $\mathbb{Z}^2$.*

Exemplo 2.3 *Reticulado hexagonal no plano gerado pela base $\left\{(1,0), (\frac{1}{2}, \frac{\sqrt{3}}{2})\right\}$.*

O nome hexagonal desse reticulado é devido ao modo como ele pode ser construído. Iniciamos com o reticulado $\mathbb{Z} \times \{0\} \subset \mathbb{R}^2$. Considere os pontos $A = (-1, 0)$, $B = (0, 0)$, $C = (1, 0)$ e duas retas perpendiculares ao eixo x nos pontos médios de $\overline{AB}$ e $\overline{BC}$. Tomamos as duas retas que passam na origem e de coeficientes angulares $\frac{\pi}{3}$ e $\frac{2\pi}{3}$. Considerando os pontos A, C e os pontos de interseção dessas retas com aquelas outras duas retas perpendiculares, obtemos um hexágono com centro na origem. Procedendo do mesmo modo em cada ponto $(2k, 0)$, obtemos uma sequência de hexágonos ao longo do eixo x. Fazendo o mesmo em cada vértice desses hexágonos obteremos o reticulado mencionado.

Exemplo 2.4 *Reticulado face centrado cúbico. Este reticulado é gerado pela base* $\{(1,0,1),(0,1,1),(1,1,0)\}$.



Exemplo 2.5 *Reticulado* $A_n, n \geq 1$.
Seja $A_n = \{(x_1, x_2, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1}; x_1 + x_2 + \cdots + x_{n+1} = 0\}$. *não é difícil perceber que* A_n *é um subgrupo discreto do* $\mathbb{R}^{n+1}$ *e portanto um reticulado. Uma matriz geradora para* A_n *é*

$$M = \begin{bmatrix} -1 & 0 & \cdots & 0 \\ 1 & -1 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \\ 0 & 0 & \cdots & 1 \end{bmatrix}_{(n+1)\times n}$$

Veja que se $v_1, v_2, \ldots, v_n$ *são os vetores colunas de* M, *então*

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0 \Rightarrow (-\alpha_1, \alpha_1 + \alpha_2, \ldots, \alpha_{n-1} - \alpha_n, \alpha_n) = 0,$$

ou seja, $\alpha_i = 0 \forall i = 1, \ldots, n$. *Observamos ainda que*

$$M^t \cdot M = \begin{bmatrix} 2 & 1 & 0 & \cdots & 0 & 0 \\ -1 & 2 & 1 & \cdots & 0 & 0 \\ 0 & -1 & 2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \cdots & 2 & 1 & \\ 0 & 0 & 0 \cdots & -1 & 2 & \end{bmatrix}_{n\times n}$$

Para o cálculo do $\det M$ *consideramos a matriz*

$$A = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 1 \end{bmatrix} = \begin{bmatrix} v \\ M^t \end{bmatrix},$$

onde $v = (1, 1, \ldots, 1) \in \mathbb{R}^{n+1}$. *Permutando a primeira linha com as linhas inferiores obtemos*

$$\det(A) = (-1)^n \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & -1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 1 \\ -1 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

Sejam $w_1, w_2, \ldots, w_{n+1}$ *as linhas da matriz anterior. Substituindo* w_{n+1} *por*

$$w'_{n+1} = w_1 + w_2 + 2w_3 + 3w_4 + \cdots + nw_{n+1}$$

obtemos

$$\det(A) = (-1)^n \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & -1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & n+1 \end{bmatrix}$$

$$\det(A) = -(n+1)$$

Por outro lado,

$$A^t = \begin{bmatrix} 1 & -1 & 0 & \cdots & 0 \\ 1 & 1 & -1 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & -1 \\ 1 & 0 & 0 & \cdots & 1 \end{bmatrix} = \begin{bmatrix} v \\ M \end{bmatrix}.$$

Logo,

$$\det(A \cdot A^t) = \det\left(\begin{bmatrix} v \\ M^t \end{bmatrix} \begin{bmatrix} v^t & M \end{bmatrix} \right)$$

$$(\det(A))^2 = \det \begin{pmatrix} v \cdot v^t & v \cdot M \\ M^t \cdot v^t & M^t \cdot M \end{pmatrix}$$

$$(n+1)^2 = \det \begin{pmatrix} n+1 & 0 \\ 0 & M^t \cdot M \end{pmatrix}$$

$$\det(M^t M) = n+1.$$

Acima usamos alguns fatos elementares sobre matrizes em blocos.
Salientamos que os reticulados mais densos em $\mathbb{R}^2$ e $\mathbb{R}^3$ são A_2 e A_3, respectivamente (ver [1], pág. 164,Teo 2). Para os casos $n = 2$ e $n = 3$ obtemos reticulados equivalentes ao reticulado hexagonal e o reticulado face centrada cúbico. Este último é encontrado, por exemplo, na estrutura atômica do ferro. Já o reticulado hexagonal é encontrado nos favos de colméias.

Seja agora $A = (a_{ij})_{m\times n}$ uma matriz. Vamos designar por $v_1, \ldots, v_n$ seus vetores colunas. Temos

$$\sum_{i=1}^{n} \alpha_i v_i = (\alpha_j \cdot a_{ij})_{m\times n} = A \cdot x,$$

onde $x = (\alpha_1, ldots, \alpha_n) \in \mathbb{Z}^n$.

Passaremos a escrever o reticulado gerado por $v_1, \ldots, v_n \in \mathbb{R}^n$ como

$$H(A) = \{Ax; x \in \mathbb{Z}^n\},$$

onde A será chamada a matriz geradora do reticulado.

Proposição 2.1 *Seja H o reticulado gerado pela matriz $A = (a_i j)_{m\times n}$. Suponha que $B = (b_{ij})_{m\times p}$ gere o mesmo reticulado, isto é, $H(A) = H(B)$. Então $p = n$.*

Prova: Consideramos os subespaços vetoriais de $\mathbb{R}^m$:

$$\langle A\rangle = \{Ax; x \in \mathbb{R}^n\} \quad \text{e} \quad \langle B\rangle = \{Bx; x \in \mathbb{R}^p\}.$$

Se $n > p$ então como cada $v_j = (a_{1j}, \ldots, a_{mj}) \in H(B) \subset \langle B\rangle$, deve-se ter que o conjunto $\{v_j\}$ é linearmente dependente, o que é uma contradição. Logo só pode ser $n \leq p$. Do mesmo modo, supondo que $p > n$, como cada $u_j = (b_{1j}, \ldots, b_{mj}) \in H(A) \subset \langle A\rangle$, deve-se ter que o conjunto $\{u_j\}$ é linearmente dependente. Portanto $p \leq n$. □

A proposição anterior nos mostra que duas bases quaisquer de um mesmo reticulado tem o mesmo número de elementos. A este número chamaremos posto. Se H é um reticulado em $\mathbb{R}^n$ cuja base contém n elementos escrevemos $posto(H) = n$. Duas bases de um mesmo reticulado são ditas equivalentes. passemos agora ao conceito de paralelepípedo fundamental.

Seja $H(A)$ um reticulado com $A = (a_{ij})_{m\times n}$. O paralelepípedo fundamental é

$$P(A) = \{Ax; 0 \leq |x| < 1\}.$$

Proposição 2.2 *Seja $H(A)$ um reticulado com $A = (a_{ij})_{m\times n}$. Dados n vetores linearmente independentes $b_1, \ldots, b_n \in H(A)$, então esses vetores formam uma base para o reticulado se, e somente se, $P(B) \cap H(A) = \{0\}$, onde B é a matriz cujas colunas são os vetores $b_1, \ldots, b_n$.*

Prova: Suponhamos que $\{b_1, \ldots, b_n\}$ seja uma base de $H(A)$. Então $H(A) \cap P(B) = H(B) \cap P(B)$. Ora, um elemento $y \in H(A) \cap P(B)$ é combinação linear, com coeficientes inteiros dos vetores $b_1, \ldots, b_n$. Por outro lado, y é a combinação linear com coeficientes em $[0, 1)$, dos mesmos vetores. Portanto $y = 0$. Reciprocamente, se $H(A) \cap P(B) = \{0\}$, como $posto(H) = n$ e $b_1, \ldots, b_n$ são linearmente independentes, então dado $x \in H$ temos

$$x = \sum_{i=1}^{n} \alpha_i b_i, \text{ com } \alpha_i \in \mathbb{R}.$$

Agora o vetor $y = \sum_{i=1}^{n} [\alpha_i] b_i \in H$. Portanto o vetor

$$x - y = \sum_{i=1}^{n} (\alpha_i - [\alpha_i]) b_i \in H.$$

Como $\alpha_i - [\alpha_i] \in [0, 1)$, então $x - y \in P(B)$, ou seja, $x - y \in P(B) \cap H$.

Logo $x = y$. □

Observação 2.1 *A afirmação de que $x \in H$ implica que $x = \sum_{i=1}^{n} \alpha_i b_i$, com $\alpha_i \in \mathbb{R}$ segue do fato de que $H \subset \langle b_1, \ldots, b_n \rangle$. Esta inclusão por sua vez decorre do seguinte: para cada $i = 1, \ldots, n$ tem-se $b_i = \sum_{i=1}^{n} \alpha_{ij} a_j$, ou seja*

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Agora, seja $T : \langle A \rangle \to \langle B \rangle$, linear e tal que $Ta_j = b_j$. então a matriz de T em relação a essas bases é $M = (a_{ij})_{n\times n}$. Como T é invertível então $A = M^{-1} \cdot B$.

Assim, se $x \in H$ tem-se $x = \sum_{i=1}^{n} \alpha_i a_i$ e da igualdade $A = M^{-1} \cdot B$ concluímos que $x \in \langle b_1, \ldots, b_n \rangle$.

2.2 O Determinante de um Reticulado

Uma matriz $A \in \mathbb{Z}^{n^2}$ é chamada de unimodular quando $\det(A) = \pm 1$.

Proposição 2.3 *Se A é uma matriz unimodular então A^{-1} também é unimodular.*

Prova: Lembremos que $A^{-1} = \dfrac{1}{\det(A)} \cdot \overline{A}$, onde $\overline{A}$ é a transposta da matriz dos cofatores de A, isto é, $\overline{A} = (A_{ij})t$, onde

$$A_{ij} = (-1)^{i+j} \cdot \det(D_{ij})$$

e D_{ij} é a matriz que se obtém de A retirando-se a i-ésima linha e a j-ésima coluna.

Assim, as entradas de A^{-1} são da forma $\dfrac{(-1)^{i+j} \cdot \det(D_{ij})}{\det(A)}$. Como $\det(D_{ij}) \in \mathbb{Z}$ as entradas de A são todas inteiras. Por outro lado a equação $A \cdot A^{-1} = I$ nos dá $\det(A^{-1}) = \pm 1$. □

Proposição 2.4 *Sejam H e L reticulados em $\mathbb{R}^m$ gerados pelas matrizes A e B em $\mathbb{R}^{m \times n}$ respectivamente. Então A e B são equivalentes, se e somente se, $A = B \cdot C$, para alguma matriz unimodular C.*

Prova: Suponhamos que $H = L$. Então para cada vetor coluna b_i da matriz B tem-se que $b_i \in H$. Isso nos diz que existe uma matriz $C \in \mathbb{Z}^{n^2}$ tal que $B = A \cdot C$. Do mesmo modo existe uma matriz $D \in \mathbb{Z}^{n^2}$ tal que $A = B \cdot D$. Daí $B = A \cdot C = B \cdot D \cdot C$. Multiplicando por B^t, temos $B^t \cdot B = B^t \cdot B \cdot D \cdot C$, o que nos dá $B^t \cdot B = (DC)^t \cdot B^t \cdot B \cdot (D \cdot C)$ e

$$\begin{gathered} \det(B^t \cdot B) = \det(DC)^t \cdot \det(B^t \cdot B) \cdot \det(DC) \Rightarrow \\ \Rightarrow (\det(B))^2 = (\det(DC))^2 \cdot (\det(B))^2 \Rightarrow \det(DC) = \pm 1. \end{gathered}$$

Logo D e C são matrizes unimodulares. Suponhamos agora que $A = B \cdot C$, onde C é uma matriz unimodular. Observe que cada vetor coluna de A é um elemento de L. Para ver isso basta perceber que

$$a_{ij} = \sum_{k=1}^{n} c_{kj} \cdot b_{ik}; \qquad C = (c_{ij})_{n \times n}.$$

Assim, a j-ésima coluna de A será

$$\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix} = c_{1j} \begin{pmatrix} b_{11} \\ b_{12} \\ \vdots \\ b_{m1} \end{pmatrix} + c_{2j} \begin{pmatrix} b_{12} \\ b_{22} \\ \vdots \\ b_{m2} \end{pmatrix} + \cdots + c_{mj} \begin{pmatrix} b_{1n} \\ b_{2n} \\ \vdots \\ b_{mn} \end{pmatrix}.$$

Logo, $H \subset L$. Por outro lado, como C é invertível então $B = A \cdot C^{-1}$. E com o mesmo argumento concluímos que $L \subset H$. □

Como consequência dessa proposição temos que $H(A) = \mathbb{Z}^n$ se, e somente se, A é unimodular. De fato, se A é unimodular, como A e I_n são equivalentes, então $H(A) = \mathbb{Z}^n$. Por outro lado, se ocorre $H(A) = \mathbb{Z}^n$, então A e I_n são equivalentes, o que nos dá que $A = I_n \cdot C$, onde C é uma matriz unimodular.

Seja H o reticulado gerado pela matriz $B \in \mathbb{R}^{m\times n}$. O determinante de H é

$$\det(H(B)) = \sqrt{|\det(B^t \cdot B)|}.$$

Observemos que o determinante de H não depende da base. Seja A uma outra matriz geradora de H, então $A = B \cdot C$, para alguma matriz unimodular C. Assim,

$$\begin{aligned}
\det(H(A)) &= \sqrt{|\det(A^t \cdot A)|} \\
&= \sqrt{|\det((BC)^t \cdot (BC))|} \\
&= \sqrt{|\det(C^t) \cdot \det(B^t \cdot B) \cdot \det(C)|} \\
&= \sqrt{|\det(B^t \cdot B)|} \\
&= \det(H(B))
\end{aligned}$$

Definimos o volume do paralelepípedo (região) fundamental por

$$vol(H) = \det(H).$$

2.3 Empacotamento

Seja H um reticulado de posto n em $\mathbb{R}^m$. Um empacotamento esférico de H é uma coleção de bolas fechadas tais que duas quaisquer dessas bolas se intersectam em no máximo um ponto. O ponto de empacotamento é o maior $\rho > 0$ tal que $B(x,\rho) \cap B(y,\rho) = \emptyset$ quaisquer que sejam $x, y \in H$. A distância mínima entre pontos de H é de

$$d_{\min}(H) = \min\{|x-y|; x, y \in H, x \neq y\}.$$

Proposição 2.5 *O raio de empacotamento de um reticulado H é* $\dfrac{d_{\min}(H)}{2}$.

Prova: Seja $\rho = \dfrac{d_{\min}(H)}{2}$. Suponhamos que exista $u \in B(x,\rho) \cap B(y,\rho)$, para algum x e algum y em H. Então

$$|x-y| \leq |u-x| + |u-y|.$$

Como $|u-x| < \rho$ e $|u-y| < \rho$, temos $|x-y| < d_{\min}(H)$, o que é uma contradição. Assim $B(x,\rho) \cap B(y,\rho) = \emptyset, \forall x, y \in H$. Seja $r > \rho$, mostraremos que existem pontos distintos $x, y \in H$ tais que $B(x,\rho) \cap B(y,\rho) \neq \emptyset$. Tomemos $x, y \in H$ tais que $|x-y| = d_{\min}(H)$. Seja $h = \dfrac{x+y}{2}$. Então

$$|h-x| = \left|\frac{y-x}{2}\right| = \rho < r \qquad \text{e} \qquad |h-y| = \left|\frac{x-y}{2}\right| = \rho < r.$$

Logo $h \in B(x,\rho) \cap B(y,\rho)$. □

Denotaremos por Δ_H e δ_h a densidade de empacotamento e a densidade de centro, respectivamente cujas definições são

$$\Delta_H = \frac{v_n \rho_H^n}{vol(H)} \quad \text{e} \quad \delta_H = \frac{\Delta_H}{v_n} = \frac{\rho_H^n}{vol(H)},$$

onde $vol(H) = \det(H)$ e v_m é o volume da esfera unitária em $\mathbb{R}^m$ e ρ_H é o raio de empacotamento de H. Para uma prova do volume da esfera consulte o apêndice.

Proposição 2.6 *Seja H um reticulado de posto n em $\mathbb{R}^m$. Então*

a) λH é um reticulado de posto n;

b) $\Delta_{\lambda H} = \Delta_H$, $\delta_{\lambda H} = \delta_H$ e $\rho_{\lambda H} = |\lambda| \cdot \rho_H$.

Prova:

a) Basta observar que $\{e_1, \ldots, e_n\}$ é a base de H então $\{\lambda e_1, \ldots, \lambda e_n\}$ é a base de λH.

b) Observemos que:

1. $vol(\lambda H) = \sqrt{|\det[(\lambda H)^t \cdot (\lambda H)]|} = |\lambda|^n \cdot vol(H)$;
2. $d_{\min}(\lambda H) = \min\{|\lambda x - \lambda y|; x, y \in H, x \neq y\} = |\lambda| d_{min}(H)$.
   Daí temos $\rho_{\lambda H} = |\lambda| \rho_H$ e

$$\Delta_{\lambda H} = \frac{v_n (|\lambda|\rho_H)^n}{vol(\lambda H)} = \frac{|\lambda|^n \cdot v_n \rho_H^n}{|\lambda|^n \cdot vol(H)} = |\lambda|^{n-n} \cdot \Delta_H.$$

$$\delta_{\lambda H} = \frac{\Delta_{\lambda H}}{v_n} = \frac{(|\lambda|\rho_H)^n}{vol(\lambda H)} = |\lambda|^{n-n} \cdot \delta_H.$$

□

Observação 2.2 *Consideremos o reticulado hexagonal do exemplo 2.3. Para esse reticulado é fácil observar que seu raio de empacotamento é $\rho = \dfrac{1}{2}$. Temos então que $\Delta = \dfrac{\pi}{2\sqrt{3}}$ e $\delta = \dfrac{1}{2\sqrt{3}}$.*

Observação 2.3 *Para o reticulado face centrada podemos calcular o raio de empacotamento usando um pouco de geometria espacial. Temos* $\rho = \frac{\sqrt{2}}{2}$ *e assim* $\Delta = \frac{\pi\sqrt{2}}{6}$ *e* $\delta = \frac{\sqrt{2}}{8}$.

Observação 2.4 *Para o reticulado* A_n*, como* $|v_i| = \sqrt{2}, i = 1, \ldots, n$ *e pela proposição 2.2 segue que o raio de empacotamento é* $\rho = \frac{\sqrt{2}}{2}$*. Assim teremos para densidade de centro* $\delta_{A_n} = \frac{2^{-n/2}}{\sqrt{n+1}}$ *e para a densidade de empacotamento* $\Delta_{A_n} = \frac{\pi^{n/2} \cdot 2^{-n/2}}{\left(\frac{n}{2}\right)!\sqrt{n+1}}$*, n for par e* $\Delta_{A_n} = \frac{2^{n/2} \cdot \pi^{(n-1)/2} \cdot \left(\frac{n-1}{2}\right)!}{n! \cdot \sqrt{n+1}}$*, se n é ímpar.*

Salientamos que os reticulados hexagonal e face centrado são os de mais alta densidade em $\mathbb{R}^2$ e $\mathbb{R}^3$, respectivamente.

2.4 Os Subgrupos Discretos do $\mathbb{R}^m$

Esta seção é dedicada a provar que os únicos subgrupos discretos de $\mathbb{R}^m$ são os reticulados de posto $n \leq m$, para isso estabeleceremos inicialmente alguns fatos sobre módulos.

Seja R um anel, um R-módulo esquerdo é um grupo abeliano A munido de uma função $f : R \times A \to A$ tal que

a) $f(r, a + b) = f(r, a) + f(r, b)$;

b) $f(r + s, a) = f(r, a) + f(s, a)$;

c) $f(r, f(s, a)) = f(rs, a)$.

Quando R uma unidade 1_R e vale que $f(1_R, a) = a$, para todo $a \in A$, chamamos A de R-módulo unitário. Um subgrupo $B \subset A$ não vazio é dito submódulo de A quando B é subgrupo de A e $f(r, b) \in B$, para todo $b \in B$. Para $X \subset A$, o submódulo gerado por X é a interseção de todos os submódulos que contém X.

Recordemos agora o conceito de módulo livre. Seja A um anel comutativo e I um conjunto de índices. Denotamos por A^I o conjunto de todas as funções de I em A pro $A^{(I)}$ o conjunto de todas as sequências $(a_i)_{i \in I}$, tais que $a_i = 0$, exceto para um número finito de índices $i \in I$. É claro que $A^{(I)} \subset A^I$, ocorrendo a igualdade apenas quando I é finito. Observe ainda que $A^{(I)}$ é submódulo de A^I (quando encaramos A^I com uma estrutura de soma componente a componente e uma multiplicação pro escalar).

Para $j \in I$ a sequência $e_j = (\delta_{ij})_{i \in I}$, tal que $\delta_{jj} = 1$ e $\delta_{ij} = 0$, se $i \neq j$ está em $A^{(I)}$. todo elemento $(a_{ij})_{j \in I}$ de A^I tem uma única expressão como combinação linear

finita dos e_j, ou seja,

$$(a_{ij})_{j\in I} = \sum_{j\in I} a_j e_j.$$

Ao conjunto $\{e_j\}_{j\in I}$ nós chamaremos de base canônica de $A^{(I)}$.

Seja A uma anel, M um A-módulo e a família $(x_i)_{i\in I}$, com $x_i \in M$. Para cada elemento $(a_i)_{i\in I}$ de $A^{(I)}$ associamos o elemento $\sum_i a_i x_i$ de M. Obtemos dessa forma uma aplicação $\varphi : A^{(I)} \to M$ que é linear.

Um subconjunto $X \subset M$ é dito linearmente independente quando para $x_i \in X$ e $a_i \in A$ tem-se a implicação

$$\sum_i a_i x_i = 0 \Rightarrow a_i = 0, \forall i.$$

Observemos ainda que

1. $\varphi(e_i) = x_i$;
2. $(x_i)_{i\in I}$ é linearmente independente se, e somente se, φ é injetiva;
3. $(x_i)_{i\in I}$ gera M se, e somente se, φ é sobrejetiva. Quando φ é uma bijeção dizemos que $(x_i)_{i\in I}$ é uma base de M. um módulo M que tem uma base é chamado de módulo livre.

Se A tem uma identidade então o A-módulo M tem uma base (ver [6], cap. 4, teo 2.1). Mas, em geral, um módulo sobre um anel não necessariamente possui uma base, com por exemplo o anel $\mathbb{Z}/n\mathbb{Z}$, para $n \neq 0, 1$. Um A-módulo M que possui uma base é chamado de módulo livre. A cardinalidade da base é chamada de posto.

Lema 2.1 *Um subgrupo H do $\mathbb{R}^m$ é discreto se, e somente se, $H \cap K$ é finito para todo compacto $K \subset \mathbb{R}^m$.*

Prova: Se H é discreto e $H \cap K$ é infinito para algum compacto $K \subset \mathbb{R}^m$, então existe uma sequência $x_n \in H \cap K$ de elementos distintos. Como K é compacto essa sequência possui ponto de acumulação em K. Logo, dado $\varepsilon > 0$ tem-se $|x_r - x_s| < \varepsilon$, para r e s suficientemente grande. Mas isso é uma contradição já que existem bolas abertas e disjuntas contendo x_r e x_s. Reciprocamente, se $H \cap K$ é finito para todo compacto $K \subset \mathbb{R}^m$, então tomando $p \in H$ e $K = B[p, \delta]$ com $\delta > 0$ temos que $H \cap K = \{p_1, \ldots, p_r\}$ é finito. Tomando $\overline{\delta} < \min\{|p - p_j|; 1 \leq j \leq r\}$ vem que $H \cap B[p, \overline{\delta}] = \{p\}$. Logo H é discreto. □

Lema 2.2 *Se R é um anel com identidade e A é um R-módulo unitário, então o submódulo gerado por $X \subset A$ é*

$$\langle X \rangle = \left\{ \sum_{i=1}^{n} r_i a_i; r_i \in R, a_i \in A \right\}.$$

Uma demonstração detalhada desse lema pode ser encontrada em [6], cap. 4, Teo. 1.5.

Proposição 2.7 *Seja H um subgrupo discreto do $\mathbb{R}^m$. Então H é um reticulado de posto $n \leq m$.*

Prova: Tomemos em H a maior quantidade possível de vetores linearmente independentes, digamos $e_1, \ldots, e_n$. Seja $K = \left\{ \sum_{i=1}^{n} \alpha_i e_i; \alpha_i \in [0,1] \right\}$. Observe que K é compacto, uma vez que K é a imagem de $f : [01] \to \mathbb{R}^m$ dada por $f(\alpha_1, \ldots, \alpha_m) = \sum_{i=1}^{n} \alpha_i e_i$.

Agora, pelo Lema 2.1 temos que $H \cap K$ é finito. Seja $x \in H$. Como $H \subset \langle H \rangle$ então $x = \sum_{i=1}^{n} \lambda_i e_i$, com $\lambda \in \mathbb{R}$. Como $e_i \in H$ e H é subgrupo de $\mathbb{R}^m$ então $y = \sum_{i=1}^{n} [\lambda_i] e_i \in H$. Logo $x - y = \sum_{i=1}^{n} (\lambda_i - [\lambda_i]) e_i \in H$. Mas $\lambda_i - [\lambda_i] \in [0,1]$ e então $x - y \in K$. Portanto $x - y \in H \cap K$.

Agora definamos, para cada $j \in \mathbb{Z}, x_j = j \cdot x - \sum_{i=1}^{n} [j \cdot \lambda_i] e_i$. Temos

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

Para $j = 1$ temos $x_1 = x - \sum_{i=1}^{n} [\lambda_i] e_i$, ou seja, $x = x_1 + \sum_{i=1}^{n} [\lambda_i] e_i$. Pelo Lema 2.2, última igualdade nos diz que o $\mathbb{Z}$-módulo H é gerado por $H \cap K$. Ora, como esse conjunto é finito e $x_j \in H \cap K$, para todo $j \in \mathbb{Z}$, então existem $j, k \in \mathbb{Z}$ distintos tais que $x_j = x_k$. Disso decorre que

$$\begin{aligned} jx - \sum_{i=1}^{n} [j \cdot \lambda_i] e_i &= kx - \sum_{i=1}^{n} [k \cdot \lambda_i] e_i \\ (j-k)x &= \sum_{i=1}^{n} ([j \cdot \lambda_i] - [k \cdot \lambda_i]) e_i \\ (j-k) \cdot \sum_{i=1}^{n} \lambda_i e_i &= \sum_{i=1}^{n} ([j \cdot \lambda_i] - [k \cdot \lambda_i]) e_i. \end{aligned}$$

Comparando os coeficientes obtemos

$$\lambda_i = \frac{[j\lambda_i] - [k\lambda_i]}{j-k} \in \mathbb{Q}.$$

Assim, todo elemento $x \in H$, em particular os elementos de $H \cap K$, é combinação linear com coeficientes racionais dos elementos $e_1, \ldots, e_n$.

Mas H é gerado como $\mathbb{Z}$-módulo pelo conjunto $H \cap K$. Como $H \cap K$ é finito, podemos tomar o mínimo múltiplo comum dos denominadores dos coeficientes de cada elemento em $H \cap K$. Seja d esse mínimo múltiplo comum. Temos então

$$dH \subset \sum_{i=1}^{n} \mathbb{Z}e_i \subset H.$$

Como o $\mathbb{Z}$-módulo dH tem o mesmo posto que H, segue que $H = \sum_{i=1}^{n} \mathbb{Z}e_i$. Isso mostra que H é um reticulado de posto n, gerado por $\{e_1, \ldots, e_n\}$. □

Uma aplicação desse resultado é o seguinte: Seja $t = (\theta_1, \ldots, \theta_n) \in \mathbb{R}^n$ tal que pelo menos uma das coordenadas é irracional. Seja $(e_1, \ldots, e_n)$ a base canônica de $\mathbb{R}^n$ e H o subgrupo de $\mathbb{R}^n$ gerado por $(e_1, \ldots, e_n, t)$. O grupo H não é discreto, pois se fosse o método empregado na proposição anterior deveria nos dá uma expressão para t como combinação linear de coeficientes racionais dos e_i's, o que é um absurdo. Portanto, para todo $\varepsilon > 0$ existem inteiros $p_i \in \mathbb{Z}, q \in \mathbb{N}, q \neq 0$ tal que $|q\theta_i - p_i| \leq \varepsilon$, o que significa que

$$\left|\theta_i - \frac{n_i}{q}\right| \leq \frac{\varepsilon}{q}, \quad \text{para todo } i = 1, \ldots, n.$$

Observemos que, simplesmente escolhendo os múltiplos $\frac{n_i}{q}$ de $\frac{1}{q}$, nós obteríamos uma aproximação

$$\left|\theta_i - \frac{n_i}{q}\right| \leq \frac{1}{2q}, n_i \in \mathbb{Z} \quad \text{para todo } q > 0.$$

2.5 Elementos Inteiros sobre Anéis e Elementos Algébricos sobre Corpos

Esta seção e a próxima são dedicadas a estabelecer alguns resultados da teoria algébrica dos números que serão necessárias para a construção de reticulados via corpos de números.

Seja R um anel e A um subanel de R. Um elemento $x \in R$ é chamado de inteiro sobre A se existe um polinômio mônico com coeficientes em A do qual ele é raiz, isto é, existem $a_0, a_1, \ldots, a_{n-1} \in A$ tais que

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

Se $P \in A[x]$ é tal que $P(x) = 0$, nós dizemos que esta última igualdade é a equação de dependência integral de x sobre A.

Proposição 2.8 *Seja R um anel, A um subanel de R e $x \in R$. As seguintes condições*

são equivalentes:

a) Existem $a_0, a_1, \ldots, a_{n-1} \in A$ *tais que*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

b) O anel $A[x]$ *é um* A*-módulo do tipo finito.*

c) Existe um subanel B *de* R *que contém* A *e* x *e que é um* A*-módulo do tipo finito.*

Prova: Seja M o A-módulo de R gerado por $1, x, \ldots, x^{n-1}$. Por (a), $x^n \in M$. Multiplicando a equação de dependência integra de x sobre A por x^j, nós obtemos

$$x^{n+j} = -a_{n-1}x^{n+j-1} - \cdots - a_0 x^j.$$

Usando indução sobre j temos que $x^{n+j} \in M$, para todo $j \geq 0$. Como $A[x]$ é um A-módulo gerado por x^k nós vemos que $A[x] = M$.

Isso mostra que (a) implica (b). A implicação $(b) \Rightarrow (c)$ é imediata. Provemos que $(c) \Rightarrow (a)$.

Seja $(y_1, \ldots, y_n)$ um conjunto de geradores de B como módulo sobre A, ou seja, $B = Ay_1 + \cdots + Ay_n$. Como $x \in B$ e B é subanel de R, segue que $xy_i \in B$ para todo $i = 1, \ldots, n$. Portanto

$$xy_i = \sum_{j=1}^{n} a_{ij}y_j, \text{ para } i = 1, \ldots, n, a_{ij} \in A, 1 \leq i, j \leq n.$$

Isso significa que

$$\sum_{j=1}^{n} (\delta_{ij}x - a_{ij})y_i = 0, i = 1, \ldots, n.$$

Considere o sistema linear homogêneo nas variáveis $(y_1, \ldots, y_n)$. Escreva d para o determinante $\det(\delta_{ij}x - a_{ij})$. Usando a regra de Cramer, obtemos $dy_i = 0$, para todo i. Isto significa que $d \cdot b = 0$, para todo $b \in B$. Em particular, $d \cdot 1 = 0$, ou seja, $d = 0$. Mas d é polinômio mônico em x. □

Proposição 2.9 *Seja* R *um anel,* A *um subanel de* R *e* $(x_i)_{1 \leq i \leq n}$ *um conjunto de elementos de* R*. Se, para todo* i*,* x_i *inteiro sobre* $A[x_1, \ldots, x_{i-1}]$ *então* $A[x_1, \ldots, x_n]$ *é um* A*-módulo do tipo finito.*

Prova: Usaremos indução sobre n. Para $n = 1$ é a afirmação (b) da proposição anterior. Suponha que $A[x_1, \ldots, x_{n-1}]$ é um A-módulo do tipo finito. Então $B = \sum_{j=1}^{p} Ab_j$. O caso $n = 1$ implica que $B[x_n] = A[x_1, \ldots, x_n]$ é um B-módulo do tipo finito. Escreva

$B[x_n] = \sum_{k=1}^{q} Bc_k$. Então

$$A[x_1, \ldots, x_n] = \sum_{k=1}^{q} Bc_k = \sum_{k=1}^{q} \left(\sum_{j=1}^{p} Ab_j \right) c_k = \sum_{j,k} Ab_j c_k.$$

Assim, $(b_j c_k)_{\substack{1 \leq j \leq p \\ 1 \leq k \leq q}}$ é um conjunto de geradores para $A[x_1, \ldots, x_n]$ com módulo sobre A. □

Corolário 2.1 *Seja R um anel, A um subanel de R, x, y elementos de R inteiros sobre A. Então $x + y, x - y$ e $x \cdot y$ são inteiros sobre A.*

Corolário 2.2 *Seja R um anel e A um subanel de R. Então o conjunto A' dos elementos de R que são inteiros sobre A é um subanel de R que contém A.*

O anel A' dos elementos inteiros sobre A é chamado de fecho integral de A em R. Quando A é um domínio integral e K o seu corpo de frações, o fecho integral de A em K é chamado de fecho integral de A. Quando A é um subanel de um anel B, nós dizemos que B é integral sobre A quando todo elemento de B é inteiro sobre A.

Proposição 2.10 *Seja C um anel, B um subanel de C e A um subanel de B. Se B é integral sobre A e C é integral sobre B, então C é integral sobre A.*

Prova: Seja $x \in C$. Então x é inteiro sobre B e assim existem $b_0, \ldots, b_{n-1} \in B$ tais que

$$x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0.$$

Ponha $B' = A[b_0, \ldots, b_{n-1}]$. Então x é inteiro sobre B'. Como B é inteiro sobre A, os b_i são inteiros sobre A. Portanto a Proposição 2.9 implica que $B'[x] = A[b_0, \ldots, b_{n-1}]$ é um A-módulo de tipo finito. Pela parte (c) da Proposição 2.8, x é inteiro sobre A. Portanto C é inteiro sobre A. □

Proposição 2.11 *Seja B um domínio integral e A um subanel de B tal que B é inteiro sobre A. Afim de que B seja corpo é necessário e suficiente que A seja corpo.*

Prova: Suponha que A é corpo e seja $b \in B, b \neq 0$, Então $A[b]$ é um espaço vetorial de dimensão finita. Por outro lado, $y \in A[b], y \mapsto yb$ é uma transformação linear. Veja que essa transformação é injetiva já que $A[b]$ é um domínio integral e $b \neq 0$. portanto essa transformação também é sobrejetiva. Existe $b' \in A[b]$ tal que $bb' = 1$. Isto significa que, para qualquer $b \neq 0, b \in B$, b é invertível em B. Logo, B é corpo. Reciprocamente, suponha que A seja corpo. Seja $a \in A \backslash \{0\}$. Então a tem inverso $a^{-1} \in B$ que satisfaz

$$a^{-n} + a_{n-1} \cdot a^{-n+1} + \cdots + a_1 \cdot a^{-1} + a_0 = 0, a_i \in A.$$

Multiplicando por a^{n-1} obtemos

$$a^{-1} = -(a_{n-1} + \cdots + a_1 a^{n-2} + a_0 a^{n-1}),$$

o que mostra que $a^{-1} \in A$. □

Um anel A é chamado de integralmente fechado quando ele é seu próprio fecho inteiro.

Exemplo 2.6 *Seja A um domínio integral e K seu corpo de frações. Então o fecho integral A' de A é integralmente fechado. Isso decorre do fato de que o fecho integral de A' é inteiro sobre A', portanto inteiro sobre A.*

Exemplo 2.7 *Todo ideal principal A é integralmente fechado. De fato, seja x um elemento do corpo de frações de A que seja inteiro sobre A. Então, existem $a_0, \ldots, a_{n-1} \in A$ tais que*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

Escreva $x = \dfrac{a}{b}$ com a e b relativamente primos em A. Substituindo $x = \dfrac{a}{b}$ na equação de dependência e multiplicando por b^n obtemos

$$a^n + b(a_{n-1}a^{n-1} + \cdots + a_1 a b^{n-2} + a_0 b^{n-1}) = 0.$$

Assim b divide a^n. Como b é relativamente primo com a, temos que b divide a, o que é uma contradição. Portanto b é uma unidade em A. Assim, $x = \dfrac{a}{b} \in A$.

Seja R um anel e K um subcorpo de R. Um elemento $x \in R$ é chamado algébrico sobre K se existem elementos $a_0, \ldots, a_n \in K$ não todos nulos, tais que

$$a_n x^n + \ldots + a_1 x + a_0 = 0.$$

De forma equivalente os monômios $(x^j)_{j\in\mathbb{N}}$ são linearmente dependentes sobre K. Um elemento de R que não é algébrico sobre K é chamado de transcendente sobre K. Exemplos de números transcendentes são $\pi, e, 2^{\sqrt{2}}$. Fato curioso sobre tais números é que, em se tratando do corpo dos reais, os números algébricos são enumeráveis ao passo que os transcendentes são não-enumeráveis. Quando $a_n \neq 0$, podemos escrever

$$x^n + \left(\frac{a_{n-1}}{a_n}\right) x^{n-1} + \cdots + \left(\frac{a_0}{a_n}\right) = 0.$$

Assim, sobre um corpo, um elemento algébrico é um elemento inteiro.

Dizemos que um anel R contendo um corpo K é algébrico sobre K, se todo elemento de R é algébrico sobre K. Se R é um corpo, então R é chamado uma extensão algébrica de K.

Dado um corpo L e um subcorpo K de L, nós chamamos a dimensão $[L : K]$ o grau de L sobre K.

Proposição 2.12 *Seja K um corpo, L uma extensão algébrica de K e M uma extensão algébrica de L. Então M é uma extensão algébrica de L. Mais ainda, $[M : K] = [M : L][L : K]$.*

Prova: A primeira afirmação é um caso especial dos resultados anteriores. Além do mais, se $(x_i)_{i\in I}$ é uma base de L sobre K e $(y_i)_{i\in J}$ é uma base de M sobre L, então $(x_i, y_j)_{(i,j)\in I\times J}$ é uma base para Msobre K. Portanto $(x_i, y_j)_{(i,j)\in I\times J}$ gera M. A relação $\sum a_{ij}x_iy_j$, com $a_{ij} \in K$ implica $(a_{ij}x_i)y_j = 0$, e assim $\sum a_{ij}x_i = 0$ para todo j, e consequentemente $a_{ij} = 0$ para todo $(i, j) \in I \times J$. Isso prova que

$$[M : K] = [M : L] \cdot [L : K].$$

□

Proposição 2.13 *Seja R um anel e K um subcorpo R. Então*

a) O conjunto K' dos elementos de R algébricos sobre K é um subanel de R que contém K;

b) Se R é um domínio integral, K' é um subcorpo de R.

Prova: (a) é um caso especial do corolário 2.2 e (b) segue da proposição 2.11. □

Seja R um anel, K um subcorpo de R e x um elemento de R. Escreveremos $K[x]$ para o anel dos polinômios sobre uma variável sobre K. Existe um único homomorfismo $\varphi : K[x] \to R$ tal que $\varphi(x) = x$ e tal que $\varphi(a) = a$, para todo $a \in K$. A imagem de φ é $K[x]$. A definição de elemento algébrico pode ser reformulada como segue:

Um elemento x é algébrico sobre $K \Leftrightarrow Ker(\varphi) \neq 0$.

De fato, se x é transcendente sobre K, então obviamente $Ker(\varphi) = 0$. Em qualquer caso o ideal $Ker(\varphi)$ é um ideal principal $(F(x))$. Se x é algébrico sobre K, ele é gerado por um polinômio não nulo $F(x)$.

Observamos que podemos assumir que o polinômio $F(x)$ é mônico, já que K é corpo. Assim $F(x)$ é unicamente determinado por K e x. Nós o chamamos de polinômio minimal de x sobre K. Algumas propriedades desse polinômio são:

a) Seja $G(x) \in K[x]$. $G(x) = 0$ se, e somente se, $F(x)$ divide $G(x)$ em $K[x]$;

b) Suponha que x é algébrico sobre K e $F(x)$ seu polinômio minimal. Usando a propriedade (a) e a proposição 2.11 obtemos o seguinte

$$K[x] \text{ é corpo} \Leftrightarrow K[x] \text{ é domínio integral} \Leftrightarrow F(x) \text{ é irredutível}$$

Por outro lado, se K é um corpo e $F(x) \in K[x]$ é irredutível, então $K[x]/(F(x))$ é um corpo contendo K e, escrevendo x para a projeção de $X \in K[x]$, nós temos $F(x) = 0$. Assim $X - x$ divide $F(x)$ no corpo $K[x]$.

Proposição 2.14 *Seja K um corpo e seja $P(x) \in K[x]$ um polinômio não constante. Existe uma extensão algébrica de grau finito K' de K tal que $P(x)$ se fatora em $K'[x]$ como produto de polinômio de grau um.*

Prova: Usamos indução sobre o grau de $P(x)$. O caso em que grau de P é 1, não há o que fazer.
Seja $F(x)$ um fator irredutível de $P(x)$. Nós temos que provar apenas que existem uma extensão K' de grau finita de K contendo um elemento x tal que $X - x$ divide $F(x)$ em $K'[x]$. Assim $P(x) = (X - x)P_1(x)$ com $P_1(x) \in K'[x]$. Por hipótese de indução, $P_1(x)$ se fatora em um produto de fatores lineares em uma extensão K' de grau finito sobre K''. Pela proposição 2.12, K' é de grau finito sobre K, e $P(x)$ é um produto de polinômios lineares em $K'[x]$. □

Falaremos agora de elementos conjugados e corpos conjugados. Dados dois corpos L e L' ambos contendo um corpo K nós chamaremos a qualquer isomorfismos $\varphi : L \to L'$ tal que $\varphi(a) = a$, para todo $a \in K$ de um k-isomorfismo de L sobre L' . Neste caso diremos que L e L' são K-isomorfos ou conjugados sobre K.

Dadas duas extensões L e L' de K, nós dizemos que dois elementos $x \in L$ e $x' \in L'$ são conjugados sobre K se existe um K-isomorfismo $\varphi : K(x) \to K(x')$ tal que $\varphi(x) = x'$. Uma tal φ é única. A existência de φ significa que x e x' são ambos transcendentes ou algébricos sobre K com o mesmo polinômio minimal.

Exemplo 2.8 *Seja $F(x)$ um polinômio irredutível de grau n sobre K e sejam $x_1, \ldots, x_n$ suas raízes em uma extensão K' de K. Então os x_i's são dois a dois conjugados sobre K e os corpos $K[x_i]$ também são conjugados dois a dois.*

Lema 2.3 *Seja K um corpo de característica zero ou um corpo finito e $F(x) \in K[x]$ um polinômio mônico irredutível com decomposição $F(x) = \prod_{i=1}^{n}(x - x_i)$ em uma extensão K' de K. Então as raízes $x_1, \ldots, x_n$ de $F(x)$ são distintas.*

Prova: Suponha que não. Então $F(x)$ tem uma raiz comum com o seu polinômio derivado $F'(x)$. Portanto, $F(x)$ divide $F'(x)$. Como o grau de F' é menor do que o grau de F , então $F'(x)$ é o polinômio nulo. Entretanto, $F(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0, a_i \in K$ e

$$F'(x) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1.$$

Assim $n \cdot 1 = 0, j \cdot a_j = 0, j = 1, \ldots, n-1$, o que é impossível em um corpo de característica zero. Se a característica é $p \neq 0$ essa relação implica que p divide n e que $a_j = 0$, para todo j não divisível por p.

Assim $F(x)$ é da forma

$$F(x) = x^{qp} + b_{q-1} \cdot x^{(q-1)p} + \cdots + b_1 x^p + b_0, b_i \in K.$$

Se cada $b_i = c_i^p$ com $c_i \in K$, então, pelo lema 2.1

$$F(x) = (x^q + c_{q-1}x^{q-1} + \cdots + c_0)^p$$

e $F(x)$ não é irredutível. Mas se K é um corpo finito com característica $p \neq 0$ a aplicação $x \mapsto x^p$ de K em K é injetiva. Portanto sobrejetiva, já que K é finito. □

Lema 2.4 *Se K é um corpo de característica $p \neq 0$, então $px = 0$ para todo $x \in K$ e $(x+y)^p = x^p + y^p$ para todo $x, y \in K$.*

Prova: Para $x \in K$, nós temos que $p \cdot x = (p \cdot 1) \cdot x = 0 \cdot x = 0$. Por outro lado

$$(x+y)^p = x^p + y^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j \cdot y^{p=j}.$$

Observe que $\binom{p}{j}$ é múltiplo de p, $1 \leq j \leq p-1$. Assim os termos no somatório são nulos em um corpo de característica p.

Observamos ainda que por indução temos $(x+y)^{p^n} = x^{p^n} + y^{p^n}$, para todo $n \geq 0$.
□

Proposição 2.15 *Seja K um corpo de característica zero ou um corpo finito e K' uma extensão finita de grau n de K e C um corpo algebricamente fechado contendo K. Então existem n K-monomorfismos distintos de K' em C.*

Prova: Em primeiro lugar recorde que um corpo C é algebricamente fechado se todo polinômio não constante $P(x) \in C[x]$ pode ser expresso como produto de fatores lineares, todos em $C[x]$. Nossa afirmação é verdadeira para qualquer extensão K' de K da forma $K[x]$, com $x \in K'$. De fato, o polinômio minimal $F(x)$ de x sobre K é de grau n. Suas raízes são todas distintas, de acordo com o lema 2.2. Para cada $i = 1, \ldots, n$ nós temos um K-isomorfismo $\sigma_i : K' \to C$ tal que $\sigma_i(x) = x_i$. Continuamos por indução sobre o grau n de K' .

Seja $x \in K'$ e considere $K \in K[x] \subset K'$ e ponha $q = [K[x] : K]$. Nós podemos assumir que $q > 1$. Nós já vimos que existem q K-isomorfismos distintos $s_1, \ldots, \sigma_q \in K[x]$ em C. Como $K[\sigma_i(x)]$ e $K[x]$ são isomorfos, é possível construir uma extensão K_i' de

$K[\sigma_i(x)]$ e um isomorfismo $\tau_i : K' \to K'_i$ que extende σ_i . Claramente $K[\sigma_i(x)]$é um corpo de característica zero ou um corpo finito. Como

$$[K'_i : K[\sigma_i(x)]] = [K' : K[x]] = \frac{n}{q} < n,$$

a hipótese de indução implica que existem $\frac{n}{q} K[\sigma_i(x)]$-isomorfismos θ_{ij} de K'_i em C. Portanto, as n aplicações $\theta_{ij} \circ \tau_i$ fornece $q \cdot \left(\frac{n}{q}\right) = n$ K -isomorfismos de K' em C.

Esses isomorfismos são distintos pois para $i \neq i', \theta_{ij} \circ \tau_i$ e $\theta_{i'j'} \circ \tau_{i'}$ diferem em $K[x]$, enquanto para $i = i'$ mas $j \neq j'$, θ_{ij} e $\theta_{ij'}$ diferem em K'. □

Corolário 2.3 *Seja K um corpo finito ou um corpo de característica zero. Seja K' uma extensão de K de grau n. Então existe um elemento x e K' (chamado elemento primitivo) tal que $K' = K[x]$.*

Prova: Se K é finito, K' é finito e seu grupo multiplicativo K'^* é composto de potências de um elemento x. Assim $K = K[x]$. Supondo que K é de característica zero e sendo assim um corpo infinito. De acordo com a proposição anterior existem n k-monomorfismos σ_i de K' em um corpo algebricamente fechado C contendo K. Para $i \neq j$ a equação $\sigma_i(y) = \sigma_j(y)(y \in K')$ define um subconjunto V_{ij} de K' que é claramente um K-subespaço do espaço vetorial K' e que é distinto de K' quando $\sigma_i \neq \sigma_j$. Como K é infinito, a união V_{ij} não é todo o K. Tomando x fora dessa união os $\sigma_i(x)$ são distintos, e assim o polinômio minimal $F(x)$ de x sobre K tem pelo menos n raízes distintas em C. Portanto o grau de F é maior ou igual a n, ou seja, $[K[x] : K] = n$. Como $K[x] \subset K'$ e $[K' : K] = n$ nós concluímos que $K' = K[x]$. □

Passamos aos conceitos de normas e traços. Seja A um anel, E um A-módulo livre de posto finito e seja U um endomorfismo de E. Se (e_i) é uma base de E e (a_{ij}) é a matriz de U com relação a essa base, então o traço, o determinante e o polinômio característico de U são, respectivamente

$$Tr(U) = \sum_{i=1}^{n} a_{ii},\ \det(U) = \det(a_{ij}) \text{ e } \det(X \cdot I_E - U) = \det(X\delta_{ij} - a_{ij}).$$

Essas fórmulas implicam que

1. $Tr(U + U') = Tr(U) + Tr(U')$;
2. $\det(U \cdot U') = \det(U) \cdot \det(U')$;
3. $\det(X \cdot I_E - U) = X^n - (Tr(U))X^{n-1} + \cdots + (-1)^n \cdot \det(U)$.

Seja B um anel e A um subanel de B tal que B é um A-módulo livre do tipo finito de posto n. Para $x \in B$, a multiplicação m_x por x é um endomorfismo do A-módulo

B.

Nós chamaremos de traço (respectivamente, norma, polinômio característico) de x, relativa a B e A o traço (respectivamente, determinante, polinômio característico) do endomorfismo m_x.

O traço e a norma de x são denotados, respectivamente, por $Tr_{B/A}(x)$ e $N_{B/A}(x)$ ou simplesmente por $Tr(x)$ e $N(x)$, quando não houver ambiguidades.

Para $x, x' \in B$ e $a \in A$ nós temos

4. $m_x + m_{x'} = m_{x+x'}$;
5. $m_x \circ x_{x'} = m_{xx'}$;
6. $m_{ax} = a \cdot m_x$.

Observemos ainda que a matriz de m_a com relação a base de B é a matriz diagonal em que a diagonal principal é formada apenas pelo elemento a. As fórmulas 1,2 e 3 nos dão

$$Tr(x + x') = Tr(x) + Tr(x')$$

$$Tr(ax) = a \cdot Tr(x), \qquad Tr(a) = n \cdot a$$

$$N(x \cdot x') = N(x) \cdot N(x'), \qquad N(a) = a^n, \qquad N(ax) = a^n \cdot N(x).$$

Proposição 2.16 *Sejam K um corpo de característica zero ou um corpo finito, L uma extensão algébrica de grau n de K, x um elemento de L e $x_1, \ldots, x_n$ raízes do polinômio minimal de x sobre K, cada uma repetida $[L : K[x]]$ vezes. Então*

$$Tr_{L/K}(x) = x_1 + \cdots + x_n, \qquad N_{L/K}(x) = x_1 \cdot \ldots \cdot x_n.$$

O polinômio característico de x, relativamente a L e K é $(x - x_1) \cdot \ldots \cdot (x - x_n)$.

Prova: Vamos primeiro tratar o caso quando x é um elemento primitivo de L sobre K. Seja $F(x)$ o polinômio minimal de x sobre K. Então L é o K-isomorfo a $K[x]/F(x)$ e $(1, x, \ldots, x^n)$ é uma base para L sobre K. Pomos$F(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. A matriz de endomorfismo m_x com relação a essa base é

$$M = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

O determinante de $X \cdot I_L - m_x$ é portanto o determinante da matriz

$$X \cdot I_n - M = \begin{bmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & X & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & a_2 \\ 0 & 0 & \cdots & \vdots & \vdots \\ \vdots & \vdots & \ddots & X & a_{n-2} \\ 0 & 0 & \cdots & -1 & x + a_{n-1} \end{bmatrix}.$$

Expandindo esse determinante como um polinômio em X, obtemos o polinômio característico de x. É claro que ele é igual a $F(x)$, o polinômio minimal de x. Usando as fórmulas para o traço e a norma temos $Tr(x) = -a_{n-1}$ e $N(x) = (-1)^n \cdot a_0$. Como x é primitivo, $F(x) = (X - x_1) \cdot \ldots \cdot (X - x_n)$. comparando os coeficientes, temos

$$Tr(x) = x_1 + \cdots + x_n, \quad N(x) = x_1 \cdot \ldots \cdot x_n.$$

Considere agora o caso geral. Ponha $r = [L : K[x]]$. É suficiente mostrar que o polinômio característico $P(x)$ de x, com relação a L e K, é igual a uma r-ésima potência do polinômio minimal de x sobre K. Seja $(y_i)_{i=1,\ldots,q}$ uma base para $K[x]$ sobre K e seja $(z_j)_{j=1,\ldots,r}$ uma base de L sobre $K[x]$. Então $(y_i z_j)$ é uma base para L sobre K e $n = q \cdot r$. Seja $M = (a_{in})$ a matriz para a multiplicação por x em $K[x]$ com relação a base (y_i). Temos $xy_i = \sum_n a_{in} y_n$. Assim temos que

$$x(y_i z_j) = \left(\sum_n a_{in} y_n \right) z_j = \sum_n a_{in}(y_n z_j).$$

Ordenando lexicograficamente a base $(y_i z_j)$ de L sobre K, nós vemos que a matriz M para a multiplicação por x em L com relação a essa base toma a forma

$$M_1 = \begin{bmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M \end{bmatrix},$$

ou seja, M ocorre r vezes na diagonal em M_1. A matriz $X \cdot I_n - M_1$ consiste de r blocos diagonais da forma $XI_q - M$. Consequentemente,

$$\det(XI_n - M_1) = (\det(x \cdot I_q - M))^r.$$

O lado esquerdo dessa equação é $P(x)$. O $\det(XI_q - M)$ é o polinômio minimal de x sobre K, de acordo com a primeira parte da demonstração. □

Proposição 2.17 *Seja A um domínio integral, K o seu corpo de frações, L uma extensão finita de K e x um elemento de L inteiro sobre A. Suponha que K tenha característica zero. Então os coeficientes do polinômio característico $P(x)$ de x relativamente a L e K, em particular $Tr_{L/K}(x)$ e $N_{L/K}(x)$, são inteiros sobre A.*

Prova: Escrevamos $P(X) = (X - x_1) \cdot \ldots \cdot (X - x_n)$. Os coeficientes de $P(X)$ são, a menos de sinal, soma de produtos dos x_i's. É suficiente mostrar que os x_i's são inteiros sobre A. Mas cada x_i é conjugado a x sobre K e assim existe um K-isomorfismo $\sigma_i : K[x] \to K[x_i]$ tal que $\sigma_i(x) = x_i$. Aplicando σ_i na equação de dependência integral de x sobre A, obtemos uma equação de dependência integral para x_i sobre A. □

Corolário 2.4 *Supondo também que A seja integralmente fechado, os coeficientes do polinômio característico de x, em particular $Tr_{L/K}(x)$ e $N_{L/K}(x)$, são elementos de A.*

Prova: Por definição esses coeficientes são elementos de K. Pela proposição anterior, eles são inteiros sobre A. □

2.6 O Discriminante

Seja B um anel e A um subanel de B tal que B é um A-módulo livre de posto finito n. Para $(x_1, \ldots, x_n) \in B^n$ definimos o discriminante do conjunto $(x_1, \ldots, x_n)$ por

$$D(x_1, \ldots, x_n) = \det(Tr_{B/A}(x_i x_j)).$$

Proposição 2.18 *Se $(y_1, \ldots, y_n) \in B^n$ é um outro conjunto de elementos de B tal que $y_i = \sum_{j=1}^{n} a_{ij} x_j$ com $a_{ij} \in A$, então*

$$D(y_1, \ldots, y_n) = (\det(a_{ij}))^2 \cdot D(x_1, \ldots, x_n).$$

Prova:

$$Tr(y_p \cdot y_q = Tr\left(\sum_{i,j} a_{pi} a_{qj} x_{ij}\right) = \sum_{i,j} a_{pi} a_{qj} Tr(x_i y_j).$$

Isto nos dá uma aplicação matricial

$$(Tr(y_p y_q)) = (a_{pi})(Tr(x_i x_j)) \cdot (a_{qj})^t.$$

Aqui estamos denotando por M^t a transposta da matriz M. Basta agora tomar o determinante de ambos os lados para completar a prova. □

Essa proposição implica que o discriminante de bases para B sobre A são associados em A, ou seja, a matriz (a_{ij}) que expressa uma base em termos da outra tem uma inversa com entradas em A. Portanto, ambos os determinantes $\det(a_{ij})$ e $\det(a_{ij})^{-1}$ são unidades em A. Definimos como o discriminante de B sobre A ao ideal de A gerado por uma base de B sobre A. Denotamos este ideal por $\mathcal{D}_{B/A}$.

Proposição 2.19 *Suponha que $\mathcal{D}_{B/A}$ contém um elemento que não é um divisor de zero. Então, afim de que o conjunto $(x_1, \ldots, x_n) \subset B^n$ seja uma base para B sobre A, é necessário e suficiente que $D(x_1, \ldots, x_n)$ gere $\mathcal{D}_{B/A}$.*

Prova: Basta provar apenas a suficiência, o outro lado já foi provado. Suponha que $d = D(x_1, \ldots, x_n)$ gere $\mathcal{D}_{B/A}$. Seja $(e_1, \ldots, e_n)$ uma base de B sobre A. Ponha $d' = D(e_1, \ldots, e_n)$ e $x_i = \sum_{j=1}^{n} a_{ij}e_j$, com $a_{ij} \in A, 1 \leq i \leq n$. Então $d = \det(a_{ij})^2 \cdot d'$. Por hipótese $Ad = \mathcal{D}_{B/A} = Ad$. Portanto, existe $b \in A$ tal que $d' = b \cdot d$. Disso segue que $d(1 - b\det(a_{ij})^2) = 0$. Como d não é divisor de zero, pois caso contrário, todo elemento de $Ad = \mathcal{D}_{B/A}$ seria divisor de zero. Logo, $1 - b \cdot \det(a_{ij})^2 = 0$. Isto significa que $\det(a_{ij})$ é invertível. E a matriz (a_{ij}) também é invertível. Consequentemente $(x_1, \ldots, x_n)$ é uma base de B sobre A. □

Proposição 2.20 *Seja K um corpo finito ou de característica zero, L uma extensão de grau n de K e $\sigma_1, \ldots, \sigma_n$ os n distintos K-isomorfismos de L em um corpo algebricamente fechado contendo K. Então se $(x_1, \ldots, x_n)$ é uma base de L sobre K,*

$$D(x_1, \ldots, x_n) = \det(\sigma_i(x_j))^2 \neq 0.$$

Prova: A primeira igualdade segue do seguinte

$$\begin{aligned} D(x_1, \ldots, x_n) &= \det(Tr(x_i x_j)) = \det\left(\sum_k \sigma_k(x_i x_j)\right) \\ &= \det\left(\sum_k \sigma_k(x_i)\sigma_k(x_j)\right) \\ &= \det(\sigma_k(x_i)) \cdot \det(\sigma_k(x_i)) = \det(\sigma_i(x_j))^2. \end{aligned}$$

Agora, se $\det(\sigma_i(x_j)) = 0$, existem $u_1, \ldots, u_n$ não todos nulos tais que $\sum_{i=1}^{n} u_i\sigma_i(x_j)) = 0$, para todo j. Por linearidade concluimos que $\sum_{i=1}^{n} u_i\sigma_i(x)) = 0$, para todo $x \in L$. O que é uma contradição, em decorrência do lema anterior. □

Observação 2.5 *Nas condições da proposição anterior, a relação $D(x_1, \ldots, x_n) \neq 0$ significa que a forma bilinear $(x, y) \mapsto Tr(x, y)$ é não degenerada, isto é, $Tr(xy) = 0$ para*

todo $y \in L$ implica que $x = 0$. Assim, a aplicação K-linear que a cada $x \in L$, associa a $s_x : y \mapsto Tr_{L/K}(xy)$, é uma injeção de L em $Hom_K(L, K)$. Como L e $Hom_K(L, K)$ tem a mesma dimensão n sobre K, segue que $x \mapsto s_x$ é uma bijeção. A existência de uma base dual de um espaço vetorial e seu dual implica que, para qualquer base $(x_1, \ldots, x_n)$ de L sobre K, existe uma base $(y_1, \ldots, y_n)$ tal que

$$Tr_{L/K}(xy) = \delta_{ij}, 1 \leq i, j \leq n.$$

Lema 2.5 *Seja G um grupo, C um corpo e $\sigma_1, \ldots, \sigma_n$ homomorfismos distintos de G no grupo multiplicativo C^*. Então os σ_i's são linearmente independentes sobre C, ou seja, $\sum u_i\sigma_i(q) = 0$, para todo $g \in G$ implica que todos os u_i's são nulos.*

Prova: Se os σ_i's são linearmente dependentes, consideramos uma relação não trivial $\sum u_i\sigma_i = 0$ $(u_i \in C)$ tal que o número q de u_i's que são nulos é mínimo. Reenumerando podemos supor que

$$u_1\sigma_1(g) + \cdots + u_q\sigma_q(g) = 0, \quad \text{para todo } g \in G. \tag{1}$$

Para g e h arbitrários temos

$$u_1\sigma_1(hg) + \cdots + u_q\sigma_q(hg) = u_1\sigma_1(h)\sigma_1(g) + \cdots + u_q\sigma_q(h)\sigma_q(g) = 0. \tag{2}$$

Multiplicando a equação (1) por $\sigma_1(h)$ e subtraindo da equação (2) obtemos

$$u_2(\sigma_1(h) - \sigma_2(h))\sigma_2(g) + \cdots + u_q(\sigma_1(h) - \sigma_q(h))\sigma_q(g) = 0.$$

Como essa igualdade vale para todo $g \in G$ e pela escolha mínima de q, segue que $u_q(\sigma_1(h) - \sigma_2(h)) = 0$. Assim $\sigma_1(h) = \sigma_2(h)$, para todo $h \in G$, já que $u_2 \neq 0$. Mas isso contradiz a hipótese de que os σ_i's são distintos. □

Proposição 2.21 *Seja A um anel integralmente fechado, K seu corpo de frações, L uma extensão de grau n de K e A' o fecho integral de A e de L. Suponha que K é de característica zero. Então A' é um A-submódulo de um A-módulo livre de posto n.*

Prova: Seja $(x_1, \ldots, x_n)$ uma base de L sobre K. Cada x_i é algébrico sobre K, assim, para cada i, nós temos uma equação da forma

$$a_n x_i^n + a_{n-1}x_i^{n-1} + \cdots + a_0, a_j \in A.$$

Podemos assumir que $a_n \neq 0$. Multiplicando por a_n^{n-1}, vemos que $a_n x_i$ é inteiro sobre A. Ponha $x_i' = a_n x_i$. Então $(x_1', \ldots, x_n')$ é uma base de L sobre K contido em A'. Pela nossa observação, existe uma outra base $(y_1, \ldots, y_n)$ de L sobre K tal que $Tr(x_i'y_j) = \delta_{ij}$.

Seja $z \in A'$. Como $(y_1, \ldots, y_n)$ é base de L sobre K podemos escrever $z = \sum_{j=1}^{n} b_j y_j$ com $b_j \in K$. Para cada i temos que $x_i' z \in A'$. Portanto $Tr(x_i' y_j) \in A$. Assim,

$$Tr(x_i' y_j) = Tr\left(\sum_j b_j x_i y_j\right) = \sum_j Tr(x_i' y_j) = \sum_j b_j \delta_{ij} = b_i.$$

Concluímos então que $b_i \in A$, para todo i, o que implica que A' é um submódulo do A-módulo livre $\sum_{j=1}^{n} A y_j$. □

Corolário 2.5 *Adicionando as hipóteses da proposição anterior o fato de A ser principal, então A' é um A-módulo livre de posto n.*

Prova: Um submódulo de um A-módulo livre é, nessa hipótese adicional, livre de posto menor ou igual a n. Por outro lado, temos que A' contém uma base de L sobre K, portanto é de posto n. □

Encerramos essa seção com o cálculo de um discriminante.

Seja K um corpo finito ou de característica zero, $L = K[x]$ uma extensão de grau n de K e $F(X)$ o polinômio minimal de x sobre K. Então

$$D(1, x, \ldots, x^n) = (-1)^{\frac{1}{2}n(n-1)} N_{L/K}(F'(x)).$$

Denotemos por $x_1, \ldots, x_n$ as raízes de $F(X)$ em uma extensão de K. Elas são conjugadas de x. Temos então

$$\begin{aligned}
D(1, x, \ldots, x^n) &= \det(\sigma_i(x^j))^2 \\
&= \det(x_i^j)^2 \\
&= \left[\prod_{i<j}(x_i - x_j)\right]^2 \quad \text{Vandermond} \\
&= c \cdot \prod_{i \neq j}(x_i - x_j) \quad (\text{onde } c = (-1)^{\frac{1}{2}n(n-1)}) \\
&= c \cdot \prod_i \left(\prod_{i \neq j}(x_i - x_j)\right) \\
&= c \cdot \prod_i F'(x_i) = c \cdot N_{L/K}(F'(x))
\end{aligned}$$

2.7 Reticulados Via Corpos de Números

Nesta seção apresentaremos um exemplo de reticulados no $\mathbb{R}^n$ o qual é a imagem, por um homomorfismo, de um ideal de um corpo de números.

Seja K um corpo de números de grau n. Vimos nos parágrafos anteriores que existem n monomorfismos distintos $\sigma_i : K \to \mathbb{C}$. Quando $\sigma_i(K) \subset \mathbb{R}$ diremos que σ_i é real. Caso contrário, σ_i é dito imaginário. Quando todos os monomorfismos são reais diz-se que K é um corpo totalmente real e quando os monomorfismos são todos imaginários diz-se que K é um corpo totalmente complexo. Se $\alpha : \mathbb{C} \to \mathbb{C}$ é a conjugação complexa, isto é, $\alpha(z) = \overline{z}$, então para cada $i = 1, \ldots, n$ tem-se $\alpha \circ \sigma_i = \sigma_j$, para algum $j = 1, \ldots, n$ e que $\sigma_i = \sigma_j$ se, e somente se, $\sigma_i(K) \subset \mathbb{R}$. Denotaremos por r_1 o número de índices i tais que $\sigma_i(K) \subset \mathbb{R}$. Vamos reordenar os monomorfismos de modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam os monomorfismos reais e $\sigma_{r_1+1}, \ldots, \sigma_n$ sejam os pares de monomorfismos imaginários.

Para cada $x \in K$ seja

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

onde $r_1 + 2r_2 = n$. Observamos que σ é um monomorfismo chamado de homomorfismo canônico. A injetividade de σ nos permite identificar $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ com $\mathbb{R}^n$.

Proposição 2.22 *Seja K um corpo de números de grau n. Se $M \subset K$ é um Z-módulo livre de posto finito n e $(x_i)_{1 \leq i \leq n}$ uma base de M e σ é o homomorfismo canônico, então $\sigma(M)$ é um reticulado no $\mathbb{R}^n$ cujo volume é*

$$vol(\sigma(M)) = 2^{-r_2} |\det(\sigma_i(x_j))|, \text{ com } 1 \leq i, j \leq n.$$

Prova: Observamos inicialmente que $(x_i)_{1 \leq i \leq n}$ é uma base de K sobre $\mathbb{Q}$. Logo, $\det(\sigma_i(x_j)) \neq 0$, com $1 \leq i, j \leq n$. A i-ésima linha da matriz de σ pode ser escrita como

$$\sigma_1(x_i), \ldots, \sigma_{r_1}(x_i), R(\sigma_{r_1+1}(x_i)), I(\sigma_{r_1+1}(x_i)), \ldots, R(\sigma_{r_1+r_2}(x_i)), I(\sigma_{r_1+r_2}(x_i)),$$

em que R e I indicam a parte real e parte imaginária. Portanto o determinante D da matriz de σ será

$$
D = \begin{vmatrix}
\sigma_1(x_1) & \cdots & \sigma_1(x_j) & \cdots & \sigma_1(x_n) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\sigma_{r_1}(x_1) & \cdots & \sigma_{r_1}(x_j) & \cdots & \sigma_{r_1}(x_n) \\
R(\sigma_{r_1+1}(x_1)) & \cdots & R(\sigma_{r_1+1}(x_j)) & \cdots & R(\sigma_{r_1+1}(x_n)) \\
I(\sigma_{r_1+1}(x_1)) & \cdots & I(\sigma_{r_1+1}(x_j)) & \cdots & I(\sigma_{r_1+1}(x_n)) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
R(\sigma_{r_1+r_2}(x_1)) & \cdots & R(\sigma_{r_1+r_2}(x_j)) & \cdots & R(\sigma_{r_1+r_2}(x_n)) \\
I(\sigma_{r_1+r_2}(x_1)) & \cdots & I(\sigma_{r_1+r_2}(x_j)) & \cdots & I(\sigma_{r_1+r_2}(x_n))
\end{vmatrix}
$$

$$
= \begin{vmatrix}
\sigma_1(x_1) & \cdots & \sigma_1(x_j) & \cdots & \sigma_1(x_n) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\sigma_{r_1}(x_1) & \cdots & \sigma_{r_1}(x_j) & \cdots & \sigma_{r_1}(x_n) \\
\dfrac{\sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)}}{2} & \cdots & \dfrac{\sigma_{r_1+1}(x_j) + \overline{\sigma_{r_1+1}(x_j)}}{2} & \cdots & \dfrac{\sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)}}{2} \\
\dfrac{\sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)}}{2i} & \cdots & \dfrac{\sigma_{r_1+1}(x_j) - \overline{\sigma_{r_1+1}(x_j)}}{2i} & \cdots & \dfrac{\sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)}}{2i} \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\dfrac{\sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)}}{2} & \cdots & \dfrac{\sigma_{r_1+r_2}(x_j) + \overline{\sigma_{r_1+r_2}(x_j)}}{2} & \cdots & \dfrac{\sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)}}{2} \\
\dfrac{\sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)}}{2i} & \cdots & \dfrac{\sigma_{r_1+r_2}(x_j) - \overline{\sigma_{r_1+r_2}(x_j)}}{2i} & \cdots & \dfrac{\sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)}}{2i}
\end{vmatrix}
$$

Na última igualdade usamos o fato de que $R(z) = \dfrac{z+\overline{z}}{2}$ e $Im(z) = \dfrac{z-\overline{z}}{2i}$. Podemos

observar ainda que $D = \left(\frac{1}{2}\right)^{r_2} \cdot \left(\frac{1}{2i}\right)^{r_2} \cdot L$, onde

$$L = \begin{vmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_j) & \cdots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \cdots & \sigma_{r_1}(x_j) & \cdots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)} & \cdots & \sigma_{r_1+1}(x_j) + \overline{\sigma_{r_1+1}(x_j)} & \cdots & \sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)} & \cdots & \sigma_{r_1+1}(x_j) - \overline{\sigma_{r_1+1}(x_j)} & \cdots & \sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)} & \cdots & \sigma_{r_1+r_2}(x_j) + \overline{\sigma_{r_1+r_2}(x_j)} & \cdots & \sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)} & \cdots & \sigma_{r_1+r_2}(x_j) - \overline{\sigma_{r_1+r_2}(x_j)} & \cdots & \sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}$$

Se substituirmos a linha $r_1 + 1$ pela soma desta com a linha $r_1 + 2$ e substituirmos a linha $r_1 + 2$ pela diferença da linha $r_1 + 1$ com a linha $r_1 + 2$, e fizermos isso para os demais pares de linhas abaixo da linha $r_1 + 2$, então

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

Usando agora que $\sigma_{j+r_2} = \overline{\sigma_j(x_i)}$, para $r_1 + 1 \leq j \leq r_1 + r_2$, temos

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

Depois de algumas permutações entre as linhas $r_1 + 2, \ldots, r_1 + 2r_2 - 1$, obtemos

$$|D| = 2^{-r_2} \cdot |\det(\sigma_i(x_j))|, \text{ com } 1 \leq i, j \leq n.$$

Assim os vetores coluna da matriz de σ são linearmente independentes e geram $\sigma(M)$, ou seja, $\sigma(M)$ é um reticulado em $\mathbb{R}^n$. □

Exemplo 2.9 *Seja* $K = \mathbb{Q}[\sqrt{-7}] = \{a + b\sqrt{-7}a, b \in \mathbb{Z}\}$. *Veja que*

$$\left\{1, \frac{1+\sqrt{-7}}{2}\right\}$$

é base para $M = \mathbb{Z}[\sqrt{-7}]$. *Sejam* $\sigma_1(a+b\sqrt{-7}) = a+b\sqrt{-7}$ *e* $\sigma_2(a+b\sqrt{-7}) = a-b\sqrt{-7}$ *os* $\mathbb{Q}$*-monomorfismos de* K *em* $\mathbb{C}$. *Como* K *é totalmente complexo* $r_1 = 0$ *e* $r_2 = 1$. *Assim, para* $x = a + b\sqrt{-7} \in K$, *temos que*

$$\sigma(x) = (R(\sigma_1(x)), I(\sigma_1(x))) = (a, b).$$

Assim a matriz de σ *será*

$$\begin{bmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{-7}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{-7}}{2}\right) \end{bmatrix} = \begin{bmatrix} 1 & \frac{1+\sqrt{-7}}{2} \\ 1 & \frac{1-\sqrt{-7}}{2} \end{bmatrix}.$$

E o volume do reticulado $\sigma(M)$ *será*

$$vol(\sigma(M)) = \frac{1}{2} \cdot \left| \frac{1-\sqrt{-7}}{2} - \frac{1+\sqrt{-7}}{2} \right| = \frac{\sqrt{-7}}{2}.$$

3 POLINÔMIOS QUADRÁTICOS E CÚBICOS

3.1 Polinômio Quadrático com Raízes Reais

Sejam $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, com $a \neq 0$ e $\Delta > 0$. Denotaremos por α_1 e α_2 os zeros de f. Observemos que $v_1 = (\alpha_1, \alpha_2)$ e $v_2 = (\alpha_2, \alpha_1)$ formam uma base para $\mathbb{R}^2$, pois

$$\begin{aligned} \det(v_1, v_2) &= \begin{vmatrix} \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_1 \end{vmatrix} \\ &= \alpha_1^2 - \alpha_2^2 \\ &= (\alpha_1 - \alpha_2)(\alpha_1 + \alpha_2). \end{aligned}$$

Mas,

$$\alpha_1 - \alpha_2 = \frac{-a + \sqrt{\Delta}}{2} - \frac{-a - \sqrt{\Delta}}{2} = \sqrt{\Delta} \quad \text{e} \quad \alpha_1 + \alpha_2 = -a.$$

E daí, $\det(v_1, v_2) = -a\sqrt{\Delta} \neq 0$.

Lema 3.1 *Com a mesma notação usada acima, seja $v = xv_1 + yv_2$ um ponto do reticulado H gerado por v_1 e v_2. Então $|v| = (a^2 - 2b)(x^2 + y^2) + 4bxy$.*

Prova: Temos que

$$\begin{aligned} |v|^2 &= \langle v, v \rangle \\ &= x^2\langle v_1, v_1 \rangle + 2xy\langle v_1, v_2 \rangle + y^2\langle v_2, v_2 \rangle \\ &= x^2(\alpha_1^2 + \alpha_2^2) + 2xy(\alpha_1\alpha_2 + \alpha_2\alpha_1) + y^2(\alpha_1^2 + \alpha_2^2) \\ &= (x^2 + y^2)(\alpha_1^2 + \alpha_2^2) + 4xy\alpha_1\alpha_2 \\ &= (x^2 + y^2)\left[(\alpha_1 + \alpha_2)^2 - 2\alpha_1\alpha_2\right] + 4xy\alpha_1\alpha_2 \\ &= (x^2 + y^2)(a^2 - 2b) + 4bxy \end{aligned}$$

□

Teorema 3.1 *Suponha que $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, onde $a \neq 0$ e $a^2 = 6b$, tenha raízes distintas α_1 e α_2. Se H é o reticulado gerado por $v_1 = (\alpha_1, \alpha_2)$ e $v_2 = (\alpha_2, \alpha_1)$, então*

a) O raio de empacotamento de H é $\rho = \sqrt{b}$;

b) O volume da região fundamental é $2b\sqrt{3}$;

c) A densidade de centro é $\delta_H = \dfrac{1}{2\sqrt{3}}$ e este é o maior valor para o centro de densidade em dimensão 2.

Prova: Seja $v \in H$. Pelo lema anterior

$$\begin{aligned} |v|^2 &= (x^2+y^2)(a^2-2b)+4bxy \\ &= (x^2+y^2)(6b-2b)+4bxy \\ &= 4b(x^2+y^2+xy) \geq 4bxy \end{aligned}$$

Podemos restringir $x, y \in \mathbb{N}$ e assim $|v|^2 \geq 4b$.
Disso decorre que $\rho = \sqrt{b}$. Agora para o volume da região fundamental temos

$$|\det(H)| = |\det(v_1, v_2)| = |a|\sqrt{a^2-4b} = \sqrt{6b} \cdot \sqrt{2b} = 2b\sqrt{3}.$$

Logo, a densidade de centro de H será

$$\delta_H = \frac{\rho^2}{vol(H)} = \frac{b}{2b\sqrt{3}} = \frac{1}{2\sqrt{3}}.$$

□

3.2 Polinômios Quadráticos com Raízes Complexas

Gostaríamos de salientar ainda a importância do estudo deste tópico matemático. A teoria da informação cujo marco inicial é o artigo A Mathematical Theory of Comunications de C. E. Shennon tem influenciado o desenvolvimento de teorias matemáticas relacionadas a tecnologias de comunicação e informação. Desde a publicação desse artigo muitas áreas da matemática, como Álgebra Linear, Corpos Finitos e Geometria Discreta têm sido utilizados para solucionar problemas relacionados a Teoria da Informação. A Teoria dos códigos corretores de erros figuram entre as aplicações do estudo de reticulados.

Seja $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, com $a \neq 0$, $\Delta < 0$ e tendo como raízes complexas α_1 e α_2. Sejam $v_1 = (Re(\alpha_1), Im(\alpha_1))$ e $v_2 = (Re(\alpha_2), Im(\alpha_2))$. Ora,

$$\alpha_i = \frac{-a \pm \sqrt{a^2-4b}}{2} = -\frac{a}{2} \pm i\frac{4b-a^2}{2}.$$

Então a matriz geradora do reticulado $H(v_1, v_2)$ será

$$\begin{bmatrix} -\frac{a}{2} & -\frac{a}{2} \\ \frac{\sqrt{4b-a^2}}{2} & -\frac{\sqrt{4b-a^2}}{2} \end{bmatrix}.$$

E assim, $\det(H) = \frac{a}{2}\sqrt{4b-a^2}$. E se $v = xv_1 + yv_2$ então

$$\begin{aligned}
|v|^2 &= \langle v, v\rangle \\
&= x^2|v_1|^2 + y^2|v_2|^2 + 2xy\langle v_1, v_2\rangle \\
&= x^2\left(\frac{a^2}{4} + \frac{4b-a^2}{4}\right) + y^2\left(\frac{a^2}{4} + \frac{4b-a^2}{4}\right) + 2xy\left(\frac{a^2}{4} - \frac{4b-a^2}{4}\right) \\
&= \frac{a^2}{4}(x^2+y^2+2xy) + \frac{4b-a^2}{4}(x^2+y^2-2xy) \\
&= \frac{a^2}{4}(x+y)^2 + \frac{4b-a^2}{4}(x-y)^2 \\
&= \frac{a^2}{4}(x+y)^2 + b(x-y)^2 - \frac{a^2}{4}(x-y)^2 \\
&= \frac{a^2}{4}((x+y)^2 - (x-y)^2) + b(x-y)^2 \\
&= a^2xy + b(x-y)^2.
\end{aligned}$$

Teorema 3.2 *Seja $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, com $a \neq 0$ e $a^2 = 3b$. Sejam α_1 e α_2 suas raízes complexas distintas de f e H o reticulado gerado por v_1 e v_2, onde $v_1 = (Re(\alpha_1), Im(\alpha_1))$ e $v_2 = (Re(\alpha_2), Im(\alpha_2))$. Então a densidade de centro é $\delta_H = \frac{1}{2\sqrt{3}}$.*

Prova: Iniciamos observando que se $v = xv_1 + yv_2 \in H$, então

$$\begin{aligned}
|v|^2 &= a^2xy + b(x-y)^2 \\
&= 3bxy + b(x^2+y^2-2xy) \\
&= b(x^2+y^2+xy).
\end{aligned}$$

Usando um mesmo argumento já utilizado antes, temos que $|v|^2 \geq b$.
O raio de empacotamento será $\rho = \frac{\sqrt{b}}{2}$. O volume da região fundamental é

$$vol(H) = \frac{|a|}{2}\sqrt{4b-a^2} = \frac{\sqrt{3b}}{2}\sqrt{b} = \frac{b\sqrt{3}}{2}.$$

Logo,

$$\begin{aligned}
\delta_H &= \frac{\left(\frac{\sqrt{b}}{2}\right)^2}{\frac{b\sqrt{3}}{2}} \\
&= \frac{1}{2\sqrt{3}}.
\end{aligned}$$

□

3.3 Polinômios Cúbicos com Raízes Reais

Lema 3.2 *Seja* $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ *com raízes reais* α_1, α_2 *e* α_3*.*
Se $M = \begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_3 & \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_3 & \alpha_1 \end{bmatrix}$*, então* $\det M = -a(a^2 - 3b)$.

Prova: Usando a regra de Sarrus encontramos $\det M = \alpha_1^3 + \alpha_2^2 + \alpha_3^2 - 3\alpha_1\alpha_2\alpha_3$. Por outro lado, as relações de Girard nos dão

$$\alpha_1 + \alpha_2 + \alpha_3 = -a, \quad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = b, \quad \alpha_1\alpha_2\alpha_3 = -c.$$

Tomando a primeira dessas relações e elevando ao cubo obtemos

$$(\alpha_1 + \alpha_2 + \alpha_3)^3 = \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3(\alpha_1 + \alpha_2 + \alpha_3)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) - 3\alpha_1\alpha_2\alpha_3$$

e fazendo as substituições obtemos

$$-a^3 = \alpha_1^3 + \alpha_2^3 + \alpha_3^3 - 3ab + 3c,$$

ou seja,

$$\alpha_1^3 + \alpha_2^3 + \alpha_3^3 = a(a^2 - 3b) + 3c \Rightarrow \alpha_1^3 + \alpha_2^3 + \alpha_3^3 - 3c = a(a^2 - 3b) \Rightarrow \det M = a(a^2 - 3b).$$

□

Lema 3.3 *Seja* $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ *com raízes reais* α_1, α_2 *e* α_3*. Defina* $v_1 = (\alpha_1, \alpha_3, \alpha_2)$*,* $v_2 = (\alpha_2, \alpha_1, \alpha_3)$ *e* $v_3 = (\alpha_3, \alpha_2, \alpha_1)$*. Se* $v = xv_1 + yv_2 + zv_3$*, com* $x, y, z \in \mathbb{Z}$*, então*

$$|v|^2 = (a^2 - 2b)(x^2 + y^2 + z^2) + 2b(xy + xz + yz).$$

Prova:

$$\begin{aligned} |v|^2 &= \langle v, v \rangle \\ &= \langle xv_1 + yv_2 + zv_3, xv_1 + yv_2 + zv_3 \rangle \\ &= x^2|v_1|^2 + y^2|v_2|^2 + z^2|v_3|^2 + 2(xy\langle v_1, v_2\rangle + xz\langle v_1, v_3\rangle + yz\langle v_2, v_3\rangle). \end{aligned}$$

Mas

$$|v_1|^2 = |v_2|^2 = |v_3|^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = a^2 - 2b$$

e

$$\langle v_1, v_2\rangle = \langle v_1, v_3\rangle = \langle v_2, v_3\rangle = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = b.$$

Logo,

$$|v|^2 = (x^2 + y^2 + z^2)(a^2 - 2b) + 2b(xy + xz + yz).$$

□

Teorema 3.3 *Seja* $f(x) = x^3 + ax^2 + bx + 1 \in \mathbb{Z}[x]$, *onde* $a > 0$, $a^2 = 4b$ *e* $b \geq 9$. *Como antes, seja* $\alpha_1, \alpha_2, \alpha_3$ *raízes de* $f(x)$ *e defina* $v_1 = (\alpha_1, \alpha_3, \alpha_2)$, $v_2 = (\alpha_2, \alpha_1, \alpha_3)$ *e* $v_3 = (\alpha_3, \alpha_2, \alpha_1)$. *Então o reticulado* H *gerado por esses vetores tem densidade de centro igual a* $\delta_H = \dfrac{\sqrt{2}}{8}$, *que é o máximo atingido em dimensão 3.*

Prova: Se $v = (\alpha_1 x + \alpha_3 y + \alpha_2 z, \alpha_2 x + \alpha_1 y + \alpha_3 z, \alpha_3 x + \alpha_2 y + \alpha_1 z)$ então

$$\begin{aligned}
|v|^2 &= (\alpha_1 x + \alpha_3 y + \alpha_2 z)^2 + (\alpha_2 x + \alpha_1 y + \alpha_3 z)^2 + (\alpha_3 x + \alpha_2 y + \alpha_1 z)^2 \\
&= (\alpha_1^2 + \alpha_2^2 + \alpha_3^2)^2(x^2 + y^2 + z^2) + 2(xy\alpha_1\alpha_3 + xz\alpha_1\alpha_2 + yz\alpha_2\alpha_3) + \\
&\quad +2(xy\alpha_1\alpha_2 + xz\alpha_2\alpha_3 + yz\alpha_1\alpha_3) + 2(xy\alpha_3\alpha_2 + xz\alpha_3\alpha_1 + yz\alpha_2\alpha_1) \\
&= 2b(x^2 + y^2 + z^2) + 2b(xy + xz + yz) \\
&= 2b(x^2 + y^2 + xy + xz + yz)
\end{aligned}$$

Veja que $|v| \geq 2b(xy + xz + yz)$. Logo, o valor mínimo para $|v|$ é $\sqrt{2b}$. Esse valor é atingido, por exemplo, em $(1, 0, 0)$. Temos então que

$$vol(H) = a(a^2 - 3b) = ab = 2b\sqrt{b}.$$

O raio de empacotamento $\rho = \dfrac{\sqrt{2b}}{2}$ e a densidade de centro é

$$\delta_H = \frac{\left(\frac{\sqrt{2b}}{2}\right)^2}{2b\sqrt{b}} = \frac{\sqrt{2}}{8}.$$

□

Uma breve observação: No enunciado supomos que α_1, α_2 e α_3 eram reais. E de fato, para um tal polinômio as três raízes são reais. (Consulte Apêndice para mais detalhes.)

4 APÊNDICE

4.1 Discriminante de um Polinômio de Grau Três

A equação mais geral do terceiro grau é $ax^3 + bx^2 + cx + d = 0$. Ela é equivalente a $x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0$. Assim, basta considerar equações em que o coeficiente de x^3 é 1. Consideremos então a equação $x^3 + ax^2 + bx + c = 0$. A substituição $x = y - \frac{a}{3}$ nos dá

$$y^3 + \left(b - \frac{a^2}{3}\right)y + \frac{2a^2}{27} - \frac{ab}{3} + c = 0.$$

Sejam $p = b - \frac{a^2}{3}$ e $q = \frac{2a^2}{27} - \frac{ab}{3} + c$. Para resolver $y^3 + py + q = 0$ consideramos $y = u + v$. Elevando ao cubo obtemos

$$y^3 - 3uvy - (u^3 + v^3) = 0.$$

Impondo que $p = -3uv$ e $q = -(u^3 + v^3)$ obtemos o sistema

$$\begin{cases} u^3 \cdot v^3 &= -\frac{p^3}{27} \\ u^3 + v^3 &= -q \end{cases}$$

Logo,

$$u^3 = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} \quad \text{e} \quad v^3 = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}.$$

E como $y = u + v$, obtemos

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}.$$

Sendo $f(x) = x^3 + px + q$, definimos como discriminante de f o número

$$\Delta = \frac{q^2}{4} + \frac{p^3}{27}.$$

Vamos analisar o gráfico de $f(x) = x^3 + px + q$. Observemos que $f'(x) = 3x^2 + p$.

- Quando $p > 0$, f é crescente e portanto terá uma única raiz real.
- Quando $p = 0$, a equação $f(x) = 0$ se reduz a $x^3 = -q$, logo tem uma raiz real e duas raízes complexas quando $q \neq 0$ e uma raiz tripla (nula) quando $q = 0$.
- Quando $p < 0$, escrevemos $p = -3r^2$, com $r > 0$. A função f se torna $f(x) =$

$x^3 - 3r^2x + q$

$$f'(x) = 3x^2 - 3r^2 = 3(x^2 - r^2) \quad \text{e} \quad f''(x) = 6x.$$

Como $f'(-r) = 0$ e $f''(-r) < 0$, segue que $x = -r$ é ponto de máximo. Do mesmo modo, $x = r$ é ponto de mínimo.

Temos três casos a considerar

a) $f(r) \cdot f(-r) > 0$;

b) $f(r) \cdot f(-r) = 0$;

c) $f(r) \cdot f(-r) < 0$.

Veja que

$$\begin{aligned} f(r) \cdot f(-r) &= (r^3 - 3r^3 + q) \cdot (-r^3 + 3r^3 + q) \\ &= (q - 2r^3) \cdot (q + 2r^3) \\ &= q^2 - 4r^6 \\ &= q^2 - 4\left(-\frac{p}{3}\right)^3 \\ &= 4\left(\frac{q^2}{4} + \frac{p^3}{27}\right) \\ &= 4\Delta. \end{aligned}$$

Daí, concluímos que

1. $\Delta = 0$ implica que f possui três raízes reais.
2. $\Delta > 0$ implica que f possui uma raiz real e duas complexas.
3. $\Delta < 0$ implica que f possui três raízes reais distintas.

Para o polinômio $x^3 + ax^2 + bx + 1$, onde $a > 0$, $a^2 = 4b$ e $b \geq 0$ temos

$$\begin{aligned} \Delta &= \frac{1}{4}\left(\frac{8ab}{27} - \frac{ab}{3} + 1\right)^2 + \frac{1}{27}\left(\frac{3b - 4b}{3}\right)^3 \\ \Delta &= -\frac{1}{4}\left(\frac{ab}{27} + 1\right)^2 - \frac{1}{27}\left(\frac{b^3}{27}\right) \\ \Delta &= -\frac{1}{4}\left(\frac{ab + 27}{27}\right)^2 - \left(\frac{b}{9}\right)^3. \end{aligned}$$

Assim $\Delta < 0$, o que implica que f possui três raízes reais distintas.

4.2 O Volume de uma Esfera em $\mathbb{R}^n$ $(n \geq 3)$

Vamos denotar por $V_n(r)$ o volume da bola $B[0,r]$. Como bem sabemos

$$V_n(r) = \int\limits_{B[0,r]} dx_1 \cdots dx_n = r^n \cdot V_n(1),$$

onde a última igualdade é decorrente da mudança de variável $x = r \cdot u$. Agora note que

$$x_1^2 + x_2^2 + \cdots + x_n^2 \leq 1 \Leftrightarrow \left\{ \begin{array}{rcl} x_1^2 + \cdots + x_{n-2}^2 & \leq & 1 - x_{n-1}^2 - x_n^2 \\ x_{n-1}^2 + x_n^2 & \leq & 1 \end{array} \right. .$$

Podemos então escrever a integral para $V_n(1)$ como

$$V_n(1) = \int_{x_{n-1}^2 + x_n^2 \leq 1} \left(\int_{x_1^2 + \cdots + x_{n-2}^2 \leq R^2} dx_1 \cdots dx_{n-2} \right) dx_{n-1} dx_n,$$

onde $R = \sqrt{1 - x_{n-1}^2 - x_n^2}$. Temos então

$$V_{n-2}(R) = R^{n-2} \cdot V_{n-2}(1) = (1 - x_{n-1}^2 - x_{n-2}^2)^{\frac{n-2}{2}} \cdot V_{n-2}(1).$$

Fazendo $x = x_{n-1}$ e $y = x_n$, temos

$$V_n(1) = V_{n-2}(1) \cdot \int_{x^2+y^2} (1 - x^2 - y^2)^{\frac{n-2}{2}} \, dxdy.$$

Usando agora coordenadas polares obtemos

$$V_n(1) = V_{n-2}(1) \int_0^{2\pi} \int_0^1 (1 - r^2)^{\frac{n-2}{2}} \, r dr d\theta = \frac{2\pi}{n} \cdot V_{n-2}(1).$$

Observemos que $V_2(1) = \pi$ e para n par temos

$$\begin{array}{rcl} V_n(1) & = & \left(\frac{2\pi}{n}\right) \cdot \left(\frac{2\pi}{n-2}\right) \cdot \ldots \cdot \left(\frac{2\pi}{6}\right) \cdot \left(\frac{2\pi}{4}\right) \cdot V_2(1) \\ & = & \frac{2^{\frac{n-2}{2}} \pi^{\frac{n}{2}}}{n(n-2) \cdot \ldots \cdot 6 \cdot 4} \\ & = & \frac{\pi^{\frac{n}{2}}}{\left(\frac{n}{2}\right)!}. \end{array}$$

Para n ímpar, temos $V_3(1) = \frac{4\pi}{3}$ e então

$$\begin{aligned} V_n(1) &= \left(\frac{2\pi}{n}\right)\cdot\left(\frac{2\pi}{n-2}\right)\cdot\ldots\cdot\left(\frac{2\pi}{7}\right)\cdot\left(\frac{2\pi}{5}\right)\cdot V_3(1) \\ &= \frac{2^{\frac{n+1}{2}}\cdot\pi^{\frac{n-1}{2}}}{n(n-2)\cdot\ldots\cdot 7\cdot 5\cdot 3} \\ &= \frac{2^{\frac{n-1}{2}}\cdot\pi^{\frac{n-1}{2}}\cdot 2\cdot 4\cdot\ldots\cdot(n-1)}{n!} \\ &= \frac{2^n\cdot\pi^{\frac{n-1}{2}}\cdot\left(\frac{n-1}{2}\right)!}{n!}. \end{aligned}$$

Portanto

$$V_n(r) = \begin{cases} \dfrac{r^n\cdot\pi^{\frac{n}{2}}}{\left(\frac{n}{2}\right)!}, \text{se } n \text{ é par,} \\ \dfrac{r^n\cdot 2^n\cdot\pi^{\frac{n-1}{2}}\cdot\left(\frac{n-1}{2}\right)!}{n!}, \text{se } n \text{ é ímpar.} \end{cases}$$

5 CONCLUSÃO

Embora a simplicidade das demonstrações para os reticulados de densidade máxima,devemos levar em consideração a idéia principal que é de construir reticulados a partir de raízes de polinômios quadráticos e cúbicos. Para tais polinômios usamos o discriminante como uma ferramenta para decidir se um dado polinômio tem raízes reais ou complexas. Para polinômios quárticos a expressão que nos dá as raízes em função de seus coeficientes é um tanto indigesta e sinceramente não sei se renderia bons frutos atacar o mesmo problema utilizando discriminante do polinômio quártico.

Se quisermos ir um pouco além,devemos pensar em um método que não utilize discriminante,uma vez que para polinômios de grau maior ou igual a cinco não existe uma fórmula que expresse as raízes em função dos coeficientes. Fica então o desafio de encontrar uma família de reticulados gerados a partir de raízes de polinômios quárticos. O passo seguinte seria verificar que condições os coeficientes de um tal polinômio deveria satisfazer para que a densidade do respectivo reticulado fosse recorde.

REFERÊNCIAS

[1] FLORES, André Luiz et al. Optimal families of two and three dimensional lattice packings from polinomials with integer coecients . *JP Journal of Algebra, Number Theory and Aplications*, v. 15, n. 1, p. 45-51, 2009.

[2] CONWAY, J. H. ; SLOANE, N. J. A. *Sphere packings, lattices, and groups* .2nd ed. New York : Springer-Verlag, 1992.

[3] LIMA, Elon Lages. *A equação do terceiro grau*. Matemática Universitária, n. 5, p. 9-23, jun. 1987.

[4] STRAPASSON , João Eloir. *Geometria discreta e códigos*. Tese (Doutorado em Matemática) - Instituto de Matemática, Estatística e Computação Científca , Universidade Estadual de Campinas, 2007.

[5] SZPIRO, Georg G. *Kepler's conjecture and Halo's proof*. New York : John Wiley & Sons, 2003.

[6] LAGARIAS, J. C. (ed.). *The Kepler conjecture : the Hales-Ferguson proof*. New York : Springer, 2011.

[7] HUNGERFORD, Thomas W. *Álgebra*. New York : Springer-Verlag, 1974.

[8] SAMUEL, Pierre. *Algebraic theory of numbers*. Mineola, New York : Dover Publications, 1970.

[9] QUILES, Kátia Regina de Oliveira. *Discriminante de corpos de números*. Dissertação (Mestrado em Matemática)- Departamento de Matemática, IBILCF, UNESP, São José do Rio Preto, 2006.

[10] NUNES, Ruikon Sillas de Oliveira. *Discriminante mínimo de corpos abelianos de grau primo*. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2009.