

Novos resultados de reticulados algébricos

Antonio Aparecido de Andrade
Agnaldo José Ferrari
Grasiele Cristiane Jorge
Robson Ricardo de Araujo
IV Workshop de Álgebra da UFG - CAC

26 de maio de 2015

Conteúdo

Histórico

Códigos lineares

Conceitos básicos de teoria dos números

Reticulados

Perturbações do homomorfismo canônico

Introdução

1. Em sistemas de comunicações o objetivo é transmitir dados de uma fonte até o usuário. O meio usado é chamado de canal, que pode ser com ou sem fio. Na transmissão o canal pode gerar distorções e o sinal recebido pode não ser o enviado.
2. A teoria dos códigos corretores de erros surgiu por volta de 1940-48, com os trabalhos de Shannon. Provando que encontrar bons códigos é equivalente a encontrar empacotamentos esféricos densos no espaço euclidiano.

Teoria de Galois: extensões e monomorfismos.

Corpos de números.

Corpos ciclotômicos e seus principais subcorpos.

Obtenções das estruturas de subcorpos de corpos ciclotômicos.

Anel dos inteiros algébricos de um corpo de números.

Norma, traço e discriminante.

Assuntos

Homomorfismo canônico e suas perturbações.

Reticulados e seus principais parâmetros: matriz geradora, região fundamental, volume e densidade de centro.

Principais famílias de reticulados: $\mathbb{Z}_n$, A_n , D_n , E_n e Λ_n (laminados).

Empacotamento esférico e densidade de centro.

Gerações de reticulados via esses homomorfismos.

Conceitos básicos

A teoria de códigos surgiu no início da década de 50, como parte complementar de um trabalho teórico do matemático americano Claude E. Shannon (1916 - 2001), que em 1948 publicou uma série de resultados estabelecendo os limites teóricos para uma comunicação confiável.

Um dos principais problemas quando se deseja transmitir alguma informação é garantir que esta chegue intacta ao destino, ou seja, que os dados recebidos sejam confiáveis. Como dependemos de instrumentos eletrônicos para essa transmissão, sempre estamos suscetíveis aos erros e às falhas desses instrumentos ou a erros dos canais em que estas informações transitam.

Código linear

Código linear

Dizemos que $C \subset \mathbb{F}_q^n$ é um código linear se C for um subespaço vetorial k -dimensional de $\mathbb{F}_q^n$.

Distância mínima

Seja C um código. Definimos a distância mínima de C como sendo o natural

$$d_C = \max \{d(u, v); u, v \in C \text{ e } u \neq v\}.$$

Matriz geradora

Um código linear C admite uma base B e, assim, cada palavra-código $u \in C$ é representada de maneira única por uma combinação linear dos vetores de B . Seja a matriz G cujas linhas são os vetores de B , ou seja, se $v_i = (v_{i1}, v_{i2}, \dots, v_{in})$ para $i = 1, 2, \dots, k$, é um vetor de B , então

$$G = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}.$$

Essa matriz é chamada matriz geradora do código C com relação à base B . Logo, se C é um código k -dimensional, então a matriz geradora de C possui ordem $k \times n$.

Código dual

Seja $C \in \mathbb{F}_q^n$ um código linear k -dimensional. Seja o complemento ortogonal de C em relação a $\mathbb{F}_q^n$, ou seja, o conjunto

$$C^\perp = \{v \in \mathbb{F}_q^n; \langle u, v \rangle = 0, \text{ para todo } u \in C\}.$$

O complemento ortogonal $C^\perp$ também é um subespaço vetorial de $\mathbb{F}_q^n$, segue que $C^\perp$ pode também ser encarado como um código linear sobre $\mathbb{F}_q$.

Código dual

Dado um código linear $C \subset \mathbb{F}_q^n$, chamamos o complemento ortogonal $C^\perp$ de código dual de C .

Matriz controle de paridade

Seja C um código linear. Uma matriz geradora H do código dual $C^\perp$ é chamada matriz controle de paridade de C .

Relação entre as matrizes geradora e controle de paridade

Resultado

Se C é um código linear cuja matriz controle de paridade é H , então $v \in C$ se, e somente se, $Hv^t = 0$.

Resultado

Se $C \subset \mathbb{F}_q^n$ é um código linear k -dimensional com matriz geradora G , então o código dual $C^\perp$ tem dimensão $n - k$.

Observação

$$GH^t = 0.$$

Principais classes

As principais classes de códigos são: cíclicos, Hamming, BCH, Reed-Solomon, Alternant, Goppa e Srivastava.

Empacotamento esférico

1. O problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no espaço euclidiano de modo que a fração do espaço coberto pelas esferas seja a maior possível. Este fato é uma versão do 18º Problema de Hilbert - 1900.
2. Usando técnicas diversas tem-se obtido soluções parciais. Um dos métodos que apresenta boas características é através do homomorfismo canônico (ou Minkowski).

Corpos de números

Seja $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão de corpos de grau n , ou seja, um corpo de números de grau n . Assim, o corpo $\mathbb{K}$ pode ser visto como um espaço vetorial de dimensão n sobre $\mathbb{Q}$.

Inteiros algébricos

Definição

1. Um elemento $\alpha \in \mathbb{K}$ é chamado um inteiro algébrico se existe um polinômio mônico não nulo $f(x)$ com coeficientes em $\mathbb{Z}$ tal que $f(\alpha) = 0$.
2. O conjunto $\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} : \alpha \text{ é um inteiro algébrico}\}$ é um anel chamado anel dos inteiros algébricos de $\mathbb{K}$ e denotado por $\mathcal{O}_K$.
3. $\mathcal{O}_{\mathbb{K}}$ tem uma base $\{\alpha_1, \dots, \alpha_n\}$ sobre $\mathbb{Z}$, onde n é o grau de $\mathbb{L}$. Em outras palavras, todo elemento $\alpha \in \mathcal{O}_{\mathbb{K}}$ pode ser escrito de modo único como $\alpha = \sum_{i=1}^n a_i \alpha_i$, onde $a_i \in \mathbb{Z}$ para todo $i = 1, 2, \dots, n$.

Definição

A $\mathbb{Z}$ -base de $\mathcal{O}_{\mathbb{K}}$ é chamada uma *base integral* de $\mathbb{K}$ (ou de $\mathcal{O}_{\mathbb{K}}$).

Traço, discriminante e norma

Definição

1. O traço de um elemento $\alpha \in \mathbb{K}$ relativamente a extensão $\mathbb{Q} \subseteq \mathbb{K}$ é definido por

$$\text{Tr}_K(\alpha) = \sum_{i=1}^n \sigma_i(\alpha).$$

2. O discriminante de $\mathbb{K}$ over $\mathbb{Q}$ é definido por

$$\mathcal{D}_K = \mathcal{D}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2,$$

onde $\{\alpha_1, \dots, \alpha_n\}$ é uma base integral de $\mathbb{K}$.

3. A norma de um ideal $\mathcal{A} \subseteq \mathcal{O}_K$ como sendo o número de elementos do anel quociente $\mathcal{O}_K/\mathcal{A}$, ou seja,
 $\mathcal{N}_K(\mathcal{A}) = \circ(\mathcal{O}_K/\mathcal{A})$.

Corpos quadráticos

Corpo quadrático

Uma extensão $\mathbb{K}$ de grau 2 sobre os racionais $\mathbb{Q}$ é chamado de corpo quadrático. Neste caso, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z}$ é livre de quadrados.

Teorema

Se $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados, então $\mathbb{O}_K$ é dado por

1. $\mathbb{Z}[\sqrt{d}]$ se $d \not\equiv 1 \pmod{4}$, e
2. $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$ se $d \equiv 1 \pmod{4}$.

Corpos ciclotômicos

Teorema

Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$ então $\mathbb{O}_K = \mathbb{Z}[\zeta_n]$.

Teorema

$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$, onde $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é o subcorpo maximal real of $\mathbb{Q}(\zeta_n)$.

Teorema

$\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ é o anel de inteiros algébricos de $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ e $\{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{\phi(n)-1}\}$ é uma base integral de $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Teorema

O discriminante de um corpo ciclotômico $\mathbb{Q}(\zeta_n)$ é dado por

$$\mathcal{D} = (-1)^{\varphi(n)} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\frac{\varphi(n)}{p-1}}}.$$

Definição

1. Sejam V um espaço vetorial de dimensão finita n sobre um corpo $\mathbb{K}$, $A \subseteq \mathbb{K}$ um anel e $v_1, \dots, v_m$ vetores de V linearmente independentes sobre $\mathbb{K}$ com $m \leq n$. Um **reticulado** com base $\beta = \{v_1, \dots, v_m\}$ é o conjunto dos elementos de V da forma

$$\mathcal{H}_\beta = \{x = \sum_{i=1}^m a_i v_i, \text{ com } a_i \in A\}.$$

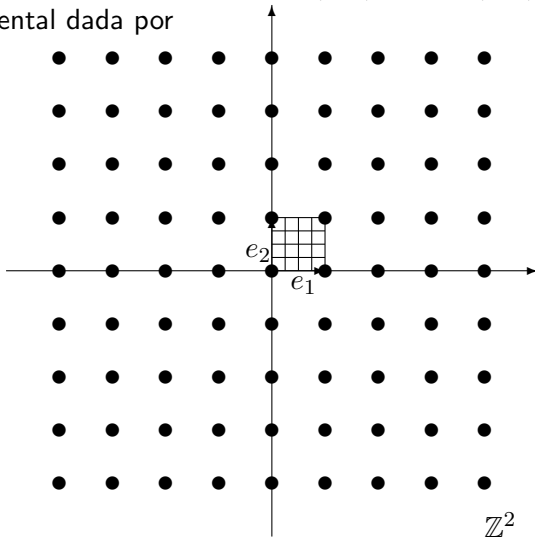
2. O conjunto

$$\mathcal{P}_\beta = \{x \in \mathbb{R} : x = \sum_{i=1}^n \lambda_i v_i, 0 \leq \lambda_i < 1\},$$

é chamado de região fundamental de $\mathcal{H}_\beta$ com relação a base $\{v_1, \dots, v_n\}$.

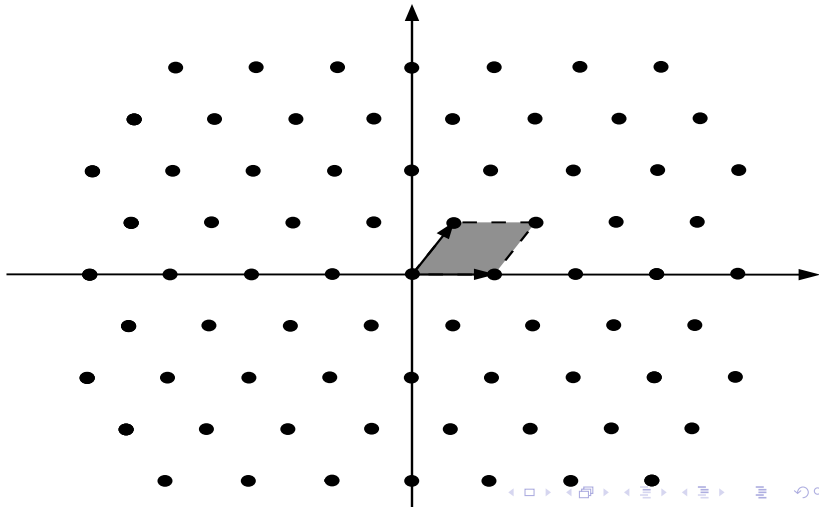
Exemplo

O reticulado $\Lambda = \mathbb{Z}^2$ é gerado por $e_1 = (1, 0)$ e $e_2 = (0, 1)$, com região fundamental dada por



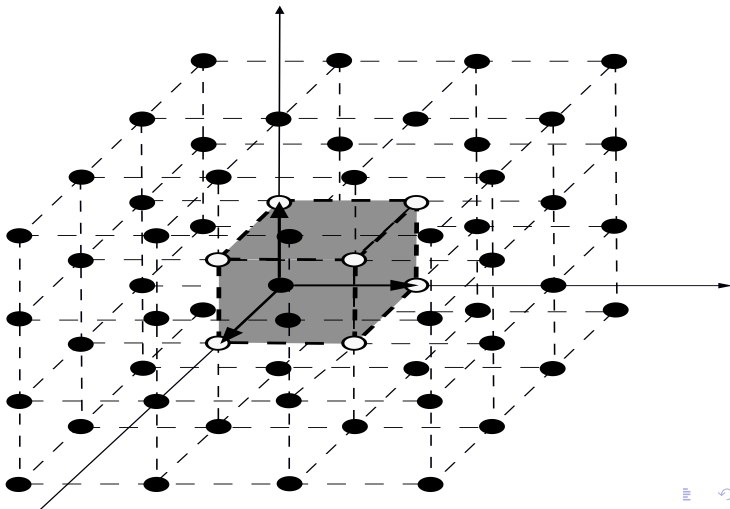
Exemplo

O reticulado gerado por $e_1 = (1, 0)$ e $e_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ tem região fundamental dada por



Exemplo

O reticulado gerado por $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ e $e_3 = (0, 0, 1)$ tem região fundamental dada por



Volume do reticulado

Definição

1. Se $v_i = (v_{i1}, v_{i2}, \dots, v_{in})$, para $i = 1, 2, \dots, n$, definimos o volume da região fundamental $\mathcal{P}_\beta$, como o módulo do determinante da matriz

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

2. O volume do reticulado $\mathcal{H}_\beta$ é definido como $\text{Vol}(\mathcal{H}_\beta) = \text{Vol}(\mathcal{P}_\beta)$.

Raio de empacotamento

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

Densidade de centro

Denotando por $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ , temos que a densidade de empacotamento de $\mathcal{H}_\beta$ é definida por

$$\Delta(\mathcal{H}_\beta) = \frac{\text{Volume da esfera}}{\text{Volume da região fundamental}} = \frac{\text{Vol}(\mathcal{B}(\rho))}{\text{Vol}(\mathcal{H}_\beta)} = \frac{\text{Vol}(\mathcal{B}(1))\rho^n}{\text{Vol}(\mathcal{H}_\beta)}.$$
 Portanto, o problema se reduz ao estudo de um outro parâmetro, chamado de densidade de centro, que é dado por

$$\delta(\mathcal{H}_\beta) = \frac{\rho^n}{\text{Vol}(\mathcal{H}_\beta)}.$$

Logo, tiramos a seguinte relação

$$\Delta(\mathcal{H}_\beta) = \text{Vol}(\mathcal{B}(1))\delta(\mathcal{H}_\beta)$$

ou seja, a densidade de empacotamento de $\mathcal{H}_\beta$ é igual ao produto entre o volume da esfera com centro na origem e raio 1 e a densidade de centro de $\mathcal{H}_\beta$.

Curiosidades

Como curiosidade, temos que para as dimensões 2 e 3, os melhores empacotamentos são conhecidos de todos e aparecem em lugares inusitados. No caso bidimensional, os favos das coméias, onde as abelhas depositam o mel, e para o caso tridimensional, o empilhamento de laranjas, que é facilmente encontrado em feiras livres.

Reticulados importantes

$$A_n = \{(x_0, x_1, \dots, x_n) \in \mathbb{Z}^{n+1} : \sum x_i = 0\}, \quad n \geq 1$$

$$D_n = \{(x_0, x_1, \dots, x_n) \in \mathbb{Z}^n : \sum x_i \equiv 0 \pmod{2}\}, \quad n \geq 3$$

$$E_8 = \{(x_0, x_1, \dots, x_8) \in \mathbb{R}^8 : \forall x_i, \quad x_i \in \mathbb{Z} \text{ ou } x_i \in \mathbb{Z} + 1/2, \quad \sum x_i \equiv 0 \pmod{2}\}$$

$$E_7 = \{x \in E_8 : xv = 0\}, \text{ para algum vetor minimal } v \in E_8.$$

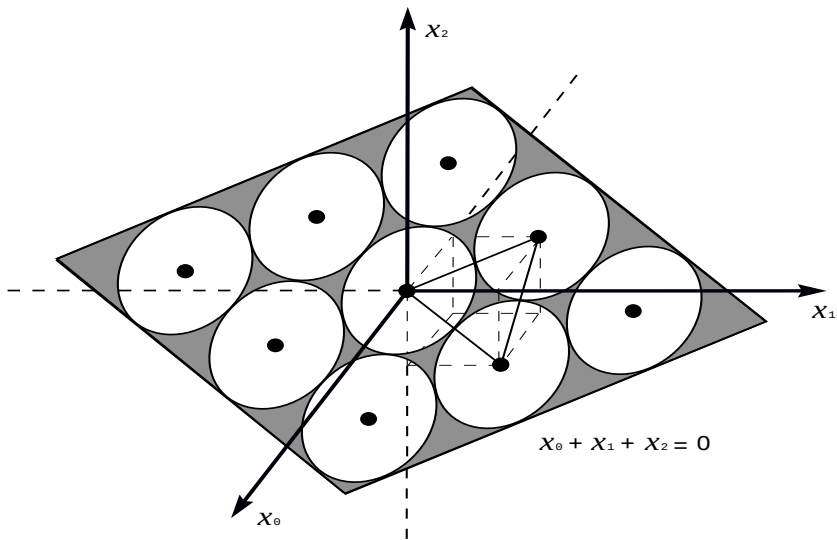
$$E_6 = \{x \in E_8 : xv = 0, \quad \forall v \in V\},$$

onde V é um A_2 -subreticulado em E_8 .

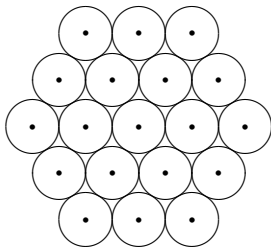
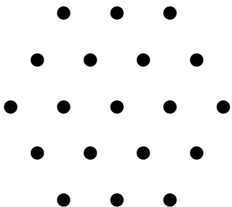
Melhores densidade de centro

<i>dim</i>	<i>densidade de centro</i>	<i>reticulado</i>
1	$1/2 = 0.50000$	$\Lambda_1 \cong A_1 \cong \mathbb{Z}$
2	$1/2\sqrt{3} \simeq 0.28868$	$\Lambda_2 \cong A_2$
3	$1/4\sqrt{2} \simeq 0.17678$	$\Lambda_3 \cong A_3 \cong D_3$
4	$1/8 = 0.12500$	$\Lambda_4 \cong D_4$
5	$1/8\sqrt{2} = 0.08839$	$\Lambda_5 \cong D_5$
6	$1/8\sqrt{3} \simeq 0.07217$	$\Lambda_6 \cong E_6$
7	$1/16 \simeq 0.06250$	$\Lambda_7 \cong E_7$
8	$1/16 \simeq 0.06250$	$\Lambda_8 \cong E_8$
12	$1/27 \simeq 0.03704$	K_{12}
24	1	Λ_{24}

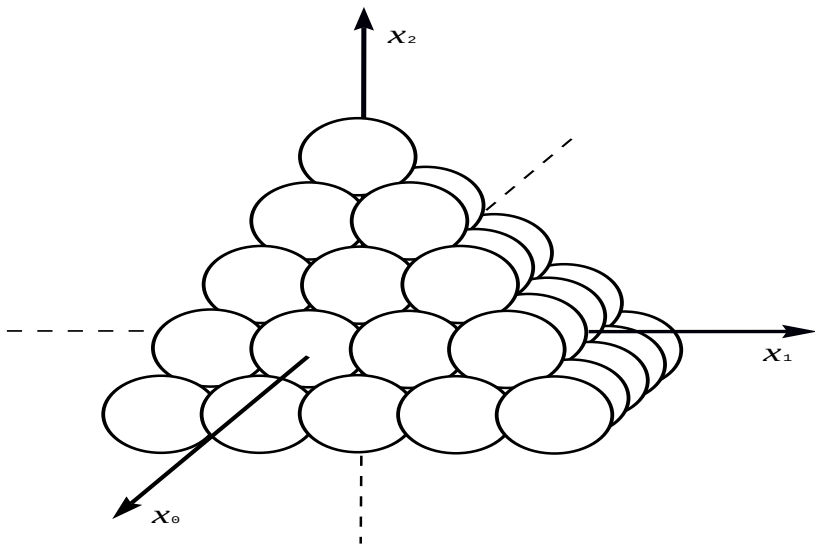
Exemplo



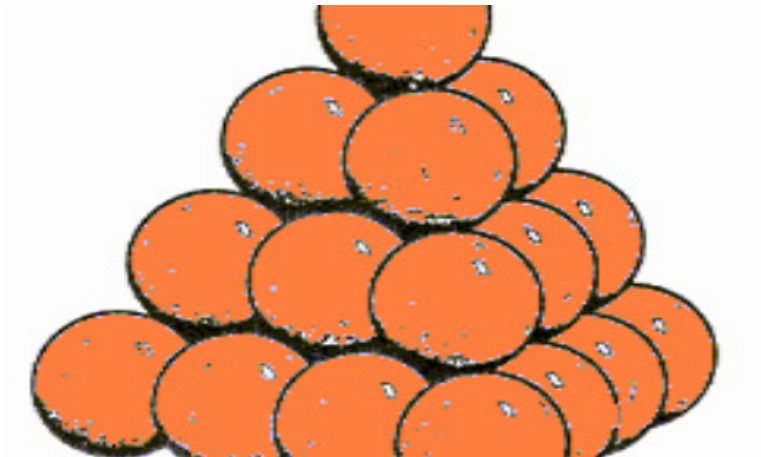
Exemplo



Exemplo



Exemplo



Homomorfismo canônico e reticulado algébrico

Definição

Seja $x \in \mathbb{K}$. A aplicação $\sigma_K : \mathbb{K} \longrightarrow \mathbb{R}^n$ definida por

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

é um homomorfismo injetivo de anéis, chamado de homomorfismo canônico (ou Minkowski), onde as notações $\Re(\beta)$ e $\Im(\beta)$ representam as partes real e imaginária do número complexo β , respectivamente.

Proposição

Se $\mathcal{A}$ é um ideal não nulo de $\mathcal{O}_K$ então $\sigma_K(\mathcal{O}_K)$ e $\sigma_K(\mathcal{A})$ são reticulados, com respectivos volumes,

$$\begin{aligned} \text{Vol}(\sigma_K(\mathcal{O}_K)) &= 2^{-r_2} |\mathcal{D}_K|^{\frac{1}{2}} \quad \text{e} \\ \text{Vol}(\sigma_K(\mathcal{A})) &= \text{Vol}(\sigma_K(\mathcal{O}_K)) \mathcal{N}_K(\mathcal{A}), \end{aligned}$$

onde $\mathcal{N}_K(\mathcal{A})$ é a norma do ideal $\mathcal{A}$.

Densidade de centro

Proposição

Se $\mathcal{A}$ é um ideal não nulo de $\mathcal{O}_K$ então a densidade de centro do reticulado $\sigma_K(\mathcal{A})$ é dada por

$$\delta(\sigma_K(\mathcal{A})) = \frac{2^{r_2}(\rho(\sigma_K(\mathcal{A})))^n}{|\mathcal{D}_K|^{\frac{1}{2}}\mathcal{N}_K(\mathcal{A})},$$

onde $\rho(\sigma_K(\mathcal{A}))$ é o raio de empacotamento do reticulado $\sigma_K(\mathcal{A})$.

Proposição

Se $x \in \mathbb{K}$, então $|\sigma_K(x)|^2 = c_K \text{Tr}_K(x\bar{x})$, onde

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

onde $\bar{x}$ é a conjugação complexa do elemento x .

Raio de empacotamento

Se $\mathbb{Q} \subseteq \mathbb{K}$ é uma extensão de grau n , totalmente real ou totalmente imaginária, $\mathcal{O}_K$ o anel dos inteiros algébricos de $\mathbb{K}$ e $\mathcal{A}$ um ideal não nulo de $\mathcal{O}_K$, então podemos reescrever o raio de empacotamento do reticulado $\sigma_K(\mathcal{A})$ da seguinte forma

$$\begin{aligned}\rho(\sigma_K(\mathcal{A})) &= \frac{1}{2} \min\{|\sigma_K(x)|, x \in \mathcal{A}, x \neq 0\} \\ &= \frac{1}{2} \min\left\{\sqrt{c_K \operatorname{Tr}_K(x\bar{x})}, x \in \mathcal{A}, x \neq 0\right\}.\end{aligned}$$

Densidade de centro

Proposição

Se $\mathcal{A}$ é um ideal não nulo de $\mathcal{O}_K$ então a densidade de centro do reticulado $\sigma_K(\mathcal{A})$ é dada por

$$\delta(\sigma_K(\mathcal{A})) = \frac{1}{2^n |\mathcal{D}_K|^{\frac{1}{2}}} \frac{t^{\frac{n}{2}}}{\mathcal{N}_K(\mathcal{A})},$$

onde $t = \min\{Tr_K(x\bar{x}), x \in \mathcal{A}, x \neq 0\}$.

Observação

Se $x \in \mathcal{A}$, $x \neq 0$, então para calcular a densidade de centro do reticulado $\sigma_K(\mathcal{A})$, o grande desafio é obter a expressão $Tr_K(x\bar{x})$, que é uma forma quadrática, e minimizá-la.

Exemplo

Exemplo

Se $\mathbb{K} = \mathbb{Q}(\zeta_6)$, onde ζ_6 é uma raiz sexta da unidade, e $\mathcal{A} = \zeta_6 \mathcal{O}_K$ é um ideal de $\mathcal{O}_K = \mathbb{Z}[\zeta_6]$, então $[\mathbb{K} : \mathbb{Q}] = 2$, $\mathcal{D}_K = \pm 3$ e $\mathcal{N}_K(\mathcal{A}) = 1$. Se $x \in \mathcal{A}$, então $x = \zeta_6(a_0 + a_1\zeta_6)$, com $a_0, a_1 \in \mathbb{Z}$, e assim $Tr_K(x\bar{x}) = 2(a_0^2 + a_0a_1 + a_1^2)$. Portanto, $t = \min\{Tr_K(x\bar{x}) : x \in \mathcal{A}, x \neq 0\} = 2$, pois é suficiente tomar $a_0 = 1$ e $a_1 = 0$, e deste modo a densidade de centro é dada por

$$\delta(\sigma_K(\mathcal{A})) = \frac{1}{2^n |\mathcal{D}_K|^{1/2}} \frac{t^{n/2}}{\mathcal{N}_K(\mathcal{A})} \simeq 0,28868,$$

que é uma densidade de centro ótima para esta dimensão, ou seja, com a mesma densidade de centro do reticulado Λ_2 .

Perturbação σ_α e reticulado ideal

Definição

Seja $x \in \mathbb{K}$. A perturbação $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ do homomorfismo canônico é definida como

$$\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), \dots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \Re(\sqrt{\alpha_{r_1+1}}\sigma_{r_1+1}(x)), \Im(\sqrt{\alpha_{r_1+1}}\sigma_{r_1+1}(x)), \dots, \Re(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x)), \Im(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x)))$$

onde $\sigma_i(\alpha) \in \mathbb{R}$ e $\alpha_i = \sigma_i(\alpha) > 0$, para todo $i = 1, 2, \dots, r_1 + r_2$ e as notações $\Re(\beta)$ e $\Im(\beta)$ representam as partes real e imaginária do número complexo β , respectivamente.

Proposição

Se $\mathcal{A}$ é um ideal não nulo de $\mathcal{O}_K$, então $\sigma_\alpha(\mathcal{O}_K)$ e $\sigma_\alpha(\mathcal{A})$ são reticulados, com respectivos volumes,

$$\begin{aligned} \text{Vol}(\sigma_\alpha(\mathcal{O}_L)) &= 2^{-r_2} |\mathcal{N}_L(\alpha) \mathcal{D}_L|^{\frac{1}{2}} \text{ e} \\ \text{Vol}(\sigma_\alpha(\mathcal{A})) &= 2^{-r_2} |\mathcal{N}_L(\alpha) \mathcal{D}_L|^{\frac{1}{2}} \mathcal{N}_L(\mathcal{A}). \end{aligned}$$

Densidade de centro

Ccorolário

Se $\mathcal{A}$ é um ideal não nulo de $\mathcal{O}_K$ então a densidade de centro do reticulado $\sigma_\alpha(\mathcal{A})$ é dada por

$$\delta(\sigma_\alpha(\mathcal{A})) = \frac{(\rho(\sigma_\alpha(\mathcal{A})))^n}{2^n |\mathcal{N}_K(\alpha) \mathcal{D}_K|^{\frac{1}{2}} \mathcal{N}_K(\mathcal{A})},$$

onde $\rho(\sigma_\alpha(\mathcal{A}))$ é o raio de empacotamento do reticulado $\sigma_\alpha(\mathcal{A})$.

Proposição

Se $x \in \mathbb{K}$ então $|\sigma_\alpha(x)|^2 = c_\alpha \text{Tr}_K(\alpha x \bar{x})$, onde

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

e $\bar{x}$ é a conjugação complexa do elemento x .

Raio de empacotamento

Proposição

Se $\mathbb{K}$ é totalmente real ou totalmente imaginária e $\mathcal{A}$ um ideal não nulo de $\mathcal{O}_K$, então podemos reescrever o raio de empacotamento do reticulado $\sigma_\alpha(\mathcal{A})$ da seguinte forma

$$\begin{aligned}\rho(\sigma_\alpha(\mathcal{A})) &= \frac{1}{2} \min\{|\sigma_\alpha(x)|, x \in \mathcal{A}, x \neq 0\} \\ &= \frac{1}{2} \min\left\{\sqrt{c_\alpha \operatorname{Tr}_K(\alpha x \bar{x})}, x \in \mathcal{A}, x \neq 0\right\},\end{aligned}$$

onde

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

e $\bar{x}$ é a conjugação complexa do elemento x .

Densidade de centro

Proposição

Se $\mathbb{K}$ é totalmente real ou totalmente imaginário e $\mathcal{A}$ um ideal não nulo de $\mathcal{O}_K$ então a densidade de centro do reticulado $\sigma_\alpha(\mathcal{A})$ é dada por

$$\delta(\sigma_\alpha(\mathcal{A})) = \frac{1}{2^n(|\mathcal{D}_K|\mathcal{N}_K(\alpha))^{1/2}} \frac{t_\alpha^{n/2}}{\mathcal{N}_K(\mathcal{A})},$$

onde $t_\alpha = \min\{Tr_K(\alpha x \bar{x}), x \in \mathcal{A}, x \neq 0\}$.

Perturbação $\sigma_{2\alpha}$

Definição

Seja $x \in \mathbb{K}$. A perturbação $\sigma_{2\alpha} : \mathbb{K} \longrightarrow \mathbb{R}^n$ do homomorfismo canônico é definida como

$$\begin{aligned} \sigma_{2\alpha}(x) = & (\sqrt{\alpha_1}\sigma_1(x), \dots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \Re(\sqrt{2\alpha_{r_1+1}}\sigma_{r_1+1}(x)), \Im(\sqrt{2\alpha_{r_1+1}}\sigma_{r_1+1}(x)), \\ & \dots, \Re(\sqrt{2\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x)), \Im(\sqrt{2\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x))), \end{aligned}$$

onde $\sigma_i(\alpha) \in \mathbb{R}$ e $\alpha_i = \sigma_i(\alpha) > 0$, para todo $i = 1, 2, \dots, r_1 + r_2$ e as notações $\Re(\beta)$ e $\Im(\beta)$ representam as partes real e imaginária do número complexo β , respectivamente.

Proposição

Se $\mathcal{A}$ é um ideal não nulo de $\mathcal{O}_K$, então $\sigma_{2\alpha}(\mathcal{O}_K)$ e $\sigma_{2\alpha}(\mathcal{A})$ são reticulados, com respectivos volumes,

$$\text{Vol}(\sigma_{2\alpha}(\mathcal{O}_K)) = (|\mathcal{D}_K| \mathcal{N}_K(\alpha))^{\frac{1}{2}} \text{ e}$$

$$\text{Vol}(\sigma_{2\alpha}(\mathcal{A})) = (|\mathcal{D}_K| \mathcal{N}(\alpha))^{\frac{1}{2}} \mathcal{N}_K(\mathcal{A}).$$

Densidade de centro

Corolário

Se $\mathcal{A}$ é um ideal não nulo de $\mathcal{O}_K$ então a densidade de centro do reticulado $\sigma_{2\alpha}(\mathcal{A})$ é dada por

$$\delta(\sigma_{2\alpha}(\mathcal{A})) = \frac{(\rho(\sigma_{2\alpha}(\mathcal{A})))^n}{(|\mathcal{D}_K| \mathcal{N}_K(\alpha))^{\frac{1}{2}} \mathcal{N}_K(\mathcal{A})},$$

onde $\rho(\sigma_{2\alpha}(\mathcal{A}))$ é o raio de empacotamento do reticulado e $\mathcal{N}_K(\alpha)$ a norma do elemento α .

Proposição

Se $x \in \mathbb{K}$ então

$$|\sigma_{2\alpha}(x)|^2 = \text{Tr}_K(\alpha x \overline{x}).$$

Raio de empacotamento

Proposição

Se $\mathbb{K}$ é totalmente real ou totalmente imaginário e $\mathcal{A}$ um ideal não nulo de $\mathcal{O}_K$, então podemos reescrever o raio de empacotamento do reticulado $\sigma_{2\alpha}(\mathcal{A})$ da seguinte forma

$$\begin{aligned}\rho(\sigma_{2\alpha}(\mathcal{A})) &= \frac{1}{2} \min\{|\sigma_{2\alpha}(x)|, x \in \mathcal{A}, x \neq 0\} \\ &= \frac{1}{2} \min\left\{\sqrt{\text{Tr}_K(\alpha x \bar{x})}, x \in \mathcal{A}, x \neq 0\right\},\end{aligned}$$

onde $\bar{x}$ é a conjugado complexo do elemento x .

Densidade de centro

Proposição

Se $\mathbb{K}$ é totalmente real ou totalmente imaginário e $\mathcal{A}$ um ideal não nulo de $\mathcal{O}_K$ então a densidade de centro do reticulado $\sigma_{2\alpha}(\mathcal{A})$ é dada por

$$\delta(\sigma_{2\alpha}(\mathcal{A})) = \frac{1}{2^n(|\mathcal{D}_K|\mathcal{N}_K(\alpha))^{1/2}} \frac{t_{2\alpha}^{n/2}}{\mathcal{N}_K(\mathcal{A})},$$

onde $t_{2\alpha} = \min\{Tr_K(\alpha x \bar{x}), x \in \mathcal{A}, x \neq 0\}$.

Estudos recentes

1. $\mathbb{Q}(\zeta_n)$, com $n = p^2 p_1 \cdots p_s$.
2. $\mathbb{Q}(\zeta_n)$, com $n = p p_1 \cdots p_s$.
3. $\mathbb{Q}(\zeta_n)$, com $n = p^s$.

Bibliografia

-  E. Bayer-Fluckiger, *Definite unimodular lattices having an automorphism of given characteristic polynomial*, Comment. Math. Helvetici 59 (1984), 509-538.
-  E. Bayer-Fluckiger, J. Martinet, *Formes quadratiques liées aux algèbres semi-simples*, J. Reine Angew. Math., 451 (1994), 51-69.
-  E. Bayer-Fluckiger, *Lattices and number fields*, Contemporary Mathematics, 241 (1999), 69-84.
-  E. Bayer-Fluckiger, *Cyclotomic modular lattices*, Journal de Théorie des Nombres de Bordeaux 12 (2000) 273-280.
-  E. Bayer-Fluckiger, *Ideal lattices*, Proceedings of the conference Number Theory and Diophantine Geometry, (Zurich, 1999), Cambridge Univ. Press (2002), 168-184.
-  E. Bayer-Fluckiger, *Modular lattices over cyclotomic fields*, Journal of Number Theory 114 (2005) 394-411.

Bibliografia

-  E. Bayer-Fluckiger, *Ideal lattices over totally real number fields and euclidian minima*, Archiv Math., 86 (2006), 217-225.
-  J.H. Conway; N.J.A. Sloane, *Sphere packing, lattices and groups*, Springer-Verlag, New York, 1999.
-  X. Giraud and J.C. Belfiore, *Constellations matched to the Rayleigh fading channel*, IEEE Trans. on Inform. Theory, Vol. 42, No. 1, pp. 106-115, 1996.
-  J. Boutros; E. Viterbo; C. Rastello; J-C. Belfiore, *Good lattice constellations for both Rayleigh fading and Gaussian channels*, IEEE Trans. Inform. Theory, Vol. 42, No. 2, pp. 502-517, 1996.
-  P. Samuel, *Algebraic theory of numbers*, Hermann, Paris, 1970.