Um pouco da teoria algébrica dos números e aplicações

Antonio Aparecido de Andrade

Departamento de Matemática, IBILCE - UNESP

15 e 16 de junho de 2023

Agradecimentos: Fapesp 2013/25977-7 e 2022/02303-0

Introdução e objetivos

Uma das aplicações da Teoria dos Números é construir reticulados com densidade ótima no espaço euclidiano. Um método de construção é a partir do homomorfismo de Minkowisk, onde a imagem de um $\mathbb{Z}$-módulo do anel de inteiros de um corpo de números de dimensão n é um reticulado no espaço $\mathbb{R}^n$.

Portanto, é de suma importância conhecer o anel de inteiros e o discriminante de um corpo de números.

Introdução

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.

Empacotamento esférico

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 18^{o} Problema de Hilbert - 1900.

Definição

Um *empacotamento esférico* no $\mathbb{R}^n$, é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$ de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto.

Empacotamento reticulado

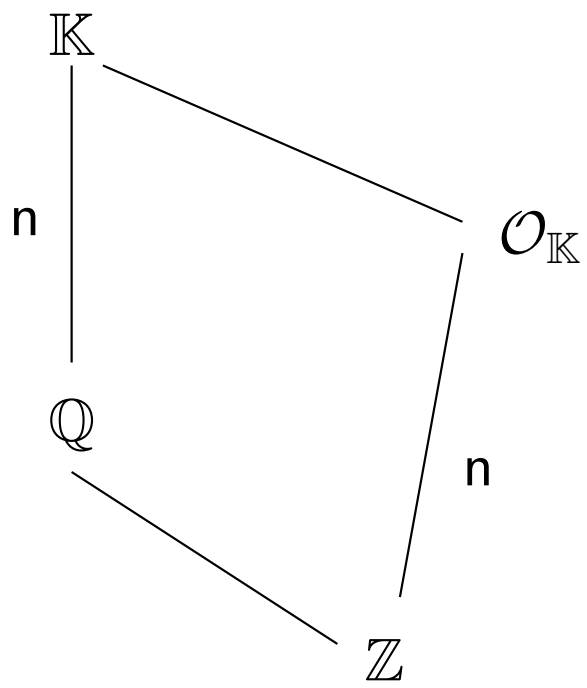
Definição

Um *reticulado* é um subgrupo discreto do $\mathbb{R}^n$, ou seja, a interseção com um conjunto compacto é finito.

Definição

Um *empacotamento reticulado* é um empacotamento em que o conjunto dos centros das esferas formam um reticulado no $\mathbb{R}^n$.

Ambiente de trabalho



Corpos de números

Definição

Um *corpo de números* $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$.

Exemplo

Um corpo quadrático é uma extensão de grau 2 de $\mathbb{Q}$, ou seja, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.

Exemplo

Um corpo ciclotômico é um corpo de números da forma $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde $\zeta_n^n = 1$ e $\zeta_n^k \neq 1$ para $0 < k < n$. O elemento ζ_n é chamado uma raiz n-ésima primitiva da unidade. Neste caso, $[\mathbb{K} : \mathbb{Q}] = \varphi(n)$.

Monomorfismos

Seja $\mathbb{K}$ um corpo de números de grau n, i.e., $\mathbb{K} = \mathbb{Q}(\alpha)$, onde $\alpha \in \mathbb{C}$ é uma raiz de um polinômio irredutível mônico $p(x) \in \mathbb{Z}[x]$.

As n raízes distintas de $p(x)$, a saber, $\alpha_1, \alpha_2, \cdots, \alpha_n$, são os conjugados de α. Se $\sigma : \mathbb{K} \to \mathbb{C}$ é um $\mathbb{Q}$-monomorfismo, então $\sigma(\alpha) = \alpha_i$, para algum $i = 1, 2, \cdots, n$.

Além disso, existem exatamente n $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$.

Monomorfismos reais ou complexos

Definição

Seja $\mathbb{K}$ um corpo de números de grau n.

1. Se $\sigma_k(\mathbb{K}) \subset \mathbb{R}$, o monomorfismo σ_k é chamado *real*.
2. Se $\sigma_k(\mathbb{K}) \not\subset \mathbb{R}$, o monomorfismo σ_k é chamado *imaginário*.

Definição

1. Se $\sigma(\mathbb{K}) \subseteq \mathbb{R}$, para todo σ, o corpo $\mathbb{K}$ é chamado *totalmente real*.
2. Se $\sigma(\mathbb{K}) \not\subseteq \mathbb{R}$, para todo σ, o corpo $\mathbb{K}$ é chamado *totalmente imaginário*.

Assinatura

Sejam r_1 o número de índices k tal que σ_k são reais. Assim, $n - r_1$ é um número par. Portanto, existe um número natural r_2 tal que $r_1 + 2r_2 = n$. Neste caso,

$$\sigma_{k+r_2}(\alpha) = \overline{\sigma_k(\alpha)},$$

para $r_1 + 1 \leq k \leq r_1 + r_2$ e $\alpha \in \mathbb{K}$.

Definição

O par (r_1, r_2) é chamado de *assinatura do corpo*.

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 $\mathcal{O}_{\mathbb{K}}$.

Base integral

Proposição

1. O anel $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n.
2. Uma base de $\mathcal{O}_{\mathbb{K}}$, como um $\mathbb{Z}$-módulo, é chamada *base integral* de $\mathbb{K}$.

No estudo de corpos de números, o grande desafio é encontrar uma base integral para $\mathcal{O}_{\mathbb{K}}$.

Definição

A *norma de um ideal* $\mathcal{A} \subseteq \mathcal{O}_K$ é definida como a cardinalidade do anel quociente $\mathcal{O}_K/\mathcal{A}$, ou seja, $\mathcal{N}(\mathcal{A}) = \circ(\mathcal{O}_K/\mathcal{A})$.

Traço, norma e discriminante

Definição

1. O *traço* e a *norma* de um elemento $\alpha \in \mathbb{K}$ relativamente a extensão $\mathbb{Q} \subseteq \mathbb{K}$ são definidos por

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad \text{e} \quad Tr(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

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

$$\mathcal{D}(\mathbb{K}) = \mathcal{D}(\alpha_1, \cdots, \alpha_n) = \det(\sigma_i(\alpha_j))^2,$$

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

Perguntas

Perguntas

Seja $\mathbb{K}$ um corpo de números de grau n.

1. Qual é o anel dos inteiros algébricos de $\mathbb{K}$?
2. Qual o discriminante?
3. Aplicações?

Primeiros passos

Primeiros resultados

André Luiz Flores - Tese de doutorado (FEEC - Unicamp). Reticulados em corpos abelianos. Orientador: Trajano.

Estudos

Corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^r})$ e $\mathbb{Q}(\zeta_{pq})$.

1. Determinou a forma traço.
2. Determinou os primeiros exemplos de reticulados algébricos via o homomorfismo de Minkowisk, com densidade de centro ótima.

Inteiros algébricos de corpos quadráticos e ciclotômicos

Corpo quadrático

Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.

1. Se $d \not\equiv 1 (mod\ 4)$, então $\{1, \sqrt{2}\}$ é uma base integral, e
2. Se $d \equiv 1 (mod\ 4)$, então $\{1, \frac{1+\sqrt{d}}{2}\}$ é uma base integral.

Corpo ciclotômico

Seja $\mathbb{L} = \mathbb{Q}(\zeta_n)$ um corpo ciclotômico. Uma base integral para $\mathbb{K}$ é dada por

$$\{1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}\}.$$

Inteiros algébricos de subcorpos de corpos ciclotômicos

Subcorpo maximal

Seja o subgrupo $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ de $\mathbb{L}$, chamado subcorpo maximal real. Uma base integral para $\mathbb{K}$ é dada por

$$\{1, \zeta_n + \zeta_n^{-1}, \ldots, \zeta_n^{\varphi(n)-1} + \zeta_n^{-(\varphi(n)-1)}\}.$$

Subcorpos de $\mathbb{L} = \mathbb{Q}(\zeta_p)$

Subcorpos de $\mathbb{L} = \mathbb{Q}(\zeta_p)$

Seja $\mathbb{K} \subset \mathbb{Q}(\zeta_p)$ um subcorpo, onde $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = m$ e $[\mathbb{K} : \mathbb{Q}] = n$. Como $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ é um grupo cíclico, segue que existe $r \in \mathbb{Z}$ tal que σ_r gera $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.

1. $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_p)$.
2. $\{\sigma_r(\theta), \sigma_{r^2}(\theta), \ldots, \sigma_{r^n}(\theta)\}$ é uma base para integral de $\mathbb{K}$.

Corpos cúbicos

Seja $\mathbb{K}$ um corpo cúbico, ou seja, $[\mathbb{K} : \mathbb{Q}] = 3$. Neste caso,

1. $\mathbb{K} = \mathbb{Q}(\theta)$.
2. $\theta \in \mathbb{C}$ é raiz de um polinômio irredutível $p(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$.
3. Base integral?

Corpos cúbicos

Saban Alaca: p-Integral Bases of Algebraic Number Fields. Tese (Doutorado) — Carleton University, 1994, fazendo uso de bases p-integrais, determinou bases integrais para corpos cúbicos da forma $\mathbb{Q}(\theta)$, com θ é uma raiz de um polinômio irredutível sobre $\mathbb{Z}$ da forma $f(x) = x^3 - ax + b \in \mathbb{Z}[x]$, sob certas condições específicas sobre os coeficientes a e b

Corpos cúbicos puros

Seja $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[3]{d}$, com d um inteiro livre de cubos. Neste caso,

1. d é livre de quadrados.
2. d não é livre de quadrados.

d é livre de quadrados

Seja $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[3]{d}$ e $d \in \mathbb{Z}$ livre de quadrados.

Teorema

O anel dos inteiros algébricos de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2, \text{ se } d \not\equiv \pm 1 (mod\ 9) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2-2\theta+\theta^2}{3}\right), \text{ se } d \equiv \pm 1 (mod\ 9). \end{cases}$$

Proposição

O discriminante de $\mathbb{K}$ é dado por

$$\mathcal{D}(\mathbb{K}) = \begin{cases} -27d^2, \text{ se } d \not\equiv \pm 1 (mod\ 9) \\ -3d^2, \text{ se } d \equiv \pm 1 (mod\ 9). \end{cases}$$

d não é livre de quadrados

Seja $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[3]{d}$ e $d \in \mathbb{Z}$ não é livre de quadrados. Neste caso, $d = m^2 n$ com m e n livre de quadrados e $mdc(m, n) = 1$.

Teorema

O anel dos inteiros algébricos de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\dfrac{\theta^2}{m}) \text{ se } d \not\equiv \pm 1 (mod\ 9), \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}(\dfrac{\theta^2 + m\theta + m}{3m}) \text{ se } d \equiv \pm 1 (mod\ 9). \end{cases}$$

Discriminante

Proposição

O discriminante de $\mathbb{K}$ é dado por

$$D(\mathbb{K}) = \begin{cases} -27m^2n^2, \text{ se } d \not\equiv \pm 1 (mod\ 9) \\ -3m^2n^2, \text{ se } d \equiv \pm 1 (mod\ 9). \end{cases}$$

Corpos quárticos puros

Seja $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[4]{d}$ e $d \in \mathbb{Z}$ é livre de quadrados.

Teorema

O anel dos inteiros algébricos de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3, \text{ se } d \not\equiv 1, 5 (mod\ 8) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{\theta^2-1}{2}\right) + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3}{2}\right), \text{ se } d \equiv 5 (mod\ 8) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{\theta^2-1}{2}\right) + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3}{4}\right), \text{ se } d \equiv 1 (mod\ 8). \end{cases}$$

Discriminante

Proposição

O discriminante de $\mathbb{K}$ é dado por

$$\mathcal{D}(\mathbb{K}) = \begin{cases} -256d^3, \text{ se } d \not\equiv 1, 5 (mod\ 8) \\ -16d^3, \text{ se } d \equiv 5 (mod\ 8) \\ -4d^3, \text{ se } d \equiv 1 (mod\ 8). \end{cases}$$

Corpos quínticos puros

Seja $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[5]{d}$ e $d \in \mathbb{Z}$ é livre de quadrados.

Teorema

O anel dos inteiros algébricos de $\mathbb{K}$ é dado por

$$\begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\theta^4, \text{ se } d \not\equiv \pm 1, \pm 7 (mod\ 25) \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\theta^3 + \mathbb{Z}\left(\frac{1+\theta+\theta^2+\theta^3+\theta^4}{5}\right), \text{ se } d \equiv \pm 1, \pm 7 (mod \end{cases}$$

Proposição

O discriminante de $\mathbb{K}$ é dado por

$$\mathcal{D}(\mathbb{K}) = \begin{cases} 3125d^4, \text{ se } d \not\equiv \pm 1, \pm 7 (mod\ 25) \\ 125d^4, \text{ se } d \equiv \pm 1, \pm 7 (mod\ 25). \end{cases}$$

Corpos sêxticos puros

Seja $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[6]{d}$ e $d \in \mathbb{Z}$ é livre de quadrados.

Teorema

O anel dos inteiros algébricos de $\mathbb{K}$ é dado por

$$\begin{cases} \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\theta^4+\mathbb{Z}\theta^5, \text{ se } d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\left(\frac{1+\theta^3}{2}\right)+\mathbb{Z}\left(\frac{4+3\theta+4\theta^2+\theta^4}{6}\right)+\mathbb{Z}\left(\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right), \text{ se } d \equiv 1 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\left(\frac{1+2\theta^2+\theta^4}{3}\right)+\mathbb{Z}\left(\frac{\theta+2\theta^3+\theta^5}{3}\right), \text{ se } d \equiv -10, -1 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\left(\frac{1+\theta^3}{2}\right)+\mathbb{Z}\left(\frac{4+3\theta+2\theta^2+\theta^4}{6}\right)+\mathbb{Z}\left(\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right), \text{ se } d \equiv 17 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\left(\frac{1+\theta^2+\theta^4}{3}\right)+\mathbb{Z}\left(\frac{\theta+\theta^3+\theta^5}{3}\right), \text{ se } d \equiv -17, 10 (mod\ 36) \\ \mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\left(\frac{1+\theta^3}{2}\right)+\mathbb{Z}\left(\frac{\theta+\theta^4}{2}\right)+\mathbb{Z}\left(\frac{\theta^2+\theta^5}{2}\right), \text{ se } d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36). \end{cases}$$

Discriminante

Proposição

O discriminante de $\mathbb{K}$ é dado por

$$\mathcal{D}(\mathbb{K}) = \begin{cases} 46656d^5, \text{ se } d \not\equiv \pm 1, \pm 17, \pm 10, -15, \\ \qquad\qquad -11, -7, -3, 5, 13 (mod\ 36) \\ 9d^5, \text{ se } d \equiv 1, 17 (mod\ 36) \\ 576d^5, \text{ se } d \equiv -17, -10, -1, 10 (mod\ 36) \\ 729d^5, \text{ se } d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36). \end{cases}$$

E agora?

1. Continuamos para o grau $7, 8, 9, 10, \ldots$?
2. Ou para os casos de grau $2p, 3p, 5p, \ldots$?
3. Ou para os casos de grau pq? Incluindo p^2.
4. Ou algo similar? Como p^2q?
5. Ou como p^n?

Extensão de grau primo

Seja $\mathbb{K}$ uma extensão de Galois de grau um primo p.

1. Pelo Teorema de Kronecker-Weber, segue que existe n mínimo tal que $\mathbb{K} \subseteq \mathbb{L} = \mathbb{Q}(\zeta_n)$.
2. $Gal(\mathbb{K} : \mathbb{Q}) =< \theta >$, onde $\theta(\zeta) = \zeta^{r^p}$, com $\mathbb{Z}_p^* =< r >$.
3. $\mathbb{K} = \mathbb{Q}(t)$, onde $t = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_n)$.

Proposição

1. Se p não ramifica em $\mathbb{L}$, então $n = p_1 p_2 \dots p_r$;
2. Se p ramifica $\mathbb{L}$, então $n = p^2 p_1 p_2 \dots p_r$,

onde $p_1, p_2, \dots, p_r$ são números primos tal que $p_i \equiv 1 (mod\ p)$, para $i = 1, 2, \dots, r$.

Anel de inteiros

Teorema

Uma base integral para $\mathbb{K}$ é dada por

1. $\{t, \theta(t), \ldots, \theta^{p-1}(t)\}$, se p não ramifica.
2. $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$, se p ramifica.
3. $\mathcal{D}(\mathbb{K}) = n^{p-1}$.

Fatos

1. Se a $\mathbb{K}$ extensão for de Galois de grau p, o anel de inteiros está completamente determinado.
2. Se for ou não de Galois, é um problema que ainda foi pouco explorado.
3. O discriminante está completamente determinado para a extensão de Galois de grau p.
4. Poucas aplicações.

Outros casos

1. Resolvemos tratar dos casos de grau p^n, com p primo.
2. $\mathbb{K} = \mathbb{Q}(\sqrt[p^n]{d})$, onde d é livre de quadrados.
3. Polinômio minimal $f(x) = x^{p^n} - d \in \mathbb{Q}[x]$.

Desafio:

1. Determinar o anel de inteiros.
2. Determinar o discriminante.
3. Aplicações?
4. Mas esses corpos possuem homomorfismos reais e complexos.
5. Como determinar a forma traço?

Reticulados no $\mathbb{R}^n$

Definição

Sejam $v_1, v_2, \ldots, v_m$ vetores de $\mathbb{R}^n$ linearmente independentes sobre $\mathbb{R}$, com $m \leq n$. O conjunto dos elementos da forma

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

é chamado de *reticulado* com base $B = \{v_1, v_2, \ldots, v_m\}$. Se $m = n$, o reticulado Λ é chamado um *reticulado completo*.

Região fundamental

Definição

O conjunto

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

é chamado de *região fundamental* de Λ com relação a base $\{v_1, v_2, \ldots, v_n\}$.

Matriz geradora

Definição

Seja $v_i = (v_{i1}, v_{i2}, \cdots, v_{in})$, para $i = 1, 2, \cdots, n$. A matriz

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

é chamada matriz *geradora do reticulado*.

Definição

O *volume do reticulado* Λ é definido por $V(\Lambda) = Vol(\mathcal{P}) = |\det(B)|$.

Empacotamento esférico

Estamos interessados em empacotamentos associado a um reticulado Λ onde as esferas são centradas nos pontos de Λ e tenham raio máximo.

Para a determinação deste raio, fixamos um número real $k > 0$ e o conjunto $\{x \in \mathbb{R}^n : ||x|| \leq k\} \cap \Lambda$. Podemos definir o número $\Lambda_{\min} = \min\{||\lambda|| : \lambda \in \Lambda \text{ e } \lambda \neq 0\}$.

Raio de empacotamento

Definição

Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e
$\Lambda_{\min} = \min\{||\lambda|| : \lambda \in \Lambda \text{ e } \lambda \neq 0\}$.

1. O número $(\Lambda_{\min})^2$ é chamado de *norma mínima* de Λ.
2. O maior raio para o qual é possível distribuir as esferas centradas nos pontos de Λ e obter um empacotamento é $\rho = \dfrac{\Lambda_{\min}}{2}$, e assim, ρ é chamado de *raio de empacotamento* de Λ.

Empacotamento esférico

Definição

Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e ρ o raio de empacotamento Λ. Consideramos $\mathcal{B}(0,\rho)$ a esfera de centro na origem e raio ρ. A *densidade de empacotamento* associada a Λ é definida por

$$\Delta(\Lambda) = \frac{\text{Volume da esfera}}{\text{Volume da região fundamental}} = \frac{\mathcal{V}ol(\mathcal{B}(0,\rho))}{\mathcal{V}ol(\Lambda)}.$$

Observação

Como $\mathcal{V}ol(\mathcal{B}(0,\rho)) = \mathcal{V}ol(\mathcal{B}(0,1))\rho^n$, segue que

$$\Delta(\Lambda) = \frac{\mathcal{V}ol(\mathcal{B}(0,1))\rho^n}{\mathcal{V}ol(\Lambda)}.$$

Densidade de centro

Definição

Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e ρ o raio de empacotamento Λ. O parâmetro

$$\delta(\Lambda) = \frac{\rho^n}{\mathcal{V}ol(\Lambda)},$$

é chamado de *densidade de centro* de Λ. Quando a densidade de centro é a maior possível chamamos-a de *densidade de centro ótima*.

Densidade de centro ótima

Dimensão	Densidade de centro ótima	Valor aproximado
2	$\frac{1}{2\sqrt{3}}$	$0,28868$
3	$\frac{1}{4\sqrt{2}}$	$0,17678$
4	$\frac{1}{8}$	$0,12500$
5	$\frac{1}{8\sqrt{2}}$	$0,08839$
6	$\frac{1}{8\sqrt{3}}$	$0,07217$

Tabela: Densidade de centro ótima de dimensão menor ou igual a 6.

Reticulados algébricos

Para cada $x \in \mathbb{K}$, a aplicação

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

é um homomorfismo injetor de anéis, chamado *homomorfismo de Minkowisk* ou *homomorfismo canônico*.

Homomorfismo de Minkowisk

Identificando $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ com $\mathbb{R}^n$, este homomorfismo pode ser visto como

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

onde $Re(x)$ representa a parte real de x e $\Im(x)$ representa a parte imaginária de x.

Reticulados algébricos

Proposição

Se $\mathcal{M} \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n, então

1. $\sigma(\mathcal{M})$ é um reticulado.
2. O volume do reticulado $\sigma(\mathcal{M})$ é dado por

$$\mathcal{V}ol(\sigma(\mathcal{M})) = \frac{\sqrt{|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]}{2^{r_2}}.$$

Definição

O reticulado $\sigma(\mathcal{M}) \subset \mathbb{R}^n$ é chamado de *reticulado algébrico*.

Densidade de centro

Proposição

A densidade de centro do reticulado $\sigma(\mathcal{M})$ é dada por

$$\delta(\sigma(\mathcal{M})) = \frac{2^{r_2}(\rho(\sigma(\mathcal{M})))^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]}.$$

Reticulados algébricos

Proposição

Se $\alpha \in \mathbb{K}$, então $||\sigma(\alpha)||^2 = c_{\mathbb{K}}\, Tr_{\mathbb{K}}(\alpha\overline{\alpha})$, 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 $\overline{\alpha}$ é a conjugação complexa do elemento α.

Raio de empacotamento

Seja $\mathbb{K}$ um corpo totalmente real ou totalmente imaginário.

Corolário

O raio de empacotamento do reticulado $\sigma(\mathcal{M})$ da seguinte forma

$$\begin{aligned}\rho(\sigma(\mathcal{M})) &= \frac{1}{2} min\{||\sigma(\alpha)||, \alpha \in \mathcal{M}, \alpha \neq 0\} \\ &= \frac{1}{2} min\left\{\sqrt{c_{\mathbb{K}} Tr_{\mathbb{K}}(\alpha\overline{\alpha})}, \alpha \in \mathcal{M}, \alpha \neq 0\right\}.\end{aligned}$$

Densidade de centro

Proposição

A densidade de centro do reticulado algébrico $\sigma(\mathcal{M})$ é dada por

$$\delta(\sigma(\mathcal{M})) = \frac{1}{2^n\sqrt{|\mathcal{D}(\mathbb{K})|}}\frac{\rho^{\frac{n}{2}}}{[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]},$$

onde $\rho = min\{\, Tr_{\mathbb{K}}(\alpha\overline{\alpha}) : \alpha \in \mathcal{M},\ \alpha \neq 0\}$.

Algoritmo

Para construir um reticulado algébrico e obter sua densidade de centro é preciso os seguintes passos.

1. Escolher um corpo de números $\mathbb{K}$ de grau n.
2. Determinar $\mathcal{O}_{\mathbb{K}}$ e $\mathcal{D}(\mathbb{K})$;
3. Escolher um $\mathbb{Z}$-módulo livre $\mathcal{M} \subseteq \mathcal{O}_{\mathbb{K}}$;
4. Determinar $\rho(\sigma(\mathcal{M})) = \frac{1}{2}\min\{||\sigma(\alpha)|| : \alpha \in \mathcal{M},\ \alpha \neq 0\}$;
5. Calcular $\delta(\sigma(\mathcal{O}_{\mathbb{K}})) = \dfrac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]}$.

Reticulados bem arrendondados

Os reticulados bem arredondados (do inglês, Well Rounded Lattices (WR)) têm sido um tópico de estudo recente, com aplicações em canais grampeados e em criptografia. Os reticulados WR são aqueles que possuem uma base em que todos os vetores têm norma coincidindo com a norma mínima do reticulado.

Fato

Existe uma infinidade de corpos de números quadráticos reais ou imaginários contendo ideais que produzem reticulados WR no plano.

Definição

Seja Λ um reticulado de posto completo no espaço euclidiano n-dimensional. A norma mínima de Λ é definida como

$$|\Lambda| = \min\{||\alpha||^2 : \alpha \in \Lambda \setminus \{0\}\},$$

onde $||\ ||$ denota a norma euclidiana usual em $\mathbb{R}^n$ e o conjunto de vetores mínimos de Λ é denotado por

$$S(\Lambda) = \{\alpha \in \Lambda : ||\alpha||^2 = |\Lambda|\}.$$

O reticulado Λ é WR se o conjunto $S(\Lambda)$ gera $\mathbb{R}^n$.

Resultados

Proposição

Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. O reticulado $\Lambda = \sigma(\mathcal{O}_{\mathbb{K}})$ é bem arrendondado se, e somente se, $d = -1$ e $d = -3$.

Proposição

Seja $\mathbb{K}$ um corpo de números. O reticulado $\Lambda = \sigma(\mathcal{O}_{\mathbb{K}})$ é bem arrendondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico.

Grau primo

Seja $\mathbb{K}$ uma extensão de Galois de primo p. Neste caso, $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, com n mínimo.

Proposição

1. Se p não ramifica em $\mathbb{L}$, então $n = p_1 p_2 \dots p_r$;
2. Se p ramifica $\mathbb{L}$, então $n = p^2 p_1 p_2 \dots p_r$,

onde $p_1, p_2, \dots, p_r$ são números primos tal que $p_i \equiv 1 (mod\ p)$, para $i = 1, 2, \dots, r$.

Teorema

Uma base integral para $\mathbb{K}$ é dada por

1. $\{t, \theta(t), \dots, \theta^{p-1}(t)\}$, se p não ramifica.
2. $\{1, \theta(t), \dots, \theta^{p-1}(t)\}$, se p ramifica.

p não ramifica

Seja o módulo

$$M_m = \{\alpha \in \mathcal{O}_{\mathbb{K}} : Tr_{\mathbb{K}}(\alpha) \equiv 0 (mod\ m)\}.$$

Proposição

M_m é um ideal se, e somente se, $m|n$.

Neste caso,

$$p_i\mathcal{O}_{\mathbb{K}} = \mathcal{B}_i^p,$$

onde $\mathcal{B}$ e $\mathcal{B}_i$ são ideais primos de $\mathcal{O}_{\mathbb{K}}$ com $\mathcal{B} \cap \mathbb{Z} = p\mathbb{Z}$ e $\mathcal{B}_i \cap \mathbb{Z} = p_i\mathbb{Z}$, para $i = 1, 2, \ldots, s$.

p não ramifica

Proposição

$M_{p_i} = \mathcal{B}_i$.

Proposição

1. $\mathcal{M}_m$ é um $\mathbb{Z}$-módulo de índice m.
2. O rank é p in $\mathcal{O}_{\mathbb{K}}$.
3. Se $m \equiv 1(mod\ p)$ and $\sqrt{\frac{n}{p+1}} \leq m \leq \sqrt{n(p+1)}$, então M_m é bem arrendondado.

p ramifica

Seja o módulo

$$M_m = \{\alpha \in \mathcal{O}_{\mathbb{K}} : Tr_{\mathbb{K}}(\alpha) \equiv 0 (mod\ m)\}.$$

Proposição

M_m é um ideal se, e somente se, $m|n$.

Proposição

1. $\mathcal{M}_m$ é um $\mathbb{Z}$-módulo de índice m.
2. O rank é p in $\mathcal{O}_{\mathbb{K}}$.

p ramifica

Seja o módulo

$$M_{m,c} = \{\alpha \in \mathcal{O}_{\mathbb{K}} : Tr_{\mathbb{K}}\left(\left(\frac{n - p^2 ct}{pn}\right)\alpha\right) \equiv 0 (mod\ m)\},$$

onde $1 \leq c \leq m-1$.

Proposição

1. $\mathcal{M}_m$ é um $\mathbb{Z}$-módulo de índice m.
2. O rank é p in $\mathcal{O}_{\mathbb{K}}$, ou seja,

$$\{m, c - \theta(t), c - \theta^2(t), \ldots, c - \theta^{p-1}(t)\}$$

é uma $\mathbb{Z}$-base de $\mathcal{M}_{m,c}$.

p ramifica

Proposição

$\mathcal{M}_{p,c} = \mathcal{B}$, para algum c.

Proposição

Se $\alpha = a_0 m + a_1(c - \theta(t)) + \cdots + a_{p-1}(c - \theta^{p-1}(t)) \in \mathcal{M}_{m,c}$ e $u = p_1 p_2 \ldots p_s$, então

$$Tr_{\mathbb{K}}(\alpha^2) = p\left(a_0^2 m^2 + 2a_0 cm \sum_{i=1}^{p-1} a_i\right)$$

$$+ \quad p\left(\sum_{i=1}^{p-1} a_i^2(c^2 + u(p-1)) + 2 \sum_{1 \le i < j \le p-1} a_i a_j (c^2 - u)\right).$$

$n = p^2$

Proposição

Se $n = p^2$, então $p\mathcal{O}_{\mathbb{K}} = \mathcal{B}^p$, onde $\mathcal{B} =< N_{\mathbb{L}/\mathbb{K}}(1 - \zeta_n) >$.

Seja

$$\mathcal{M}_{p,1} = \{a_0 + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathcal{O}_{\mathbb{K}}\}$$

tal que

$$a_0 + a_1 + \cdots + a_{p-1} \equiv 0(mod\ p)\}.$$

$n = p^2$

O conjunto

$$\{1-t, 1-\theta(t), \ldots, 1-\theta^{p-1}(t)\}$$

é uma $\mathbb{Z}$-base de $M_{p,1}$.

Proposição

Se
$\alpha = a_0(1-t) + a_1(1-\theta(t)) + \cdots + a_{p-1}(1-\theta^{p-1}(t)) \in \mathcal{M}_{m,1}$,
então

$$Tr_{\mathbb{K}}(\alpha^2) = p^2 \sum_{i=0}^{p-1} a_i^2.$$

$n = p^2$

Corolário

$\mathcal{M}_{p,1}$ é ortogonal e WR com base mínima

$$\{1 - t, 1 - \theta(t), \ldots, 1 - \theta^{p-1}(t)\}.$$

A. C. M. M. Chagas. *Uma contribuição à teoria dos números e aplicações*, Tese de Doutorado, Ibilce - Unesp, São José do Rio Preto - SP, 2015.

Araujo, R. R. *Reticulados algébricos e aplicações a códigos e criptografia*, Tese de Doutorado, Imecc - Unicamp, 2018.

Fachini, L. S. *Uma introdução aos corpos de números de grau menor ou igual a 6*, Dissertação de Mestrado em Matemática, UNESP, 2021.

Araujo, R. R., Costa, S. I. R. *Well-rounded algebraic lattices in odd prime dimension*. Archiv der Mathematik, **112**(2), 139-148, 2019.

Muito obrigado.