XI Bienal de Matemática 2024
Universidade Federal de São Carlos - UFSCar
29 de julho a 02 de agosto de 2024

Grupo das Classes via Redes Complexas

A fórmula de Dirichlet do número de classes para corpos quadráticos imaginários

Ribeiro Bernardo Silvério, Marcus Vinicius[1] e Teixeira Godinho, Hemar.

Resumo: *Por meio de ideais do anel dos inteiros algébricos de um corpo imaginário quadráticos em paralelo com Redes Complexas é possível construir um grupo abeliano finito $\mathcal{C}l(-n)$ conhecido como Grupo das Classes. Através de conceitos da Análise Complexa, definimos a função Zeta Dedekind junto às séries de Dirichlet permitindo definir e caracterizar a Função Zeta de Riemann e as L–Funções de Dirichlet resultando na fórmula do número das classes de ideais a qual representa a ordem do grupo $\mathcal{C}l(-n)$.*

Palavras-chave: *Anel dos inteiros Algébricos de $\mathbb{Q}(\sqrt{-n})$; Grupo das classes; Redes Complexas; Fórmula do número das classes.*

1. Introdução

Seja n um inteiro positivo livre de quadrados, um **corpo quadrático imaginário** é um subcorpo do corpo dos números complexos do tipo $\mathbb{Q}(\sqrt{-n}) = \{x + y\sqrt{-n};\ x,\ y \in \mathbb{Q}\}$ formando uma extensão de dimensão 2 vista como um espaço vetorial sobre o corpo dos racionais $\mathbb{Q}$. Note que $\{1,\ \sqrt{-n}\}$ e $\{1,\ \frac{1+\sqrt{-n}}{2}\}$ formam bases de $\mathbb{Q}(\sqrt{-n})$ sobre $\mathbb{Q}$ dado n módulo 4. Nesse sentido, através dos dois automorfismos, $\delta_1(\alpha) = \alpha$ e $\delta_2(\alpha) = \overline{\alpha}$ com $\alpha \in \mathbb{Q}(\sqrt{-n})$, aplicados às bases, caracterizamos Δ_{-n} como o **discriminante** de $\mathbb{Q}(\sqrt{-n})$ por:

$$\Delta_{-n} = det\left(\begin{pmatrix} \delta_1(1) & \delta_2(1) \\ \delta_1(\beta_{-n}) & \delta_2(\beta_{-n}) \end{pmatrix}\right)^2$$

onde $\beta_{-n} = \begin{cases} \sqrt{-n} & \text{se } n \equiv 1,\ 2 \pmod 4 \\ \frac{1+\sqrt{-n}}{2} & \text{se } n \equiv 3 \pmod 4 \end{cases}$; obtemos então que

$$\Delta_{-n} = \begin{cases} -4n & \text{se } n \equiv 1,\ 2 \pmod 4; \\ -n & \text{se } n \equiv 3 \pmod 4. \end{cases}$$

2. O anel dos inteiros algébricos $\mathcal{O}_{-n}$

O anel dos inteiros algébricos de $\mathbb{Q}\left(\sqrt{-n}\right)$ é descrito por:

$$\mathcal{O}_{-n} = \begin{cases} \mathbb{Z} + \sqrt{-n}\cdot\mathbb{Z} & \text{se } n \equiv 1,\ 2 \pmod 4; \\ \mathbb{Z} + \left(\frac{1+\sqrt{-n}}{2}\right)\cdot\mathbb{Z} & \text{se } n \equiv 3 \pmod 4. \end{cases}$$

Ideais Fracionários de $\mathcal{O}_{-n}$

Definição 1 *Para $I = (\alpha_1,\ \alpha_2)$ um ideal de $\mathcal{O}_{-n}$, dizemos que $\mathcal{I}$ é um **ideal fracionário** se existe um número algébrico não-nulo $\gamma \in \mathcal{O}_{-n}$ tal que*

$$\mathcal{I} = \frac{1}{\gamma}I = \left(\frac{\alpha_1}{\gamma},\ \frac{\alpha_2}{\gamma}\right) \subset \mathcal{O}_{-n}.$$

Proposição 1 *Todo ideal primo em $\mathcal{O}_{-n}$ possui um único elemento primo $p \in \mathbb{N}$. Assim a fatoração prima de um ideal principal (p) em $\mathcal{O}_{-n}$ é da forma:*

$$\begin{cases} (p) & se\ \left(\frac{-n}{p}\right) = -1 \\ \wp_1\cdot\wp_2 & se\ \left(\frac{-n}{p}\right) = 1 \\ \wp^2 & se\ \left(\frac{-n}{p}\right) = 0 \end{cases}$$

onde $\wp_1$, $\wp_2$ e $\wp$, ideais primos de $\mathcal{O}_{-n}$, são determinados pelo elemento primo p e $\left(\frac{-n}{p}\right)$ denota o símbolo de Legendre módulo p.

Teorema 1 *Todo ideal não-nulo $\mathcal{I} \subset \mathcal{O}_{-n}$ possui uma fatoração única em ideais primos $\wp_1, \ldots, \wp_k$ tal que*

$$\mathcal{I} = \prod_{i=1}^{k} \wp_i^{e_i},\ \text{onde } e_i \in \mathbb{N} \text{ para todo } i \in [1,\ k].$$

O grupo $\mathcal{C}l(-n)$

O grupo das classes de ideais de $\mathbb{Q}\left(\sqrt{-n}\right)$ é dado pelo quociente:

$$\mathcal{C}l\left(-n\right) = \frac{\text{Ideais fracionários de } \mathcal{O}_{-n}}{\text{Ideais Principais fracionários de } \mathcal{O}_{-n}}.$$

Redes Complexas

Definição 2 *Um conjunto $\Lambda \subset \mathbb{C}$ é dito uma **rede complexa** se existem $\alpha, \beta \in \Lambda$, elementos não nulos, tais que:*

$$\Lambda = \langle \alpha,\ \beta\rangle = \{m_1\alpha + m_2\beta;\ m_1,\ m_2 \in \mathbb{Z}\}\ e\ im(\tfrac{\beta}{\alpha}) \neq 0.$$

Definição 3 *Duas redes complexas Λ, $\tilde{\Lambda}$ são ditas **equivalentes** se existir $\delta \in \mathbb{C}$ não-nulo tal que $\Lambda^* = \delta\cdot\Lambda$, ou seja*

$$\Lambda = \langle \alpha,\ \beta\rangle \sim \Lambda^* \iff \Lambda^* = \langle \delta\alpha,\ \delta\beta\rangle\,.$$

Ideais de $\mathcal{O}_{-n}$ são interpretados como redes complexas possuindo uma propriedade chamada de multiplicação complexa, a saber:

Definição 4 *Dado $\rho \in \mathbb{C}\setminus\mathbb{Z}$, é dito que Λ é uma rede complexa com **multiplicação complexa** por ρ (denote MC_ρ) se $\rho\Lambda \subset \Lambda$.*

Nos restringimos a estudar redes com $MC_{\beta_{-n}}$ para concluir que:

Teorema 2 *Toda rede com $MC_{\beta_{-n}}$ é equivalente a uma única rede $\langle 1,\ \mathfrak{j}\rangle$ onde $\mathfrak{j} = \frac{a+\sqrt{-n}}{b}$ tal que:*

- *Se $\beta_{-n} = \sqrt{-n}$:*
  - *(i) $a, b \in \mathbb{Z}$;*
  - *(ii) $0 < b \leq 2\sqrt{\frac{n}{3}}$;*
  - *(iii) $-b < 2a \leq b$;*
  - *(iv) $a^2 + n \geq b^2$ (e $a \geq 0$ se $a^2 + n = b^2$);*
  - *(v) $b \mid a^2 + n$.*
- *Se $\beta_{-n} = \frac{1+\sqrt{-n}}{2}$:*
  - *(i) a ímpar e b par;*
  - *(ii) $0 < b \leq 2\sqrt{\frac{n}{3}}$;*
  - *(iii) $-b < 2a \leq b$;*
  - *(iv) $a^2 + n \geq b^2$ (e $a \geq 0$ se $a^2 + n = b^2$);*
  - *(v) $2b \mid a^2 + n$.*

Através do Teorema 2, em [1], o grupo das classes $\mathcal{C}l(-n)$ é abordado como um subconjunto de $\mathbb{C}$ composto por elementos da forma $\frac{a+\sqrt{-n}}{b}$. Como já fora definido $\mathcal{C}l(-n)$, o tamanho desse grupo é relacionado e determinado pela compatibilidade entre ideais de $\mathcal{O}_{-n}$ e redes equivalentes com $MC_{\sqrt{-n}}$ ou $MC_{\frac{1+\sqrt{-n}}{2}}$, assim:

Teorema 3 *O grupo das classes $\mathcal{C}l(-n)$ é finito.*

Logo, a representação da quantidade de redes equivalentes com $MC_{\beta_{-n}}$ é dada pela ordem do grupo $\mathcal{C}l(-n)$ intitulada ***número de classes*** (denote por $h(-n)$).

3. Fórmula para o número de classes

Definição 5 *A **Função Zeta Dedekind** de $\mathbb{Q}(\sqrt{-n})$ é descrita para $s \in \mathbb{R}$ como:*

$$\zeta_{-n}(s) \overset{def}{=} \sum_{\mathcal{I}\subset\mathcal{O}_{-n}} \mathcal{N}(\mathcal{I})^{-s} = \prod_{\wp\subset\mathcal{O}_{-n}} \left(1 - \mathcal{N}(\wp)^{-s}\right)^{-1}$$

em que $\mathcal{N}$ define a função norma.

Proposição 2 *Para $s > 1$, a função zeta Dedekind converge e assume uma forma em produto de Euler dada por:*

$$\zeta_{-n}\left(s\right) = \prod_{(\frac{-n}{p})=1} \left(1 - p^{-s}\right)^{-2} \cdot \prod_{(\frac{-n}{p})=0} \left(1 - p^{-s}\right)^{-1} \cdot \prod_{(\frac{-n}{p})=-1} \left(1 - p^{-2s}\right)^{-1}$$

com p primo; mais ainda, possui um polo simples em $s = 1$ com resíduo $\frac{h(-n)\cdot\pi}{A\cdot w_{-n}}$ em que w_{-n} denota a ordem do conjunto das unidades de $\mathcal{O}_{-n}$ e A a área do paralelogramo de vértices $0,\ 1,\ \beta_{-n},\ 1 + \beta_{-n}$ onde:

$$w_{-n} = \begin{cases} 2\ se\ n \neq 1, 3 \\ 4\ se\ n = 1 \\ 6\ se\ n = 3 \end{cases} \quad e\ A = \begin{cases} \sqrt{n}\ se\ n \equiv 1,\ 2 \pmod 4 \\ \frac{\sqrt{n}}{2}\ \ se\ n \equiv 3 \pmod 4 \end{cases}.$$

Proposição 3 *Para $s > 1$, temos que*

$$\zeta_{-n}\left(s\right) = \zeta\left(s\right)\cdot L_{-n}(s)$$

onde $\zeta\left(s\right)$ denota a função Zeta de Riemann e a $L-$função de Dirichlet dada pela série $L_{-n}\left(s\right) \overset{def}{=} \sum \left(\frac{\Delta_{-n}}{m}\right) m^{-s}$.

Teorema 4 *Seja $h(-n)$ o número das classes de $\mathbb{Q}(\sqrt{-n})$:*

$$L_{-n}(1) = \begin{cases} \dfrac{h(-n)\cdot\pi}{\sqrt{n}\cdot w_{-n}} & se\ n \equiv 1, 2 \pmod 4; \\[2ex] \dfrac{2\cdot h(-n)\cdot\pi}{\sqrt{n}\cdot w_{-n}} & se\ n \equiv 3 \pmod 4. \end{cases}$$

Por métodos analíticos, maneiras alternativas e interessantes de se encontrar/associar $h(-n)$ são apresentadas por Daniel Marcus em "*Number Fields*" provando que:

$$L_{-n}(1) = -\frac{\pi}{|\Delta_{-n}|^{\frac{2}{3}}} \cdot \sum_{m=1}^{|\Delta_{-n}|-1} m\ \chi_{-n}(m);$$

e em [2], ambos expondo o vínculo explícito com os caracteres quadráticos de Dirichlet dado por $\chi_{-n}(m) = \left(\frac{\Delta_{-n}}{m}\right)$, demonstrando o seguinte resultado:

Teorema 5 *Para um corpo quadrático imaginário com $\Delta_{-n} < -4$, temos que o número de classes de ideais é dada por:*

$$h(-n) = \frac{1}{2 - \chi_{-n}(2)} \sum_{0<m<\frac{|\Delta_{-n}|}{2}} \chi_{-n}(m).$$

Assim, por [2], o número de classes em $\mathcal{O}_{-p}$ quando $p \equiv 3 \pmod 4$, pela equação acima é:

$$h(-p) = \begin{cases} R - \tilde{R} & \text{se } p \equiv 7 \pmod 8; \\ \dfrac{R - \tilde{R}}{3} & \text{se } p \equiv 3 \pmod 8; \end{cases}$$

onde R denota o número de resíduos quadráticos e $\tilde{R}$ o número de resíduos não-quadráticos sob o intervalo aberto $(0,\ \frac{p}{2})$.

Utilizando sequências de Lehmer e métodos de resolução de Equações Diofantinas não lineares, em [3], Zhu e Wang demonstram que:

Teorema 6 *Seja $\mathbb{Q}(\sqrt{a^2 - \delta k^d})$ onde $a^2 - \delta k^d < 0$ é um inteiro livre de quadrados. Se $a = 2^m$ e $\delta = 1$, então*

$$h(-n) \equiv \begin{cases} 0 \pmod{\frac{d}{3}} & \text{caso: } \begin{array}{l} \text{ou } 3 \mid d \text{ e } 2^{2m} - k^d \equiv 5 \pmod 8; \\ \text{ou } d = 3 \text{ e } k = \frac{2^{2m+2}-1}{3}; \end{array} \\ 0 \pmod d & \text{caso contrário.} \end{cases}$$

Referências

[1] WESTON, Tom. **Lectures Lectures on the Dirichlet Class Number Formula for Imaginary Quadratic Fields**, 2004.

[2] BOREVICH, Z. I. and SHAFAREVICH, I. R.. **Number Theory**, Academic press, London, 1966.

[3] MINHUI, Zhu and TINGTING, Wang, **The divisibility of the class number of the imaginary quadratic field** $\mathbb{Q}(\sqrt{2^{2m} - k^n})$, Glasgow Math, pgs. 149-154, 2012.

Apoios:

CAPES CNPq FAPESP INCTMat

[1] Afiliação. Este autor foi apoiado pela CAPES e CNPq