Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Grupo das Classes Ideais via Redes Complexas: A fórmula de Dirichlet do número de classes e sua divisibilidade para o corpo imaginário $\mathbb{Q}\left(\sqrt{2^{2m}-k^d}\right)$.

Marcus Vinícius Ribeiro Bernardo Silvério

Brasília - DF
2024

Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Marcus Vinícius Ribeiro Bernardo Silvério

Grupo das Classes Ideais via Redes Complexas: A fórmula de Dirichlet do número de classes e sua divisibilidade para o corpo imaginário $\mathbb{Q}\left(\sqrt{2^{2m}-k^d}\right)$.

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Orientador: Hemar Teixeira Godinho

Brasília - DF

2024

Está página deverá ser substituída por uma folha contendo a ficha catalográfica.

Está página deverá ser substituída por uma folha contendo as assinaturas dos membros da banca, e deve ser colocada após a ficha catalográfica

"A arte de fazer matemática consiste em achar aquele caso especial no qual haja todos os germes de uma generalização."

– David Hilbert

Agradecimentos

Primeiramente à Deus pelo discernimento. E aos meus pais Ivete Ribeiro Bernardo Silvério e Hamilton Bernardo Silvério pelo apoio e confiança que depositaram à mim.

Essa trajetória foi extremamente difícil mas nela tive amigos que contibuíram e me ajudaram a não desistir; dentre eles, cito os que de alguma forma participaram dessa minha caminhada sendo Elvys, Leonardo, Renan, Thallys, Pedro, João, Pablo, Bruna, Iagho, Lais, Franklin, Andres, Eva, Thatyane, Carlos, Wallef, Matheus, Raquel, Henrylla, Saulo, Jadde, Márcio, Isabela, Marina, Paul, Hellen, Milena, Monique, Rayssa, Rebecca, Maycon, Giovana, Tedy, Tamarozzi e, em especial à essas três pessoas que pude aprender, compartilhar ideias e viver momentos incríveis até aqui: Manoel Fernardo dos Reis, Millena Andrade da Silva e Roberto Junior Dias.

À Univesidade de Brasília, agradeço aos Professores Drs. Andrea, Alex, Aline, Ary, José Luis, Luís Henrique, Ma To Fu, Manuela, Wilian pelas disciplinas ministradas e coordenação durante essa etapa do mestrado.

Em especial ao meu orientador por fazer parte desta etapa que muito contribuiu para a minha evolução acadêmica; devido ao período difícil que a humanidade passou, nossas reuniões e contato acadêmico foram interrompidos, mas independente disso, foi imprescindivel a vontade do senhor em deixar minusciosamente um trabalho que possa contribir para estudos futuros. Ao Professor Dr. Hemar Teixeira Godinho, meu muito obrigado.

Agradradecimentos também à empresa ÁTOMO Automação e Comércio de Materiais Elétricos Ltda, a qual atualmente presto serviço na cidade de Baúru-SP, na pessoa de Geraldo de Andrade Costa Filho, Ivonete Ribeiro de Andrade Costa e Geraldo de Andrade Costa Neto.

Meu agradecimento à CAPES e CNPq pelo financiamento de bolsa durante o período em que estive presente em Brasília (dois anos) que me permitiram residir na região do Distrito Federal e estar próximo ao ambiente acadêmico.

Resumo

A presente dissertação tem o objetivo de apresentar o anel dos inteiros algébricos de um corpo númerico quadrático via Teoria de Ideais em paralelo com um tema da área de Geometria dos Números denominado Redes Complexas a fim de construir um grupo abeliano finito conhecido como Grupo das Classes. Em seguida, são discutidos conceitos de Análise (Séries de Dirichlet e Produtos de Euler), a Função Zeta de Riemann, $L-$Funções, Caracteres de Dirichlet e o processo de como deduzir e se evidenciar o objetivo principal da fórmula do número das classes de ideais de Dirichlet. Por fim, é detalhado um artigo de Zhu Minhui e Wang Tingting que envolvem conceitos de Equações Diofantinas e Números de Lehmer para explorar propriedades do número das classes de ideais de $\mathbb{Q}(\sqrt{2^{2m} - k^d})$.

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

Abstract

The present dissertation aims to present the ring of algebraic integers of a square numeric field via Ideals Theory in parallel with a theme in the area of Geometry of Numbers called Complex Lattices in order to set up a finite abelian group known as Class Group. Then are discussed concepts of Analysis (Dirichlet Series and Euler Products), the Riemann Zeta Function, $L-$Functions, Dirichlet's Characters and the process of how to deduce and evidence Dirichlet's formula's main objective of the number of ideal classes. Finally, an article by Zhu Minhui and Wang Tingting [7] which involves concepts of Diofantine Equations and Lehmer's Numbers is detailed to explore the properties of the number of ideal class from $\mathbb{Q}(\sqrt{2^{2m}-k^d})$.

Keywords: Ring of Algebraic Integers of $\mathbb{Q}(\sqrt{2^{2m}-k^d})$; Class Group; Complex Lattices; Class Number Formula.

Lista de Símbolos

Símbolo	Descrição
$\mathbb{N}$	Conjunto dos Números Naturais
$\mathbb{Z}$	Conjunto dos Números Inteiros
$\mathbb{Z}_{>0}$	Conjunto dos Números Inteiros Positivos
$\mathbb{Q}$	Conjunto dos Números Racionais
$\mathbb{C}$	Conjunto dos Números Complexos
$\mathbb{Q}(\sqrt{-n})$	Sub-corpo dos Complexos
$\mathcal{O}_{-n}$	Anel dos Inteiros Algébricos do corpo $\mathbb{Q}(\sqrt{-n})$
$\mathbb{U}_{-n}$	Conjunto das unidades de $\mathcal{O}_{-n}$
$\mathbb{Z}[X, Y]$	Anel de Polinômio de duas variáveis com coeficientes inteiros
$SL_2(\mathbb{Z})$	Conjunto de Matrizes 2×2 sobre $\mathbb{Z}$ com determinante 1
$\sum$	Somatório
$\prod$	Produtório
$\mathcal{N}$	Função Norma
$\mathcal{T}r$	Função Traço
$irr_{\mathbb{Q}}(\alpha)$	Polinômio irredutível de α sobre $\mathbb{Q}$
$\mathbb{X}^{\times}$	Conjunto $\mathbb{X}$ que não possui o elemento nulo
$\#\mathbb{X}$	Cardinalidade de um conjunto finito $\mathbb{X}$
$\varnothing$	Conjunto Vazio
α	Alfa
β	Beta
ζ	Zeta
η	Eta
γ	Gama
χ	Qui
ϵ	Épsilon
μ	Mi
ν	Ni
ξ	Quissi
δ	Delta
Δ	Delta maiúsculo
Λ	Lâmbda maiúsculo
$\left(\frac{-n}{m}\right)$	Símbolo de Jacobi

$\left(\frac{-n}{p}\right)$	Símbolo de Legendre
$\chi_{-n}(m)$	Caracter de Dirichlet módulo m
$\mathcal{B}$	Base integral
$\mathfrak{D}$	Domínio Fundamental
β_{-n}	Elemento da base integral de $\mathbb{Q}(\sqrt{-n})$ sobre $\mathbb{Q}$
Δ_{-n}	Discriminante do corpo $\mathbb{Q}(\sqrt{-n})$
mdc	Máximo Divisor Comum
$\mathcal{I}$, $\mathcal{J}$, $\mathcal{K}$	Ideais do anel dos inteiros algébricos
$\wp$	Ideal primo do anel dos inteiros algébricos
im	Parte imaginária de um número
re	Parte real de um número
$\zeta(s)$	Função Zeta de Riemann
$\zeta_{-n}(s)$	Função Zeta Dedekind
$\mathcal{C}l(-n)$	Grupo das Classes
$\mathcal{C}_{\mathcal{I}}$, $\mathcal{C}_{\mathcal{J}}$, $\mathcal{C}_{\mathcal{K}}$	Classes de ideais do grupo das classes
$h(-n)$	Número de Classes de Ideais

Sumário

Lista de Figuras

Introdução

O estudo da Teoria de Anéis surge a partir dos estudos da teoria dos inteiros algébricos e anéis de polinimômios introduzido pelo alemão Jilius Wilhelm Richard Dedekind (1831-1916) em seu conceito base, e por volta de 1920, através da matemática alemã Amalie Emmy Noether, foi publicado no trabalho *Ideal Theory in Rings* os fundamentos axiomáticos para essa teoria. Antes, em seu contexto histórico, Johann Peter Gustav Lejeune Dirichlet (1805-1859) já contibuía com a análise matemática nos conceitos de funções, aplicando funções analíticas ao cálculo de problemas aritméticos e estabelecendo critérios de convergência para as séries.

Nos capítulos 1 e 2 da presente dissertação, nos fundamentamos nas notas de Tom Weston [19] a qual o mesmo, em 2004, escreveu "*Lectures On the Dirichlet Class Number Formula for Imaginary Quadratic Fields*" baseado em notas de aula realizadas no "*Ross Program*" de verão nos E.U.A.

No primeiro capítulo é apresentado duas ideias principais: Propriedades dos ideais do anel dos inteiros algébricos do corpo quadrático imaginário e Redes complexas. O tópico que envolve a teoria de anéis e corpos traz maneiras de se identificar o anel $\mathcal{O}_{-n}$ por meio do inteiro positivo livre de quadrados n que caracteriza o corpo quadrático $\mathbb{Q}(\sqrt{-n})$ e, como estamos analisando tal anel, os ideais produzidos junto à soma, multiplicação, normas e divisibilidade (Ideais Fracionários), possuem propriedades por serem domínios Dedeking que proporcionam uma fatoração única em ideais primos de $\mathcal{O}_{-n}$. Na segunda etapa deste primeiro capítulo, estudamos Redes Complexas que basicamente são subconjuntos de $\mathbb{C}$, exibindo de maneira suscinta propriedades de equivalências e, um elemento em específico chamado j–invariante concebido por um algorítmo descrito em [19] onde o mesmo se encontra em uma região do plano complexo conhecido pelo Domínio Fundamental e todos os conceitos se vinculam ao conceito de MC (multiplicação complexa), assim redes equivalentes são caracterizadas e, que ao final do capítulo, o vínculo entre redes e ideais de $\mathcal{O}_{-n}$ por meio da similiradade formando um conjunto finito conhecido como o grupo das Classes de Ideais.

No segundo capítulo apresentamos métodos analíticos que buscam concluir que a função ζ–Dedekind do corpo $\mathbb{Q}(\sqrt{-n})$ possui um pólo simples no ponto igual à 1 com resíduo $\frac{h\pi}{Aw}$. Iniciamos com conceitos da Análise Complexa tais como a convergência de séries de Dirichlet para números reais, e a sua relação com a função $\zeta(s)$

de Riemann quando $s > 1$ junto à fórmula do produto de Euler. Feito esses apontamentos, entramos na área da Teoria dos Números mostrando algumas propriedades básicas do símbolo de Jacobi/Legendre relacionando com o caracter quadrático de Dirichlet; diante à essas explicações, o real motivo que traz o vínculo dessas duas definições é o discriminante Δ_{-n} do corpo $\mathbb{Q}(\sqrt{-n})$, que fora introduzido no primeiro capitulo, atrelado à funções denominadas L–funções de Dirichlet.

Por fim, no terceiro capitulo é exposto um artigo, com autoria de Zhu Minhui e Wang Tingting [7] intitulado "*The divisibility of the class number of the imaginary quadratic field* $\mathbb{Q}(\sqrt{2^{2m} - k^d})$" onde m, $d \in \mathbb{Z}_{>0}$, k é um inteiro ímpar maior que 1 e $2^{2m} < k^d$, que propõe caracterizar valores, por meio do número da classe de formas primitivas binárias quadráticas com discriminante Δ_{-d} embasada na L–função e a ζ–Dedekind, mediante aos parâmetros tal qual determinam o corpo e determinar critérios de divisiblidade de $h(2^{2m} - k^d)$. São detalhados o conjunto solução de Equações Diofantinas do tipo $X^2 + DY^2 = k^Z$ onde D, $k > 1$ inteiros com mdc$(2D, k) = 1$ e X, Y, $Z \in \mathbb{N}$ com mdc$(X, Y) = 1$ e sequências definidas como "números de Lehmer" a partir dos pares de Lehmer (μ, ν) onde $(\mu + \nu)^2$ e $\mu \cdot \nu$ coprimos e μ/ν não é uma raiz da unidade tal que μ, ν são inteiros algébricos.

O objetivo principal da dissertação é mostrar um dos métodos no meio acadêmico para se encontrar propriedades de divisibilidade pontuais para o número de classes ideais $h(-n)$ de um corpo quadrático imaginário. Os resultados no terceiro capítulo, são fundamentados no artigo de Z. Minhui e W. Tingting [7] que se utiliza dos artigos [5], [12], [17] e [20] como referências e, para o primeiro capítulo toda teoria de ideais de $\mathcal{O}_{-n}$ e redes complexas se baseiam em [6], [4], [3], [15], [8], [9], [14], [10], [16], [18] e [19], e como complemento fundamental para o estudo final, utilizamos para compreensão do segundo capítulo, as referências [1], [3], [11], [2] , [9], [13], [16], [19] e [21].

Capítulo 1

Corpos Numéricos e o Anel dos Inteiros Algébricos

A base para iniciarmos o estudo das Seções 1.1, 1.2 e 1.3 são encontradas em [14, Cap. 1-3], [9, Cap. 1-2 e 4], [8, Cap. 1-3], [10, Cap. 3-5 e 7], [6, Cap. 12] e [15, Cap. 1-2] onde é apresentada uma exposição mais detalhada da teoria de anéis, anéis Noetherianos, domínios Dedekind, $\mathbb{Z}-$módulos, ideais fracionários e corpos.

1.1 Corpos Quadráticos Imaginários

Definição 1.1.1. *Seja $n \in \mathbb{Z}$, um **corpo quadrático** é um subcorpo do corpo dos números complexos da forma $\mathbb{Q}(\sqrt{n}) = \{x + y\sqrt{n};\ x, y \in \mathbb{Q}\}$ e $\mathbb{Q} \subset \mathbb{Q}(\sqrt{n})$, em outras palavras, é uma extensão de dimensão 2 vista como um espaço vetorial sobre o corpo dos racionais $\mathbb{Q}$.*

Teorema 1.1.1. *Seja $\mathcal{F}$ um corpo quadrático, então existe um único inteiro livre de quadrados n tal que $\mathcal{F} = \mathbb{Q}(\sqrt{n})$.*

Demonstração. Considere $\mathcal{F} = \mathbb{Q}(\alpha)$ e suponha que α seja raiz de um polinômio mônico irredutível $f(s) \in \mathbb{Q}[s]$. Assim temos:

$$\alpha = \tfrac{-a+\sqrt{\Delta}}{2} \text{ ou } \alpha = \tfrac{-b-\sqrt{\Delta}}{2}$$

com $\Delta = b^2 - 4c \in \mathbb{Q}$. Logo $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta})$.

Seja

$$\Delta = \frac{p}{q} = \frac{pq}{q^2}$$

então

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{pq}).$$

Por fim, escreva $pq = k^2 n$, com n sendo um inteiro livre de quadrados. Portanto

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{n}).$$

□

Quando $n < 0$, dizemos que $\mathbb{Q}(\sqrt{n})$ é um ***corpo quadrático imáginário***; e partir daqui, iremos denotar este corpo como sendo $\mathbb{Q}(\sqrt{-n})$.

1.2 Anel dos Inteiros Algébricos

Fixado n um inteiro positivo livre de quadrados, é intuitivo pensar que o anel dos inteiros algébricos do corpo $\mathbb{Q}(\sqrt{-n})$ seja o subanel $\mathbb{Z}[\sqrt{-n}] = \{a + b\sqrt{-n};\, a, b \in \mathbb{Z}\}$, mas não é tão simples assim. Para detalharmos tal anel, é necessário de início, entendermos o polinômino irredutível (de grau 2) a partir da(s) sua(s) raíz(es) que estejam em $\mathbb{Q}(\sqrt{-n})$. A partir desse ponto, denotaremos o polinômio irredutível de α por $irr_{\mathbb{Q}}(\alpha)$. Assim para $\alpha, \beta \in \mathbb{Q}(\sqrt{-n})$ defina essas três funções:

Definição 1.2.1. *A função* ***conjugado*** *de $\mathbb{Q}(\sqrt{-n})$ é um homomorfismo de anéis:*

$$\begin{array}{ccc} {}^{-} : \mathbb{Q}(\sqrt{-n}) & \longrightarrow & \mathbb{Q}(\sqrt{-n}) \\ \alpha = x + y\sqrt{-n} & \longmapsto & \overline{\alpha} = x - y\sqrt{-n} \end{array}$$

onde

$$\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$$
$$\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}.$$

Definição 1.2.2. *A função* ***traço*** *de $\mathbb{Q}(\sqrt{-n})$ é um homomorfismo aditivo tal que:*

$$\begin{array}{ccc} \mathcal{T}r : \mathbb{Q}(\sqrt{-n}) & \longrightarrow & \mathbb{Q} \\ \alpha & \longmapsto & \mathcal{T}r(\alpha) = \alpha + \overline{\alpha} \end{array}$$

o que nada mais é que:

$$\mathcal{T}r(x + y\sqrt{-n}) = (x + y\sqrt{-n}) + (x - y\sqrt{-n}) = 2 \cdot x.$$

Definição 1.2.3. *A função* ***norma*** *de $\mathbb{Q}(\sqrt{-n})$ é um homomorfismo multiplicativo tal que:*

$$\begin{array}{ccc} \mathcal{N} : \mathbb{Q}(\sqrt{-n})^{\times} & \longrightarrow & \mathbb{Q}^{\times} \\ \alpha & \longmapsto & \mathcal{N}(\alpha) = \alpha \cdot \overline{\alpha} \end{array}$$

o que nada mais é que:

$$\mathcal{N}(x + y\sqrt{-n}) = (x + y\sqrt{-n}) \cdot (x - y\sqrt{-n}) = x^2 + n \cdot y^2.$$

Observação 1.2.1.

- Como $\mathcal{T}r(\alpha), \mathcal{N}(\alpha) \in \mathbb{Q}$, segue que

$$\overline{\mathcal{T}r(\alpha)}, \overline{\mathcal{N}(\alpha)} \in \mathbb{Q}.$$

- Seja $\alpha \in \mathbb{Q}(\sqrt{-n})$ e escreva $\alpha = x + y\sqrt{-n}$. Observe que:

$$\alpha^2 - \mathcal{T}r(\alpha) \cdot \alpha + \mathcal{N}(\alpha) = 0,$$

ou seja,

$$irr_{\mathbb{Q}}(\alpha) = s^2 - \mathcal{T}r(\alpha) \cdot s + \mathcal{N}(\alpha) \in \mathbb{Q}(s).$$

Definição 1.2.4. *Seja $\alpha \in \mathbb{Q}(\sqrt{-n})$. Dizemos que α é um* ***inteiro algébrico*** *se $irr_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[s]$. Segue da observação acima que α é inteiro algébrico se, e somente se,*

$$\mathcal{T}r(\alpha), \mathcal{N}(\alpha) \in \mathbb{Z}.$$

Vamos denotar por $\mathcal{O}_{-n}$ o conjunto dos inteiros algébricos de $\mathbb{Q}(\sqrt{-n})$, e o conjunto $\mathcal{O}_{-n}$ forma um anel.

O próximo resultado apresenta uma descrição detalhada desse anel.

Teorema 1.2.1. *O anel dos inteiros algébricos $\mathcal{O}_{-n}$ é descrito como*

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

Demonstração. Primeiramente, observe que

$$irr_{\mathbb{Q}}(\sqrt{-n}) = s^2 + n \in \mathbb{Z}[s]$$

e

$$irr_{\mathbb{Q}}\left(\frac{1+\sqrt{-n}}{2}\right) = s^2 - s + \frac{1+n}{4} \in \mathbb{Z}[s].$$

Ou seja,

$$\mathbb{Z}[\sqrt{-n}] \subseteq \mathcal{O}_{-n}$$

e

$$\mathbb{Z}\left[\frac{1+\sqrt{-n}}{2}\right] \subseteq \mathcal{O}_{-n} \text{ caso } n \equiv 3 \pmod 4.$$

Agora tome $\alpha = a + b\sqrt{-n} \in \mathcal{O}_{-n}$, logo

$$\mathcal{T}r(\alpha) = 2a \in \mathbb{Z}$$

e

$$\mathcal{N}(\alpha) = a^2 + nb^2 \in \mathbb{Z}.$$

Assim,

$$4a^2 + 4nb^2 \in \mathbb{Z} \implies n(2b)^2 \in \mathbb{Z}.$$

Como n é livre de quadrados, necessariamente $2b \in \mathbb{Z}$. Escreva $2a = u$ e $2b = v$, desse modo

$$a^2 + nb^2 \in \mathbb{Z} \implies u^2 + nv^2 \equiv 0 \pmod 4.$$

Se $n \equiv 1,\ 2 \pmod 4$ então

$$0 \equiv u^2 + nv^2 \equiv u^2 + v^2,\ u^2 + 2v^2 \pmod 4$$

$$\implies$$

$$u,\ v \text{ são pares, pois } s^2 \equiv 0,\ 1 \pmod 4$$

portanto $a,\ b \in \mathbb{Z}$ e

$$\mathcal{O}_{-n} = \mathbb{Z}[\sqrt{-n}].$$

Se $n \equiv 3 \pmod 4$ então

$$0 \equiv u^2 + nv^2 \equiv u^2 + 3v^2 \pmod 4 \implies u \equiv v \pmod 2,$$

ou seja, u e v possuem a mesma paridade.

Escreva

$$\alpha = \frac{u}{2} + \frac{v}{2}\sqrt{-n} = \frac{u-v}{2} + v\frac{1+\sqrt{-n}}{2},$$

como $u - v \equiv 0 \pmod 2$ temos que

$$\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{-n}}{2}\right] \implies \mathcal{O}_{-n} = \mathbb{Z}\left[\frac{1+\sqrt{-n}}{2}\right].$$

□

Observação 1.2.2.

É fácil ver que $\{1,\ \sqrt{-n}\}$ e $\{1,\ \frac{1+\sqrt{-n}}{2}\}$ são bases de $\mathbb{Q}(\sqrt{-n})$ sobre $\mathbb{Q}$; de acordo com o teorema acima, também são bases de $\mathcal{O}_{-n}$ dependendo do valor de n módulo 4. Nesse sentido, denominamos essas bases de ***bases integrais*** de $\mathbb{Q}(\sqrt{-n})$.

Definição 1.2.5. *Temos dois automorfismos em* $\mathbb{Q}(\sqrt{-n})$ *dados por*

$$\begin{array}{rccc} \delta_1: & \mathbb{Q}(\sqrt{-n}) & \longrightarrow & \mathbb{Q}(\sqrt{-n}) \\ & \alpha & \longmapsto & \alpha \end{array} \quad e \quad \begin{array}{rccc} \delta_2: & \mathbb{Q}(\sqrt{-n}) & \longrightarrow & \mathbb{Q}(\sqrt{-n}) \\ & \alpha & \longmapsto & \overline{\alpha} \end{array}.$$

Vamos denotar por $\mathcal{B}_{-n}$ *a base*

$$\mathcal{B}_{-n} = \begin{cases} \{1, \sqrt{-n}\} & \text{se } n \equiv 1, 2 \pmod 4; \\ \\ \{1, \frac{1+\sqrt{-n}}{2}\} & \text{se } n \equiv 3 \pmod 4; \end{cases}$$

portanto $\mathcal{B}_{-n}$ *é base integral de* $\mathbb{Q}(\sqrt{-n})$.

Escrevendo $\mathcal{B}_{-n} = \{1, \beta_{-n}\}$, *então defina* Δ_{-n} *como o* ***discriminante*** *de* $\mathbb{Q}(\sqrt{-n})$ *onde:*

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

Teorema 1.2.2. *O discriminante de* $\mathbb{Q}(\sqrt{-n})$ *é dado por:*

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

Demonstração. Como visto acima

$$\Delta_{-n} = \left|\begin{pmatrix} 1 & 1 \\ \sqrt{-n} & -\sqrt{-n} \end{pmatrix}\right|^2 = \left(-2\sqrt{-n}\right)^2 = -4n \text{ se } n \equiv 1, 2 \pmod 4$$

e

$$\Delta_{-n} = \left|\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{-n}}{2} & \frac{1-\sqrt{-n}}{2} \end{pmatrix}\right|^2 = \left(-\sqrt{-n}\right)^2 = -n \text{ se } n \equiv 3 \pmod 4.$$

□

Definição 1.2.6. *Sejam* $x_1, x_2 \in \mathcal{O}_{-n}$*:*

- $x_1 \mid x_2$ *(lê-se* x_1 ***divide*** x_2*) se existe* $x_3 \in \mathcal{O}_{-n}$ *tal que* $x_2 = x_1 \cdot x_3$*;*
- *se* $x_1 \mid 1$ *então* x_1 *é chamado de* ***unidade****;*
- x_1 *é chamado* ***irredutivel*** *se* x_1 *não é uma unidade e para* $x_1 = x_2 \cdot x_3$*, ou* x_2 *ou* x_3 *é uma unidade.*

Propriedade 1.2.1. *Para x_1, $x_2 \in \mathcal{O}_{-n}$ temos:*

(i) *Se $x_1 \mid x_2$ em $\mathcal{O}_{-n}$ então $\mathcal{N}(x_1) \mid \mathcal{N}(x_2)$ em $\mathbb{Z}$.*

(ii) *Seja $x_1 \in \mathcal{O}_{-n}$ uma unidade, se e só se $\mathcal{N}(x_1) = 1$.*

(iii) *Se $\mathcal{N}(x_1)$ é primo em $\mathbb{Z}$ então x_1 é irredutível em $\mathcal{O}_{-n}$.*

Demonstração. *(i)* Temos por hipótese $x_2 = x_1 \cdot x_3$, assim $\mathcal{N}(x_2) = \mathcal{N}(x_1) \cdot \mathcal{N}(x_3)$, portanto $\mathcal{N}(x_1) \mid \mathcal{N}(x_2)$.

(ii) Por definição de unidade, $x_1 \mid 1$, e usando o resultado do item (i), $\mathcal{N}(x_1) \mid 1$ em $\mathbb{Z}$, logo $\mathcal{N}(x_1) = \pm 1$. Como a norma

$$\mathcal{N}(a + b\sqrt{-n}) = a^2 + nb^2 \in \mathbb{N} \cup \{0\},$$

segue que $\mathcal{N}(x_1) = 1$.

Reciprocamente, temos que $\mathcal{N}(x_1) = 1$ implica em $x_1 \cdot \overline{x_1} = 1$, logo $x_1 \mid 1$.

(iii) Utilizando os dois itens anteriores; toda fatoração de x_1 a qual não possui elemento unitário implica numa fatoração de $\mathcal{N}(x_1)$ sem elemento unitário, assim, se $\mathcal{N}(x_1)$ é um elemento primo então x_1 é irredutível em $\mathcal{O}_{-n}$.

□

Teorema 1.2.3. *O conjunto $\mathbb{U}_{-n}$ das unidades de $\mathcal{O}_{-n}$ é dado por:*

$$\mathbb{U}_{-n} = \begin{cases} \{\pm 1, \pm i\} & \text{se } n = 1; \\ \{\pm 1, \pm \xi, \pm \xi^2\} & \text{se } n = 3 \text{ onde } \xi = \frac{1+\sqrt{-3}}{2}; \\ \{\pm 1\} & \text{caso contrário.} \end{cases}$$

Demonstração. Dado $\alpha = a + b\sqrt{-n}$ uma unidade de $\mathcal{O}_{-n}$ temos

$$\mathcal{N}(\alpha) = a^2 + nb^2 = 1.$$

Primeiramente, para $n \equiv 1, 2 \pmod 4$ e $n \neq 1$, pelas condições $a, b \in \mathbb{Z}$ e $a^2 + nb^2 = 1$, implica que $a = \pm 1$ e $b = 0$, logo as unidades são $\mathbb{U}_{-n} = \{\pm 1\}$.

Quando $n = 1$, onde $\mathcal{O}_{-n} = \mathbb{Z} + \sqrt{-1} \cdot \mathbb{Z}$ logo $a^2 + b^2 = 1$, assim as possibilidades, para o par $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$, o que se traduz nas unidades de $\mathbb{Z}[\sqrt{-1}]$, ou seja, $\mathbb{U}_{-1} = \{\pm 1, \pm i\}$.

Agora, para $n \equiv 3 \pmod 4$ e $n \neq 3$ as condições dão que $2a, 2b \in \mathbb{Z}$, assim $(2a)^2 + n(2b)^2 = 4(a^2 + nb^2) = 4$, logo só pode ocorrer com $a = \pm 1$ e $b = 0$, nesse caso $\mathbb{U}_{-n} = \{\pm 1\}$.

Para o caso $n = 3$, temos

$$a^2 + 3b^2 = 4 \implies (a,\, b) \in \{(\pm 2,\, 0), (\pm 1,\, \pm 1)\}.$$

Mais ainda, $\mathcal{O}_{-3} = 1 \cdot \mathbb{Z} + \left(\frac{1+\sqrt{-3}}{2}\right) \cdot \mathbb{Z}$ e como existem seis possibilidades para o par $(a,\, b)$, temos que:

$$\mathbb{U}_{-3} = \left\{ \pm 1,\, \pm \left(\frac{1+\sqrt{-3}}{2}\right),\, \pm \left(\frac{1+\sqrt{-3}}{2}\right)^2 \right\}.$$

□

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

Antes de prosseguir nesta seção, é necessário entender que o anel $\mathcal{O}_{-n}$ pode ser visto como um ***domínio de Dedekind***, em outras palavras, um domínio que satisfaz as seguintes propriedades:

- $\mathcal{O}_{-n}$ é noetheriano;
- todo ideal primo não-nulo de $\mathcal{O}_{-n}$ é maximal;
- $\mathcal{O}_{-n}$ é integralmente fechado em $\mathbb{Q}(\sqrt{-n})$.

Para mais detalhes ver [15, Cap. 1] e [9, Cap. 1 e 2]. Sendo assim, iniciamos com:

Definição 1.3.1. *Seja $I \subset \mathcal{O}_{-n}$, um conjunto não-vazio. Dizemos que I é um ideal de $\mathcal{O}_{-n}$ se:*

(i) $\alpha,\, \beta \in I \implies \alpha \pm \beta \in I$;

(ii) $\lambda \in \mathcal{O}_{-n}$ e $\beta \in I \implies \lambda \cdot \beta \in I$.

Definição 1.3.2. *Dados $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_{-n}$, o conjunto*

$$I = \{a_1 \cdot \alpha_1 + \ldots + a_r \cdot \alpha_r;\, \alpha_1, \ldots, \alpha_r \in \mathcal{O}_{-n}\}$$

*é um ideal do anel dos inteiros algébricos $\mathcal{O}_{-n}$, chamado de ideal **gerado** por $\alpha_1, \ldots, \alpha_r$ e denotado por $I = (\alpha_1, \ldots, \alpha_r)$. No caso de $I = (\alpha)$ onde $\alpha \in \mathcal{O}_{-n}$, dizemos que I é um ideal **principal**.*

Lema 1.3.1. *Todo ideal de $\mathcal{O}_{-n}$ é gerado por no máximo dois elementos.*

Demonstração. Seja $\{1,\, \beta_{-n}\}$ uma base integral de $\mathcal{O}_{-n}$ e I um ideal deste anel. Tome $\alpha \neq 0$ tal que $\alpha = a + b\beta_{-n} \in I$, logo:

$$\alpha^2 - \mathcal{T}r(\alpha)\cdot\alpha + \mathcal{N}(\alpha) = 0 \text{ (raiz de } irr_{\mathbb{Q}}(\alpha))$$

e em particular,

$$\mathcal{N}(\alpha) = \mathcal{T}r(\alpha)\cdot\alpha - \alpha^2 \in I \cap \mathbb{Z}.$$

Portanto, $I_0 = \mathcal{I} \cap \mathbb{Z}$ é ideal não-nulo de $\mathbb{Z}$, assim $I_0 = (m)$ para algum $m \in \mathbb{Z}$ (todo ideal de $\mathbb{Z}$ é principal). Agora defina

$$I_1 = \{r \in \mathbb{Z};\ s + r\beta_{-n} \in I,\ \text{para algum } s \in \mathbb{Z}\}.$$

Como

$$\alpha = a + b\beta_{-n} \in I \implies b \in I_1,$$

e por notar que I_1 também é um ideal de $\mathbb{Z}$, logo $I_1 = (t)$, e por definição de I_1, existe $u_0 \in \mathbb{Z}$ tal que $u_0 + t\beta_{-n} \in I$. Agora, temos que

$$\alpha = a + b\beta_{-n} \implies b \in I_1 \implies b = l\cdot t,$$

assim

$$\alpha - l(u_0 + t\beta_{-n}) = (a + b\beta_{-n}) - l(u_0 + t\beta_{-n}) = a - lu_0$$
$$\Longrightarrow$$
$$a - lu_0 \in I \cap \mathbb{Z} = I_0 \implies a - lu_0 = \lambda m.$$

Portanto,

$$\alpha = l(u_0 + t\beta_{-n}) + \lambda m$$
$$\Longrightarrow$$
$$I = m\cdot\mathbb{Z} + (u_0 + t\beta_{-n})\cdot\mathbb{Z} \subseteq m\cdot\mathcal{O}_{-n} + (u_0 + t\beta_{-n})\cdot\mathcal{O}_{-n}.$$

□

Exemplo 1.3.1.

O ideal $(29,\ 13 - \sqrt{-5}) \subset \mathcal{O}_{-5}$ é principal gerado por $3 + 2\sqrt{-5}$.

Para verificar isso, vale mostrar que acontecem:

- $(3 + 2\sqrt{-5}) \subseteq (29,\ 13 - \sqrt{-5})$;
- $(29,\ 13 - \sqrt{-5}) \subseteq (3 + 2\sqrt{-5})$.

Para o primeiro caso é necessário obter $3+2\sqrt{-5}$ como uma combinação linear dos fatores 29 e $13 - \sqrt{-5}$, a saber (tratar como elementos e não ideais por meio dos parênteses):

$$3 + 2\sqrt{-5} = 29\cdot 1 + (13 - \sqrt{-5})\cdot(-2).$$

No segundo caso, note que, por definição, o ideal $(3 + 2\sqrt{-5})$ é o conjunto formado de múltiplos do elemento $3 + 2\sqrt{-5}$, logo este elemento divide ambos 29 e $13 - 2\sqrt{-5}$, de fato:

$$29 = (3 + 2\sqrt{-5}) \cdot (3 - 2\sqrt{-5}),$$

e

$$13 - 2\sqrt{-5} = (3 + 2\sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

Definição 1.3.3. *Sejam I, J ideais de $\mathcal{O}_{-n}$, e escreva $I = (x_1, y_1)$, $J = (x_2, y_2)$. Defina:*

(i) $I + J = (x_1, x_2, y_1, y_2)$;

(ii) $I \cdot J = (x_1 \cdot y_1, x_1 \cdot y_2, x_2 \cdot y_1, x_2 \cdot y_2)$.

Veja que $I + J$ e $I \cdot J$ são também ideais de $\mathcal{O}_{-n}$.

Observação 1.3.1.

Segue diretamente da definição acima que $I \cdot J \subseteq I \cap J$.

Exemplo 1.3.2.

Para o corpo $\mathbb{Q}(\sqrt{-5})$, temos que o seu anel de inteiros algébricos é $\mathbb{Z}[\sqrt{-5}]$, a qual não é um domínio de fatoração única. Tomando 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, que são elementos irredutíveis e não associados, temos:

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6.$$

Note que através de ideais primos (detalhamos adiante) em $\mathbb{Z}[\sqrt{-5}]$ podemos "consertar" a fatoração única, a saber:

$$I = (2, 1 + \sqrt{-5}),$$

$$J = (3, 1 + \sqrt{-5}),$$

$$K = (3, 1\sqrt{-5}).$$

Assim,

$$I = (2, 1 + \sqrt{-5}) = (2, 2 - [1 - \sqrt{-5}], 2 - [1 + \sqrt{-5}]) = (2, 1 - \sqrt{-5})$$

então:

$$\begin{aligned} I \cdot J &= (2, 1 + \sqrt{-5}) \cdot (3, 1 + \sqrt{-5}) \\ &= (6, 2 \cdot [1 + \sqrt{-5}], 3 \cdot [1 + \sqrt{-5}], [1 + \sqrt{-5}]^2) \\ &= (1 + \sqrt{-5}) \cdot (1 + \sqrt{-5}, 2, 3, 1 + \sqrt{-5}) \\ &= (1 + \sqrt{-5}) \cdot (1) \\ &= (1 + \sqrt{-5}); \end{aligned}$$

$$\begin{aligned} J \cdot K &= (3,\, 1+\sqrt{-5}) \cdot (3,\, 1-\sqrt{-5}) \\ &= (9,\, 3\cdot[1+\sqrt{-5}],\, 3\cdot[1-\sqrt{-5}],\, 6) \\ &= (3) \cdot (3,\, 1+\sqrt{-5},\, 1-\sqrt{-5},\, 2) \\ &= (3) \cdot (1) \\ &= (3); \end{aligned}$$

$$\begin{aligned} I \cdot K &= (2,\, 1+\sqrt{-5}) \cdot (3,\, 1-\sqrt{-5}) \\ &= (2,\, 1-\sqrt{-5}) \cdot (3,\, 1-\sqrt{-5}) \\ &= (6,\, 2\cdot[1-\sqrt{-5}],\, 3\cdot[1-\sqrt{-5}],\, [1-\sqrt{-5}]^2) \\ &= (1-\sqrt{-5}) \cdot (1+\sqrt{-5},\, 2,\, 3,\, 1-\sqrt{-5}) \\ &= (1-\sqrt{-5}) \cdot (1) \\ &= (1-\sqrt{-5}); \end{aligned}$$

$$\begin{aligned} I \cdot I &= (2,\, 1+\sqrt{-5})^2 \\ &= (2,\, 1+\sqrt{-5}) \cdot (2,\, 1-\sqrt{-5}) \\ &= (4,\, 2\cdot[1+\sqrt{-5}],\, 2\cdot[1-\sqrt{-5}],\, 6) \\ &= (2) \cdot (2,\, 1+\sqrt{-5},\, 1-\sqrt{-5},\, 3) \\ &= (2) \cdot (1) \\ &= (2) \end{aligned}$$

logo,

$$(6) = (2) \cdot (3) = (1+\sqrt{-5}) \cdot (1-\sqrt{-5}) = I^2 \cdot J \cdot K.$$

Definição 1.3.4. *Seja $I \subset \mathcal{O}_{-n}$, defina o ideal*

$$\overline{I} = \{\bar{\alpha}\,;\alpha \in I\}$$

onde $\overline{\alpha}$ é o conjugado de α.

Definição 1.3.5. *Seja I um ideal de $\mathcal{O}_{-n}$, defina a* ***norma do ideal*** *I como*

$$\mathcal{N}(I) = |^{\mathcal{O}_{-n}}/_{I}|\,.$$

Observação 1.3.2.

Já vimos que, no Teorema 1.2.1 e no Lema 1.3.1 acima, $\mathcal{O}_{-n} = \mathbb{Z} + \beta_{-n}\mathbb{Z}$ e $\mathcal{I} = m\mathbb{Z} + (u_0 + t\beta_{-n})\mathbb{Z}$. Segue da teoria de anéis que

$$\mathcal{N}(I) = |^{\mathcal{O}_{-n}}/_{I}| = |det(a_{ij})|$$

onde

$$\begin{cases} m &= a_{11}\cdot 1 + a_{12}\cdot\beta_{-n}; \\ u_0 + t\beta_{-n} &= a_{21}\cdot 1 + a_{22}\cdot\beta_{-n}. \end{cases}$$

Como

$$det(a_{ij}) = \begin{vmatrix} m & 0 \\ u_0 & t \end{vmatrix} = mt \implies \mathcal{N}(I) = |mt|.$$

Segue da definição que se $I = (\alpha)$, um ideal principal, então $\mathcal{N}(I) = \mathcal{N}(\alpha) \in \mathbb{N}$.

Uma propriedade fundamental de normas de um ideal em $\mathcal{O}_{-n}$, porém extremamente técnica e que iremos omitir sua demonstração, é apresentada a seguir:

Lema 1.3.2. *Sejam I, J ideais de $\mathcal{O}_{-n}$. Então*

$$\mathcal{N}(I \cdot J) = \mathcal{N}(I) \cdot \mathcal{N}(J).$$

Demonstração. Ver [4, Teo 9.3.2, pg 229].

□

Lema 1.3.3. *Existe $d \in \mathbb{N}$ tal que*

$$I \cdot \overline{I} = (d),$$

com $d = \mathcal{N}(x)$ para algum $x \in I$.

Demonstração. Escreva $I = (\alpha,\, \beta)$, logo

$$I \cdot \overline{I} = (\alpha\overline{\alpha},\, \beta\overline{\beta},\, \alpha\overline{\beta},\, \overline{\alpha}\beta).$$

Como $\alpha \cdot \overline{\alpha} = \mathcal{N}(\alpha) \in \mathbb{Z}$, $\beta \cdot \overline{\beta} = \mathcal{N}(\beta) \in \mathbb{Z}$ e $\overline{\alpha\overline{\beta} + \overline{\alpha}\beta} = \alpha\overline{\beta} + \overline{\alpha}\beta$, segue que

$$\alpha\overline{\beta} + \overline{\alpha}\beta \in \mathbb{Q} \cap \mathcal{O}_{-n} = \mathbb{Z}.$$

Seja então $d = \text{mdc}(\alpha\overline{\alpha},\, \beta\overline{\beta},\, \alpha\overline{\beta} + \overline{\alpha}\beta) \in \mathbb{N}$, assim:

$$d = r \cdot \alpha\overline{\alpha} + s \cdot \beta\overline{\beta} + t(\alpha\overline{\beta} + \overline{\alpha}\beta) \quad \text{com} \quad r,\, s,\, t \in \mathbb{Z};$$

deste modo, quer dizer que $d \in I \cdot \overline{I}$, portanto

$$(d) \subseteq I \cdot \overline{I}.$$

Por outro lado, temos que

$$\alpha\overline{\alpha} = d \cdot u, \quad \beta\overline{\beta} = d \cdot v, \quad \alpha\overline{\beta} + \overline{\alpha}\beta = d \cdot w$$

com u, v, $w \in \mathbb{Z}$. Observe que ambos:

$$\frac{\overline{\alpha}\beta}{d} \quad \text{e} \quad \frac{\alpha\overline{\beta}}{d}$$

são raízes do polinômio $f(s) = s^2 - ws + uv \in \mathbb{Z}[s]$, o que implica em:

$$\frac{\overline{\alpha}\beta}{d} = \delta \in \mathcal{O}_{-n} \quad \text{e} \quad \frac{\alpha\overline{\beta}}{d} = \lambda \in \mathcal{O}_{-n}$$
$$\Longrightarrow$$
$$\overline{\alpha}\beta = \delta d \in (d) \quad \text{e} \quad \alpha\overline{\beta} = \lambda d \in (d)$$
$$\Longrightarrow$$
$$I \cdot \overline{I} \subseteq (d).$$

□

Mostramos agora uma importante particularidade dos ideais do anel dos inteiros algébricos em que, para I um ideal qualquer de $\mathcal{O}_{-n}$, dizemos que $\mathcal{I}$ é um ***ideal fracionário*** de $\mathcal{O}_{-n}$ se existe um número algébrico não-nulo $\gamma \in \mathcal{O}_{-n}$ tal que

$$\mathcal{I} = \frac{1}{\gamma} I \subset \mathcal{O}_{-n};$$

ou seja, significa que os elementos de um ideal fracionário tem o elemento γ como um denominador comum. Por definição, $\mathcal{O}_{-n}$ é finitamente gerado, então para $\gamma \in {\mathcal{O}_{-n}}^{\times}$ e $I = (\alpha_1, \alpha_2)$, temos que:

$$\mathcal{I} = \frac{1}{\gamma}(\alpha_1, \alpha_2) = \left(\frac{\alpha_1}{\gamma}, \frac{\alpha_2}{\gamma}\right);$$

o que verifica também que se para $\mathcal{I}$ e $\mathcal{J}$ ideais fracionários de $\mathcal{O}_{-n}$, com denominadores em comum γ e η respectivamente, então $\gamma \cdot \eta$ é um denominador comum para $\mathcal{I} + \mathcal{J}$ e $\mathcal{I} \cdot \mathcal{J}$. Assim, podemos garantir que sempre haverá um inteiro algébrico multiplicando um ideal fracionário resultando em um ideal comum de $\mathcal{O}_{-n}$, em outras palavras:

$$\gamma \cdot \mathcal{I} = I \subset \mathcal{O}_{-n};$$

dessa forma, o elemento inverso e neutro pertencem também ao anel $\mathcal{O}_{-n}$ já que é possível escrever

$$1 \cdot \mathcal{I} = I \subset \mathcal{O}_{-n}.$$

Em consequência direta do Lema 1.3.2, é válido também para ideais fracionários que:

Lema 1.3.4. *Sejam $\mathcal{I}$, $\mathcal{J}$ ideais fracionários de $\mathcal{O}_{-n}$. Então*

$$\mathcal{N}(\mathcal{I} \cdot \mathcal{J}) = \mathcal{N}(\mathcal{I}) \cdot \mathcal{N}(\mathcal{J}).$$

Demonstração. Para $\mathcal{I}$ e $\mathcal{J}$ ideais fracionários de $\mathcal{O}_{-n}$, existem ideais I, J e elementos não-nulos γ, η de $\mathcal{O}_{-n}$ tais que:

$$\mathcal{I} = \tfrac{1}{\gamma} I \quad \text{e} \quad \mathcal{J} = \tfrac{1}{\eta} J \quad \text{onde} \quad \mathcal{I}\mathcal{J} = \tfrac{1}{\gamma\,\eta} I\,J,$$

assim

$$\mathcal{N}(\mathcal{I}\mathcal{J}) = \frac{\mathcal{N}(IJ)}{\mathcal{N}((\gamma\eta))} = \frac{\mathcal{N}(IJ)}{\mathcal{N}((\gamma)(\eta))} = \frac{\mathcal{N}(I)}{\mathcal{N}((\gamma))}\frac{\mathcal{N}(J)}{\mathcal{N}((\eta))} = \mathcal{N}(\mathcal{I})\mathcal{N}(\mathcal{J}).$$

□

A partir daqui, por estarmos considerando o anel dos inteiros algébricos $\mathcal{O}_{-n}$, chamaremos, a menos que seja explicitado/conveniente, somente de ideais os ideais fracionários deste anel.

Definição 1.3.6. *Seja $\mathcal{I}$ um ideal próprio de $\mathcal{O}_{-n}$. Dizemos que $\mathcal{I}$ é um* ***ideal primo*** *se, sempre que $xy \in \mathcal{I}$ então ou $x \in \mathcal{I}$ ou $y \in \mathcal{I}$ para quaisquer x, $y \in \mathcal{O}_{-n}$.*

Lema 1.3.5. *Sejam $\mathcal{I}$, $\mathcal{J}$, $\wp$ ideais de $\mathcal{O}_{-n}$, com $\wp$ um ideal primo. Então se $\mathcal{I}\cdot\mathcal{J} \subseteq \wp$ então ou $\mathcal{I} \subseteq \wp$ ou $\mathcal{J} \subseteq \wp$.*

Demonstração. Vamos supor que $\mathcal{I} \nsubseteq \wp$. Sejam $x \in \mathcal{I}$ qualquer e $y \in \mathcal{J}$ qualquer. Por hipótese, $xy \in \wp$, logo devemos ter que $y \in \wp$, pois $\wp$ é primo. Portanto $\mathcal{J} \subseteq \wp$.

□

Definição 1.3.7. *Sejam $\mathcal{I}$, $\mathcal{J}$ ideais de $\mathcal{O}_{-n}$. Dizemos que $\mathcal{I}$ divide $\mathcal{J}$ se existir um ideal $\mathcal{K}$ de $\mathcal{O}_{-n}$ tal que*

$$\mathcal{J} = \mathcal{I}\cdot\mathcal{K}.$$

Segue então que se $\mathcal{I}$ divide $\mathcal{J}$ temos $\mathcal{J} \subseteq \mathcal{I}$.

Proposição 1.3.1. *Sejam $\mathcal{I}$, $\mathcal{J}$ ideais de $\mathcal{O}_{-n}$. Então:*

(i) $\mathcal{J} \subseteq \mathcal{I} \iff \mathcal{I}$ *divide* $\mathcal{J}$*;*

(ii) Se $\wp$ é ideal primo e $\wp$ divide $\mathcal{I}\mathcal{J}$ então ou $\wp$ divide $\mathcal{I}$ ou $\wp$ divide $\mathcal{J}$.

Demonstração. O item (ii) segue do item (i) associado ao Lema 1.3.5 acima. Vamos primeiramente supor que $\mathcal{J} \subseteq \mathcal{I}$ e que $\mathcal{I} = (\alpha)$ ideal principal.

Observe que $\mathcal{K} = \{\alpha^{-1}\beta;\ \beta \in \mathcal{J}\}$ é ideal de $\mathcal{O}_{-n}$, pois

$$\beta = \alpha\lambda \text{ tal que } \lambda \in \mathcal{O}_{-n} \implies \alpha^{-1}\beta = \lambda \in \mathcal{O}_{-n},$$

assim temos que $\alpha\cdot\mathcal{K} = \mathcal{J}$ logo $\mathcal{I}\mathcal{K} = \mathcal{J}$.

Em geral, $\overline{\mathcal{I}}\mathcal{J} \subseteq \overline{\mathcal{I}}\mathcal{I} = (d)$ pelo Lema 1.3.3, logo, existe um ideal $\mathcal{K}$ tal que

$$\begin{aligned}(d)\mathcal{K} = \overline{\mathcal{I}}\mathcal{J} &\implies \overline{\mathcal{I}}\mathcal{I}\mathcal{K} = \overline{\mathcal{I}}\mathcal{J} \\ &\implies \overline{\mathcal{I}}\mathcal{I}(\overline{\mathcal{I}}\mathcal{K}) = \overline{\mathcal{I}}\mathcal{I}\mathcal{J} \\ &\implies d\mathcal{I}\mathcal{K} = d\mathcal{J} \\ &\implies \mathcal{I}\mathcal{K} = d^{-1}\cdot(d\mathcal{I}\mathcal{K}) = d^{-1}\cdot(d\mathcal{J}) = \mathcal{J}.\end{aligned}$$

□

Proposição 1.3.2. *Se $\mathcal{I} \subset \mathcal{O}_{-n}$ é um ideal primo, então existe um único primo $p \in \mathbb{N}$ tal que $\mathcal{I} \mid (p)$.*

Demonstração. Como $\mathcal{I}\cdot\overline{\mathcal{I}} = (d)$, logo $\mathcal{I} \mid (d)$; por $d \in \mathbb{Z}$, a partir da sua decomposição em números primos, temos, em termos de ideais:

$$(d) = (\mathrm{p}_1)\cdot\ldots\cdot(\mathrm{p}_k).$$

Por hipótese $\mathcal{I}$ é um ideal primo, logo $\mathcal{I} \mid (\mathrm{p}_i)$, onde $i = 1, \ldots, k$. Além disso, se $q \in \mathcal{I}$ é primo, com $q \neq \mathrm{p}_i$ então $1 = \mathrm{mdc}(\mathrm{p}_i, q) \in \mathcal{I}$, um absurdo pois $\mathcal{I} \neq \mathcal{O}_{-n}$

□

Proposição 1.3.3. *Todo ideal primo $\wp \subset \mathcal{O}_{-n}$ contém um único elemento primo $p \in \mathbb{N}$. Assim a fatoração prima de um ideal principal (p) em $\mathcal{O}_{-n}$ é da forma:*

- $p = 2$,

$$(p) = \begin{cases} \left(2,\, 1+\sqrt{-n}\right)^2 & \text{se } n \equiv 1 \pmod 4; \\ \left(2,\, \sqrt{-n}\right)^2 & \text{se } n \equiv 2 \pmod 4; \\ (2) & \text{se } n \equiv 3 \pmod 8; \\ (2,\, \beta_{-n})\cdot\left(2,\, \overline{\beta_{-n}}\right) & \text{se } n \equiv 7 \pmod 8; \end{cases}$$

com $\{1, \beta_{-n}\}$ a base integral de $\mathcal{O}_{-n}$, ou

- $p > 2$,

$$(p) = \begin{cases} (p) & \text{se } \left(\frac{-n}{p}\right) = -1; \\ (p,\, a+\sqrt{-n})\cdot(p,\, a-\sqrt{-n}) & \text{se } \left(\frac{-n}{p}\right) = 1; \\ (p,\, \sqrt{-n})^2 & \text{se } \left(\frac{-n}{p}\right) = 0; \end{cases}$$

onde $\left(\frac{-n}{p}\right)$ *denota o símbolo de Legendre módulo* p*, dado por:*

$$\left(\frac{-n}{p}\right) = \begin{cases} -1 & \text{se } \nexists\ a \in \mathbb{Z} \text{ tal que } a^2 \equiv -n \pmod{p}, \\ 1 & \text{se } \exists\, a \in \mathbb{Z} \text{ tal que } a^2 \equiv -n \pmod{p}, \\ 0 & \text{se } p \mid -n. \end{cases}$$

Demonstração. Vamos supor que $\left(\frac{-n}{p}\right) = 1$:

Caso p não divide $-n$ então p também não divide a, deste modo, para ideais $\wp_1 = (p, a + \sqrt{-n})$ e $\wp_2 = (p, a - \sqrt{-n})$ de $\mathcal{O}_{-n}$, suponha que vale $\wp_1 = \wp_2$, assim

$$(a + \sqrt{-n}) + (a - \sqrt{-n}) = 2a \in \wp_1,$$

mas note que se $2a \in \mathbb{Z}$ e $\wp_1 \cap \mathbb{Z} = (p)$, e isso resulta que $p \mid 2a$, um absurdo; portanto

$$\wp_1 \neq \wp_2.$$

Para provar que $(p) = \wp_1 \cdot \wp_2$ segue que:

$$\begin{aligned} \wp_1 \cdot \wp_2 &= (p,\, a + \sqrt{-n}) \cdot (p,\, a - \sqrt{-n}) \\ &= (p^2,\, p \cdot [a + \sqrt{-n}],\, p \cdot [a - \sqrt{-n}],\, a^2 + n) \\ &= (p) \cdot (p,\, a + \sqrt{-n},\, a - \sqrt{-n},\, \tfrac{a^2+n}{p}) \\ &= (p) \cdot \mathcal{I},\ \text{pois } a^2 \equiv n \pmod{p}. \end{aligned}$$

Como $\text{mdc}(2a,\, p) = 1$, existem $x_1,\, x_2 \in \mathbb{Z}$ tais que $x_1 \cdot 2a + x_2 \cdot p = 1$, o mesmo que:

$$1 = x_1 \cdot (a + \sqrt{-n}) + x_1 \cdot (a - \sqrt{-n}) + x_2 \cdot p \implies 1 \in \mathcal{I} \implies \mathcal{I} = \mathcal{O}_{-n},$$

portanto $\wp_1 \cdot \wp_2 = (p)$.

Agora suponha que $\left(\frac{-n}{p}\right) = -1$:

Seja $\wp$ um ideal primo de $\mathcal{O}_{-n}$ tal que $\wp$ divide (p). Se $(p) \neq \wp$ existe algum $x \in \wp \setminus (p)$. Como

$$\mathcal{N}(\wp) \mid \mathcal{N}((p)) \implies \mathcal{N}(\wp) \mid p^2.$$

Temos que $(x) \subseteq \wp$ e pela Proposição 1.3.1 $\wp$ divide (x), logo

$$\mathcal{N}(\wp) \mid \mathcal{N}((x)) \implies p \mid \mathcal{N}((x)).$$

Escreva $x = a + b\beta_{-n}$ com $\{1, \beta_{-n}\}$ base de $\mathcal{O}_{-n}$, então

$$\mathcal{N}(x) = \begin{cases} a^2 + nb^2 & \text{se } n \equiv 1,\ 2 \pmod 4; \\ a^2 + ab + \frac{1+n}{4} & \text{se } n \equiv 3 \pmod 4. \end{cases}$$

Vamos supor que p não divide b; nesse caso, como p divide $\mathcal{N}(x)$, teremos, em ambos os casos módulo 4, que

$$(ab^{-1})^2 \equiv -n \pmod p \quad \text{ou} \quad (2ab^{-1} + 1)^2 \equiv -n \pmod p,$$

ou seja, $\left(\frac{-n}{p}\right) = 1$, um absurdo. Portanto

$$p \mid b \implies p \mid a \implies p \mid x \implies \wp = (p).$$

Vamos supor $\left(\frac{-n}{p}\right) = 0$, ou seja, $p \mid -n$.

Seja $\wp = (p,\ \sqrt{-n})$, então

$$\wp^2 = (p,\ \sqrt{-n}) \cdot (p,\ \sqrt{-n}) = (p^2,\ p\sqrt{-n},\ -n) = (p) \cdot \left(p,\ \sqrt{-n},\ \frac{-n}{p}\right).$$

Note que o $\mathrm{mdc}(p,\ \frac{-n}{p}) = 1$, assim, para $a,\ b \in \mathbb{Z}$:

$$1 = a \cdot p + b \cdot \frac{-n}{p} \in \left(p,\ \sqrt{-n},\ \frac{-n}{p}\right) \implies \left(p,\ \sqrt{-n},\ \frac{-n}{p}\right) = (1)$$

logo $(p) = \wp^2$.

Para o caso em que $p = 2$ e $n \equiv 1 \pmod 4$:

Seja $\wp = (2,\ 1 + \sqrt{-n})$; observe que

$$1 - \sqrt{-n} = 2 - (1 + \sqrt{-n}),$$

ou seja, podemos escrever $\wp = (2,\ 1 - \sqrt{-n})$, assim

$$\begin{aligned} \wp^2 &= (2,\ 1 + \sqrt{-n}) \cdot (2,\ 1 - \sqrt{-n}) \\ &= \left(4,\ 2 \cdot [1 + \sqrt{-n}],\ 2 \cdot [1 - \sqrt{-n}],\ 1 + n\right) \\ &= (2) \cdot \left(2,\ 1 + \sqrt{-n},\ 1 - \sqrt{-n},\ \tfrac{1+n}{2}\right). \end{aligned}$$

Note que

$$n = 4k - 3 \implies \frac{1 + 4k - 3}{2} = 2k - 1$$

para algum $k \in \mathbb{Z}$, assim é possivel obter:

$$1 = 2(k) + (-1) \cdot (2k-1) \in \left(2,\, 1+\sqrt{-n},\, 1-\sqrt{-n},\, \frac{1+n}{2}\right)$$
$$\Longrightarrow$$
$$\left(2,\, 1+\sqrt{-n},\, 1-\sqrt{-n},\, \frac{1+n}{2}\right) = (1),$$

portanto $(2) = (2,\, 1+\sqrt{-n})^2$.

Supondo $p = 2$ e $n \equiv 2 \pmod 4$:

Dado $\wp = (2,\, \sqrt{-n})$, temos:

$$\wp^2 = (2,\, \sqrt{-n}) \cdot (2,\, \sqrt{-n}) = (4,\, 2 \cdot \sqrt{-n},\, -n) = (2) \cdot \left(2,\, \sqrt{-n},\, \frac{-n}{2}\right).$$

Por hipótese, $n \equiv 2 \pmod 4$, ou seja $\frac{-n}{2} = 2m - 1$ para algum $m \in \mathbb{Z}$, assim é possivel obter:

$$1 = \frac{-n}{2} + 2m \in \left(2,\, \sqrt{-n}, \frac{-n}{2}\right) \implies \left(2,\, \sqrt{-n}, \frac{-n}{2}\right) = (1),$$

portanto $(2) = (2,\, \sqrt{-n})^2$.

Considerando $p = 2$ e $n \equiv 3 \pmod 8$, usamos o mesmo argumento já provado no primeiro caso quando $p > 2$ e $\left(\frac{-n}{p}\right) = -1$, a saber:

Para $\wp$ um ideal primo de $\mathcal{O}_{-n}$ tal que $\wp$ divide (2); caso $\wp \neq (2)$, existe algum $x \in \wp \setminus (2)$. Como

$$\mathcal{N}(\wp) \mid \mathcal{N}((2)) \implies \mathcal{N}(\wp) \mid 4.$$

Temos que $(x) \subseteq \wp$ e, pela Proposição 1.3.1 $\wp$ divide (x) logo

$$\mathcal{N}(\wp) \mid \mathcal{N}((x)) \implies 2 \mid \mathcal{N}((x)).$$

Seja $x = a + b\beta_{-n}$ com $\{1,\, \beta_{-n}\}$ base de $\mathcal{O}_{-n}$ e $n \equiv 3 \pmod 4$, então

$$\mathcal{N}(x) = a^2 + ab + \frac{1+n}{4}.$$

Supondo $2 \nmid b$; nesse caso, por $2 \mid \mathcal{N}(x)$, teremos que

$$(2ab^{-1} + 1)^2 \equiv -n \pmod p,$$

ou seja, $\left(\frac{-n}{p}\right) = 1$, absurdo. Portanto

$$2 \mid b \implies 2 \mid a \implies 2 \mid x \implies \wp = (2).$$

Para o último caso em que $p = 2$ e $n \equiv 7 \pmod 8$:

Afirmamos que

$$\left(2, \frac{1+\sqrt{-n}}{2}\right) \cdot \left(2, \frac{1-\sqrt{-n}}{2}\right) = (2).$$

O que pode se notar é que para um ideal $\mathcal{I} \subset \mathcal{O}_{-n}$ temos:

$$\begin{aligned}
\left(2, \tfrac{1+\sqrt{-n}}{2}\right) \cdot \left(2, \tfrac{1-\sqrt{-n}}{2}\right) &= \left(4, 1+\sqrt{-n}, 1-\sqrt{-n}, \frac{1+n}{4}\right) \\
&= (2) \cdot \left(2, \beta_{-n}, \overline{\beta_{-n}}, \frac{1+n}{8}\right) \\
&= (2) \cdot \mathcal{I}
\end{aligned}$$

concluindo que $\mathcal{I} = \mathcal{O}_{-n}$ desde que $\beta_{-n} + \overline{\beta_{-n}} = 1$. Observe que se caso

$$\left(2, \frac{1+\sqrt{-n}}{2}\right) = \left(2, \frac{1-\sqrt{-n}}{2}\right)$$

temos

$$1 = \left(\frac{1+\sqrt{-n}}{2}\right) + \left(\frac{1-\sqrt{-n}}{2}\right) \in \left(2, \frac{1+\sqrt{-n}}{2}\right)$$

o que é impossível, pois se fosse, teríamos:

$$(2) = \left(2, \frac{1-\sqrt{-n}}{2}\right),$$

um absurdo; logo

$$\left(2, \frac{1+\sqrt{-n}}{2}\right) \neq \left(2, \frac{1-\sqrt{-n}}{2}\right),$$

provando a proposição.

□

Antes de provarmos o resultado da fatoração de ideais em $\mathcal{O}_{-n}$, uma consequência importante envolvendo ideais primos se faz necessária:

Lema 1.3.6. *Sejam $\wp$, $\mathcal{Q}_0$, $\mathcal{Q}_1$ ideais primos de $\mathcal{O}_{-n}$, com $\wp \neq \mathcal{Q}_0$ e $\wp \neq \mathcal{Q}_1$. Se $\wp \cdot \mathcal{Q}_0 = \wp \cdot \mathcal{Q}_1$ então $\mathcal{Q}_0 = \mathcal{Q}_1$.*

Demonstração. Como $\mathcal{Q}_1$ é primo e $\mathcal{Q}_1 \mid \wp \cdot \mathcal{Q}_0$, segue da Proposição 1.3.1 que $\mathcal{Q}_1 \mid \wp$ ou $\mathcal{Q}_1 \mid \mathcal{Q}_0$. Como $\wp$ e $\mathcal{Q}_0$ também são primos e $\mathcal{Q}_1 \neq \wp$, segue que $\mathcal{Q}_1 = \mathcal{Q}_0$.

□

Definição 1.3.8. *Seja $\mathcal{I}$ um ideal próprio*[1] *de $\mathcal{O}_{-n}$, dizemos que:*

- *$\mathcal{I}$ é **irredutível** se para todo ideal $\mathcal{J}$, $\mathcal{K} \subset \mathcal{O}_{-n}$:*

$$\mathcal{J} \cdot \mathcal{K} = \mathcal{I} \implies \mathcal{J} = \mathcal{I} \text{ ou } \mathcal{K} = \mathcal{I}.$$

- *$\mathcal{I}$ é **maximal** se para todo ideal $\mathcal{J} \subset \mathcal{O}_{-n}$:*

$$\mathcal{I} \subset \mathcal{J} \implies \mathcal{J} = \mathcal{I} \text{ ou } \mathcal{J} = \mathcal{O}_{-n}.$$

Proposição 1.3.4. *Para todo ideal do anel $\mathcal{O}_{-n}$, as sentenças são equivalentes:*

(i) Ideais primos;

(ii) Ideais irredutiveis;

(iii) Ideais maximais.

Demonstração. Sejam $\mathcal{I}$, $\mathcal{J}$, $\mathcal{K}$ ideais de $\mathcal{O}_{-n}$.

$(i) \implies (ii)$:

Se $\mathcal{I}$ é um ideal primo tal que $\mathcal{I} = \mathcal{J} \cdot \mathcal{K}$, então por definição $\mathcal{I} \mid \mathcal{J} \cdot \mathcal{K}$. Suponha que, sem perda de generalidade, $\mathcal{I} \mid \mathcal{J}$. Mais ainda, temos também que $\mathcal{J} \mid \mathcal{I}$, assim pela Proposição 1.3.1:

$$\mathcal{I} \subset \mathcal{J} \text{ e } \mathcal{J} \subset \mathcal{I}$$

ou seja $\mathcal{I} = \mathcal{J}$, portanto o ideal $\mathcal{I}$ é irredutivel.

$(ii) \implies (iii)$:

Se $\mathcal{I}$ é um ideal irredutível com $\mathcal{I} \subset \mathcal{J}$. Pela Proposição 1.3.1:

$$\mathcal{J} \mid \mathcal{I} \iff \exists \mathcal{K} \text{ tal que } \mathcal{I} = \mathcal{J} \cdot \mathcal{K},$$

assim $\mathcal{I} = \mathcal{J}$ ou $\mathcal{I} = \mathcal{K}$, então, pela hipótese $\mathcal{I}$ deve ser o próprio anel $\mathcal{O}_{-n}$. Portanto $\mathcal{I}$ é maximal.

[1] ou seja, $\mathcal{I} \subset \mathcal{O}_{-n}$ e $\mathcal{I} \neq \mathcal{O}_{-n}$.

$(iii) \implies (i)$:

Se $\mathcal{I}$ é um ideal maximal, sabemos que $^{\mathcal{O}_{-n}}/_{\mathcal{I}}$ é um corpo. Como todo corpo é um dominío de integridade, implica diretamente que $^{\mathcal{O}_{-n}}/_{\mathcal{I}}$ é um domínio de integridade, logo $\mathcal{I}$ é um ideal primo.

□

Teorema 1.3.1. *(Fatoração Única de Ideais) Todo ideal não-nulo $\mathcal{I} \subset \mathcal{O}_{-n}$ possui uma fatoração única em ideais primos, ou seja,*

$$\mathcal{I} = \prod_{i=1}^{k} \wp_i,$$

onde $\wp_1, \ldots, \wp_k$ são ideais primos.

Demonstração. Unicidade: Sejam $\wp_j, \mathcal{Q}_m$ ideais primos de $\mathcal{O}_{-n}$, não necessariamente distintos onde $1 \leq j \leq l$ e $1 \leq k \leq m$, tais que

$$\wp_1 \cdots \wp_l = \mathcal{Q}_1 \cdots \mathcal{Q}_m,$$

então, sem perda de generalidade, suponha que

$$\mathcal{Q}_1 \cdots \mathcal{Q}_m \subseteq \wp_1.$$

Como $\wp_j$ e $\mathcal{Q}_k$ são primos, segue que $\wp_1 = \mathcal{Q}_k$. Podemos então assumir $\wp_1 = \mathcal{Q}_1$ e pelo Lema 1.3.6, segue que

$$\wp_2 \cdots \wp_l = \mathcal{Q}_2 \cdots \mathcal{Q}_m.$$

Indutivamente obtemos $l = m$ e $\wp_j = \mathcal{Q}_j$ para $1 \leq j \leq l = m$.

Existência: Pelo fato de $\mathcal{O}_{-n}$ ser noetheriano e que todo ideal maximal é primo, suponha $\mathcal{S}$ um conjunto de ideais de $\mathcal{O}_{-n}$ que não se escrevem como um produto de ideais primos. Como $\mathcal{O}_{-n}$ é noetheriano, $\mathcal{S}$ possui algum ideal maximal $\mathcal{I}$, assim:

$$\mathcal{I} \subseteq \wp.$$

Por $\mathcal{I}$ estar em $\mathcal{S}$, implica que $\mathcal{I} \neq \wp$, logo vai existir algum $\mathcal{J} \in \mathcal{S}$ tal que:

$$\mathcal{I} = \wp \cdot \mathcal{J}.$$

Isso nos resulta que $\mathcal{I} \subseteq \mathcal{J}$, mais ainda $\mathcal{I} = \mathcal{J}$; mas pelo Lema 1.3.5 temos que $\mathcal{O}_{-n} = \wp$, o que não pode ocorrer. Sendo assim, $\mathcal{J}$ não pertence ao conjunto $\mathcal{S}$, e por $\mathcal{I}$ ser maximal temos que $\mathcal{I}$ se fatora em ideais primos $\wp$ e $\mathcal{J}$, uma contradição; portanto $\mathcal{S} = \emptyset$, assim todo ideal de $\mathcal{O}_{-n}$ se fatora em ideais primos.

□

Teorema 1.3.2. *Seja $\mathcal{I}$ um ideal de $\mathcal{O}_{-n}$, então:*

$$\mathcal{I} \cdot \overline{\mathcal{I}} = (\mathcal{N}(\mathcal{I})).$$

Demonstração. Se $\mathcal{I} = (1)$, então o resultado segue. Suponha $\mathcal{I}$ diferente do ideal trivial, assim pela fatoração em ideais primos, seja

$$\mathcal{I} = {\wp_1}^{a_1}\overline{\wp_1}^{b_1} \cdots {\wp_r}^{a_r}\overline{\wp_r}^{b_r}{\mathcal{Q}_1}^{c_1} \cdots {\mathcal{Q}_s}^{c_s}{\mathcal{R}_1}^{d_1} \cdots {\mathcal{R}_t}^{d_t},$$

onde $\wp_1$, ..., $\wp_r$ ideais primos distintos tais que

$$\wp \cdot \overline{\wp} = (p), \quad \mathcal{N}(\wp) = \mathcal{N}(\overline{\wp}) = p \quad \text{e} \quad \wp \neq \overline{\wp};$$

os $\mathcal{Q}_1$, ..., $\mathcal{Q}_s$ ideais primos distintos tais que

$$\mathcal{Q} = \overline{\mathcal{Q}} = (q) \quad \text{e} \quad \mathcal{N}(\mathcal{Q}) = q^2;$$

os $\mathcal{R}_1$, ..., $\mathcal{R}_t$ ideais primos distintos tais que

$$\mathcal{R} = \overline{\mathcal{R}}, \quad \mathcal{R}^2 = (r) \quad \text{e} \quad \mathcal{N}(\mathcal{R}) = r;$$

com p, q, s primos racionais. Pela função de conjugação em ideais de $\mathcal{O}_{-n}$, é fácil ver que $\overline{\mathcal{I} \cdot \mathcal{J}} = \overline{\mathcal{I}} \cdot \overline{\mathcal{J}}$, assim

$$\overline{\mathcal{I}} = \overline{\wp_1}^{a_1}{\wp_1}^{b_1} \cdots \overline{\wp_r}^{a_r}{\wp_r}^{b_r}{\mathcal{Q}_1}^{c_1} \cdots {\mathcal{Q}_s}^{c_s}{\mathcal{R}_1}^{d_1} \cdots {\mathcal{R}_t}^{d_t}.$$

Logo,

$$\begin{aligned}
\mathcal{I} \cdot \overline{\mathcal{I}} &= {\wp_1}^{a_1+b_1} \cdot \overline{\wp_1}^{a_1+b_1} \cdots {\wp_r}^{a_r+b_r} \cdot \overline{\wp_r}^{a_r+b_r}{\mathcal{Q}_1}^{2c_1} \cdots {\mathcal{Q}_s}^{2c_s} \cdot {\mathcal{R}_1}^{2d_1} \cdots {\mathcal{R}_t}^{2d_t} \\
&= (p_1)^{a_1+b_1} \cdots (p_r)^{a_r+b_r}(q_1)^{2c_1} \cdots (q_s)^{2c_s}(r_1)^{d_1} \cdots (r_t)^{d_t} \\
&= ({p_1}^{a_1+b_1} \cdots {p_r}^{a_r+b_r}{q_1}^{2c_1} \cdots {q_s}^{2c_s}{r_1}^{d_1} \cdots {r_t}^{d_t}).
\end{aligned}$$

Mais ainda, pela função norma ser multiplicativa, temos que

$$\begin{aligned}
\mathcal{N}(\mathcal{I}) &= \mathcal{N}(\wp_1)^{a_1}\mathcal{N}(\overline{\wp_1})^{b_1} \cdots \mathcal{N}(\wp_r)^{a_r}\mathcal{N}(\overline{\wp_r})^{b_r}\mathcal{N}(\mathcal{Q}_1)^{c_1} \cdots \\
&\quad \mathcal{N}(\mathcal{Q}_s)^{c_s}\mathcal{N}(\mathcal{R}_1)^{d_1} \cdots \mathcal{N}(\mathcal{R}_t)^{d_t} \\
&= p_1^{a_1}p_1^{b_1} \cdots p_r^{a_r}p_r^{b_r}q_1^{2c_1} \cdots q_s^{2c_s}r_1^{d_1} \cdots r_t^{d_t}.
\end{aligned}$$

Portanto,

$$\mathcal{I} \cdot \overline{\mathcal{I}} = (\mathcal{N}(\mathcal{I})).$$

□

Exemplo 1.3.3.

Fatorando o ideal principal $\left(-55+187\sqrt{-5}\right)$ em ideais primos de $\mathbb{Z}[\sqrt{-5}]$.

Calculando sua norma:

$$\mathcal{N}(-55+187\sqrt{-5}) = 177870 = 2\cdot 3\cdot 5\cdot 7^2\cdot 11^2. \tag{1.1}$$

Temos então que $(-55+187\sqrt{-5})$ está contido em um ideal de norma 2, um ideal de norma 3, um ideal de norma 5 e:

- um ideal de norma 7^2 ou dois idais de norma 7;
- um ideal de norma 11^2 ou dois idais de norma 11.

Pela Proposição 1.3.3, temos:

$$\begin{cases} (2) = (2,\ 1+\sqrt{-5})^2; \\ (3) = (3,\ 1+\sqrt{-5})\cdot(3,\ 1-\sqrt{-5}); \\ (5) = (5,\ \sqrt{-5})^2; \\ (7) = (7,\ 3+\sqrt{-5})\cdot(7,\ 3-\sqrt{-5}); \\ (11) \text{ é ideal primo então } \mathcal{N}((11)) = 11^2. \end{cases} \tag{1.2}$$

Pela ideia da Proposição 1.3.3, um fato importante é que $\mathcal{N}(\mathcal{I}) \in \mathcal{I}$. Denotando $\mathcal{I}_2$, $\mathcal{I}_3$, $\mathcal{I}_5$ e $\mathcal{I}_7$ ideais tendo norma 2, 3, 5 e 7 respectivamente, segue que:

$$\begin{cases} \mathcal{N}(\mathcal{I}_2) = 2 \implies (2) \subseteq \mathcal{I}_2; \\ \mathcal{N}(\mathcal{I}_3) = 3 \implies (3) \subseteq \mathcal{I}_3; \\ \mathcal{N}(\mathcal{I}_5) = 5 \implies (5) \subseteq \mathcal{I}_5; \\ \mathcal{N}(\mathcal{I}_7) = 7 \implies (7) \subseteq \mathcal{I}_7. \end{cases}$$

Pela equação (1.2) só existe um ideal de norma 2, ou seja, $\mathcal{I}_2 = (2,\ 1+\sqrt{-5})$, e apenas um ideal de norma 5, ou seja, $\mathcal{I}_5 = (5, \sqrt{-5})$. Outro fato é que, existem dois ideais de norma 3 e dois ideais de norma 7, assim, a partir da fatoração na equação (1.1), um dos ideais de norma 3 aparece na fatoração do ideal $(-55+187\sqrt{-5})$, e como na equação (1.1) aparece 7^2, pode acontecer dois ideais com norma 7 estarem nessa fatoração.

Citados esses ideais de norma 7, se os dois dividem $(-55+187\sqrt{-5})$, e como o produtos deles é (7), então:

$$(-55+187\sqrt{-5}) \subseteq (7) \implies \exists x \in \mathbb{Z}\sqrt{-5} \text{ tal que } 7x = -55+187\sqrt{-5}, \qquad (1.3)$$

o que não acontece. Logo, somente um deles aparece na fatoração.

Temos então as possibilidades usando:

$$(3,\, 1+\sqrt{-5}), \quad (3,\, 1-\sqrt{-5}),$$

$$(7,\, 3+\sqrt{-5}), \quad (7,\, 3-\sqrt{-5}).$$

Aqui, nos deparamos com um processo bem trabalhoso quanto às contas devido a esses dois ideais que procuramos possuirem dois geradores; pelo Exemplo 1.3.2, nos serve de auxílio, pois no fim, tais multiplicações de ideais com dois geradores se tornam um ideal principal. Como $\mathcal{I}_2 = (2,\, 1+\sqrt{-5})$ com

$$(2,\, 1+\sqrt{-5}) \cdot \mathcal{I}_3 \mid (-55+187\sqrt{-5}),$$

mais ainda, somente $(1+\sqrt{-5})$ ou $(1-\sqrt{-5})$ podem conter $(-55+187\sqrt{-5})$, então pelo Exemplo 1.3.2, só podemos ter que $\mathcal{I}_3 = (3,\, 1-\sqrt{-5})$.

O mesmo raciocínio se vale pra encontrar $\mathcal{I}_7$. Fazendo alguns cálculos, que serão omitidos, chegamos em: $(2,\, 1+\sqrt{-5}) \cdot \mathcal{I}_7$ pode ser $(3-\sqrt{-5})$ ou $(3+\sqrt{-5})$. Ao usar os processos da equação (1.3), temos que:

- para o ideal $(3-\sqrt{-5})$:

$$(3-\sqrt{-5})\cdot x = (3-\sqrt{-5})\cdot(a+b\sqrt{-5}) = (3a+5b)+(3b-a)\sqrt{-5} = -55+187\sqrt{-5}$$

$$\implies$$

$$\begin{cases} 3a+5b = -55 \\ 3b-a = 187 \end{cases} \implies b = \frac{253}{7} \notin \mathbb{Z} \implies 3-\sqrt{-5} \nmid -55+187\sqrt{-5}.$$

- para o ideal $(3+\sqrt{-5})$:

$$(3-\sqrt{-5})\cdot x = (3-\sqrt{-5})\cdot(a+b\sqrt{-5}) = (3a-5b)+(a+3b)\sqrt{-5} = -55+187\sqrt{-5}$$

$$\implies$$

$$\begin{cases} 3a-5b = -55 \\ a+3b = 187 \end{cases} \implies \begin{cases} a = 55 \\ b = 44 \end{cases} \implies x = 55+44\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$$

$$\implies$$

$$3+\sqrt{-5} \mid -55+187\sqrt{-5}.$$

Assim $\mathcal{I}_7 = (3+\sqrt{-5})$, portanto a fatoração se dá por:

$$(-55+187\sqrt{-5}) = (2,\, 1+\sqrt{-5}) \cdot (3,\, 1-\sqrt{-5}) \cdot (3+\sqrt{-5})^2 \cdot (11).$$

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

Tome um conjunto formado por todos os ideais fracionários do corpo $\mathbb{Q}(\sqrt{-n})$ e denote-o por $\mathbb{I}_{-n}$. Afirmamos que:

Lema 1.4.1. *O conjunto $\mathbb{I}_{-n}$ forma um grupo abeliano sob a multiplicação em $\mathcal{O}_{-n}$.*

Demonstração. Seja $\mathcal{K} \in \mathbb{I}_{-n}$ um ideal fracionário, logo existe $\gamma \in \mathcal{O}_{-n}$ não-nulo tal que $\gamma\mathcal{K}$ é ideal de $\mathcal{O}_{-n}$. A multiplicação entre os ideais de $\mathcal{O}_{-n}$ é claramente comutativa e associativa. Para verificar a existência do elemento neutro (identidade) basta ver que é o próprio $\mathcal{O}_{-n} = (1)$. Resta então encontrar o elemento inverso: pelos resultados provados no Lema 1.3.3 e na Proposição 1.3.1 garante que existe um ideal $\mathcal{I}$ tal que $\gamma\mathcal{K}\mathcal{I}$ é principal. Tome o ideal fracionário $\mathcal{J} = \frac{\gamma}{\eta}\mathcal{I}$, logo:

$$\mathcal{K}\mathcal{J} = \frac{\gamma}{\eta}\mathcal{K}\mathcal{I} = (1),$$

assim $\mathcal{J}$ é um inverso de $\mathcal{K}$ em $\mathbb{I}_{-n}$ portanto o mesmo forma um grupo abeliano com a multiplicação.

□

Feito isso, é possivel obter um conjunto de $\mathbb{I}_{-n}$ e então definir o $\mathbb{P}_{-n}$ como sendo o subgrupo formado pelos ideais principais fracionários, logo caracterizamos o grupo de classes ideais $\mathcal{C}l(-n)$ do corpo numérico $\mathbb{Q}(\sqrt{-n})$ o grupo quociente:

$$\mathcal{C}l(-n) = {}^{\mathbb{I}_{-n}}\!/_{\mathbb{P}_{-n}}.$$

Assim entende-se que os elementos desse grupo, dita ***classe ideal***, são classes laterais de $\mathbb{P}_{-n}$, e para garantir que essa classe de ideais existe, observe que:

Lema 1.4.2. *Seja $\mathcal{C}$ uma classe ideal então existe um ideal na classe $\mathcal{C}$.*

Demonstração. Para $\mathcal{I}$ um ideal fracionário em $\mathcal{C}$, existe um $\gamma \in \mathbb{Q}(\sqrt{-n})^{\times}$ tal que $\gamma\mathcal{I}$ é um ideal de $\mathcal{O}_{-n}$. Desde que $(\gamma) \in \mathbb{P}_{-n}$, temos que $\gamma\mathcal{I} \in \mathcal{C}$.

□

Logo, por meio dessa relação podemos definir:

Definição 1.4.1. *Seja $\mathcal{I}$ um ideal qualquer de $\mathcal{O}_{-n}$, denote por $\mathcal{C}_{\mathcal{I}}$ a **classe** do ideal $\mathcal{I}$; alternativamente podemos escrever apenas $\mathcal{C}$ tal que para todo $\mathcal{I} \in \mathcal{C}$.*

Definição 1.4.2. *Sejam $\mathcal{I}$, $\mathcal{J}$ ideais de $\mathcal{O}_{-n}$. Se existem γ, $\eta \in \mathcal{O}_{-n}$ tal que*

$$(\gamma) \cdot \mathcal{I} = (\eta) \cdot \mathcal{J},$$

*então $\mathcal{I}$ e $\mathcal{J}$ são ditos **similares** (denote $\mathcal{I} \simeq \mathcal{J}$).*

Proposição 1.4.1. *Todo ideal principal de $\mathcal{O}_{-n}$ é similar à $\mathcal{O}_{-n}$.*

Demonstração. Seja $\mathcal{I} = (\gamma)$ ideal principal de $\mathcal{O}_{-n}$, logo

$$\mathcal{I} = (\gamma) \cdot \mathcal{O}_{-n} \implies \mathcal{I} \simeq \mathcal{O}_{-n}.$$

□

Esta última propriedade nos mostra em termos de classe ideal que para todo ideal principal (α) de $\mathcal{O}_{-n}$, então $(\alpha) \in \mathcal{C}_1$.

Proposição 1.4.2. *O produto de ideais similares é também similiar.*

Demonstração. Sejam $\mathcal{I}_1$, $\mathcal{I}_2$, $\mathcal{J}_1$, $\mathcal{J}_2$ ideais de $\mathcal{O}_{-n}$ tais que $\mathcal{I}_1 \simeq \mathcal{J}_1$ e $\mathcal{I}_2 \simeq \mathcal{J}_2$, então por definição existem γ_1, γ_2, η_1, $\eta_2 \in \mathcal{O}_{-n}$ onde:

$$(\gamma_1) \cdot \mathcal{I}_1 = (\eta_1) \cdot \mathcal{J}_1$$

e

$$(\gamma_2) \cdot \mathcal{I}_2 = (\eta_2) \cdot \mathcal{J}_2;$$

ao multiplicar as equações acima, temos:

$$(\gamma_1) \cdot \mathcal{I}_1 \cdot (\gamma_2) \cdot \mathcal{I}_2 = (\eta_1) \cdot \mathcal{J}_1 (\eta_2) \cdot \mathcal{J}_2$$

$$\implies$$

$$(\gamma_1 \cdot \gamma_2) \cdot \mathcal{I}_1 \cdot \mathcal{I}_2 = (\eta_1 \cdot \eta_2) \cdot \mathcal{J}_1 \cdot \mathcal{J}_2.$$

Como $\gamma_1 \cdot \gamma_2$, $\eta_1 \cdot \eta_2 \in \mathcal{O}_n$ e tomando $\gamma_1 \cdot \gamma_2 = \gamma_3$ e $\eta_1 \cdot \eta_2 = \eta_3$, obtemos:

$$(\gamma_3) \cdot \mathcal{I}_1 \cdot \mathcal{I}_2 = (\eta_3) \mathcal{J}_1 \cdot \mathcal{J}_2,$$

logo, por definição de similaridade:

$$\mathcal{I}_1 \cdot \mathcal{I}_2 \simeq \mathcal{J}_1 \cdot \mathcal{J}_2.$$

□

É possivel então definir o produto de duas classes de ideais, a qual não depende da escolha dos ideais em $\mathcal{O}_{-n}$ vide Proposição 1.4 tomando $\mathcal{I} \in \mathcal{C}$ e $\mathcal{J} \in \tilde{\mathcal{C}}$ ideais de $\mathcal{O}_{-n}$, e assim:

$$\mathcal{C} \cdot \tilde{\mathcal{C}} \overset{def}{=} \mathcal{C}_{\mathcal{I}} \cdot \mathcal{C}_{\mathcal{J}} = \mathcal{C}_{\mathcal{I}.\mathcal{J}}.$$

Definição 1.4.3. *Defina a* ***classe inversa*** *em $\mathcal{C}l(-n)$ dada pela conjugação de uma classe ideal $\mathcal{C}$. Por meio do Teorema 1.3.2 sabemos que $\mathcal{I} \cdot \overline{\mathcal{I}} = (\mathcal{N}(\mathcal{I}))$, então*

$$\mathcal{C}_{\mathcal{I}} \cdot \mathcal{C}_{\overline{\mathcal{I}}} = \mathcal{C}_1,$$

assim:

$$\mathcal{C}^{-1} \overset{def}{=} \left\{ \overline{\mathcal{I}};\, \mathcal{I} \in \mathcal{C} \right\}.$$

Como a similaridade possui uma relação de equivalência diante das classes ideais, tal classe $\mathcal{C}^{-1}$ satisfaz as propriedades de multiplicação de ideais por similaridade, assim o resultado principal desta seção evidencia que:

Lema 1.4.3. *O conjunto $\mathcal{C}l(-n)$ é um grupo abeliano com a operação definida acima.*

Demonstração. Dados $\mathcal{I} \in \mathcal{C}$, $\mathcal{J} \in \tilde{\mathcal{C}}$, $\mathcal{K} \in \mathcal{C}^*$ temos:

Elemento Neutro:

Como já visto, $\mathcal{I} \cdot \mathcal{O}_{-n} = \mathcal{I}$, então:

$$\mathcal{C} \cdot \mathcal{C}_{\mathcal{O}_{-n}} = \mathcal{C}_{\mathcal{I}} \cdot \mathcal{C}_1 = \mathcal{C}_{\mathcal{I}\cdot 1} = \mathcal{C}_{\mathcal{I}} = \mathcal{C}$$

logo $\mathcal{C}_1$ é o elemento neutro.

Comutatividade:

Note que para ideais $\mathcal{I}$ e $\mathcal{J}$ no anel $\mathcal{O}_{-n}$, temos que

$$\mathcal{I} \cdot \mathcal{J} = \mathcal{J} \cdot \mathcal{I}$$

assim:

$$\mathcal{C} \cdot \tilde{\mathcal{C}} = \mathcal{C}_{\mathcal{I}} \cdot \mathcal{C}_{\mathcal{J}} = \mathcal{C}_{\mathcal{I}\cdot\mathcal{J}} = \mathcal{C}_{\mathcal{J}\cdot\mathcal{I}} = \mathcal{C}_{\mathcal{J}} \cdot \mathcal{C}_{\mathcal{I}} = \tilde{\mathcal{C}} \cdot \mathcal{C}.$$

Associatividade:

Pela multiplicação entre classes ideais não depender da escolha dos ideais, por definição, sabemos que:

$$(\mathcal{C} \cdot \tilde{\mathcal{C}}) \cdot \mathcal{C}^* = (\mathcal{C}_{\mathcal{I}} \cdot \mathcal{C}_{\mathcal{J}}) \cdot \mathcal{C}_{\mathcal{K}} = \mathcal{C}_{(\mathcal{I}\cdot\mathcal{J})} \cdot \mathcal{C}_{\mathcal{K}} = \mathcal{C}_{(\mathcal{I}\cdot\mathcal{J})\cdot\mathcal{K}}$$

Como a multiplicação entre ideais de $\mathcal{O}_{-n}$ é associtiva, segue da equação acima que:

$$\mathcal{C}_{(\mathcal{I}\cdot\mathcal{J})\cdot\mathcal{K}} = \mathcal{C}_{\mathcal{I}\cdot(\mathcal{J}\cdot\mathcal{K})} = \mathcal{C}_{\mathcal{I}} \cdot \mathcal{C}_{(\mathcal{J}\cdot\mathcal{K})} = \mathcal{C}_{\mathcal{I}} \cdot (\mathcal{C}_{\mathcal{J}} \cdot \mathcal{C}_{\mathcal{K}}) = \mathcal{C} \cdot (\tilde{\mathcal{C}} \cdot \mathcal{C}^*).$$

Inverso:

A partir da Definição 1.4.3, o elemento inverso é facilmente encontrado, a saber:

$$\mathcal{C} \cdot \mathcal{C}^{-1} = \mathcal{C}_{\mathcal{I}} \cdot \mathcal{C}_{\overline{\mathcal{I}}} = \mathcal{C}_{\mathcal{I}\cdot\overline{\mathcal{I}}} = \mathcal{C}_{(\mathcal{N}(\mathcal{I}))} = \mathcal{C}_1.$$

Portanto, provadas essas propriedades, $\mathcal{C}l(-n)$ é um grupo abeliano sob a multiplicação de classes ideais.

□

O próximo objetivo é concluir/compreender a cardinalidade/finitude do grupo de classes ideais $\mathcal{C}l(-n)$ que é chamado de número de classes denotado por $h(-n)$.

1.5 Redes Complexas

Nesta seção traremos a relação direta entre os ideais do anel $\mathcal{O}_{-n}$ com os conceitos e propriedades das redes complexas, tendo como objetivo principal apresentar a finitude do grupos das classes de ideais via classes de redes equivalentes.

Definição 1.5.1. *Um conjunto $\Lambda \subset \mathbb{C}$ é dito uma* ***rede complexa*** *se existem elementos não nulos α, $\beta \in \Lambda$ tais que:*

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

Usaremos a notação da rede complexa Λ como $\Lambda = \langle \alpha, \beta \rangle$. Quando $im\left(\frac{\beta}{\alpha}\right) > 0$, dizemos que o par α e β é uma base ***normalizada*** de Λ.

Se α^*, β^* é outra base de Λ, segue que

$$\begin{aligned} \alpha^* &= a\alpha + b\beta \\ \beta^* &= c\alpha + d\beta \end{aligned} \tag{1.4}$$

e a matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tem que ser invertível, ou seja, é necessário de $ad - bc = \pm 1$. Com isso, provamos o seguinte lema:

Lema 1.5.1. *Seja Λ uma rede complexa com α, β uma base normalizada de Λ e inteiros a, b, c, d tais que $ad - bc = \pm 1$. Então toda base da rede Λ é da forma $a\alpha + b\beta$, $c\alpha + d\beta$. Será uma base normalizada se e só se $ad - bc = 1$.*

Demonstração. Basta mostrar que o par α^*, β^* visto na equação (1.4) é base normalizada se, e somente se, $ad - bc = 1$. Para o último resultado, considere $\mathrm{j} = \frac{\beta}{\alpha}$ e tome x, y a parte real e imaginária de j respectivamente. Assim:

$$\begin{aligned} \frac{\beta^*}{\alpha^*} &= \frac{c\alpha + d\beta}{a\alpha + b\beta} \\ &= \frac{c + d\mathrm{j}}{a + b\mathrm{j}} \\ &= \frac{(c + d\mathrm{j})(a + b\bar{\mathrm{j}})}{(a + b\mathrm{j})(a + b\bar{\mathrm{j}})} \\ &= \frac{ac + ad\mathrm{j} + bc\bar{\mathrm{j}} + bd\mathrm{j}\bar{\mathrm{j}}}{|a + b\mathrm{j}|^2} \\ &= \frac{(ac + adx + bcx + bd|\mathrm{j}|^2) + (ad - bc)yi}{|a + b\mathrm{j}|^2}, \end{aligned}$$

logo

$$im\left(\frac{c+d\mathfrak{j}}{a+b\mathfrak{j}}\right) = \frac{ad-bc}{|a+b\mathfrak{j}|^2}\cdot im(\mathfrak{j}). \tag{1.5}$$

Portanto $im\left(\frac{\beta^*}{\alpha^*}\right) > 0 \iff ad-bc=1$, já que $im(\mathfrak{j}) > 0$ por definição.

□

1.5.1 Redes equivalentes

Definição 1.5.2. *Duas redes complexas Λ, Λ^* são ditas* ***equivalentes*** *se existir um $\delta \in \mathbb{C}^\times$ tal que $\Lambda^* = \delta\cdot\Lambda$, ou seja*

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

Definição 1.5.3. *Seja $\Lambda = \langle \alpha,\, \beta\rangle$ uma rede complexa com α, β base normalizada, defina o $\mathfrak{J}-$**conjunto** de Λ como*

$$\mathfrak{J}(\Lambda) \overset{def}{=} \left\{ \frac{\beta^*}{\alpha^*};\ \alpha^*,\, \beta^* \text{ uma base normalizada de } \Lambda \right\}.$$

Pelo Lema 1.5.1 e tomando $\mathfrak{j} = \frac{\beta}{\alpha}$ tem-se que o par $\alpha^* = \alpha a + \beta b$ e $\beta^* = \alpha c + \beta d$, com $ad-bc=1$ é também base normalizada de Λ. Assim podemos escrever

$$\frac{\beta^*}{\alpha^*} = \frac{c+d\cdot\mathfrak{j}}{a+b\cdot\mathfrak{j}}$$

e então concluir que:

$$\mathfrak{J}(\Lambda) = \left\{ \frac{c+d\cdot\mathfrak{j}}{a+b\cdot\mathfrak{j}};\ \text{com } ad-bc=1 \right\}. \tag{1.6}$$

Lema 1.5.2. *Sejam Λ, Λ^* redes complexas e $\mathfrak{j}^* \in \mathbb{C}$ com $im(\mathfrak{j}^*) > 0$, então:*

(i) $\Lambda \sim \langle 1,\, \mathfrak{j}^*\rangle \iff \mathfrak{j}^* \in \mathfrak{J}(\Lambda)$,

(ii) $\Lambda \sim \Lambda^* \iff \mathfrak{J}(\Lambda) = \mathfrak{J}(\Lambda^*) \iff \mathfrak{J}(\Lambda)\cap\mathfrak{J}(\Lambda^*) \neq \emptyset$.

Demonstração. *(i)* Vamos supor que $\Lambda \sim \langle 1,\, \mathfrak{j}^*\rangle$, logo existe um $\kappa \in \mathbb{C}^\times$ onde o par κ, $\mathfrak{j}^*\cdot\kappa$ é uma base normalizada de Λ, logo podemos escrever:

$$\mathfrak{j}^* = \frac{\mathfrak{j}^*\cdot\kappa}{\kappa} \in \mathfrak{J}(\Lambda).$$

Reciprocamente, se $\mathfrak{j}^* \in \mathfrak{J}(\Lambda)$ então existem α, β tais que $\mathfrak{j}^* = \frac{\beta}{\alpha}$ e $\Lambda = \langle \alpha,\, \beta\rangle$. Como

$$\Lambda = \langle \alpha\cdot 1,\, \alpha\cdot {}^{\beta}\!/_{\alpha}\rangle,$$

segue que $\Lambda \sim \langle 1,\, \mathfrak{j}^*\rangle$.

(*ii*) Suponha que $\Lambda = \langle \alpha, \beta \rangle \sim \Lambda^* = \langle \alpha^*, \beta^* \rangle$, logo existe $\kappa \in \mathbb{C}^\times$ tal que

$$\begin{cases} \alpha^* = \kappa \cdot \alpha \\ \beta^* = \kappa \cdot \beta \end{cases} \implies \frac{\beta^*}{\alpha^*} = \frac{\beta}{\alpha} \implies \mathfrak{J}(\Lambda^*) = \mathfrak{J}(\Lambda).$$

Por noções de conjuntos, se $\mathfrak{J}(\Lambda) = \mathfrak{J}(\Lambda^*)$, a interseção deles será diferente do vazio. Agora, seja $\mathfrak{j} \in \mathfrak{J}(\Lambda) \cap \mathfrak{J}(\Lambda^*)$, logo pelo item (*i*):

$$\Lambda \sim \langle 1, \mathfrak{j} \rangle \sim \Lambda^*.$$

□

Através do lema acima, surge uma maneira de encontrar redes equivalentes por meio dos números complexos $\mathfrak{j} \in \mathfrak{J}(\Lambda)$ e $\mathfrak{j}^* \in \mathfrak{J}(\Lambda^*)$ sem relacionar às redes, mas sim seus $\mathfrak{J}$–conjuntos; isso se resume, com os resultados do Lema 1.5.2, à:

$$\Lambda = \langle \alpha, \beta \rangle \sim \langle \alpha^*, \beta^* \rangle = \Lambda^* \iff \mathfrak{j} = \frac{\beta}{\alpha} = \frac{\beta^*}{\alpha^*} = \mathfrak{j}^*. \tag{1.7}$$

Note que em particular, tomando $m \in \mathbb{Z}$,

$$\begin{cases} a = d = 1 \\ b = 0 \\ c = m \end{cases} \quad \text{e} \quad \begin{cases} a = d = 0 \\ b = 1 \\ c = -1 \end{cases}$$

temos respectivamente:

$$\mathfrak{j} + m, \ -\mathfrak{j}^{-1} \in \mathfrak{J}(\Lambda).$$

Lema 1.5.3. *Seja Λ uma rede complexa, então para todo elemento $\mathfrak{j} \in \mathfrak{J}(\Lambda)$, o conjunto:*

$$\{im(\mathfrak{j}^*); \ \mathfrak{j}^* \in \mathfrak{J}(\Lambda), \ im(\mathfrak{j}^*) > im(\mathfrak{j})\}$$

é finito.

Demonstração. Pelas equações (1.5) e (1.6) temos que

$$im(\mathfrak{j}^*) = im\left(\frac{c + d\mathfrak{j}}{a + b\mathfrak{j}}\right) = \frac{1}{|a + b\mathfrak{j}|^2} \cdot im(\mathfrak{j})$$

logo

$$im(\mathfrak{j}^*) > im(\mathfrak{j}) \iff |a + b\mathfrak{j}| < 1,$$

e o resultado segue do fato de existirem um número finito de inteiros a, b tais que $-1 < a + b\mathfrak{j} < 1$.

□

O conjunto $\{im(\mathfrak{j});\, \mathfrak{j} \in \mathfrak{J}(\Lambda)\}$ é infinito, mas o Lema 1.5.3 nos diz que esse conjunto possui um máximo. Basta tomar qualquer $\mathfrak{j}_1 \in \mathfrak{J}(\Lambda)$ e observar que existe somente uma quantidade finita de $\mathfrak{j} \in \mathfrak{J}(\Lambda)$ tais que $im(\mathfrak{j}) > im(\mathfrak{j}_1)$. Seja $\mathfrak{j} \in \mathfrak{J}(\Lambda)$ um elemento com parte imaginária máxima, então nesse caso devemos ter $|\mathfrak{j}| \geq 1$, caso contrário, teríamos, com $\mathfrak{j} = x + yi$,

$$-\mathfrak{j}^{-1} = -\frac{x - yi}{x^2 + y^2} = \frac{-x}{x^2 + y^2} + \frac{y}{x^2 + y^2} i \in \mathfrak{J}(\Lambda)$$

e

$$im(-\mathfrak{j}^{-1}) = \frac{y}{x^2 + y^2} > y = im(\mathfrak{j}).$$

Observe também que se $\mathfrak{j} \in \mathfrak{J}(\Lambda)$, é sempre possível escrever $re(\mathfrak{j}) = x + \theta$ com $x \in \mathbb{Z}$ e $|\theta| \leq 1/2$. Assim $\mathfrak{j} - x \in \mathfrak{J}(\Lambda)$ possui a mesma parte imaginária, mas com parte real menor possível.

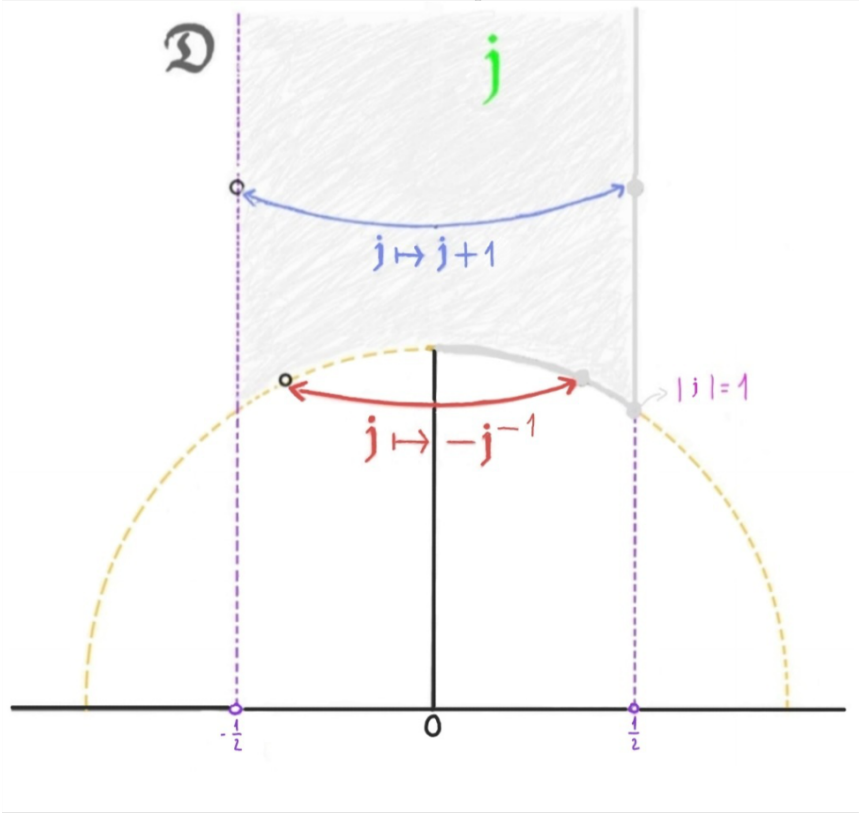
1.5.2 j-invariantes

O ***domínio fundamental*** é uma região definido por $\mathfrak{D} \subset \mathbb{C}$ onde:

$$\begin{aligned}
\mathfrak{D} \;=\; & \left\{ z \in \mathbb{C};\, im(z) > 0,\, |re(z)| < \frac{1}{2},\, |z| > 1 \right\} \\
& \bigcup \left\{ z \in \mathbb{C};\, im(z) > 0,\, 0 \leq re(z) < \frac{1}{2},\, |z| = 1 \right\} \\
& \bigcup \left\{ z \in \mathbb{C};\, im(z) \geq \frac{\sqrt{3}}{2},\, re(z) = \frac{1}{2},\, |z| > 1 \right\}.
\end{aligned}$$

Note que esta região $\mathfrak{D}$ possui muitos detalhes em seus limitantes e isso torna as exceções em [18, pg. 86] equivalentes sob a ação do grupo $SL_2(\mathbb{Z})$ à um único ponto $\mathfrak{j}$. Assim a interpretação desses pontos sobre $\mathfrak{D}$ são:

Figura 1.1: Domínio Fundamental sobre $SL_2(\mathbb{Z})$
Fonte: Elaborada pelo autor.



Lema 1.5.4. *Para uma rede complexa Λ, então*

$$\mathfrak{J}(\Lambda) \cap \mathfrak{D} = \{\mathrm{j}_\Lambda\},$$

onde j_Λ é dita a j*-invariante da rede Λ.*

Demonstração. Existência: Como vimos, o conjunto $\mathfrak{J}(\Lambda) \cap \mathfrak{D}$ é não vazio, já que se $|\mathrm{j}| = 1$ e $re(\mathrm{j}) < 0$, então basta tomar $-\mathrm{j}^{-1} \in \mathfrak{J}(\Lambda)$ com $im(\mathrm{j}) = im(-\mathrm{j}^{-1})$, $re(-\mathrm{j}^{-1}) \geq 0$ e $|-\mathrm{j}^{-1}| = 1$.

Unicidade: Vamos agora provar que essa interseção contém exatamente um elemento. Suponha que existam, sem perda de generalidade, dois elementos j_0 e j_1 tais que $im(\mathrm{j}_0) \geq im(\mathrm{j}_1)$. Por hipótese, existem inteiros a, b, c, d com $ad - bc = 1$ tal que

$$\mathrm{j}_0 = \frac{c + d\mathrm{j}_1}{a + b\mathrm{j}_1}$$

e então

$$im(\mathrm{j}_0) = \frac{1}{|a + b\mathrm{j}_1|^2} \cdot im(\mathrm{j}_1) \implies |a + b\mathrm{j}_1| \leq 1.$$

Entretanto, como $\mathrm{j}_1 \in \mathfrak{D}$ então $im(\mathrm{j}_1) \geq \frac{\sqrt{3}}{2}$, assim para $\mathrm{j}_1 = x + y\frac{\sqrt{3}}{2}i$ devemos ter $y \geq 1$, logo

$$1 \geq |a + b\mathfrak{j}_1|^2 = (a + bx)^2 + \left(yb\frac{\sqrt{3}}{2}\right)^2 \geq y^2b^2\frac{3}{4} \geq b^2\frac{3}{4}.$$

Portanto

$$1 \geq |a + b\mathfrak{j}_1| \geq \frac{\sqrt{3}}{2} \cdot |b| \geq \frac{\sqrt{3}}{2} \cdot b.$$

Como $b \in \mathbb{Z}$, segue que

$$|a + b\mathfrak{j}_1| \leq 1 \text{ somente quando } b = \{-1,\, 0,\, 1\}.$$

- Para $b = 0$ temos $a = \pm 1$, como $ad - bc = 1$ devemos ter que $a = d$, logo

$$\mathfrak{j}_0 = \mathfrak{j}_1 \pm c.$$

Desde que $\mathfrak{D}$ não possua elementos distintos de um inteiro não-nulo, conclui-se que

$$\mathfrak{j}_0 = \mathfrak{j}_1. \tag{1.8}$$

- Para $b = 1$ temos $|a + \mathfrak{j}_1| \leq 1$ e $|a + \mathfrak{j}_1| > \frac{\sqrt{3}}{2}$.

Tomando $\mathfrak{j}_1 = x + iy$ então $a + \mathfrak{j} = (x + a) + iy$ assim:

$$(x + a)^2 + y^2 \leq 1 \implies a = 0 \implies c = -1$$

logo

$$\mathfrak{j}_0 = \frac{-1 + d\mathfrak{j}_1}{\mathfrak{j}_1} = -{\mathfrak{j}_1}^{-1} + d. \tag{1.9}$$

Para $\mathfrak{j}_1 = z + iw$ tal que $z^2 + w^2 \geq 1$, $|z| \leq \frac{1}{2}$ e $w \geq \frac{\sqrt{3}}{2}$

$$-{\mathfrak{j}_1}^{-1} = \frac{-z}{z^2 + w^2} + i\frac{w}{z^2 + w^2}$$

temos: o que nos dá

$$|-{\mathfrak{j}_1}^{-1}| = \frac{z^2 + w^2}{z^2 + w^2} = 1.$$

Caso $z^2 + w^2 > 1$, temos que $|re(-{\mathfrak{j}_1}^{-1})| < \frac{1}{2}$ e $0 < im(-{\mathfrak{j}_1}^{-1}) < \frac{\sqrt{3}}{2}$, então

$$-{\mathfrak{j}_1}^{-1} \in \mathfrak{D}.$$

Caso $z^2 + w^2 = 1$, temos que $|re(-{\mathfrak{j}_1}^{-1})| \leq \frac{1}{2}$ e $im(-{\mathfrak{j}_1}^{-1}) = \frac{\sqrt{3}}{2}$, então

$$-{\mathfrak{j}_1}^{-1} \in \mathfrak{D}.$$

Portanto da equação (1.9), utilizando-se do mesmo argumento para concluir a equação (1.8), implica que

$$\mathfrak{j}_0 = -{\mathfrak{j}_1}^{-1}.$$

- Para $b = -1$, recai sob os mesmos passos do item $b = 1$, e o resultado segue.

□

Como resultado deste último lema, é possivel concluir que a caracterização de uma rede complexa $\langle 1, \mathrm{j}_\Lambda \rangle$ a partir de um único elemento do domínio fundamental é equivalente à uma outra rede complexa qualquer. Logo, um algorítmo é determinado para se encontrar essa j-invariante, assim:

Proposição 1.5.1. *Seja Λ uma rede e fixado $\mathrm{j} \in \mathfrak{J}(\Lambda)$. Então j_Λ pode ser obtido através do algorítmo:*

(1) Escolha $\mathrm{j}_0 = \mathrm{j}$ e $k = 0$.

(2) Seja $\mathrm{j}_{k+1} = \mathrm{j}_k + m$ para um único $m \in \mathbb{Z}$ tal que

$$-\frac{1}{2} < re(\mathrm{j}_k + m) \leq \frac{1}{2}.$$

(3) Se $\mathrm{j}_{k+1} \in \mathfrak{D}$, então $\mathrm{j}_\Lambda = \mathrm{j}_{k+1}$. Caso contrário, tome $\mathrm{j}_{k+2} = -\frac{1}{\mathrm{j}_{k+1}}$

(4) Se $\mathrm{j}_{k+2} \in \mathfrak{D}$, então $\mathrm{j}_\Lambda = \mathrm{j}_{k+2}$. Caso contrário, então retorne ao passo (2), substituindo k por $k + 2$.

Demonstração. Ver [19, pg. 13].

□

1.5.3 Multiplicação Complexa (MC)

Os ideais de corpos quadráticos imaginários podem ser interpretados como redes no plano complexo possuindo uma propriedade chamada de multiplicação complexa, a saber:

Definição 1.5.4. *Dado $\rho \in \mathbb{C} \setminus \mathbb{Z}$, é dito que Λ é uma rede complexa com **multiplicação complexa** por ρ se $\rho\Lambda \subset \Lambda$, ou seja, quando $\rho\Lambda$ é uma subrede de Λ. Nesse caso dizemos que Λ é rede com $\boldsymbol{MC}_\rho$.*

Lema 1.5.5. *Seja Λ uma rede complexa com MC_ρ, então*

$$\rho = \frac{X \pm \sqrt{X^2 - 4Y}}{2}$$

com $X, Y \in \mathbb{Z}$ tal que $X^2 - 4Y < 0$. Mais ainda, caso X par:

$$\rho = \sqrt{\left(\frac{X^2}{2} - Y\right)};$$

e para X ímpar:

$$\rho = \frac{1}{2} \cdot \left(1 + \sqrt{X^2 - 4Y}\right),$$

com $X^2 - 4Y \equiv 1 \pmod 4$.

Demonstração. Para esta primeira parte da prova, temos que dados α, β uma base de Λ, é fato que $\rho \cdot \alpha$, $\rho \cdot \beta \in \Lambda$ (por ter MC_ρ). Assim, existem inteiros não nulos s, t, u, v tais que:

$$\left\{ \begin{array}{rcl} \rho \cdot \alpha & = & \alpha \cdot s + \beta \cdot t \\ \rho \cdot \beta & = & \alpha \cdot u + \beta \cdot v \end{array} \right. \implies \left\{ \begin{array}{rcl} \rho & = & s + \frac{\beta}{\alpha} \cdot t \\ \\ \rho & = & v + \frac{\alpha}{\beta} \cdot u \end{array} \right. ;$$

manipulando as duas equações acima, obtemos:

$$\frac{\beta}{\alpha} = \frac{\rho - s}{t} = \frac{u}{\rho - v}$$

$$\implies$$

$$\rho^2 - (s + v) \cdot \rho + (sv - ut) = 0$$

logo, basta tomar $X = s + v$ e $Y = sv - ut$ e encontrar as raízes desta função quadrática, e o resultado segue.

Observe que se

$$\rho\alpha = \alpha a + \beta b, \quad \rho\beta = \alpha a^* + \beta b^*$$

então se verifica uma propriedade de que

$$\langle (\rho + c)\alpha,\, (\rho + c)\beta \rangle$$

é também uma subrede de $\langle \alpha,\, \beta \rangle = \Lambda$ para todo $c \in \mathbb{Z}$; assim:

Supondo $X = 2k$,

$$X^2 - 4Y = \frac{4}{4} \cdot X^2 - 4Y = 4\left[\left(\frac{X}{2}\right)^2 - Y\right]$$

$$\implies$$

$$\rho = \frac{2k \pm 2\sqrt{\left(\frac{X}{2}\right)^2 - Y}}{2} = k \pm \sqrt{\left(\frac{X}{2}\right)^2 - Y},\ \forall k \in \mathbb{Z}.$$

Supondo $X = 2l + 1$ tal que $l \in \mathbb{Z}$,

$$X^2 - 4Y = 4l^2 + 4l + 1 - 4Y;$$

note que $X \equiv 1 \pmod 4$, assim $X^2 - 4Y = 4m + 1$ para todo $m \in \mathbb{Z}$, então

$$\rho = \frac{2l + 1 \pm \sqrt{4m+1}}{2} = l + \frac{1 \pm \sqrt{4m+1}}{2}.$$

Pela propriedade de multiplicação complexa citada no início da demonstração, o resultado se vale em ambos os casos, portanto o lema está provado.

□

Lembrando que para o anel $\mathcal{O}_{-n}$, sua base integral é $\{1, \beta_{-n}\}$ com

$$\beta_{-n} = \sqrt{-n} \text{ se } n \equiv 1, 2 \pmod 4$$

ou

$$\beta_{-n} = \tfrac{1+\sqrt{-n}}{2} \text{ se } n \equiv 3 \pmod 4.$$

Nos restringimos a estudar redes com β_{-n} nesses casos específicos; sendo assim, vamos supor que $\beta_{-n} = \sqrt{-n}$ e $n \equiv 1, 2 \pmod 4$ e que Λ tenha $MC_{\beta_{-n}}$. Nesse caso,

$$\sqrt{-n} \cdot \Lambda \subseteq \Lambda. \tag{1.10}$$

Se $\Lambda^* \sim \Lambda = \langle \alpha, \beta \rangle$, então existe $\rho \in \mathbb{C}^\times$ tal que $\Lambda^* = \langle \rho\alpha, \rho\beta \rangle$. Observe que

$$\beta_{-n} \cdot \Lambda^* = \langle \beta_{-n} \cdot \rho\alpha, \beta_{-n} \cdot \rho\beta \rangle = \langle \rho(\beta_{-n}\alpha), \rho(\beta_{-n}\beta) \rangle .$$

Por $\beta_{-n} \cdot \alpha, \beta_{-n} \cdot \beta \in \Lambda$ (pela equação (1.10)), segue que $\sqrt{-n} \cdot \Lambda^* \subseteq \Lambda^*$, ou seja, Λ^* é também $MC_{\beta_{-n}}$.

Como toda rede complexa é equivalente a uma única rede $\langle 1, \mathfrak{j} \rangle$ com $\mathfrak{j} \in \mathfrak{D}$, encontrar redes com multiplicação complexa β_{-n} equivale a encontrar $\mathfrak{j} \in \mathfrak{D}$ tais que

$$\beta_{-n} \cdot \langle 1, \mathfrak{j} \rangle \subseteq \langle 1, \mathfrak{j} \rangle .$$

Considerando $\beta_{-n} = \sqrt{-n}$, nesse caso $\sqrt{-n} \cdot \langle 1, \mathfrak{j} \rangle \subseteq \langle 1, \mathfrak{j} \rangle$ implica que existem $a, b, c, d \in \mathbb{Z}$ tais que

$$\sqrt{-n} = -a + b\mathfrak{j}$$

e

$$\sqrt{-n} \cdot \mathfrak{j} = c + d\mathfrak{j}$$

logo,

$$\mathfrak{j} = \frac{a + \sqrt{-n}}{b} \implies \frac{ad + n}{b} + \frac{d - a}{b}\sqrt{-n} = c.$$

Como $c \in \mathbb{Z}$, temos que $d = a$, concluindo que

$$c = \frac{a^2 + n}{b}. \tag{1.11}$$

Para o caso $\beta_{-n} = \frac{1+\sqrt{-n}}{2}$, note que para encontrarmos a $\mathfrak{j}$–invariante (que é única), devemos considerar também que

$$\sqrt{-n} = -a + b\mathfrak{j}$$

então:

$$\beta_{-n} \cdot \mathfrak{j} = c + d\mathfrak{j}$$
$$\Longrightarrow$$
$$\left(\frac{1+\sqrt{-n}}{2}\right)\left(\frac{a+\sqrt{-n}}{b}\right) = c + d\left(\frac{a+\sqrt{-n}}{b}\right)$$
$$\Longrightarrow$$

$$\begin{aligned} c &= \frac{a+\sqrt{-n}+a\sqrt{-n}-n}{2b} - \frac{da+d\sqrt{-n}}{b} \\ &= \frac{a-2da-n}{2b} + \frac{a+1-2d}{2b}\sqrt{-n}. \end{aligned}$$

Como $c \in \mathbb{Z}$, devemos ter $a+1-2d = 0$, concluindo assim que a é ímpar, disso:

$$c = -\frac{n+a^2}{2b}; \tag{1.12}$$

Por $n \equiv 3 \pmod 4$ e $a = 2d-1$, pela equação (1.12), para algum $k \in \mathbb{Z}$ temos que:

$$\begin{aligned} c &= -\frac{4k+3+(4d^2-4d+1)}{2b} \\ &= -\frac{2(k+d^2-d)+2}{b}, \end{aligned}$$

resultando em que b é par; portanto:

Teorema 1.5.1. *Seja* $\mathfrak{j} \in \mathfrak{D}$ *e* $n \equiv 1, 2 \pmod 4$. *Toda rede com* $MC_{\sqrt{-n}}$ *é equivalente a uma única rede* $\langle 1, \mathfrak{j}\rangle$ *onde* $\mathfrak{j} = \frac{a+\sqrt{-n}}{b}$ *tal que:*

(1) $a, b \in \mathbb{Z}$;

(2) $0 < b \leq 2\sqrt{\frac{n}{3}}$;

(3) $-b < 2a \leq b$;

(4) $a^2 + n \geq b^2$ *(e* $a \geq 0$ *se* $a^2 + n = b^2$*)*;

(5) $b \mid a^2 + n$.

Demonstração. Os casos *(1)* e *(5)* foram vistos acima na equação (1.11). Como $\frac{a+\sqrt{-n}}{b} \in \mathfrak{D}$, segue que

$$\left|\frac{a}{b}\right| \leq -\frac{1}{2}$$

e

$$\left|\frac{a+\sqrt{-n}}{b}\right| \geq 1$$

ou seja,

$$\frac{a^2}{b^2} + \frac{n}{b^2} \geq 1,$$

e isso resulta os casos *(3)* e *(4)*.

Observe que, por $2a \geq b$, então $a^2 \leq \frac{b^2}{4}$. Assim,

$$b^2 \leq a^2 + n \leq \frac{b^2}{4} + n \implies n \geq \frac{3b^2}{4},$$

o que nos dá o item *(2)*.

□

Teorema 1.5.2. *Seja* $\mathfrak{j} \in \mathfrak{D}$ *e* $n \equiv 1, 2 \pmod 4$. *Toda rede com* $MC_{\frac{1+\sqrt{-n}}{2}}$ *é equivalente a uma única rede* $\langle 1, \mathfrak{j}\rangle$ *onde* $\mathfrak{j} = \frac{a+\sqrt{-n}}{b}$ *tal que:*

(1) a *ímpar e* b *par*;

(2) $0 < b \leq 2\sqrt{\frac{n}{3}}$;

(3) $-b < 2a \leq b$;

(4) $a^2 + n \geq b^2$ *(e* $a \geq 0$ *se* $a^2 + n = b^2$*)*;

(5) $2b \mid a^2 + n$.

Demonstração. Pelas contas desenvolvidas que resultam na equação (1.12) e utilizando raciocínio similar ao Teorema 1.5.1, os casos *(1)* à *(5)* estão provados.

□

Através desses dois últimos resultados, Weston aborda o grupo das classes como um subconjunto de $\mathbb{C}$ formado por elementos da forma $\frac{a+\sqrt{-n}}{b}$. Como já fora definido $\mathcal{C}l(-n)$, resta dar uma conclusão sob o tamanho desse grupo, e a resposta para esse questionamento é a compatibilidade entre ideais de $\mathcal{O}_{-n}$ e redes equivalentes com $MC_{\sqrt{-n}}$ ou $MC_{\frac{1+\sqrt{-n}}{2}}$.

Teorema 1.5.3. *O grupo das classes $\mathcal{C}l(-n)$ é finito.*

Demonstração. A finitude é dada pela quantidade restrita de pares de inteiros $(a,\, b)$ satifazendo as condições *(1) – (5)* dos Teoremas 1.5.1 e 1.5.2 para algum inteiro positivo livre de quadrados n.

□

Assim, a representação da quantidade de redes equivalentes com $MC_{\sqrt{-n}}$ ou $MC_{\frac{1+\sqrt{-n}}{2}}$ é dada por $|\mathcal{C}l(-n)|$ denominada o ***número de classes*** (denotada $h(-n)$); uma exemplificação é:

Exemplo 1.5.1.

Para determinar a ordem do grupo $\mathcal{C}l(-26)$ usamos o Teorema 1.5.1. Por *(2)* temos que $1 \leq b \leq 2\sqrt{26/3} = 5,89$, logo $1 \leq b \leq 5$. Calculando as possiblidades para a mediante o item *(3)* e, com uma certa demanda de tempo para se verificar os itens *(4)* e *(5)*, concluímos que os pares válidos são: $(0,\, 1)$, $(0,\, 2)$, $(1,\, 3)$, $(-1,\, 3)$, $(2,\, 5)$, $(-2,\, 5)$. Assim, os elementos j's associados aos pares formam o conjunto

$$\left\{\sqrt{-26},\, \frac{\sqrt{-26}}{2},\, \frac{1+\sqrt{-26}}{3},\, \frac{-1+\sqrt{-26}}{3},\, \frac{2+\sqrt{-26}}{5},\, \frac{-2+\sqrt{-26}}{5}\right\}.$$

Logo, $h(-26) = 6$.

Observação 1.5.1.

Segundo o Teorema 1.5.1, as redes complexas equivalentes com $MC_{\sqrt{-26}}$, a partir da j-invariante relacionada aos pares $(a,\, b)$, são respectivamente:

$$\left\langle 1,\, \sqrt{-26}\right\rangle,\, \left\langle 2,\, \sqrt{-26}\right\rangle,\, \left\langle 3,\, 1+\sqrt{-26}\right\rangle,$$

$$\left\langle 3,\, -1+\sqrt{-26}\right\rangle,\, \left\langle 5,\, 2+\sqrt{-26}\right\rangle,\, \left\langle 5,\, -2+\sqrt{-26}\right\rangle.$$

Portanto, a relação entre os ideais do grupo das classes com o conjunto de redes equivalentes com multiplicação complexa β_{-n} é dado por:

Proposição 1.5.2. *Seja $\mathcal{I} \subset \mathcal{O}_{-n}$, quando considerado como um subconjunto de $\mathbb{C}$, o ideal é uma rede complexa com $MC_{\beta_{-n}}$. Mais ainda, m, $a + b\sqrt{-n}$ é uma base de $\mathcal{I}$ se:*

- *m é o menor inteiro positivo de $\mathcal{I}$;*

- $a + b\sqrt{-n} \in \mathcal{I}$ *com o coeficiente positivo mínimo de* $\sqrt{-n}$.

  Em particular, se $n \equiv 3 \pmod 4$ *então* $b \in \frac{1}{2}\mathbb{Z}$.

Demonstração. Como o ideal $\mathcal{I} \subset \mathcal{O}_{-n}$, então o mesmo é fechado para a multiplicação por $\beta_{-n} \in \mathcal{O}_{-n}$, logo $\mathcal{I}$ possui $\mathrm{MC}_{\beta_{-n}}$.

Queremos provar que $\mathcal{I}$ é uma rede, então basta mostrar que:

$$\mathcal{I} = \{mx + (a + b\sqrt{-n})y;\ x,\ y \in \mathbb{Z}\}.$$

Para a primeira inclusão de $\mathcal{I} \subset \{mx + (a + b\sqrt{-n})y;\ x,\ y \in \mathbb{Z}\}$; supondo $c + d\sqrt{-n} \in \mathcal{I}$, é possível escolher $y \in \mathbb{Z}$ tal que $0 \leq d - by < b$ onde

$$(c + d\sqrt{-n}) - (a + b\sqrt{-n}) \cdot y = (c - ay) + (d - by) \cdot \sqrt{-n} \in \mathcal{I}.$$

Tomando b como um elemento minimal, segue que $d = by$; assim, em particular

$$(c + d\sqrt{-n}) - (a + b\sqrt{-n}) \cdot y = c - ay \in \mathcal{I},$$

é um inteiro divisível por m, então existe um $x \in \mathbb{Z}$ tal que $c - ay = mx$ portanto

$$c + d\sqrt{-n} = mx + (a + b\sqrt{-n})y \in \mathcal{I}.$$

Para a outra inclusão, pela definição de ideais, toda combinação linear de m e $a + b\sqrt{-n}$ pertence à $\mathcal{I}$.

O caso particular segue devido a paridade de b, ou seja, por $n \equiv 3 \pmod 4$:

$$\mathcal{O}_{-n} = \left\{a + b\sqrt{-n};\ 2a,\ 2b \in \mathbb{Z},\ 2a \equiv 2b \pmod 2\right\}.$$

□

É através da similaridade de ideais que podemos obter uma correspondência, já que estamos tratando de redes e multiplicações complexas, com a equivalência de redes, ou seja, classes de redes complexas se conectam com classes de ideais.

Lema 1.5.6. *Temos que* $\mathcal{I}$ *e* $\mathcal{J}$ *são similiares se e somente se são redes equivalentes. Em particular:*

$$\mathcal{I} \simeq \mathcal{J} \iff \mathrm{j}_{\mathcal{I}} = \mathrm{j}_{\mathcal{J}},$$

onde $\mathrm{j}_{\mathcal{I}}$ *e* $\mathrm{j}_{\mathcal{J}}$ *denotam a* j*–invariante das redes (vistas como ideais)* $\mathcal{I}$ *e* $\mathcal{J}$ *rescpectivamente.*

Demonstração. Para a primeira implicação, seja $\mathcal{I} \simeq \mathcal{J}$, pela definição existem γ, $\eta \in \mathcal{O}_{-n}$ não-nulos onde

$$(\gamma) \cdot \mathcal{I} = (\eta) \cdot \mathcal{J} \implies \mathcal{I} = \frac{\eta}{\gamma} \cdot \mathcal{J},$$

que é a definição de $\mathcal{I}$ e $\mathcal{J}$ serem equivalentes.

Por outro lado, caso $\mathcal{I}$ e $\mathcal{J}$, vistos como redes, são equivalentes, logo por definição existe um $\gamma \in \mathbb{C}^{\times}$ tal que $\mathcal{I} = \gamma \cdot \mathcal{J}$. Fixado um elemento não nulo $x \in \mathcal{J}$, temos que $\gamma \cdot x \in \mathcal{I}$, e se ainda, $\mathcal{I}$ e $\mathcal{J}$ sejam vistos como ideais de $\mathcal{O}_{-n}$, segue que

$$\frac{\gamma \cdot x}{x} \in \mathbb{Q}(\sqrt{-n}).$$

Assim, conseguimos encontrar um inteiro a tal que $a \cdot \gamma \in \mathcal{O}_{-n}$, logo

$$\mathcal{I} = (\gamma) \cdot \mathcal{J} \iff (a) \cdot \mathcal{I} = (a \cdot \gamma) \cdot \mathcal{J},$$

onde a, $a \cdot \gamma \in \mathcal{O}_{-n}$; portanto $\mathcal{I} \simeq \mathcal{J}$.

O caso particular segue diretamente da equação (1.7), assim

$$\mathcal{I} \simeq \mathcal{J} \iff \mathcal{I} \sim \mathcal{J} \iff \mathfrak{j}_{\mathcal{I}} = \mathfrak{j}_{\mathcal{J}}.$$

□

Corolário 1.5.1. *Se para uma rede complexa qualquer com $MC_{\beta_{-n}}$, a qual sua* j*-invariante é dada pelas condições dos Teoremas 1.5.1 e 1.5.2, então:*

$$\left\langle b, a + \sqrt{-n} \right\rangle \subset \mathcal{O}_{-n}.$$

Demonstração. Ver [19, pg. 40].

□

Ao detalhar o Exemplo 1.5.1, nota-se uma grande quantidade de passos até se determinar os pares (a, b) que satifazem os itens *(1) - (5)* do Teorema 1.5.1, e é de se esperar que à medida que n cresça, a dificuldade irá ser diretamente proporcional. Nisso, Weston em suas notas, apresenta $h(-n)$, a princípio, vinculada à uma função específica (definida e detalhada no segundo capítulo relacionando símbolos de Jacobi e séries numéricas), e a maneira em que esta função assume distintos valores dado n, uma "constante" se mostra candidata à "corrigir" uma equação se relacionando com a quantidade de redes com $MC_{\beta_{-n}}$ em consequência do conjunto finito $\mathcal{C}l(-n)$, demonstrado no Teorema 1.5.3.

A seguir, observamos uma tabela de verificação onde à medida que os valores do inteiro positivo livre de quadrados n (com $n \equiv 1, 2 \pmod 4$) aumentam consideravelmente, $h(-n)$ é "notavelmente próximo à um número inteiro" (Weston [19, pg. 19]):

Figura 1.2: Tabela de amostragem para $n \equiv 1,\ 2 \pmod 4$
Fonte: Tom Weston, editada pelo autor.

$-n$	$h(-n)$
2	1,00
6	2,00
10	2,00
13	2,00
14	4,00
17	4,00
21	4,00
22	2,00
26	6,00
29	6,00
30	4,00
15701	132,00
2905509	2187,92

1.5.4 Pontos de rede de um valor absoluto limitado

Seja $\Lambda = \langle \alpha, \beta \rangle$ uma rede complexa e $\mathcal{P}$ o paralelogramo de vértices na origem, α, β e $\alpha+\beta$, onde denota-se por A a área de $\mathcal{P}$. Ao fixarmos $t > 0$, podemos estimar quantos pontos de Λ possuem norma de no máximo t, o que significa ter:

$$B_t = \big\{ z \in \mathbb{C}; |z| \leq t \big\},$$

e assim encontar a quantidade de pontos (ou tamanho) de $\Lambda \cap B_t$.

A ideia do lema a seguir, é tomar um paralelogramo $\mathcal{P}$ e outros paralelogramos com vértices $\lambda \in \Lambda$, onde $\mathcal{P}_\lambda$ denota a translação de $\mathcal{P}$ por qualquer λ (que são todos congruentes a $\mathcal{P}$), cobrindo a área de B_t e encontrar a quantidade aproximada de $\pi \cdot t^2/A$ translações, consequentemente $\pi \cdot t^2/A$ pontos λ's estimando tal erro limitado a área de B_t, assim:

Lema 1.5.7. *Existe uma constante $\mathcal{L}$ dependendo somente de Λ tal que*

$$\left| \#\Lambda \cap B_t - \frac{\pi t^2}{A} \right| \leq \mathcal{L} \cdot t.$$

Demonstração. Defina

$$\begin{aligned} Q_1(t) &= \#\{\lambda \in \Lambda;\ \mathcal{P}_\lambda \subseteq B_t\}; \\ Q_2(t) &= \#\{\lambda \in \Lambda \cap B_t\}; \\ Q_3(t) &= \#\{\lambda \in \Lambda;\ \mathcal{P}_\lambda \cap B_t \neq \varnothing\}. \end{aligned}$$

A partir das propriedades desses pontos definidos, alguns resultados intuitivos podem ser certamente deduzidos:

- os λ's estão em B_t caso $\mathcal{P}_\lambda$ esteja em B_t;
- $\mathcal{P}_\lambda$ intersecta B_t caso os λ's estejam em B_t;

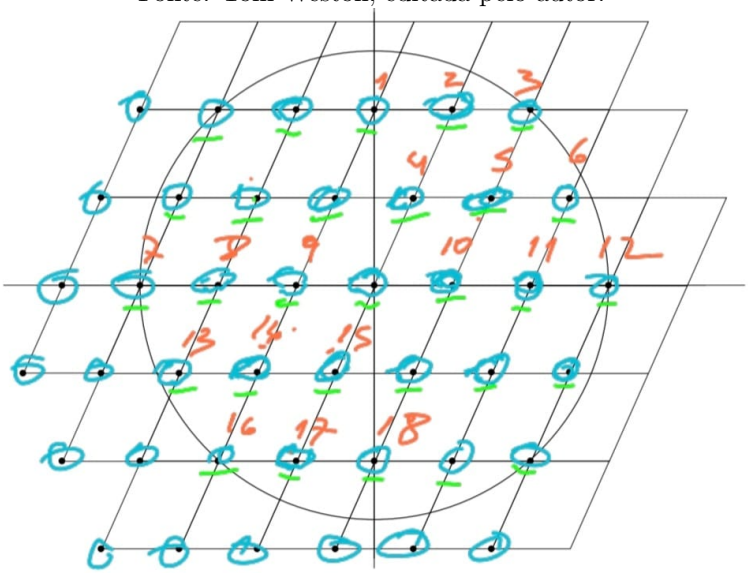
assim:

$$Q_1(t) \leq Q_2(t) \leq Q_3(t).$$

Para uma exemplificação dessas representações, considere a rede $\langle 2,\ 1+\sqrt{-5}\rangle$ e tome o parâmetro $t = 6$, assim:

Ilustramos $Q_1(6) = 18$, $Q_2(6) = 29$ e $Q_3(6) = 42$ dado por:

Figura 1.3: $\langle 2,\ 1+\sqrt{-5}\rangle \cap B_6$
Fonte: Tom Weston, editada pelo autor.



.

Feito isso, ainda que seja possível se estimar uma cota para $Q_1(t)$ e $Q_3(t)$, façamos alguns apontamentos importantes:

(i) devido a área de B_t ser dada por $\pi \cdot t^2$ a qual permite ter no máximo $\dfrac{\pi \cdot t^2}{A}$ translações disjuntas de $\mathcal{P}$, então

$$Q_1(t) \leq \frac{\pi \cdot t^2}{A};$$

(ii) devido às translações de $\mathcal{P}$ que intersectam B_t cubram todo B_t, então

$$\frac{\pi \cdot t^2}{A} \leq Q_3(t);$$

"Nada pode se afirmar em relação à $Q_2(t)$" (Weston, [19, pg. 21]), assim utilizaremos da diagonal maior d do paralelogramo $\mathcal{P}$ para solucionar tal inconsistencia de $Q_2(t)$.

(iii) $\forall \lambda \in \Lambda \cap B_t \implies \mathcal{P}_\lambda \subseteq B_{t+d} \implies Q_1(t) \leq Q_2(t+d) \leq \dfrac{\pi \cdot (t+d)^2}{A}$;

(iv) Se $\mathcal{P}_\lambda \cap B_{t-d} \neq \varnothing$ então $\mathcal{P}_\lambda \subseteq B_t$, logo

$$\frac{\pi \cdot (t-d)^2}{A} \leq Q_3(t-d) \leq Q_1(t).$$

A partir de (iii) e (iv),

$$\left| Q_2(t) - \frac{\pi \cdot t^2}{A} \right| \leq \frac{\pi}{A}(2td + d^2) \leq \mathcal{L} \cdot t$$

com $\mathcal{L} = \frac{\pi}{A}(2d + d^2)$.

□

A prova desse lema será primordial para o entendimento do resultado principal do segundo capítulo, conectando os ideais e as redes complexas (estudo algébrico/geométrico) com as séries de Dirichlet (estudo analítico).

Capítulo 2

Fórmula do Número das Classes

2.1 Conceitos Analíticos

Vamos introduzir as séries de Dirichlet para entender convergências de certas séries bem como produtos de Euler e encontrar seus limitantes para, ao final deste capítulo, compreender os caminhos para a fórmula principal da dissertação.

Definição 2.1.1. *Uma* ***série real de Dirichlet*** *é definida como uma função do tipo*

$$f(s) \stackrel{def}{=} \sum_{m=1}^{\infty} a_m \, m^{-s}$$

tais que $s \in \mathbb{R}$ *e* a_m *uma sequência de números reais.*

Proposição 2.1.1. *Se existem* $b, t \in \mathbb{R}_{>0}$ *tais que, para todo* $M \geq 1$

$$\left| \sum_{m=1}^{M} a_m \right| \leq bM^t$$

então a série de Dirichlet

$$f(s) = \sum_{m=1}^{\infty} a_m \, m^{-s}$$

converge para $s > t$ *com* $f(s)$ *sendo uma função contínua.*

Demonstração. Convergência:

Denotando

$$\mathfrak{A}_M = \sum_{m=1}^{M} a_m,$$

por hipótese temos que $|\mathfrak{A}_M|$ é limitada. Seja um inteiro $M \geq 1$ e fixado $s > t$, podemos rearranjar termos a quais se vale:

$$\sum_{m=M}^{M+R} a_m m^{-s} = \mathfrak{A}_{M+R} \cdot (M+R)^{-s} - \mathfrak{A}_{M-1} \cdot M^{-s} + \sum_{m=M}^{M+R-1} \mathfrak{A}_m \left(m^{-s} - (m+1)^{-s}\right)$$

$$\Longrightarrow$$

$$\left|\sum_{m=M}^{M+R} a_m m^{-s}\right| \leq b \cdot \left((M+R)^{t-s} + (M-1)^{t-s} + \sum_{m=M}^{M+R-1} m^t \left(m^{-s} - (m+1)^{-s}\right)\right).$$

Observe que o termo $m^{-s} - (m+1)^{-s}$ nos mostra que:

Tomando $g(x) = x^{-s}$, note que a função $g(x)$ é contínua no intervalo $[m,\, m+1]$ e derivável em $(m,\, m+1)$, pelo Teorema do Valor Médio temos que existe um número c, onde $0 < c < 1$ tal que

$$g(m+1) = g(m) + g'(m + c \cdot 1) \cdot 1$$

assim,

$$(m+1)^{-s} = m^{-s} + (-s)(m+c)^{-s-1} \implies m^{-s} - (m+1)^{-s} = s(m+c)^{-s-1} < s m^{-s-1};$$

feito isso, obtemos:

$$\begin{aligned}\left|\sum_{m=M}^{M+R} a_m m^{-s}\right| &\leq b \cdot \left((M+R)^{t-s} + (M-1)^{t-s} + s \cdot \sum_{m=M}^{M+R-1} m^{t-s-1}\right) \\ &\leq b \cdot \left((M+R)^{t-s} + (M-1)^{t-s} + s \cdot \sum_{m=M}^{\infty} m^{t-s-1}\right).\end{aligned}$$

Substituindo o somatório pela integral, temos:

$$\begin{aligned}\left|\sum_{m=M}^{M+R} a_m m^{-s}\right| &\leq b \cdot \left((M+R)^{t-s} + (M-1)^{t-s} + s \cdot \int_{M-1}^{\infty} m^{t-s-1}\right) \\ &\leq b \cdot \left((M+R)^{t-s} + (M-1)^{t-s} + \frac{s}{s-t} \cdot (M-1)^{t-s}\right) \\ &\leq b \cdot \left((M+R)^{t-s} + \frac{2s-t}{s-t} \cdot (M-1)^{t-s}\right).\end{aligned}$$

Como $s > t$, fazendo $M + R \longrightarrow \infty$:

$$\left|\sum_{m=M}^{\infty} a_m m^{-s}\right| \leq \frac{b(2s-t)}{s-t} \cdot (M-1)^{t-s} \tag{2.1}$$

assim, para $M \longrightarrow \infty$, da equação (2.1):

$$\left| \sum_{m=1}^{\infty} a_m m^{-s} \right| \longrightarrow 0$$

que se traduz na convergência de $\sum_{m=1}^{\infty} a_m m^{-s}$.

Continuidade:

Pela desigualdade triangular e da equação (2.1), para $M \geq 1$:

$$\begin{aligned} |f(r) - f(s)| &\leq \left| f(r) - \sum_{m=1}^{M} a_m m^{-r} \right| + \left| \sum_{m=1}^{M} a_m m^{-r} - \sum_{m=1}^{M} a_m m^{-s} \right| \\ &\quad + \left| \sum_{m=1}^{M} a_m m^{-s} - f(s) \right| \\ &= \left| \sum_{m=M+1}^{\infty} a_m m^{-r} \right| + \left| \sum_{m=M+1}^{\infty} a_m m^{-s} \right| + \left| \sum_{m=1}^{M} a_m m^{-r} - \sum_{m=1}^{M} a_m m^{-s} \right| \\ &\leq \frac{b(2r-t)}{r-t} \cdot M^{t-r} + \frac{b(2s-t)}{s-t} \cdot M^{t-s} + \left| \sum_{m=1}^{M} a_m m^{-r} - \sum_{m=1}^{M} a_m m^{-s} \right|. \end{aligned}$$

Dado $\epsilon > 0$ e fixando um $\tilde{s}$ tal que $t < \tilde{s} < s$, podemos encontrar um M grande o suficiente onde para todo $r > \tilde{s}$ temos:

$$\frac{b(2r-t)}{r-t} \cdot M^{t-r} + \frac{b(2r-t)}{r-t} \cdot M^{t-r} < \frac{2\epsilon}{3}.$$

Note que $\tilde{s}$ evita o caso em que $\frac{1}{r-t} \longrightarrow \infty$. Assim para todo $r > \tilde{s}$:

$$|f(r) - f(s)| \leq \frac{2\epsilon}{3} + \left| \sum_{m=1}^{M} a_m m^{-r} - \sum_{m=1}^{M} a_m m^{-s} \right|.$$

Por $\sum_{m=1}^{M} a_m m^{-r}$ ser uma função contínua de r, portanto é possível obter um δ com $0 < \delta < s - \tilde{s}$ tal que

$$\left| \sum_{m=1}^{M} a_m m^{-r} - \sum_{m=1}^{M} a_m m^{-s} \right| < \frac{\epsilon}{3}$$

para todo r com $|r - s| < \delta$.

Assim, existe um r onde obtemos $|f(r) - f(s)| < \epsilon$.

□

2.1.1 A função $\zeta(s)$

Definição 2.1.2. *Uma função $f(s)$ complexa definida para $s > t$, tal que*

$$\lim_{s\to t^+} f(s) = \infty \ e \ \lim_{s\to t^+} (s-t)f(s) = \mathcal{A} \neq 0,$$

*é dita ter um **pólo simples** em $s = t$, e $\mathcal{A}$ é dito ser o **resíduo** de $f(s)$ em $s = t$.*

Assim, a partir da definição de $f(s)$ é possivel se encontrar uma outra função, chamada "função Zeta de Riemann", quando $a_m = 1$ para todo $m \in \mathbb{N}$, sendo:

$$\zeta(s) \stackrel{def}{=} \sum_{m=1}^{\infty} m^{-s}.$$

Um resultado sobre a função Zeta de Riemann é que esta função possui um pólo simples em $s = 1$ com resíduo 1.

2.1.2 Produto de Euler

O resultado principal deste tópico é garantir que

$$\zeta(s) = \prod_p \left(1 - p^{-s}\right)^{-1}, \tag{2.2}$$

onde $s > 1$ e o produtório se dá sobre todos os números primos p, assim:

Definição 2.1.3. *Seja $\{a_m\}$ uma sequência de números reais, então:*

- *$\{a_m\}$ é dita **multiplicativa** se $a_{i\cdot j} = a_i \cdot a_j$ sempre que o $mdc(i, j) = 1$;*
- *$\{a_m\}$ é dita **completamente multiplicativa** se $a_{i\cdot j} = a_i \cdot a_j$ para todo i, j.*

Proposição 2.1.2. *(i) Se existe uma constante $b > 0$ em que $\sum_{m=1}^{M} |a_m| \leq bM$ com $M \in \mathbb{Z}_{>0}$ e $\{a_m\}$ sendo multiplicativa então, para $s > 1$:*

$$\sum_{m=1}^{\infty} a_m\, m^{-s} = \prod_p \left(\sum_{i=1}^{\infty} a_{p^i}\, p^{-is} \right).$$

(ii) Se ainda, a_m é completamente multiplicativa e $|a_p| \leq p$, então, para $s > 1$ temos:

$$\sum_{m=1}^{\infty} a_m\, m^{-s} = \prod_p \left(1 - a_p \cdot p^{-s}\right)^{-1}.$$

Demonstração. Primeiramente, fixamos $s > 1$. Assumindo que $a_m \geq 0$ a partir das hipóteses e utilizando a Proposição 2.1.1 a série $\sum a_m m^{-s}$ converge. Para $l \geq 1$ vamos denotar o conjunto

$$P_l = \{m \in \mathbb{Z}_{>0};\, p_k \mid m \ \text{com} \ 1 \leq k \leq s\}$$

onde p_k é o k-ésimo número primo, assim

$$\sum_{m \in P_l} a_m \cdot m^{-s}$$

é convergente pois é sub sequência de M, donde $\sum_m a_m m^{-s}$ é convergente.

Como todo elemento de P_l pode ser escrito unicamente na forma $p_1^{i_1} \cdots p_l^{i_l}$, e pela hipótese de a_m ser uma sequência multiplicativa, segue:

$$\begin{aligned}
\sum_{m \in P_l} a_m \cdot m^{-s} &= \sum_{i_1, \ldots, i_l \geq 0} a_{p_1^{i_1}} \cdots a_{p_l^{i_l}} \cdot \left(p_1^{i_1} \cdots p_l^{i_l}\right)^{-s} \\
&= \sum_{i_1, \ldots, i_l \geq 0} a_{p_1^{i_1}} \cdot p_1^{-i_1 s} \cdots a_{p_l^{i_l}} \cdot p_l^{-i_l s} \\
&= \prod_{j=1}^{l} \left(\sum_{i=0}^{\infty} a_{p_i^j} \cdot p_j^{-is} \right).
\end{aligned}$$

Ao denotar

$$\sum_{m \in P_l} a_m \cdot m^{-s} = p_l$$

e

$$\sum_{m}^{\infty} a_m \cdot m^{-s} = p$$

segue que ao fazer $l \longrightarrow \infty$ tem-se

$$p_l \longrightarrow p.$$

Logo os produtórios parciais $\prod_{j=1}^{l} \left(\sum_i^{\infty} a_{p_j^i} p_j^{-is} \right)$ irão convergir para

$$\prod_{p} \left(\sum_{i=1}^{\infty} a_{p_i^j} p_j^{-is} \right),$$

o que demonstra o item (i).

Caso a_m seja completamente multiplicativa e $a_{p^j} \leq p^j$ (retiramos o valor absoluto pelo mesmo motivo de convergência absoluta), temos que $a_{p_j} \cdot p_j^{-s} < 1$ logo

$$\begin{aligned}(1 - a_{p_j} \cdot p_j^{-s})^{-1} &= 1 + a_{p_j} \cdot p_j^{-s} + a_{p_j}^2 \cdot p_j^{-2s} + \cdots \\ &= 1 + a_{p_j} \cdot p_j^{-s} + a_{p_j^2} \cdot p_j^{-2s} + \cdots\end{aligned}$$

portanto

$$\sum_{m=1}^{\infty} a_m \, m^{-s} = \prod_p \left(1 - a_p \cdot p^{-s}\right)^{-1};$$

demonstrando o item (ii)

□

Uma consequência da proposição acima é que a função zeta, para $s > 1$, já que $\{a_m\}_{m\in\mathbb{N}} = 1$, é descrita pelo produto de Euler como:

$$\zeta(s) = \sum_{m=1}^{\infty} m^{-s} = \prod_p \left(1 - p^{-s}\right)^{-1}.$$

2.2 A relação entre $\left(\frac{-n}{m}\right)$ e $\chi_{-n}(m)$

Iniciamos esta seção com a seguinte definição: para a, m números inteiros positivos tais que o mdc$(a, m) = 1$, dizemos que a é um *resíduo quadrático módulo* m se existe $x \in \mathbb{Z}$ tal que $x^2 \equiv a \pmod{m}$, caso não exista, a é dito um *resíduo não quadrático.*

2.2.1 O símbolo de Legendre

Seja a um inteiro positivo e p um primo ímpar, o ***símbolo de Legendre*** é caracterizado por:

$$\left(\frac{a}{p}\right) = \begin{cases} -1 & \text{se } a \text{ não é um resíduo quadrático módulo } p; \\ 1 & \text{se } a \text{ é um resíduo quadrático módulo } p; \\ 0 & \text{se } p \mid a. \end{cases}.$$

Vamos estender esses resultados definindo:

$$\left(\frac{a}{-1}\right) = \begin{cases} 1 & \text{se } a \geq 0 \\ -1 & \text{se } a < 0 \end{cases}; \left(\frac{a}{2}\right) = \begin{cases} 1 & \text{se } n \equiv 1, 7 \pmod 8; \\ -1 & \text{se } n \equiv 3, 5 \pmod 8; \\ 0 & \text{se } 2 \mid -n. \end{cases} \tag{2.3}$$

Assim, algumas propriedades do símbolo de Legendre se fazem necessárias para relacioná-lo com o resultado desta seção.

Propriedade 2.2.1. *Para a, $b \in \mathbb{Z}$ não divisíveis por p, q primos positivos ímpares distintos, temos:*

(i) Critério de Euler: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$;

(ii) Função completamente multiplicativa: $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(iii) $\left(\frac{a^2}{p}\right) = 1$;

(iv) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \pmod 4; \\ -1 & \text{se } p \equiv 3 \pmod 4. \end{cases}$;

(v) $\left(\frac{2}{p}\right) = \begin{cases} -1 & \text{se } p \equiv 1, 7 \pmod 8; \\ 1 & \text{se } p \equiv 3, 5 \pmod 8. \end{cases}$;

(vi) $\left(\frac{3}{p}\right) = \begin{cases} -1 & \text{se } p \equiv 5, 7 \pmod{12}; \\ 1 & \text{se } p \equiv 1, 11 \pmod{12}. \end{cases}$;

(vii) Lei da Reciprociade Quadrática: $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

O item (*vii*) pode ser reescrito, em especial, como:

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{se } p \equiv q \equiv 3 \pmod 4; \\ \left(\frac{q}{p}\right) & \text{caso contrário.} \end{cases}$$

Para mais detalhes e demonstrações dessas propriedades, basta consultar as referências [2, Cap. 5] e [9, Cap. 5 Sec. 16]; em consequência de todos os resultados, a partir daqui, vamos considerar $a = -n$ onde n é um inteiro positivo livre de quadrados.

A seguir, apresentamos uma generalização do símbolo de Legendre onde, para $-n$ relativamente primo com o inteiro positivo ímpar m, sendo:

$$m = \prod_{i=1}^{k} p_i^{e_i}$$

com p_i primos distintos e $e_i \in \mathbb{N}$ para todo $i \in [1, k]$, podemos definir o ***símbolo de Jacobi*** como:

$$\left(\frac{-n}{m}\right) = \left(\frac{-n}{p_1}\right)^{e_1} \cdot \left(\frac{-n}{p_2}\right)^{e_2} \cdots \left(\frac{-n}{p_k}\right)^{e_k}.$$

Note que os símbolos à direita são de Legendre, assim o símbolo de Jacobi satisfaz a propriedade de ser uma função completamente multiplicativa, ou seja, caso $m_1 \cdot m_2$ seja relativamente primo com m temos que

$$\left(\frac{m_1 \cdot m_2}{m}\right) = \left(\frac{m_1}{m}\right) \cdot \left(\frac{m_2}{m}\right).$$

Definidos os símbolos e suas principais propriedades, ao analisar as séries de Dirichlet nos deparamos com sequências de números reais da forma a_m que, em um caso especial (das $L-$funções que iremos ver adiante), se faz necessario relacionar o símbolo de Legendre/Jacobi quando esta sequência é vista como uma função de $-n$ sendo resíduo (ou não) quadrático módulo m.

2.2.2 O caracter de Dirichlet

Nesta subseção é apresentado os caracteres de Dirichlet de maneira suscinta e direcionada ao tema de estudo, para sua exposição mais detalhada ver Apostol [1, Cap. 6] e Otto Endler [9, Cap. 5 Sec. 16].

O ***caracter (quadrático) de Dirichlet*** de um corpo $\mathbb{Q}(\sqrt{-n})$ é um homomorfismo

$$\chi_{-n} : {}^{\mathbb{Z}}\!/_{|\Delta_{-n}|\mathbb{Z}} \longrightarrow \{-1,\, 0,\, 1\}$$

definido para $m \in \mathbb{Z}_{>0}$ por:

$$\chi_{-n}(m + |\Delta_{-n}|\mathbb{Z}) = \left(\frac{\Delta_{-n}}{m}\right) = \begin{cases} 0 & \text{se } \mathrm{mdc}(m,\, |\Delta_{-n}|) > 1; \\ (-1)^{\frac{m-1}{2}} \cdot \left(\frac{m}{n}\right) & \text{se } n \equiv 1 \pmod 4; \\ \left(\frac{m}{n}\right) & \text{se } n \equiv 3 \pmod 4; \\ (-1)^{\frac{m^2+4m-5}{8}} \cdot \left(\frac{m}{n/2}\right) & \text{se } n \equiv 2 \pmod 8; \\ (-1)^{\frac{m^2-1}{8}} \cdot \left(\frac{m}{n/2}\right) & \text{se } n \equiv 6 \pmod 8. \end{cases}$$

As propriedades a seguir são consequências da definição e do Teorema 1.2.2.

Propriedade 2.2.2. *(i) χ_{-n} é periodico módulo $|\Delta_{-n}|$, ou seja,*

$$m_1 \equiv m_2 \pmod{|\Delta_{-n}|} \implies \left(\frac{\Delta_{-n}}{m_1}\right) = \left(\frac{\Delta_{-n}}{m_2}\right) \textit{ (ver Shurman [16, pg 9])};$$

(ii) O carácter de Dirichlet é uma função ímpar, ou seja, $\chi_{-n}(-1) = -1$, e isso ocorre pelo fato de considerarmos um corpo quadrático imaginário (ver Borevich e Shafarevich [3, pg 348]).

Lema 2.2.1. *Para qualquer inteiro $b \geq 1$:*

$$\sum_{m=b}^{b-1+4n} \left(\frac{-n}{m}\right) = 0.$$

Demonstração. Pela primeira propriedade de χ_{-n} ser periódico $|\Delta_{-n}|$, vamos denotar por

$$S = \sum_{m \pmod{4n}} \left(\frac{-n}{m}\right).$$

Note que por meio da aplicação da Lei de Reciprocidade Quadrática em conjunto ao Teorema Chinês dos Resto é possivel escolher um $m_0 \in 4n\mathbb{Z}^{\times}$ tal que $\left(\frac{\Delta_{-n}}{m_0}\right) = -1$, logo:

$$\left(\frac{-n}{m_0}\right) \cdot S = \left(\frac{-n}{m_0}\right) \cdot \sum_{m \pmod{4n}} \left(\frac{-n}{m}\right).$$

Como o símbolo de Legendre é multiplicativo e por $m \cdot m_0 \in 4n\mathbb{Z}^{\times}$, temos:

$$\begin{aligned} -S &= \sum_{m \pmod{4n}} \left(\frac{-n}{m \cdot m_0}\right) \\ &= \sum_{m \pmod{4n}} \left(\frac{-n}{m_1}\right) \\ &= S \end{aligned}$$

provando o lema.

□

2.3 $L-$Funções de Dirichlet

A partir daqui, utilizando das propriedades em decorrência do símbolo do Legendre, iremos considerar o símbolo de Jacobi $\left(\frac{\Delta_{-n}}{m}\right)$ unicamente por $\left(\frac{-n}{m}\right)$; quando for conveniente, o fator Δ_{-n} será expressado.

Definição 2.3.1. *Uma $L-$**função de Dirichlet** do corpo numérico $\mathbb{Q}\left(\sqrt{-n}\right)$ é definida, para $s > 1$ onde $s \in \mathbb{R}$, como:*

$$L_{-n}(s) \overset{def}{=} \sum_{m=1}^{\infty} \left(\frac{-n}{m}\right) m^{-s}.$$

Proposição 2.3.1. *A função $L_{-n}(s)$, quando $s > 0$, converge para uma função contínua. Para $s > 1$ existe um produto de Euler dado por:*

$$L_{-n}(s) = \prod_p \left(1 - \left(\frac{-n}{p}\right) p^{-s}\right)^{-1}.$$

Demonstração. Segue da Proposição 2.1.1 e do item (ii) da Proposição 2.1.2.

□

2.4 Normas limitadas dos ideais de $\mathcal{O}_{-n}$

Algumas notações e propriedades serão muito importantes nessa presente seção para se conectar os resultados obtidos nas Seções 1.3 1.4 e 1.5 junto às convergências das séries de Dirichlet.

Lema 2.4.1. *O número de ideais de $\mathcal{O}_{-n}$ com norma m é finito.*

Demonstração. Seja $\mathcal{I}$ um ideal de $\mathcal{O}_{-n}$, pelo Teorema 1.3.2 temos que $\mathcal{N}(\mathcal{I}) \subset \mathcal{I}$. Portanto pela fatoração de ideais:

$$(\mathcal{N}(\mathcal{I})) = \wp_1{}^{e_1} \cdots \wp_r{}^{e_r}$$

e como $\mathcal{I} \mid (\mathcal{N}(\mathcal{I}))$ segue que $\mathcal{I} = \wp_1{}^{a_1}\overline{\wp_1}^{b_1} \cdots \wp_r{}^{a_r}\overline{\wp_r}^{b_r}$ com $0 \leq a_i,\, b_i \leq e_i$, ou seja, existe um número finito de ideais em $\mathcal{I}$.

□

Proposição 2.4.1. *Seja $a_m \in \mathbb{N}$ o número de ideais com norma m, então:*

(i) $\{a_m\}_{m\in\mathbb{N}}$ *é multiplicativa.*

(ii) Seja p um número primo:

$$a_p = 1 + \left(\frac{-n}{p}\right) = \begin{cases} 2 & se\ \left(\frac{-n}{p}\right) = 1; \\ 0 & se\ \left(\frac{-n}{p}\right) = -1; \\ 1 & se\ \left(\frac{-n}{p}\right) = 0. \end{cases}$$

(iii) Para $s > 1$,

$$\sum_{i=1}^{\infty} a_{p^i}\, p^{-is} = \begin{cases} (1-p^{-s})^{-2} & se\ \left(\dfrac{-n}{p}\right) = 1; \\ (1-p^{-2s})^{-1} & se\ \left(\dfrac{-n}{p}\right) = -1; \\ (1-p^{-s})^{-1} & se\ \left(\dfrac{-n}{p}\right) = 0. \end{cases}$$

Demonstração. (i) Pela definição de a_m, temos pela fatoração em potências de primos distintos que

$$m = \prod_{i=1}^{k} p_i^{j_i};$$

mais ainda, através do Teorema 1.3.1, para $\mathcal{I}$ um ideal de $\mathcal{O}_{-n}$,

$$\mathcal{I} = \prod_{r=1}^{s} \wp_r{}^{e_r}.$$

Note que

$$m = \mathcal{N}(\mathcal{I}) = \prod_{r=1}^{s} \mathcal{N}(\wp_r{}^{e_r}) = \prod_{i=1}^{k} p_i^{j_i}$$

assim

$$a_m = \prod_{i=1}^{k} a_{p_i^{j_i}}.$$

Logo $\{a_m\}_{m\in\mathbb{N}}$ é multiplicativa, provando o *(i)* .

(ii) Note que o discriminante, dado n um inteiro positivo livre de quadrados:

$$\text{ou } \Delta_{-n} = -n \quad \text{ou } \Delta_{-n} = -4n;$$

e pela Proposição 1.3.3, temos dois casos:

- para $p > 2$, o resultado segue diretamente pela norma dos ideais primos.

- para $p = 2$, observe que:

Caso $2 \mid \Delta_{-n}$ então $-n \equiv 2 \pmod 4$, logo existe um único ideal de norma 2, a saber $(2, \sqrt{-n})^2$.

Caso $2 \nmid \Delta_{-n}$, note que $n \equiv 7 \pmod 8$ implica em $n \equiv 3 \pmod 4$, ou seja, verifica-se do primeiro item da Proposição 1.3.3, que os ideais primos $(2, 1+\sqrt{-n})^2$ e $(2, \beta_{-n})(2, \overline{\beta_{-n}})$ são determinados por $\left(\frac{\Delta_{-n}}{2}\right) = 1$, enquanto o ideal (2) é determinado por $\left(\frac{\Delta_{-n}}{2}\right) = -1$; o que prova o item *(ii)*.

(iii) • Caso $\left(\dfrac{-n}{p}\right) = 1$:

Sejam $\wp_1, \wp_2$ ideais primos de $\mathcal{O}_{-n}$, tal que

$$(p) = \wp_1 \cdot \wp_2 = (p,\, a + \sqrt{-n}) \cdot (p,\, a - \sqrt{-n});$$

como $\mathcal{N}(\wp_1) = \mathcal{N}(\wp_2) = p$, então para ideais que possuem norma p^i são da forma

$$\wp_1^k \cdot \wp_2^{i-k} \text{ para } 0 \leq k \leq i.$$

Logo, por indução $a_{p^i} = i + 1$. Fixado um inteiro m e $s > 0$, temos então que a série

$$\begin{aligned}
\sum_{i=0}^{\infty}(i+1)m^{-is} &= \sum_{i=0}^{\infty} m^{-is} + \sum_{i=0}^{\infty} i \cdot m^{-is} \\
&= \frac{1}{1-m^{-s}} + \left(m^{-s} + 2m^{-2s} + 3m^{-3s} + \cdots\right) \\
&= \frac{1}{1-m^{-s}} + \left[m^{-s} \cdot \left(1 + 2m^{-s} + 3m^{-s} + \cdots\right)\right] \\
&= \frac{1}{1-m^{-s}} + m^{-s} \cdot \left[\sum_{i=0}^{\infty}(i+1)m^{-is}\right];
\end{aligned}$$

disso, podemos evidenciar a série:

$$\left(1 - m^{-s}\right) \cdot \sum_{i=0}^{\infty}(i+1)m^{-is} = \frac{1}{1-m^{-s}},$$

portanto

$$\sum_{i=0}^{\infty} a_{p^i}\, p^{-is} \longrightarrow (1 - p^{-s})^{-2}.$$

- Caso $\left(\frac{-n}{p}\right) = 0$:

Seja $\wp$ um ideal primo de $\mathcal{O}_{-n}$ tal que $\wp^2 = (p, \sqrt{-n})^2$, assim $\mathcal{N}(\wp) = p$, então existe apenas um ideal $\wp^i$ com norma p^i, assim $a_{p^i} = 1$ logo

$$\sum_{i=0}^{\infty} p^{-is} \longrightarrow (1 - p^{-s})^{-1}.$$

- Caso $\left(\frac{-n}{p}\right) = -1$:

Seja p primo, com $(p) = \wp$ um ideal primo de $\mathcal{O}_{-n}$ então $\mathcal{N}(\wp) = p^2$.

Para algum inteiro j positivo, se i for par, com a_p multiplicativa, por indução:

$$\begin{array}{rcccccl} a_{p^2} & = & a_p \cdot a_p & \Longleftrightarrow & \#a_{p^2} & = & 1 \quad \text{pois} \quad \mathcal{N}(\wp) = p^2 \\ a_{p^4} & = & a_{p^2} \cdot a_{p^2} & \Longleftrightarrow & \#a_{p^4} & = & 1 \quad \text{pois} \quad \mathcal{N}(\wp^2) = p^4 \\ & \cdots & & & & & \\ a_{p^{2j}} & = & a_{p^j} \cdot a_{p^j} & \Longleftrightarrow & \#a_{p^{2j}} & = & 1 \quad \text{pois} \quad \mathcal{N}(\wp^j) = p^{2j} \end{array}$$

ou seja,

$$\sum_{i=0}^{\infty} p^{-is} = \sum_{i=0}^{\infty} p^{-2js} \longrightarrow (1 - p^{-2s})^{-1};$$

Se i for ímpar, com a_p multiplicativa, por indução e usando o resultado anterior do caso par, concluímos que a_{p^i}:

$$\begin{array}{rcccccl} a_p & = & a_p & \Longleftrightarrow & \#a_p & = & 0 \quad \text{pois} \quad \mathcal{N}(\wp) = p^2 \\ a_{p^3} & = & a_{p^2} \cdot a_p & \Longleftrightarrow & \#a_{p^2} & = & 0 \quad \text{pois} \quad \mathcal{N}(\wp^2) = p^4 \\ & \cdots & & & & & \\ a_{p^{2j+1}} & = & a_{p^j} \cdot a_{p^j} \cdot a_p & \Longleftrightarrow & \#a_{p^{2j+1}} & = & 0 \quad \text{pois} \quad \mathcal{N}(\wp^j) = p^{2j} \end{array}$$

ou seja, não existe nenhum ideal $\wp$ que tenha norma p^{2j+1}, logo a série é nula.

Portanto o item *(iii)* está provado.

□

Para se entender tais convergências das séries de Dirichlet, são usados conceitos de redes complexas e a finitude das classes de ideais e assim, encontrar uma cota para somas do tipo $A_K \stackrel{def}{=} \sum_{k=1}^{K} a_k$ com $K \geq 1$; seguem então, notações/definições que serão importantes e essenciais para a compreensão da fórmula do número de classes.

Seja $a_k(\mathcal{C})$ o número de ideais com norma k dentro da classe $\mathcal{C} \in \mathcal{C}l(-n)$, defina então

$$a_k = \sum_{\mathcal{C} \in \mathcal{C}l(-n)} a_k(\mathcal{C});$$

observe que $a_k \in \mathbb{N}$ de acordo com o Lema 2.4.1 e o Teorema 1.5.3, assim definimos:

- $A_K(\mathcal{C}) \stackrel{def}{=} \sum_{k=1}^{K} a_k(\mathcal{C})$;
- $\#\mathbb{U}_{-n}$ denotado por w;

Segue assim a ideia de se limitar A_K através das cotas de $A_K(\mathcal{C})$ para cada classe $\mathcal{C} \in \mathcal{C}l(-n)$; a princípio, estimaremos a partir da classe $\mathcal{C}_1$ de ideais principais.

Supondo que $\mathcal{N}(\mathcal{I}) = k$, podemos determinar o número de ideais de classe $\mathcal{C}_1$ com norma k desconsiderando a repetição de seus elementos associados [1], ou seja, caso $\mathcal{I} = (\alpha_1) = (\alpha_2)$ com $\alpha_1, \alpha_2 \in \mathcal{O}_{-n}$, ambos se dividem um ao outro e, como todo elemento de $\mathcal{O}_{-n}$ possui w associados, temos

$$a_k(\mathcal{C}_1) = \frac{b_k}{w},$$

onde b_k é a quantidade de elementos (devido à classe $\mathcal{C}_1$) em $\mathcal{O}_{-n}$ com norma k.

Agora, ao analisar a soma $B_K \stackrel{def}{=} \sum_{k=1}^{K} b_k$, é possível se estimar uma cota por meio de uma bola de raio K no espaço complexo a qual a mesma está sob uma rede complexa $\mathcal{O}_{-n}$ de base $\langle 1, \beta_{-n} \rangle$, assim

$$\begin{aligned} B_K &= \{\alpha \in \mathcal{O}_{-n};\, \mathcal{N}(\alpha) \leq K\} \\ &= \left\{\alpha \in \mathcal{O}_{-n};\, |\alpha| \leq \sqrt{K}\right\}. \end{aligned}$$

Note que $\mathcal{N}(\alpha) = |\alpha|^2$ pois $\mathcal{I} \in \mathcal{C}_1$ e, como ainda a área do paralelogramo de vértices 0, 1, β_{-n}, $1 + \beta_{-n}$ é:

$$A = \begin{cases} \sqrt{n} & \text{se } n \equiv 1,\, 2 \pmod 4; \\ \\ \frac{\sqrt{n}}{2} & \text{se } n \equiv 3 \pmod 4; \end{cases} \tag{2.4}$$

pelo Lema 1.5.7, existe uma constante C positiva tal que para todo $K \geq 1$, temos que:

$$\left| B_K - \frac{\pi K}{A} \right| \leq C \cdot \sqrt{K}.$$

Mas como queremos encontrar tal cota para $A_K(\mathcal{C}_1)$, basta fazer uma manipulação algébrica para então obter que:

[1] sejam quaisquer x, $y \in \mathcal{O}_{-n}$, existe um elemento invertível $w \in \mathcal{O}_{-n}$ tal que $x = w \cdot y$.

$$A_K(\mathcal{C}_1) = \frac{1}{w}\sum_{k=1}^{K} b_k \overset{\text{Lema } 1.5.7}{\Longrightarrow} \left| A_K(\mathcal{C}_1) - \frac{\pi\, K}{w\, A} \right| \leq C_1 \cdot \sqrt{K},$$

com $C_1 > 0$.

Determinamos assim, uma estimativa para a soma sobre ideais de classe $\mathcal{C}_1$ e o mesmo vale para qualquer classe de ideais, a saber:

Proposição 2.4.2. *Seja $\mathcal{C}$ uma classe de ideais qualquer do corpo $\mathbb{Q}(\sqrt{-n})$. Existe uma constante $C^\star$ tal que*

$$\left| A_K(\mathcal{C}) - \frac{\pi\, K}{w\, A} \right| \leq C^\star \cdot \sqrt{K}.$$

Demonstração. Antes de iniciar a prova, sem perda de generalidade, usamos dos Teoremas 1.5.1 e 1.5.2, tomando $\frac{a+\sqrt{-n}}{b}$ como a $\mathfrak{j}-$invariante da classe $\mathcal{C}^{-1}$ e

$$\mathcal{J} = (b,\, a + \sqrt{-n}) \in \mathcal{C}^{-1}.$$

Seja $\mathcal{I}$ um ideal numa classe $\mathcal{C}$, então para algum $\alpha \in \mathcal{O}_{-n}$:

$$\mathcal{C} \cdot \mathcal{C}^{-1} = \mathcal{C}_1 \Longleftrightarrow \mathcal{I} \cdot \mathcal{J} = (\alpha) \Longleftrightarrow (\alpha) \subseteq \mathcal{J},$$

o que de fato permite construir uma bijeção entre esses conjuntos de ideais de $\mathcal{O}_{-n}$ por meio de suas normas e classes como sendo:

$$\begin{array}{ccc} \{\mathcal{I} \in \mathcal{C};\, \mathcal{N}(\mathcal{I}) = k\} & \longrightarrow & \left\{ \begin{array}{l} \mathcal{I}^{'} \text{ ideal principal de } \mathcal{O}_{-n}; \\ \mathcal{J} \mid \mathcal{I}^{'} \text{ e } \mathcal{N}(\mathcal{I}^{'}) = k \cdot \mathcal{N}(\mathcal{J}) \end{array} \right\}. \\ \mathcal{I} & \longmapsto & \mathcal{I}^{'} = \mathcal{I} \cdot \mathcal{J} \end{array} \tag{2.5}$$

Seja $b_k(\mathcal{J})$ o número de elementos do ideal $\mathcal{J}$ com norma $k \cdot \mathcal{N}(\mathcal{J})$, pela equação (2.5) obtemos que:

$$a_k\,(\mathcal{C}) = \frac{b_k(\mathcal{J})}{w}. \tag{2.6}$$

Note que o fato de w estar na equação (2.6), é porque recai novamente em ideais principais e os mesmos possuem elementos associados que geram o mesmo ideal, então é necessário retirar essas repetições de elementos de $\mathcal{J}$ com norma $k \cdot \mathcal{N}(\mathcal{J})$.

Usando o mesmo raciocínio sobre B_K, então

$$\begin{aligned} B_K(\mathcal{J}) &= \sum_{k=1}^{K} b_k(\mathcal{J}) \\ &= \#\left\{\alpha \in \mathcal{O}_{-n};\, \mathcal{N}(\alpha) \leq K \cdot \mathcal{N}(\mathcal{J})\right\} \\ &= \#\left\{\alpha \in \mathcal{O}_{-n};\, |\alpha| \leq \sqrt{K \cdot \mathcal{N}(\mathcal{J})}\right\}. \end{aligned}$$

Como estamos sob a rede complexa $\langle b, a+\sqrt{-n}\rangle$, por (2.4) a área do paralelogramo é $b\sqrt{n}$ e, pelo Lema 1.5.7, existe uma constante $C_{\mathcal{J}}$ onde:

$$\left| B_K(\mathcal{J}) - \frac{\pi\, K\, \mathcal{N}(\mathcal{J})}{b\sqrt{n}} \right| \leq C_{\mathcal{J}} \cdot \sqrt{\mathcal{N}(\mathcal{J})} \cdot \sqrt{K}.$$

Manipulando algebricamente, de modo análogo ao argumento anterior, temos que a área a partir do paralelogramo gerado por $\langle 1, \beta_{-n}\rangle$ é $A = \frac{b\sqrt{n}}{\mathcal{N}(\mathcal{J})}$ e — note que $\mathcal{N}(\mathcal{J}) = b$ ou $2b$ (ver Weston [19, pg 44]) — através da soma de $A_K(\mathcal{C})$, implica em:

$$\left| A_K(\mathcal{C}) - \frac{\pi\, K}{w\, A} \right| \leq C_{\mathcal{C}} \cdot \sqrt{K} \quad \text{para todo} \quad K \geq 1 \quad \text{com} \quad C_{\mathcal{C}} = \frac{C_{\mathcal{J}} \cdot \sqrt{\mathcal{N}(\mathcal{J})}}{w}.$$

Para finalizar, basta tomar $C^\star$ como a maior das constantes $C_{\mathcal{C}}$ passando por todas as classes $\mathcal{C}$ de ideais de $\mathcal{O}_{-n}$ (a qual é finita).

□

Corolário 2.4.1. *Existe uma constante C tal que para todo $K \geq 1$*

$$\left| A_K - \frac{h\, \pi\, K}{w\, A} \right| \leq C \cdot \sqrt{K},$$

onde h denota a quantidade de classes ideais $h(-n)$.

Demonstração. Seja A_K já definido, a partir dos argumentos e do resultado da proposição acima, basta realizar a soma sobre todas as classes de ideais de $\mathcal{O}_{-n}$ em A_K. Note que se faz necessária a inclusão do termo h para contabilizar a quantidade de classes de ideais (finita) que ocorre no somatório no qual é controlada pela constante para manter a desigualdade válida.

□

2.5 Função ζ-Dedekind

Definição 2.5.1. *A **Função Zeta Dedekind** do corpo quadrático $\mathbb{Q}(\sqrt{-n})$ é descrita para $s \in \mathbb{R}$ como:*

$$\zeta_{-n}(s) \stackrel{def}{=} \sum_{\mathcal{I} \subset \mathcal{O}_{-n}} \mathcal{N}(\mathcal{I})^{-s}.$$

Note que esta função se dá sob ideais de $\mathcal{O}_{-n}$, o que nos permite manipular a fatoração única e, através da interpretação deste somatório pelas propriedades

da função zeta de Riemann na equação (2.2), é possível reescrevê-la como uma multiplicação de ideais primos onde:

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

Assim, a função zeta Dedekind pode ser reinterpretada como uma série de Dirichlet — seja a_m definido no início da Seção 2.4 como a quantidade de ideais em $\mathcal{O}_{-n}$ com norma igual à m — dada por:

$$\zeta_{-n}(s) = \sum_{m=1}^{\infty} \frac{a_m}{m^s}.$$

Proposição 2.5.1. *Para $s > 1$, a função zeta Dedekind converge e assume uma forma em produto de Euler dada por:*

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

com p primo; mais ainda, possui um polo simples em $s = 1$ com resíduo $\frac{h\,\pi}{A\,w}$.

Demonstração. Pelo Corolário 2.4.1:

$$\begin{aligned} \left| A_K - \frac{h\,\pi\,K}{w\,A} \right| \leq C \cdot \sqrt{K} \quad &\Longrightarrow \quad A_K \leq \frac{h\,\pi\,K}{w\,A} + C \cdot \sqrt{K} \\ &\Longrightarrow \quad A_K \leq \frac{h\,\pi\,K}{w\,A} + C \cdot K \qquad (2.7) \\ &\Longrightarrow \quad |A_K| \leq \left(\frac{h\,\pi}{w\,A} + C \right) \cdot K \end{aligned}$$

Assim, pela última desigualdade acima, valem as condições da Proposição 2.1.1 implicando que para $s > 1$ a função $\zeta_{-n}(s)$ é convergente.

Para provar que $\zeta_{-n}(s)$ pode ser escrita por um produto de Euler, basta usar as Proposições 2.1.2 e 2.4.1, ou seja:

$$\begin{aligned} \prod_{p} \left(\sum_{i=1}^{\infty} a_{p^i}\, p^{-is} \right) &= \prod_{p} \left[(1 - p^{-s})^{-2} \cdot (1 - p^{-2s})^{-1} \cdot (1 - p^{-s})^{-1} \right] \\ &= \prod_{\left(\frac{-n}{p}\right)=1} (1 - p^{-s})^{-2} \cdot \prod_{\left(\frac{-n}{p}\right)=-1} (1 - p^{-2s})^{-1} \cdot \prod_{\left(\frac{-n}{p}\right)=0} (1 - p^{-s})^{-1}. \end{aligned}$$

Ao calcular o resíduo em $s = 1$, definimos primeiro a série:

$$f(s) = \sum_{k=1}^{\infty} \left(a_k - \frac{h\,\pi}{w\,A} \right) \cdot k^{-s};$$

fazendo sua parcial do termo que acompanha k^{-s} temos:

$$\left| \sum_{k=1}^{K} \left(a_k - \frac{h\,\pi}{w\,A} \right) \right| = \left| A_K - \frac{h\,\pi\,K}{w\,A} \right| \leq C \cdot \sqrt{K},$$

logo pela Proposição 2.1.1, $f(s)$ converge para $s > \frac{1}{2}$. Assim, para $s > 1$ temos que:

$$\zeta_{-n}(s) = \sum_{k=1}^{\infty} a_k k^{-s} = \sum_{k=1}^{\infty} a_k k^{-s} - \sum_{k=1}^{\infty} \frac{h\,\pi}{w\,A} k^{-s} + \sum_{k=1}^{\infty} \frac{h\,\pi}{w\,A} k^{-s} = f(s) + \frac{h\,\pi}{w\,A} \zeta(s),$$

e devido sua parcial convergir pela equação (2.7), obtemos:

$$\left| \sum_{k=1}^{K} \left(a_k - \frac{h\,\pi}{w\,A} + \frac{h\,\pi}{w\,A} \right) \right| = |A_K| \leq \left(\frac{h\,\pi}{w\,A} + C \right) \cdot K.$$

Com $f(s)$ estando definida para $s = 1$, é possivel ver que:

$$\lim_{s \to 1^+} \zeta_{-n}(s) = f(1) + \frac{h\,\pi}{w\,A} \lim_{s \to 1^+} \zeta(s) = +\infty,$$

ou seja, o limite de $\zeta_{-n}(s)$ existe, então:

$$\begin{aligned} \lim_{s \to 1^+} (s-1)\,\zeta_{-n}(s) &= \lim_{s \to 1^+} (s-1)\,f(s) + \frac{h\,\pi}{w\,A} \lim_{s \to 1^+} (s-1)\,\zeta(s) \\ &= (1-1)\,f(1) + \frac{h\,\pi}{w\,A} \lim_{s \to 1^+} (s-1)\,\zeta(s) \\ &= \frac{h\,\pi}{w\,A}. \end{aligned}$$

□

2.6 A fórmula para $h(-n)$

A seguir, apresentamos a *fórmula do número de classes de Dirichlet* a partir da fatoração da função ζ-Dedekind e a relação com χ_{-n}.

Proposição 2.6.1. *Para $s > 1$, temos que*

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

Demonstração. Pela Proposição 2.3.1 podemos reescrever $L_{-n}(s)$ mediante os casos do símbolo de Legendre e, por Zhao [21] com p_1, p_2 e p_3 números primos, temos:

$$L_{-n}(s) = \prod_{\left(\frac{-n}{p_1}\right)=1} (1-p_1^{-s})^{-1} \cdot \prod_{\left(\frac{-n}{p_2}\right)=0} 1 \cdot \prod_{\left(\frac{-n}{p_3}\right)=-1} (1+p_3^{-s})^{-1}.$$

Como estamos sob produtos de Euler com $s > 1$, multiplicando a função zeta de Riemann na equação acima, obtemos:

$$\begin{aligned}\zeta(s) \cdot L_{-n}(s) &= \prod_{\left(\frac{-n}{p_1}\right)=1} (1-p_1^{-s})^{-2} \cdot \prod_{\left(\frac{-n}{p_2}\right)=0} (1-p_2^{-s})^{-1} \cdot \prod_{\left(\frac{-n}{p_3}\right)=-1} (1-p_3^{-s})^{-1}(1+p_3^{-s})^{-1} \\ &= \prod_{\left(\frac{-n}{p_1}\right)=1} (1-p_1^{-s})^{-2} \cdot \prod_{\left(\frac{-n}{p_2}\right)=0} (1-p_2^{-s})^{-1} \cdot \prod_{\left(\frac{-n}{p_1}\right)=-1} (1-p_3^{-2s})^{-1}. \qquad (2.8)\end{aligned}$$

Mas veja que pela Proposição 1.3.3, podemos relacionar os números primos que ocorrem na equação (2.8) advindo das normas dos ideais de $\mathcal{O}_{-n}$ onde:

- $\left(\frac{-n}{p}\right) = 1 \implies \exists\, \wp_1,\ \tilde{\wp}_1 \subset \mathcal{O}_{-n}$ tal que $\wp_1 \cdot \tilde{\wp}_1 = (p_1)$

onde $\wp_1$ e $\tilde{\wp}_1$ ambos ideais primos. Tomando a norma, temos:

$$\mathcal{N}(\wp_1 \cdot \tilde{\wp}_1) = \mathcal{N}(\wp_1) \cdot \mathcal{N}(\tilde{\wp}_1) = \mathcal{N}((p_1)) = p_1 \cdot \overline{p_1} = p_1^2$$

$$\implies$$

$$\mathcal{N}(\wp_1) = \mathcal{N}(\tilde{\wp}_1) = p_1.$$

- $\left(\frac{-n}{p}\right) = 0 \implies \exists\, \wp_2 \subset \mathcal{O}_{-n}$ tal que $\wp_2^2 = (p_2)$

com $\wp_2$ sendo um ideal primo onde:

$$\mathcal{N}(\wp_2) = p_2.$$

- $\left(\frac{-n}{p}\right) = -1 \implies \exists\, \wp_3 \subset \mathcal{O}_{-n}$ tal que $\wp_3 = (p_3)$

com $\wp_3$ sendo um ideal primo, assim:

$$\mathcal{N}(\wp_3) = \mathcal{N}((p_3)) = p_3 \cdot \overline{p_3} = p_3^2.$$

Portanto, reescrevendo o produtório de Euler em termos das normas dos ideais, conlui-se que $\zeta(s) \cdot L_{-n}(s)$ se torna:

$$\prod_{\left(\frac{-n}{p_1}\right)=1}(1-\mathcal{N}(\wp_1)^{-s})^{-1}(1-\mathcal{N}(\tilde{\wp}_1)^{-s})^{-1}\cdot\prod_{\left(\frac{-n}{p_2}\right)=0}(1-\mathcal{N}(\wp_2)^{-s})^{-1}\cdot\prod_{\left(\frac{-n}{p_3}\right)=-1}(1-\mathcal{N}(\wp_3)^{-s})^{-1}.$$

Note que todo ideal primo do anel $\mathcal{O}_{-n}$ aparece uma única vez pois recai em um dos casos da Proposição 1.3.3; dessa forma, pelo Teorema 1.3.1 e a Proposição 2.5.1, obtemos:

$$\zeta(s)\cdot L_{-n}(s)=\prod_{\wp\subset\mathcal{O}_{-n}}\left(1-\mathcal{N}(\wp)^{-s}\right)^{-1}=\sum_{\mathcal{I}\subset\mathcal{O}_{-n}}\mathcal{N}(\mathcal{I})^{-s}.$$

Logo,

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

□

Teorema 2.6.1. *Seja $h(-n)$ o número das classes de $\mathbb{Q}(\sqrt{-n})$ e*

$$w_{-n}=\begin{cases}2 & \text{se } n\neq 1,3;\\ 4 & \text{se } n=1;\\ 6 & \text{se } n=3;\end{cases}$$

a quantidade de elementos do conjunto das unidades de $\mathcal{O}_{-n}$, temos que:

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

Demonstração. Como $L_{-n}(s)$ é contínua para $s>0$, temos

$$\begin{aligned}L_{-n}(1) &= \lim_{s\to 1^+}L_{-n}(s)\\ &= \lim_{s\to 1^+}\frac{\zeta_{-n}(s)}{\zeta(s)}\\ &= \lim_{s\to 1^+}\frac{(s-1)\cdot\zeta_{-n}(s)}{(s-1)\cdot\zeta(s)}\\ &= \frac{\lim_{s\to 1^+}(s-1)\cdot\zeta_{-n}(s)}{\lim_{s\to 1^+}(s-1)\cdot\zeta(s)}\\ &= \frac{h(-n)\cdot\pi}{A\cdot w_{-n}}.\end{aligned}$$

Logo, para finalizar a prova, mediante à n módulo 4, o valor de A é determinado pela equação (2.4); e o resultado segue.

□

Uma outra maneira interessante de encontrar $h(-n)$ é apresentada por Borevich e Shafarevich [3] por um teorema a qual traz o vínculo explícito com os caracteres quadráticos de Dirichlet através de métodos analíticos:

Teorema 2.6.2. *Para um corpo quadratico imaginário com $\Delta_{-n} < -4$ e carater χ_{-n}, temos que o número de classes de ideais é dada por:*

$$h(-n) = \frac{1}{2 - \chi_{-n}(2)} \sum_{0<m<|\Delta_{-n}|/2} \chi_{-n}(m). \tag{2.9}$$

Demonstração. Ver [3, pg 346].

□

Exemplo 2.6.1.

Seja o corpo $\mathbb{Q}(\sqrt{-39})$, seu carater quadrático está em $\mathbb{Z}/39\mathbb{Z}$, assim:

$$\chi_{-39}(m) = \begin{cases} 0 & \text{se } m = 3,\ 6,\ 9,\ 12\,15,\ 18,\ 21,\ 24,\ 27,\ 30,\ 33,\ 36,\ 39; \\ 1 & \text{se } m = 1,\ 2,\ 4,\ 5,\ 8,\ 10,\ 11,\ 16,\ 20,\ 22,\ 25,\ 32; \\ -1 & \text{se } m = 7,\ 14,\ 17,\ 19,\ 23,\ 28,\ 31,\ 34,\ 35,\ 37,\ 38. \end{cases}$$

Pela equação (2.9), temos:

$$h(-39) = \sum_{m=1}^{19} \chi_{-39}(m) = (8 - 4) = 4.$$

Ao confrontar o resultado dos Teoremas 2.6.1 e 2.6.2, conclui-se que:

$$L_{-n}(1) > 0;$$

uma outra maneira de comprovar este resultado, é via métodos analíticos em Daniel [13, Cap. 7], onde:

- se $\mathcal{F}$ um corpo quadrático real,

$$L_n(1) = -\frac{2}{\sqrt{\Delta_n}} \cdot \sum_{1\leq m<\Delta_n/2} \chi_n(m)\ log\left(sen\frac{n\pi}{\Delta_n}\right);$$

- se $\mathcal{F}$ um corpo quadrático imaginário,

$$L_{-n}(1) = -\frac{\pi}{|\Delta_{-n}|^{2/3}} \cdot \sum_{m=1}^{|\Delta_{-n}|-1} m\ \chi_{-n}(m). \tag{2.10}$$

Observação 2.6.1.

O Exemplo 2.6.1 se verifica também pela equação (2.10), ou seja, daí a necessidade de se calcular todos os caracteres quadráticos para se obter o valor de $L_{-n}(1)$ bem como, se utilizar alternativamente, do Teorema 2.6.1.

Note que para um corpo quadrático $\mathbb{Q}(\sqrt{-p})$ tal que $p \equiv 3 \pmod 4$, ao aplicar o Teorema 2.6.2 obtemos:

(i) $\Delta_{-p} = -p$;

(ii) $\chi_{-p}(r) = \left(\frac{r}{p}\right)$;

(iii) $\chi_{-p}(2) = \begin{cases} 1 & \text{se } p \equiv 7 \pmod 8; \\ -1 & \text{se } p \equiv 3 \pmod 8. \end{cases}$

Assim, segundo Borevich e Shafarevich [3], o número de classes em $\mathcal{O}_{-p}$ resulta em:

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

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

Surge então, estudos que visam explorar as propriedades da fórmula do número das classes mediante seus valores relacionado ao inteiro livre de quadrados caracterizando o corpo quadrático considerado.

Capítulo 3

Resultados

Antes de detalhar o artigo principal de estudo de Wang e Tingting [7], se faz necessário adotar algumas notações relacionando conceitos abordados nos capítulos 1 e 2 a fim de não causar indefinições e, além disso, são apresentadas características do discriminante de um corpo quadrático imaginário para determinar o número de classes, alguns resultados de Equações Diofantinas e parâmetros dos pares de Lehmer que servem de "limitantes" para a conclusão desta dissertação.

- O número de classes de ideais $h(-n)$ do corpo quadrático imaginário $\mathbb{Q}(\sqrt{-n})$ será denotado por:

$$h(\Delta_{-n}) = \begin{cases} h(-n) & \text{se } n \equiv 3 \pmod 4; \\ h(-4n) & \text{caso contrário.} \end{cases}$$

- Seja D um inteiro positivo, existem inteiros positivos n e f, únicos tal que

$$D \stackrel{def}{=} n \cdot f^2, \tag{3.1}$$

  onde n é um inteiro livre de quadrados.

- Para o corpo quadrático imaginário $\mathbb{Q}(\sqrt{-D})$ temos que:

$$-D = a^2 - \delta k^d, \tag{3.2}$$

  onde $a,\ k,\ d \in \mathbb{N}$, $\text{mdc}(a,\ k) = 1$, $k > 1$, $\delta \in \{1,\ 4\}$ e $a^2 < \delta k^d$.

O estudo apresentado é uma generalização do resultado de Yasuhiro Kishi [12] a qual demonstra a divisibilidade do número de classes do corpo imaginário $\mathbb{Q}(\sqrt{2^{2m} - 3^d})$ por d. Ambos artigos ([7] e [12]) se utilizam de métodos de resolução por Equações Diofantinas não lineares, as quais são detalhados em artigos posteriormente citados.

3.1 Resultados Principais

Da teoria das formas binárias quadráticas, a relação entre o discriminante de um corpo imaginário quadrático no Teorema 1.2.2 é definida por:

Definição 3.1.1. *Um discriminante Δ_{-n} é dito um* ***discriminante fundamental*** *se não possui como divisor um primo ímpar ao quadrado ou $\Delta_{-n} \equiv 8, 12 \pmod{16}$.*

Lema 3.1.1. *Para $n > 3$ e $n \equiv 3 \pmod 4$ temos que*

$$h(-n) = \begin{cases} h(-4n) & \text{se } n \equiv 7 \pmod 8; \\ \\ \dfrac{1}{3}h(-4n) & \text{se } n \equiv 3 \pmod 8. \end{cases}$$

Demonstração. Pelo Teorema 2.6.1, desde de que $n \geq 7$, temos

$$h(-4n) = \frac{2\sqrt{n}}{\pi} L_{-4n}(1) \tag{3.3}$$

e

$$h(-n) = \frac{\sqrt{n}}{\pi} L_{-n}(1) \tag{3.4}$$

Na equação (3.3), a L–função se caracteriza por meio do discriminante cujo o símbolo de Legendre é $\left(\frac{-4n}{m}\right)$; desde que $n \equiv 3 \pmod 4$, pela Definição 3.1.1 o discriminante $-n$ é fundamental enquanto $-4n$ não é, logo por Hua [11, Teo. 11.2], a $L-$função possui uma propriedade onde:

$$L_{-4n}(1) = \left(1 - \left(\frac{-n}{2}\right) \cdot \frac{1}{2}\right) L_{-n}(1). \tag{3.5}$$

Como visto na equação (2.3), sabemos que:

$$\left(\frac{-n}{2}\right) = \begin{cases} 1 & \text{se } n \equiv 7 \pmod 8; \\ -1 & \text{se } n \equiv 3 \pmod 8. \end{cases} \tag{3.6}$$

Substituindo (3.6) em (3.5), obtemos

$$L_{-4n}(1) = \begin{cases} \dfrac{1}{2}L_{-n}(1) & \text{se } n \equiv 7 \pmod 8; \\ \\ \dfrac{3}{2}L_{-n}(1) & \text{se } n \equiv 3 \pmod 8. \end{cases} \tag{3.7}$$

Portanto, por pelos resultados obtidos em (3.4), (3.3) e (3.7), o lema está provado.

□

Corolário 3.1.1.

$$h(-n) = \begin{cases} \dfrac{1}{3}h(-4n) & \text{se } n > 3 \text{ e } n \equiv 3 \pmod 8; \\ \\ h(-4n) & \text{caso contrário.} \end{cases}$$

Lema 3.1.2. *Seja D e k inteiros positivos tais que D, $k > 1$ e $mdc(2D,\, k) = 1$. Se a equação*

$$X^2 + D \cdot Y^2 = k^Z \quad \text{tal que} \quad X,\, Y,\, Z \in \mathbb{N}, \quad mdc(X,\, Y) = 1 \quad e \quad Z > 0 \tag{3.8}$$

possui soluções $(X,\, Y,\, Z)$, então toda solução $(X,\, Y,\, Z)$ em (3.8) pode ser expressada como

$$Z = Z_1 \cdot t, \quad t \in \mathbb{N}$$

e

$$X + Y \cdot \sqrt{-D} = \epsilon_1 \cdot \left(X_1 + \epsilon_2 \cdot Y_1 \cdot \sqrt{-D}\right)^t \quad \text{onde} \quad \epsilon_1,\, \epsilon_2 \in \{1,\, -1\}$$

com $X_1,\, Y_1,\, Z_1 \in \mathbb{N}$ satisfazendo

$$X_1{}^2 + D \cdot Y_1{}^2 = k^{Z_1} \quad \text{tal que} \quad mdc(X_1,\, Y_1) = 1 \quad e \quad Z_1 \mid h(4D).$$

Demonstração. Para provar este resultado usamos um caso especial dado por Heuberger e Le [5, Teo. 6.2] tomando o par $(D_1,\, D_2) = (1,\, -D)$.

Podemos assumir então que a solução $(X,\, Y,\, Z)$ em (3.8) está numa classe de soluções do conjunto S_l (para mais detalhes ver o artigo [5]) e, seja $(X_1,\, Y_1,\, Z_1)$ denotando uma solução para S_l tal que $X_1,\, Y_1 > 0$ e $Z_1 \leq Z$ para todas soluções de $(X,\, Y,\, Z) \in S_l$, o lema está provado.

□

Lema 3.1.3. *Para $x,\, y,\, m,\, n \in \mathbb{N}$, a equação*

$$x^m - y^n = 1 \quad \text{onde} \quad min(x,\, y,\, m,\, n) > 1$$

possui apenas uma única solução $(x,\, y,\, m,\, n) = (3,\, 2,\, 2,\, 3)$.

Lema 3.1.4. *Para $y,\, m,\, n \in \mathbb{N}$ e $n > 2$, a equação*

$$2^{2m+2} - 3y^n = 1 \tag{3.9}$$

não possui solução.

Demonstração. Fazendo uma simples manipulação, temos a diferença de quadrados:

$$(2^{m+1}+1)\cdot(2^{m+1}-1)=3y^n$$

assim, desde que o mdc$(2^{m+1}+1,\, 2^{m+1}-1)=1$, temos da equação (3.9) duas possibilidades:

i) $2^{m+1}+1=a^n$ e $2^{m+1}-1=3b^n$ com $y=ab$, $a,\, b\in\mathbb{N}$;

ii) $2^{m+1}+1=b^n$ e $2^{m+1}-1=3a^n$ com $y=ab$, $a,\, b\in\mathbb{N}$.

Mas note que no item *i*), obtemos $a^n-2^{m+1}=1$ e pelo Lema 3.1.3 implica que a única solução possível é:

$$(a,\, 2,\, n,\, m+1)=(3,\, 2,\, 2,\, 3),$$

mas por hipótese $n>2$, logo este caso é descartado.

Agora, para o item *ii*), tem-se $2^{m+1}-b^n=1$ e utilizando do Lema 3.1.3 conclui-se que não possui solução, pois claramente

$$(2,\, b,\, m+1,\, n)=(2,\, 2,\, 2,\, 3)\neq(3,\, 2,\, 2,\, 3)=(x,\, y,\, m,\, n).$$

Portanto a equação (3.9) não possui solução.

□

Definição 3.1.2. *Sejam μ, ν inteiros algébricos. Definimos $(\mu,\, \nu)$ como um* ***par de Lehmer*** *se $(\mu+\nu)^2$, $\mu\cdot\nu\in\mathbb{Z}$ sejam coprimos com μ/ν não sendo uma raiz da unidade.*

Considerando:

$$a=(\mu+\nu)^2,\quad c=\mu\cdot\nu$$

para $\epsilon\in\{1,\, -1\}$, temos

$$\mu=\frac{1}{2}\left(\sqrt{a}+\epsilon\sqrt{b}\right),\quad \nu=\frac{1}{2}\left(\sqrt{a}-\epsilon\sqrt{b}\right)$$

onde $b=a-4c$.

Propriedade 3.1.1.

- Dizemos que o par $(a,\, b)$ são os ***parâmetros*** do par de Lehmer $(\mu,\, \nu)$;
- A ***equivalência*** entre dois pares de Lehmer $(\mu_1,\, \nu_1)$ e $(\mu_2,\, \nu_2)$ ocorre quando:

$$\frac{\mu_1}{\mu_2}=\frac{\nu_1}{\nu_2}\in\{1,\, -1,\, i,\, -i\};$$

- Sejam $(a_1,\, b_1)$ e $(a_2,\, b_2)$ parâmetros dos pares de Lehmer $(\mu_1,\, \nu_1)$ e $(\mu_2,\, \nu_2)$ respectivamente, afirmamos que

$$(a_2,\, b_2) = (\epsilon \cdot a_1,\, b_1).$$

Definição 3.1.3. *Fixado um par de Lehmer $(\mu,\, \nu)$ e $r \in \mathbb{N}$, definimos a* ***sequência de números de Lehmer*** *de $(\mu,\, \nu)$ por:*

$$Lh_r(\mu,\, \nu) = \begin{cases} \dfrac{\mu^r - \nu^r}{\mu - \nu} & \text{se } r \text{ é ímpar;} \\ \dfrac{\mu^r - \nu^r}{\mu^2 - \nu^2} & \text{se } r \text{ é par.} \end{cases} \tag{3.10}$$

Observação 3.1.1.

Sejam $(\mu_1,\, \nu_1)$ e $(\mu_2,\, \nu_2)$ pares de Lehmer equivalentes, pela relação dos parâmetros citados conclui-se que

$$Lh_r(\mu_1,\, \nu_1) = \pm Lh_r(\mu_2,\, \nu_2).$$

Definição 3.1.4. *Seja p um número primo, p é dito um* ***divisor primitivo*** *do número de Lehmer $Lh_r(\mu,\, \nu)$ sempre que:*

- $p \mid Lh_r(\mu,\, \nu)$;
- $p \nmid a \cdot b \cdot \ldots \cdot Lh_{r-1}(\mu,\, \nu)$.

Caso um número de Lehmer $Lh_r(\mu,\, \nu)$ não possuir divisor primo, o par $(\mu,\, \nu)$ é dito r*–**defeituoso***.

Lema 3.1.5. *Seja r satisfazendo $6 < r \leq 30$ e $r \neq 8,\, 10,\, 12$. A menos de equivalência, para $a > 0$ todos os parâmetros $(a,\, b)$ dos pares r–defeituosos são dados por:*

- $r = 7$; $(a,\, b) = (1,\, -7),\, (1,\, -19),\, (3,\, -5),\, (5,\, -7),\, (13,\, -3),\, (14,\, -22)$.
- $r = 9$; $(a,\, b) = (5,\, -3),\, (7,\, -1),\, (7,\, -5)$.
- $r = 13$; $(a,\, b) = (1,\, -7)$.
- $r = 14$; $(a,\, b) = (3,\, -13),\, (5,\, -3),\, (7,\, -1),\, (7,\, -5),\, (19,\, -1),\, (22,\, -14)$.
- $r = 15$; $(a,\, b) = (7,\, -1),\, (10,\, -2)$.
- $r = 18$; $(a,\, b) = (1,\, -7),\, (3,\, -5),\, (5,\, -7)$.
- $r = 24$; $(a,\, b) = (3,\, -5),\, (5,\, -3)$.
- $r = 26$; $(a,\, b) = (7,\, -1)$.

- $r = 30$; $(a,\, b) = (1,\, -7),\, (2,\, -10)$.

Demonstração. Ver [17, Teo. 4.5 pg. 17].

□

Lema 3.1.6. *Para $r > 30$, então nenhum par de Lehmer é r–defeituoso.*

Demonstração. Ver [20, Teo. 1 pg. 02].

□

Teorema 3.1.1. *Seja o corpo quadrático imaginário $\mathbb{Q}(\sqrt{a^2 - \delta k^d})$. Se $a = 2^m$ e $\delta = 1$, então*

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

Demonstração. Por hipótese, $a = 2^m$ e $\delta = 1$, e a partir da caracterização do inteiro livre de quadrado, desde que o $\mathrm{mdc}(2^m,\, k) = 1$ e $k > 1$, implica claramente que k é um inteiro positivo ímpar. Por meio das equações (3.1) e (3.2) relacionando com a equação (3.8), encontramos da equação diofantina

$$X^2 + n \cdot Y^2 = k^Z \quad \text{tal que} \quad X,\, Y,\, Z \in \mathbb{N}, \quad \mathrm{mdc}(X,\, Y) = 1 \quad \text{e} \quad Z > 0$$

que:

$$\begin{aligned} -D = -nf^2 \quad &\Longrightarrow \quad -nf^2 = a^2 - \delta k^d \\ &\Longrightarrow \quad -2^{2m} - nf^2 = -(1)k^d \\ &\Longrightarrow \quad 2^{2m} + nf^2 = k^d \\ &\Longrightarrow \quad X^2 - (-nY^2) = k^Z \text{ com solução } (X,\, Y,\, Z) = (2^m,\, f,\, d). \end{aligned}$$

Pelo Lema 3.1.2, temos

$$d = Z_1 \cdot t, \quad t \in \mathbb{N} \tag{3.11}$$

$$2^m + f \cdot \sqrt{-n} = \epsilon_1 \cdot \left(X_1 + \epsilon_2 \cdot Y_1 \cdot \sqrt{-n}\right)^t \quad \text{tal que} \quad \epsilon_1,\, \epsilon_2 \in \{1,\, -1\} \tag{3.12}$$

com inteiros positivos X_1, Y_1, Z_1 satisfazendo

$$X_1{}^2 + n \cdot Y_1{}^2 = k^{Z_1} \quad \text{tal que} \quad \mathrm{mdc}(X_1,\, Y_1) = 1 \quad \text{e} \quad Z_1 \mid h(-4n). \tag{3.13}$$

Como k é ímpar, das definições em (3.1) e (3.2), verificamos que existe um $\gamma_3 \in \mathbb{Z}_{>0}$, tal que para $\gamma_1,\, \gamma_2 \in \mathbb{Z}_{>0}$ satisfaz a seguinte implicação:

$$2^{2m}-k^d=-nf^2=-D \implies 2\gamma_1-(2\gamma_2+1)=-2\gamma_3+1=-nf^2 \implies \begin{cases} D \text{ ímpar} \\ n \text{ ímpar} \\ f \text{ ímpar} \end{cases};$$

mais ainda, das condições estabelecidas em (3.13), conclui-se que para $g_1,\ g_2 \in \mathbb{Z}_{>0}$:

$$X_1{}^2 + (2g_1+1)\cdot Y_1{}^2 = (2g_2+1)^{Z_1},$$

ocasionando em dois casos: ou X_1 é par e Y_1 é ímpar ou X_1 é ímpar e Y_1 é par; portanto a multiplicação $X_1 \cdot Y_1$ é um número par.

A partir daqui, iremos adotar algumas notações a fim de analisar minusciosamente o fator $\left(X_1+\epsilon_2\cdot Y_1\cdot\sqrt{-n}\right)^t$ em (3.12).

Sejam:

- N — termo qualquer a qual acompanha $\sqrt{-n}$;
- E — termo que representa as potências quaisquer de X_1;
- G — termo que representa as potências quaisquer de Y_1;
- H — termo qualquer a qual acompanha $-n$ e que não acompanha $\sqrt{-n}$.

Pelo binômio de Newton e seus coeficientes determinados pelo triângulo de Pascal, se t for par, então:

$$\begin{cases} t=0 & \implies & 1 \\ t=2 & \implies & E+2EGN+GH \\ t=4 & \implies & E+4EGN+6EGH+4EGN+GH \\ t=6 & \implies & E+6EGN+15EGH+20EGN+15EGH+6EGN+GH \\ & \vdots & \end{cases}$$

Note que pela equação (3.12), desde que f seja ímpar, os coeficientes que acompanham o fator $(\sqrt{-n})$, pela equação (3.12), deveriam ser ímpar, o que não acontece; concluímos assim que t deve ser um número ímpar.

Ao expandir o binômio da equação (3.12)

$$\epsilon_1\cdot\left[\sum_{i=0}^{t}\binom{t}{i}{X_1}^{t-i}\cdot\left(\epsilon_2 Y_1\sqrt{-n}\right)^i\right]$$

encontramos:

$$\epsilon_1 \cdot \Bigg[\underbrace{\binom{t}{0} {X_1}^t}_{\text{estrutura } 2^m} + \underbrace{\binom{t}{1} {X_1}^{t-1} \cdot \left(\epsilon_2 Y_1 \sqrt{-n}\right)}_{\text{estrutura } f} + \underbrace{\binom{t}{2} {X_1}^{t-2} \cdot \left(\epsilon_2 Y_1 \sqrt{-n}\right)^2}_{\text{estrutura } 2^m}$$

$$+ \cdots +$$

$$\underbrace{\binom{t}{t-2i} {X_1}^{2i} \cdot \left(\epsilon_2 Y_1 \sqrt{-n}\right)^{t-2i}}_{\text{estrutura } f} + \underbrace{\binom{t}{t-2i+1} {X_1}^{2i-1} \left(\epsilon_2 Y_1 \sqrt{-n}\right)^{t-2i+1}}_{\text{estrutura } 2^m}$$

$$+ \cdots +$$

$$\underbrace{\binom{t}{t-1} {X_1}^1 \cdot \left(\epsilon_2 Y_1 \sqrt{-n}\right)^{t-1}}_{\text{estrutura } 2^m} + \underbrace{\binom{t}{t} \left(\epsilon_2 Y_1 \sqrt{-n}\right)^t}_{\text{estrutura } f} \Bigg] .$$

Observe que são nas posições ímpares que o termo 2^m se estrutura, e pelo fato de t ser um número ímpar, o termo inferior do coeficiente binomial é par, assim os fatores ϵ_2 e $(\sqrt{-n})$ desaparecem devido às suas potências pares; ao analisar o que estrutura f, vemos uma necessidade de isolarmos o termo $(\sqrt{-n})$ como fator comum em relação aos outros termos que o compõem devido às potências ímpares.

Note que pela propriedade dos termos binomiais, para $0 \leq 2i \leq t$:

$$\binom{t}{t-2i} = \binom{t}{2i},$$

assim, por uma mudança de limitantes e, ao evidenciar as variáveis X_1 e Y_1, temos $(t-1)$-ésimos termos tal que $0 \leq i \leq \frac{t-1}{2}$; através dessas manipulações algébricas:

$$2^m = \epsilon_1 X_1 \cdot \sum_{i=0}^{(t-1)/2} \binom{t}{2i} {X_1}^{t-2i-1} \left(-n {Y_1}^2\right)^i \tag{3.14}$$

e

$$f = \epsilon_1 \epsilon_2 Y_1 \cdot \sum_{i=0}^{(t-1)/2} \binom{t}{2i+1} {X_1}^{t-2i-1} \left(-n {Y_1}^2\right)^i \tag{3.15}$$

Como f é ímpar, pela equação (3.15) concluímos que Y_1 é ímpar e X_1 é par. Mais ainda, desde que

$$\sum_{i=0}^{(t-1)/2} \binom{t}{2i} {X_1}^{t-2i-1} \left(-n{Y_1}^2\right)^i$$

seja ímpar, da equação (3.14), evidenciamos que $X_1 = 2^m$ e

$$\sum_{i=0}^{(t-1)/2} \binom{t}{2i} 2^{m(t-2i-1)} \left(-n{Y_1}^2\right)^i = \pm 1. \tag{3.16}$$

Sejam

$$\mu = 2^m + Y_1\sqrt{-n}, \quad \nu = -2^m + Y_1\sqrt{-n}; \tag{3.17}$$

temos os seguintes resultados:

$$\begin{cases} \mu + \nu &= 2Y_1\sqrt{-n}; \\ \mu - \nu &= 2^{m+1}; \\ \mu \cdot \nu &= -k^{Z_1}. \end{cases} \tag{3.18}$$

Note que em (3.18), obtemos:

$$(\mu + \nu)^2 = -4n{Y_1}^2, \quad \mu \cdot \nu = -k^{Z_1}$$

e como consequência, garantimos que $(\mu + \nu)^2$ e $\mu \cdot \nu$ são inteiros coprimos.

Da equação (3.17) temos também que o quociente μ/ν satisfaz uma equação do segundo grau da forma:

$$k^{Z_1} \left(\mu/\nu\right)^2 + 2(2^{2m} - n{Y_1}^2) \left(\mu/\nu\right) + k^{Z_1} = 0. \tag{3.19}$$

De fato, seja $F(s) = k^{Z_1}(s)^2 + 2(2^{2m} - n{Y_1}^2)(s) + k^{Z_1}$, temos que o discriminante deste polinômio quadrático é:

$$\begin{aligned} \Delta &= 4\left[\left(2^{2m} - n{Y_1}^2\right)^2 - k^{2Z_1}\right] \\ &= 4\left[\left(2^{2m} - n{Y_1}^2\right)^2 - \left(2^{2m} + n{Y_1}^2\right)^2\right] \\ &= -16 \cdot 2^{2m} n{Y_1}^2; \end{aligned}$$

assim, as raízes de $F(s)$ se dão por:

$$s = \frac{-2\left(2^{2m} - n{Y_1}^2\right) \pm 4 \cdot 2^m Y_1\sqrt{-n}}{2k^{Z_1}} = \frac{\left(-2^{2m} + n{Y_1}^2\right)}{k^{Z_1}} \pm \frac{2 \cdot 2^m Y_1\sqrt{-n}}{k^{Z_1}}.$$

Como

$$\frac{\mu}{\nu} = \frac{2^m + Y_1\sqrt{-n}}{-2^m + Y_1\sqrt{-n}} = \frac{\left(-2^{2m} + n{Y_1}^2\right)}{2^{2m} + n{Y_1}^2} + \frac{2 \cdot 2^m Y_1\sqrt{-n}}{2^{2m} + n{Y_1}^2},$$

logo μ/ν é raiz de $F(s)$.

Por $k > 1$ e

$$\text{mdc}(k^{Z_1},\, 2(2^{2m} - nY_1{}^2)) = 1 = \text{mdc}(2^{2m} + nY_1,\, 2(2^{2m} - nY_1{}^2)),$$

concluímos de (3.19) que μ/ν não é uma raiz da unidade, logo $(\mu,\, \nu)$ é um par de Lehmer com parâmetros $(-4nY_1{}^2,\, 2^{2m+2})$.

Pela definição de números de Lehmer em (3.10), podemos encontrar tais números a partir de (3.16) e (3.17) que

$$Lh_t(\mu,\, \nu) = \pm 1;$$

e por definição, isso implica que estes números de Lehmer não possuem divisor primo. Portanto, pelo limitante citado no Lema 3.1.6 vemos que $t \leq 30$ e, por t ser ímpar, do Lema 3.1.5, a menos de equivalência, $t \in \{1,\, 3,\, 5\}$, logo:

- $t = 5$

  Da equação (3.16):

  $$2^{4m} - 10 \cdot 2^{2m} nY_1{}^2 + 5 \cdot (nY_1{}^2)^2 = \pm 1; \tag{3.20}$$

  desde que $nY_1{}^2$ seja ímpar, da equação (3.20) temos uma contradição pelo fato de

  $$2^{4m} - 10 \cdot 2^{2m} nY_1{}^2 + 5 \cdot n^2 Y_1{}^4 \equiv 5 \not\equiv \pm 1 \pmod 8.$$

- $t = 3$

  Da equação (3.16) e, desde que $2^{2m} \equiv 1 \pmod 3$:

  $$2^{2m} - 3nY_1{}^2 = 1; \tag{3.21}$$

  pelo fato de $X_1 = 2^{2m}$ e associando as equações (3.13) e (3.21), temos:

  $$2^{2m+2} - 3k^{Z_1} = 1. \tag{3.22}$$

Desde que $k > 1$, pelo Lema 3.1.4 vemos da equação (3.22) que $Z_1 = 1$. Assim, pela equação (3.11) obtemos:

$$d = 3, \quad Z_1 = 1 \quad \text{e} \quad k = \frac{1}{3}(2^{2m+2} - 1). \tag{3.23}$$

Pelos valores encontrados, relacionando em (3.11), temos que $t = 1$ e

$$d = Z_1 \tag{3.24}$$

exceto o caso da equação (3.23).

Portanto, por (3.13) e (3.24):

$$d \mid h(-4n) \tag{3.25}$$

exceto quando se vale (3.23).

Mais ainda, pelo Corolário 3.1.1 concluímos das equações (3.23) e (3.25) que o Teorema 3.1.1 está provado.

□

Referências

[1] T. M. Apostol. *Introduction to analytic number theory.* Springer Science Business Media, New York, 1998.

[2] J. P. de O. Santos. *Introdução à Teoria dos Números.* IMPA, Rio de Janeiro, 1998.

[3] Z. I. Borevich e I. R. Shafarevich. *Number Theory.* Academic press, London, 1966.

[4] S. Alaca e K. S. Williams. *Introductory Algebraic Number Theory.* Cambridge University Press, New York, 2004.

[5] C. Heuberger e M. H. Le. *On the generalized Ramanujan–Nagell equation* $x^2 + D = p^Z$. *Number Theory*, pages 312–331, 1999.

[6] K. Ireland e M. Rosen. *A classical introduction to modern number theory.* Springer Science Business Media, 1990.

[7] Z. Minhui e W. Tingting. *The divisibility of the class number of the imaginary quadratic field* $\mathbb{Q}(\sqrt{2^{2m} - k^n})$. *Glasgow Math*, pages 149–154, 2012.

[8] A. Garcia e Y. Lequain. *Elementos de álgebra.* IMPA, 2018.

[9] O. Endler. *Teoria dos números algébricos.* IMPA, Rio de Janeiro, 2014.

[10] A. Gonçalves. *Introdução à álgebra.* IMPA, Rio de Janeiro, 2017.

[11] L. K. Hua. *Introduction to number theory.* Springer-Verlag, Berlin, 1982.

[12] Y. Kishi. *Note on the divisibility of the class number of certain imaginary quadratic fields. Glasgow Math*, page 207–208, 2010.

[13] D. Marcus. *Number fields.* Springer-Verlag, 1977.

[14] C. P. Milies. *Anéis e Módulos.* Livraria da Física, 2018.

[15] R. A. Mollin. *Algebraic Number Theory.* CRC Press, Canada, 1999.

[16] J. Shurman. *The ideal class number formula for an imaginary quadratic field. Redação fornecida para um curso de Verão de Teoria dos números na Faculdade Reed*, 2021.

[17] P. M. Voutier. *Primitive divisors of Lucas and Lehmer sequences. Math. Comp*, pages 869–888, 1995.

[18] T. Weston. *Algebraic number theory. Lecture Note given at Harvard*, 1999.

[19] T. Weston. *Lectures on the dirichlet class number formula for imaginary quadratic fields.* 2004.

[20] G. Hanrot Y. Bilu and P. M. Voutier (with an appendix by M. Mignotte). *Existence of primitive divisors of Lucas and Lehmer numbers. Journal Reine Angew*, page 75–122, 2001.

[21] R. Zhao. *The Class Number Formula for Quadratic Fields and Related Results.* 2016.