Universidade Estadual de Campinas

Instituto de Matemática, Estatística
e Computação Científica

Eider de Jesus Avelar da Silva

Códigos Perfeitos sobre Grafos de Inteiros Gaussianos e de Eisenstein-Jacobi

CAMPINAS
2019

Eider de Jesus Avelar da Silva

Códigos Perfeitos sobre Grafos de Inteiros Gaussianos e de Eisenstein-Jacobi

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática Aplicada e Computacional.

Orientadora: Cintya Wink de Oliveira Benedito

Este exemplar corresponde à versão final da Dissertação defendida pelo aluno Eider de Jesus Avelar da Silva, e orientada pela Profa. Dra. Cintya Wink de Oliveira Benedito.

Campinas
2019

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

Si38c

Silva, Eider de Jesus Avelar da, 1962-
Códigos perfeitos sobre grafos de inteiros gaussianos e de Eisenstein-Jacobi / Eider de Jesus Avelar da Silva. – Campinas, SP : [s.n.], 2019.

Orientador: Cintya Wink de Oliveira Benedito.
Dissertação (mestrado profissional) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Códigos corretores de erros (Teoria da informação). 2. Teoria dos grafos. 3. Anéis quocientes. 4. Teoria dos números. I. Benedito, Cintya Wink de Oliveira, 1985-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Perfect codes over gaussian integer graphs and Eisenstein-Jacobi
Palavras-chave em inglês:
Error-correcting codes (Information theory)
Graph theory
Quotient rings
Number theory
Área de concentração: Matemática Aplicada e Computacional
Titulação: Mestre em Matemática Aplicada e Computacional
Banca examinadora:
Cintya Wink de Oliveira Benedito [Orientador]
Reginaldo Palazzo Júnior
Carina Alves
Data de defesa: 26-04-2019
Programa de Pós-Graduação: Matemática Aplicada e Computacional

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0002-9257-4196
- Currículo Lattes do autor: http://lattes.cnpq.br/0106208078290245

Dissertação de Mestrado Profissional defendida em 26 de abril de 2019 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). CINTYA WINK DE OLIVEIRA BENEDITO

Prof(a). Dr(a). REGINALDO PALAZZO JÚNIOR

Prof(a). Dr(a). CARINA ALVES

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Aos meus pais, Genezio Silva (in memória) e Eleura Avelar,
a minha querida e amada esposa Claudia Avelar
e as minhas filhas Rebeca e Rachel Avelar dedico este trabalho.

Agradecimentos

Primeiramente ao meu Deus, toda honra, glória e louvor.

Aos meus pais Genezio Silva (in memória) e Eleura Avelar, pelo amor, educação e todos os ensinamentos que me fizeram quem eu sou.

A minha amada esposa Cláudia, pelo amor, companheirismo e cuidado em todos os momentos da minha vida.

As minhas filhas Rebeca e Rachel, pelo amor e motivação em todos os momentos da jornada.

Aos meus amigos que fiz durante o mestrado, em especial ao Ricardo, Caroline, Dutra, Juscimar e Adriano por todo apoio e companheirismo.

Aos professores da Universidade Ceuma - campus Imperatriz e Uemasul, em especial Fausto Lucena e Murilo Barros, e muitos outros que foram importantes em diversos momentos dessa caminhada.

Aos professores do mestrado pelo conhecimento transmitido, em especial Profa. Dra. Sueli Costa e Prof. Dr. Cristiano Torezzan.

Aos professores da Banca examinadora.

A minha orientadora, Profa. Dra. Cintya Wink de Oliveira Benedito, pela paciência, dedicação e condução sábia em todo processo. Meu muito obrigado!

Resumo

Códigos corretores de erros são uma importante subárea da teoria da informação. O objetivo deste trabalho é a construção de códigos perfeitos para espaços de sinais bidimensionais. Para este fim serão utilizados elementos da teoria dos grafos, números e códigos. As constelações quadráticas e hexagonais serão modeladas por grafos circulantes de grau quatro e seis, respectivamente denominados grafos gaussianos e de Eisenstein-Jacobi. As palavra-código consideradas são os elementos dos anéis quocientes dos inteiros gaussianos e de Eisenstein-Jacobi, e a métrica é baseada na distância dos vértices dos grafos circulantes. O conjunto perfeito dominante da teoria dos grafos, aplica-se nos grafos gaussianos e de Eisenstein-Jacobi. A obtenção deste conjunto de dominação nos leva diretamente a construção de códigos perfeitos sobre grafos dos inteiros gaussianos e de Eisenstein-Jacobi.

Palavras-chave: Grafos circulantes, grafos gaussianos, grafos de Eisenstein-Jacobi, anel quociente e conjunto perfeito dominante.

Abstract

Error-correcting codes are an important sub-area of information theory. The main of this work is the construction of perfect codes for two-dimensional signal spaces. For this purpose will be used elements of graph, number and code theory. The quadratic and hexagonal constellations will be modeled by circulating graphs of degree four and six; Gaussian and Eisenstein-Jacobi graphs respectively. The codewords considered are the elements of the quotient rings of the Gaussian integers and Eisenstein-Jacobi. The metric is based on the distance of the vertices of the circulanting graphs. The perfect dominating set in graph theory applies in the Gaussian and Eisenstein-Jacobi graphs. The attainment of this set of domination leads us directly to the construction of perfect codes over Gaussian integers and Eisentein-Jacobi graphs.

Keywords: Circulanting graphs, gaussian graphs, Eisenstein-Jacobi graphs, quotient ring and perfect dominating set.

Índice de Símbolos

$\mathbb{N}$:	Conjunto dos números naturais
$\mathbb{Z}$:	Conjunto dos números inteiros
$\mathbb{Q}$:	Conjunto dos números racionais
$\mathbb{R}$:	Conjunto dos números reais
$\mathbb{C}$:	Conjunto dos números complexos
$(\mathbf{G},*)$:	Grupo
$(\mathbf{A},+,.)$:	Anel
$\mathbf{I}$:	Ideal
$\langle a_1, a_2, \ldots, a_n \rangle$:	Ideal gerado por $a_1, a_2, \ldots, a_n$
$\langle \alpha \rangle$:	Ideal gerado por α
$a \equiv b \mod m$:	a congruente a b módulo m
$\frac{\mathbf{A}}{\mathbf{I}}$:	Anel quociente de A por I
$\mathrm{Im}(\phi)$:	Imagem do homomorfismo
$\mathrm{Ker}(\phi)$:	Núcleo do homomorfismo
$\mathbb{K}$,$\mathbb{L}$:	Corpos
M,N:	Módulos
$\mathbb{L}\|\mathbb{K}$:	$\mathbb{L}$ extensão de $\mathbb{K}$
$[\mathbb{L} : \mathbb{K}]$:	Grau de $\mathbb{L}$ sobre $\mathbb{K}$
$\mathbb{K}[\mathbf{X}]$:	Conjunto de todos os polinômios na indeterminada $\mathbf{X}$ com coeficientes em $\mathbb{K}$
σ:	Monomorfismo de $\mathbb{K}$ em $\mathbb{C}$
$\prod$:	Produtório
$\sum$:	Somatório
$\mathcal{N}(\alpha)$:	Norma de α
$\mathcal{T}(\alpha)$:	Traço de α
$\mathbf{Q}(d)$:	Corpo quadrático
$\mathbf{Q}(\alpha)$:	Corpo de números
$\mathcal{O}_{\mathbb{K}}$:	Conjunto de todos os inteiros algébricos sobre $\mathbb{Z}$
$\mathcal{N}(\mathbf{I})$:	Norma do ideal I
$\mathcal{D}_{\mathbb{K}}$:	Discriminante de $\mathbb{K}$
$\mathbb{Z}[i]$:	Anel dos inteiros gaussianos
$\mathbb{Z}[\omega]$:	Anel dos inteiros de Eisenstein-Jacobi
$\mathbf{A}$:	Alfabeto
$\mathcal{C}$:	Código corretor de erros
$R(\mathcal{C})$:	Taxa de informação de $\mathcal{C}$
$B(a,t)$:	Bola de centro a e raio t
$S(a,t)$:	Esfera de centro a e raio t
$\lfloor t \rfloor$:	Menor inteiro

$dim_K\mathcal{C}$:	Dimensão do código $\mathcal{C}$
$\omega(x)$:	Peso de x
$\omega(\mathcal{C})$:	Peso de $\mathcal{C}$
$(\mathbb{E}, d)$:	Espaço métrico
S:	Constelação de sinais
$U(S)$:	Grupo de simetrias de S em $\mathbb{E}$
$\mathcal{V}_S(s_0)$:	Região de Voronoi de s_0
$PD(s_0)$:	Perfil de distância global de s_0
$\mathcal{G} = (\mathcal{V}, \mathcal{A})$:	Grafo
$\mathcal{V}$:	Conjunto de vértices
$\mathcal{A}$:	Conjunto de arestas
$\delta(\mathcal{G})$:	Grau mínimo de um grafo
$\Delta(\mathcal{G})$:	Grau máximo de um grafo
K_n:	Grafo completo
Cay:	Grafo de Cayley
$\mathbb{Z}_n$:	Grupo aditivo do inteiros módulo n
$\mathbf{C}_n(a_1, a_2, \ldots, a_n)$:	Grafo circulante
$\mathbb{Z}[\rho]_\alpha$:	Ideal de $\mathbb{Z}[\rho]_\alpha$ gerado por α
D_α:	Distância sobre o anel quociente
$\mathcal{G}_\alpha$:	Grafo gaussiano gerado por α
$W_\alpha(\beta)$:	Peso do vértice β
$\mathcal{J}_\alpha$:	Grafo Eisenstein-Jacobi gerado por α
$\mathcal{V}_\eta$:	Região de Voronoi associada com $\eta \in \mathcal{C}$
t:	Raio de cobertura do código
$\mathbf{B}_t(\eta)$:	Bola de raio t centradas nos pontos de $\mathcal{C}$
$\frac{\mathcal{G}_\alpha}{\beta}$:	Grafo quociente de $\mathcal{G}_\alpha$ por β
$\dim_{\mathbb{Q}}\mathbb{L}$:	Dimensão de $\mathbb{L}$ sobre $\mathbb{Q}$

Sumário

Introdução **12**

1 Conceitos Iniciais **14**
1.1 Conceitos básicos de álgebra 14
1.2 Teoria Algébrica dos Números 26
1.2.1 Corpos quadráticos 28

2 Códigos Corretores de Erros **32**
2.1 Códigos Corretores de Erros 33
2.2 Códigos de Bloco Lineares 36
2.3 Constelações de Sinais e Regiões de Voronoi 42

3 Grafos **43**
3.1 Considerações Históricas 43
3.2 Definições e Terminologia 44
3.3 Grafo Circulante 49
3.4 Grafo Gaussiano 52
3.5 Grafo de Eisenstein-Jacobi 63

4 Códigos Perfeitos sobre Inteiros Gaussianos e Eisenstein-Jacobi **69**
4.1 Códigos Perfeitos sobre Grafos Gaussianos 69
4.1.1 Grafo Quociente 73
4.2 Códigos Perfeitos sobre Grafos de Eisenstein-Jacobi 74

Conclusão **79**

Referências Bibliográficas **80**

Introdução

A teoria dos códigos corretores de erros nasceu em 1948, com a publicação de *A mathematical theory of communication* de C. E. Shannon [19]. Em tal publicação é demonstrado o Teorema da Capacidade do Canal, onde em linhas gerais diz que para a transmissão de dados abaixo de uma certa taxa **C** (símbolos por segundo), chamada de capacidade do canal, é possível obter a probabilidade de erro tão pequena quanto se deseja através de códigos corretores de erros apropriados. Desde então, surgiram importantes trabalhos entre os quais os de D. Slepian [21], na década de 60 e o de G. D. Forney[20], na década de 90, que introduz o conceito de códigos geometricamente uniformes. Esses códigos são caracterizados pela existência de isometrias (simetrias) internas, que permitem a construção de instrumentos para uma análise aprofundada da performance de um código.

A teoria dos códigos corretores de erros trata da correção dos dados obtidos na transmissão. Geralmente na transmissão de informações ocorrem interferências que as modificam. Esse tipo de problema é comum nos meios de comunicação. Para solucioná-los incorpora-se algum tipo de redundância aos dados originais e através delas é possível recuperar as informações originais. A utilização dos códigos corretores de erros provém da necessidade de se armazenar e transmitir grande número de dados, muitos dos quais são sensíveis a erros. Este processo requer cada vez mais sistemas eficientes e seguros. Devido a isto e a grandes avanços tecnológicos, a teoria de códigos corretores de erros continua sendo uma área de forte interesse de estudo atualmente.

Grafos aparecem constantemente como modelos de qualquer estrutura complexa, por exemplo; vias férreas, canalizações de água ou gás, condutores elétricos ou em sistemas de telecomunicações. A teoria dos grafos estuda as estruturas discretas que modelam as relações entre os objetos de um determinado conjunto.

Conjuntos perfeitos t-dominantes resultam na teoria de códigos em códigos perfeitos para a métrica de Hamming e para a métrica de Lee, [16]. Neste contexto de relacionar grafos com códigos, em [29], foi apresentado uma condição suficiente para obter códigos perfeitos t dominantes utilizando grafos gaussianos e grafos de Eisenstein-Jacobi, se estes existirem. Em [24, 29] foi introduzida uma nova métrica proveniente da teoria dos grafos sobre constelações do tipo QAM modeladas por inteiros gaussianos e em [27] sobre constelações hexagonais modeladas por inteiros de Eisenstein-Jacobi. Estas métricas são baseadas na distância dos vértices de grafos circulantes, uma classe dos grafos de Cayley, definidos sobre anéis dos inteiros. Esses grafos são modelos matemáticos das constelações bidimensionais. A partir dessa construção, [11] foram apresentados códigos perfeitos e quase-perfeitos de grafos sobre anéis quocientes de inteiros e também utilizando ordem dos quatérnios. Já em [26], foram estabelecido a conexão de grafos circulantes com códigos esféricos rotulados por grupos cíclicos e códigos perfeitos na métrica de Lee.

Seguindo as construções apresentadas em [11, 24, 29], este trabalho tem como objetivo elucidar tais construções e apresentar novos exemplos de códigos perfeitos utilizando conjuntos t-dominantes sobre grafos de inteiros gaussianos e de Eisenstein-Jacobi, para

espaços de sinais em dimensão 2. Para alcançar tal objetivo, se faz necessário estabelecer uma relação entre a teoria de códigos, a teoria de grafos e a teoria algébrica dos números. Mais precisamente, estabelecendo uma relação entre códigos perfeitos, grafos circulantes e anéis de inteiros de corpos quadráticos.

As palavra-código consideradas neste trabalho são elementos de anéis finitos complexos: anel dos inteiros gaussianos e inteiros de Eisenstein- Jacobi. Os anéis quocientes são definidos mediante uma relação de equivalência determinada pelos múltiplos de um inteiro gerador. Os anéis gaussianos e de Eisenstein-Jacobi possuem uma norma multiplicativa, que determina a cardinalidade do anel quociente e a ordem dos grafos circulantes considerados. Os vértices dos grafos constituem o alfabeto e a adjacência é determinada pela cardinalidade do conjunto de unidades. O conjunto perfeito dominante da teoria de grafos se aplica nos grafos gaussianos e de Eisenstein-Jacobi. Em cada caso existem condições suficientes para a sua existência. A obtenção dos conjuntos de dominação nos leva diretamente na construção de códigos perfeitos sobre os alfabetos considerados.

O software Mathematica e o pacote tikz foram utilizados na construção dos exemplos e na representação geométrica dos códigos.

Este trabalho foi estruturado da seguinte maneira.

No Capítulo 1 apresentamos os elementos algébricos fundamentais para o desenvolvimento deste trabalho. Com esse objetivo definiremos as seguintes estruturas algébricas: grupos, anéis, ideais e corpos, além dos principais resultados envolvendo tais conceitos. Além disso, também apresentamos um estudo sobre a teoria algébrica dos números, definindo conceitos importantes como corpos de números e anéis dos inteiros, tais conceitos serão aplicados em uma família muito importante de corpo de números, os corpos quadráticos.

No Capítulo 2 apresentamos os códigos corretores de erros e resultados importantes aplicados neste trabalho, como o conceito de códigos perfeitos e distância em um código. Para exemplificar, apresentamos uma classe importante de códigos corretores de erros que são os códigos de bloco lineares.

No Capítulo 3 apresentamos definições gerais da teoria de grafos, com objetivo de estudar uma classe especial de grafos: os grafos circulantes. Em especial, estaremos interessados em grafos circulantes de graus 4 e 6 definidos sobre quocientes de anéis de inteiros gaussianos e de Eisenstein-Jacobi, os chamados grafos gaussianos e grafos Eisenstein-Jacobi.

No Capítulo 4 apresentamos a construção de códigos perfeitos sobre grafos gaussianos e de Eisenstein-Jacobi. Definimos conjuntos perfeitos t-dominantes sobre grafos e códigos perfeitos, além de resultados fundamentais na construção desses códigos.

Capítulo 1

Conceitos Iniciais

Neste capítulo iremos apresentar os principais elementos de álgebra e teoria algébrica dos números, que serão necessários para o desenvolvimento dos demais capítulos.

Na Seção 1.1 inicialmente definimos o conceito de operações para então definirmos as estruturas algébricas de grupos, anéis e corpos, e suas principais propriedades. Apresentamos também os conceitos de ideais e anéis quocientes que serão muito importantes neste trabalho. Em seguida, apresentamos algumas definições sobre espaços vetoriais e módulos.

Na Seção 1.2 foram apresentados os conceitos de corpo de números, inteiros algébricos, anel de inteiros, traço, norma e discriminante. Tais conceitos serão aplicados em uma classe muito importante de corpos de números; os corpos quadráticos. Como principais exemplos de anéis inteiros de corpos quadráticos apresentamos os inteiros gaussianos e os inteiros de Eiseistein-Jacobi. Tais anéis serão a estrutura fundamental para a construção de códigos perfeitos via grafos no Capítulo 4.

As principais referências utilizadas neste capítulo foram [1, 3, 4, 11, 13–15, 22, 28, 30].

1.1 Conceitos básicos de álgebra

Nesta seção veremos os conceitos principais de álgebra abstrata que são as ferramentas básicas para o desenvolvimento deste trabalho. Entre eles, conceito de operações, grupos, anéis, ideais, corpos e módulos, assim como suas principais propriedades.

Definição 1.1.1. Seja $\mathbf{E}$ um conjunto não vazio, uma aplicação $* : \mathbf{E} \times \mathbf{E} \to \mathbf{E}$ é chamada *operação* sobre $\mathbf{E}$. Dizemos que $\mathbf{E}$ é um conjunto da operação $*$.

Exemplo 1.1.1. (a) A aplicação $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, tal que $f(x, y) = x + y$ é a operação de adição sobre $\mathbb{Z}$.

(b) A aplicação $f : \mathbb{Q}^* \times \mathbb{Q}^* \to \mathbb{Q}^*$, tal que $f(x, y) = \frac{x}{y}$ é a operação de divisão sobre $\mathbb{Q}^*$.

Seja $*$ uma operação sobre um conjunto não vazio $\mathbf{E}$.

1. Dizemos que $*$ é associativa quando $x * (y * z) = (x * y) * z$, quaisquer que sejam $x, y, z \in \mathbf{E}$.

2. Dizemos que $*$ é comutativa quando $x * y = y * x$, quaisquer que sejam $x, y \in \mathbf{E}$.

3. Dizemos que $\mathbf{e} \in \mathbf{E}$ é um elemento neutro para a operação $*$ quando $\mathbf{e} * x = x * \mathbf{e} = x$, para qualquer $x \in \mathbf{E}$.

4. Dizemos que $x \in \mathbf{E}$ é um elemento simetrizável para a operação $*$ que tem neutro $\mathbf{e}$, se existe $x' \in \mathbf{E}$, tal que $x' * x = \mathbf{e} = x * x'$. O elemento x' é chamado simétrico de x para a operação $*$.

5. Dizemos que um elemento $a \in \mathbf{E}$ é regular (ou simplificável) em relação à operação $*$ se: $a * x = a * y \Rightarrow x = y$ e $x * a = y * a \Rightarrow x = y$, quaisquer que sejam $x, y \in \mathbf{E}$.

6. Sejam $*$ e $\bigtriangleup$ duas operações sobre $\mathbf{E}$. Dizemos que $\bigtriangleup$ é distributiva em relação à operação $*$ se: $x \bigtriangleup (y * z) = (x \bigtriangleup y) * (x \bigtriangleup z)$ e $(y * z) \bigtriangleup x = (y \bigtriangleup x) * (z \bigtriangleup x)$, quaisquer que sejam $x, y, z \in \mathbf{E}$.

Exemplo 1.1.2. Seja $\mathbf{E}$ um conjunto não vazio e $x * y = \sqrt{x^2 + y^2}$, onde $x, y \in \mathbf{E}$. Vamos mostrar que a operação $*$ sobre $\mathbf{E}$ é associativa, comutativa e tem elemento neutro. Sejam $x, y, z \in \mathbf{E}$, assim

- $x * (y * z) = \sqrt{x^2 + (y * z)^2} = \sqrt{x^2 + (\sqrt{y^2 + z^2})^2} = \sqrt{x^2 + y^2 + z^2}$ e $(x * y) * z = \sqrt{(x * y)^2 + z^2} = \sqrt{(\sqrt{x^2 + y^2})^2 + z^2} = \sqrt{x^2 + y^2 + z^2}$. Logo, a operação $*$ é associativa.
- $x * y = \sqrt{x^2 + y^2} = \sqrt{y^2 + x^2} = y * x$, logo $*$ é comutativa.
- $x * \mathbf{e} = \mathbf{e} * x \Rightarrow \sqrt{x^2 + \mathbf{e}^2} = x \Rightarrow x^2 + \mathbf{e}^2 = x^2 \Rightarrow \mathbf{e}^2 = 0 \Rightarrow \mathbf{e} = 0$, logo existe elemento neutro $\mathbf{e}$ para a operação $*$.

Proposição 1.1.1. [1] Se a operação $*$ em $\mathbf{E}$ tem elemento neutro $\mathbf{e}$, ele é único.

Demonstração. Sejam $\mathbf{e}$ e $\mathbf{e}'$ elementos neutros da operação $*$ em $\mathbf{E}$, então por definição temos que: $\mathbf{e} * \mathbf{e}' = \mathbf{e}'$ e $\mathbf{e} * \mathbf{e}' = \mathbf{e}$, respectivamente. Logo, $\mathbf{e}' = \mathbf{e}$. ■

Proposição 1.1.2. [1] Se a operação $*$ em $\mathbf{E}$ é associativa, possui elemento neutro $\mathbf{e}$ e um elemento $x \in \mathbf{E}$ simetrizável, então o simétrico de x é único.

Demonstração. Seja $x \in \mathbf{E}$ simetrizável. Se x' e x'' são simétricos de x, por definição temos que:

$$x' = \mathbf{e} * x' = (x'' * x) * x' = x'' * (x * x') = x'' * \mathbf{e} = x''.$$

■

Definição 1.1.2. Seja $*$ uma operação sobre um conjunto $\mathbf{E}$ não vazio e $\mathbf{A}$ um subconjunto não vazio de $\mathbf{E}$. Dizemos que $\mathbf{A}$ é uma parte fechada de $\mathbf{E}$ para a operação $*$ se, e somente se, $x \in \mathbf{A}$ e $y \in \mathbf{A} \Rightarrow x * y \in \mathbf{A}$, para todo $x, y \in \mathbf{A}$.

A seguir veremos o conceito de grupo que é fundamental para o nosso trabalho, pois eles são usados para capturar a simetria interna de uma estrutura. Anéis e Espaços Vetoriais são grupos juntamente com as suas operações e axiomas adicionais.

Definição 1.1.3. Sejam $\mathbf{G}$ um conjunto não vazio e $*$ uma operação sobre $\mathbf{G}$. Dizemos que $\mathbf{G}$ é um *grupo* em relação a $*$, se, e somente se,

(i) $a * (b * c) = (a * b) * c$, $\forall a, b, c \in \mathbf{G}$ (associativa);

(ii) $\exists \mathbf{e} \in \mathbf{G} \mid a * \mathbf{e} = \mathbf{e} * a = a$,$\forall a \in \mathbf{G}$ (elemento neutro);

(iii) $\forall a \in \mathbf{G}$, $\exists a' \in \mathbf{G} \mid a * a' = a' * a = \mathbf{e}$ (elemento simétrico).

Exemplo 1.1.3. (a) Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são grupos com a operação de adição usual.

(b) Os conjuntos $\mathbb{Q}^*$, $\mathbb{R}^*$ e $\mathbb{C}^*$ são grupos com a operação de multiplicação usual.

Observação 1.1.1. Chamaremos grupos com a operação de adição usual de grupos aditivos e grupos com a operação de multiplicação usual de grupos multiplicativos.

Definição 1.1.4. Um grupo $(\mathbf{G}, *)$ é dito *comutativo* ou *abeliano* se, e somente se, $*$ é comutativa. Além disso, $\mathbf{G}$ é *finito*, quando $\mathbf{G}$ é finito e, a cardinalidade de $\mathbf{G}$ é chamada de *ordem* de $\mathbf{G}$.

Exemplo 1.1.4. O conjunto dos números reais $\mathbb{R}$, munido da operação $*$ definida por $x * y = x + y - 3$ é um grupo comutativo. De fato, para todo $x, y, z \in \mathbb{R}$ temos que:

(i) $x * (y * z) = x + y * z - 3 = x + (y + z - 3) - 3 = x + y + z - 6$ e $(x * y) * z = (x * y) + z - 3 = (x + y - 3) + z - 3 = x + y + z - 6$. Logo, a operação $*$ é associativa.

(ii) $x * \mathbf{e} = \mathbf{e} * x = x \Rightarrow x + \mathbf{e} - 3 = x \Rightarrow \mathbf{e} = 3$. Logo, $\mathbf{e} = 3$ é o elemento neutro.

(iii) Dado $x \in \mathbb{R}$, $\exists y \in \mathbb{R} \mid y = -x$ onde $x * y = x + (-x) - 3 = 3$. Logo, x é simetrizável.

Portanto, $(\mathbb{R}, *)$ é um grupo. Além disso,

(iv) $x * y = x + y - 3 = y + x - 3 = y * x$. Logo $*$ é comutativa.

Portanto, $(\mathbb{R}, *)$ é um grupo comutativo ou abeliano.

A seguir definiremos grupos cíclicos. No Capítulo 3 veremos um exemplo importante de grafos, os grafos circulantes que são grupos cíclicos.

Definição 1.1.5. Seja $\mathbf{G}$ um grupo multiplicativo. Dado $a \in \mathbf{G}$, define-se a *potência* m-ésima de a, para todo $m \in \mathbb{Z}$, da seguinte maneira:

(i) Se $m > 0$, então $a^m = a^{m-1}a$.

(ii) Se $m < 0$, então $a^m = (a^{-m})^{-1}$.

(iii) Se $m = 0$, então $a^0 = \mathbf{e}$ (elemento neutro).

Definição 1.1.6. Um grupo multiplicativo $\mathbf{G}$ é chamado *grupo cíclico*, se existe um elemento $a \in \mathbf{G}$ tal que $\mathbf{G} = \{a^m | m \in \mathbb{Z}\}$. Denotamos por $\mathbf{G} = \langle a \rangle$ e o elemento a é dito *gerador* de $\mathbf{G}$.

Exemplo 1.1.5. O grupo multiplicativo $\mathbf{G} = \{1, -1\}$ é cíclico uma vez que $\mathbf{G} = \{(-1)^m | m \in \mathbb{Z}\} = \langle -1 \rangle = \{1, -1\}$.

Definição 1.1.7. O menor número inteiro $h > 0$, tal que $a^h = \mathbf{e}$ chama-se *período* ou *ordem* do elemento a. Denotamos por $o(a) = h$.

Exemplo 1.1.6. O elemento $i \in \mathbb{C}^*$ tem período 4, pois $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.

Definição 1.1.8. Dado um elemento a de um grupo multiplicativo $\mathbf{G}$, $a^m = \mathbf{e}$ se, e somente se, $m = 0$, dizemos que o elemento a tem *período zero ou ordem zero*, e que o grupo $\langle a \rangle$ é um *grupo cíclico infinito*.

Proposição 1.1.3. [1] Seja a um elemento de um grupo multiplicativo $\mathbf{G}$. Se a ordem de a é $h > 0$, então $\langle a \rangle$ é um grupo finito de ordem h dado por $\langle a \rangle = \{\mathbf{e}, a, a^2, \ldots, a^{h-1}\}$.

Demonstração. Mostraremos primeiro que o conjunto $\{e, a, \ldots, a^{h-1}\}$ tem exatamente h elementos. De fato, se $0 \leq i < j < h$ e $a^i = a^j$, então $0 < j - i < h$ e $a^{j-i} = e$, o que é um absurdo pois $o(a) = h$. Logo, não há elementos iguais nesse conjunto e são h os seus elementos. Mostraremos agora que $\langle a \rangle = \{e, a, a^2, \ldots, a^{h-1}\}$. Para isso, é suficiente mostrar que o primeiro desses conjuntos está contido no segundo. Seja $x \in \langle a \rangle$, então existe $m \in \mathbb{Z}$ de maneira que $x = a^m$. Usando o algoritmo da divisão em $\mathbb{Z}$ com relação aos elementos inteiros m e h temos que existem $q, r \in \mathbb{Z}$ tais que

$$m = hq + r \ (0 \leq r < h).$$

Assim,

$$x = a^m = a^{hq+r} = a^{hq}a^r = (a^h)^q a^r = e^q a^r = ea^r = a^r.$$

Como $0 \leq r < h$, então $x \in \{e, a, a^2, \ldots, a^{h-1}\}$. Logo, $\langle a \rangle \subset \{e, a, a^2, \ldots, a^{h-1}\}$ e portanto, $\langle a \rangle = \{e, a, a^2, \ldots, a^{h-1}\}$. ■

A seguir veremos o conceito de Anel, bem como as suas principais propriedades.

Definição 1.1.9. Seja $\mathbf{A}$ um conjunto não vazio, munido das operações de adição $(+)$ e multiplicação $(\cdot)$. A terna $(\mathbf{A}, +, \cdot)$ é chamada de *Anel*, se $\mathbf{A}$ é um grupo abeliano em relação à operação $(+)$ e se a operação $(\cdot)$ satisfaz as seguintes condições:

(i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $\forall a, b, c \in \mathbf{A}$ (associativa).

(ii) $a \cdot (b + c) = a \cdot b + a \cdot c$, $\forall a, b, c \in \mathbf{A}$ (distributiva).

Definição 1.1.10. Um anel $(\mathbf{A}, +, \cdot)$ é *comutativo*, se a operação $(\cdot)$ for comutativa. E, $(\mathbf{A}, +, \cdot)$ é um anel com *unidade*, se existe $1 \in \mathbf{A}$, tal que $1 \cdot a = a \cdot 1 = a$, para todo $a \in \mathbf{A}$.

Exemplo 1.1.7. Os conjuntos numéricos $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são anéis comutativos com unidade.

Definição 1.1.11. Um anel $(\mathbf{A}, +, \cdot)$ é chamado *domínio* ou *domínio de integridade*, se para todo $a, b \in \mathbf{A}$, com $a \neq 0$ e $b \neq 0$, implica que $a \cdot b \neq 0$, ou equivalentemente, para todo $a, b \in \mathbf{A}$, com $a \cdot b = 0$ implica que $a = 0$ ou $b = 0$.

Definição 1.1.12. Dados $\mathbf{A}$ e $\mathbf{B}$ anéis, uma função $\phi : \mathbf{A} \to \mathbf{B}$ será chamada *homomorfismo de anéis*, se para todo $a, b \in \mathbf{A}$ forem verificadas as seguintes igualdades:

(i) $\phi(a + b) = \phi(a) + \phi(b)$,

(ii) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$,

(iii) $\phi(1_A) = 1_B$,

onde 1_A é o elemento neutro da multiplicação de $\mathbf{A}$ e 1_B é o elemento neutro da multiplicação de $\mathbf{B}$.

Definição 1.1.13. Quando um homomorfismo é injetor ele é chamado *monomorfismo*, e quando for bijetor *isomorfismo*. Dois anéis são considerados idênticos se forem *isomorfos*, ou seja, existem entre eles um isomorfismo. O isomorfismos $\phi : \mathbf{A} \to \mathbf{A}$ é chamado *automorfismos*.

Definição 1.1.14. Seja $\mathbf{A}$ um anel e $\emptyset \neq \mathbf{B} \subset \mathbf{A}$. $\mathbf{B}$ será dito *subanel* de $\mathbf{A}$, se $\mathbf{B}$ é um anel com as mesmas operações de $\mathbf{A}$ porém restritas aos elementos de $\mathbf{B}$.

Definição 1.1.15. Seja $\mathbf{A}$ um anel. Dizemos que um elemento $a \in \mathbf{A}$ é inversível, se existir um elemento $b \in \mathbf{A}$ tal que $a \cdot b = 1$. Neste caso, b é chamado inverso de a.

Ideais são subconjuntos especiais de um anel, por exemplo o conjunto dos pares e ímpares são ideais do anel dos números inteiros $\mathbb{Z}$. É importante salientar que ideais geram anéis. Veremos no Capítulo 4 que códigos perfeitos podem ser obtidos a partir de anéis quocientes gerados por ideais. A seguir apresentamos tais conceitos.

Definição 1.1.16. Um subconjunto não vazio $\mathbf{I}$ de um anel comutativo $\mathbf{A}$ será chamado *ideal* de $\mathbf{A}$, se as seguintes condições são satisfeitas:

(i) Se $a, b \in \mathbf{I}$, então $a - b \in \mathbf{I}$;

(ii) Se $a \in \mathbf{A}$ e $b \in \mathbf{I}$, então $a \cdot b \in \mathbf{I}$.

Exemplo 1.1.8. Todos os subconjuntos do anel $\mathbb{Z}$ dos números inteiros da forma $n\mathbb{Z} = \{nq \mid n, q \in \mathbb{Z}\}$, são ideais. De fato:

- $0 \in n\mathbb{Z}$, pois $0 = n0$.
- Se $q_1, q_2 \in n\mathbb{Z}$, então $nq_1 - nq_2 = n(q_1 - q_2) \in n\mathbb{Z}$.
- Se $q \in n\mathbb{Z}$ e $a \in \mathbb{Z}$, então $a(nq) = n(aq) \in n\mathbb{Z}$

Definição 1.1.17. Seja $\mathbf{A}$ um anel comutativo e $a_1, a_2, \ldots, a_n \in \mathbf{A}$, onde $n \geq 1$. O subconjunto de $\mathbf{A}$, indicado por $\langle a_1, a_2, \ldots, a_n \rangle$, tal que

$$\langle a_1, a_2, \ldots, a_n \rangle = \{x_1a_1 + x_2a_2 + \cdots + x_na_n \mid x_1, x_2, \ldots, x_n \in \mathbf{A}\}$$

é um ideal em $\mathbf{A}$.

Definição 1.1.18. O ideal $\langle a_1, a_2, \ldots, a_n \rangle$ é chamado *ideal gerado* por $a_1, a_2, \ldots, a_n$. Um ideal gerado por um só elemento $a \in \mathbf{A}$ é dito *ideal principal* gerado por a. Neste caso, além da notação $\langle a \rangle$, usa-se também $a\mathbf{A}$. Se todos os ideais de um anel de integridade são principais, então este anel é chamado *anel principal*. Particularmente, se $\mathbf{A}$ é um domínio de integridade onde todo ideal é principal, dizemos que $\mathbf{A}$ é um *domínio principal*.

Exemplo 1.1.9. $\langle 2, 3 \rangle = \mathbb{Z}$

Definição 1.1.19. Seja $\mathbf{I}$ um ideal do anel $\mathbf{A}$. $\mathbf{I}$ será chamado *ideal primo*, se $\mathbf{I} \neq \mathbf{A}$, e se para todo $a, b \in \mathbf{A}$, com $a \cdot b \in \mathbf{I}$, então $a \in \mathbf{I}$ ou $b \in \mathbf{I}$.

Exemplo 1.1.10. O Ideal $3\mathbb{Z}$ em $\mathbb{Z}$ é primo, pois $3\mathbb{Z} \neq \mathbb{Z}$ e

$$ab \in 3\mathbb{Z} \Rightarrow 3|ab \Rightarrow 3|a \text{ ou } 3|b \Rightarrow a \in 3\mathbb{Z} \text{ ou } b \in 3\mathbb{Z}.$$

Definição 1.1.20. Um ideal $\mathbf{M}$ de $\mathbf{A}$ com $\mathbf{M} \neq \mathbf{A}$ é chamado *ideal maximal* se, para todo ideal $\mathbf{I}$ tal que $\mathbf{M} \subset \mathbf{I} \subset \mathbf{A}$ e $\mathbf{M} \neq \mathbf{I}$, temos que $\mathbf{I} = \mathbf{A}$.

Exemplo 1.1.11. $15\mathbb{Z}$ não é ideal máximal de $\mathbb{Z}$, pois $15\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}$.

As congruências (aritmética modular) foram introduzidas por Gauss em 1801, publicada na sua obra prima *"Investigações em aritmética"*. Elas são o instrumento adequado quando damos ênfase ao resto na divisão euclidiana. A seguir veremos a definição, propriedades básicas e resultados importantes como classe residual, para chegarmos na definição de anel quociente.

Definição 1.1.21. Sejam $\mathbf{A}$ um anel e $m \in \mathbf{A}$. Dados $a, b \in \mathbf{A}$, dizemos que a é *congruente* a b módulo m, se $m \mid (a-b)$. Escrevemos, $a \equiv b \mod m$. Se m não divide a diferença $a-b$, então diz-se que a é incongruente a b módulo m. Escrevemos $a \not\equiv b \mod m$

Exemplo 1.1.12. Em $\mathbb{Z}$, tem-se que

$$\begin{aligned} 3 &\equiv 24 \mod 7 \text{ , porque } 7 \mid (3-24) \\ -31 &\equiv 11 \mod 6 \text{ , porque } 6 \mid (-31-11) \\ -15 &\equiv -63 \mod 8 \text{ , porque } 8 \mid (-15+63) \\ 25 &\not\equiv 13 \mod 7 \text{ , porque } 7 \nmid (25-13) \end{aligned}$$

Proposição 1.1.4. [4] Sejam $\mathbf{A}$ um anel e a, b, c, a', b' elementos quaisquer de $\mathbf{A}$. Para algum $m \in \mathbf{A}$, com $m \neq 0$, tem-se que

(i) $a \equiv a \mod m$.

(ii) Se $a \equiv b \mod m$, então $b \equiv a \mod m$.

(iii) Se $a \equiv b \mod m$ e $b \equiv c \mod m$, então $a \equiv c \mod m$.

(iv) Se $a \equiv a' \mod m$ e $b \equiv b' \mod m$, então $a+b \equiv a'+b' \mod m$ e $a \cdot b \equiv a' \cdot b' \mod m$.

Demonstração.

(i) Como $m \neq 0$, então para todo $a \in \mathbf{A}$ segue que $m \mid (a-a)$. Logo, $a \equiv a \mod m$.

(ii) Por hipótese $a \equiv b \mod m$, então $m \mid (a-b)$. Mas como $b-a = -(a-b)$, segue que $m \mid (b-a)$. Logo, $b \equiv a \mod m$.

(iii) Por hipótese $a \equiv b \mod m$ e $b \equiv c \mod m$, então

$$m \mid (a-b) \text{ e } m \mid (b-c) \Rightarrow m \mid [(a-b)+(b-c)] \Rightarrow m \mid (a-c).$$

Logo, $a \equiv c \mod m$.

(iv) Por hipótese $a \equiv a' \mod m$ e $b \equiv b' \mod m$, então

$$m \mid (a-a') \text{ e } m \mid (b-b') \Rightarrow m \mid (a-a')+(b-b') \Rightarrow m \mid (a+b)-(a'-b').$$

Logo, $a+b \equiv a'+b' \mod m$. Como $a \cdot b - a' \cdot b' = a \cdot (b-b') + b'(a-a')$, segue que $m \mid (a \cdot b - a' \cdot b')$. Portanto, $a \cdot b \equiv a' \cdot b' \mod m$. ■

Pela Proposição 1.1.4 verificamos que $\equiv$ é uma relação de equivalência.

Definição 1.1.22. Chamamos de *classe residual* de um elemento $a \in \mathbf{A}$, módulo m, o conjunto

$$\bar{a} = \{x \in \mathbf{A}; x \equiv a \mod m\} = \{a + m \cdot \lambda; \lambda \in \mathbf{A}\}$$

O elemento a será chamado *representante* da classe residual $\bar{a}$. Fazendo $m\mathbf{A} = \{m \cdot \lambda; \lambda \in \mathbf{A}\}$, podemos escrever $\bar{a} = a + m\mathbf{A}$. O conjunto de todas as classes residuais em $\mathbf{A}$ módulo m é denotado por $\mathbf{A}_m$.

Exemplo 1.1.13. Seja $a \in \mathbb{Z}$ e $m = 2$, então $\bar{0}$=$\{x \in \mathbb{Z} \mid x \equiv 0 \mod 2\}$=$\{x \in \mathbb{Z} \mid x$ é par$\}$ e $\bar{1}$=$\{x \in \mathbb{Z} \mid x \equiv 1 \mod 2\}$=$\{x \in \mathbb{Z} \mid x$ é ímpar$\}$. Temos também que $\bar{a} = \bar{0}$, se a é par e $\bar{a} = \bar{1}$, se a é impar.

Exemplo 1.1.14. Seja $a \in \mathbb{Z}$ e $m = 5$, então:

$$\bar{a} = \begin{cases} \bar{0}, \text{ se a é múltiplo de 5} \\ \bar{1}, \text{ se a tem resto 1 quando dividido por 5} \\ \bar{2}, \text{ se a tem resto 2 quando dividido por 5} \\ \bar{3}, \text{ se a tem resto 3 quando dividido por 5} \\ \bar{4}, \text{ se a tem resto 4 quando dividido por 5} \end{cases}$$

Proposição 1.1.5. [4] Quaisquer que sejam os elementos $a, b \in \mathbf{A}$, temos que:

(i) $\bar{a} = \bar{b}$ se, e somente se, $m \mid (a - b)$; ou seja, $a - b \in m\mathbf{A}$.

(ii) $\bar{a} \cap \bar{b} \neq \emptyset$ se, e somente se, $\bar{a} = \bar{b}$.

(iii) $\mathbf{A} = \cup_{a \in \mathbf{A}} \bar{a}$.

(iv) Se $\mathbf{A}$ é um domínio, existe uma bijeção entre $\bar{a}$ e $m\mathbf{A}$.

Demonstração.

(i) Como $a \in \bar{a}$, se $\bar{a} = \bar{b}$, segue que $a \in \bar{b}$. Logo, se $a \equiv b \mod m$ então $b \equiv a \mod m$ e portanto, $m \mid (a - b)$. Reciprocamente, considere $a \equiv b \mod m$. Logo, $x \equiv a \mod m$ se, e somente se, $x \equiv b \mod m$. Portanto, $\bar{a} = \bar{b}$.

(ii) $c \in \bar{a} \cap \bar{b} \iff c \equiv a \mod m$ e $c \equiv b \mod m \iff a \equiv b \mod m \iff \bar{a} = \bar{b}$.

(iii) Para todo $a \in \mathbf{A}$, temos que $a \in \bar{a}$. Logo, $\mathbf{A} \subset \cup_{a \in \mathbf{A}} \bar{a} \subset \mathbf{A}$ e então $\mathbf{A} = \cup_{a \in \mathbf{A}} \bar{a}$.

(iv) Considere a aplicação

$$\begin{array}{rccc} \psi : & m\mathbf{A} & \longrightarrow & \bar{a} \\ & mx & \mapsto & a + mx \end{array}$$

temos que ψ é bem definida e é bijetora, pois

$$\psi(mx) = \psi(my) \Rightarrow a + mx = a + my \Rightarrow x = y.$$

■

Definição 1.1.23. Chama-se *sistema completo de restos módulo m* todo o conjunto $S = \{r_1, r_2, \ldots, r_m\}$ de m inteiros tal que um inteiro qualquer a é congruente módulo m a um único elemento r_i $(1 \leq i \leq m)$ de S.

Teorema 1.1.1. [28] O conjunto $S = \{0, 1, 2, \ldots, m-1\}$ é um sistema completo de restos módulo m.

Demonstração. Com efeito, o conjunto S tem m elementos e, além disso, qualquer que seja o inteiro a, temos pelo algoritmo da divisão que

$$a = mq + r \text{ , com } 0 \leq r \leq m,$$

o que implica que $a \equiv r \mod m$. Como o resto r só pode assumir os m valores $0, 1, 2, \ldots, m-1$, segue-se que o inteiro a é congruente módulo m a um único desses m inteiros. ■

Exemplo 1.1.15. O conjunto $S = \{0, 1, 2, 3, 4, 5, 6\}$ é um sistema completo de restos módulo 7.

Teorema 1.1.2. [28] Se $S = \{r_1, r_2, \ldots, r_m\}$ é um sistema completo de restos módulo m, então os elementos de S são congruentes módulo m aos inteiros $0, 1, 2, \ldots, m-1$, numa certa ordem.

Exemplo 1.1.16. O conjunto $\{-2, -1, 0, 1, 2\}$ é um sistema completo de restos módulo 5, pois:

$$\begin{aligned} -2 &\equiv 3 \mod 5 \\ -1 &\equiv 4 \mod 5 \\ 0 &\equiv 0 \mod 5 \\ 1 &\equiv 1 \mod 5 \\ 2 &\equiv 2 \mod 5. \end{aligned}$$

Observação 1.1.2. As operações de adição e multiplicação definidas em $\mathbf{A}_m$ são respectivamente:

$$\bar{a} + \bar{b} = \overline{a + b}$$
$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

Teorema 1.1.3. [4] O conjunto das classes residuais $\mathbf{A}_m$ munido das operações de adição e multiplicação é um anel com $\bar{0}$ e $\bar{1}$, respectivamente como os elementos neutros para a adição e para a multiplicação.

Demonstração. Pela definição da operação de adição em $\mathbf{A}_m$ e pela associatividade da adição em $\mathbf{A}$, temos que

$$(\bar{a} + \bar{b}) + \bar{c} = \overline{a+b} + \bar{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \bar{a} + \overline{b+c} = \bar{a} + (\bar{b} + \bar{c}).$$

Agora, pela definição das operações em $\mathbf{A}_m$ e pela distributividade da multiplicação com respeito à adição em $\mathbf{A}$, temos que

$$\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \overline{b+c} = \overline{a(b+c)} = \overline{ab + ac} = \overline{a.b} + \overline{a.c} = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}.$$

■

A seguir veremos que anéis quocientes são classes residuais, veremos a sua definição e alguns resultados importantes que são fundamentais para o desenvolvimento dos Capítulos 3 e 4.

A relação de congruência em $\mathbb{Z}$ estudada anteriormente, pode ser definida em termos de ideais da seguinte maneira

$$a \equiv b \mod n \iff b - a \in \langle n \rangle,$$

onde $\langle n \rangle$ é o ideal gerado por n. Generalizando, definimos a seguinte relação binária em anéis.

Definição 1.1.24. Sejam $\mathbf{A}$ um anel e $\mathbf{I}$ um ideal de $\mathbf{A}$. A relação binária em $\mathbf{A}$ é definida por

$$a \equiv b \mod \mathbf{I} \iff b - a \in \mathbf{I}.$$

Proposição 1.1.6. [3] Se $a \equiv b \mod \mathbf{I}$ e $c \equiv d \mod \mathbf{I}$, então $a + c \equiv b + c \mod \mathbf{I}$ e $a.c \equiv b.d \mod \mathbf{I}$.

Definição 1.1.25. Sejam $\mathbf{A}$ um anel, $\mathbf{I}$ um ideal de $\mathbf{A}$ e $a \in \mathbf{A}$. Define-se *a classe residual de a módulo* $\mathbf{I}$, como sendo o conjunto

$$\bar{a} = a + \mathbf{I} = \{a + x \mid x \in \mathbf{I}\}.$$

Sejam $\mathbf{A}$ um anel e $\mathbf{I}$ um ideal de $\mathbf{A}$. Denotamos por $\mathbf{A/I}$ o conjunto das classes residuais dos elementos de $\mathbf{A}$ módulo $\mathbf{I}$ e definimos neste conjunto as seguintes operações de adição e multiplicação

$$\bar{a} + \bar{b} = \overline{a + b}, \text{ isto é } (a + \mathbf{I}) + (b + \mathbf{I}) = (a + b) + \mathbf{I};$$

$$\bar{a} \cdot \bar{b} = \overline{a.b}, \text{ isto é } (a + \mathbf{I})(b + \mathbf{I}) = (ab) + \mathbf{I}.$$

Definição 1.1.26. Seja $\mathbf{A} \neq \mathbf{I}$. $\mathbf{A/I}$ munido das operações definidas acima é um anel, chamado *anel quociente* de $\mathbf{A}$ por $\mathbf{I}$.

Exemplo 1.1.17. Se $\mathbf{A} = \mathbb{Z}$ e $\mathbf{I} = \langle m \rangle$ para algum inteiro $m > 1$, então $\mathbf{A/I} = \mathbb{Z}_m$. Para $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ com as operações de adição e multiplicação apresentadas nas tabelas abaixo é um anel quociente.

$$\left[\begin{array}{c|cc} + & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{1} \\ \bar{1} & \bar{1} & \bar{0} \end{array}\right] \quad \left[\begin{array}{c|cc} \cdot & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{0} \\ \bar{1} & \bar{0} & \bar{1} \end{array}\right]$$

Teorema 1.1.4. [1] Sejam $\mathbf{A}$ e $\mathbf{B}$ anéis e $\phi : \mathbf{A} \to \mathbf{B}$ um homomorfismo, então:

(i) $\mathrm{Im}(\phi)$ é um subanel de $\mathbf{B}$.

(ii) $\mathrm{Ker}(\phi)$ é um ideal de $\mathbf{A}$.

(iii) ϕ é injetora se, e somente se, $\mathrm{Ker}(\phi) = 0$.

(vi) Os anéis $\mathbf{A}/\mathrm{Ker}(\phi)$ e $\mathrm{Im}(\phi)$ são isomorfos (Primeiro Teorema do Isomorfismo).

Teorema 1.1.5. [30] Sejam $\mathbf{I}$ e $\mathbf{J}$ ideais do anel $\mathbf{A}$.

(i) Existe um isomorfismo de anéis $\dfrac{\mathbf{I}}{(\mathbf{I} \cap \mathbf{J})} \cong \dfrac{(\mathbf{I} + \mathbf{J})}{\mathbf{J}}$(Segundo Teorema do Isomorfismo).

(ii) Se $\mathbf{I} \subset \mathbf{J}$, então $\dfrac{\mathbf{J}}{\mathbf{I}}$ é um ideal em $\dfrac{\mathbf{A}}{\mathbf{I}}$ e existe um isomorfismo de anéis $\dfrac{\left(\frac{\mathbf{A}}{\mathbf{I}}\right)}{\left(\frac{\mathbf{J}}{\mathbf{I}}\right)} \cong \dfrac{\mathbf{A}}{\mathbf{J}}$

(Terceiro Teorema do Isomorfismo)

A seguir apresentaremos o conceito de corpo, bem como suas propriedades e principais resultados.

Definição 1.1.27. Um anel comutativo com unidade $\mathbb{K}$, chama-se *corpo*, se todo elemento não nulo de $\mathbb{K}$ é invertível. Ou seja, se para todo $a \in \mathbb{K}$, com $a \neq 0$, existe $b \in \mathbb{K}$ tal que $a \cdot b = 1$.

Exemplo 1.1.18. **(a)** Os anéis $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.

(b) O anel $\mathbb{Z}$ não é corpo, pois os elementos em $\mathbb{Z}$ não possuem inverso multiplicativo.

Definição 1.1.28. Dado um corpo $\mathbb{K}$, um subconjunto $\mathbb{L} \subset \mathbb{K}$, com $\mathbb{L} \neq \emptyset$, é chamado *subcorpo* de $\mathbb{K}$ se:

(i) $1 \in \mathbb{L}$;

(ii) $a, b \in \mathbb{L} \Rightarrow a - b \in \mathbb{L}$ e

(iii) $a, b \in \mathbb{L}$ e $b \neq 0 \Rightarrow a \cdot b^{-1} \in \mathbb{L}$.

Exemplo 1.1.19. O conjunto dos números racionais $\mathbb{Q}$ é subcorpo dos números reais $\mathbb{R}$

Definição 1.1.29. Seja o anel $\mathbf{A}$ um domínio de integridade. Dizemos que um corpo $\mathbb{K}$ é o *corpo de frações* do anel $\mathbf{A}$ se $\mathbb{K}$ for o menor corpo contendo $\mathbf{A}$.

Exemplo 1.1.20. $\mathbb{Q}$ é o corpo das frações do anel $\mathbb{Z}$

Definição 1.1.30. Um corpo $\mathbb{K}$ é finito, quando o conjunto $\mathbb{K}$ é finito. A quantidade de elementos do conjunto $\mathbb{K}$ é chamada *ordem* do corpo $\mathbb{K}$.

Teorema 1.1.6. [4] O anel $\mathbb{Z}_m$ é um corpo se, e somente se, m é um número primo.

Exemplo 1.1.21. $\mathbb{Z}_2$ é um corpo, porém $\mathbb{Z}_6$ não é um corpo , pois $\bar{2} \cdot \bar{3} = \bar{0}$.

Proposição 1.1.7. [3] Sejam $\mathbf{A}$ um anel e $\mathbf{I}$ um ideal de $\mathbf{A}$ com $\mathbf{I} \neq \mathbf{A}$. Temos que

(i) $\mathbf{A/I}$ é um domínio se, e somente se, $\mathbf{I}$ é ideal primo;

(ii) $\mathbf{A/I}$ é um corpo se, e somente se, $\mathbf{I}$ é ideal maximal.

A seguir apresentaremos o conceito e as principais propriedades de espaços vetoriais. Um espaço vetorial é uma estrutura algébrica fechada para as operações de adição e multiplicação por um escalar, com suas respectivas propriedades.

Definição 1.1.31. Sejam dados um corpo $\mathbb{K}$ e um conjunto $\mathbf{V}$. Dizemos que $\mathbf{V}$ é um *espaço vetorial* sobre $\mathbb{K}$, ou um $\mathbb{K}$-*espaço vetorial* $\mathbf{V}$, se forem definidas as operações de adição em $\mathbf{V}$ e uma multiplicação dos elementos de $\mathbf{V}$ por escalares de $\mathbb{K}$

$$\begin{array}{rccc} + : & \mathbf{V} \times \mathbf{V} & \to & \mathbf{V} \\ & (\mathbf{v}, \mathbf{w}) & \mapsto & \mathbf{v} + \mathbf{w} \end{array} \qquad \begin{array}{rccc} \cdot : & \mathbb{K} \times \mathbf{V} & \to & \mathbf{V} \\ & (\lambda, \mathbf{v}) & \mapsto & \lambda \cdot \mathbf{v} \end{array} ,$$

possuindo as seguintes propriedades:

1. $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$.
2. $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$.
3. $\mathbf{u} + \mathbf{0} = \mathbf{u}$.
4. $\mathbf{u} + (-\mathbf{u}) = \mathbf{0}$.
5. $(\lambda + \mu) \cdot \mathbf{u} = \lambda \cdot \mathbf{u} + \mu \cdot \mathbf{u}$.
6. $\lambda \cdot (\mathbf{u} + \mathbf{v}) = \lambda \cdot \mathbf{u} + \lambda \cdot \mathbf{v}$.

7. $(\lambda \cdot \mu) \cdot \mathbf{u} = \lambda \cdot (\mu \cdot \mathbf{u})$.

8. $\forall\ \mathbf{u} \in \mathbf{V}$, $1 \cdot \mathbf{u} = \mathbf{u}$, onde 1 é a unidade de $\mathbb{K}$.

para todo $\mathbf{u}, \mathbf{v} \in \mathbf{V}$ e $\lambda, \mu \in \mathbb{K}$.

Exemplo 1.1.22. O conjunto de todas as n-uplas de números reais $\mathbb{R}^n$ é um $\mathbb{R}$-espaço vetorial. Da mesma forma, $\mathbb{C}^n$ é um $\mathbb{C}$-espaço vetorial.

Exemplo 1.1.23. Seja $\mathbb{K} = \mathbb{Z}_5$. Então, $V = \mathbb{Z}_3$ com as operações de soma e multiplicação módulo-3 é um $\mathbb{Z}_5$-espaço vetorial.

Definição 1.1.32. Dados $\mathbf{V}$ um $\mathbb{K}$-espaço vetorial e $\mathbf{W}$ um subconjunto não vazio de $\mathbf{V}$, então $\mathbf{W}$ munido das operações de adição e multiplicação por escalares definidas em $\mathbf{V}$ é um subespaço vetorial de $\mathbf{V}$, se for também um $\mathbb{K}$-espaço vetorial.

Observação 1.1.3. Para que $\mathbf{W} \subset \mathbf{V}$, com $\mathbf{W} \neq \emptyset$, seja um subespaço vetorial do espaço vetorial $\mathbf{V}$, basta verificarmos que:

$$\forall \mathbf{u}, \mathbf{v} \in \mathbf{W} \text{ e } \forall \lambda \in \mathbb{K}\ ,\ \mathbf{u} + \lambda \cdot \mathbf{v} \in \mathbf{W}.$$

Definição 1.1.33. Dado $\mathbf{V}$ um $\mathbb{K}$-espaço vetorial, então $\mathbf{v}_1, \cdots, \mathbf{v}_n \in \mathbf{V}$ são ditos *linearmente independentes* se $\lambda_1 \cdot \mathbf{v}_1 + \cdots + \lambda_n \cdot \mathbf{v}_n = 0$, com $\lambda_1, \cdots, \lambda_n \in \mathbb{K}$, segue que $\lambda_1 = \cdots = \lambda_n = 0$. Caso contrário, os vetores $\mathbf{v}_1, \cdots, \mathbf{v}_n$ são ditos *linearmente dependentes*.

Definição 1.1.34. Dado $\mathbf{V}$ um $\mathbb{K}$-espaço vetorial, dizemos que um subconjunto $\mathbf{B} = \{\mathbf{v}_1, \cdots, \mathbf{v}_n\} \subset \mathbf{V}$ *gera* $\mathbf{V}$ quando todo elemento $v \in \mathbf{V}$ puder ser escrito da forma

$$v = \lambda_1 \cdot \mathbf{v}_1 + \cdots + \lambda_n \cdot \mathbf{v}_n,$$

com $\lambda_1, \cdots, \lambda_n \in \mathbb{K}$.

Definição 1.1.35. Dado um $\mathbb{K}$-espaço vetorial $\mathbf{V}$. Dizemos que um subconjunto $\mathbf{B}$ de $\mathbf{V}$ é uma *base* de $\mathbf{V}$, se $\mathbf{B}$ gera $\mathbf{V}$ e os elementos de $\mathbf{B}$ forem linearmente independentes sobre $\mathbb{K}$. O número de elementos de uma base é chamado *dimensão* de $\mathbf{V}$ sobre $\mathbb{K}$ e denotado por $\dim_{\mathbb{K}}\mathbf{V}$.

Definição 1.1.36. Sejam $\mathbf{V}$ e $\mathbf{W}$ dois $\mathbb{K}$-espaços vetoriais. Dizemos que uma função $\mathbf{T} : \mathbf{V} \to \mathbf{W}$ é uma *transformação linear* quando a seguinte condição for verificada:

$$\forall \mathbf{u}, \mathbf{v} \in \mathbf{V}, \forall \lambda \in \mathbb{K}, \mathbf{T}(\mathbf{u} + \lambda \cdot \mathbf{v}) = \mathbf{T}(\mathbf{u}) + \lambda \cdot \mathbf{T}(\mathbf{v}).$$

Definição 1.1.37. Seja $\mathbf{T} : \mathbf{V} \to \mathbf{W}$ uma transformação linear.

(i) O *núcleo* de $\mathbf{T}$ é o $\mathbb{K}$-subespaço vetorial de $\mathbf{V}$ definido por

$$\text{Ker}\mathbf{T} = \{\mathbf{v} \in \mathbf{V}; \mathbf{T}(\mathbf{v}) = 0\}.$$

(ii) A *imagem* de $\mathbf{T}$ é o $\mathbb{K}$-subespaço vetorial de $\mathbf{W}$ definido por

$$\text{Im}\mathbf{T} = \{\mathbf{T}(\mathbf{v}); \mathbf{v} \in \mathbf{V}\}$$

A seguir apresentaremos o conceito de módulo sobre um anel, que é a generalização da noção de espaço vetorial, que em vez de um corpo, temos um anel como o conjunto de escalares.

Definição 1.1.38. Seja **A** um anel. Um conjunto não vazio **M** é dito um **A-módulo** se **M** é um grupo abeliano com relação à operação $(+)$ e munido de uma aplicação $\phi : \mathbf{A} \times \mathbf{M} \to \mathbf{M}$, definida por $\phi(a, m) = am$, que satisfaz:

(i) $a(m + n) = am + an$;

(ii) $(a + b)m = am + bn$;

(iii) $(ab)m = a(bm)$;

(iv) $1m = m$,

para todo $a, b \in \mathbf{A}$ e $m, n \in \mathbf{M}$.

Definição 1.1.39. Um subgrupo aditivo N do A-módulo M é chamado A-**submódulo** de M se para todo $a \in A$ e $n \in N$ então $an \in N$.

Dado um A-módulo M e um A-submódulo N podemos construir o **módulo quociente** M/N da mesma forma como construímos o anel quociente, onde

$$a(m + N) = am + N,$$

para todo $a \in A$ e $m \in M$.

Definição 1.1.40. Um A-módulo M é chamado *finitamente gerado* se existem elementos $x_1, x_2, \ldots, x_n \in M$ tal que todo $m \in M$ é da forma $m = a_1x_1 + a_2x_2 + \cdots + a_nx_n$, com $a_i \in A$, onde $i = 1, \ldots, n$. Neste caso, dizemos que $x_1, x_2, \ldots, x_n$ formam um sistema de geradores de M.

Definição 1.1.41. Sejam A um anel, M um A-módulo e $x_1, \ldots, x_n \in M$. Dizemos que $\{x_1, \ldots, x_n\}$ é uma base de M se $x_1, \ldots, x_n$ forma um sistema de geradores de M e se forem linearmente independentes, ou seja, se existem $a_1, \ldots, a_n \in A$, tais que $a_1x_1 + a_2x_2+, \ldots, a_nx_n = 0$ implica $a_i = 0$, para todo $i = 1, \ldots, n$.

Definição 1.1.42. Um A-módulo que possui uma base é chamado *A-módulo livre*.

Definição 1.1.43. Sejam A um anel e M, N dois A-módulos. Dizemos que uma aplicação $f : M \to N$ é um **homomorfismo de A-módulos** se satisfaz as seguintes condições:

(i) $f(x + y) = f(x) + f(y)$

(ii) $f(ax) = af(x)$,

para todo $x, y \in M$ e $a \in A$. Se além disso, a aplicação f for injetora, dizemos que f é um **monomorfismo de A-módulos** e, se f for bijetora dizemos que f é um **isomorfismo de A-módulos**.

Teorema 1.1.7. [22](Teorema do Isomorfismo de Módulos) Se A é um anel, M, N são dois A-módulos e $f : M \to N$ um homomorfismo de A-módulos, então os módulos $M/Ker(f)$ e $Im(f)$ são isomorfos.

1.2 Teoria Algébrica dos Números

Nesta seção apresentaremos os principais conceitos, propriedades e resultados de teoria algébrica dos números. Vamos apresentar os conceitos de inteiros algébricos, corpo de números, anel dos inteiros, norma, traço e discriminante. Tais conceitos serão exemplificados em uma classe muito importante de corpos de números que são os corpos quadráticos.

Definição 1.2.1. Sejam $\mathbb{L}$ um corpo e $\mathbb{K}$ um subcorpo de $\mathbb{L}$. Dizemos que $\mathbb{L}$ é uma *extensão* de $\mathbb{K}$, e denotamos por $\mathbb{L} \mid \mathbb{K}$.

Definição 1.2.2. A dimensão de $\mathbb{L}$ como $\mathbb{K}$-espaço vetorial, denotada por $[\mathbb{L} : \mathbb{K}]$ é chamada *grau da extensão*. Dizemos que $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$ de grau $[\mathbb{L} : \mathbb{K}] = n$, quando uma base do $\mathbb{K}$-espaço tiver n elementos.

Definição 1.2.3. Para qualquer $\alpha \in \mathbb{L}$, se existir $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ não nulo, tal que, $\mathrm{P}(\alpha) = 0$, então o elemento α será chamado *algébrico* sobre $\mathbb{K}$. Se $\alpha \in \mathbb{L}$ não for algébrico será chamado *transcendente* sobre $\mathbb{K}$.

Exemplo 1.2.1. Seja $\alpha = \sqrt{3} \in \mathbb{R}$. Temos que α é algébrico sobre $\mathbb{Q}$, pois α é raiz do polinômio $X^2 - 3 \in \mathbb{Q}[\mathrm{X}]$.

Exemplo 1.2.2. Considere agora $\alpha = 3 + \sqrt{2} \in \mathbb{R}$. Observe que

$$(\alpha - \sqrt{2})^2 = 9 \Longrightarrow \alpha^2 - 2\alpha\sqrt{2} + 2 = 9 \Longrightarrow (\alpha^2 - 7)^2 = (2\sqrt{2}\alpha)^2 \Longrightarrow \alpha^4 - 22\alpha^2 + 49 = 0.$$

Logo, existe um polinômio $\mathrm{P(X)} = X^4 - 22X^2 + 49 \in \mathbb{Q}[\mathrm{X}]$, tal que $\alpha = 3 + \sqrt{2} \in \mathbb{R}$ é raiz. Portanto, α é algébrico sobre $\mathbb{Q}$.

Definição 1.2.4. Se $\alpha \in \mathbb{L}$ é um número algébrico sobre $\mathbb{K}$, então existe um único polinômio irredutivel mônico $\mathrm{P}_{\alpha|K}$ de grau mínimo tal que $\mathrm{P}_{\alpha|K}(\alpha) = 0$. $\mathrm{P}_{\alpha|K}$ é chamado *polinômio minimal* de α sobre $\mathbb{K}$.

Definição 1.2.5. Um *corpo de números* $\mathbb{L}$ é uma extensão finita do corpo $\mathbb{Q}$ dos números racionais. Se $\dim_{\mathbb{Q}}\mathbb{L} = n$, dizemos que $\mathbb{L}$ é um corpo de números de grau n.

Definição 1.2.6. Sejam $\mathbb{L}$ um corpo e $\mathbb{K}$ um subcorpo de $\mathbb{L}$. Dizemos que $\mathbb{L}$ é uma extensão algébrica de $\mathbb{K}$ se todo $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$. Uma extensão $\mathbb{L}$ de $\mathbb{K}$ algébrica é finita se existirem elementos $\alpha_1, \alpha_2, \ldots, \alpha_n$ algébricos sobre $\mathbb{K}$ tais que $\mathbb{L} = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Definição 1.2.7. Seja $\mathbb{K}$ um corpo de números. Se $\alpha \in \mathbb{K}$ é raiz de um polinômio mônico $\mathrm{P(X)} \in \mathbb{Z}[\mathrm{X}]$, dizemos que α é um *inteiro algébrico* sobre $\mathbb{Z}$.

Exemplo 1.2.3. $\sqrt[5]{10}$ é um inteiro algébrico, pois é raiz do polinômio $X^5 - 10 \in \mathbb{Z}[\mathrm{X}]$.

Teorema 1.2.1. [13] Se $\mathbb{K}$ é um corpo de números, então $\mathbb{K} = \mathbb{Q}(\alpha)$ para algum inteiro algébrico α.

O conjunto de todos os inteiros algébricos de um corpo forma um anel, chamado de anel dos inteiros que definiremos a seguir.

Definição 1.2.8. Sejam $\mathbb{K}$ um corpo de números e $\alpha \in \mathbb{K}$ um inteiro algébrico sobre $\mathbb{Z}$. O conjunto de todos os inteiros algébricos α sobre $\mathbb{Z}$ denotado por

$$\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K}; f(\alpha) = 0, f(x) \in \mathbb{Z}[\mathrm{X}]\}$$

é um anel, chamado de *anel dos inteiros* de $\mathbb{K} \mid \mathbb{Q}$.

Definição 1.2.9. Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$. Uma $\mathbb{Z}$-base do grupo abeliano $\mathcal{O}_{\mathbb{K}}$ é chamada *base integral* de $\mathbb{K}$, ou de $\mathcal{O}_{\mathbb{K}}$. Se $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base integral de $\mathcal{O}_{\mathbb{K}}$, então todo elemento $\alpha \in \mathcal{O}_{\mathbb{K}}$ pode ser escrito de modo único como $\alpha = \sum_{i=1}^{n} a_i\alpha_i$, onde $a_i \in \mathbb{Z}$ para todo $i = 1, \ldots, n$.

Proposição 1.2.1. [14] Se $\mathbb{K}$ é um corpo de números de grau n, então todo ideal $\mathbf{I} \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n.

Teorema 1.2.2. [13] Se $\mathbb{K}$ é um corpo de números e $[\mathbb{K} : \mathbb{Q}] = n$, então existem n monomorfismos distintos σ_i de $\mathbb{K}$ em $\mathbb{C}$ que fixam $\mathbb{Q}$ definidos por $\sigma_i(\alpha) = \alpha_i$, para todo $i = 1, \ldots, n$, onde $\alpha_1, \ldots, \alpha_n$ são as raízes do polinômio minimal $f(X) \in \mathbb{Q}[\mathrm{X}]$.

Definição 1.2.10. Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os n-monomorfismos distintos

$$\sigma_i : \mathbb{K} \to \mathbb{C}$$

Dizemos que σ_i é um *homomorfismo real* se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$. Caso contrário dizemos que σ_i é um *homomorfismo imaginário*. Se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$ para todo $i = 1, \ldots, n$, então dizemos que $\mathbb{K}$ é um corpo *totalmente real*. Caso σ_i seja imaginário para todo $i = 1, \ldots, n$, dizemos que $\mathbb{K}$ é um corpo *totalmente imaginário*.

A seguir definimos os conceitos de traço e norma.

Definição 1.2.11. Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão de corpos com $[\mathbb{L} : \mathbb{K}] = n$. Se $\sigma_1, \ldots, \sigma_n$ são os n-monomorfismos distintos de $\mathbb{L}$ em $\mathbb{C}$ que fixam $\mathbb{Q}$, então definimos

$$\mathcal{N}(\alpha) = \mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad \text{e} \quad \mathcal{T}r(\alpha) = \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha) = \sum_{i=0}^{n} \sigma_i(\alpha),$$

como a *norma* e o *traço* de um elemento $\alpha \in \mathbb{L}$, respectivamente.

Observação 1.2.1. Seja $\mathbb{L} \subseteq \mathbb{K}$ um corpo de números com dimensão $[\mathbb{L} \mid \mathbb{K}] = n$. As seguintes propriedades são válidas para todo $x_1, x_2 \in \mathbb{L}$ e $\alpha \in \mathbb{K}$:

1. $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(x_1 + x_2) = \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(x_1) + \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(x_2)$
2. $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha x_1) = \alpha\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(x_1)$
3. $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha) = n\alpha$
4. $\mathcal{N}_{\mathbb{L}|\mathbb{K}}(x_1x_2) = \mathcal{N}_{\mathbb{L}|\mathbb{K}}(x_1)\mathcal{N}_{\mathbb{L}|\mathbb{K}}(x_2)$
5. $\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha x_1) = \alpha^n\mathcal{N}_{\mathbb{L}|\mathbb{K}}(x_1)$
6. $\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha) = \alpha^n$

Proposição 1.2.2. [13] Se $\alpha \in \mathbb{K}$ é um inteiro algébrico então $\mathcal{N}_{\mathbb{K}|\mathbb{Q}}(\alpha)$ e $\mathcal{T}_{\mathbb{K}|\mathbb{Q}}(\alpha)$ são elementos inteiros.

Definição 1.2.12. Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\mathbf{I}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Define-se como *norma do ideal* $\mathbf{I}$ a cardinalidade do anel quociente $\mathcal{O}_{\mathbb{K}}/\mathbf{I}$ dada por

$$\mathcal{N}(\mathbf{I}) = \#\frac{\mathcal{O}_{\mathbb{K}}}{\mathbf{I}}.$$

Teorema 1.2.3. [13] Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ seu respectivo anel de inteiros. Se $\mathbf{I} = \langle\alpha\rangle$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$ então $\mathcal{N}(\mathbf{I}) =\mid \mathcal{N}(\alpha) \mid$.

Proposição 1.2.3. [11] A norma $\mathcal{N}(\mathbf{I})$ do ideal $\mathbf{I}$ é finita.

Definição 1.2.13. Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ que fixam $\mathbb{Q}$ e $\{\beta_1, \ldots, \beta_n\}$ uma base integral de $\mathbb{K}$ sobre $\mathbb{Q}$. Definimos o *discriminante* dessa base por

$$\mathcal{D}_{\mathbb{K}} = \left[det \begin{pmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \ldots & \sigma_n(\beta_1) \\ \sigma_1(\beta_2) & \sigma_2(\beta_2) & \ldots & \sigma_n(\beta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \sigma_2(\beta_n) & \ldots & \sigma_n(\beta_n) \end{pmatrix} \right]^2 = det[\sigma_j(\beta_i)]^2.$$

1.2.1 Corpos quadráticos

Nesta subseção apresentaremos uma classe de corpo de números muito importante, os corpos quadráticos. Exemplificaremos os conceitos de anel dos inteiros, traço, norma e discriminante vistos anteriormente para esta classe de corpos. Em especial, veremos os exemplos dos inteiros gaussianos e inteiros de Eiseistein-Jacobi, que são anéis de inteiros de corpos quadráticos. Tais anéis serão a base para as construções de códigos perfeitos a serem apresentadas neste trabalho.

Definição 1.2.14. Um *corpo quadrático* é uma extensão de grau 2 sobre o corpo $\mathbb{Q}$ dos números racionais.

Proposição 1.2.4. [11] Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.

Demonstração. Se $\mathbb{K}$ é um corpo quadrático, então todo elemento $\alpha \in \mathbb{K}$ tal que $\alpha \notin \mathbb{Q}$ é de grau 2 sobre $\mathbb{Q}$. Pelo Teorema 1.2.1 temos que $\mathbb{K} = \mathbb{Q}(\alpha)$. Tomando o polinômio minimal de α sobre $\mathbb{K}$, $m_\alpha(X) = X^2 + bX + c$, e resolvendo a equação quadrática $\alpha^2 + b\alpha + c = 0$, obtemos que $2\alpha = -b \mp \sqrt{b^2 - 4c}$. Portanto, $\mathbb{K} = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{b^2 - 4c})$. Observando que $b^2 - 4c$ é um número racional da forma $\frac{u}{v} = \frac{uv}{v^2}$,com u,$v \in \mathbb{Z}$, temos que $\mathbb{Q}(\sqrt{b^2 - 4c}) = \mathbb{Q}(\sqrt{uv})$. Assim, como $uv \in \mathbb{Z}$, segue que uv é fatorado em produtos de primos. Portanto, $\mathbb{Q}(uv) = \mathbb{Q}(\sqrt{d})$,onde d é inteiro livre de quadrados. ■

Exercício 1.2.1. São exemplos de corpos quadráticos:

(i) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

(ii) $\mathbb{Q}(i) = \{a + b\sqrt{i} \mid a, b \in \mathbb{Q}\}$, onde $i^2 = -1$.

Observação 1.2.2. O elemento $\sqrt{d} \in \mathbb{K}$ é uma raiz do polinômio irredutível $x^2 - d$, e seu conjugado é $-\sqrt{d}$. Assim, os monomorfismos de um corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ são

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d} \quad \text{e} \quad \sigma_2(a + b\sqrt{d}) = a - b\sqrt{d},$$

com $a, b \in \mathbb{Q}$. Deste modo, temos que o traço e a norma de um corpo quadrático serão da forma

$$\mathcal{T}r(a + b\sqrt{d}) = \sigma_1(a + b\sqrt{d}) + \sigma_2(a + b\sqrt{d}) = 2a \in \mathbb{Q}$$

e

$$\mathcal{N}(a + b\sqrt{d}) = \sigma_1(a + b\sqrt{d})\sigma_2(a + b\sqrt{d}) = a^2 - db^2 \in \mathbb{Q}.$$

Exemplo 1.2.4. Seja $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ um corpo quadrático. Dado que $\sigma_1(a+b\sqrt{d}) = a+b\sqrt{d}$ e $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$, se $x = a + b\sqrt{3} \in \mathbb{K}$, então

$$\mathcal{N}(x) = a^2 - 3b^2 \quad \text{e} \quad \mathcal{T}r(x) = 2a.$$

Teorema 1.2.4. [13] Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadráticode modo que $d \not\equiv 0 \mod 4$.

(i) Se $d \equiv 2$ ou $d \equiv 3 \mod 4$, então o anel dos inteiros de $\mathbb{K}$ é dado por $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\sqrt{d}\right] = \{a + b\sqrt{d}; a, b \in \mathbb{Z}\}$ e $\{1, \sqrt{d}\}$ é uma base integral.

(ii) Se $d \equiv 1 \mod 4$, então o anel dos inteiros de $\mathbb{K}$ é dado por $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{\frac{1}{2}(a + b\sqrt{d}); a, b \in \mathbb{Z} \text{ e de mesma paridade}\right\}$ e $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ é uma base integral.

Demonstração. Como $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático com d livre de quadrados e $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ é um inteiro algébrico, temos pela Proposição 1.2.2 que $2a$ e $a^2 - db^2$ são números inteiros. Fazendo $a = p/2, b = q/2$ com $a, b \in \mathbb{Z}$ obtemos $a^2 - db^2 = p^2 - dq^2 \in 4\mathbb{Z}$. Note que se $d \equiv 2$ ou $3 \mod 4$ então p e q são pares, caso contrário teríamos $p^2 \equiv dq^2 \equiv d \mod 4$ o que é equivalente a dizer que $d \equiv 0 \mod 4$ ou $d \equiv 1 \mod 4$, o que é um absurdo. Portanto, concluímos que q é par e assim $q^2 \equiv 0 \mod 4$. Segue que $p^2 \equiv dp^2 \equiv 0 \mod 4$, o que implica dizer que p também é par. Logo, se $\alpha = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$ então $\alpha \in \mathbb{Z}[\sqrt{d}]$ e assim $\mathcal{O} \subset \mathbb{Z}[\sqrt{d}]$.
Por outro lado, tomando $\alpha \in \mathbb{Z}[\sqrt{d}]$, temos que α é raiz do polinômio $x^2 - 2ax + a^2 - db^2$, pois $2a, a^2 - db^2 \in \mathbb{Z}$. Logo, $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathbb{K}}$. Portanto $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$.
Caso seja $d \equiv 1 \mod 4$, então p e q tem a mesma paridade, pois $p^2 - dq^2 \in 4\mathbb{Z}$. Se p e q são pares então $a, b \in \mathbb{Z}$. Logo, $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Mas se p e q são ímpares, então $\alpha = a + b\sqrt{d} = p/2 + q/2\sqrt{d} = (p-q)/2 + q((1+\sqrt{d})/2) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Portanto, $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, ou seja, $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Por outro lado, se $\alpha = a+b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ com $a, b \in \mathbb{Z}$, temos que $2a+b \in \mathbb{Z}$ e $(a+b/2)^2-d(b/2)^2 = a^2+ab+(1-d)b^2/4 \in \mathbb{Z}$, pois $d \equiv 1 \mod 4$. Logo, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subset \mathcal{O}_{\mathbb{K}}$, pois os coeficientes

do polinômios minimal de $\alpha, m(x) = x^2 - (2a+b)x + a^2 + ab + (1-d)b^2/4$ estão em $\mathbb{Z}$. Portanto, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathcal{O}_{\mathbb{K}}$. ■

Exemplo 1.2.5. Seja $\mathbb{K} = \mathbb{Q}(\sqrt{3})$, então $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$ e $\{1, \sqrt{3}\}$ é uma base integral de $\mathcal{O}_{\mathbb{K}}$. Seja $\mathbf{I} = (2-\sqrt{3})\mathcal{O}_{\mathbb{K}} = \langle 2-\sqrt{3}\rangle$ é um ideal de $\mathcal{O}_{\mathbb{K}}$, então pelo Teorema 1.2.3, obtemos

$$\begin{aligned} \mathcal{N}(\mathbf{I}) &= |\,\mathcal{N}(\alpha)\,| \\ &= |\,(2-\sqrt{3})(2+\sqrt{3})\,| \\ &= |\,4-3\,| \\ &= 1. \end{aligned}$$

Proposição 1.2.5. [13] Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ será dado por:

(i) $\mathcal{D}_{\mathbb{K}} = d$ se $d \equiv 1 \mod 4$.

(ii) $\mathcal{D}_{\mathbb{K}} = 4d$ se $d \equiv 2$ ou $d \equiv 3 \mod 4$.

Demonstração. Sejam σ_1 e σ_2 os $\mathbb{Q}$-monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$ que fixam $\mathbb{Q}$, com $d \in \mathbb{Z}$ livre de quadrados, definidos por $\sigma_1(a+b\sqrt{d}) = a+b\sqrt{d}$ e $\sigma_2(a+b\sqrt{d}) = a-b\sqrt{d}$. Se $d \equiv 2$ ou $3 \mod 4$ então $\{1, \sqrt{d}\}$ é uma base integral de $\mathbb{K}$ sobre $\mathbb{Q}$, logo por definição obtemos:

$$\mathcal{D}_{\mathbb{K}} = \left[det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{d}) & \sigma_2(\sqrt{d}) \end{pmatrix}\right]^2 = \left[det\begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}\right]^2 = \left[-\sqrt{d} - \sqrt{d}\right]^2 = 4d.$$

De maneira análoga, se $d \equiv 1(\mod 4)$ teremos que $\{1, \frac{1+\sqrt{d}}{2}\}$ será uma base integral de $\mathbb{K}$ sobre $\mathbb{Q}$, logo por definição, temos que:

$$\mathcal{D}_{\mathbb{K}} = \left[det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{d}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{d}}{2}\right) \end{pmatrix}\right]^2 = \left[det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{pmatrix}\right]^2 = d.$$

■

Exemplo 1.2.6. **(i)** Se $\mathbb{K} = \mathbb{Q}(\sqrt{3})$, então o discriminante de $\mathbb{K}$ é $\mathcal{D}_{\mathbb{K}} = 4.3 = 12$.

(ii) Se $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, então o discriminante de $\mathbb{K}$ é $\mathcal{D}_{\mathbb{K}} = 5$.

Para finalizar este capítulo, definimos dois anéis dos inteiros de corpos quadráticos que serão muito importante no nosso trabalho: os inteiros gaussianos e os inteiros de Eisenstein-Jacobi. Nas Seções 3.4 e 3.5 as propriedades e os principais resultados sobre os inteiros gaussianos e os inteiros de Eisenstein-Jacobi serão apresentados, respectivamente, e grafos a partir deles serão obtidos.

Definição 1.2.15. Um *inteiro gaussiano* é um número complexo da forma $a+bi$ com a e b inteiros. Tomando o corpo de números $\mathbb{K} = \mathbb{Q}\left(\sqrt{-1}\right) = \{a + b\sqrt{-1} | a, b \in \mathbb{Q}\}$, então o anel dos inteiros de $\mathbb{K}$, $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$, onde $i = \sqrt{-1}$, é chamado de *anel dos inteiros gaussianos* .

Definição 1.2.16. Tomando o corpo de números $\mathbb{K} = \mathbb{Q}\left(\sqrt{-3}\right) = \{a + b\sqrt{-3} | a, b \in \mathbb{Q}\}$, o anel dos inteiros de $\mathbb{K}$, $\mathbb{Z}[\omega] = \{x + y\omega | x, y \in \mathbb{Z}\}$, onde $\omega = \dfrac{-1 + \sqrt{-3}}{2}$, é chamado de *anel dos inteiros de Eisenstein-Jacobi* .

Capítulo 2

Códigos Corretores de Erros

Neste capítulo iremos apresentar os principais conceitos que envolvem esta teoria. Na Seção 2.1, conceitos gerais sobre códigos corretores de erros serão definidos, finalizando a seção definindo códigos perfeitos, conceito que será de grande importância neste trabalho. Na Seção 2.2, apresentamos uma classe muito importante de códigos corretores de erros, que são os códigos de bloco lineares, exemplificando a sua codificação e decodificação. E, na Seção 2.3, apresentamos os conceitos de constelação de sinais, região de Voronoi e códigos geometricamente uniformes. As principais referências utilizadas neste capítulo foram [4, 5, 11]

A seguir ilustraremos os princípios dessa teoria com um exemplo.

Suponhamos que temos um robô que se move sobre um tabuleiro quadriculado, de modo que, ao darmos um dos comandos (Leste, Oeste, Norte ou Sul), o robô se desloca do centro de uma casa para o centro da casa contígua indicada pelo comando.

Os quatro comandos acima podem ser codificados como elementos de $\{0,1\} \times \{0,1\}$ como se segue:

$$\begin{array}{rcl} Leste & \rightarrow & 00 \\ Oeste & \rightarrow & 01 \\ Norte & \rightarrow & 10 \\ Sul & \rightarrow & 11 \end{array}$$

A representação binária de cada uma dessas quatro mensagens igualmente prováveis é como mostrada no lado direito. Suponhamos, agora, que esses pares ordenados devam ser transmitidos via um canal e que o sinal no caminho sofra interferências. Imaginemos que a mensagem 00 possa, na chegada, ser recebida como 01, o que faria com que o robô, em vez de ir para o Leste, fosse para Oeste. O que se faz, então, é introduzir redundâncias que permitam detectar e corrigir erros.

Podemos, por exemplo, realizar o seguinte mapa:

$$\begin{array}{rcl} 00 & \rightarrow & 00000 \\ 01 & \rightarrow & 01011 \\ 10 & \rightarrow & 10110 \\ 11 & \rightarrow & 11101 \end{array}$$

Note que as duas primeiras posições reproduzem a representação binária das mensagens, enquanto que as três posições restantes são as redundâncias introduzidas. O mapa estabelecido é chamado *código de canal*. Esse procedimento pode ser esquematizado como mostra a Figura 2.1.

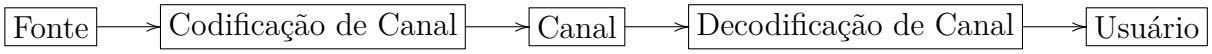

Figura 2.1

2.1 Códigos Corretores de Erros

Definição 2.1.1. Seja **A** um conjunto finito, chamado *alfabeto*, com q elementos ($|\mathbf{A}|$= q). Um *código corretor de erros* $\mathcal{C}$, de comprimento n é um subconjunto próprio qualquer de $\mathbf{A}^n$. Cada elemento de $\mathcal{C}$ é chamado *palavra-código* (no alfabeto **A**).

Exemplo 2.1.1. O conjunto $C = \{00, 11, 22\}$ é um código sobre o corpo finito $\mathbb{F}_3$.

Definição 2.1.2. Seja $m = |\mathcal{C}|$, o número de palavra-código de um código corretor de erros . A taxa de informação de $\mathcal{C}$ é definida como:

$$R(\mathcal{C}) = \frac{\log_q m}{n}.$$

Se o conjunto **A** for um corpo finito e $\mathcal{C}$ for um subespaço vetorial de dimensão k de $\mathbf{A}^n$, teremos que $|\mathcal{C}|= \mathbf{q}^k$, portanto $R(\mathcal{C}) = \dfrac{k}{n}$

Assumindo que todas as palavras do código são equiprováveis, uma forma de decodificar utilizada é a decodificação por *máxima verossimilhança*. Ou seja, a palavra recebida será interpretada como a palavra-código que está "mais próxima" dela. Essa noção de proximidade é expressada por uma função distância no conjunto $\mathbf{A}^n$ definida a seguir.

Definição 2.1.3. Uma função $d : \mathbf{A}^n \times \mathbf{A}^n \to \mathbb{R}$ é chamada *função distância* se, e somente se, satisfaz as seguintes propriedades:

(i) Positividade: $d(x, y) \geq 0$ e $d(x, y) = 0 \iff \mathbf{x} = \mathbf{y}$.

(ii) Simetria: $d(x, y) = d(y, x)$.

(iii) Desigualdade Triangular: $d(x, y) \leq d(x, z) + d(z, y)$.

Uma função distância muito utilizada é a *distância de Hamming*, que conta o número de símbolos diferentes entre duas palavras código.

Definição 2.1.4. Dados dois elementos $\mathbf{u}, \mathbf{v} \in \mathbf{A}^n$, a *distância de Hamming* entre **u** e **v** é definida como

$$d(\mathbf{u}, \mathbf{v}) = |\{i; u_i \neq v_i, 1 \leq i \leq n\}|$$

Exemplo 2.1.2. Considere o alfabeto $\mathbf{A} = \{0, 1\}$. Então,

$$\begin{aligned} \mathbf{A}^4 \;=\; & \{0000, 0001, 0010, 0100, 0110, 0101, 0111, \\ & 0011, 1111, 1110, 1101, 1100, 1000, 1011, 1001, 1010\} \end{aligned}$$

Assim, os subconjuntos $C_1 = \{0000, 0001, 0101\}$, $C_2 = \{0011, 1111, 1000, 1011, 1010\}$ são códigos de comprimento 4 e seus elementos são chamados de palavra-código no alfabeto **A**.

Em $\mathbf{A}^4$, temos por exemplo as seguintes distâncias Hamming.

- $d(0000, 0001) = 1$
- $d(0000, 1111) = 4$
- $d(0101, 1011) = 3$
- $d(0110, 1111) = 2$

As propriedades contidas na função distância caracterizam uma métrica. Por isso, a distância de Hamming entre elementos de $\mathbf{A}^n$ é chamada também *métrica de Hamming*.

Proposição 2.1.1. [4] $(\mathbf{A}^n, d)$ é um espaço métrico, onde d é a métrica de Hamming.

Demonstração. Vamos mostrar as três condições da Definição 2.1.3.

(i) Como $d(u, v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}|$ e $|\{i; u_i \neq v_i, 1 \leq i \leq n\}| \geq 0$, pois é um número natural, temos que $d(u, v) \geq 0$,$\forall u, v \in A^n$. Agora $d(u, v) = 0$ significa que $u_i = v_i$, para todo i com $1 \leq i \leq n$,portanto $u = v$.

(ii) É imediato a verificação que $d(u, v) = d(v, u)$.

(iii) Para mostrarmos que $d(u, v) \leq d(u, w) + d(w, v)$ observemos inicialmente que $d(u, v) = |\{i; u_i \neq v_i\}| = n - |A|$, onde $A = \{i; u_i = v_i\}$. Daí se $B = \{i; u_i = w_i\}$ e $C = \{i; w_i = v_i\}$, temos que: Se $i \in B$ e C, então $i \in A$. Daí $B \cap C \subset A$. logo $A^c \subset (B \cap C)^c = B^c \cup C^c$. Portanto, $d(u, v) = |A^c| \leq |B^c \cup C^c| \leq |B^c| + |C^c| = d(u, w) + d(w, v)$.

■

Definição 2.1.5. Seja $\mathcal{C}$ um código. A *distância mínima* de $\mathcal{C}$ é o número

$$d = min\{d(u, v); u, v \in \mathcal{C}, u \neq v\}.$$

Definição 2.1.6. Dados um elemento $a \in \mathbf{A}^n$ e um número real $t \geq 0$, definimos *bola* de centro em a e raio t como sendo o conjunto

$$B(a, t) = \{u \in \mathbf{A}^n; d(u, a) \leq t\},$$

Lema 2.1.1. [4] Seja $\mathcal{C}$ um código com distância mínima d. Se c e c' são palavras distintas de $\mathcal{C}$, então

$$B(c, \kappa) \cap B(c^{'}, \kappa) = \emptyset.$$

Demonstração. Se $x \in B(c, \kappa) \cap B(c^{'}, \kappa)$, então $d(x, c) \leq \kappa$ e $d(x, c') \leq \kappa$, então pela simetria e pela desigualdade triangular, temos que

$$d \leq d(c, c') \leq d(x, c) + d(x, c') \leq 2\kappa \leq d - 1$$

■

A importância da distância mínima d de um código é que através dela pode-se determinar a capacidade de correção e detecção de erros, como veremos a seguir.

Teorema 2.1.1. [4] Seja $\mathcal{C}$ um código corretor de erros com distância mínima d. Então, $\mathcal{C}$ pode corrigir até $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$ erros e detectar até $d - 1$ erros, onde $\lfloor t \rfloor$ representa o menor inteiro de um número real t.

Demonstração. Suponhamos que ao transmitirmos uma palavra-código $\mathcal{C}$ do código cometemos t erros com $t \leq \kappa$, recebendo a palavra $\mathbf{r}$, então $d(r, c) = t \leq \kappa$; enquanto que , pelo Lema 2.1.1, a distância de $\mathbf{r}$ a qualquer outra palavra do código é maior do que κ. Isso determina $\mathcal{C}$ univocamente a partir de $\mathbf{r}$. Por outro lado, dada uma palavra-código, podemos nela introduzir até $d-1$ erros sem encontrar outra palavra do código, e assim, a detecção do erro será possível. ■

O Teorema 2.1.1 nos mostra que um código terá melhor capacidade de correção de erros quanto maior for a sua distância mínima. Portanto, para a teoria dos códigos é fundamental o cálculo de d ou determinar uma cota inferior para ele.

A seguir é apresentada uma estratégia para efetuar a correção de uma palavra recebida quando for possível, [33]. Seja $\mathcal{C}$ um código com distância mínima d e $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$. Suponhamos que o receptor receba a palavra r. O algoritmo abaixo irá efetuar a correção de erros quando for possível.

(i) Estabeleça as bolas de raio κ em torno das palavras do código e assim, se r pertencer à alguma dessas bolas, basta trocar a palavra r pela palavra do centro da bola.

(ii) Se r não pertencer a nenhuma bola de raio κ em torno de uma palavra $c \in \mathcal{C}$ então não será possível decodificar r com boa margem de segurança.(Em decodificação subótima pode ocorrer isso).

Definição 2.1.7. Sejam $\mathbf{A}$ um alfabeto e n um número natural. Dizemos que uma função $\mathbf{F} : \mathbf{A}^n \longrightarrow \mathbf{A}^n$ é uma *isometria* de $\mathbf{A}^n$ se ela preserva distâncias de Hamming. Em símbolos,

$$d(F(x), F(y)) = d(x, y); \forall x, y \in \mathbf{A}^n.$$

Proposição 2.1.2. [4] Toda isometria de $\mathbf{A}^n$ é uma bijeção de $\mathbf{A}^n$.

Demonstração. Seja $\mathbf{F} : \mathbf{A}^n \longrightarrow \mathbf{A}^n$ uma isometria. Suponha que para $x, y \in \mathbf{A}^n$, tenhamos que $F(x) = F(y)$. Logo, $d(x, y) = d(F(x), F(y)) = 0$, o que implica que $x = y$, portanto F é injetora. Como toda aplicação injetora de um conjunto finito é sobrejetora, concluímos que F é uma bijeção. ■

Definição 2.1.8. Dois códigos C e C' em $\mathbf{A}^n$ são ditos equivalentes se existir uma isometria $\mathbf{F}$ de $\mathbf{A}^n$ tal que $F(C) = C'$.

Alguns códigos possuem propriedades especiais em relação à função distância, como veremos a seguir.

Definição 2.1.9. Um código $\mathcal{C} \subset \mathbf{A}^n$ com distância mínima d é dito *t-perfeito*, $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ se, e somente se, a reunião das bolas disjuntas centradas em palavras-código com raio t cobre todo $\mathbf{A}^n$.

$$\bigcup_{\mathbf{a} \in \mathcal{C}} \mathbf{B}(\mathbf{a}, t) = \mathbf{A}^n$$

Observação 2.1.1. [5] Um código é t-perfeito se, e somente se, para cada elemento ω de $\mathbf{A}^n$ (recebido) existe uma única palavra a do código que dista deste elemento no máximo t. Desta maneira, ω será decodificado como a por verossimilhança e t erros serão corrigidos.

No Capítulo 4, veremos códigos satisfazendo esta propriedade, ou seja, códigos perfeitos, porém obtidos a partir da estrutura de um grafo.

2.2 Códigos de Bloco Lineares

Nesta seção apresentamos uma classe especial de códigos corretores de erros que são os códigos de bloco lineares. Exemplificaremos a sua codificação utilizando uma matriz geradora e sua decodificação por máxima verossimilhança.

Definição 2.2.1. Seja $\mathbb{K}$ um corpo finito com q elementos tomado como alfabeto. Um código $C \subset \mathbb{K}^n$ será chamado *código de bloco linear*, se for um subespaço vetorial de $\mathbb{K}^n$.

Um código de bloco linear $\mathcal{C}$ pode ser caracterizado pelos parâmetros (n, k). Se $v \in \mathcal{C}$, então v é uma palavra-código de $\mathcal{C}$. Para valores de $q = 2$ esse código será binário e para $q = 3$ esse código será ternário. Em geral, a quantidade de palavra-código de um código $\mathcal{C} = (n, k)$ sobre $\mathbb{K}$ é q^k.

Observação 2.2.1. [4] Podemos descrever um código linear $\mathcal{C}$ como imagem ou núcleo de transformações lineares.

(i) Descrevendo $\mathcal{C}$ como imagem de uma transformação linear. Escolha uma base $v_1, v_2, \ldots, v_k$ de $\mathcal{C}$ e considere a aplicação linear

$$\begin{aligned} T : \mathbb{K}^k &\to \mathbb{K}^n \\ x = (x_1, x_2, \ldots, x_k) &\mapsto x_1v_1 + x_2v_2 + \cdots + x_kv_k \end{aligned}$$

Temos que T é uma transformação linear injetora,como

$$\begin{aligned} x_1v_1 + x_2v_2 + \cdots + x_kv_k = y_1v_1 + y_2v_2 + \ldots y_kv_k &\Leftrightarrow \\ (x_1 - y_1)v_1 + (x_2 - y_2)v_2 + \cdots + (x_k - y_k)v_k = 0 &\Leftrightarrow \\ x_1 = y_1, x_2 = y_2, \ldots, x_k = y_k \end{aligned}$$

pois $v_1, v_2, \ldots, v_k$ é uma base de C, portanto linearmente independentes.

A imagem de T é $\mathcal{C}$, em símbolos,

$$Im(T) = \mathcal{C}.$$

Essa é a forma paramétrica do subespaço $\mathcal{C}$, pois os elementos de $\mathcal{C}$ são parametrizados pelos elementos $x \in \mathbb{K}^k$ através de T, o que torna fácil gerar todos os elementos de $\mathcal{C}$, porém é difícil decidir se $v \in \mathbb{K}^n$ pertence ou não a $\mathcal{C}$, para isso, é necessário resolver o sistema de n equações com k incógnitas $x_1, x_2, \ldots, x_k$

$$x_1v_1 + x_2v_2 + \cdots + x_kv_k = v.$$

(ii) Descrevendo $\mathcal{C}$ através do núcleo de uma transformação linear. Considere um subespaço $\mathcal{C}'$ de $\mathbb{K}^n$ complementar de $\mathcal{C}$, isto é, $\mathcal{C} \oplus \mathcal{C}' = \mathbb{K}^n$, e a aplicação linear

$$\begin{aligned} H : \mathcal{C} \oplus \mathcal{C}' &\to \mathbb{K}^{n-k} \\ u \oplus v &\mapsto v \end{aligned}$$

Seja k a dimensão do código $\mathcal{A}$ e seja $v_1, v_2, \ldots, v_k$ uma base qualquer de $\mathcal{C}$. Todo elemento de $\mathcal{C}$ se escreve de modo único na forma

$$\lambda_1v_1 + \lambda_2v_2 + \ldots, \lambda_kv_k,$$

onde os $\lambda_i, i = 1, \ldots, k$, são elementos de $\mathbb{K}$. $dim_K\mathcal{C} = \log_q M$, pois

$$M = |\mathcal{C}| = q^k \Rightarrow k = \log_q q^k = \log_q M.$$

Todo código linear é por definição um espaço vetorial de dimensão finita.

Definição 2.2.2. Seja $\mathbb{K}$ um corpo finito. Dois códigos lineares $\mathbb{C}$ e $\mathcal{C}'$ são *linearmente equivalentes* se existir uma isometria linear $T : \mathbb{K}^n \to \mathbb{K}^n$ tal que $T(\mathcal{C}) = \mathcal{C}'$.

Definição 2.2.3. Dois códigos lineares são linearmente equivalentes se, e somente se, cada um deles pode ser obtido do outro mediante uma sequência de operações do tipo:

(i) Multiplicação dos elementos numa dada posição fixa por um escalar não nulo em todas as palavras.

(ii) Permutação das posições de todas as palavra-código, mediante uma permutação fixa de $\{1, 2, \ldots, n\}$.

Definição 2.2.4. Dado $x \in \mathbb{K}^n$, o número inteiro $\omega(x) = |\{i; x_i \neq 0\}|$ é chamado *peso* de x, ou seja, $\omega(x) = d(x, 0)$, onde d representa a métrica de Hamming.

Definição 2.2.5. O peso de um código linear $\mathcal{C}$ é o inteiro

$$\omega(\mathcal{C}) = \min\{\omega(x); x \in \mathcal{C} \setminus \{0\}\}.$$

No resultado a seguir veremos que, a distância mínima de um código linear $\mathcal{C}$ será igual ao peso mínimo de $\mathcal{C}$.

Proposição 2.2.1. [4] Seja $\mathcal{C} \subset \mathbb{K}^n$ um código linear com distância mínima d. Temos que

(i) $\forall x, y \in \mathbb{K}^n$, $d(x, y) = \omega(x - y)$.

(ii) $d = \omega(\mathcal{C})$.

Demonstração. O item (i) segue das definições da métrica de Hamming e do peso de um código. O item (ii) decorre do fato que, $\forall x, y \in \mathcal{C}$, com $x \neq y$, tem-se $z = x - y \in \mathcal{C} \setminus \{0\}$ e $d(x, y) = \omega(z)$. ■

Observação 2.2.2. Se d é a distância mínima de um código $\mathcal{C}$ então denotamos $\mathcal{C}$ em relação à terna de inteiros (n, k, d), onde k é a dimensão de $\mathcal{C}$ sobre $\mathbb{K}$, e d a distância mínima de $\mathcal{C}$.

Definição 2.2.6. Sejam $\mathbb{K}$ o corpo finito com q elementos , $\mathcal{C} \subset \mathbb{K}^n$ um código linear e $\mathrm{B} = \{v_1, v_2, \ldots v_k\}$ uma base ordenada de $\mathcal{C}$. Considere a matriz $\mathbf{G}$, cujas linhas são os vetores $v_i = (v_{i1}, \ldots, v_{in})$, $i = 1, \ldots, k$, isto é,

$$\mathbf{G} = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \ldots & v_{kn} \end{pmatrix}$$

A matriz $\mathbf{G}$ é chamada *matriz geradora de* C associada à base B.

Observação 2.2.3. Considere transformação linear definida por

$$\begin{array}{rccc} T: & \mathbb{K}^k & \to & \mathbb{K}^n \\ & x & \mapsto & xG \end{array}$$

Se $x = (x_1, \ldots, x_k)$, temos que

$$T(x) = xG = x_1 v_1 + \cdots + x_k v_k,$$

logo $T\left(\mathbb{K}^k\right) = \mathcal{C}$. Podemos considerar $\mathbb{K}^k$ como sendo a representação q-ária das mensagens, $\mathcal{C}$ o código de canal e a transformação T uma codificação. Dessa forma, a matriz geradora de um código de bloco linear se torna um codificador natural para $\mathcal{C}$.

Exemplo 2.2.1. Considere o código, cuja a matriz geradora é dada por:

$$G = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Seja $x = (1101)$ a mensagem na entrada no codificador, então a palavra-código correspondente será:

$$\begin{aligned} u &= x \cdot G \\ u &= \begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \\ u &= \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \end{aligned}$$

Exemplo 2.2.2. Tome $\mathbb{K} = \mathbb{F}_2$ e seja

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Considere a transformação linear

$$\begin{array}{rccc} T: & \mathbb{F}_2^4 & \to & \mathbb{F}_2^7 \\ & x & \mapsto & xG \end{array}.$$

Logo, temos um código linear $\mathcal{C}$ em $\mathbb{F}_2^7$, como a imagem de T.

Dada a palavra recebida 1110000 , gostaríamos de decodificá-la, ou seja, encontrar o vetor x de $\mathbb{F}_2^4$ da qual ela se origina por meio de T. Para isso, temos que resolver o seguinte sistema:

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix} \cdot G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix},$$

isto é,

$$\begin{cases} x_1 + x_2 + x_3 = 1 \\ x_1 + x_4 = 0 \\ x_1 = 0 \\ x_2 + x_4 = 1 \\ x_2 = 1 \\ x_3 + x_4 = 0 \\ x_3 = 0 \end{cases},$$

cuja solução é $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 0$. Portanto, $x = (0100)$.

Definição 2.2.7. Diremos que uma matriz geradora **G** de um código $\mathcal{C}$ está na *forma padrão* se tivermos

$$G = \begin{pmatrix} Id_k & | & P \end{pmatrix},$$

onde Id_k é a matriz identidade $k \times k$ e P, uma matriz $k \times (n-k)$.

Teorema 2.2.1. [4] Dado um código $\mathcal{C}$, existe um código equivalente $\mathcal{C}'$ com uma matriz geradora na forma padrão.

Exemplo 2.2.3. Dada a matriz geradora,

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Aplicando uma sequência de operações sobre a matriz geradora G, do tipo:

- Permutação de duas colunas;
- Multiplicação de uma coluna por um escalar não nulo;
- Adição de um múltiplo escalar de uma coluna a outra.

Obtemos,

$$G' = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right),$$

onde

$$Id_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{e} \quad A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Definição 2.2.8. Seja $\mathcal{C}$ um código (n, k). Se $G = (I_k|P)$ for uma matriz geradora de $\mathcal{C}$ na forma padrão, então $H = (-P_t|I_{n-k})$ é chamada matriz de verificação de paridade de $\mathcal{C}$, em que P_t é a transposta de P de ordem $(n-k) \times k$ e, I_{n-k} a matriz identidade de ordem $n-k$.

A matriz H é utilizada na decodificação e na identificação de uma palavra $\mathbf{v}$ como palavra-código, pois como

$$G \cdot H^t = (I_k|P) \cdot (-P_t|I_{n-k}) = -P + P = 0,$$

se $\mathbf{v} \in \mathcal{C}$, então,

$$\mathbf{v} = \mathbf{u} \cdot G \Rightarrow \mathbf{c} \cdot H_t = \mathbf{u} \cdot (G \cdot H^t) = 0,$$

ou seja, $\mathbf{v}$ é uma palavra-código.

Exemplo 2.2.4. Seja $\mathcal{C}$ um código binário $(6, 3)$ com uma matriz geradora

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Como G se encontra na forma padrão, pela Definição 2.2.8, obtemos:

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Agora, vamos verificar se $\mathbf{v} = (100111)$ é uma palavra-código de $\mathcal{C}$. Para isso, precisamos multiplicá-lo por H^t:

$$\mathbf{v} \cdot H^t = (100111) \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (000).$$

Como a multiplicação resultou em um vetor nulo, a palavra recebida é uma palavra-código, ou seja $\mathbf{v} \in \mathcal{C}$.

Definição 2.2.9. Seja $\mathcal{C}$ um código de bloco linear (n, k) com matriz verificação de paridade H. Suponhamos que uma palavra-código $\mathbf{c} \in \mathcal{C}$ é transmitida por um canal ruidoso e $\mathbf{r}$ seja o vetor recebido. Então, o *vetor erro* é definido por:

$$\mathbf{e} = \mathbf{r} - \mathbf{c}.$$

Exemplo 2.2.5. Em um dado código binário, se transmitirmos $\mathbf{c} = (010011)$ e recebermos $\mathbf{r} = (101011)$, então, o erro introduzido é:

$$\mathbf{e} = (010011) - (101011) = (111000).$$

Ao receber a mensagem $\mathbf{r}$, o decodificador precisa determinar onde ocorreram os erros no vetor, de acordo com seu parâmetro de distância do código, d. Considerando $d \geq 3$, assim como, na codificação quando verificamos se o vetor é uma palavra-código, também multiplicaremos $\mathbf{r}$ por H^t. Essa multiplicação é denominada *síndrome*,

$$\mathbf{s} = \mathbf{r} \cdot H^t.$$

Caso $\mathbf{s} = 0$, então $\mathbf{r}$ é uma palavra-código de $\mathcal{C}$. Caso contrário, $\mathbf{r}$ não é uma palavra-código e é detectada a presença de erros na mensagem. Porém, há a possibilidade de $\mathbf{r}$ ser uma palavra-código diferente de $\mathbf{c}$. Quando isso acontece, o vetor $\mathbf{e}$ é idêntico a essa outra palavra-código não nula de $\mathcal{C}$ e dizemos que ocorreu um padrão de erro não detectável. Existem $2^k - 1$ desses erros.

Observação 2.2.4. Consideraremos que, se $\mathbf{e} \cdot H^t = 0$ e $\mathbf{r} \cdot H^t = 0$, então, $\mathbf{r} \in C$ e $\mathbf{c} = \mathbf{r}$.

Consideremos $\mathcal{C}$, um código de bloco linear com distância mínima $d \geq 3$, capaz de corrigir t erros, tal que $t = \lfloor \frac{d-1}{2} \rfloor$. Seja $\mathbf{e}$, o vetor erro introduzido na palavra-código $\mathbf{c}$ e $\mathbf{r}$, o vetor recebido. Caso $\mathbf{s} = 0$, então, $\mathbf{c} = \mathbf{r}$. Caso contrário, se houve um erro então, $\mathbf{e} = (0, 0, \ldots, a, 0, \ldots, 0)$, para $a \neq 0$ na i-ésima posição. Assim,

$$\mathbf{e} \cdot H^t = a \cdot h_i,$$

onde, h_i é a i-ésima coluna da matriz verificação de paridade, H, do código $\mathcal{C}$. Logo, no processo inverso, fazemos:

$$\mathbf{r} \cdot H^t = a \cdot h_i.$$

Então, consideramos o vetor erro como o vetor com todas as componentes nulas menos na i-ésima posição que teremos a. A seguir será apresentado as etapas para utilizar essa técnica.

Algoritmo para correção de um erro:

1. Calcule $s = \mathbf{r} \cdot H^t$;
2. Se $\mathbf{s} = 0$, então $\mathbf{r} = \mathbf{c}$;
3. Se $\mathbf{s} \neq 0$, compare $\mathbf{s}$ com as colunas de H.
4. Se existirem i e a, tais que $\mathbf{s} = a \cdot h_i$, então $\mathbf{e} = (0, 0, \ldots, a, \ldots, 0)$ com a na i-ésima posição e 0 nas demais;
5. Corrija r fazendo $\mathbf{c} = \mathbf{r} - \mathbf{e}$;
6. Se a etapa 4 não ocorrer, então há mais de um erro e esse algoritmo não poderá ser utilizado.

Exemplo 2.2.6. Seja $\mathcal{C}$ um código com matriz verificação de paridade:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Se $\mathbf{r} = (10100)$ é o vetor recebido, demonstraremos como encontrar a palavra-código utilizando as etapas descritas acima.

- **Etapa 1**: calcular a síndrome:

$$\mathbf{s} = \mathbf{r} \cdot H^t = (10100) \cdot \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} = (010).$$

  Como $s \neq 0$, passaremos para a Etapa 3:

- **Etapa 3**: comparar $\mathbf{s}$ com as colunas de H.

  A síndrome é igual a quarta coluna da matriz H, h_4.

- **Etapa 4**: Temos que,

$$\mathbf{s} = h_4.$$

  Então, $\mathbf{e} = (00010)$.

- **Etapa 5**: corrigir $\mathbf{r}$:

$$\mathbf{c} = \mathbf{r} - \mathbf{e} = (10100) - (00010) = (10110).$$

  Portanto, a palavra-código correta é (10110). Para conferirmos, basta multiplicarmos essa palavra por H^t e verificar se resulta em um vetor nulo:

$$\mathbf{c} \cdot H^t = (10110) \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (000).$$

  Portanto $\mathbf{c}$ é uma palavra-código.

2.3 Constelações de Sinais e Regiões de Voronoi

Em um sistema de transmissão de dados, analógico ou digital, são utilizados formas de inserir as informações em um sinal de rádio frequência. Estas formas de inserção de informação em um sinal são chamadas *modulação*. Na modulação QAM (Quadrature Amplitude Modulation), os símbolos são mapeados em um diagrama de fase e quadratura, sendo que cada símbolo apresenta uma distância específica da origem do diagrama que representa a sua amplitude. Este diagrama é chamado de constelação de sinais do tipo QAM, que em nosso estudo são modeladas por inteiros gaussianos e de Eisenstein-Jacobi.

Nesta seção veremos os conceitos de constelações de sinais e regiões de Voronoi, que são fundamentais para os objetivos do nosso trabalho.

Definição 2.3.1. Uma *constelação de sinais* S é um subconjunto finito de pontos em um espaço métrico $(\mathbb{E}, d)$. Os pontos da constelação são chamados *sinais*.

Definição 2.3.2. [11] Seja $U(S)$ o grupo de simetrias de S em $\mathbb{E}$. Uma constelação de sinais é dita *geometricamente uniforme* se para quaisquer sinais $s_0, s_1 \in S$, existe uma isometria $T \in U(S)$, tal que $T(s_0) = s_1$, ou seja, $U(S)$ age transitivamente em S. Equivalentemente,

$$U(s_0) = \{T(s_0) : T \in U(S)\} = S.$$

Definição 2.3.3. Um código $\mathcal{C} \subset \mathbf{A}^n$ é chamado *geometricamente uniforme* se, e somente se, dadas duas palavras quaisquer $\mathbf{x}$ e $\mathbf{y}$ do código existe uma isometria $\phi : \mathbf{A}^n \longrightarrow \mathbf{A}^n$ tal que:

(i) $\phi(\mathcal{C}) = \mathcal{C}$ (a isometria leva o código no código)

(ii) $\phi(\mathbf{x}) = \mathbf{y}$.

Definição 2.3.4. Sejam S uma constelação de sinais e $s_0 \in S$. A *região de Voronoi de* s_0 consiste dos pontos que estão mais próximos de s_0 que de qualquer outro ponto de S, ou seja,

$$\mathcal{V}_S(s_0) = \{s \in \mathbb{E} : d(s, s_0) \leq d(s, r), \forall r \in S, s \neq s_0\}.$$

Definição 2.3.5. O *perfil de distância global* com relação a s_0, denotado por $PD(s_0)$, é dado pelo conjunto das distâncias dos pontos de S com relação a s, ou seja,

$$PD(s_0) = \{d(s_0, s) : s \in S\}.$$

O próximo Teorema estabelece a relação entre uma constelação de sinais geometricamente uniforme e regiões de Voronoi.

Teorema 2.3.1. [11] Seja S uma constelação de sinais. Se S é uniforme, então:

(i) Todas as regiões de Voronoi são congruentes;

(ii) O perfil de distância global é o mesmo para qualquer sinal $s \in S$.

Definição 2.3.6. Uma constelação de sinais S está casada a um grupo $\mathcal{G}$, se existe uma aplicação sobrejetora $\eta : \mathcal{G} \longrightarrow S$ tal que

$$d(\eta(h_1), \eta(h_2) = d(\eta(e), \eta(h_1^{-1}h_2)), \forall h_1, h_2 \in \mathcal{G},$$

onde e é o elemento neutro de $\mathcal{G}$ e d é uma distância em S. A aplicação η é uma *aplicação casada*. Além disso, se η é injetora, então dizemos que η^{-1} é um *rotulamento casado*. Nesse caso, dizemos que η é um rotulamento isométrico.

Capítulo 3

Grafos

Neste trabalho, o objeto do estudo são grafos gaussianos e de Eisenstein-Jacobi, que podem ser usados na construção de códigos perfeitos onde a distância entre duas palavras-código é a distância do grafo entre dois vértices rotulados do anel com tais palavras código [24].

Neste capítulo, primeiramente será realizado um breve histórico sobre a teoria dos grafos. Em seguida na Seção 3.2, elucida-se algumas definições e terminologias básicas da teoria dos grafos. Na Seção 3.3 os grafos circulantes são definidos, com o objetivo de apresentar os grafos gaussianos e os grafos de Eisenstein-Jacobi, nas Seções 3.4 e 3.5, os quais mostraremos que são grafos circulantes de graus quatro e seis, respectivamente. As principais referências utilizadas neste capitulo foram [11, 25, 26, 29].

3.1 Considerações Históricas

A teoria dos grafos começou a ser desenvolvida no século XVIII quando Euler em 1736 utilizou-a para resolver o problema das "Pontes de Königsberg".

A antiga cidade de Königsberg cortada pelo rio Pregel, território da Prússia até 1945 hoje pertence a Rússia e é chamada Prególia. O rio Pregel rodeia uma ilha (Kneiphof) e, à direita do mapa, separa-se em dois ramos. Para a acessibilidade dos moradores foram construídas sete pontes.

Os habitantes passaram a buscar uma rota ao redor da cidade onde cruzariam apenas uma única vez em cada ponte. Após tentativas frustadas, acreditava-se impossível existir um caminho que cumprisse tais condições. Em 1736, Leonhard Euler(1707-1783) tratou matematicamente o problema e ficou comprovada a impossibilidade de achar tal rota. Em seu artigo, *"Solutio Problematis ad Geometrian Situs Pertinentis"* , ele produziu o que ficou conhecido como primeiro trabalho sobre teoria dos grafos. Ele propôs que as margens e a ilha seriam representadas por vértices e as pontes seriam as arestas.

Outros matemáticos contribuíram para o desenvolvimento dos grafos, entre eles: Arthur Cayley (1821-1895), no artigo *"On the Analytical Forms Called Trees"* apresenta resultados sobre o número de ávores com N vértices. Sir William Rowan Hamilton (1805-1865) desenvolveu jogos utilizando vértices e arestas de um dodecaedro. Dénes König (1884-1944) escreveu o primeiro livro texto sobre teoria dos grafos. Francis Guthrie (1831-1899) e August De Morgan(1806-1871) investigaram o *Teorema das Quatro Cores*.

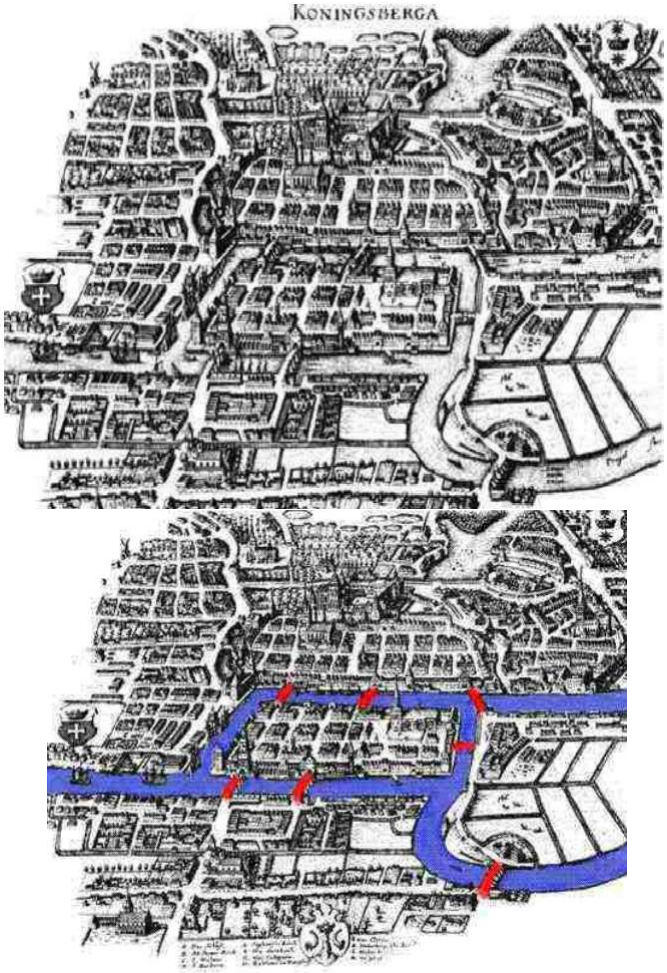

Figura 3.1: Cidade de Königsberg (séc XVIII) e Rio Pregel

3.2 Definições e Terminologia

Um grafo é formado por dois conjuntos: um de vértices e outro de arestas que conectam pares de vértices. A seguir vamos definir grafos e algumas propriedades relevantes ao desenvolvimento e entendimento deste trabalho.

Definição 3.2.1. Um *grafo* $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ é uma estrutura formada por um conjunto enumerável e não vazio $\mathcal{V}$ de elementos chamados *vértices, pontos ou nós*, e um conjunto $\mathcal{A} \subset \mathcal{V} \times \mathcal{V}$ de pares não direcionados de vértices chamados *linhas ou arestas*.

Exemplo 3.2.1. Na Figura 3.3, temos um grafo $\mathcal{G}_1 = (\mathcal{V}, \mathcal{A})$, onde $\mathcal{V} = \{a_1, a_2, a_3, a_4, a_5, a_6\}$ é o conjunto de vértices e

$$\mathcal{A} = \{(a_1, a_3), (a_1, a_2), (a_2, a_3), (a_4, a_1), (a_4, a_2), (a_4, a_5), (a_5, a_6), (a_6, a_1)\}$$

é o conjunto de arestas.

Definição 3.2.2. Quando o conjunto de arestas $\mathcal{A}$ de um grafo $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ for um conjunto de pares direcionados, dizemos que $\mathcal{G}$ é um *digrafo* e chamamos os pares direcionados de *arcos*.

Exemplo 3.2.2. Na Figura 3.4, temos um exemplo de um digrafo $\mathcal{G}_2 = (\mathcal{V}, \mathcal{A})$, onde

$$\begin{aligned} \mathcal{V} &= \{a_1, a_2, a_3, a_4, a_5, a_6\} \text{ e} \\ \mathcal{A} &= \{(a_1, a_3), (a_1, a_2), (a_2, a_3), (a_4, a_1), (a_4, a_2), (a_4, a_5), (a_5, a_6), (a_6, a_1)\}. \end{aligned}$$

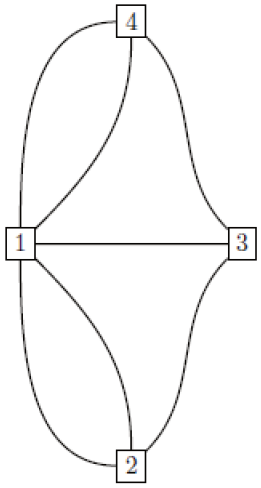

Figura 3.2: Grafo proposto por Euler, em 1736

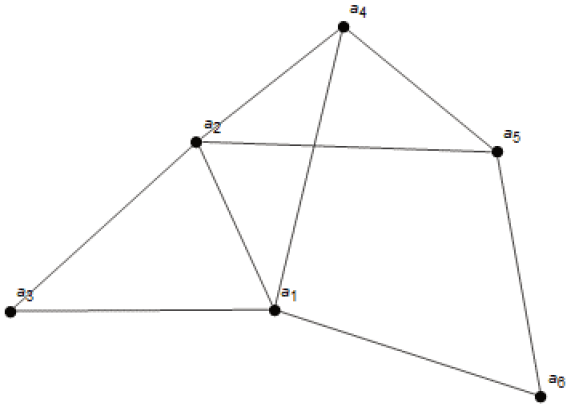

Figura 3.3: $\mathcal{G}_1 = (\mathcal{V}, \mathcal{A})$

Definição 3.2.3. Seja $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ um grafo, onde $\mathcal{V} = \{v_1, \cdots, v_n\}$ é o conjunto de vértices e $\mathcal{A} = \{a = (v_i, v_j) \mid 1 \leq i, j \leq n\}$ é o conjunto de arestas. Temos que:

(i) A quantidade n de vértices do grafo $\mathcal{G}$ é chamada *ordem* do grafo.

(ii) Os vértices v_i e v_j são chamados *adjacentes* ou *conectados*, se existir uma aresta $a \in \mathcal{A}$, tal que $a = (v_i, v_j)$. Neste caso, dizemos que a aresta a é *incidente* aos vértices v_i e v_j.

(iii) O *grau* de um vértice v é o número de arestas incidentes em v. O *grau mínimo* de um grafo é denotado por $\delta(\mathcal{G})$ e o *grau máximo* por $\Delta(\mathcal{G})$, e representam o menor e maior número de arestas incidentes em um vértice do grafo, respectivamente.

(iv) A *distância* $d(v_1, v_2)$ entre dois vértices adjacentes v_1 e v_2 de um grafo é o comprimento entre eles. O *diâmetro* de um grafo é o máximo de todas as distâncias entre quaisquer par de vértices.

Observação 3.2.1. Grafos ou dígrafos são finitos quando $\mathcal{V}$ e $\mathcal{A}$ são finitos. E são infinitos quando pelo menos um dos conjuntos é infinito.

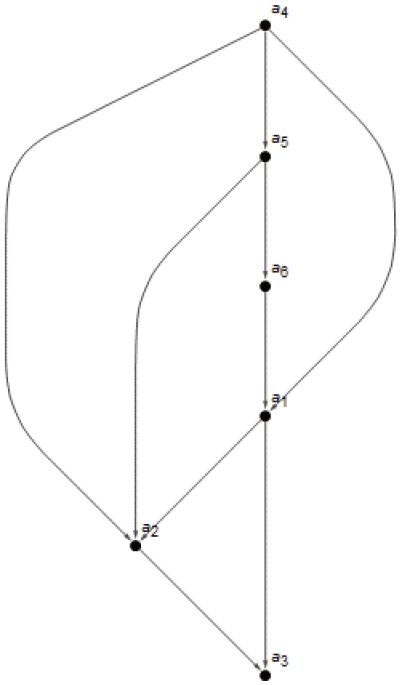

Figura 3.4: $\mathcal{G}_2 = (\mathcal{V}, \mathcal{A})$

Definição 3.2.4. Um grafo $\mathcal{G}$ é chamado *k-regular* quando todos os seus vértices têm o mesmo grau k, ou seja, quando $\delta(\mathcal{G}) = \Delta(\mathcal{G}) = k$.

Exemplo 3.2.3. Na Figura 3.5 temos um exemplo de um grafo 4-regular, pois todos os seus vértices tem grau 4.

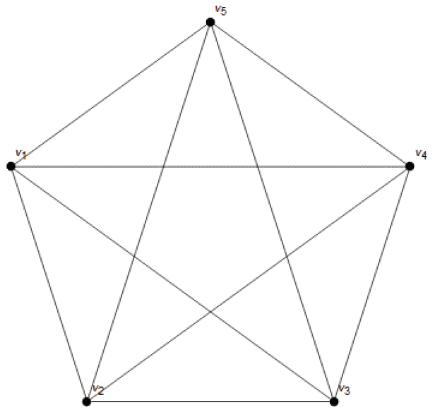

Figura 3.5: Grafo 4-regular

Definição 3.2.5. Dados dois grafos $\mathcal{G}_1 = (\mathcal{V}_1, \mathcal{A}_1)$ e $\mathcal{G}_2 = (\mathcal{V}_2, \mathcal{A}_2)$. Um *isomorfismo* de $\mathcal{G}_1$ em $\mathcal{G}_2$ é uma bijeção $f : \mathcal{V}_1 \longrightarrow \mathcal{V}_2$, tal que $(v_i, v_j) \in \mathcal{A}_1$ se, e somente se, $(f(v_i), f(v_j)) \in \mathcal{A}_2$, para todo $v_i, v_j \in \mathcal{V}_1$.

Definição 3.2.6. Seja $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ um grafo.

(i) Uma sequência de vértices adjacentes é chamada *cadeia*.

(ii) Quando uma cadeia não passa duas vezes pelo mesmo vértice é dita *elementar*, e se não passa duas vezes pela mesma aresta, é chamada *simples*.

(iii) O *comprimento* de uma cadeia é o número de arestas que a compõe.

(iv) Uma cadeia é *fechada*, quando o vértice inicial é o mesmo que o vértice final.

(v) Uma cadeia simples, elementar e fechada, com comprimento maior ou igual a 3 vértices é chamada *ciclo*.

Definição 3.2.7. Um grafo $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ é *conexo* se houver pelo menos uma cadeia ligando cada par de vértices deste grafo. Dizemos que um grafo $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ é *desconexo* se não for conexo.

Exemplo 3.2.4. Na Figura 3.6, temos um grafo conexo $\mathcal{G} = (\mathcal{V}, \mathcal{A})$, com vértices $\mathcal{V} = \{a_1, a_2, a_3, a_4\}$ e arestas $\mathcal{A} = \{(a_1, a_3), (a_1, a_2), (a_2, a_3), (a_2, a_4)\}$.

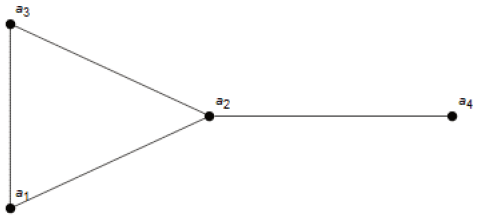

Figura 3.6: Grafo conexo

Exemplo 3.2.5. Na Figura 3.7, temos um grafo desconexo $\mathcal{G} = (\mathcal{V}, \mathcal{A})$, com vértices $\mathcal{V} = \{a_1, a_2, a_3, a_4, a_5\}$ e arestas $\mathcal{A} = \{(a_1, a_3), (a_1, a_2), (a_2, a_3), (a_5, a_4)\}$.

Figura 3.7: Grafo desconexo

Definição 3.2.8. Um grafo $\mathcal{G}_s = (\mathcal{V}_s, \mathcal{A}_s)$ é chamado *subgrafo* de um grafo $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ se $\mathcal{V}_s \subseteq \mathcal{V}$ e $\mathcal{A}_s \subseteq \mathcal{A}$. Neste caso, dizemos também que $\mathcal{G}$ é um *supergrafo* de $\mathcal{G}_s$.

Observação 3.2.2. Se $\mathcal{G}$ for desconexo, então ele é formado por pelo menos dois subgrafos conexos, distintos em relação aos vértices e maximais em relação à inclusão. Observe que o grafo desconexo da Figura 3.7 é formado por dois subgrafos conexos.

Definição 3.2.9. Um subgrafo conexo do grafo $\mathcal{G}$ é chamado *componente conexa* de $\mathcal{G}$.

Definição 3.2.10. Um grafo $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ de n vértices é dito *completo*, e denotado por K_n, se todos os pares de vértices distintos são adjacentes.

Exemplo 3.2.6. Na Figura 3.8 temos um grafo completo K_6.

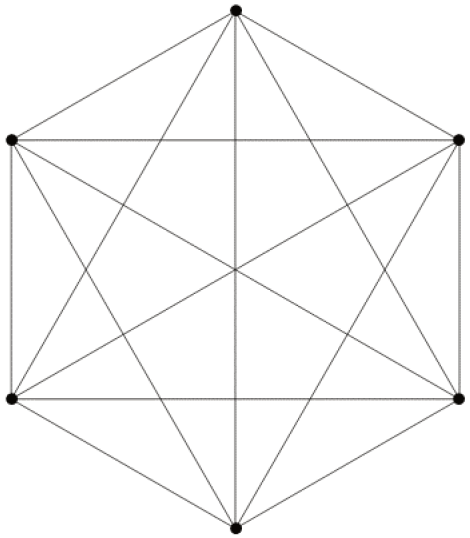

Figura 3.8: Grafo completo K_6

Definição 3.2.11. Dizemos que um grafo é *planar* se a sua representação gráfica puder ser desenhada no plano de maneira que suas arestas não se cruzem.

Exemplo 3.2.7. Na Figura 3.9, temos um grafo planar $\mathcal{G} = (\mathcal{V}, \mathcal{A})$, com vértices $\mathcal{V} = \{a_1, a_2, a_3, a_4\}$ e arestas $\mathcal{A} = \{(a_1, a_3), (a_1, a_2), (a_2, a_1), (a_2, a_3), (a_4, a_3), (a_4, a_2)\}$.

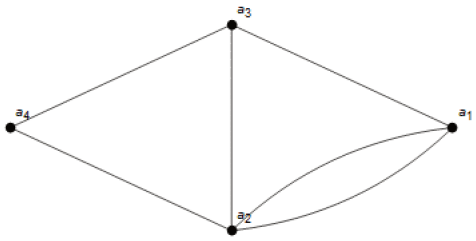

Figura 3.9: Grafo planar

Definição 3.2.12. Sejam $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ um grafo e $\mathbf{D} \subseteq \mathcal{V}$ um conjunto. Dizemos que $\mathbf{D}$ é um *conjunto dominante* se todo vértice de $\mathcal{V}$ ou está em $\mathbf{D}$ ou é adjacente a um de seus vértices. O número de dominação de um grafo $\mathcal{G}$, é a cardinalidade do menor conjunto dominante de $\mathcal{G}$. Seja v um vértice, isto é, $v \in \mathbf{D}$, ele é chamado *vértice dominante*. Um vértice é dito *dominado* quando possui um vizinho dominante.

Exemplo 3.2.8. Na Figura 3.10, o conjunto $D = \{v_2, v_3, v_4\}$ é um conjunto dominante de $\mathcal{G}$.

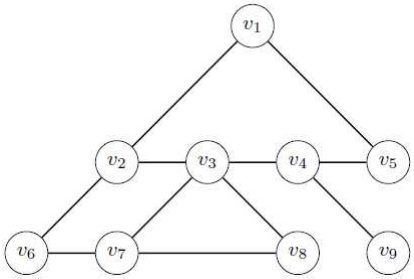

Figura 3.10: Grafo que possui conjunto dominante

3.3 Grafo Circulante

Neste trabalho usaremos uma classe especial de grafos chamados grafos circulantes. Inicialmente iremos definir os grafos de Cayley. Com o objetivo de associar a teoria dos grupos à teoria dos grafos, Arthur Cayley em 1878, introduziu tais grafos. Um grafo de Cayley é formado por um grupo e um conjunto gerador do grupo, onde os vértices estão associados aos elementos do grupo e as arestas estão associadas aos elementos do conjunto gerador.

Definição 3.3.1. Dados $(\mathbf{G}, *)$ um grupo (finito ou infinito) e S um subconjunto finito e não vazio de $\mathcal{G}$, o grafo de Cayley, denotado por $\text{Cay} = (\mathbf{G}, S)$ é um grafo com o conjunto de vértices $\mathcal{V} = \mathbf{G}$ e o conjunto de arestas

$$\mathcal{A} = \{(x, y) \mid x * y \in \mathbf{G} \text{ e existe } s \in S \text{ com } y = x * s\},$$

onde $*$ denota a operação do grupo.

Exemplo 3.3.1. O grafo completo K_n é um grafo de Cayley no grupo aditivo $\mathbb{Z}_n$ dos inteiros módulo n com conjunto gerador formado por todos os elementos diferentes de zero de $\mathbb{Z}_n$.

Exemplo 3.3.2. O grafo completo K_5 é um grafo de Cayley no grupo aditivo $\mathbb{Z}_5$, onde $\mathbb{Z}_5 = \mathbf{G} = \{0, 1, 2, 3, 4\}$ e $S = \{1, 2, 3, 4\}$ o conjunto gerador.

Observação 3.3.1. O grafo de Cayley $\text{Cay} = (\mathbf{G}, S)$ é conexo se, e somente se, S gera $\mathbf{G}$.

Veremos a seguir que um grafo circulante é um grafo de Cayley formado pelo par $(\mathbb{Z}_n, \mathbf{C})$, $\mathbf{C} \subseteq \mathbb{Z}_n$ é um conjunto gerador arbitrário, ou seja, são grafos de Cayley definidos sobre grupos cíclicos.

Definição 3.3.2. Um grafo *circulante* com n vértices e saltos $\{a_1, \ldots, a_k\}$, denotado por $\mathbf{C}_n(a_1, \ldots, a_k)$, é um grafo não direcionado onde cada vértice v é adjacente a todos os vértices $v \pm a_i \mod n$, com $1 \leq i \leq k$ e $k < n/2$.

Observação 3.3.2. Se $a_k \neq n/2$, então o grafo circulante $\mathbf{C}_n(a_1, \ldots, a_k)$ é um grafo regular de grau $2k$, isto é, $\delta(\mathbf{C_n(a_1, \ldots, a_k)}) = \Delta(\mathbf{C_n(a_1, \ldots, a_k)} = 2k$. Neste caso, dizemos que $\mathbf{C}_n(a_1, \ldots, a_k)$ é um grafo circulante de grau $2k$. Entretanto, se $a_k = n/2$, então o grafo circulante $\mathbf{C}_n(a_1, \ldots, a_k)$ é de grau $2k - 1$.

Exemplo 3.3.3. Na Figura 3.11 apresentamos o grafo circulante $\mathbf{C}_{10}(2, 4, 7)$, que é um grafo regular de grau $2k = 6$, pois $a_k = 7 \neq 5 = \frac{n}{2}$ e, na Figura 3.12 temos o grafo circulante $\mathbf{C}_{10}(1, 3, 5)$, que é um grafo regular de grau $2k - 1 = 5$, pois $a_k = 5 = \frac{10}{2}$.

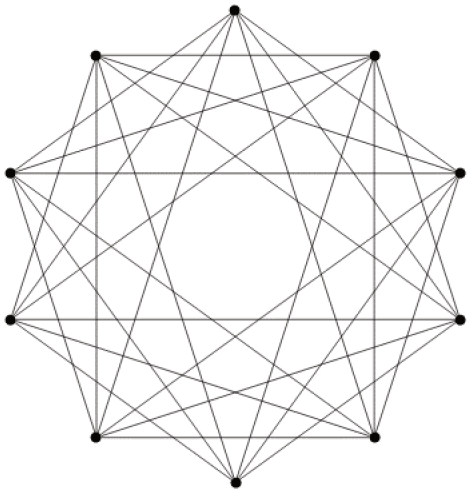

Figura 3.11: $\mathbf{C}_{10}(2, 4, 7)$

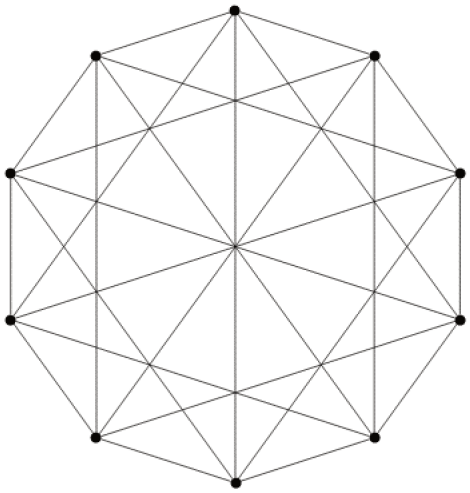

Figura 3.12: $\mathbf{C}_{10}(1, 3, 5)$

Observação 3.3.3. Seja v_j um vértice de um grafo circulante $\mathcal{G}$. Como grafos circulantes são grafos de Cayley rotulado pelo grupo $\mathbb{Z}_n$, então $v_j \in \mathbb{Z}_n$.

Teorema 3.3.1. [26] Se $\mathcal{G} = \mathbf{C}_n(a_1, a_2, \ldots, a_k)$ é um grafo circulante com $\text{mdc}(a_1, a_2, \ldots, a_k) = d$, então $\mathcal{G}$ é um grafo com d componentes conexas em que cada componente contém apenas um vértice de rótulo r , com $0 \leq r < d$.

Demonstração. Dados dois vértices v_i e v_j de um grafo circulante $\mathcal{G}$, existe uma cadeia conectando estes vértices se, e somente se, existe uma sequência de vértices $v_i = v_{i0}, \ldots, v_{il} = v_j$, com v_r vizinho de v_{r+1}, para todo $r = i_0, \ldots, i_{l-1}$. Mas v_r é vizinho de v_{r+1} se, e somente se, $v_{r+1} = v_r + a_s$, para algum $s \in \{\pm a_1, \ldots, \pm a_k\}$. Logo, v_i e v_j estão na mesma componente conexa se, e somente se, $v_j = v_i + \sum_s p_s a_s$, onde $p_s \in \mathbb{Z}$. Então, $v_j - v_i = \sum_k p_s a_s \mod n$, o que equivale a $v_j - v_i = \sum_k p_s a_s + ln$. Esta equação é linear dentro do anel dos inteiros e terá solução se, e somente se, d dividir $v_i - v_j$. Portanto, concluí-se que existem d componentes conexas, onde $\mathcal{C}(r)$ é a componente que contém o vértice r , $0 \leq r < d$.

■

Observação 3.3.4. [26] A componente $\mathcal{C}(r)$, que é um subgrafo de $\mathcal{G}$, pode ser vista como o grafo circulante $\mathcal{C}_{n/d}(a_1/d, \ldots, a_k/d)$ através do isomorfismo de grafos dado por:

$$\begin{array}{rcl} \phi : \mathcal{C}(r) & \longrightarrow & \mathcal{C}_{n/d}(a_1/d, \ldots, a_k/d) \\ x & \longmapsto & (x-r)/d. \end{array}$$

Se x e $y \in \mathcal{C}(r)$ são vizinhos, então $x - y = \pm a_s$, para algum s. Logo, dividindo ambos os lados por d temos que

$$\frac{x-y}{d} = \pm\frac{a_s}{d} \implies \frac{(x-y)-(y-r)}{d} = \pm\frac{a_s}{d}.$$

Portanto, $\dfrac{x-r}{d}$ é vizinho de $\dfrac{y-r}{d}$.

Corolário 3.3.1. [26] Um grafo circulante $\mathbf{C}_n(a_1, \ldots, a_k)$ é conexo se, e somente se, $\text{mdc}(n, a_1, \ldots, a_k) = 1$.

Como vimos na Observação 3.3.2, um grafo circulante tem grau $2k$ ou $2k-1$. Neste trabalho estamos interessados em duas famílias especiais de grafos circulantes de grau 4 e 6 da seguinte forma:

(i) Grau 4: $\mathbf{C}_n(a_1, a_2)$, onde $n = a_1^2 + a_2^2$.

(ii) Grau 6: $\mathbf{C}_n(a_1, a_2, a_2 - a_1)$, onde $n = a_1^2 + a_2^2 - a_1.a_2$.

A seguir apresentamos exemplos de representantes de tais famílias.

Exemplo 3.3.4. Na Figura 3.13, temos um grafo circulante de grau 4, $\mathbf{C}_{13}(2, 3)$, onde $13 = 2^2 + 3^2$.

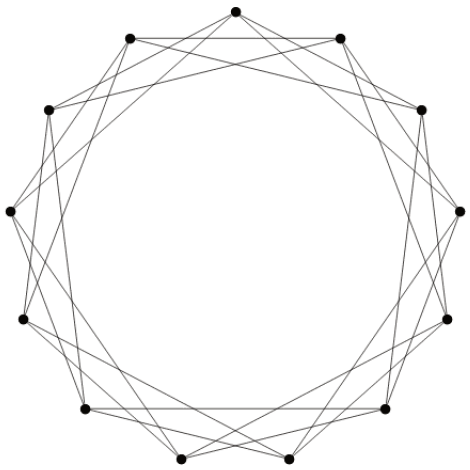

Figura 3.13: $\mathbf{C}_{13}(2, 3)$

Exemplo 3.3.5. Na Figura 3.14, temos um grafo circulante $\mathbf{C}_{13}(3, 4, 1)$, de grau 6, tal que $13 = 3^2 + 4^4 - 3 \cdot 4$.

Definição 3.3.3. Um grafo circulante de grau 4, contendo um número máximo de nós $\mathbf{C}_{k^2+(k+1)^2}(k, k+1)$, onde k é o diâmetro do grafo, é chamado *grafo denso circulante de grau quatro.*

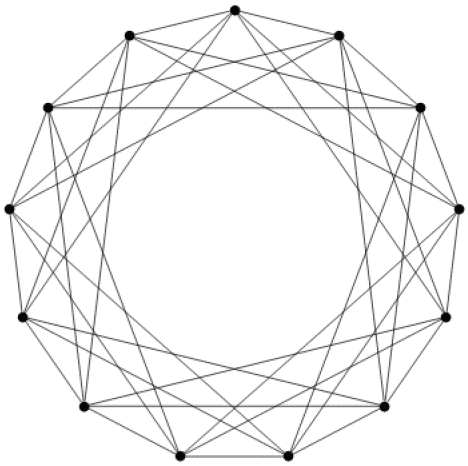

Figura 3.14: $\mathbf{C}_{13}(3, 4, 1)$

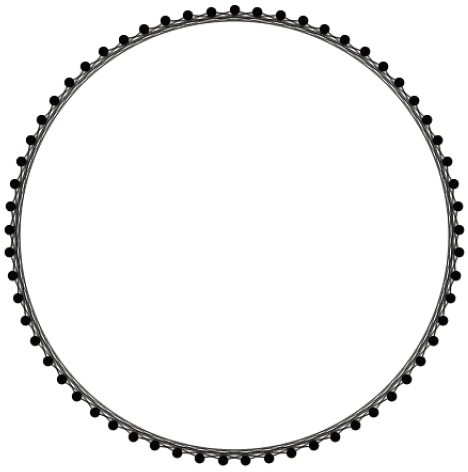

Figura 3.15: $\mathbf{C}_{61}(5, 6)$

Exemplo 3.3.6. Na Figura 3.15, temos o grafo denso circulante $\mathbf{C}_{61}(5, 6)$, de grau 4.

Se nas famílias de graus 4 e 6 apresentadas acima, ao invés de relacionarmos os vértices dos grafos com elementos de um grupo, relacionarmos com os elementos do anel quociente de inteiros gaussianos e de Eisenstein-Jacobi, respectivamente, podemos definir duas famílias de grafos circulantes: grafos de grau quatro com vértices rotulados por inteiros gaussianos, denotado por grafos gaussianos e grafos de grau seis com vértices rotulados por inteiros de Eisenstein-Jacobi, denotado por grafos Eisenstein-Jacobi. Nas Seções 3.4 e 3.5, apresentamos tais famílias detalhadamente com o objetivo de obter códigos perfeitos sobre tais grafos no Capítulo 4.

3.4 Grafo Gaussiano

Grafos gaussianos são circulantes de grau quatro. Eles são uma família especial de grafos de Cayley definidos sobre anéis quocientes de inteiros gaussianos utilizando as unidades do anel como conjunto de geradores. Para o anel dos inteiros gaussianos a constelação de sinais associada possui região de Voronoi formada por quadrados.

Na Definição 1.2.15 apresentamos os inteiros gaussianos e o anel dos inteiros gaussianos que é dado por

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \text{ , onde } i = \sqrt{-1}.$$

Se $\alpha = a + bi \in \mathbb{Z}[i]$ sua norma será

$$\begin{array}{rcl} \mathcal{N} : \mathbb{Z}[i] & \longrightarrow & \mathbb{Z}^+ \\ a + bi & \longmapsto & a^2 + b^2 \end{array}$$

Como vimos na Observação 1.2.1, a função valor absoluto em $\mathcal{N}$ é multiplicativa. Assim,

$$\mathcal{N}(wz) = \mathcal{N}(w)\mathcal{N}(z) \text{ , } \forall w, z \in \mathbb{Z}[i].$$

A seguir, veremos alguns resultados importantes sobre os elementos invertíveis e os ideais em $\mathbb{Z}[i]$.

Proposição 3.4.1. [3] Sejam $\mathbb{Z}[i]$ o anel dos inteiros gaussianos e $\alpha \in \mathbb{Z}[i]$. As seguintes afirmações são equivalentes:

(i) α é invertível em $\mathbb{Z}[i]$.

(ii) $\mathcal{N}(\alpha) = 1$.

(iii) $\alpha \in \{-1, 1, -i, i\}$.

Teorema 3.4.1. [3] $\mathbb{Z}[i]$ é um domínio principal.

Demonstração. Seja $\mathbf{I}$ um ideal de $\mathbb{Z}[i]$. Se $\mathbf{I} = 0$, nada temos a provar. Suponha que $\mathbf{I} \neq 0$. Considere o conjunto

$$\Lambda = \{\mathcal{N}(z) | z \in \mathbf{I} \setminus \{0\}\} \subset \mathbb{N}.$$

Como Λ é um conjunto não vazio de $\mathbb{N}$, então Λ possui um menor elemento $n \in \mathbb{N}$. Seja $\alpha \in \mathbf{I} \setminus \{0\}$ tal que $\mathcal{N}(\alpha) = n$. Vamos provar que $\mathbf{I} = \langle\alpha\rangle$. De fato, dado que $\alpha \in \mathbf{I}$, segue que $\langle\alpha\rangle \subset \mathbf{I}$. Por outro lado, se $z \in \mathbf{I}$, então existem $\gamma, \rho \in \mathbb{Z}[i]$ tais que $z = \alpha \cdot \gamma + \rho$, com $\mathcal{N}(\rho) < \mathcal{N}(\alpha)$. Suponha por absurdo que $\rho \neq 0$, logo

$$\rho = z - \alpha \cdot \gamma \in \mathbf{I},$$

com $0 < \mathcal{N}(\rho) < \mathcal{N}(\alpha) = n$, o que é uma contradição pela escolha de α. Isto implica que $z = \alpha \cdot \gamma \in \langle\alpha\rangle$, e consequentemente $\mathbf{I} \subset \langle\alpha\rangle$. Portanto, $\mathbf{I} = \langle\alpha\rangle$. ■

Definição 3.4.1. Se $\langle\alpha\rangle$ denota o ideal de $\mathbb{Z}[i]$ gerado por α, então o anel quociente $\dfrac{\mathbb{Z}[i]}{\langle\alpha\rangle}$, denotado por $\mathbb{Z}[i]_\alpha$, é chamado *anel quociente dos inteiros gaussianos.*

Teorema 3.4.2. [29] Seja $0 \neq \alpha \in \mathbb{Z}[i]$. Então, $\mathbb{Z}[i]_\alpha$ tem $\mathcal{N}(\alpha)$ elementos.

Demonstração. Seja $\alpha \neq 0$ um inteiro gaussiano e $n = \mathcal{N}(\alpha)$. Então $\mathbb{Z}[i]_n$ tem n^2 elementos. Note que se $\beta = b_1 + b_2 i$ e $\beta' = b_1' + b_2' i$ são congruentes módulo n, então existe $\beta'' = b_1'' + b_2'' i$ tal que $\beta - \beta' = \beta'' n$ e $b_1 - b_1' = b_1'' n$ e $b_2 - b_2' = b_2'' n$. Assim sendo, $b_1 \equiv b_1' \mod n$ e $b_2 \equiv b_2' \mod n$, o que implica que temos n^2 possibilidades para coeficientes de β.

Agora, temos que $\langle \mathcal{N}(\alpha)\rangle = \langle \bar{\alpha}\alpha\rangle \subseteq \langle \alpha\rangle$. Temos pelo terceiro Teorema do Isomorfismo (1.1.4), que

$$\frac{\frac{\mathbb{Z}[i]}{\langle \bar{\alpha}\alpha\rangle}}{\frac{\langle \alpha\rangle}{\langle \bar{\alpha}\alpha\rangle}} \approxeq \frac{\mathbb{Z}[i]}{\langle \alpha\rangle}$$

Então aplicando a consequência do Teorema de Lagrange para índices de grupos abelianos, [2], temos que a cardinalidade de $\frac{\mathbb{Z}[i]}{\langle \bar{\alpha}\alpha\rangle}$ é nm, onde a cardinalidade de $\frac{\langle \alpha\rangle}{\langle \bar{\alpha}\alpha\rangle}$ é denotado por n e o de $\frac{\mathbb{Z}[i]}{\langle \alpha\rangle}$ é denotado por m. Finalmente, temos que a função

$$f : \frac{\mathbb{Z}[i]}{\langle \bar{\alpha}\rangle} \longrightarrow \frac{\langle \alpha\rangle}{\langle \bar{\alpha}\alpha\rangle}$$

definida por $f(\beta + \langle \bar{\alpha}\rangle) = \beta\alpha + \langle \bar{\alpha}\alpha\rangle$, é um isomorfismo e, $\frac{\mathbb{Z}[i]}{\langle \bar{\alpha}\rangle}$ tem o mesmo número de elementos de $\frac{\mathbb{Z}[i]}{\langle \alpha\rangle}$, o que conclui a demonstração.

■

Exemplo 3.4.1. Dado $\alpha = 2 + 3i \in \mathbb{Z}[i]$, temos que $\mathcal{N}(\alpha) = 2^2 + 3^3 = 13$. Assim, pelo Teorema 3.4.2, $\mathbb{Z}[i]_{2+3i}$ tem 13 elementos. Tais elementos são obtidos pelo quociente do anel $\mathbb{Z}[i]$ com o ideal $\langle 2 + 3i\rangle$, isto é, tomamos os elementos de $\mathbb{Z}[i]$ e fazemos módulo $(2 + 3i)$. Dessa forma,

$$\mathbb{Z}[i]_{2+3i} = \{0, 1, 2, -1, -2, i, 2i, -i, -2i.1 + i, 1 - i, -1 - i, -1 + i\}.$$

A representação geométrica dos elementos de $\mathbb{Z}[i]_{2+3i}$ é dada na Figura 3.16.

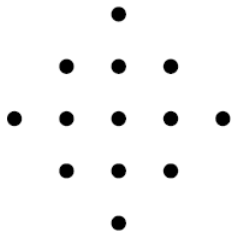

Figura 3.16: Constelação $\mathbb{Z}[i]_{2+3i}$

Exemplo 3.4.2. Dado $\alpha = 3 + 4i \in \mathbb{Z}[i]$, temos que $\mathcal{N}(\alpha) = 3^2 + 4^2 = 25$. Assim, pelo Teorema 3.4.2, $\mathbb{Z}[i]_{3+4i}$ tem 25 elementos, obtidos pelo quociente do anel $\mathbb{Z}[i]$ com o ideal $\langle 3 + 4i\rangle$. Dessa forma,

$$\begin{aligned}\mathbb{Z}[i]_{3+4i} \;=\; & \{0, 1, 2, 3, -1, -2, -3, i, 2i, 3i, -i, -2i, -3i, 1 + i, 1 + 2i, 1 - i, 1 - 2i, -1 - 2i,\\ & -1 + i, -1 + 2i, 2 + i, -2 + i, 2 - i, -2 - i\}.\end{aligned}$$

A representação geométrica dos elementos de $\mathbb{Z}[i]_{3+4i}$ é mostrada na Figura 3.17.

Teorema 3.4.3. [29] Sejam $\alpha = a + bi \in \mathbb{Z}[i]$ e $n = \mathcal{N}(\alpha) = a^2 + b^2$. Então $\mathbb{Z}_n$ e $\mathbb{Z}[i]_\alpha$ são anéis isomorfos se, e somente se, $\text{mdc}(a, b) = 1$.

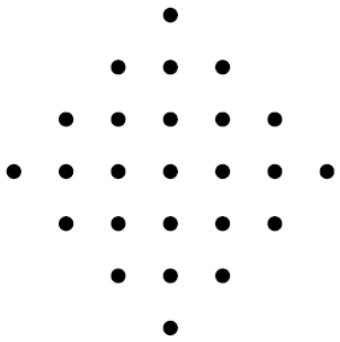

Figura 3.17: Constelação $\mathbb{Z}[i]_{3+4i}$

Demonstração. Primeiro vamos mostrar a implicação direta. Se $\mathbb{Z}_n$ e $\mathbb{Z}[i]_\alpha$ são isomorfos, vamos denotar esse isomorfismo de anéis por $f : \mathbb{Z}[i]_\alpha \longrightarrow \mathbb{Z}_n$. Suponhamos que $\text{mdc}(a, b) = d \neq 1$, o que implicaria no absurdo de $\mathbb{Z}[i]_\alpha$ e $\mathbb{Z}_n$ não serem isomorfos. Como $d = \text{mdc}(a, b)$ divide a e b, temos que $\dfrac{\mathcal{N}(\alpha)}{d}$ é um inteiro. Portanto, $1 < d$ implica que $0 < \dfrac{\mathcal{N}(\alpha)}{d} < n$. Logo,

$$f\left(\frac{\mathcal{N}(\alpha)}{d}\right) = \frac{\mathcal{N}(\alpha)}{d} f(1) = \frac{\mathcal{N}(\alpha)}{d} \neq 0 \mod n.$$

Por outro lado, $\dfrac{\mathcal{N}(\alpha)}{d} = \alpha\dfrac{\bar{\alpha}}{d} = 0 \mod \alpha$, o que é uma contradição uma vez que obtemos $f(0) \neq 0$. Para mostrar a outra implicação, considere a seguinte função:

$$\begin{array}{rcl} \mu : \mathbb{Z}_n & \longrightarrow & \mathbb{Z}[i]_\alpha \\ g & \longrightarrow & g' \mod \alpha \end{array}$$

Inicialmente, observe que μ é bem definida, ou seja, se g , $g' \in \mathbb{Z}_n$ tal que $g \equiv g' \mod n$, então existe $z \in \mathbb{Z}$ tal que $g - g' = zn = z\alpha\bar{\alpha}$. Logo, $g \equiv g' \mod \alpha$. Além disso, μ é injetiva, pois se $\mu(g) \equiv 0 \mod \alpha$, então $g \equiv 0 \mod n$. Seja, $\mu(g) = g = \beta\alpha$, com $\beta = x + yi \in \mathbb{Z}[i]$. Logo, $g = (x + yi)(a + bi) = (xa - yb) + (xb + ya)i$, ou seja,

$$\left\{ \begin{array}{rcl} xa - yb & = & g \\ xb + ya & = & 0 \end{array} \right\}.$$

Resolvendo a segunda equação segue que $(x, y) = (-at, bt)$, onde $t \in \mathbb{Z}$. Substituindo na primeira equação obtemos $g = -ata - btb = (-t)(a^2 + b^2) = -tn$, assim $g \equiv 0 \mod n$. Para finalizar, resta mostrar que a função é sobrejetora. Vamos considerar $\gamma = x + yi$ e um par de inteiros (x_0, y_0) tal que $x_0 b + y_0 a = -y$. Então,

$$x + yi + (x_0 + y_0 i)(a + bi) = (x + x_0 a - y_0 b) + (y + x_0 b + y_0 a)i = x + x_0 a - y_0 b = g$$

é um inteiro tal que $g \equiv \gamma \mod \alpha$.

■

Corolário 3.4.1. [29] Seja $0 \neq \alpha \in \mathbb{Z}[i]$.

(i) Se $\beta \in \mathbb{Z}[i]$ tal que β divide α, então o ideal gerado por β, $\langle\beta\rangle \subseteq \mathbb{Z}[i]_\alpha$ tem $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)}$ elementos.

(ii) Se $\beta \in \mathbb{Z}[i]$ tal que β não divide α e $\eta = \text{mdc}(\beta, \alpha)$, então o ideal $\langle\beta\rangle \subseteq \mathbb{Z}[i]_\alpha$ é gerado por η e tem $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\eta)}$ elementos.

Demonstração. O primeiro item é consequência imediata do Teorema 3.4.2 e do Teorema 1.1.5. Se β divide α, temos que $\langle\alpha\rangle \subseteq \langle\beta\rangle$. Então, $\dfrac{\langle\beta\rangle}{\langle\alpha\rangle}$, é um ideal de $\dfrac{\mathbb{Z}[i]}{\langle\alpha\rangle}$. Assim,

$$\frac{\frac{\mathbb{Z}[i]}{\langle\alpha\rangle}}{\frac{\langle\beta\rangle}{\langle\alpha\rangle}} \cong \frac{\mathbb{Z}[i]}{\langle\beta\rangle},$$

onde verificamos que $\dfrac{\langle\beta\rangle}{\langle\alpha\rangle}$ tem ordem $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)}$. Para o segundo item, vamos considerar que $\gamma = \text{mdc}(\alpha, \beta)$. Então, existe $\gamma_1, \gamma_2 \in \mathbb{Z}[i]$ tal que $\gamma = \gamma_1\beta + \gamma_2\alpha$. Isso implica que $\gamma \equiv \gamma_1\beta \mod \alpha$, assim $\langle\gamma\rangle \subseteq \langle\beta\rangle$. Por outro lado, desde que γ divide β então $\langle\beta\rangle \subseteq \langle\gamma\rangle$. Finalmente, temos que aplicar o primeiro item deste corolário para $\langle\gamma\rangle$ desde que γ divide α. ■

Para relacionar grafos com os inteiros gaussianos, em [29] uma métrica D_α sobre um subconjunto de inteiros gaussianos é definida. A seguir, apresentamos tal métrica com o objetivo de definir o que chamaremos de grafos gaussianos.

Definição 3.4.2. Para β , $\gamma \in \mathbb{Z}[i]_\alpha$, considere $x + yi$ uma classe de $\beta - \gamma$ com $|x|+|y|$ mínimo. A distância D_α entre β e γ é

$$D_\alpha(\beta, \gamma) = \min\{|x|+|y| \text{ , tal que } (\beta - \gamma) \equiv x + yi \mod \alpha\}. \tag{3.4.1}$$

Teorema 3.4.4. [24] D_α define uma distância sobre o anel quociente $\mathbb{Z}[i]_\alpha$.

Demonstração. Sejam β, γ e η elementos de $\mathbb{Z}[i]_\alpha$. Vamos mostrar que

$$D_\alpha(\beta, \eta) \leq D_\alpha(\beta, \gamma) + D_\alpha(\gamma, \eta).$$

Suponha que:

(i) $D_\alpha(\beta, \eta) = |x|+|y|$ onde $\beta - \eta \equiv x + yi \mod \alpha$ e $|x|+|y|$ é mínimo.

(ii) $D_\alpha(\beta, \gamma) = |x'|+|y'|$ onde $\beta - \gamma \equiv x' + y'i \mod \alpha$ e $|x'|+|y'|$ é mínimo.

(iii) $D_\alpha(\gamma, \eta) = |x''|+|y''|$ onde $\gamma - \eta \equiv x'' + y''i(\mod \alpha)$ e $|x''|+|y''|$ é mínimo.

Consequentemente, temos que $\beta - \eta \equiv (x' + x'') + (y' + y'')i \mod \alpha$. Portanto

$$\begin{aligned} D_\alpha(\beta, \eta) &\leq |x' + x''|+|y' + y''| \\ &\leq |x'|+|y'|+|x''|+|y''| \\ &= D_\alpha(\beta, \gamma) + D_\alpha(\gamma, \eta). \end{aligned}$$

■

Exemplo 3.4.3. Considere o anel quociente $\mathbb{Z}[i]_{3+4i}$.

(i) Para $\gamma = 1 + 2i, \beta = -1 \in \mathbb{Z}[i]_{3+4i}$, temos que $\gamma - \beta = 2 + 2i$. Logo, $D_\alpha(\gamma, \beta) = 4$.

(ii) Para $\beta = 1 + 2i$ e $\gamma = -3i$, temos que $\gamma - \beta = 1 + 5i \equiv -2 + i \mod \alpha$. Logo $D_\alpha(\beta, \gamma) = 2 + 1 = 3$.

Agora, a partir da Definição 3.4.2, que estabelece a distância entre elementos do anel quociente de inteiros gaussianos, apresentamos a relação de tais elementos com o conceito de grafos, o que chamaremos de grafos gaussianos.

Definição 3.4.3. Dado $\alpha = a + bi \in \mathbb{Z}[i]$ com $\text{mdc}(a, b) = 1$, definimos o *grafo gaussiano* gerado por α por $\mathcal{G}_\alpha = (\mathcal{V}, \mathcal{A})$, onde:

(i) $\mathcal{V} = \mathbb{Z}[i]_\alpha$ é o conjunto de vértices, e

(ii) $\mathcal{A} = \{(\beta, \gamma) \in \mathcal{V} \times \mathcal{V} \mid D_\alpha(\beta, \gamma) = 1\}$ é o conjunto de arestas.

Observação 3.4.1. Se $\beta, \gamma \in \mathbb{Z}[i]_\alpha$, então $D_\alpha(\beta, \gamma) = 1$, é equivalente a $\gamma - \beta \equiv \pm 1, \pm i \mod \alpha$.

Observação 3.4.2. De acordo com o Teorema 3.4.2, o grafo gaussiano gerado por $\alpha \in \mathbb{Z}[i]$ tem ordem $\mathcal{N}(\alpha)$.

O resultado a seguir mostra que grafos gaussianos são de fato grafos circulantes de grau 4, ou seja, cada vértice é adjacente a outros quatros diferentes vértices.

Teorema 3.4.5. [24] Seja $\alpha = a + bi \in \mathbb{Z}[i]$ tal que $\text{mdc}(a, b) = 1$. Então, $\mathbf{C}_n(a, b)$, onde $n = a^2 + b^2$, e $\mathcal{G}_\alpha$ são grafos isomorfos. O isomorfismo de grafos é

$$\begin{array}{rcl} \Theta : \mathbb{Z}_{\mathcal{N}(\alpha)} & \longrightarrow & \mathbb{Z}[i]_\alpha \\ j & \longmapsto & x + yi \mod \alpha, \end{array}$$

onde $j \equiv ax + by \mod \mathcal{N}(\alpha)$.

Demonstração. Seja $n = \mathcal{N}(\alpha) = a^2 + b^2$, a ordem do grafo circulante e do grafo gaussiano. Inicialmente, pelo Corolário 3.3.1, o grafo circulante $\mathbf{C}_n(a, b)$ é conexo se, e somente se $\text{mdc}(a, b, n) = 1$, o que é equivalente para $\text{mdc}(a, b) = 1$. Ou seja, neste caso, e somente neste caso, para algum vértice $j \in \mathbb{Z}_n$, existem inteiros $x, y \in \mathbb{Z}$ tal que $j \equiv ax + by \mod \mathcal{N}(\alpha)$. Assim, se $j \in \mathbb{Z}$ tal que $j \equiv ax + by \mod n$ e $h \equiv j \mod n$, então a função pode ser descrita por $\Theta(j) \equiv \Theta(h) \mod \alpha$. Provaremos que Θ é uma bijeção que preserva a adjacência.

(i) Para mostrar que Θ é injetiva, devemos provar que $\Theta(j) \equiv \Theta(h) \mod \alpha$, com $j, h \in \mathbb{Z}_n$, implica que $j \equiv h \mod n$. Sejam $\Theta(j) = x + yi$ e $\Theta(h) = x' + y'i$. Então $(x - x') + (y - y')i = \beta\alpha$, com $\beta \in \mathbb{Z}[i]$. Como $\beta = \beta_1 + \beta_2 i$, segue que

$$(x - x') + (y - y')i = \beta\alpha = (\beta_1 a - \beta_2 b) + (\beta_1 b + \beta_2 a)i.$$

Assim,

$$\begin{array}{rcl} x - x' & = & \beta_1 a - \beta_2 b \Longrightarrow a(x - x') = \beta_1 a^2 - \beta_2 ab \\ y - y' & = & \beta_1 b - \beta_2 a \Longrightarrow b(y - y') = \beta_1 b^2 + \beta_2 ab \end{array}$$

Logo, $a(x - x') + b(y - y') = \beta_1(a^2 + b^2)$, com $\beta_1 \in \mathbb{Z}$, de onde segue que $j \equiv h \mod n$.

(ii) Para mostrar que Θ é sobrejetora, considere $x + yi \in \mathbb{Z}[i]_\alpha$. Vamos encontrar $j \in \mathbb{Z}_n$, tal que $j \equiv ax + by \mod n$. Essa equivalência é pelo fato de que a equação diofantina com variáveis x, y e z, $ax + by + zn = j$ tem solução. Como $\text{mdc}(a, b, n) = \text{mdc}(a, b) = 1$ por hipótese, segue que essa equação tem uma solução inteira para algum j.

(iii) Finalmente, mostraremos que Θ preserva a adjacência. Para isso, sejam $j_1, j_2 \in \mathbb{Z}_n$ vértices adjacentes em $\mathbf{C}_n(a, b)$, isto é, $j_1 - j_2 \equiv \pm a, \pm b \mod n$. Mas, note que $\Theta(\pm a) = \pm 1$ e $\Theta(\pm b) = \pm i$, o que implica que a imagem dos vértices são também adjacentes em $\mathcal{G}_\alpha$.

■

Observação 3.4.3. Dados $a + bi$, $c + di \in \mathbb{Z}[i]$ temos que $\mathcal{G}_{a+bi} \cong \mathcal{G}_{c+di}$ se, e somente se, existe $u \in \{\pm 1, \pm i\}$ tal que $a + bi = u(c + di)$ ou $a - bi = u(c + di)$.

Um grafo gaussiano é gerado por um inteiro gaussiano $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$, tal que $0 < a \leq b$. Podemos representar graficamente um grafo gaussiano de forma bidimensional na forma de malhas. A ideia é organizar os $a^2 + b^2$ vértices do grafo em duas malhas de $a \times a$ e $b \times b$ vértices.

Os resultados a seguir caracterizam os vértices e as arestas dos grafos gaussianos nesta representação em malhas. As demonstrações serão omitidas pelo uso de outras ferramentas que não são foco neste trabalho.

Teorema 3.4.6. [29] Sejam $a, b \in \mathbb{Z}$, tal que $0 < a \leq b$, e considere dois conjuntos finitos da seguinte forma:

(i) $S_a = \{x + yi \in \mathbb{Z}[i] \mid 0 \leq x \leq a - 1 \text{ e } 0 \leq y \leq a - 1\}$.

(ii) $S_b = \{x + yi \in \mathbb{Z}[i] \mid a \leq x \leq a + b - 1 \text{ e } 0 \leq y \leq b - 1\}$.

Então, $\mathcal{D} = S_a \cup S_b$ é um sistema de resíduos reduzido de $\mathbb{Z}[i]_\alpha$.

Teorema 3.4.7. [29] Sejam $a, b \in \mathbb{Z}$, tal que $0 < a \leq b$. Suponha que todos os pontos do conjunto $\mathcal{D}$, como no Teorema 3.4.6, são conectados como malha e que suas arestas sejam definidas como:

(i) Se $0 \leq x \leq b - 1$, então x é adjacente a $(x + a) + (b - 1)i$.

(ii) Se $b \leq x \leq a + b - 1$, então x é adjacente a $(x - b) + (a - 1)i$.

(iii) Se $0 \leq y \leq a - 1$, então yi é adjacente a $(a + b - 1) + (y + b - a)i$.

(iv) Se $a \leq y \leq b - 1$, então $a + yi$ é adjacente a $(a + b - 1) + (y - a)i$.

Então, o grafo definido por este padrão de adjacência é isomorfo ao grafo gaussiano gerado por $\mathcal{G}_{a+bi}$.

Nos exemplos a seguir, apresentamos algumas representações de grafos gaussianos na forma de malha de acordo com os Teoremas 3.4.6 e 3.4.7. Consideraremos o vértice 0 localizado, por conveniência, no canto inferior esquerdo da malha menor. Os quatro vértices adjacentes ao vértice zero são $\{\pm 1, \pm i\}$.

Exemplo 3.4.4. Seja $\alpha = 2 + 3i \in \mathbb{Z}[i]$. Como $\text{mdc}(2, 3) = 1$, pela Definição 3.4.3, $\mathcal{G}_{2+3i} = (\mathcal{V}, \mathcal{A})$, onde $\mathcal{V} = \mathbb{Z}[i]_{2+3i}$ e $\mathcal{A} = \{(\beta, \gamma) \in \mathcal{V} \times \mathcal{V} \mid D_\alpha(\beta, \gamma) = 1$, ou $\gamma - \beta \equiv \pm 1, \pm i \mod 2 + 3i\}$ é um grafo gaussiano gerado por $2 + 3i$. Pelo Teorema 3.4.2, $\mathcal{G}_{2+3i}$ tem 13 vértices e pelo Teorema 3.4.6,

$$\mathcal{D} = \{0, 1, i, 1 + i, 2, 3, 4, 2 + i, 2 + 2i, 3 + i, 3 + 2i, 4 + i, 4 + 2i\}$$

é um sistema de resíduos reduzido de $\mathbb{Z}[i]_{2+3i}$, tal que $\mathcal{V} = \mathcal{D}$. Na Figura 3.18, o conjunto $\mathcal{D}$ foi organizado em duas malhas de 2^2 e 3^2 vértices, respectivamente. Seguindo o padrão de adjacência descrito no Teorema 3.4.7, as conexões dos vértices são:

$$(0, 2 + 2i), (1, 3 + 2i), (2, 4 + 2i), (3, i), (4, 1 + i), (i, 4 + 2i) \text{ e } (2 + 2i, 4).$$

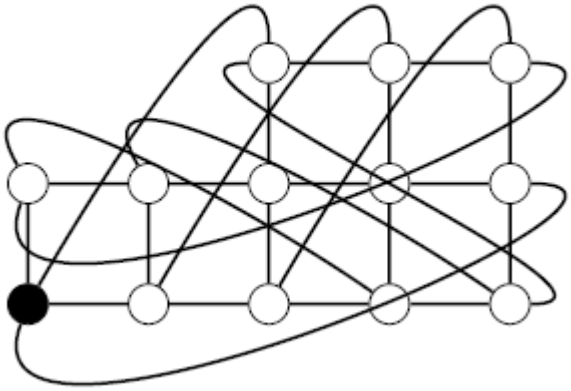

Figura 3.18: Malha em 2D de $\mathcal{G}_{2+3i}$

Exemplo 3.4.5. Seja $\alpha = 3 + 4i \in \mathbb{Z}[i]$. Como $\text{mdc}(3, 4) = 1$, pela Definição 3.4.3, $\mathcal{G}_{3+4i} = (\mathcal{V}, \mathcal{A})$ é um grafo gaussiano gerado por $3 + 4i$, onde $\mathcal{V} = \mathbb{Z}[i]_{3+4i}$ e $\mathcal{A} = \{(\beta, \gamma) \in \mathcal{V} \times \mathcal{V} \mid D_\alpha(\beta, \gamma) = 1$, ou $\gamma - \beta \equiv \pm 1, \pm i \mod 3 + 4i\}$. Pelo Teorema 3.4.2, $\mathcal{G}_{3+4i}$ tem 25 vértices e pelo Teorema 3.4.6,

$$\begin{aligned} \mathcal{D} \;=\; & \{0, 1, 2, i, 2i, 1 + i, 1 + 2i, 2 + i, 2 + 2i, 3, 4, 5, 6, 3 + i, 3 + 2i, 3 + 3i, \\ & 4 + i, 4 + 2i, 4 + 3i, 5 + i, 5 + 2i, 5 + 3i, 6 + i, 6 + 2i, 6 + 3i\} \end{aligned}$$

é um sistema de resíduos reduzido de $\mathbb{Z}[i]_{3+4i}$, onde $\mathcal{V} = \mathcal{D}$. Na Figura 3.19, o conjunto $\mathcal{D}$ foi organizado em duas malhas de 3^2 e 4^2 vértices, respectivamente. Seguindo o padrão de adjacência descrito no Teorema 3.4.7, as conexões dos vértices são:
$(0, 3 + 3i), (1, 4 + 3i), (2, 5 + 3i), (3, 6 + 3i), (0, 6 + i)$,
$(i, 6 + 2i), (2i, 6 + 3i), (4, 2i), (5, 1 + 2i), (6, 2 + 2i)$ e $(3 + 3i, 6)$.

Exemplo 3.4.6. De modo análogo aos Exemplos 3.4.4 e 3.4.5, $\mathcal{G}_{6+8i} = (\mathcal{V}, \mathcal{A})$ é um grafo gaussiano gerado por $6 + 8i$. O conjunto $\mathcal{D}$ agora possui 100 pontos, os quais foram organizados em duas malhas de 6^2 e 8^2 vértices, respectivamente, como representado na Figura 3.20. Seguindo o padrão de adjacência descrito no Teorema 3.4.7, as conexões dos vértices são:
$(0, 6 + 7i), (1, 7 + 7i), (2, 8 + 7i), (3, 9 + 7i), (4, 10 + 7i), (5, 11 + 7i), (6, 12 + 7i)$,
$(7, 13 + 7i), (8, 5i), (9, 1 + 5i), (10, 2 + 5i), (11, 3 + 5i), (12, 4 + 5i), (13, 5 + 5i), (0, 13 + 2i)$,
$(i, 13 + 3i), (2i, 13 + 4i), (3i, 13 + 5i), (4i, 13 + 6i), (5i, 13 + 7i), (6 + 6i, 13), (6 + 7i, 13 + i)$.

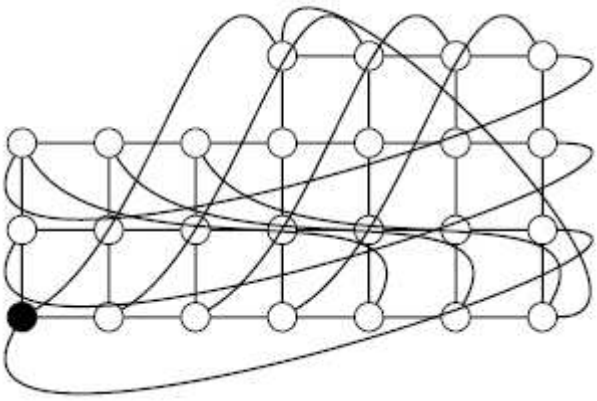

Figura 3.19: Malha em 2D de $\mathcal{G}_{3+4i}$

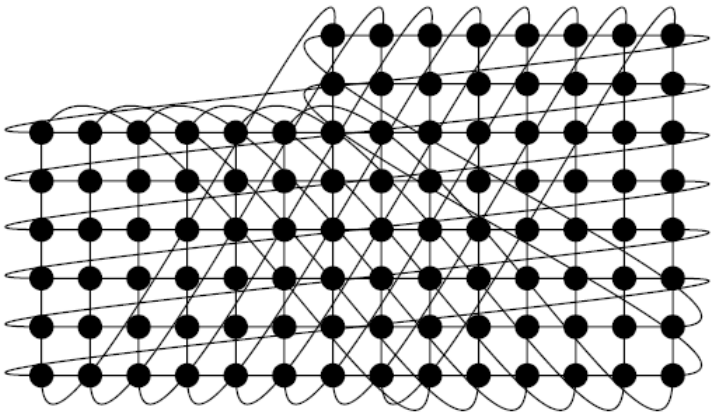

Figura 3.20: Malha em 2D de $\mathcal{G}_{6+8i}$

A partir das Definições 3.4.2 e 3.4.3, podemos estender o conceito de distância entre os elementos do anel quociente $\mathbb{Z}[i]_\alpha$, para os elementos do grafo gaussiano $\mathcal{G}_\alpha$.

Definição 3.4.4. Dado β, $\gamma \in \mathcal{G}_\alpha$. A distância D_α entre β e γ é definida por

$$D_\alpha(\beta,\gamma) = \min\{|x|+|y| \text{ , tal que } (\beta-\gamma) \equiv x+yi \mod \alpha\}. \tag{3.4.2}$$

Além disso, o peso do vértice β (distância para o vértice 0) é definido por

$$W_\alpha(\beta) = D_\alpha(\beta,0) = min\{|x|+|y| \text{ , tal que } \beta \equiv x+yi \mod \alpha\}. \tag{3.4.3}$$

Para calcular a distribuição de distância do grafo gaussiano é suficiente encontrar o número de vértice de peso s, que será denotado por $\Delta_\alpha(s)$. A seguir, serão apresentados resultados que caracterizam a distribuição de peso dos grafos gaussianos de ordem par e que nos orientam a construção de uma nova representação gráfica para tais grafos.

Teorema 3.4.8. [29] Seja $0 \neq \alpha = a+bi \in \mathbb{Z}[i]$, tal que $0 \leq a \leq b$, $n = a^2+b^2$ um inteiro ímpar e $t = \dfrac{a+b-1}{2}$. A distribuição da distancia do grafo $\mathcal{G}_\alpha$ é da seguinte forma:

(i) $\Delta_\alpha(0) = 1$.

(ii) $\Delta_\alpha(s) = 4s$, se $1 \leq s \leq t$.

(iii) $\Delta_\alpha(s) = 4(b-s)$, se $t < s \leq b-1$.

Teorema 3.4.9. [29] Seja $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$, tal que $0 \leq a \leq b$, $n = a^2 + b^2$ um inteiro par e $t = \dfrac{a+b-1}{2}$. Quando $a < b$, a distribuição de distancia do grafo $\mathcal{G}_\alpha$ é da seguinte forma:

(i) $\Delta_\alpha(0) = 1$.

(ii) $\Delta_\alpha(s) = 4s$ se $0 < s < t$.

(iii) $\Delta_\alpha(t) = 2(b-1)$.

(iv) $\Delta_\alpha(s) = 4(b-s)$, se$t < s < b$.

(v) $\Delta_\alpha(b) = 1$.

E, quando $0 < a = b$, a distribuição de distância do grafo $\mathcal{G}_{b+bi}$ é da seguinte forma:

(i) $\Delta_\alpha(0) = 1$.

(ii) $\Delta_\alpha(s) = 4s$ se $0 < s < b$.

(iii) $\Delta_\alpha(b) = 2b-1$.

Corolário 3.4.2. [29] Seja $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$, tal que $0 \leq a \leq b$ e $n = a^2 + b^2$. O diâmetro k do grafo gaussiano $\mathcal{G}_{a+bi}$ é:

$$k = \begin{cases} b, \text{ se } n \text{ é par} \\ b-1, \text{ se } n \text{ é ímpar} \end{cases}$$

Exemplo 3.4.7. Considere o grafo gaussiano $\mathcal{G}_{2+3i}$. Como $n = 2^2 + 3^2 = 13$ é um inteiro ímpar e $t = \dfrac{4}{2} = 2$, pelo Teorema 3.4.8, a distribuição de peso de $\mathcal{G}_{2+3i}$ é a seguinte:

$$\begin{aligned} \Delta_\alpha(0) &= 1 \text{ (1 vértice com peso 0)} \\ \Delta_\alpha(1) &= 4 \text{ (4 vértices com peso 1)} \\ \Delta_\alpha(2) &= 8 \text{ (8 vértices com peso 2)} \end{aligned}$$

Pelo Corolário 3.4.2, o diâmetro de $\mathcal{G}_{2+3i}$ é $k = 2$, isto é, a distância máxima entre os vértices de $\mathcal{G}_{2+3i}$ é 2. Utilizando a distribuição de peso, cuja característica especial é de que todos os vértices são obtidos a uma distância mínima do vértice central, que declaramos zero, na Figura 3.21, representamos graficamente o grafo $\mathcal{G}_{2+3i}$, cujos vértices são rotulados de acordo com o Exemplo 3.4.1, ou seja,

$$\mathcal{V} = \mathbb{Z}[i]_{2+3i} = \{0, 1, 2, -1, -2, i, 2i, -i, -2i.1+i, 1-i, -1-i, -1+i\}.$$

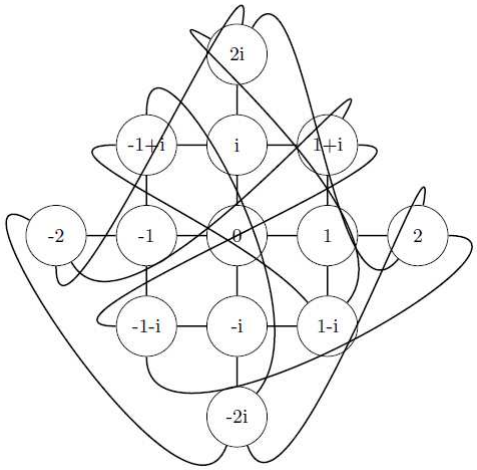

Figura 3.21: Grafo $\mathcal{G}_{2+3i}$

Exemplo 3.4.8. Considere o grafo $\mathcal{G}_{3+4i}$. Como $n = 3^2 + 4^2 = 25$ é um inteiro ímpar e $t = \dfrac{6}{2} = 3$, pelo Teorema 3.4.8, a distribuição de peso de $\mathcal{G}_{3+4i}$ é a seguinte:

$$\begin{aligned}
\Delta_\alpha(0) &= 1 \text{ (1 vértice com peso 0)} \\
\Delta_\alpha(1) &= 4 \text{ (4 vértices com peso 1)} \\
\Delta_\alpha(2) &= 8 \text{ (8 vértices com peso 2)} \\
\Delta_\alpha(3) &= 12 \text{ (12 vértices com peso 3)}
\end{aligned}$$

Pelo Corolário 3.4.2, o diâmetro de $\mathcal{G}_{3+4i}$ é $k = 3$.Utilizando a distribuição de peso, na Figura 3.22 representamos o grafo $\mathcal{G}_{3+4i}$, cujos vértices são rotulados de acordo com o Exemplo 3.4.2, ou seja,

$$\begin{aligned}
\mathbb{Z}[i]_{3+4i} = \{&0, 1, 2, 3, -1, -2, -3, i, 2i, 3i, -i, -2i, -3i, 1+i, 1+2i, 1-i, 1-2i, -1-2i, \\
&-1+i, -1+2i, 2+i, -2+i, 2-i, -2-i\}.
\end{aligned}$$

Exemplo 3.4.9. Considere o grafo $\mathcal{G}_{6+8i}$. Como $n = \mathcal{N}(6+8i) = 100$ é um inteiro par e $t = \dfrac{14}{2} = 7$. Pelo Teorema 3.4.9, a distribuição de peso de $\mathcal{G}_{6+8i}$ é a seguinte:

$$\begin{aligned}
\Delta_\alpha(0) &= 1 \text{ (1 vértice com peso 0)} \\
\Delta_\alpha(1) &= 4 \text{ (4 vértices com peso 1)} \\
\Delta_\alpha(2) &= 8 \text{ (8 vértices com peso 2)} \\
\Delta_\alpha(3) &= 12 \text{ (12 vértices com peso 3)} \\
\Delta_\alpha(4) &= 16 \text{ (16 vértices com peso 4)} \\
\Delta_\alpha(5) &= 20 \text{ (20 vértices com peso 5)} \\
\Delta_\alpha(6) &= 24 \text{ (24 vértices com peso 6)} \\
\Delta_\alpha(7) &= 14 \text{ (14 vértices com peso 7)} \\
\Delta_\alpha(8) &= 1 \text{ (1 vértices com peso 8).}
\end{aligned}$$

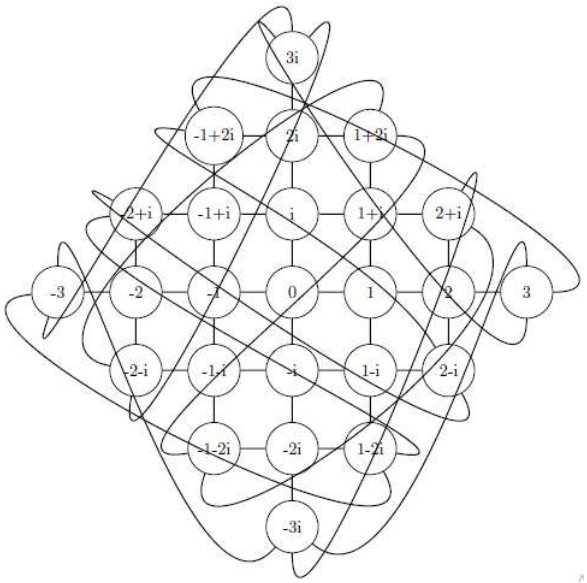

Figura 3.22: $\mathcal{G}_{3+4i}$

Pelo Corolário 3.4.2, o diâmetro de $\mathcal{G}_{6+8i}$ é $k = 8$. Devido a grande quantidade de vértices, omitimos a representação do grafo gaussiano $\mathcal{G}_{6+8i}$, porém, com as informações fornecidas neste exemplo é possível obtê-la.

3.5 Grafo de Eisenstein-Jacobi

A seguir definiremos uma família de grafos em termos dos inteiros de Eisenstein-Jacobi. Mostraremos que tal família são grafos circulantes de grau seis . Para o anel dos inteiros de Eisenstein-Jacobi, a constelação de sinais possui região de Voronoi dada por hexágonos.

Na Definição 1.2.16 apresentamos o anel dos inteiros Eisenstein-Jacobi que é dado por

$$\mathbb{Z}[\omega] = \{x + y\omega | x, y \in \mathbb{Z}\} \text{ , onde } \omega = \frac{-1 + \sqrt{-3}}{2}.$$

Observe que $\omega^2 + \omega + 1 = 0$. Se $\alpha = x + y\omega \in \mathbb{Z}[\omega]$, então sua norma será dada por

$$\begin{array}{rcl} \mathcal{N} : \mathbb{Z}[\omega] & \longrightarrow & \mathbb{N} \\ x + y\omega & \longmapsto & x^2 + y^2 - xy \end{array}$$

Observação 3.5.1. Note que:

(i) $\mathcal{N}(x + y\omega) = (x + y\omega)(\overline{x + y\omega})$, desde que $\overline{x + y\omega} = (x - y) - y\omega$

(ii) As unidades de $\mathbb{Z}[\omega]$ são os elementos com norma unitária que são $\{\pm 1, \pm\omega, \pm\omega^2\}$.

Definição 3.5.1. Se $\langle\alpha\rangle$ denota um ideal de $\mathbb{Z}[\omega]$ gerado por α, então o anel quociente $\dfrac{\mathbb{Z}[\omega]}{\langle\alpha\rangle}$, onde $\alpha \in \mathbb{Z}[\omega]$, denotado por $\mathbb{Z}[\omega]_\alpha$, é chamado *anel quociente dos inteiros de Eisenstein-Jacobi*.

Temos resultados similares aos apresentados para os inteiros gaussianos são válidos para os inteiros de Eisenstein-Jacobi. A seguir, apresentamos alguns desses resultados.

Teorema 3.5.1. [24] Seja $\alpha = a+b\omega \in \mathbb{Z}[\omega]$, tal que $\text{mdc}(a,b) = 1$, e considere $n = \mathcal{N}(\alpha)$. Então, $\mathbb{Z}_n$ e $\mathbb{Z}[\omega]_\alpha$ são anéis isomorfos.

Demonstração. Vamos provar que a função

$$\begin{array}{rccl} f : \mathbb{Z}_n & \longrightarrow & \mathbb{Z}[\omega]_\alpha \\ v & \longrightarrow & v \mod \alpha \end{array}$$

é um isomorfismo de anéis. Inicialmente, oberve que f está bem definida, pois se $v \equiv u \mod n$, então existe $r \in \mathbb{Z}$, tal que $v - u = rn = r\alpha\bar{\alpha}$, para $v \equiv u \mod \alpha$. Para mostrar que f é injetora, considere $v \equiv u \mod \alpha$. Então, existe $\gamma = x + y\omega \in \mathbb{Z}[\omega]$ tal que

$$v - u = \gamma\alpha = (x + y\omega)(a + b\omega) = (ax - by) + (bx + (a - b)y)\omega,$$

de onde obtemos as equações

$$\begin{cases} ax - by = v - u \\ bx + (a - b)y = 0 \end{cases}.$$

Da segunda equação, temos que

$$\{(x, y) = ((a - b)t, -bt) | t \in \mathbb{Z}\} \text{ , desde que } \text{mdc}(a, b) = 1.$$

Agora, substituindo esse valor na primeira equação segue que

$$v - u = a(a - b)t - b(-bt) = (a^2 + b^2 - ab)t = t\mathcal{N}(a + b\omega) = tn \text{ , para } v \equiv u \mod n,$$

como queríamos provar. Agora, para mostrar que f é sobrejetora, considere $\gamma = x + y\omega \in \mathbb{Z}[\omega]_\alpha$. Vamos mostrar que existe $v \in \mathbb{Z}_n$, tal que $v \equiv \gamma \mod \alpha$, ou similarmente, que existem inteiros (x_0, y_0) tal que $(x + y\omega) + (x_0 + y_0\omega)(a + b\omega)$ é um inteiro. Para isso, a parte imaginária deve ser zero, isto é, $bx_0 + (a - b)y_0 = -y$ que sempre tem uma solução com $\text{mdc}(a, b) = 1$, por hipótese.

■

Teorema 3.5.2. [29] Seja $0 \neq \alpha \in \mathbb{Z}[\omega]$. Então, $\mathbb{Z}[\omega]_\alpha$ tem $\mathcal{N}(\alpha)$ elementos.

Corolário 3.5.1. [27] Seja $0 \neq \alpha = a + b\omega \in \mathbb{Z}[\omega]$.

(i) Se $\beta \in \mathbb{Z}[\omega]$ divide α. Então o ideal gerado por β, isto é, $\langle\beta\rangle \subset \mathbb{Z}[\omega]_\alpha$, contém $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)}$ elementos.

(ii) Se $\beta \in \mathbb{Z}[\omega]$ não divide α, e $\eta = \text{mdc}(\beta, \alpha)$. Então o ideal $\langle\beta\rangle \subset \mathbb{Z}[\omega]_\alpha$ é gerado por η e contém $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\eta)}$ elementos.

Exemplo 3.5.1. Dado $\alpha = 2 + 3\omega \in \mathbb{Z}[\omega]$, temos que $\mathcal{N}(\alpha) = 7$ e, pelo Teorema 3.5.2, $\mathbb{Z}[\omega]_{2+3\omega}$ tem 7 elementos, obtidos pelo quociente do anel $\mathbb{Z}[\omega]$ com o ideal $\langle 2 + 3\omega\rangle$, ou seja, tomamos os elementos de $\mathbb{Z}[\omega]$ e fazemos módulo $(2 + 3\omega)$. Dessa forma, obtemos

$$\mathbb{Z}[\omega]_{2+3\omega} = \{0, 1, -1, \omega, -\omega, -1 - \omega, 1 + \omega\}.$$

Representamos graficamente $\mathbb{Z}[\omega]_{2+3\omega}$ na Figura 3.23.

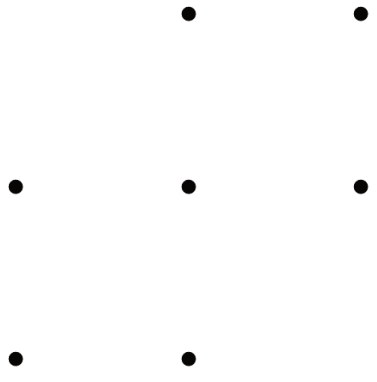

Figura 3.23: $\mathbb{Z}[\omega]_{2+3\omega}$

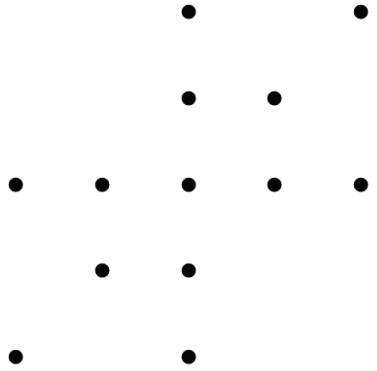

Figura 3.24: $\mathbb{Z}[\omega]_{3+4\omega}$

Exemplo 3.5.2. Dado $\alpha = 3 + 4\omega \in \mathbb{Z}[\omega]$, temos que $\mathcal{N}(\alpha) = 13$. Pelo Teorema 3.5.2, $\mathbb{Z}[\omega]_{3+4\omega}$ tem 13 elementos, obtidos pelo quociente do anel $\mathbb{Z}[\omega]$ e o ideal $\langle 3 + 4\omega \rangle$, ou seja, tomamos os elementos de $\mathbb{Z}[\omega]$ e fazemos $\mod 3 + 4\omega$. Dessa forma, obtemos

$$\mathbb{Z}[\omega]_{3+4\omega} = \{0, 1, -1, \omega, -\omega, 1 + \omega, -1 - \omega, 2, -2, 2\omega, -2\omega, 2 + 2\omega, -2 - 2\omega\}.$$

Representamos graficamente $\mathbb{Z}[\omega]_{3+4\omega}$ na Figura 3.24.

Temos também a noção de distância entre os elementos do anel quociente dos inteiros de Eiseintein-Jacobi.

Definição 3.5.2. Seja $0 \neq \alpha \in \mathbb{Z}[\omega]$. Para $\beta, \gamma \in \mathbb{Z}[\omega]_\alpha$, considere $x + y\omega + z\omega^2$ uma classe de $\beta - \gamma$ com $|x|+|y|+|z|$ mínimo. A distância D_α entre β e γ é definida por

$$D_\alpha(\beta, \gamma) = \{|x|+|y|+|z| \mid \gamma - \beta \equiv x + y\omega + z\omega^2 \mod \alpha\}.$$

Teorema 3.5.3. [24] D_α define a distância sobre o anel quociente $\mathbb{Z}[\omega]_\alpha$.

Exemplo 3.5.3. Para o anel quociente $\mathbb{Z}[\omega]_{3+4\omega}$:

(i) Se $\gamma = \omega$ e $\beta = -\omega$, temos que $\gamma - \beta = 2\omega$. Logo, $D_\alpha(\beta, \gamma) = 2$.

(ii) Se $\gamma = 1 + \omega$ e $\beta = -1$, temos que $\gamma - \beta = 2 + \omega \equiv -2 \mod \alpha$. Logo, $D_\alpha(\beta, \gamma) = 2$.

Apresentamos a seguir o conceito de grafo de Eisenstein-Jacobi a partir do seu anel quociente.

Definição 3.5.3. Seja $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, com $\text{mdc}(a, b) = 1$ e considere o anel quociente $\mathbb{Z}[\omega]_\alpha$. Chamamos $\mathcal{J}_\alpha = (\mathcal{V}, \mathcal{A})$ de *grafo de Eisenstein-Jacobi* gerado por α, onde:

(i) $\mathcal{V} = \mathbb{Z}[\omega]_\alpha$ é o conjunto de vértices, e

(ii) $\mathcal{A} = \{(\beta, \gamma) \in \mathcal{V} \times \mathcal{V} \mid D_\alpha(\beta, \gamma) = 1\}$.

Observação 3.5.2. Se $D_\alpha(\beta, \gamma) = 1$ então $(\gamma - \beta) \equiv \pm 1, \pm\omega, \pm\omega^2 \mod \alpha$, isto é, um par de vértices é conectado por uma aresta se, e somente se, a sua diferença módulo α é uma unidade de $\mathbb{Z}[\omega]$.

O teorema a seguir mostra que um grafo de Eisenstein-Jacobi, é um grafo circulante de grau 6.

Teorema 3.5.4. [24] Seja $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, tal que $\text{mdc}(a, b) = 1$ e $n = \mathcal{N}(\alpha) = a^2 + b^2 - ab$. Então, os grafos $\mathcal{J}_\alpha$ e $\mathbf{C}_n(a, b, a - b)$ são isomorfos.

Demonstração. Como $\text{mdc}(a, b) = 1$, então um inteiro m pode ser representado na forma $m \equiv bx - ay \mod n$. Vamos mostrar que

$$\begin{array}{rcl} \Theta : \mathbb{Z}_n & \longrightarrow & \mathbb{Z}[\omega]_\alpha \\ m & \longmapsto & x + y\omega \mod \alpha \end{array}$$

é um isomorfismo de grafos. Θ está bem definido, pois se $bx - ay \equiv 0 \mod n$, então existe q,$t \in \mathbb{Z}$ tal que

$$\left\{ \begin{array}{rcl} x & = & q(a + b) + at \\ y & = & q(2b - a) + bt \end{array} \right. .$$

Então,

$$\begin{array}{rcl} \Theta(bx - ay) & = & x + y\omega \\ & = & q((a + b) + (2b - a)\omega) + t(a + b)\omega \\ & = & q(1 - \omega)(a + b\omega) + t(a + b\omega) \\ & \equiv & 0(\mod \alpha) \end{array}$$

Além disso, Θ é injetora. De fato, se $\Theta(bx - ay) = x + y\omega \equiv 0 \mod \alpha$, então existe c,$d \in \mathbb{Z}$ tal que $x + y\omega = (ac - db) + (ad + bc - db)\omega$. Assim,

$$\left\{ \begin{array}{rcl} x & = & ac - bd \\ y & = & ad + bc - db \end{array} \right. ,$$

de onde obtemos que

$$bx - ay = -d(a^2 + b^2 - ab) = -dn \equiv 0 \mod n.$$

Como ambos os conjuntos tem o mesmo número de elementos, Θ é uma bijeção. Agora, se dois vértices u, v são adjacentes no grafo circulante, então $u - v \equiv \pm a, \pm b, \pm(a - b) \mod n$. Assim, $\Theta(u) - \Theta(v) = \Theta(u - v) \equiv \pm\Theta(a), \pm\Theta(b), \pm\Theta(a - b)$, o que implica que $\Theta(a) = \omega$,$\Theta(b) = -1$ e $\Theta(a - b) = \Theta(a) - \Theta(b) = 1 + \omega$. Logo, $D_\alpha(\Theta(u), \Theta(v)) = 1$, e portanto, $\Theta(u)$ e $\Theta(v)$ são vértices adjacentes em $\mathcal{J}_\alpha$. ■

Finalizamos, apresentando exemplos de representações de grafos de Eisenstein-Jacobi.

Exemplo 3.5.4. Considere o grafo $\mathcal{J}_{2+3\omega} = (\mathcal{V}, \mathcal{A})$, onde pela Definição 3.5.3 e pelo Exemplo 3.5.1 segue que

$$\mathcal{V} = \mathbb{Z}[\omega]_{2+3\omega} = \{0, 1, -1, \omega, -\omega, -1-\omega, 1+\omega\},$$

e assim,

$$\begin{aligned}\mathcal{A} \;=\; & \{(0,1),(0,1+\omega),(0,\omega),(0,-1),(0,-1-\omega),(0,-\omega),(1,1+\omega),(1,\omega),(1,-1),\\ & (1,-1-\omega),(1,-\omega),(1+\omega,\omega),(1+\omega,-1),(1+\omega,-1-\omega),(1+\omega,-\omega),(\omega,-1),\\ & (\omega,-1-\omega),(\omega,-\omega),(-1,-1-\omega),(-1,-\omega),(-1-\omega,-\omega)\}.\end{aligned}$$

Na Figura 3.25, apresentamos o grafo $\mathcal{J}_{2+3\omega}$, com seus vértices e adjacências.

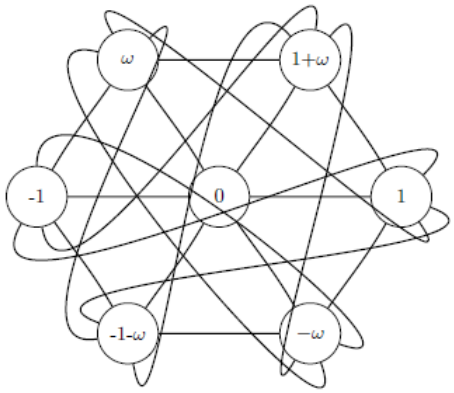

Figura 3.25: $\mathcal{J}_{2+3\omega}$

Exemplo 3.5.5. Considere o grafo $\mathcal{J}_{3+4\omega} = (\mathcal{V}, \mathcal{A})$, onde pela Definição 3.5.3 e pelo Exemplo 3.5.2 segue que

$$\mathcal{V} = \mathbb{Z}[\omega]_{3+4\omega} = \{0, 1, -1, \omega, -\omega, 1+\omega, -1-\omega, 2, -2, 2\omega, -2\omega, 2+2\omega, -2-2\omega\},$$

e assim,

$$\begin{aligned}\mathcal{A} \;=\; & \{(0,1),(0,1+\omega),(0,\omega),(0,-1),(0,-1-\omega),(0,-\omega),(1,2),(1,1+\omega),\\ & (1,-\omega),(1,2\omega),(1,-2),(1+\omega,2+2\omega),(1+\omega,\omega),(1+\omega,-2),(1+\omega,-2-2\omega),\\ & (\omega,2\omega),(\omega,-1),(\omega,-2-2\omega),(\omega,-2\omega),(-1,-2),(-1,-1-\omega),(-1,2),\\ & (-1,-2\omega),(-1-\omega,-2-2\omega),(-1-\omega,-\omega),(-1-\omega,2),(-1-\omega,2+2\omega),\\ & (-\omega,-2\omega),(-\omega,2+2\omega),(-\omega,2\omega),(2,2\omega),(2,-2-2\omega),\\ & (2+2\omega,-2-2\omega),(2+2\omega,-2),(2+2\omega,-2\omega),\\ & (2\omega,-2-2\omega),(2\omega,-2\omega),(-2,-2\omega)\}.\end{aligned}$$

Na Figura 3.26, apresentamos o grafo $\mathcal{J}_{3+4\omega}$, com seus vértices e adjacências.

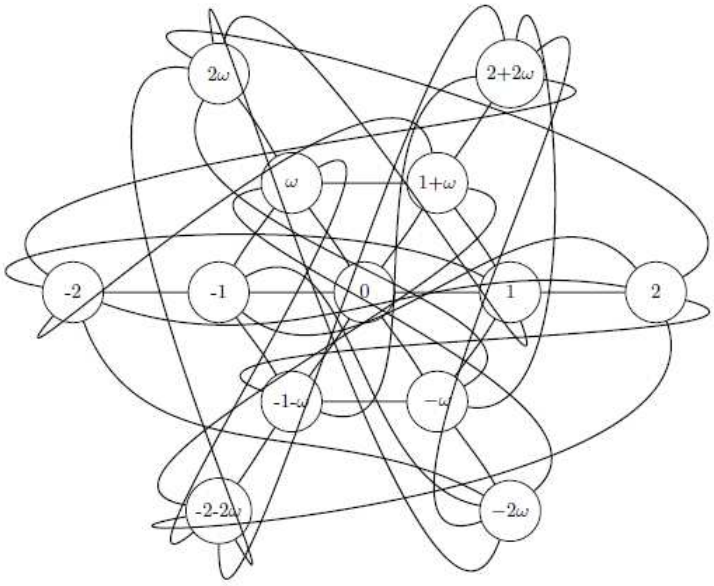

Figura 3.26: $\mathcal{J}_{3+4\omega}$

Capítulo 4

Códigos Perfeitos sobre Inteiros Gaussianos e Eisenstein-Jacobi

Neste capítulo apresentamos uma construção de códigos perfeitos sobre grafos circulantes de graus quatro e seis, respectivamente grafos gaussianos e grafos de Eisenstein-Jacobi. As construções apresentadas neste capítulo foram baseadas nas referências, [11, 24, 29], porém novos exemplos e representações de tais códigos serão apresentadas. Um código sobre um grafo será definido como um subconjunto não vazio do conjunto de vértices deste grafo, cujos elementos formam a região de Voronoi associada a eles. Quando esses elementos são centros das bolas de raio t e formam uma partição do conjunto de vértices, o código será dito perfeito corretor de t erros e o grafo associado será chamado de t-dominante.

Considere um grafo $\mathcal{G}_\alpha = (\mathcal{V}, \mathcal{A})$, onde $\mathcal{V} = \mathbb{Z}[i]_\alpha$ ou $\mathcal{V} = \mathbb{Z}[\omega]_\alpha$, no caso de um grafo gaussiano ou de um grafo de Eisenstein-Jacobi, como nas Definições 3.4.3 e 3.5.3, respectivamente. Considere também a distância D_α, definida para tais conjuntos como em (3.4.2) e (3.5.2), respectivamente.

Definição 4.0.1. Dado um grafo $\mathcal{G}_\alpha = (\mathcal{V}, \mathcal{E})$, um *código* em $\mathcal{G}_\alpha$ é um subconjunto não vazio $\mathcal{C}$ de $\mathcal{G}_\alpha$.

O subconjunto $\mathcal{V}_\eta$ formado pelos elementos de $\mathcal{V}$, para os quais $\eta \in \mathcal{C}$ é o ponto mais próximo em $\mathcal{C}$, isto é, $\mathcal{V}_\eta = \{\tau \in \mathcal{V}; D_\alpha(\eta, \tau) = D_\alpha(\eta, \mathcal{C})\}$ é a região de Voronoi $\mathcal{V}_\eta$ associada a $\eta \in \mathcal{C}$. O número $t = \max\{D_\alpha(\eta, \mathcal{C}) \mid \eta \in \mathcal{V}\}$ é chamado *raio de cobertura* do código, que é o menor número t tal que as bolas de raio t centradas nos pontos de $\mathcal{C}$, dadas por $\mathbf{B}_t(\eta) = \{\tau \in \mathcal{V} \mid D_\alpha(\eta, \tau) \leq t\}$ cobrem $\mathcal{V}$. O número $\delta = \min\{D_\alpha(\eta, \tau) \mid \eta, \tau \in \mathcal{C}, \eta \neq \tau\}$ é a distância mínima de $\mathcal{C}$ e $\delta \leq 2t+1$, a igualdade vale quando as bolas de raio t centradas nos pontos de $\mathcal{C}$ formam uma partição de $\mathcal{V}$. Um código com está propriedade é chamado *perfeito* e é dito corretor de t erros.

Assim como nas Seções 3.4 e 3.5, os grafos gaussianos e de Eisenstein-Jacobi são separadamente apresentados, respectivamente. Neste capítulo, apresentaremos a construção de códigos perfeitos sobre grafos de inteiros gaussianos na Seção 4.1 e, na Seção 4.2 será apresentada a construção de códigos perfeitos sobre grafos de inteiros de Eisenstein-Jacobi.

4.1 Códigos Perfeitos sobre Grafos Gaussianos

Nesta seção vamos apresentar códigos corretores de erros sobre constelações QAM, modeladas por grafos gaussianos. Nessas constelações cada ponto de sinal tem quatro outros pontos vizinhos de distância um, o que os torna adequados para serem modelados

pelo anel dos inteiros gaussianos. Veremos que esses códigos são perfeitos e a métrica empregada é a distância entre os vértices do grafo que modelam a constelação $\mathbb{Z}[i]_\alpha$.

A seguir definiremos conjuntos perfeitos t-dominantes sobre grafos gaussianos, que são ideais de $\mathbb{Z}[i]_\alpha$. Esses conjuntos geram diretamente códigos perfeitos sobre anéis quocientes gaussianos.

Definição 4.1.1. Sejam $\alpha = a + bi \in \mathbb{Z}[i]$, tal que $\text{mdc}(a, b) = 1$ e $0 < a < b$, e $\mathcal{G}_\alpha = (\mathcal{V}, \mathcal{A})$ um grafo gaussiano. Dado $t \leq b$, um vértice γ é dito *t-dominar* o vértice β, se $\beta \in \mathbf{B}_t(\gamma)$, onde $\mathbf{B}_t(\gamma) = \{\eta \in \mathbb{Z}[i]_\alpha \mid D_\alpha(\eta, \gamma) \leq t\}$ é uma bola de raio t centrada em γ embutida em $\mathcal{G}_\alpha$. Um subconjunto de vértices S é chamado *conjunto perfeito t-dominante* se cada vértice de $\mathcal{G}_\alpha$ é t-dominar de um único vértice em S.

Teorema 4.1.1. [29] Seja $0 \neq \alpha \in \mathbb{Z}[i]$ e t um inteiro positivo. Temos que:

i) Se $\beta = t + (t + 1)i$ divide α, então o ideal $S = \langle\beta\rangle \subseteq \mathbb{Z}[i]_\alpha$ é um conjunto perfeito t-dominante em $\mathcal{G}_\alpha$;

ii) Se $\bar{\beta} = t - (t + 1)i$ divide α, então o ideal $S = \langle\bar{\beta}\rangle \subseteq \mathbb{Z}[i]_\alpha$ é um conjunto perfeito t-dominante em $\mathcal{G}_\alpha$.

Demonstração. Seja $\alpha = a + bi \in \mathbb{Z}[i]$. Pelo Corolário 3.4.1, S tem exatamente

$$\frac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)} = \frac{a^2 + b^2}{t^2 + (t + 1)^2}$$

elementos. Observe que, $\mathcal{N}(\beta) = \mathcal{N}(\bar{\beta})$, assim, a prova do primeiro e segundo item seguem o mesmo procedimento. Sejam $\beta_1, \beta_2 \in S = \langle\beta\rangle$. Então, $\beta_1 = \alpha_1\beta$ e $\beta_2 = \alpha_2\beta$, onde $\alpha_1, \alpha_2 \in \mathbb{Z}[i]$. Temos que provar que

$$D_\alpha(\beta_1, \beta_2) = D_\alpha(\alpha_1\beta, \alpha_2\beta) = D_\alpha((\alpha_1 - \alpha_2)\beta, 0) \geq 2t + 1,$$

onde D_α denota a distância do grafo gaussiano. Para isso, é suficiente provar que para qualquer $\eta \in \mathbb{Z}[i]$, tal que $\eta\beta \not\equiv 0 \mod \alpha$, então $D_\alpha(\eta\beta, 0) \geq 2t + 1$ e, para $\eta \in \{1, i, -1, -i\}$ temos que $D_\alpha(\eta\beta, 0) = 2t + 1$. Suponha o contrário. Se $D_\alpha(\eta\beta, 0) < 2t + 1$, então $\eta\beta \equiv x + yi \mod \alpha$, com $|x|+|y| < 2t + 1$ mínimo. Portanto, $\eta\beta = (x + yi) + \gamma_1\alpha = (x + yi) + \gamma_2\beta$, onde $\gamma_1, \gamma_2 \in \mathbb{Z}[i]$, implica que $x + yi = \beta(\eta - \gamma_2)$. Agora, $\mathcal{N}(x + yi) \leq 4t^2$ desde que $|x|+|y| \leq 2t$. Como $\mathcal{N}(\beta) = 2t^2 + 2t + 1 > 2t^2$ para $t > 0$, então $\mathcal{N}(\eta - \gamma_2) < 2$. Consequentemente, $x + yi = \beta u$, com $u \in \{1, i, -1, -i\}$. Assim em qualquer caso, $|x|+|y| = 2t + 1$ é uma contradição. ■

Observação 4.1.1. Dado β tal que $\beta = t \pm (t + 1)i$, sua norma $\mathcal{N}(\beta) = 2t^2 + 2t + 1$ resulta no número de pontos da região de Voronoi, que pode ser vista como uma esfera de Lee de raio t, onde cada ponto do grafo é uma célula da esfera.

Exemplo 4.1.1. Seja $\alpha = 8 + 9i = (1 - 2i)(2 - 5i)(-1) \in \mathbb{Z}[i]$. Como $\beta = 1 - 2i$ divide $\alpha = 8+9i$, pelo Corolário 3.4.1, o ideal $S = \langle 1-2i\rangle \subseteq \mathbb{Z}[i]_{8+9i}$ tem 29 elementos. Portanto,

$$\begin{aligned} S = \langle 1 - 2i\rangle \;=\; & \{0, 1 - 2i, -1 + 2i, 2 + i, -2 - i, 2 - 4i, -2 + 4i, 3 - i, 1 + 3i, \\ & -1 - 3i, 4 + 2i, -4 - 2i, -2 - 6i, 2 + 6i, 4 - 3i, 5, -3 - 4i, -5i, \\ & -5, 3 + 4i, -4 + 3i, 5i, 7 + i, 1 - 7i, -7 - i, -1 + 7i, 6 - 2i, -6 + 2i\}. \end{aligned}$$

Como $\beta = 1-2i$ é da forma $\bar{\beta} = t-(t+1)i$, com $t = 1$, pelo Teorema 4.1.1, $S = \langle 1-2i\rangle \subseteq \mathbb{Z}[i]_{8+9i}$ é um conjunto perfeito 1-dominante no grafo $\mathcal{G}_{8+9i}$, representado na Figura 4.1. Os pontos destacados em negrito são os centros das bolas de raio $t = 1$.

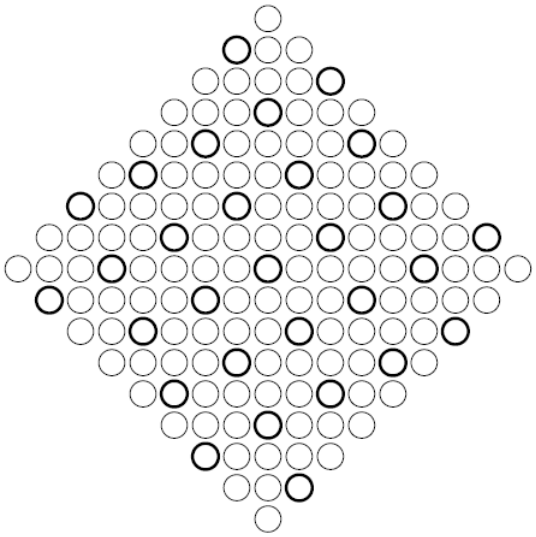

Figura 4.1: Conjunto Perfeito 1-dominante em G_{8+9i}

Exemplo 4.1.2. Seja $\alpha = 10 + 11i = (2 - 3i)(-1 + 4i) \in \mathbb{Z}[i]$. Como $\beta = 2 - 3i$ divide $\alpha = 10 + 11i$, pelo Corolário 3.4.1, o ideal $S = \langle 2 - 3i \rangle \subseteq \mathbb{Z}[i]_{10+11i}$ tem 17 elementos, logo

$$\begin{aligned} S = \langle 2 - 3i \rangle \;\; = \;\; & \{0, 2 - 3i, -2 + 3i, 3 + 2i, -3 - 2i, 4 - 6i, -4 + 6i, 5 - i, -1 - 5i, \\ & 1 + 5i, -5 + i, 6 + 4i, -6 - 4i, 1 - 8i, 8 + i, -1 + 8i, -1 + 8i, -8 - i\}. \end{aligned}$$

Como $\beta = 2 - 3i$ é da forma $\bar{\beta} = t - (t+1)i$, com $t = 2$, pelo Teorema 4.1.1, $S = \langle 2 - 3i \rangle \subseteq \mathbb{Z}[i]_{10+11i}$ é um conjunto perfeito 2-dominante no grafo $\mathcal{G}_{10+11i}$, representado na Figura 4.2. Os pontos destacados em negrito são os centros das bolas de raio $t = 2$.

Pode-se assim definir um código $\mathcal{C} = S$ sobre $\mathbb{Z}[i]_\alpha$ cujas palavras-código são os elementos de S e formam um ideal. Iremos mostrar que tais códigos são perfeitos com distância mínima igual a $2t + 1$. Como vimos, um código $\mathcal{C}$ é chamado perfeito, se as bolas de raio t centradas nos pontos de $\mathcal{C}$ particionam o conjunto de pontos $\mathcal{V}$, ou seja, é um código que corrige todos os padrões com até t erros e nenhum padrão com $t + 1$ erros ou mais.

Veremos a seguir que, se t é um inteiro positivo tal que $t + (t+1)i$ ou $t - (t+1)i$ divide α, então existe um conjunto S perfeito t-dominante de $\mathcal{G}_\alpha$ que é um ideal de $\mathbb{Z}[i]_\alpha$.

Lema 4.1.1. Seja t um inteiro positivo e $\alpha \in \mathbb{Z}[i]$. Para cada $\eta \in \mathbb{Z}[i]_\alpha$ temos que

$$B_t(\eta) \cap B_t(0) = \emptyset \iff D_\alpha(\eta, 0) \geq 2t + 1.$$

Teorema 4.1.2. Seja $\alpha = a+bi \in \mathbb{Z}[i]$ e t um inteiro positivo. Se existir um código perfeito $\mathcal{C}$ t-corretor de erros sobre $\mathbb{Z}[i]_\alpha$, então este deve ser gerado por $t + (t+1)i$ ou $t - (t+1)i$.

Demonstração. Seja $\mathcal{C}$ um código perfeito t-corretor de erros sobre $\mathbb{Z}[i]_\alpha$, com cardinalidade $\dfrac{\mathcal{N}(\alpha)}{t^2 + (t+1)^2}$. Então, $\mathcal{C}$ é gerado por um elemento $\beta = x + yi \in \mathbb{Z}[i]$ tal que $\beta | \alpha$ é um domínio de ideais principais. Além disso, este elemento deve satisfazer o Corolário 3.4.1, onde a cardinalidade é o número

$$\frac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)} = x^2 + y^2 = t^2 + (t+1)^2.$$

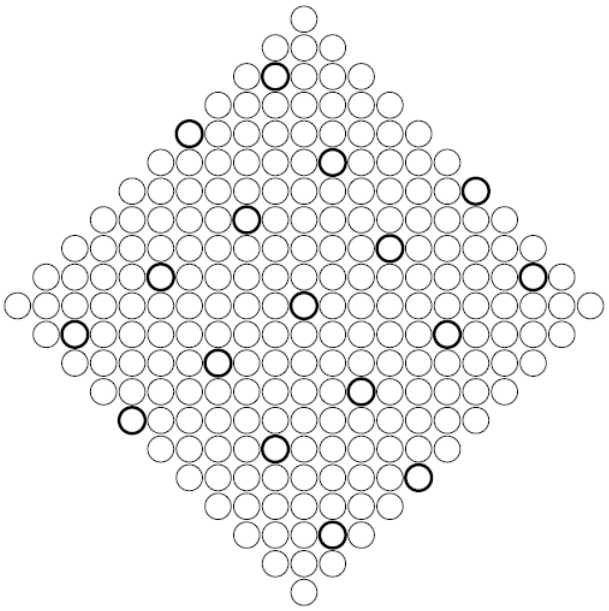

Figura 4.2: Conjunto Perfeito 2-dominante em G_{10+11i}

Agora, vamos mostrar que necessariamente $|x|+|y|= 2t+1$. Se $|x|+|y|< 2t+1$, temos que $D_\alpha(\beta,0) \leq |x|+|y|< 2t+1$ e pelo Lema 4.1.1

$$B_t(\eta) \cap B_t(0) = \emptyset \iff D_\alpha(\eta,0) \geq 2t+1,$$

o que não ocorre pois 0 e β pertencem a $\mathcal{C}$. Agora, se $|x|+|y|> 2t+1$, temos que $x^2+y^2 = t^2+(t+1)^2$. Então,

$$\begin{aligned} |x|> 2t+1-|y| &\implies |x|^2> (2t+1)^2 - 2(2t+1)|y|+|y|^2 \\ &\implies t^2+(t+1)^2 = x^2+y^2 > (2t+1)^2 - 2(2t+1)|y|+|y|^2+|y|^2 \\ &\implies 0 > t(t+1) - (2t+1)|y|+|y|^2= (|y|-(t+1))(|y|-t), \end{aligned}$$

que é também uma contradição pois y e t são inteiros. Assim, necessariamente $|x|+|y|= 2t+1$. Logo,

$$|x|+|y|= 2t+1 \implies x^2+y^2 = t^2+(t+1)^2 \implies \beta = x+yi,$$

de onde segue que $|x|= t$ e $|y|= t+1$ ou $|x|= t+1$ e $|y|= t$, e portanto, $\beta = t+(t+1)i$ ou $\beta = t-(t+1)i$.

■

Portanto, concluímos que, dado um conjunto perfeito t-dominante S, nas condições dos Teoremas 4.1.1 e 4.1.2, ele forma um código perfeito. A seguir, apresentamos exemplos de códigos perfeitos t-dominantes sobre grafos gaussianos.

Exemplo 4.1.3. Como vimos no Exemplo 4.1.1, o ideal $S = \langle 1-2i\rangle \subseteq \mathbb{Z}[i]_{8+9i}$ é um conjunto perfeito 1-dominante no grafo $\mathcal{G}_{8+9i}$. Portanto, um código perfeito que corrige todos os padrões com 1 erro e nenhum padrão com 2 ou mais erros é dado pelo conjunto S. Na Figura 4.3, as 29 palavras-código do código perfeito gerado por $S = \langle 1-2i\rangle$ são identificadas no grafo pelos pontos destacados em negrito, formando os baricentros dos 29 polígonos fundamentais (contendo 5 elementos cada) que recobrem a constelação de sinais composta pelos 145 elementos de $\mathbb{Z}[i]_{8+9i}$.

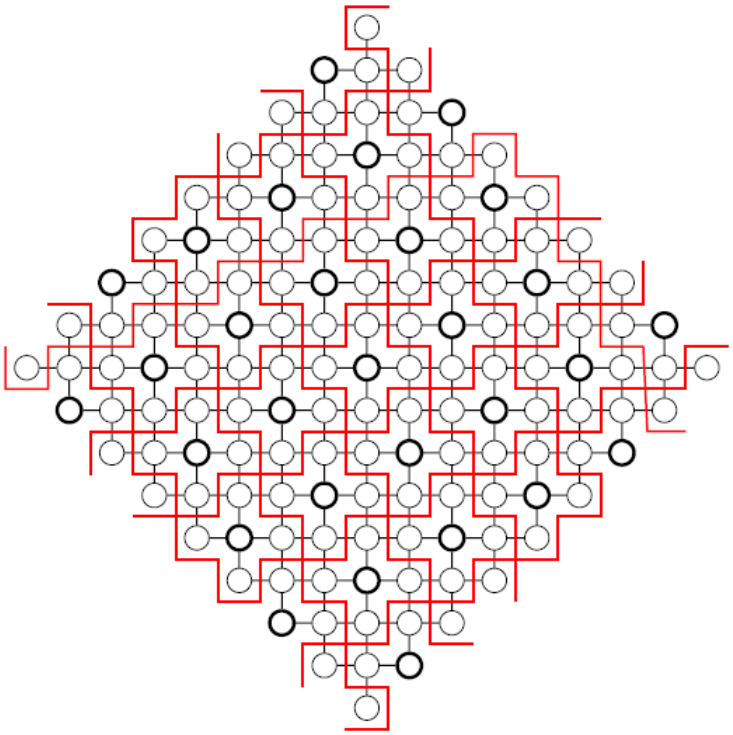

Figura 4.3: Código Perfeito 1-dominante em $\mathcal{G}_{8+9i}$

Exemplo 4.1.4. Como vimos no Exemplo 4.1.2, o ideal $S = \langle 2 - 3i \rangle \subseteq \mathbb{Z}[i]_{10+11i}$, é um conjunto perfeito 2-dominante no grafo $\mathcal{G}_{10+11i}$. Portanto, um código perfeito que corrige todos os padrões com 2 erros e nenhum padrão com 3 ou mais erros é dado pelo conjunto S. Na Figura 4.4, as 17 palavras-código do código perfeito gerado por $S = \langle 2 - 3i \rangle$ são identificadas no grafo pelos pontos destacados em negrito, formando os baricentros dos 17 polígonos fundamentais (contendo 13 elementos cada) que recobrem a constelação de sinais, contendo os 221 elementos de $\mathbb{Z}[i]_{10+11i}$.

4.1.1 Grafo Quociente

Nesta subseção, iremos definir um grafo quociente de um grafo gaussiano.

Definição 4.1.2. [29] Seja $0 \neq \alpha \in \mathbb{Z}[i]$ tal que existe um inteiro positivo t tal que $t + (t+1)i$ ou $t - (t+1)i$ divide α. Se β for este divisor exato e $\mathcal{G}_\alpha$ o grafo gaussiano gerado por α, então definimos o *grafo quociente* de $\mathcal{G}_\alpha$ por β, denotado por, $\dfrac{\mathcal{G}_\alpha}{\beta} = (\mathcal{V}, \mathcal{A})$, da seguinte forma:

(i) O ideal $\mathcal{V} = \langle \beta \rangle$ é o conjunto de vértices.

(ii) $\mathcal{A} = \{(\gamma_1, \gamma_2) \in \mathcal{V} \times \mathcal{V} \mid D_\alpha(\gamma_1, \gamma_2) = 2t + 1\}$ é o conjunto de arestas, onde D_α é a distância do grafo em $\mathcal{G}_\alpha$.

Teorema 4.1.3. [29] Seja $0 \neq \alpha \in \mathbb{Z}[i]$ tal que existe um inteiro positivo t tal que $t + (t+1)i$ ou $t - (t+1)i$ divide α. Se β for este divisor exato e $\mathcal{G}_\alpha$ o grafo gaussiano gerado por α. Então, os grafos $\dfrac{\mathcal{G}_\alpha}{\beta}$ e $\mathcal{G}_{\frac{\alpha}{\beta}}$ são isomorfos.

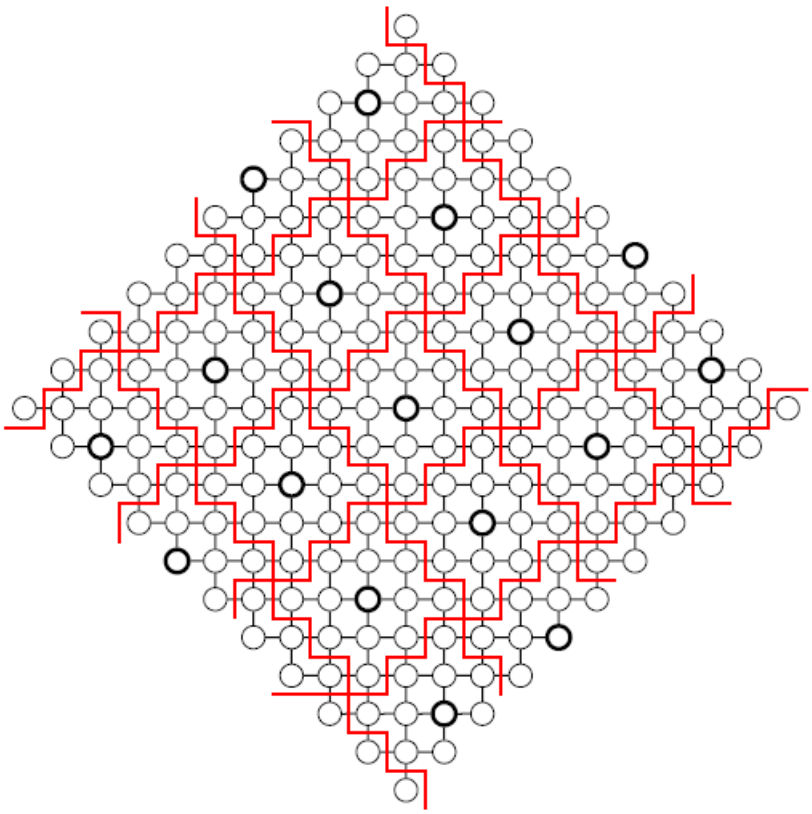

Figura 4.4: Código Perfeito 2-dominante em $\mathbb{Z}_{10+11i}$

Exemplo 4.1.5. Seja $\alpha = 3 + 4i = (1 - 2i)(-1 + 2i) \in \mathbb{Z}[i]$. Como $\beta = 1 - 2i$ divide α, temos que o ideal gerado por $1 - 2i$ forma um código perfeito 1-corretor sobre $\mathbb{Z}[i]_\alpha$. A Figura 4.5 ilustra o código perfeito sobre $\mathbb{Z}[i]_{3+4i}$ e o grafo quociente $\dfrac{\mathcal{G}_{3+4i}}{1-2i}$.

4.2 Códigos Perfeitos sobre Grafos de Eisenstein-Jacobi

Nesta seção vamos apresentar códigos perfeitos sobre grafos de inteiros de Eisenstein-Jacobi. Nessas constelações cada ponto de sinal tem seis outros pontos vizinhos com distância um, o que os torna adequados para serem modelados pelo anel dos inteiros de Eisenstein-Jacobi.

Iniciamos definindo conjuntos perfeitos t-dominantes sobre grafos de Eisenstein-Jacobi, que são ideais de $\mathbb{Z}[\omega]_\alpha$,onde $\omega = \dfrac{-1+\sqrt{-3}}{2}$. Analogamente, como no caso gaussiano, esses ideais irão gerar diretamente códigos perfeitos sobre anéis quocientes de Eisenstein-Jacobi em relação à distância do grafo associado.

Dado $0 \neq \alpha = a + b\omega \in \mathbb{Z}[\omega]$, $\mathcal{J}_\alpha$ um grafo de Eisenstein-Jacobi, um inteiro $t > 0$, e um vértice $\eta \in \mathcal{J}_\alpha$. Uma bola de raio t centrado em η embutido em $\mathcal{J}_\alpha$ é o conjunto

$$\mathbf{B}_t(\eta) = \{\gamma \in \mathcal{J}_\alpha \mid D_\alpha(\gamma, \eta) \leq t\}.$$

Para algum β, a cardinalidade de $B_t(\beta)$ é $1 + \sum_{d=1}^{t} 6d = 3t^2 + 3t + 1$[29].

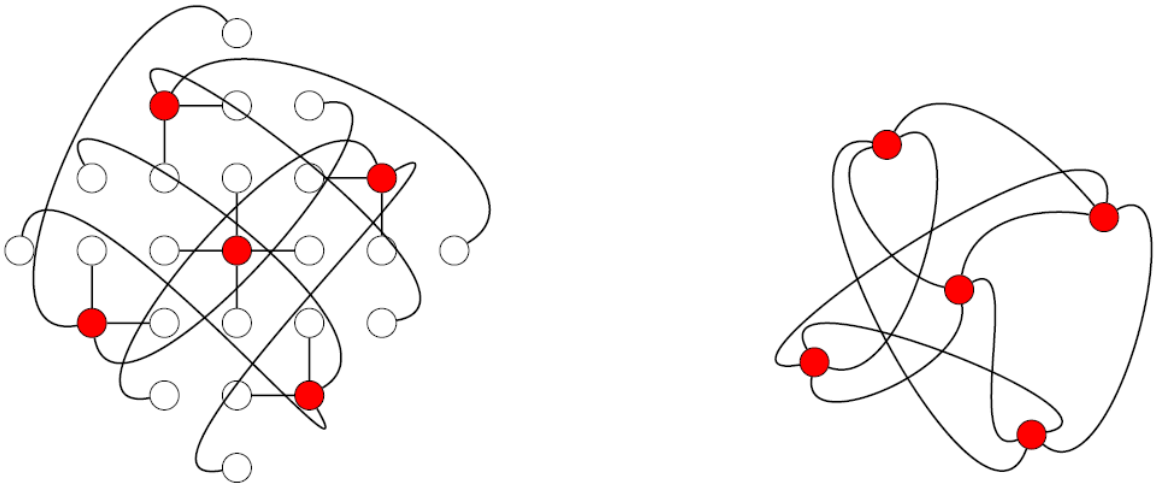

Figura 4.5: Código perfeito sobre $\mathbb{Z}[i]_{1-2i}$ e grafo quociente $\dfrac{G_{3+4i}}{1-2i}$

Definição 4.2.1. Um vértice η de $\mathcal{J}_\alpha$ é dito *t-dominar* o vértice $\beta \in \mathcal{J}_\alpha$, se $\beta \in B_t(\eta)$. Um subconjunto S de vértices é chamado *conjunto perfeito t-dominante* se cada vértice de $\mathcal{J}_\alpha$ é t-dominante de um único vértice em S.

Observação 4.2.1. Se S é um conjunto perfeito t-dominante, então $S+\beta \mod \alpha = \{\eta+\beta \mod \alpha \mid \eta \in S\}$ é também um conjunto perfeito t-dominante. Consequentemente , podemos supor que $0 \in S$.

Teorema 4.2.1. [27] Dado $0 \neq \alpha = a + b\omega \in \mathbb{Z}[\omega]$ e t um inteiro positivo.

(i) Se $\beta = t + (2t+1)\omega$ divide α, então o ideal $S = \langle\beta\rangle \subseteq \mathbb{Z}[\omega]_\alpha$ é um conjunto perfeito t-dominante em $\mathcal{J}_\alpha$.

(ii) Se $\bar{\beta} = (t+1) + (2t+1)\omega$ divide α , então o ideal $S = \langle\bar{\beta}\rangle = \langle\bar{\beta}\rangle \subseteq \mathbb{Z}[\omega]_\alpha$ é um conjunto perfeito t-dominante em $\mathcal{J}_\alpha$.

Demonstração. Vamos provar a primeira afirmação do Teorema. A segunda é provada de forma semelhante. O ideal $\langle\beta\rangle$ tem $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)}$ elementos, onde $\mathcal{N}(\beta) = 3t^2 + 3t + 1$. Primeiro vamos provar que $\beta = t + (2t+1)\omega$ é tal que $D_\alpha(\beta, 0) = 2t + 1$. Como $\beta \equiv (t+1)\omega + t(1+\omega) \mod \alpha$ e $|t+1|+|t| = 2t+1$, temos que $D_\alpha(\beta, 0) \leq 2t+1$. A seguir vamos mostrar que a distância é exatamente $2t+1$, caso contrário, a representação $\beta \equiv x+y\omega+z\omega^2 \mod \alpha$ implicaria $|x|+|y|+|z| \leq 2t$. Portanto, existe um $\eta \in \mathbb{Z}[\omega]$ tal que $\eta\beta = x+y\omega+z\omega^2 \in \mathbb{Z}[\omega]$. Como $\mathcal{N}(\beta) > 3t^2$ e $\mathcal{N}(x+y\omega+z\omega^2) \leq 24t^2$, obtemos $\mathcal{N}(\eta) < 8$. Agora, se $\eta = c+d\omega$ com $c, d \in \mathbb{Z}$, temos que $\eta\beta = (ct - d(2t+1)) + (c(2t+1) - d(t+1)\omega$ e, portanto

$$\begin{cases} x - z &= ct - d(2t+1) \\ y - z &= c(2t+1) - d(t+1) \end{cases}. \tag{4.2.1}$$

Logo,

$$\begin{cases} |x|+|z| &\geq |ct - d(2t+1)| \\ |y|+|z| &\geq |c(2t+1) - d(t+1)| \end{cases}. \tag{4.2.2}$$

Como $\mathcal{N}(\eta) \leq 7$, existem três casos diferentes a serem estudados

(i) Se $0 \leq |c| < |d|$, então $|x|+|y| \geq |ct - d(2t+1)| \geq |d||2t+1| > 2t$.

(ii) Se $0 \leq |d| < |c|$, então $|y|+|z| \geq |c(2t+1) - d(t+1)| \geq |c|(2t+1) > 2t$.

(iii) Se $0 \neq |c| = |d|$, temos duas possibilidades. Se $c = -d$, qualquer um dos casos anteriores produz $|x|+|z| > 2t$ ou $|y|+|z| > 2t$. Se $c = d$, da relação (4.2.1) temos $|x|+|y| \geq |c(t+1) + dt| = |2ct + c| = |c|(2t+1) > 2t$.
Em qualquer caso $|x|+|y|+|z| > 2t$, que é uma contradição.

Finalmente, vamos provar que todos os elementos do ideal $\langle\beta\rangle$ estão a uma distância maior ou igual a $2t+1$ um do outro. Assumindo o contrário, existe $\eta' \in \mathbb{Z}[\omega]$ tal que $D_\alpha(\eta'\beta, 0) < 2t+1$. Então, $\eta'\beta \equiv x + y\omega + z\omega^2 \mod \alpha$, com $|x|+|y|+|z| \leq 2t$. Logo, existe $\eta \in \mathbb{Z}[\omega]$ tal que $\eta\beta = x + y\omega + z\omega^2 \in \mathbb{Z}[\omega]$. Essa condição produz uma contradição, concluindo a prova.

■

Observação 4.2.2. Podemos observar que, dado $\beta = t+(2t+1)\omega$ ou $\beta = (t+1)+(2t+1)\omega$, sua norma $\mathcal{N}(\bar{\beta}) = 3t^2 + 3t + 1$ resulta no número de pontos da região de Voronoi, dada por hexágonos de raio t.

Exemplo 4.2.1. Como $\alpha_1 = (1+3\omega)^2 = -8 - 9\omega \in \mathbb{Z}[\omega]$, temos que $\beta = 1 + 3\omega$, divide $\alpha_1 = -8 - 9\omega$. Além disso, $\beta = 1 + 3\omega$ é da forma $\beta = t + (2t+1)\omega$, com $t = 1$. Logo, pelo Teorema 4.2.1, o ideal $S = \langle 1+3\omega\rangle = \{0, 1+3\omega, -3-2\omega, -2+\omega, 2-\omega, 3+2\omega, -1-3\omega\}$ é um conjunto perfeito 1-dominante em $\mathcal{J}_{-8-9\omega}$. Na Figura 4.6, representamos a constelação de sinal gerada por $\mathbb{Z}[\omega]_{-8-9\omega}$, onde os vértices destacados em negrito são os centros das bolas de raio $t = 1$.

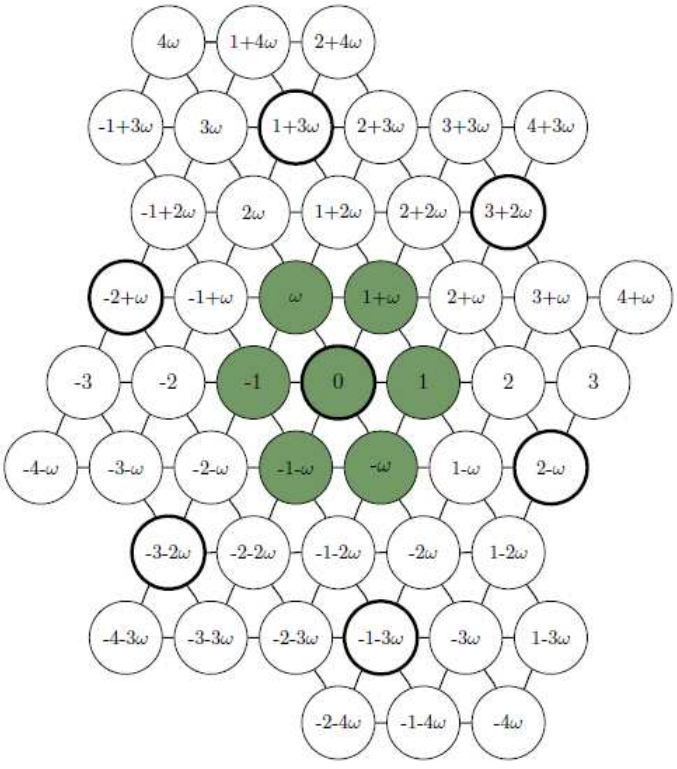

Figura 4.6: Conjunto Perfeito 1-dominante em $\mathcal{J}_{-8-9\omega}$

Exemplo 4.2.2. Seja $\alpha_2 = (1+2\omega)(2+5\omega) = -8-\omega$. Como $\beta = 2+5\omega$ é um divisor de $\alpha_2 = -8-\omega$ e é da forma $\beta = t+(2t+1)\omega$, com $t=2$, então pelo Teorema 4.2.1, o ideal $S = \langle 2+5\omega\rangle = \{-5-3\omega, 0, 5+3\omega\}$ é um conjunto perfeito 2-dominante do grafo $\mathcal{J}_{-8-\omega}$. Na Figura 4.7, representamos a constelação de sinal gerada por $\mathbb{Z}[\omega]_{-8-\omega}$, onde os vértices destacados em negrito são os centros das bolas de raio $t=2$.

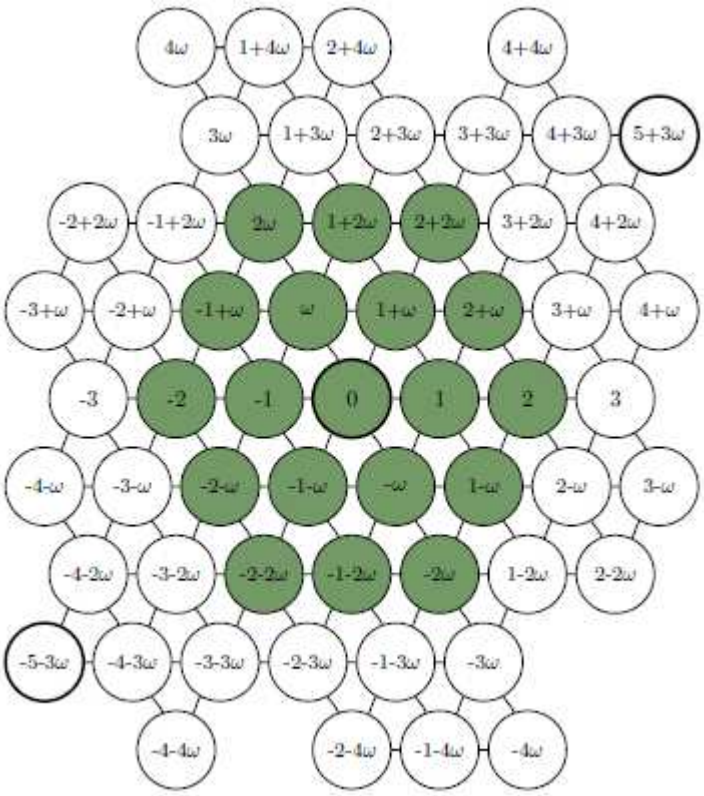

Figura 4.7: Conjunto Perfeito 2-dominante em $\mathcal{J}_{-8-\omega}$

Conjuntos perfeitos t-dominantes em grafos Eisenstein-Jacobi, geram códigos perfeitos em relação à distância do grafo associado, além disso, os conjuntos t-dominantes são ideais de $\mathbb{Z}[\omega]_\alpha$.

Definição 4.2.2. Para qualquer $\alpha = a+b\omega \in \mathbb{Z}[\omega]$, tal que $\beta = t+(2t+1)\omega$, definimos $\mathcal{C} = \langle\beta\rangle$, o ideal gerado por β, como um código perfeito sobre $\mathbb{Z}[\omega]_\alpha$ em relação a métrica D_α.

Para finalizar, apresentamos um exemplo de código perfeito 1-dominante sobre grafos de Eisenstein-Jacobi.

Exemplo 4.2.3. Dado $\alpha = -8-3\omega \in \mathbb{Z}[\omega]$, temos que $\mathcal{N}(\alpha) = 49$, e pelo Teorema 3.5.2, $\mathbb{Z}[\omega]_{-8-3\omega}$ tem 49 elementos. Como $\alpha = -8-3\omega = (1+3\omega)^2$ e fazendo $\beta = 1+3\omega$ pelo Teorema 4.2.1 segue que $\beta = 1+3\omega$ satisfaz condições estabelecidas, e portanto o ideal $\langle\beta\rangle = \langle 1+3\omega\rangle$ é um conjunto perfeito 1-dominante em $\mathbb{Z}[\omega]_{-8-3\omega}$. Então, o código perfeito que corrige todos os padrões com 1 erro e nenhum padrão com 2 ou mais erros, que pelo Corolário 3.5.1 possui $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)} = \dfrac{49}{7} = 7$ elementos, é dado por

$$S = \{0, 1+3\omega, -3-2\omega, -2+\omega, 2-\omega, 2-\omega, 3+2\omega, -1-3\omega\},$$

no qual é identificado no grafo pelos pontos cheios, formando os baricentros dos 7 polígonos fundamentais (contento 7 elementos cada) que recobrem a constelação hexagonal de sinais, contendo os 49 elementos de $\mathbb{Z}[\omega]_{-8-3\omega}$ como ilustrado na Figura 4.8.

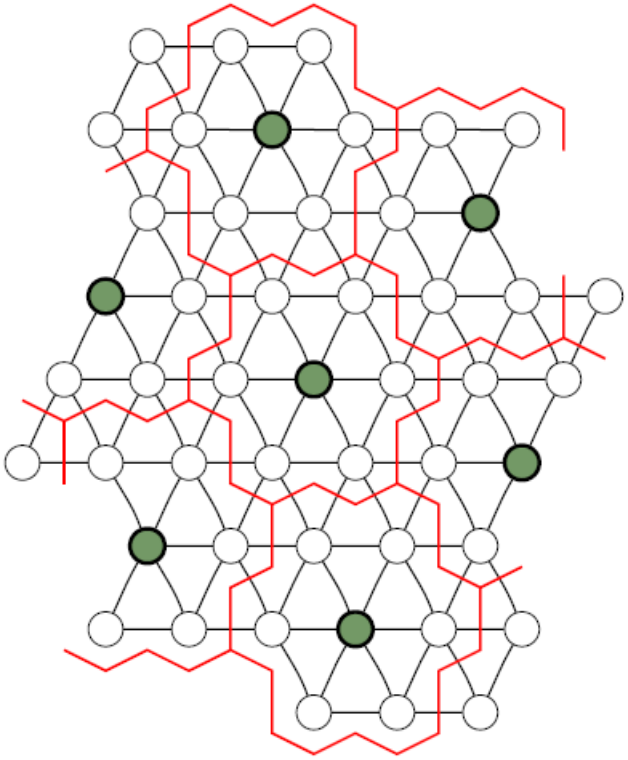

Figura 4.8: Código Perfeito 1-Corretor sobre $\mathbb{Z}[\omega]_{-8-3\omega}$

Conclusão

Este trabalho foi dedicado a construção de códigos perfeitos sobre grafos gaussianos e de Eisenstein-Jacobi, circulantes de grau quatro e seis respectivamente. Para essa construção realizou-se inicialmente um estudo envolvendo a teoria dos números, códigos e grafos, o qual forneceu os fundamentos básicos necessários para o seu desenvolvimento.

Para definir esses códigos é necessário a construção algébrica dos grafos gaussiano ($\mathcal{G}_\alpha$) e de Eisenstein-Jacobi ($\mathcal{J}_\alpha$), e para tal foi definido o anel quociente dos inteiros complexos $\mathbb{Z}[\rho]_\alpha$, onde $\rho = i$ ou $\rho = \dfrac{-1+\sqrt{-3}}{2}$ e a distância definida sobre eles D_α, onde verificou-se que é uma métrica. O conjunto de vértices e arestas desses grafos são dados por, $\mathcal{V} = \mathbb{Z}[\rho]_\alpha$ e $\mathcal{A} = \{(\beta,\gamma) \in \mathcal{V} \times \mathcal{V} \mid D_\alpha(\beta,\gamma) = 1\}$. Um subconjunto $\mathcal{C}$ não vazio de $\mathcal{G}_\alpha$ ou $\mathcal{J}_\alpha$ é definido como um código sobre os grafos gaussianos e de Eisenstein-Jacobi.

Vimos que um código $\mathcal{C}$ é chamado perfeito se as bolas de raio t centradas nos pontos de $\mathcal{C}$ particionam $\mathcal{V}$, ou seja, é um código que corrige todos os padrões com até t erros e nenhum padrão com $t+1$ erros ou mais. Além disso, um subconjunto de vértices S é dito conjunto perfeito t-dominante se cada vértice de $\mathcal{G}_\alpha$ ou $\mathcal{J}_\alpha$ é t-dominar de um único vértice em S. Dessa forma, neste trabalho foi apresentada a construção de códigos perfeitos a partir de conjuntos t-dominantes de $\mathcal{G}_\alpha$ ou $\mathcal{J}_\alpha$. Destacamos, as construções dos Exemplos 4.1.3, 4.1.4 onde apresentamos as constelações de sinais, destacando as palavras-código de códigos perfeitos 1 e 2-dominante, respectivamente, via grafos gaussianos. E também, as construções do Exemplo 4.2.3, onde apresentamos a constelação de sinal, detacando as palavras-código do código perfeito 1-dominante via grafos de Eisenstein-Jacobi.

Existem muitos trabalhos sendo desenvolvidos nesta linha de pesquisa, por exemplo [24],[29],[11],[27],[25],[32]. Ainda há muito a ser explorado, principalmente nos códigos sobre grafos de Eisenstein-Jacobi, onde existem pouca literatura disponível.

Como perspectivas futuras a partir deste trabalho podemos projetar diferentes grupos de códigos perfeitos , tais como, código perfeito para a métrica de Lee. Podemos também gerar códigos quase-perfeitos derivados de grafos sobre anéis dos inteiros, que são capazes de corrigir mais padrões de erros que os códigos perfeitos com menor cardinalidade. E a construção de códigos geometricamente uniformes derivados de grafos sobre anéis quocientes de inteiros.

Referências Bibliográficas

[1] DOMINGUES, H, H., IEZZI, G. ; Álgebra Moderna. São Paulo: Atual, 1982

[2] GARCIA, A., LEQUAIN, I. ; álgebra: um curso de introdução. Rio de Janeiro, Instituto de Matemática Pura e Aplicada,1988

[3] HEFEZ, A. ; Curso de Álgebra, Volume 1. Rio de Janeiro, Instituto de Matemática Pura e Aplicada,CNPq, 1993.

[4] HEFEZ, A., VILLELA, M.L.T. ; Códigos Corretores de Erros. Rio de Janeiro, IMPA, 2008

[5] LAVOR, C.; Uma introdução à Teoria de Códigos. São Carlos, SP: SBMAC, 2006

[6] BOAVENTURA, P.O., SAMUEL, J.; Grafos: Introdução e prática. São Paulo: Editora Blucher, 2009

[7] BOLDRINI, J.L., ... [et al.].; Álgebra Linear. 3.ed. São Paulo: Harper & Row do Brasil, 1980

[8] LIMA, E. L. ; Álgebra Linear. Instituto de Matemática Pura e Aplicada, CNPq,1995 Rio de Janeiro

[9] BENEDITO, C.W.O. ; Construção de grupos fuchsianos aritméticos provenientes de álgebras dos quatérnios e ordens maximais dos quatérnios associados a reticulados hipérbólicos. Campinas, SP:[s.n.],2014

[10] DUTRA, E.; Construções do reticulado E8 via teoria algébrica dos números, álgebra dos quatérnios e álgebra dos octônios. Campinas, SP:[s.n], 2016

[11] QUEIROZ, C.R.O.Q. ; Códigos geometricamente uniformes derivados de grafos sobre anéis quocientes de inteiros e de ordens dos quartérnios. Campinas, [S.P.:s.n],2011

[12] LIMA, E. L. ; Espaços métricos. Rio de Janeiro,Instituto de Matemática Pura e Aplicada, CNPq,1977

[13] STEWART, I.N., TALL, D.; Algebric number theory. London: Chapman and Hall,1987

[14] SAMUEL, P.; Algebric theory of Numbers. Paris:Hermann, 1970

[15] GONÇALVES, A.; introdução à ágebra. Rio de Janeiro: IMPA,2011

[16] BERLEKAMP, E. R.; Algebraic Coding Theory. Aegean Park Press, 1984

[17] MIYAMOTO, G.A.; Códigos de Subespaço geometricamente uniformes. Campinas, SP:[s.n.],2015

[18] HAMMING, R.W.; Error Detecting and Error Correcting Codes. The Bell Systems Technical Journal, vol. XXIX,$n°2$, April, 1950

[19] SHANNON, C.E.; A mathematical Theory of Communication. Bell System Technical Journal,vol.27,pp.379-423,July,1948

[20] FORNEY, J.G.D.; Geometrically Uniform Codes. IEEE Trans. inf. Theory, v.37 no. 5, p.1241-1260,Sep. 1991

[21] SLEPIAN, D.; Group Codes for the Gaussian Channel. Bell Sys. Tech. Journal, vol. 37, 1968,p. 575-602.

[22] MILIES, F.C.P.; Anéis e módulos. São Paulo:L.P.M,1972

[23] OTTO, E.; Teoria dos números algébricos. Rio de Janeiro:IMPA,2014

[24] MARTINEZ, C., BEIVIDE, R., GABIDULIN,E.; Perfecto codes from metrics induces by circulant graphs. IEEE Trans. on Inform. Theory,vol.53 No.53 No.9,pp.3042-3052, September 2007

[25] COSTA, S.I.R., MUNIZ, M., AGUSTIN, E., PALAZZO,R.; Graphs,Tessellations,and Perfect Codes on Flat Tori. IEEE Trans. Inform. Theory,vol.50(10):2363-2377,2004

[26] STRAPASON, J.E.; Geometria Discreta e Códigos. Campinas,[S.P.:s.n],2005

[27] MARTINEZ, C., STAFFORD, E., BEIVIDE, R., GABIDULIN, E.; Modeling Hexagonal Constellations with Eisenstein-Jacobi Graphs. Problems of Information Transmission, Vol 44. No.1,pp.1-11,2008

[28] ALENCAR, F. E.; Teoria das Congruências. São Paulo,1986

[29] MARTINEZ, C.; Códigos y Grafos sobre Anillos de Enteros Complejos. Santander: Enero 2007

[30] HUNGERFORD, T.W.; Algebra. Springer - Verlag New York Inc. 1974

[31] MARTINEZ, C., MORETÓ, M., BEIVIDE, R., GABIDULIN,E.; A Generalization of Perfect Lee Codes over Gaussian Integers. 1-4244-0504-1/06 ©2006 IEEE.

[32] HUBER, K.; Codes over Gaussian integers. IEEE Trans. Inform. Theory,vol.40(1):207-216,1994

[33] SILVA, A. T.; Construções de códigos binários a reticulados e códigos esféricos. Campinas, SP:[s.n], 2007