UNIVERSIDADE DA BEIRA INTERIOR
Faculdade de Ciências

Os Grafos dos Divisores de Zero de um Anel

Versão final após defesa

Paulino Gregório Armando Kuebo

Dissertação para obtenção do Grau de Mestre em
Matemática para Professores
(2º ciclo de estudos)

Orientador: Prof. Doutor Celino José Martins Miguel

Covilhã, Julho de 2018

Dedicatória

Dedico este trabalho em especial, a minha família, ao meu orientador, aos meus colegas de formação, à todos quanto contribuíram para que este trabalho fosse concluído.
Aos meus familiares que mesmo distante souberam compreender este momento.

Agradecimentos

Agradeço à Deus todo poderoso, pela força e determinação dos objetivos.

Ao meu Orientador, Professor Doutor Celino José Martins Miguel, pelo tema que foi-me proposto, pela ajuda, pelo tempo cedido que mesmo diante das suas ocupações sempre teve paciência em orientar-me.

À minha família pela paciência que sempre tiveram durante este período de formação.

Ao meu querido filho, Patrício Pemba Kuebo, que mesmo distante dele soube compreender-me.

Aos meus colegas, Dr. Afonso Júnior, Lic. Joaquim Dongo Kosi, Lic. Fernando Angelino Policarpo, Lic. João Nenkamba, Lic. José Massanga, Lic. Luís Mbundo, Lic. Gonçalo Carlota, Lic. Salviano Costa, Lic. Sebastião Lukeba, Lic. Mamana Combo que sempre deram-me forças e pelo encorajamento dos momentos mais difíceis da minha formação.

Aos meus familiares, Isabel António Pemba, Manuela Maria, Mateus Mendes, Gregório Lau Kuebo, Paulina Armando Maria, Paulo Kuebo, Imaculada Mendes, Domingos Mendes, Olga Chipeca, e tantos outros, pelas palavras de apoio e consolo.

À todos os Professores da Universidade da Beira Interior em particular, os Professores do Departamento de Matemática, pelo apoio dado desde a nossa chegada cá em Portugal e não só pelo enquadramento das diversas temáticas abordadas no decorrer da nossa formação.

À Escola Superior Politécnica do Zaire/Soyo, em nome do Coordenador MsC. Jerónimo Pio Aida, e de todos os Professores desta mesma instituição o meu muito obrigado.

À Reitoria da Universidade 11 de Novembro, pelo fato de ser selecionado para o Plano de Formação de Quadros de Angola.

Resumo

Neste trabalho estudamos os grafos de divisores de zero para anéis. Trataremos de forma mais exaustiva os anéis comutativos, uma vez que para estes anéis existe um conjunto de resultados mais abrangente. No entanto no último capítulo apresentamos alguns breves resultados para anéis não comutativos. Neste caso em vez de um grafo simples, temos um grafo dirigido. No trabalho damos especial atenção ao anel dos inteiros de Gauss módulo n, fazendo um estudo bastante completo do grafo divisor de zero para este anel.

Palavras Chave:

Anel, grafo, divisor de zero, diâmetro, cintura, número cromático, clique, inteiros de Gauss, grafo de linha.

Abstract

In this work we study zero-divisors graphs of rings. We will deal more exhaustively with the commutative rings, since for these rings there is a more comprehensive set of results. However in the last chapter we present some brief results for noncommutative rings. In this case instead of a simple graph, we have a directed graph. In the work we give special attention to the ring of the integers of Gauss modulo n, making a fairly complete study of the zero-divisor graph for this ring.

Keywords:

Ring, graph, zero-divisor, diameter, girth, chromatic number, click, Gaussian integers, line graph.

Lista de Símbolos

$Z[i]$-	Anel dos inteiros de Gauss
$U(R)$-	Grupo das unidades do anel R
$V(G) -$	Conjunto de vértices do grafo G
$E(G)$-	Conjunto de arestas do grafo G
$d_G(v)$ ou $deg(v)$-	Grau do vértice v
$\tau(R)$-	Grafo dos divisores de zero do anel R
$g(G)$-	Cintura do grafo G
$diam(G)$-	Diâmetro do grafo G
$r(G)$ ou $rad(G)$-	Raio do grafo G
$e(G)$-	excentricidade do grafo G
$Z(R)$-	Conjunto dos divisores de zero do anel R
F_q-	Corpo Finito com q elementos
Z_n-	Anel de inteiros módulo n
$K^{m,n}$ ou $K_{m,n}$-	Grafo bipartido Completo
$ann(x)$-	Anulador de x
$\langle n \rangle$-	Ideal principal gerado por n
$Z_n[i]$-	Anel dos inteiros Gaussianos modulo n
$\gamma(G)$-	Número de Dominação do grafo G
K_n-	Grafo Completo de n vértices
$c(G)$-	Número de componentes do grafo G
$L(G)$-	Grafo de Linha do grafo G
$\chi(G)$-	Número Cromático do grafo G

$\omega(G)$- Clique do grafo G

$M_n(R)$- Anel das matrizes de ordem n e de elementos no anel R

N- Números naturais

Z - Anel dos inteiros racionais

Q- Corpo dos racionais

R- Números reais

$R[X]$- Anel de polinómios na indeterminada x e com coeficientes em R

Índice

Introdução

O presente trabalho está composto por 5 capítulos, no qual alguns temas foram estudados taxativamente no nosso trabalho, e outros podem ser para futuras investigações acerca do tema em causa. Neste trabalho falaremos mais sobre anéis comutativos e seus grafos de divisores de zero. No entanto no último capítulo falaremos sobre anéis não comutativos e respectivos grafos de divisores de zero.

O estudos dos anéis originou-se na teoria de polinómios e da teoria de inteiros algébricos. O termo anel (Zahliring) foi criado por David Hilbert em 1897 em $[30]$.

Em 1921, Emmy Noether, criou a primeira fundação axiomática da teoria de anéis comutativos em $[30]$.

Além de ser uma teoria linda e profunda por direito próprio, a teoria dos anéis comutativos é importante como base para muitos ramos da matemática.

Muitos dos problemas do mundo real podem descrever-se (definir-se) na linguagem dos grafos, ou seja, por intermédio de uma figura que consiste num conjunto de pontos e um conjunto de linhas que ligam alguns pares de pontos. Mais geralmente uma relação binária R definida sobre um conjunto V, pode representar-se graficamente, por um conjunto de pontos que corresponde ao conjunto V e por um conjunto de arcos (ou linhas não orientadas, no caso da relação R ser simétrica) que ligam pares de pontos $x, y \in V$ tais que xRy. Este modo de representação regista e torna evidente muitas propriedades que, por vezes, não são fáceis de detectar ou explicar de outro modo.

A teoria dos grafos é um ramo da Matemática que estuda as relações entre objetos de um determinado conjunto. Para tal são empregados estruturas chamados de Grafos $G(V,E)$, onde V é um conjunto não vazio de objetos denominados vértices e E é um subconjunto de pares não ordenados de V chamados arestas.

A idéia de grafo de divisor de zero de um anel comutativo foi introduzida por I. Beck em [10], onde ele estava principalmente interessado em coloração. Esta investigação das colorações de um anel comutativo foi então continuada por D. Anderson e M. Naseer em [5]. Sua definição era ligeiramente diferente da nossa; Eles deixaram todos os elementos de R ser vértices e fizeram $x\ e\ y$ distintos adjacentes se e somente se $xy = 0$. Denotamos seu grafo de divisor de zero de R por $\tau_0(R)$. Nossos resultados para $\tau(R)$ têm análogos naturais a $\tau_0(R)$; No entanto, sentimos que a nossa definição ilustra melhor a estrutura divisor de zero de R.

CAPÍTULO 1

BREVES NOÇÕES SOBRE ANÉIS.

Neste capítulo expomos alguns conceitos da Teoria de Anéis. Procurámos não ser exaustivos, limitámo-nos aos princípios básicos e algumas noções necessárias para o resto do trabalho. Daremos especial ênfase aos anéis comutativos bem como ao anel dos inteiros de Gauss, uma vez que é para estes anéis que faremos grande parte do estudo do grafo divisor de zero.

1.1 Noções Históricas.

A álgebra comutativa é essencialmente o estudo dos anéis que ocorrem na teoria dos números algébricos e geometria algébrica.

O assunto, conhecido pela primeira vez como teoria ideal, começou com o trabalho de Richard Dedekind, baseado em trabalhos anteriores de Ernst Kummer e Leopold Kronecker. Mais tarde, David Hilbert apresentou o termo anel para generalizar os trabalhos anteriores. Hilbert introduziu uma abordagem mais abstrata para substituir os métodos mais concretos e computacionalmente, fundamentados em coisas como análise complexa e teoria invariante clássica. Por sua vez, Hilbert influenciou fortemente Emmy Noether, que reformulou muitos resultados anteriores em termos de uma condição de cadeia ascendente, agora conhecida como a condição de Noetheriano. Outro marco importante foi o trabalho do estudante de Hilbert, Emanuel Lasker, que introduziu ideais primários e provou a primeira versão do teorema Lasker-Noether.

A figura principal responsável pelo nascimento da álgebra comutativa como sujeito maduro foi Wolfgang Krull, que introduziu as noções fundamentais de localização de um anel, bem como a dos anéis locais regulares. Ele estabeleceu o conceito da dimensão Krull de um anel, primeiro para os anéis de Noetheriano antes de avançar para expandir sua teoria para cobrir anéis de valoração geral e anéis de Krull. Esses resultados prepararam o caminho para a introdução da álgebra comutativa em geometria algébrica, uma idéia que revolucionaria o último assunto.

Grande parte do desenvolvimento moderno da álgebra comutativa enfatiza os módulos. Ambos os ideais de um anel R e álgebras R são casos especiais de módulos R, de modo que a teoria dos módulos engloba a teoria ideal e a teoria das extensões de anel. Embora já tenha sido incipiente no trabalho de Kronecker, a abordagem moderna da álgebra comutativa usando a teoria dos módulos geralmente é creditada a Krull e Noether.

Os Inteiros de Gauss.

O Matemático alemão Carl F. Gauss produziu em todos os ramos da matemática. Mas sabe-se que sentia especial prazer pela investigação em Aritmética. Foi ele quem lançou os fundamentos da moderna Teoria dos Números em sua monumental obra "Disquisitiones Arithmeticae" que contém grandes contribuições à Aritmética e à Álgebra, publicada em 1801. Os inteiros de Gauss ou conjunto dos Inteiros Gaussianos são números complexos da forma $a + bi$, onde $a\ e\ b$ são inteiros e $i = \sqrt{-1}$. O conjunto $Z[i]$ dos inteiros de Gauss surgiu entre os anos de 1808 e 1825, época em que o matemático Carl F. Gauss investigava a reciprocidade cúbica $(x^3 \equiv q\ (mod\ p)$, onde $p\ e\ q\ são\ primos)$ e também a reciprocidade biquadrática $(x^4 \equiv q\ (mod\ p)$, onde $p\ e\ q$ são primos). Gauss percebeu que essa investigação se tornava mais fácil trabalhando em $Z[i]$, o anel dos Inteiros de Gauss.

Desse modo, Gauss estendeu a ideia de Número Inteiro quando definiu $Z[i]$, pois descobriu que muito da antiga teoria de Euclides sobre factoração de inteiros poderia ser transportada para esse conjunto com consequências importantes para a Teoria dos Números.

Gauss desenvolveu uma Teoria de Factorização em primos para esses números Complexos e demonstrou que essa decomposição em primos é única, tal qual no Conjunto dos Números Inteiros. O uso desse estudo foi de fundamental importância para a demonstração do Último Teorema de Fermat.

O desenvolvimento da Teoria dos Números Algébricos foi, em parte, em função das tentativas de solução da equação diofantina, também conhecida como equação de Fermat

$$x^n + y^n = z^n$$

pois os inteiros algébricos aparecem de maneira natural, como ferramenta para tratar desse assunto.

Essa generalização do Conjunto dos Números Inteiros dá exemplos especiais de desenvolvimento muito mais profundos que chamamos de Teoria dos Números Algébricos. Essa teoria é profunda e poderosa. Além do interesse e fascínio que exerce por suas próprias propriedades, fornece muitas aplicações à Teoria dos Números que permitem uma compreensão de vários fenômenos antes obscuros e misteriosos.

1.2 Conceitos Fundamentais da Teoria de Anéis.

Definição 1.2.1: Um anel é um conjunto A≠ ∅ cujos elementos podem ser adicionados e multiplicados. Um anel designa-se por $(\boldsymbol{A}, +, \cdot)$ isto é, são dadas duas operações $(x, y) \rightarrow x + y$ **e** $(x, y) \rightarrow x \cdot y$ aos pares de elementos de $A\ em\ A$ satisfazendo as seguintes condições:

1. Para todo $x\ e\ y \in A$ temos a comutatividade da soma, a saber

$$x + y = y + x$$

2. Para todo $x\, e\, y \in A$ temos a associatividade da soma, a saber,

$$(x + y) + z = x + (y + z)$$

3. Existe um elemento e em A tal que $x + e = x$ para todo $x \in A$.

Note: $e = 0$. Este é chamado elemento neutro da adição.

4. Para todo elemento $x \in A$ existe um elemento $y\, em\, A$ tal que $x + y = 0$.

Note: $y = -x$. Este é também chamado de simétrico de x.

5. Para todo $x, y, z \in A$ temos a associatividade da multiplicação, a saber

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

6. Para todo $x, y, z \in A$ temos a distributividade da multiplicação à direita e esquerda, a saber.

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad e \quad (y + z) \cdot x = y \cdot x + z \cdot x$$

Observações:

1) Observe que a multiplicação não necessita ser comutativa. Quando isto ocorrer, dizemos que A é um anel comutativo.

2) Um anel não necessita ter elemento neutro da multiplicação (isto é, um elemento y tal que $x \cdot y = y \cdot x = x$ *para todo* $x \in A$). Este elemento se existir é chamado de identidade do anel e denotado por 1. Quando um anel A possui o elemento neutro da multiplicação dizemos que A é um anel com identidade.

3) Os elementos não nulos de um anel com identidade não necessitam ter inversos multiplicativos (isto é, y é inverso multiplicativo de *x* se e somente se $x \cdot y = y \cdot x = 1$). Os elementos de um anel A que possuem inverso multiplicativo são chamados de invertíveis de A ou unidades de A.

Usaremos a notação $U(A) = \{x \in A | \, x \text{ é } uma\ unidade\ de\ A\}$.

Definição 1.2.2: Um elemento $a \neq 0$ de um anel A diz-se divisor de zero à esquerda e um divisor de zero à direita se existe um elemento $b \in A$ com $b \neq 0$ tal que $ab = 0\, e\, ba = 0$, respectivamente.

Definição 1.2.3: Seja ***(A,***$+,\cdot$) um anel e seja *B* um subconjunto não vazio de *A*. Então *B* é um subanel de *A* se, e só se, $\forall x, y \in B$ $são\ satisfeita\ as\ condições$:

I. $x - y \in B$
II. $x \cdot y \in B$

Exemplos: O conjunto $B = \{0, 3, 6\}$ é um subanel de $(Z_{12}, +, \cdot)$.

$$B = \{0, 3, 6\}$$

O conjunto $B = Z\sqrt{3} = \left\{a + b\sqrt{3}\,, a, b \in Z\right\}$ é um subanel do anel $(R, +, \cdot)$: R são os números reais.

Note que:

$$x - y, \qquad x \cdot y \in Z\sqrt{3}, \forall x, y \in Z\sqrt{3}$$

$$x \in Z\sqrt{3}: x = a + b\sqrt{3}; a, b \in Z$$

$$y \in Z\sqrt{3}: y = c + d\sqrt{3}; c, d \in Z$$

$$x \cdot y = \left(a + b\sqrt{3}\right) \cdot \left(c + d\sqrt{3}\right) = (ac + 3bd) + (ad + bc)\sqrt{3}$$

Portanto $x \cdot y \in Z\sqrt{3}$

$$x - y = \left(a + b\sqrt{3}\right) - \left(c + d\sqrt{3}\right) = (a - c) + (b - d)\sqrt{3}$$

Portanto $x - y \in Z\sqrt{3}$. Logo $Z\sqrt{3}$ é $um\ subanel\ de\ (R, +, \cdot)$

Definição 1.2.4: Seja ***(A,***$+,\cdot$) um anel. Um subanel $I \subset A$ é um ideal de A, se para cada $a \in A$ e para cada $x \in I, temos$:

$$a \cdot x \in I\ e\ x \cdot a \in I.$$

Observação: *Um anel possui pelo menos dois ideais, ele próprio e o ideal formado pelo zero do anel*.

Exemplo: O subanel $\{0,2\}$, é um ideal do anel $\langle Z_4, +, \cdot\rangle$.

De facto:

$$I = \{0,2\} \subset \langle Z_4, +, \cdot\rangle, \forall x \in I, \forall a \in Z_4: x \cdot a \in I, Z_4 = \{0,1,2,3\}$$

$$x = 0 \to 0 \cdot 0 = 0 \in I$$

$$0 \cdot 1 = 0 \in I$$

$$0 \cdot 2 = 0 \in I$$

$$0 \cdot 3 = 0 \in I$$

$$x = 2 \to 2 \cdot 0 = 0 \in I$$

$$2 \cdot 1 = 2 \in I$$

$$2 \cdot 2 = 0 \in I$$

$$2 \cdot 3 = 2 \in I. Logo, \{0,2\} \text{ é } um\ ideal\ de \langle Z_4, +, \cdot \rangle$$

O conjunto Q é um subanel de R, mas não é um ideal de R.

É evidente que Q subanel de R. Agora note que

$$x = 2 \in Q\ e\ a = \sqrt{2} \in R, logo\ x \cdot a = 2\sqrt{2} \notin Q, logo\ (Q, +, \cdot)\ não\ é\ ideal\ de\ R.$$

O conjunto: $\langle 2 \rangle = 2Z = \{2m, m \in Z\}$ $é\ um\ ideal\ do\ anel\ (Z, +, \cdot)$.

$$\forall x \in 2Z, \forall a \in Z: x \cdot a \in Z$$

$$x \in 2Z: x = 2m, m \in Z$$

$x \cdot a = 2m \cdot a = 2(m \cdot a) \to x \cdot a = 2ma, portanto, \langle 2 \rangle$ é $um\ ideal\ de\ 2Z$.

O conjunto $M_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}; a, b, c, d \in R \right\}, A = \langle M_2, +, \times \rangle$ é um anel não comutativo e com unidade.

O conjunto $B = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, a, b \in R \right\}$ é um subanel de *A*. *R* são os números reais. Mas B não é um ideal de A.

Uma classe importante de anéis é apresentada na seguinte definição.

Definição 1.2.5: Um inteiro de gauss é um número complexo da forma $a + bi$ com $a\ e\ b$ inteiros, cujo conjunto denotamos por $Z[i]$.

Propriedades.

O anel dos inteiros de Gauss tem as seguintes propriedades:

- ✓ Os elementos invertíveis são $1, i, -1\ e\ -i$.
- ✓ Dois inteiros gaussianos z e w dizem-se associados se e só se z=wu para alguma unidade u.
- ✓ Um inteiro gaussiano diz-se primo se for não unidade e for divisível apenas pelos seus associados e pelas unidades.
- ✓ É um Domínio Fatorial, ou seja, todo elemento tem factorização única num produto de gaussianos primos (a menos de elementos invertíveis). Note-se que alguns números primos no anel dos inteiros são compostos nos inteiros de Gauss, por exemplo $5 = (2+i)\,(2-i)$. Os inteiros de Gauss que não podem ser expressos por produto de outros dois inteiros Gaussianos de módulo maior que 1 são chamados de primos de Gauss.
- ✓ Pode se tornar um domínio euclidiano com a norma $N(a\ +\ b\ i)\ =\ a^2\ +\ b^2$.

Anéis Quocientes.

Definição 1.2.6: Seja R um anel e I um ideal de R. Defina em R uma relação de equivalência de forma que $x \sim y$ se e só se $x - y$ é um elemento de I. Para o elemento x a sua classe de equivalência é

$[x] = x\ +\ I$. Se no conjunto das classes de equivalência for definida uma adição por $(x+I) + (y+I) = (x+y)+I$ e uma multiplicação por $(x+I)(y+I)\ =\ xy\ +\ I$ obtemos um anel que é chamado anel quociente de R por I e denotado por R/I.

Definição 1.2.7: Todo anel comutativo com identidade $1 \neq 0$ e sem divisores de zero é chamado domínio de integridade.

Teorema 1.2.8: O conjunto dos Inteiros de Gauss é um Domínio de integridade. Em [29]

Demonstração: Com efeito, $0\ =\ 0\ +\ 0i\ \in Z[i]$. Como $1 = 1\ +\ 0i$, então $1 \in Z[i]$.
Sejam $z\ =\ a + bi$ e $w\ =\ c + di$ dois Inteiros de Gauss, isto é, $a;\ b;\ c;\ d\ \in Z$, então $z - w$ e $z \cdot w$ também são Inteiros de Gauss pois

$$z - w = (a - c) + (b - d)i,$$

$$z \cdot w = (ac - bd) + (ad + bc)i,$$

$$w \cdot z = (ca - db) + (da + cb)i = (ac - bd) + (ad + bc)i = z \cdot w$$

Onde $(a-c), (b-d), (ac-bd)\ e\ (ad+cb)$ são inteiros. Logo $Z[i]$ é um anel comutativo com identidade. Além disso.

$$z \cdot w = 0 \rightarrow |z \cdot w| = 0$$

$$|z| \cdot |w| = 0 \rightarrow |z| = 0\ ou\ |w| = 0$$

$$|z| = 0 \leftrightarrow z = 0\ e$$

$$|z| = \sqrt{a^2 + b^2} \quad \blacksquare$$

Os inteiros Gaussianos $Z[i]$ são a generalização mais simples do comum inteiros Z e eles se comportam da mesma maneira. Em particular, $Z[i]$ goza de factorização única, ou seja todo o inteiro gaussiano de pode factorizar num produto de gaussianos primos de forma única (a menos de multiplicação por unidades) e isso nos permite trabalhar sobre $Z[i]$ da mesma maneira que fazemos sobre Z. Fazemos isso porque $Z[i]$ é o lugar natural para estudar certas propriedades de Z. Em particular, é o melhor lugar para examinar somas de dois quadrados, porque em $Z[i]$ podemos factorizar uma soma de dois quadrados inteiros em fatores lineares:

$$x^2 + y^2 = (x - yi)(x + yi).$$

***Z*[*i*] e sua norma**.

Definiremos também uma função muito importante na aritmética desse conjunto que é chamada de Norma, onde:

Definição 1.2.9: Para $z = a + bi \in Z[i]$, a Norma é o produto

$$N(z) = z\bar{z} = (a + bi)(a - bi) = a^2 + b^2:$$

Pensando em $a + bi$ como um número complexo, sua Norma é o quadrado de seu

módulo.

$$|a + bi| = \sqrt{a^2 + b^2}, N(a + bi) = a^2 + b^2 = |a + bi|^2$$

A razão pela qual preferem lidar com Normas em $Z[i]$ em vez de valores absolutos é que as Normas são inteiros (em vez de raízes quadradas) e as propriedades de divisibilidade em Z vão fornecer informações importantes sobre as propriedades de divisibilidade em $Z[i]$. Isto é baseado na seguinte propriedade algébrica da Norma. Em [29]

Teorema 1.2.10: A Norma é multiplicativa, ou seja, $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$.

Demonstração: Fazendo $z = a + bi\ e\ w = c + di$. Então $z \cdot w = (a + bi) \cdot (c + di)$.

Então temos:

$$N(z)N(w) = (a^2 + b^2)(c^2 + d^2) = (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2 \qquad (1)$$

$$N(zw) = (ac - bd)^2 + (ad + bc)^2$$

$$= (ac)^2 - 2acbd + (bd)^2 + (ad)^2 + 2adbc + (bc)^2$$

$$= (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2 \qquad (2)$$

Verificamos que 1 e 2 tem o mesmo resultados, logo

$$N(zw) = N(z)N(w) \quad \blacksquare$$

Determinaremos a seguir os inteiros de Gauss que tem inversos multiplicativos em $Z[i]$.

Divisibilidade e primos em $Z[i]$ *e* Z

$$N(a + bi) = |a + bi|^2 = a^2 + b^2$$

é mais útil na teoria dos números do que o valor absoluto porque a norma é sempre um número inteiro comum. A propriedade multiplicativa da norma implica que, se um inteiro Gaussiano α divide um inteiro Gaussiano γ, isto é, se

$$\gamma = \alpha\beta \; para \; algum \; \beta \in Z \; [i],$$

Então

$$N(\gamma) = N(\alpha)N(\beta),$$

isto é, a $N(\alpha) \; divide \; a \; N(\gamma)$.

Por isso, as questões sobre divisibilidade em $Z[i]$ geralmente se reduzem a questões sobre divisibilidade em Z.

Teorema 1.2.11: ***Factorização prima em*** $Z[i]$. Qualquer inteiro Gaussiano não nulo e não unidade é factorizado em um produto de Gaussianos primos. A prova é semelhante à prova em Z. Em [29]

Demonstração*:* Considere qualquer inteiro Gaussiano γ. Se γ em si é um primo Gaussiano, então terminamos. Se não, então $\gamma = \alpha\beta$ para alguns $\alpha, \beta \in Z[i]$ com menor norma. Se α, β não são ambos primos Gaussianos, factorizamos em Gaussiano inteiros de norma ainda menor, e assim por diante. Esse processo deve terminar desde as normas, sendo números naturais, não podem diminuir para sempre. Por conseguinte, eventualmente obter uma factorização prima Gaussiana de γ. ■

Como em Z, não é imediatamente claro que a factorização prima é única. No entanto, vemos nesta secção que a factorização prima única detém em $Z[i]$ pelas mesmas razões que em Z.

Conjugados.

O conjugado de $z = a + bi$ é $\bar{z} = a - bi$. As propriedades básicas da conjugação

(não apenas em $Z[i]$, mas para todos os números complexos z) são

i. $z\bar{z} = |z|^2$,
ii. $\overline{z_1 + z_2} = \bar{z_1} + \bar{z_2}$,
iii. $\overline{z_1 - z_2} = \bar{z_1} - \bar{z_2}$,
iv. $\overline{z_1 \times z_2} = \bar{z_1} \times \bar{z_2}$.

Estes podem ser verificados escrevendo $z_1 = a_1 + b_1 i, z_2 = a_2 + b_2 i$ e trabalhando ambos os lados de cada identidade. Usamos essas propriedades de conjugação para que dê o primeiro passo para uma classificação de primos Gaussianos.

Teorema 1.2.12: ***Primos Gaussianos Reais***. Um primo comum $p \in N$ é um primo Gaussiano $\Leftrightarrow p$ não é a soma de dois quadrados. (E obviamente $p < 0$ é um primo Gaussiano $\Leftrightarrow -p \in N$ é um primo Gaussiano). Em [29]

Demonstração: ($\Leftarrow$) Suponhamos que tenhamos um p primo comum que não é um primo Gaussiano, de modo que se divide em $Z\,[i]$:

$$p = (a + bi)\,\gamma,$$

onde $a + bi\, e\, \gamma$ são números inteiros Gaussianos com $N(a + bi) < p^2$ e $N(\gamma) < p^2$ e também $N(a + bi) > 1 \;\; e\, N(\gamma) > 1$. Tomando conjugados de ambos os lados, obtemos

$$p = (a - bi)\,\bar{\gamma},$$

uma vez que p é $real$ e, portanto, $p = \bar{p}$. Multiplicando estas duas expressões para p dá

$$p^2 = (a - bi)\,(a + bi)\,\gamma\bar{\gamma}$$

$$= (a^2 + b^2)|\gamma|^2,$$

onde tanto $a^2 + b^2$, $|\,\gamma\,|^2 > 1$. Mas a única tal factorização de p^2 é pp, portanto,

$$p = a^2 + b^2.$$

($\Rightarrow$) Inversamente, se um primo p comum é igual $a^2 + b^2$ com $a, b \in Z$ então p não é um primo Gaussiano porque tem a factorização Gaussiana primo

$$p = (a - bi)\,(a + bi)$$

e $N(a + ib) = N(a - ib) < N(p)$. ■

Observe também que os fatores $a - bi\, e\, a + bi$ de p são primos Gaussianos porque a sua norma é o número primo $a^2 + b^2 = p$. Além disso, todos os Gaussianos primos $a +$

$bi, onde\ a, b \neq 0,$ vêm em pares conjugados como este. Isto é então, porque se um membro do par se factorizar em $\alpha\beta$, então o seu conjugado é fatorizado em $\overline{\alpha\beta}$.

O que ainda não está claro é se todos os primos Gaussianos $a + bi\ com\ a, b$ diferentes de zero são fatores de primos comuns $p = a^2 + b^2$. É concebível que $a + bi$ pode ser um primo Gaussiano enquanto $a^2 + b^2$ é um produto de dois ou mais primos comuns. Nesta Seção descartamos isso com a ajuda de uma única factorização prima em $Z[i]$.

De qualquer forma, podemos ver que esclarecimentos adicionais sobre a natureza dos primos Gaussianos depende de encontrar outra maneira de descrever os primos comuns que são somas de dois quadrados. Os primos que não são somas de dois quadrados são da forma $4n + 3$. O complemento a este resultado que qualquer primo da forma $4n + 1$ é uma soma de dois quadrados e um famoso teorema descoberto por Fermat.

Divisão em $Z[i]$

A factorização prima única em $Z[i]$, como em Z, depende do algoritmo euclidiano, que depende por sua vez:

Teorema 1.2.13: ***Propriedade de divisão de*** $Z[i]$. $Se\ \alpha, \beta \neq 0$ estiverem em $Z[i]$ então existem μ, ρ pertencentes a Z[i] e tal que

$$\alpha = \mu\beta + \rho \quad com\ N|\rho| < N|\beta|.$$

Demonstração: Esta propriedade torna-se óbvia uma vez que se vê que o Gaussiano múltiplo inteiro $\mu\beta$ de qualquer inteiro Gaussiano $\beta \neq 0$ forma uma grade quadrada em o plano complexo. Isso ocorre porque a multiplicação de β por i roda o vetor de $0\ a\ \beta$ através de $90°$, portanto, $0, \beta\ e\ i\beta$ são três cantos de um quadrado. Todos os outros múltiplos de β são somas (ou diferenças) de $\beta\ e\ i\beta$, portanto, eles estão no cantos de uma grade quadrada. (Figura 1). Em [29]

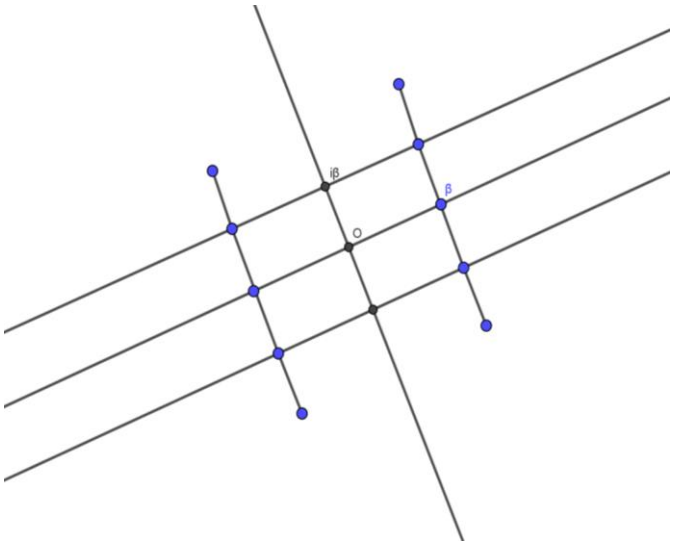

Figura 1: Múltiplos dos Inteiros Gaussianos

Qualquer número inteiro Gaussiano α está em um desses quadrados, e há um canto mais próximo $\mu\beta$ (não necessariamente único, mas não importa). Então

$$\alpha = \mu\beta + \rho, onde \mid \rho \mid = distância\ ao\ canto\ mais\ próximo,$$

então | ρ | é menor do que o lado de um quadrado, a saber | ß |. ■

Graças à propriedade da divisão que temos

1. Um algoritmo euclidiano $para\ Z[i]$
2. $mdc\ (\alpha, \beta) = \mu\alpha + \nu\beta\ para\ alguns\ \mu, \nu \in Z[i]$.
3. A propriedade do divisor primo: se um π primo divide $\alpha\beta$, então π divide $\alpha\ ou\ \pi\ divide\ \beta$.

Como uma primeira aplicação de factorização prima única em $Z[i]$, completamos a descrição dos primos Gaussianos. Lá encontramos que os primos reais Gaussianos são primos comuns que não são somas de dois quadrados e seus negativos. Também é claro que o Gaussiano imaginário puro os primos são da forma $\pm ip$, onde p é um primo Gaussiano real. Assim, ele permanece para descrever os primos Gaussianos $a + bi$ com a, b diferentes de zero.

Teorema 1.2.14: ***Primos Gaussianos Imaginários***. Os primos Gaussianos $a + bi\ com\ a, b$ diferentes de zero são fatores de primos comuns p da forma $a^2 + b^2$. Em [29]

Demonstração: Primeiro, como observado na Seção anterior, se $a + bi$ é um primo Gaussiano então é $a - bi$ $(porque\ se\ a - bi = \alpha\beta$ não é primo, nem é $a + bi = \alpha\beta)$.

Em seguida, $(a - bi)(a + bi)$ é uma factorização Gaussiana prima (necessariamente única) do

$$p = a^2 + b^2 = (a - bi)(a + bi).$$

Mas p deve ser um primo comum. Na verdade, se

$$p = rs\ com\ 1 < r, s < p\ e\ r, s \in Z,$$

então os fatores primos Gaussianos de $r\ e\ s$ dão uma factorização Gaussiana prima de p diferente de $(a - bi)\ (a + bi)$ (ou dois fatores reais $r\ e\ s, ou \geq$ quatro fatores complexos). ■

CAPÍTULO 2

BREVES NOÇÕES SOBRE TEORIA DE GRAFOS.

Neste capítulo expomos alguns conceitos da Teoria de Grafos, definições e alguns exemplos. Apenas definimos as noções necessárias para o trabalho. Para um estudo mais profundo da teoria dos grafos o leitor pode consultar [21, 36, 48].

2.1 Noções Históricas.

Podemos dizer, como **Harary**, que a teoria dos grafos foi redescoberta muitas vezes; ou, então, que problemas do interesse de diversas áreas foram estudados separadamente e mostraram características semelhantes. Importante, de qualquer modo, é observar que o período transcorrido entre a demonstração de Euler sobre o problema das sete pontes de Konigsberg e a última década do século XIX - mais de 150 anos viu, apenas, o surgimento de alguns poucos trabalhos. Assim é que, em 1847, **Kirchhoff** utilizou modelos de grafos no estudo de circuitos eléctricos e ao fazê-lo, criou a teoria das árvores, - uma classe de grafos, para caracterizar conjuntos de ciclos independentes. Dez anos mais tarde, **Cayley** seguiria a mesma trilha, embora tendo em mente outras aplicações, dentre as quais se destaca a enumeração dos isômeros dos hidrocarbonetos alifáticos saturados, em química orgânica. Enfim, **Jordan** (1869) se ocupou também das árvores, de um ponto de vista estritamente matemático.

Muitos eventos que provaram ser importantes são relacionados com problemas com pouca aplicação prática: **Hamilton**, em 1859, inventou um jogo que consistia na busca de um percurso fechado envolvendo todos os vértices de um dodecaedro regular, de tal modo que cada um deles fosse visitado uma única vez. É interessante, aliás, observar que os problemas de Hamilton e de Euler encontraram aplicação, respectivamente um e dois séculos mais tarde, no campo da pesquisa operacional. **Kempe** (1879) procurou, sem sucesso, demonstrar a "conjectura das quatro cores", apresentada por **Guthrie** a **De Morgan**, provavelmente em 1850. Este problema, um dos mais importantes já abordados pela teoria dos grafos, oferece interesse apenas teórico: trata-se de provar que todo mapa desenhado no plano e dividido em um número qualquer de regiões pode ser colorido com um máximo de quatro cores sem que duas regiões fronteiriças recebam a mesma cor. **Taity** (1880) divulgou também uma "prova", infelizmente baseada numa conjectura falsa e **Heawood** (1890) mostrou que a prova de Kempe estava errada, obtendo no processo uma prova válida para 5 cores; a prova para 4 cores somente foi obtida em 1976. A importância do problema reside nos desenvolvimentos teóricos trazidos pelas tentativas de resolvê-lo, as quais enriqueceram a teoria dos grafos em diversos recursos ao longo da primeira metade do século XX: exemplificando, **Birkhoff** (1912)

definiu os polinómios cromáticos; **Whitney** (1931) criou a noção de grafo dual e **Brooks** (1941) enunciou um teorema fornecendo um limite para o número cromático de um grafo.

Outros eventos importantes podem ser citados: **Menger** (1926) demonstrou um importante teorema sobre o problema da desconexão de itinerários em grafos e **Kuratowski** (1930) encontrou uma condição necessária e suficiente para a planaridade de um grafo. **Turán** (1941) foi o pioneiro do ramo conhecido como teoria extremal de grafos e **Tutte** (1947) resolveu o problema da existência de uma cobertura minimal em um grafo. Vale a pena registrar que o termo grafo foi usado pela primeira vez por **Sylvester** em 1878 e que o primeiro livro específico sobre grafos foi publicado por **Konig** em 1936, uma época na qual, conforme **Wilder**, o assunto era considerado "um campo morto".

A partir de 1956, com a publicação dos trabalhos de **Ford** e **Fulkerson** (1956), **Berge** (1957) e **Ore** (1962), o interesse pela teoria dos grafos começou a aumentar, crescendo rapidamente no mundo todo: conforme cita **Harary**, em 1969 foi publicada por J. Turner. A imensa maioria dos livros sobre grafos foi publicada depois de 1970, em grande parte sob a influência das obras de Berge e Harary. O desenvolvimento dos computadores levou à publicação de várias obras dedicadas aos algoritmos de grafos, abrindo assim possibilidades crescentes de utilização aplicada da teoria.

2.2 *Noções Básicas da Teoria de Grafos.*

Nesta seção, falaremos sobre os grafos não orientados.

Definição 2.2.1: Designa-se por grafo (não orientado) um terno $G = (V(G), E(G), \psi(G))$, onde $V = V(G)$ é um conjunto não vazio, $E = E(G)$ é um conjunto disjunto de V e ψG é uma função tal que, para cada $e \in E, \psi G(e)$ denota um par não ordenado de elementos (não necessariamente distintos) de V. Neste caso, V designa-se por conjunto de Vértices, E por conjunto de arestas e ψG por função de incidência.

Definição 2.2.2: ***(Grafo simples)***. Um grafo diz-se simples se não contém arestas paralelas nem lacetes.

Definição 2.2.3: Dado um grafo G simples, designa-se por grafo complementar de G e denota-se por G^C, um grafo simples cujo conjunto de vértices é $V(G)$ e no qual dois vértices são adjacentes se e só se não são adjacentes em G.

Figura 2: Grafo G. figura 3: Grafo G^C

Definição 2.2.4: Dois grafos $G = (V(G), E(G), \psi(G))$ e $H = (V(H), E(H), \psi(H))$ dizem-se isomorfos, denotando-se esta relação de isomorfismo por $G \cong H$, se existem duas bijeções $\varphi: V(G) \to V(H)$ *e* $\theta: E(G) \to E(H)$ tais que

$$\psi G(e) = uv \text{ se e só se } \psi H\big(\theta(e)\big) = \varphi(u)\varphi(v)$$

Por outras palavras dois grafos dizem-se isomorfos se existe uma bijeção entre os respetivos conjuntos de vértices e uma bijeção entre os respetivos conjunto de arestas que preservam as relações de adjacência e de incidência.

Definição 2.2.5: Designa-se por isomorfismo entre dois grafos simples G *e* H, uma bijeção $\varphi: V(G) \to V(H)$ tal que

$$uv \in E(G) \text{ se e só se } \varphi(u)\varphi(v) \in E(H)$$

De acordo com as Definições 2.4 e 2.5, podemos concluir que dois grafos são isomorfos quando existe um isomorfismo entre eles.

Aresta Incidente: é aquela que liga dois vértices distintos.

Arestas Adjacentes: são aquelas que estão ligadas a um mesmo vértice e não são arestas múltiplas.

Vértices Adjacentes: são aqueles que estão ligados por uma mesma aresta.

Ao número de vértices de um grafo G chamamos de *ordem de* G, que indicamos por $v(G)$ ou apenas v, e ao número de arestas de um grafo G chamamos *dimensão de* G, que indicamos por $\varepsilon(G)$ ou apenas ε.

Definição 2.2.6: Dado um grafo G e um vértice $v \in V(G)$, designamos por grau de v o número de arestas incidentes no vértice v, que indicamos por $d_G(v)$. O maior grau dos vértices de G indicamos por $\Delta(G)$ e o menor grau dos vértices de G indicamos por $\delta(G)$.

Caminho: é uma sucessão de vértices e arestas tal que cada aresta liga o vértice que a precede ao vértice que a segue, não repetindo arestas.

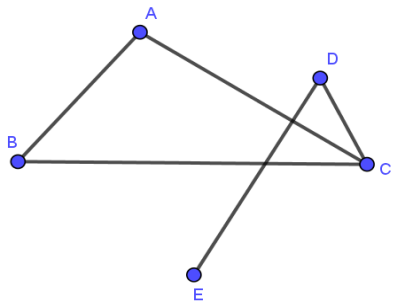

Figura 4

Os vértices A, B, C e D representam um caminho neste grafo.

Caminho Fechado: é aquele que começa e termina no mesmo vértice.

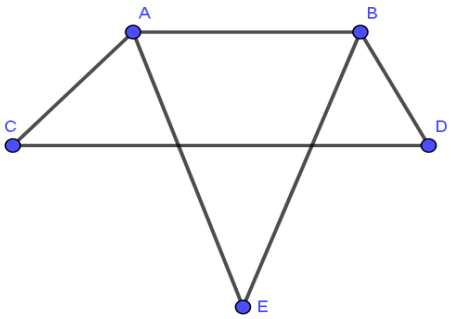

Figura 5

Ciclo: é um caminho fechado.

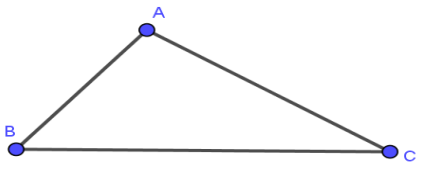

Figura 6

Passeio: é um caminho onde pode haver repetição de arestas e de vértices.

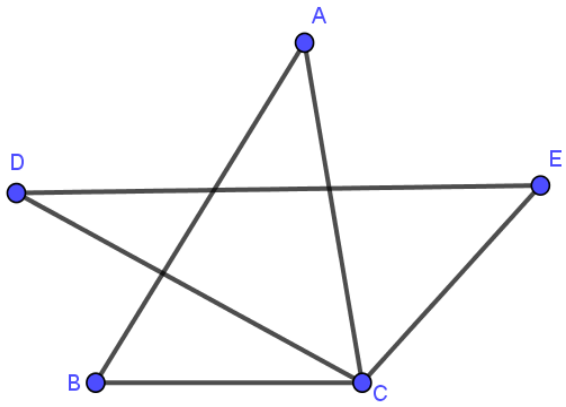

Figura 7

Ponte: é uma aresta cuja remoção reduz a conexidade do grafo.

Exemplo: h *e* i são as pontes do grafo.

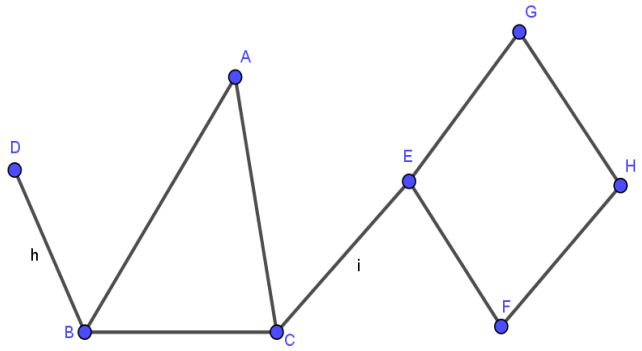

Figura 8

Subgrafo de um Grafo G: é aquele cujo o conjunto dos vértices e o conjunto das arestas são subconjuntos do conjunto de vértices e de arestas, respetivamente, de G.

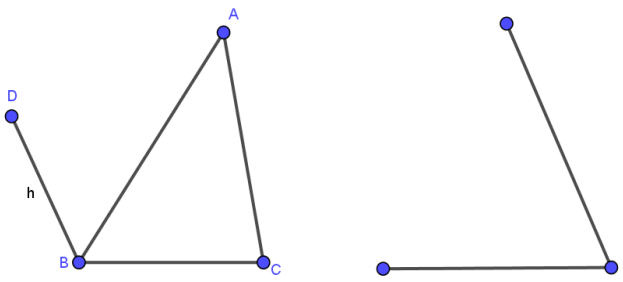

Figura 9: Grafo G e Figura 10: Subgrafo de G

Definição 2.2.7: Dado um grafo G, eliminando todos os lacetes e substituindo cada conjunto de arestas paralelas por uma única aresta obtemos um subgrafo abrangente de G ao qual chamamos de *subgrafo de suporte de arestas*.

Grafo completo: dizemos que G é um grafo completo quando todos os vértices são adjacentes.

Grafo Bipartido: é aquele em que o conjunto dos seus vértices admite uma partição $\{V_1; V_2\}$ de tal maneira que toda a aresta de G une um vértice de V_1 a um vértice de V_2.

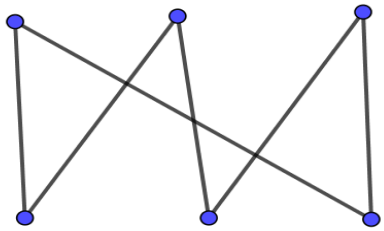

Figura 11

Nota: Um grafo é bipartido se e só se não tem circuitos de comprimento ímpar.

Definição 2.2.8*:* Dizemos que G é um grafo conexo se para cada par de vértices existe sempre um caminho que os une.

Grafo Desconexo: é aquele que não é conexo.

Componentes Conexas: de um grafo desconexo, são subgrafos conexos, disjuntos em relação aos vértices e maximais em relação à inclusão.

Floresta: é um grafo cujas componentes conexas são árvores.

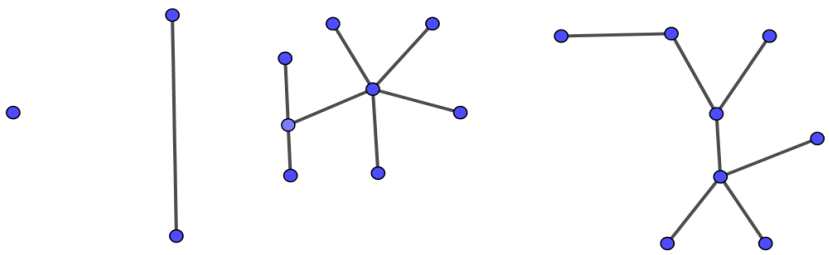

Figura 12

Definição 2.2.9: Chamamos cintura do G ao comprimento do ciclo de menor comprimento de $G, caso\ exista; caso\ contrário\ dizemos\ que\ g(G) = \infty.$

Excentricidade: Seja G um grafo e v um vértice, então a maior distância entre v e todos os outros vértices de G designa-se por excentricidade de v e denota-se por $e_G(v)\ ou\ e(v)$

Diâmetro: Dado um grafo G, a maior excentricidade dos seus vértices designa-se por diâmetro.

Raio: é a distância mínima de todos os vértices G.

Centro: são os vértices onde as excentricidades são mais pequenas.

Exemplo: Dado o grafo G indica o diâmetro, o raio, a excentricidade e a cintura do grafo completo de ordem 5.

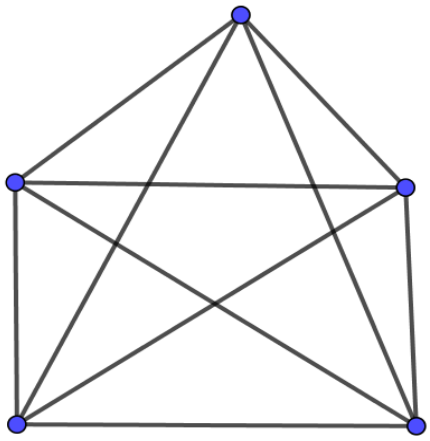

Figura 13

$$Temos: diam(G) = 1, r(G) = 1, g(G) = 3, e(G) = 1$$

Grafo Regular: é um grafo no qual todos os vértices têm o mesmo grau.

Grafo Planar: é um grafo que pode ser imerso no plano de tal forma que suas arestas não se cruzam.

Grafo Estrela: é um grafo onde existe um vértice central que é adjacente a todos os outros vértices do grafo.

Grafo Euleriano: um grafo G é Euleriano se e somente se G é conexo e cada vértice de G tem grau par.

Grafo Hamiltoniano: um grafo G é dito ser Hamiltoniano se existe um ciclo em G que contenha todos os seus vértices, sendo que cada vértice só aparece uma vez no ciclo.

CAPÍTULO 3

O GRAFO DIVISOR DE ZERO DE UM ANEL COMUTATIVO.

Neste capítulo trataremos da noção do grafo dos divisores de zero. Este é o tema principal do trabalho. Apresentamos definições e demonstrações de alguns teoremas importantes. Apresentamos também alguns exemplos.

3.1 O Grafo Divisor de Zero de um anel comutativo.

Seja R um anel comutativo com identidade e seja $Z\,(R)$ seu conjunto de divisores de zero. Associamos um grafo (simples) $\tau(R)\ a\ R\ com\ vértices\ Z(R)^* = Z\,(R) - \{0\}$, isto é, $V\big(\tau(R)\big) = Z(R)^*$ conjunto de divisores zero não nulos de R e para distintos $x, y \in Z(R)^*$ Os vértices $x\ e\ y$ são adjacentes se e somente se $xy = 0$. Assim, $\tau(R)$ é o grafo vazio se e somente $se\ R$ é um domínio integridade.

Exemplo: $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

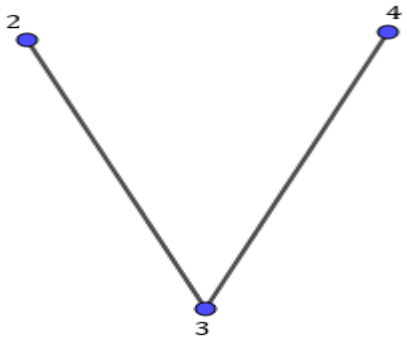

Figura 14: $\tau(Z_6)$

O principal objetivo deste capítulo é estudar a interação das propriedades teóricas de R com as propriedades teóricas de $\tau(R)$. Este estudo ajuda a iluminar a estrutura de R.

$Para\ x, y \in Z^*(R), defina\ x \sim y\ se\ xy = 0\ ou\ x = y$. A relação é sempre reflexiva e simétrica, mas não usualmente transitiva. O grafo de divisor de zero $\tau(R)$ mede esta falta de transitividade no sentido de que ~ é transitiva se e somente se $\tau(R)$ estiver completo.

A idéia de grafo de divisor de zero de um anel comutativo foi introduzida por I. Beck em [10], onde ele estava principalmente interessado em coloração. Esta investigação das colorações de um anel comutativo foi então continuada por D. Anderson e M. Naseer em [5]. Sua definição era ligeiramente diferente da nossa; Eles deixaram todos os elementos de R ser vértices e $x\ e\ y$ são adjacentes se e somente se $xy = 0$. Denotamos seu grafo de divisor de zero de R por $\tau_0(R)$. Em $\tau_0(R)$, o vértice 0 é adjacente a cada outro vértice. Nossos resultados para $\tau(R)$ têm análogos naturais a $\tau_0(R)$; No entanto, sentimos que a nossa definição ilustra melhor a estrutura divisor de zero de R.

Na seção 3.2, damos muitos exemplos, mostramos que $\tau(R)$ é conexo e $diam(\tau(R)) \leq 3$, e determinamos quando $\tau(R)$ é um grafo completo ou um grafo estrela. Um passo-chave é caracterizar quando um vértice é adjacente a todos os outros vértices. Na terceira seção, estudamos o grupo de automorfismo do $\tau(R)$.

Incluiremos definições básicas da teoria dos grafos conforme necessário. Referências básicas para a teoria de grafos são $[21, 28, 36]$; Para a teoria dos anéis comutativos, ver $[9, 32, 34]$. Todos os anéis R são comutativos com identidade excepto no último capítulo. Como de costume, os anéis de inteiros e $inteiros\ modulo\ n$ serão denotados por $Z\ e\ Z_n$, respectivamente, e F_q será o corpo finito com q elementos.

3.2. *Exemplos:*

$Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.

×	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5

5	0	5	2	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Figura 15: $\tau(Z_9)$

3.3 *Propriedades de* $\boldsymbol{\tau(R)}$

Nesta seção, mostramos que $\tau(R)$ é sempre conexo e tem diâmetro menor ou igual a 3. Determinamos quais grafos completos e grafo estrela podem ser realizados como $\tau(R)$. Começamos com alguns exemplos que motivam resultados posteriores.

Exemplo: (a) Abaixo estão os grafos de divisor de zero para vários anéis. Observe que esses exemplos mostram que anéis não-isomorfos podem ter o mesmo grafo de divisor de zero e que o grafo de divisor zero não deteta elementos nilpotente..

$Z_4 = \{0, 1, 2, 3\}$.

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Figura 16: $\tau(Z_4)$

(b) Na parte a) acima, todos os grafos conexos com menos de quatro vértices podem ser realizados como $\tau(R)$. Dos onze grafos com quatro vértices, apenas seis são conexos. Destes seis, apenas os três grafos seguintes podem ser realizados como $\tau(R)$.

$Z_3 \times Z_3 = \{(\bar{x}, \bar{y}) : \bar{x}, \bar{y} \in Z_3\} = (\bar{0}, \bar{0});\ (\bar{0}, \bar{1});\ (\bar{0}, \bar{2}); (\bar{1}, \bar{0});\ (\bar{1}, \bar{1});\ (\bar{1}, \bar{2});\ (\bar{2}, \bar{0});\ (\bar{2}, \bar{1});\ (\bar{2}, \bar{2}) : (\bar{x}, \bar{y}) \cdot (\bar{w}, \bar{z}) = (\bar{0}, \bar{0})$

$(\bar{0}, \bar{1}) \cdot (\bar{1}, 0) = (\bar{0}, \bar{0}).$

$(\bar{0}, \bar{2}) \cdot (\bar{2}, \bar{0}) = (\bar{0}, \bar{0}).$

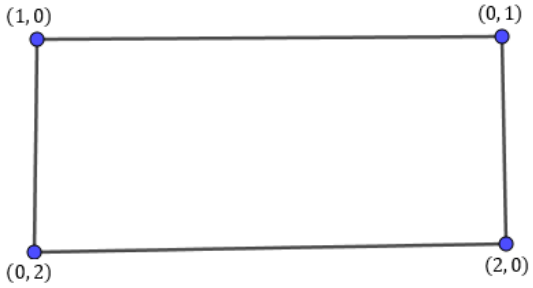

Figura 17: $\tau(Z_3 \times Z_3)$

$Z_{25} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}, \overline{18}, \overline{19}, \overline{20}, \overline{21}, \overline{22}, \overline{23}, \overline{24}\}.$

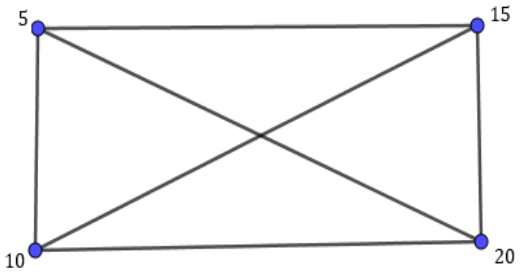

Figura 18: $\tau(Z_{25})$

$Z_2 \times F_4.$

$Z_2 = \{\bar{0}, \bar{1}\}.$

$P_1(x) = x^2 + x + 1.$

$P_2(x) = x^2 + 1.$

$P_2(\bar{0}) = \bar{0} + \bar{1} = \bar{1}.$

$P_2(\bar{1}) = \bar{1} + \bar{1} = \bar{0}.$

$P_1(\bar{0}) = \bar{0} + \bar{0} + \bar{1} = \bar{1}.$

$P_1(\bar{1}) = \bar{1} + \bar{1} + \bar{1} = \bar{1}.$

$F_4 = \{a + bu; a \in Z_2 \; e \; u \in F_4\}.$

$P(u) = u^2 + u + 1.$

$F_4 = \{0, 1, u, u + 1\}.$

Tabela da soma.

$+$	0	1	u	$u+1$
0	0	1	u	$u+1$
1	1	0	$u+1$	u
u	u	$u+1$	0	1
$u+1$	$u+1$	u	1	0

Tabela da multiplicação.

$\times$	0	1	u	$u+1$
0	0	0	0	0
1	0	1	u	$u+1$
u	0	u	$u+1$	1
$u+1$	0	$u+1$	1	u

Observação:

$$u^2 + u + 1 = 0 \leftrightarrow u^2 = -u - 1 \leftrightarrow u^2 = u + 1$$

$Z_2 \times F_4 = \{(x, y): x \in Z_2 \; e \; y \in F_4\}$

$$(0,0);\ (0,1);\ (0,u);\ (0,u+1);\ (1,0);\ (1,1);\ (1,u);\ (1,u+1)$$

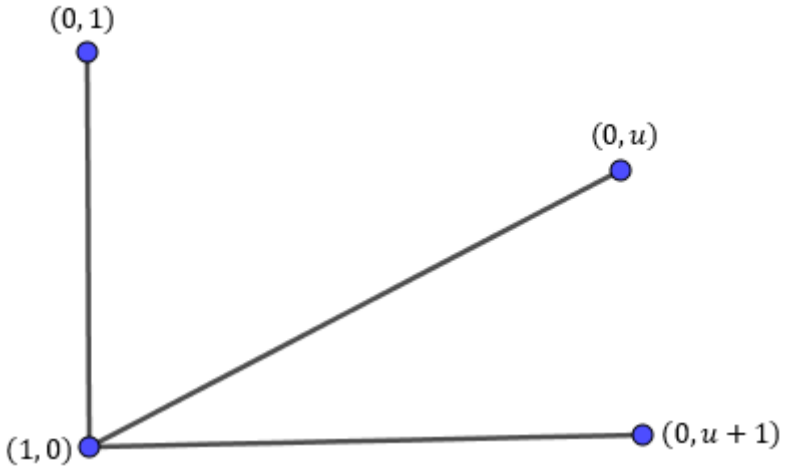

Figura 19: $\tau(Z_2 \times F_4)$

Em seguida, esboçamos uma prova de que o τ grafo com vértices $\{a, b, c, d\}$ e arcos $a - b, b - c, c - d$ não pode ser realizado como $\tau(R)$.

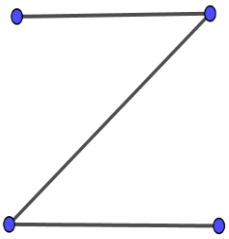

Figura 20

Suponha que existe um anel R com $Z(R) = \{0, a, b, c, d\}$ e acima das relações de divisores de zero. Então $a + c \in Z(R)$ uma vez que $(a + c)\, b = 0$. Portanto, $a + c$ deve ser $0, a, b, c \; ou \; d$. Uma simples verificação produz $a + c = b$ como a única possibilidade. Similarmente, $b + d = c$. Daí $b = a + c = a + b + d$; Assim $a + d = 0$. Assim, $bd = b(-a) = 0$, uma contradição. As provas dos outros dois grafos conexos não-realizáveis em quatro vértices são semelhantes.

(c) Vimos acima que $\tau(R)$ pode ser um triângulo ou quadrado. Mas $\tau(R)$ não pode ser um n-gon para qualquer $n \geq 5$. (As provas são semelhantes àquela da parte (b) acima. Isto também se segue diretamente dos **Teoremas 3.3.1** e **3.3.4.**) No entanto, para cada $n \geq 3$, há um divisor de zero de grafo com um ciclo n. Para $R_n = \frac{Z_2[X_1, \ldots, X_n]}{I}$ onde $I = (X_1^2, \ldots, X_n^2, X_1X_2, \ldots, X_nX_1)$. Então $\tau(R_n)$ é finito e tem um ciclo de comprimento n, ou seja, $X_1 - X_2 - \cdots - \cdots X_n - X_1$.

Sejam $A \; e \; B$ domínios de integridades e seja $R = A \times B$. Então $\tau(R)$ é um grafo bipartido completo (isto é, $\tau(R)$ pode ser dividido em dois conjuntos de vértices disjuntos $V_1 = \{(a, 0) : a \in A^*\}$ e $V_2 = \{(0, b) : b \in B^*\}$ e dois vértices $x \; e \; y$ são adjacentes se e somente se estiverem em conjuntos de vértices distintos) com $|\tau(R)| = |A| + |B| - 2$. O grafo bipartido

completo com conjuntos de vértices com $m\ e\ n$ elementos, respetivamente, será denotado por $K^{m,n}$. Um grafo bipartido completo da forma $K^{1,n}$ é chamado de grafo de estrela. Se $A = Z_2$, então $\tau(R)$ é um grafo em estrela $|\tau(R)| = |B|$. Por exemplo, $\tau(F_p \times F_q) = K^{p-1,q-1}$ e $\tau(Z_2 \times F_q) = K^{1,q-1}$. Damos dois exemplos específicos.

$Z_2 \times Z_7 =$
$\{(\bar{0},\bar{0});(\bar{0},\bar{1});(\bar{0},\bar{2});(\bar{0},\bar{3});(\bar{0},\bar{4});(\bar{0},\bar{5});(\bar{0},\bar{6});(\bar{1},\bar{0});(\bar{1},\bar{1});(\bar{1},\bar{2});(\bar{1},\bar{3});(\bar{1},\bar{4});(\bar{1},\bar{5});(\bar{1},\bar{6})\}$.

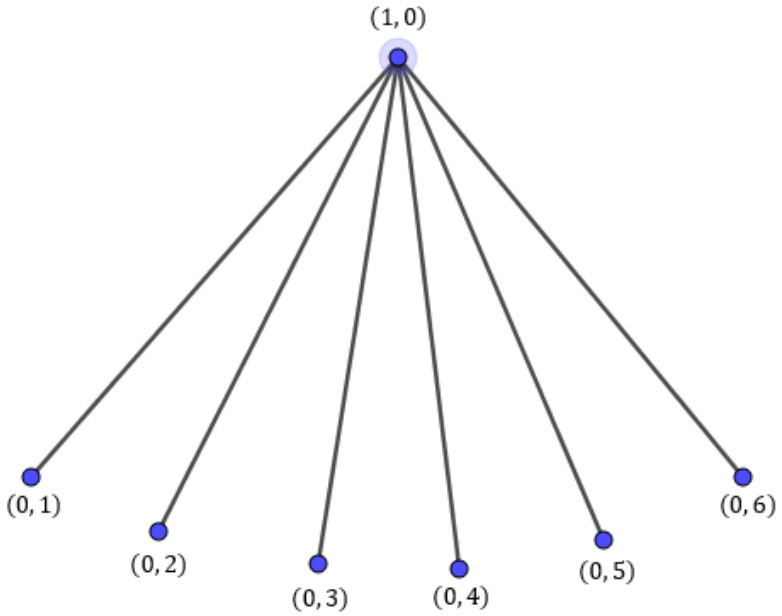

Figura 21: $\tau(Z_2 \times Z_7)$

$Z_3 \times Z_5 =$
$\{(\bar{0},\bar{0});(\bar{0},\bar{1});(\bar{0},\bar{2});(\bar{0},\bar{3});(\bar{0},\bar{4});(\bar{1},\bar{0});(\bar{1},\bar{1});(\bar{1},\bar{2});(\bar{1},\bar{3});(\bar{1},\bar{4});(\bar{2},\bar{0});(\bar{2},\bar{1});(\bar{2},\bar{2});(\bar{2},\bar{3});(\bar{2},\bar{4})\}$

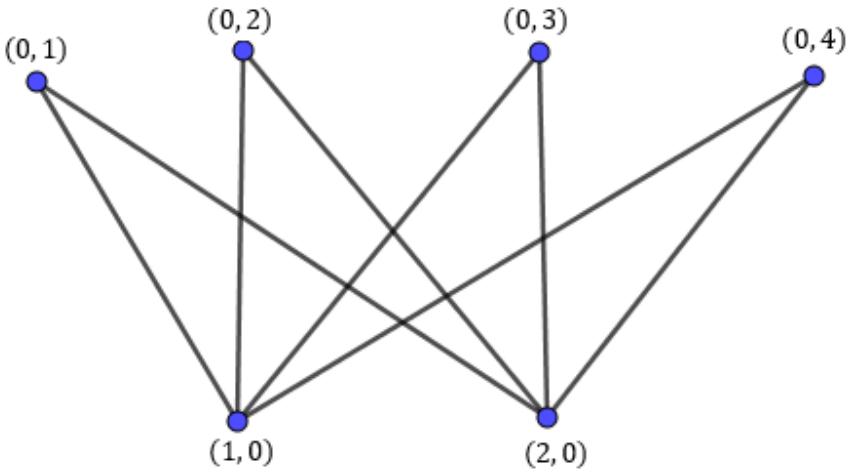

Figura 22: $\tau(Z_3 \times Z_5)$

Naturalmente, $\tau(R)$ pode ser infinito (isto é, um anel pode ter um número infinito de divisores de zero). Mas $\tau(R)$ é provavelmente de maior interesse quando é finito, pois então se pode desenhar $\tau(R)$. Vamos afirmar a maioria dos resultados em um cenário tão geral quanto possível, e, em seguida, muitas vezes se especializam para o caso finito. Em seguida, mostramos que $\tau(R)$ é finito (exceto caso trivial quando $\tau(R)$ está vazio) somente quando R é ele mesmo finito. Assim, muitas vezes restringiremos o caso em que R é um anel finito. Lembre-se que se R é finito, então cada elemento de R é uma unidade ou um divisor de zero, cada ideal primo de R é um aniquilador ideal e cada divisor de zero de R é nilpotente se e somente se R é local. Além disso, se R é um anel local finito com M ideal maximal, então $|R| = p^n$ para algum primo p e inteiro $n \geq 1$. Então $|\tau(R)| = p^m - 1$ para algum inteiro $m \geq 0$. A essência de nosso primeiro resultado é que $Z(R)$ é finita se e somente se R é finito ou um domínio integridade (este resultado, com uma prova diferente, e o fato de que $|R| \leq |Z(R)|^2 \; quando \; 2 \leq |Z(R)| \infty$ são devidas a N. Ganesan $[17, Teorema\ 1]$; em $[32]$ para análogos não comutativos).

Teorema 3.3.1: Seja R um anel comutativo. Então $\tau(R)$ é finito e somente se R é finito ou um domínio de integridade. Em particular, se $1 \leq |\tau(R)| < \infty$ então R é finito e não um corpo. Em $[36]$.

Demonstração. Suponha que $\tau(R)(= Z(R)^*)$ seja finito e não vazio. Então existe, $x, y \in R$ não nulos com $xy = 0$. Seja $I = ann\,(x)$. Então $I \subset Z\,(R)$ é finito e $ry \in I$ para todo $r \in R$. Se R é infinito, então existe um $i \in I$ com $j = \{r \in R | ry = i\}$ infinito. Para qualquer $r, s \in j, (r - s)y = 0$ então $ann(y) \subset Z(R)$ é infinito, uma contradição. Assim, R deve ser finito. ■

Teorema 3.3.2: Seja R um anel comutativo. Então $\tau(R)$ é conexo e $diam\big(\tau(R)\big) \leq 3$. Além disso, se $\tau(R)$ contém um ciclo, então $g\big(\tau(R)\big) \leq 7$. Em $[36]$

Demonstração: Seja $x, y \in Z(R)^*$ distintos. Se $xy = 0$, então $d\,(x, y) = 1$. Então suponha que xy seja diferente de zero. Se $x^2 = y^2 = 0$, então $x - xy - y$ é um caminho de comprimento 2; assim $d\,(x, y) = 2$. Se $x^2 = 0\, e\, y^2 \neq 0$, então há um $b \in Z\,(R)^* - (x, y)$ com $xy = 0$. Se $bx = 0$, então $x - b - y$ é um caminho de comprimento 2. Se $bx \neq 0$, então $x - bx - y$ é um caminho de comprimento 2. Em ambos os casos, $d(x, y) = 2$. Um argumento semelhante é válido se $y^2 = 0\, e\, x^2 \neq 0$. Assim, podemos assumir que $xy,\ x^2\, e\, y^2$ são todos diferentes de zero. Portanto, há um, $a, b \in Z(R)^* - \{x, y\}\, com\, ax = by = 0$. Se $a = b$, então $x - a - y$ é um caminho de comprimento 2. Assim, podemos assumir que $a \neq b$. Se $ab = 0$, então $x - a - b - y$ é um caminho de comprimento 3 e, portanto, $d\,(x, y) \leq 3$. Se $ab \neq 0$, então $a - ab - y$ é um caminho de comprimento 2; assim $d\,(x, y) = 2$. Daí $d\,(x, y) \leq 3$, e, portanto, $diam\,(\tau(R)) \leq 3$. ■

Definição 3.3.3: um anel diz-se artiniano se satisfaz a condição de cadeia descendente ou seja sobre ideais.

Exemplos:

- ✓ Um domínio de integridade artiniano é um corpo.
- ✓ Um anel com uma quantidade finita de ideais, é artiniano. Em particular, um anel finito (tal como Z/nZ) é artiniano.
- ✓ Seja k um corpo. Então $k[t]/(t^n)$ é artiniano para todo inteiro positivo n.
- ✓ Se I é um ideal não nulo de um domínio de Dedekind A então A/I é um anel artiniano de ideal principal.

Teorema 3.3.4: Seja R um anel artiniano comutativo (em particular, R poderia ser um anel comutativo finito). Se $\tau(R)$ contém um ciclo, então $g(\tau(R)) \leq 4$. Em [36]

Demonstração: Suponha que $\tau(R)$ contenha um ciclo. R é um produto finito direto dos anéis locais artinianos. Em primeiro lugar, suponha que R seja local com o ideal maximal diferente de zero M. Então $M = ann\,(x)$ para algum $x \in M^*$. Se houver distintos $y, z \in M^* - \{x\}$ com $yz = 0$, então $y - x - z - y$ é um triângulo. Caso contrário, $\tau(R)$ não contém ciclos, uma contradição. Neste caso, $g(\tau(R)) = 3$. Em seguida, suponha que $R = R_1 \times R_2$. Se ambos $|R_1| \geq 3$ e $|R_2| \geq 3$, então podemos escolher $a_i \in R_i - \{0, 1\}$. Então $(1,0) - (0,1) - (a_1, 0) - (0, a_2) - (1,0)$ é um quadrado. Então, neste caso, $g(\tau(R)) \leq 4$ Assim, podemos assumir que $R_1 = Z_2$. Se $|Z(R_2)| \leq 2$, então $\tau(R)$ não contém ciclos, uma contradição. Portanto, devemos ter $|Z(R_2)| \geq 3$. Como o $\tau(R)$ é conexo, existem distintos, $x, y \in Z(R_2)^*$ com $xy = 0$. Assim, $(\bar{0}, x) - (\bar{1}, y) - (\bar{0}, y) - (\bar{0}, x)$ é um triângulo. Portanto, neste caso, $g(\tau(R)) = 3$. Assim, em todos os casos, $g(\tau(R)) \leq 4$. ■

Teorema 3.3.5: Seja R um anel comutativo. Então $\tau(R)$ é completo se e somente se

$R \cong Z_2 \times Z_2$ *ou* $xy = 0$ *para todo* $x, y \in Z(R)$ Em [13]

Demonstração: $(\leftarrow)$ *por definição*.

$(\rightarrow)$ Suponha que $\tau(R)$ esteja completo, mas há um $x \in Z(R)$ com $x^2 \neq 0$. Mostramos que $x^2 = x$. Se não $x^3 = x^2 x = 0$. Portanto, $x^2 (x + x^2) = 0$ com $x^2 \neq 0$, então $x + x^2 \in Z(R)$ Se $x + x^2 = x$, então $x^2 = 0$, uma contradição. Assim, $x + x^2 \neq x$, então $x^2 = x^2 + x^3 = x(x + x^2) = 0$ uma vez que $\tau(R)$ está completa, novamente uma contradição. Assim, $x^2 = x$. A prova do teorema anterior, temos $R \cong Z_2 \times A$ ... e necessariamente $A \cong Z_2$. ■

Exemplo: Para cada inteiro $n \geq 1$, seja $R_n = Z_2[x]/(x^{n+1})$, um anel local finito. Então x^n é o único vértice adjacente a cada outro vértice. No entanto, para $n \geq 3$, $\tau(R_n)$ não é um grafo em estrela, uma vez que os vértices $x^{n-1} + x^n$ *e* x^{n-1} também são adjacentes. Nota que $|\tau(R_n)| = 2^n - 1$.

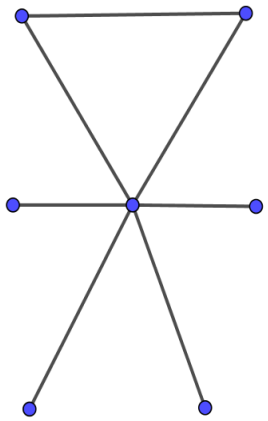

Figura 23

3.4 *Automorfismo de* $\boldsymbol{\tau(\mathbf{R})}$.

Para qualquer grafo $\tau(R)$, o grau de um vértice x de $\tau(R)$ é $\delta(x) = |\{y \in \tau(R)\}|y$ é adjacente a x. Para um vértice x do grafo de divisores de zero $\tau(R)$, temos que $\delta(x) = |ann(x) - \{0, x\}|$.

Agora nos especializamos em $\tau(Z_n)$ e estabelecemos alguma notação. Seja $n \geq 4$ não é um inteiro primo, e seja $X = \{d \in Z | 1 < d < n \; e \; d|n\}$. Para cada $d \in X$, seja $V_d = \{\bar{x} \in Z_n | 1 < x < n \; e \; mdc(x, n) = d\} \left(= U(Z_n)\bar{d} \subset Z(Z_n)^*\right)$ e $n_d = |V_d|$.

Teorema 3.4.1: Seja $n \geq 4$ um inteiro não-primo. Então $Aut\big(\tau(Z_n)\big)$ é um produto (finito) direto de grupos simétricos. Especificamente, $Aut\big(\tau(Z_n)\big) \cong \Pi\big(S_{n_d}/d \in X\big)$, em que $X = \{d \in Z | 1 < d < n \; e \; d/n|\}$ e $n_d = |\{x \in Z | 1 < x < n \; e \; mdc(x, n) = d\}(= |V_d|)$. Em [13]

Demonstração: Use a mesma notação como acima. Como dois vértices de $\tau(Z_n)$. tem o mesmo grau se e somente se eles estiverem no mesmo V_d e automorfismo do grafo preservam o grau, temos $f(V_d) = V_d$ para cada $f \in Aut\big(\tau(Z_n)\big) \; e \; d \in X$. Define $\varphi: Aut\big(\tau(Z_n)\big) \rightarrow \Pi\{S_{n_d} | d \in X\} \; para \; \varphi(f) = (f|V_d), com \; f|V_d$ visto de forma natural como um elemento de S_n. Pelo comentário acima, φ é um monomorfismo de grupo bem definido. Para mostrar isso φ é surjectivo, basta mostrar que, para cada $d \in X$ fixo e a permutação partir de $\alpha \; a \; V_d$, existe um $f \in Aut\big(\tau(Z_n)\big)$ .. com $f|V_d = \alpha \; e \; f|V_d = 1_{V_d}$ para todo $d \neq \acute{d} \; em \; X$. Isso se segue, pois para qualquer $x, y \in V_d \; e \; a \in Z_n, ax = 0$ se e somente se $ay = 0$. ■

***Corolário 3.4.2*. Seja $n \geq 4$ um número inteiro não primo. Então**

- ✓ $Aut\big(\tau(Z_n)\big)$ é trivial se e somente $n = 4$.
- ✓ $Aut\big(\tau(Z_n)\big)$ é abeliano se e somente $se \; n = 4, 6, 8, 9, ou \; 12$.

Em particular, $Aut\big(\tau(Z_n)\big) \cong Z_2$ quando $n = 6, 8, ou \; 9$, e $Aut\big(\tau(Z_{12})\big) \cong Z_2 \times Z_2 \times Z_2$.

Exemplo: Ilustramos a prova do **Teorema 3.4.1** por computação de $Aut(\tau(Z_{12}))$. Temos $x = \{2,3,4,6\}$, e assim $V_2 = \{\overline{2}, \overline{10}\}$; $V_3 = \{\overline{3}, \overline{9}\}$; $V_4 = \{\overline{4}, \overline{8}\}, e\ V_6 = \{\overline{6}\}$ Assim, $Aut(\tau(Z_{12})) \cong S_2 \times S_2 \times S_2 \times S_1 \cong Z_2 \times Z_2 \times Z_2$. Isto também é evidente a partir das simetrias óbvias do grafo do divisor de zero de Z_{12} abaixo.

×	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	4	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

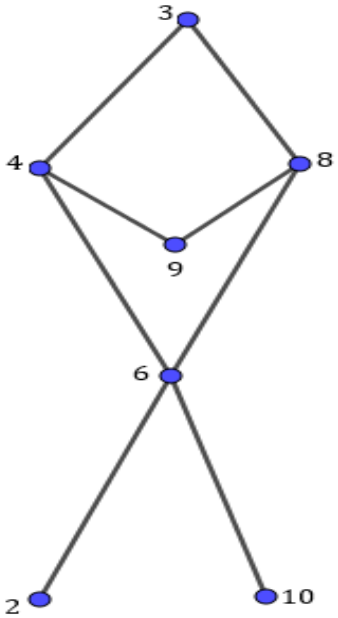

Figura 24: $\tau(Z_{12})$

CAPÍTULO 4

O GRAFO DOS DIVISORES DE ZERO DOS INTEIROS DE GAUSS MÓDULO n.

Neste capítulo estudamos o grafo dos divisores de zero de um anel de grande importância, o anel dos inteiros de Gauss módulo n.

4.1 Introdução.

Seja n um número natural e $\langle n\rangle$ o ideal principal gerado por n em $Z[i]$, $Z_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ o anel de inteiros modulo n. Então o anel de fator $Z[i]/\langle n\rangle$ é isomorfo para $Z_n[i] = \{\bar{a} + \bar{b}\imath : \bar{a}, \bar{b} \in Z_n\}$, o que implica que $Z_n[i]$ é um anel de ideal principal. O anel $Z_n[i]$ é chamado de anel de inteiros Gaussianos modulo n.

Foi mostrado em Abu Osba $[1]$ que $\bar{a} + i\bar{b}$ é uma unidade em $Z_n[i]$ se e somente se $\bar{a}^2 + \bar{b}^2$ é uma unidade em Z_n . E se $n = \prod_{j=1}^{s} a_j^{k_j}$ é a decomposição prima do número inteiro positivo n então $Z_n[i]$ é o produto direto dos anéis $Z_{a_j{}^{k_j}}[i]$. Também se $m = t^k$ para alguns primo t e inteiro positivo k então $Z_m[i]$ é local se e somente se $t = 2\, ou\, t \equiv 3\,(mod 4)$.

Recordemos que em um grafo $\tau(R)$, Um conjunto dominante é um conjunto de vértices A tal que todo vértice fora de A é adjacente a pelo menos um vértice em A. O número dominante de um grafo $\tau(R)$ denotado por $\delta(\tau)$ é o menor número da forma $|A|$, onde A é um conjunto dominante.

O caso quando n é um primo ou a potência de um primo é considerado primeiro. Então o caso geral é considerado.

O número de vértices em cada grafo, o diâmetro e a cintura são encontrados.

As caracterizações completas, em termos de n, são dadas nos casos em que o grafo $\tau(Z_n[i])$ é planar, regular, Euleriano, completo ou bipartido completo.

4.2 GRAFO DOS DIVISORES DE ZERO PARA $\mathbf{Z_{t^n}[i]}$

Nesta seção, as propriedades básicas de $\tau(Z_{t^n}[i])$ são estudados. Três casos são considerados: Quando $t = 2, t \equiv 3\,(mod 4), ou\, t \equiv 1\,(mod 4)$.

4.2.1 Grafo dos divisores de zero para $\mathrm{Z_{2^n}[i]}$

Note-se que 2 não é um primo Gaussiano, uma vez que $2 = (1+i)(1-i)$; no entanto, $2 = -i(1+i)^2$, então $Z_2[i]$ é isomorfo para o anel local $Z[i]/\langle(1+i)^2\rangle$ com seu único ideal

maximal $\{\bar{0}, \bar{1} + i\bar{1}\}$. Observe que $1 - i = -i(1 + i)$, e então os dois elementos são associados em $Z[i]$, e geram o mesmo ideal maximal. Além disso, em $Z_2[i]$ temos $\bar{1} + i\bar{1} = \bar{1} - i\bar{1}$. Assim, temos $V(\tau(Z_2[i])) = \{\bar{1} + i\bar{1}\}$, o que implica que $\tau(Z_2[i])$ é o grafo nulo N_1, isto é, um grafo com um vértice e sem arestas.

Agora, seja n um inteiro superior a 1. Então $2^n = (-1)^n(1 + i)^{2n}$ e assim

$Z_{2^n}[i] \cong \frac{Z[i]}{\langle 2^n \rangle} = Z[i]/\langle (1 + i)^{2n} \rangle$. Daí $Z_{2^n}[i]$ é local com o seu único ideal maximal $M = \langle \bar{1} + i\bar{1} \rangle$ e então $V(\tau(Z_{2^n}[i])) = \langle \bar{1} + i\bar{1} \rangle \backslash \{\bar{0}\}$. É fácil provar o seguinte lema.

Lema 4.2.1.1: O único ideal maximal em $Z_{2^n}[i]$ é $\{\bar{a} + i\bar{b} : a \; e \; b \; são \; ambos \; pares \; ou \; ímpares\}$.

Observe que $(-i)^{n-1}(\bar{1} + i\bar{1})^{2n-1} = (\bar{2})^{n-1}(\bar{1} + i\bar{1})$, Por isso, temos o seguinte Teorema.

Teorema 4.2.1.2: Seja $n > 1$. Então para todo $\alpha \in Z_{2^n}[i] \; temos \; \alpha(\bar{2})^{n-1}(\bar{1} + i\bar{1}) = \bar{0} \; ou \; \alpha(\bar{2})^{n-1}(\bar{1} + i\bar{1}) = (\bar{2})^{n-1}(\bar{1} + i\bar{1})$.

Demonstração: Se α não é uma unidade, então $\alpha = (\bar{a} + i\bar{b})(\bar{1} + i\bar{1}) \in \langle \bar{1} + i\bar{1} \rangle$, o que implica que $\alpha(\bar{2})^{n-1}(\bar{1} + i\bar{1}) = (\bar{2})^{n-1}(\bar{a} + i\bar{b})(\bar{1} + i\bar{1})^{2n} = \bar{0}$. Então, suponha que α é uma unidade e, portanto, $\alpha = \bar{a} + i\bar{b}$ com $a \; e \; b$ não são nem pares nem ímpares. Assim $(\bar{2})^{n-1}(\bar{1} + i\bar{1})(\alpha - \bar{1}) = (\bar{2})^{n-1}(\bar{1} + i\bar{1})(\bar{a} - \bar{1} + i\bar{b}) = \bar{0}$, já que neste caso $a - 1 \; e \; b$ são ambos pares ou ambos são ímpares, e nesse caso $\alpha - 1 \in \langle \bar{1} + i\bar{1} \rangle$. Portanto $\alpha(\bar{2})^{n-1}(\bar{1} + i\bar{1}) = (\bar{2})^{n-1}(\bar{1} + i\bar{1})$. ■

Já que $Z_{2^n}[i]$ é local com $Z(Z_{2^n}[i]) = \langle \bar{1} + i\bar{1} \rangle$ como seu ideal maximal, $Z(Z_{2^n}[i])$ é um aniquilador ideal e, portanto, existe um vértice adjacente a cada vértice em $\tau(Z_{2^n}[i])$, Anderson e Livingston [7]. Na verdade, para qualquer vértice α em $\tau(Z_{2^n}[i]), \alpha$ é adjacente a $(\bar{1} + i\bar{1})^{2n-1}$.

Teorema 4.2.1.3: Para $n \geq 1, |V(\tau(Z_{2^n}[i]))| = 2^{2n-1} - 1$.

Demonstração: O número de unidades em $Z_{2^n}[i]$ é $2^{2n-1} - 1 \; em \; [30]$. Assim sendo, $|V(\tau(Z_{2^n}[i]))| = 2^{2n} - 2^{2n-1} - 1 = 2^{2n-1} - 1$. ■

Teorema 4.2.1.4: Para $n > 1, diam(\tau(Z_{2^n}[i])) = 2$.

Demonstração: $\tau(Z_{2^n}[i])$ não é completo, desde $\bar{2} \; e \; \bar{1} + i\bar{1}$ são vértices em $\tau(Z_{2^n}[i])$ mas $\bar{2}(\bar{1} + i\bar{1}) \neq 0$, então para $\alpha(\bar{1} + i\bar{1})\beta(\bar{1} + i\bar{1})$ tem vértices em $\tau(Z_{2^n}[i])$ com $\alpha, \beta \in \tau(Z_{2^n}[i]) \; e \; \alpha(\bar{1} + i\bar{1})\beta(\bar{1} + i\bar{1}) \neq \bar{0}$. Então temos o caminho: $\alpha(\bar{1} + i\bar{1}) \ldots (\bar{1} + i\bar{1})^{n-1} \ldots \beta(\bar{1} + i\bar{1}), portanto \; diam(Z_{2^n}[i]) = 2$. ■

Teorema 4.2.1.5: Para $n > 1, \; g(\tau(Z_{2^n}[i])) = 3$.

Demonstração: Para $n = 2$, temos o ciclo $\bar{2} \cdots i\bar{2} \cdots \bar{2} + i\bar{2} \cdots \bar{2}$. Para $n > 2$, sempre temos os ciclos $\bar{2}^{n-1} \cdots \bar{2} \cdots i\bar{2}^{n-1} \cdots \bar{2}^{n-1}$, portanto $g(\tau(Z_{2^n}[i])) = 3$. ■

Exemplo: $V(\tau(Z_4[i])) = \{\bar{2},\ i\bar{2}, \bar{2} + i\bar{2}, \bar{1} + i\bar{1}, \bar{1} + i\bar{3}, \bar{3} + i\bar{1}, \bar{3} + i\bar{3}\ \}$.

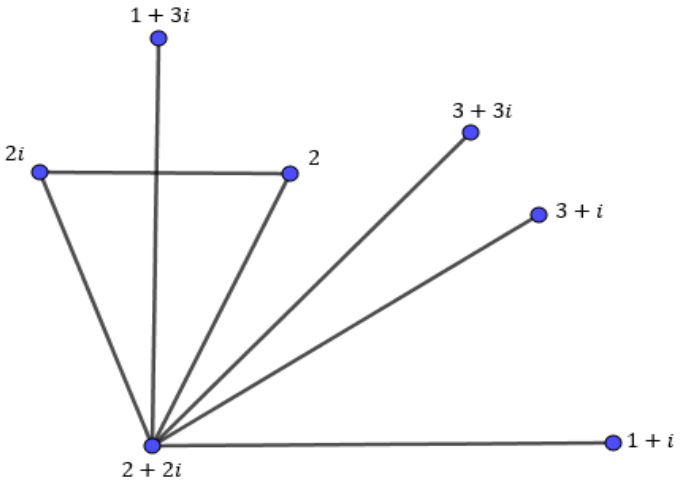

Figura 25: $\tau(Z_4[i])$

4.2.2 Grafo dos Divisores de Zero para $\mathbf{Z_{q^n}[i], q \equiv 3(mod4)}$.

Se $q \equiv 3(mod4)$, então q é um primo Gaussiano, e então $Z_q[i]$ é um corpo de decomposição para o polinômio $g(x) = x^2 + 1$ sobre o corpo Z_q *e* $Z_q[i]$ é isomorfo para o corpo $Z[i]/\langle q \rangle$. Então, neste caso $Z_q[i]$ não tem divisores de zero diferente de zero.

Se $n > 1$, então $Z_{q^n}[i] \cong Z[i]/\langle q^n \rangle$ é anel local com ideal maximal $\langle q \rangle$. Portanto $V\left(\tau(Z_{q^n}[i])\right) = \langle \bar{q} \rangle \backslash \{\bar{0}\}$.

Para qualquer vértice $\alpha\bar{q}$ em $\tau(Z_{q^n}[i])$, $\alpha\bar{q}$ é adjacente para $\bar{q}^{n-1}$. Na verdade, neste caso, se $\alpha\bar{q}$ é um vértice em $\tau(Z_{q^n}[i])$, então $\alpha\bar{q}$ é adjacente a cada elemento em $\langle \bar{q}^{n-1} \rangle \backslash \{\bar{0}\}$.

Agora, para determinar o número de vértices em $\tau(Z_{q^n}[i])$.

Teorema 4.2.2.1: Para $n > 1, \left|V\left(\tau(Z_{q^n}[i])\right)\right| = q^{2n-2} - 1$.

Demonstração: O número de unidades em $Z_{q^n}[i]$ é $q^{2n} - q^{2n-2}$. Cross [20]. Assim sendo, $\left|V\left(\tau(Z_{q^n}[i])\right)\right| = |\langle \bar{q} \rangle| - 1 = q^{2n} - (q^{2n} - q^{2n-2}) - 1 = q^{2n-2} - 1$.

É claro que $\tau(Z_{q^2}[i])$ é um grafo completo K_{q^2-1} e então $diam\left(\tau(Z_{q^n}[i])\right) = 1$. Para $n > 2$, $Z_{q^n}[i]$ não é completo e $diam\left(\tau(Z_{q^n}[i])\right) = 2$, visto que se $\alpha\bar{q}, \beta\bar{q}$ são vértices em $\tau(Z_{q^n}[i]), \alpha, \beta \in Z_{q^n}[i], e\ \alpha\bar{q}, \beta\bar{q} \neq \bar{0}$, então temos $\alpha\bar{q} \neq \bar{q}^{n-1}$ e $\beta\bar{q} \neq \bar{q}^{n-1}$. Assim, temos o caminho $\alpha\bar{q} \ldots \bar{q}^{n-1} \ldots \beta\bar{q}$, portanto o resultado. ■

Teorema 4.2.2.2: Para $n > 1, g\left(\tau(Z_{q^n}[i])\right) = 3$.

Demonstração: Se $n = 2, então\ \tau(Z_{q^n}[i])$ é completo com mais de 3 vértices, e assim $g\left(\tau(Z_{q^n}[i])\right) = 3. Se\ n > 2$, sempre temos o ciclo $\bar{q}^{n-1} \ldots \bar{q} \ldots i\bar{q}^{n-1} \ldots \bar{q}^{n-1}$, portanto $g\left(\tau(Z_{q^n}[i])\right) = 3$. ■

4.2.3 Grafo dos Divisores de Zero para $\mathbf{Z_{p^n}[i], p \equiv 1(mod4)}$.

Seja p um inteiro primo que seja congruente com 1 módulo 4. Então, há um inteiro c tal que $c^2 \equiv -1\ (mod p)$, e existe também um $a, b \in Z$ de tal modo que $p = a^2 + b^2 = (a + ib)(a - ib)$, além disso, $a + ib\ e\ a - ib$ são primos Gaussianos em $Z[i]$. Assim, os ideais $(a + ib)\ e\ (a - ib)$ são os únicos ideais maximais em $Z[i]$ contendo p, já que $Z[i]$ é um domínio de factorização única. Por isso, temos $Z_p[i] \cong \frac{Z[i]}{\langle p \rangle} \cong \left(\frac{Z[i]}{\langle a+ib \rangle}\right) \times (Z[i]/\langle a - ib \rangle)$. Os ideais $\langle \bar{a} + i\bar{b} \rangle\ e\ \langle \bar{a} - i\bar{b} \rangle$ são os únicos ideais maximais em $Z_p[i]$. O número de unidades em $Z_p[i]$ é $(p - 1)^2$, Cross [20] o que implica que $\left|V\left(\tau(Z_{p^n}[i])\right)\right| = p^2 - (p-1)^2 - 1 = 2p - 2$.

Exemplo: $Z_9 = \{\bar{3}, \bar{6}, \bar{3}i, \bar{6}i, \bar{3} + \bar{3}i, \bar{3} + \bar{6}i, \bar{6} + \bar{3}i, \bar{6} + \bar{6}i\}$

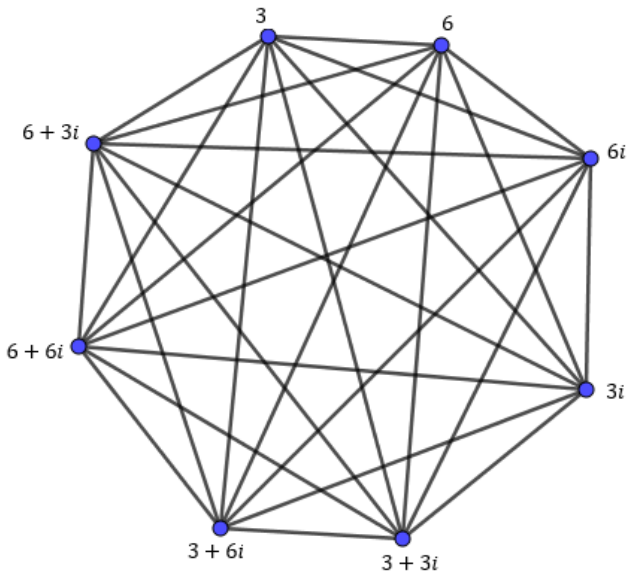

Figura 26: $\tau(Z_9[i])$

Além disso, $\tau(Z_p[i])$ é o grafo bipartido completo $K_{p-1,\ p-1}$ e, portanto, $diam\left(\tau(Z_p[i])\right) = 2$ e $g\left(\tau(Z_p[i])\right) = 4$.

Para investigar o caso mais geral, para $p \equiv 1\,(mod 4), n > 1\ e\ p = a^2 + b^2$. Então $p^n = (a^2 + b^2)^n = (a + ib)^n(a - ib)^n$, e, portanto, p^n está contido apenas dois ideais maximais em $Z[i]$, ou seja, $\langle \bar{a} + i\bar{b}\rangle\ e\ \langle \bar{a} - i\bar{b}\rangle$. Por isso, temos: $Z_{p^n}[i] \cong Z[i]/\langle p^n\rangle \cong (Z[i]/\langle (a + ib)^n\rangle) \times (Z[i]/\langle (a - ib)^n\rangle)$.

Neste caso, $V\left(\tau(Z_{p^n}[i])\right) = \left(\langle \bar{a} + i\bar{b}\rangle \cup \langle \bar{a} - i\bar{b}\rangle\right)\backslash\{\bar{0}\}$ .O número de unidades em $Z_{p^n}[i]$ é $(p^n - p^{n-1})^2$, Cross [20], portanto, temos o seguinte teorema.

Teorema 4.2.3.1: Para $n > 1, V\left(\tau(Z_{p^n}[i])\right) = 2p^{2n-1} - p^{2n-2} - 1$.

Teorema 4.2.3.2: Para $n > 1, diam\left(\tau(Z_{p^n}[i])\right) = 3$.

Demonstração: Seja $p = a^2 + b^2$. É claro que $d(\bar{a} + i\bar{b}, \bar{a} - i\bar{b}) > 1$. Se existe $\bar{x} + i\bar{y}$ de modo que $(\bar{a} - i\bar{b})(\bar{x} + i\bar{y}) = \bar{0} = (\bar{a} + i\bar{b})(\bar{x} + i\bar{y})$, então p^n divide $(ax + by), (ay - bx), (ax - by)\ e\ (ay + bx)$. Então, p^n divide $2ax\ e\ 2by$ e, portanto, p^n divide $x\ e\ y$, isto é, $\bar{x} + i\bar{y} = \bar{0}$. Assim, $d(\bar{a} + i\bar{b}, \bar{a} - i\bar{b}) > 2$. Assim, temos o caminho $(\bar{a} + i\bar{b}) \dots (\bar{a} + i\bar{b})^{n-1}(\bar{a} - i\bar{b})^n \dots (\bar{a} + i\bar{b})^n(\bar{a} - i\bar{b})^{n-1} \dots (\bar{a} - i\bar{b})$ e visto que o diâmetro de um grafo de divisor de zero de um anel comutativo finito com unidade é sempre inferior ou igual a 3, em $[7]$ obtemos o resultado. ■

Teorema 4.2.3.3: Para $n > 1, g\left(\tau(Z_{p^n}[i])\right) = 3$.

Demonstração: Se $n = 2$, então considere o ciclo $\bar{p} \dots \bar{p} + i\bar{p} \dots i\bar{p} \dots \bar{p}$. Para $n > 2$, sempre temos o ciclo $(\bar{p})^{n-1} \dots \bar{p} \dots i(\bar{p})^{n-1} \dots (\bar{p})^{n-1}$, portanto $g\left(\tau(Z_{p^n}[i])\right) = 3$. ■

4.3 Grafo dos Divisores de Zero para $\mathbf{Z_n[i]}$

Nesta seção, os inteiros q e q_j são usados implicitamente para denotar primos congruente com $3\ modulo\ 4$, enquanto $p\ e\ p_s$ denotam números inteiros congruentes com $1\ módulo\ 4$.

O caso geral será agora investigado. Assumindo que $n = \prod_{j=1}^{m} {t_j}^{n_j}$. A função $\theta: Z_n[i] \to \prod_{j=1}^{m} Z_{{t_j}^{n_j}}[i]$ de tal modo que $\theta(\bar{x} + i\bar{y}) = \left(\left(x\ mod(t_j)\right)^{n_j}\right) + i\left(y\ mod(t_j)^{n_j}\right)_{j=1}^{m}$é um isomorfismo.

Seja agora $n = 2^k \times \prod_{j=1}^{m} {q_j}^{\alpha_j} \times \prod_{s=1}^{l} {p_s}^{\beta_s}$. Então, o número de unidades em $Z_n[i]$ é $2^{2k-1} \times \prod_{j=1}^{m}\left({q_j}^{2\alpha_j} - {q_j}^{2\alpha_j - 2}\right) \times \prod_{s=1}^{l}\left({p_s}^{\beta_s} - {p_s}^{\beta_s - 1}\right)^2$, portanto, temos o seguinte lema.

Lema 4.3.1: Seja $n = 2^k \times \prod_{j=1}^{m} {q_j}^{\alpha_j} \times \prod_{s=1}^{l} {p_s}^{\beta_s}$. Então $\left|V\left(\tau\left(Z_{p^n}[i]\right)\right)\right| = n - \left(2^{2k-1} \times \prod_{j=1}^{m}\left({q_j}^{2\alpha_j} - {q_j}^{2\alpha_j-2}\right) \times \prod_{s=1}^{l}\left({p_s}^{\beta_s} - {p_s}^{\beta_s-1}\right)^2\right) - 1$.

Diâmetro e Cintura para $\tau\left(Z_{p^n}[i]\right)$

É mostrado em Axtell [10] que se $R_1 \, e \, R_2$ são anéis comutativos com identidade e sem divisores de zero diferente de zero, então $diam(R_1 \times R_2) = 3$. Usando isso juntamente com os resultados acima, obtemos o seguinte teorema.

Teorema 4.3.2: Seja n um inteiro positivo maior que 1. Então:

1) $diam\left(\tau(Z_n[i])\right) = 1$ se e somente se $n = q^2$;
2) $diam\left(\tau(Z_n[i])\right) = 2$ se e somente se $n = p \; ou \; n = 2^m \; com \; m \geq 2 \; ou \; n = q^m \; com \; m \geq 3$;
3) $diam\left(\tau(Z_n[i])\right) = 3$ se e somente se $m = p^m \; com \; m \geq 2 \; ou \; n$ é divisível pelo menos por dois primos distintos.

Foi mostrado anteriormente que, para qualquer $t \, e \, n > 1, g\left(\tau(Z_{t^n}[i])\right) = 3$ e $g\left(\tau\left(Z_p[i]\right)\right) = 4$. Agora, estudamos mais casos.

Teorema 4.3.3: Seja $n = \prod_{j=1}^{m} {t_j}^{n_j}$ seja a fatorização prima de n. Então:

1) Se $n_k > 1 \, para \; algum \; k, então \; g\left(\tau(Z_n[i])\right) = 3$;
2) Se $n_k = 1 \, para \; todo \; k \; e \; m \geq 3, então \; g\left(\tau(Z_n[i])\right) = 3$;
3) Se $n = p_1 \times p_2 \; ou \; n = p_1 \times q \; ou \; n = p_1 \times 2, então \; g\left(\tau(Z_n[i])\right) = 3$;
4) Se $n = q_1 \times q_2, então \; g\left(\tau(Z_n[i])\right) = 4$;
5) Se $n = 2 \times q, então \; g\left(\tau(Z_n[i])\right) = 4$.

Demonstração: 1) suponha que $n_k > 1$. Definimos $\bar{x}_j = \begin{cases} \bar{t}_k \; j = k \\ \bar{0} \; j \neq k \end{cases}$ e seja $\bar{x} = \left(\bar{x}_j\right)_{j=1}^{m} \in \prod_{j=1}^{m} {t_j}^{n_j}[i]$. Então consideramos o ciclo: $\bar{x}^{n_k-1} \ldots i\bar{x} \ldots \bar{x}^{n_k-1} + i\bar{x}^{n_k-1} \ldots \bar{x}^{n_k-1}$, portanto $g\left(\tau(Z_n[i])\right) = 3$.

2) Seja $\bar{x}_j = \begin{cases} \bar{1} \; j = 1 \\ \bar{0} \; j \neq 1 \end{cases}$, $\bar{y}_j = \begin{cases} \bar{1} \; j = 2 \\ \bar{0} \; j \neq 2 \end{cases}$ $e \; \bar{z}_j = \begin{cases} \bar{1} \; j = 3 \\ \bar{0} \; j \neq 3 \end{cases}$ $e \; seja \; \bar{x} = \left(\bar{x}_j\right)_{j=1}^{m}$ e $\bar{y} = \left(\bar{y}_j\right)_{j=1}^{m}$, e $\bar{z} = \left(\bar{z}_j\right)_{j=1}^{m}$. Então $\bar{x}, \bar{y}, \bar{z} \in \prod_{j=1}^{m} Z_{t_j}[i]$ e temos o ciclo: $\bar{x} \ldots \bar{y} \ldots \bar{z} \ldots \bar{x}$, portanto $g\left(\tau(Z_n[i])\right) = 3$.

3) Seja $p_1 = a^2 + b^2$. Então temos ciclos:

$\left(\bar{a} + i\bar{b}, \bar{0}\right) \ldots (\bar{0}, \bar{1}) \ldots \left(\bar{a} - i\bar{b}, \bar{0}\right) \ldots \left(\bar{a} + i\bar{b}, \bar{0}\right)$, portanto $g\left(\tau(Z_n[i])\right) = 3$.

Para 4) e 5). Em Axtell [10] ■

Exemplo: $Z_5 = \{\bar{2} + \bar{1}i, \bar{2} + \bar{4}i, \bar{3} + \bar{1}i, \bar{3} + \bar{4}i, \bar{1} + \bar{2}i, \bar{1} + \bar{3}i, \bar{4} + \bar{2}i, \bar{4} + \bar{3}i\}$

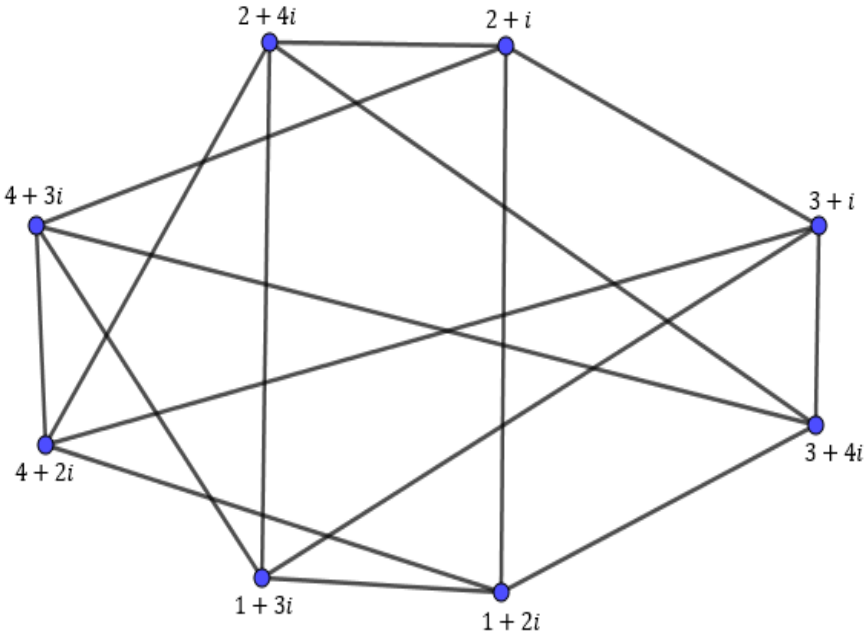

Figura 27: $\tau(Z_5[i])$

4.3.1 Quando $\tau(\mathbf{Z_n}[\mathbf{i}])$ É completo ou bipartido completo?

Foi mostrado em Anderson e Livingston [7] que, para um anel comutativo $R, \tau(R)$ é completo se e somente se $R \cong Z_2 \times Z_2$ ou $xy = 0$ para todo o $x, y \in \tau(R)$.

Teorema 4.3.1.1. O grafo $\tau(Z_n[i])$ é completo se e somente se $n = q^2$.

Demonstração. Foi mostrado anteriormente que se $n = q^2$, então, $\tau(Z_n[i])$ é um grafo completo. Assim Suponha que $\tau(Z_n[i])$ é completo. Então n é um número composto não divisível por a^3 para qualquer número primo a, uma vez que neste caso $\bar{a}$ não é adjacente a $i\bar{a}$. Além disso, n é não é divisível por dois primos distintos a, b, uma vez que neste caso, $\bar{a}$ é um vértice em $\tau(Z_n[i])$, mas $\bar{a}$ não é adjacente a $i\bar{a}$. Claramente $p \nmid n$, pois se $p = a^2 + b^2$, então $\bar{p}$ não é adjacente para $\bar{a} + i\bar{b}$, temos também$2 \nmid n$, uma vez que $\bar{1} + i\bar{1}$ não é adjacente a $\bar{2}$. Então $n = q^2$. ■

É claro que se $\tau(R)$ é um grafo bipartido completo $K_{m,n}$ com $min\{m, n\} \geq 2$, então $g(\tau(R)) = 4$, então, se $\tau(R)$ contém um ciclo com comprimento 3, não pode ser um grafo bipartido completo ou mesmo bipartido.

Lema 4.3.3.2: Seja $R = R_1 \times R_2$. Então $\tau(R)$ é um grafo bipartido completo se e somente se $R_1 e\ R_2$ são domínios de integridade.

Demonstração: Se $R = R_1 \times R_2$, onde $R_1 e\ R_2$ são domínios de integridades, então $\tau(R)$ é um grafo bipartido completo com $A = \{(x, 0): x \in R_1 \backslash \{0\}\} e\ B = \{(0, b): b \in R_1 \backslash \{0\}\}$ como o dois

conjuntos disjuntos de vértices, de modo que todo vértice em A seja adjacente a cada vértice em B, e não temos outra adjacência. Agora, se R_1 não é um domínio de integridade, com $x, y \in R_1 \backslash \{0\}\, e\, xy = 0$, então temos o 3-ciclo $(x,0) \dots (y,0) \dots (0,1) \dots (x,0)$, então $\tau(R)$ não é um grafo bipartido completo. ■

Se R é um produto direto de mais de dois domínios de integridades não triviais, então R é reduzido e a interseção de dois ideais principais não é trivial, então, $\tau(R)$ é grafo bipartido não completo, Akbari [2]. Então, se $p \equiv 1\ (mod 4)$, com $p = a^2 + b^2$, então $\tau(Z_p[i])$ é um grafo bipartido completo, já que $Z_p[i] \cong Z[i]/\langle p\rangle \cong Z[i]/\langle a + ib\rangle \times Z[i]/\langle a - ib\rangle$. E se $q_1\, e\, q_2$ são dois primos, tais que $q_j \equiv 3\ (mod 4)$, para cada j, então $\tau(Z_{q_1 q_2}[i])$ é um grafo bipartido completo, já que $Z_{q_1 q_2}[i] \cong Z_{q_1}[i] \times Z_{q_2}[i]$, um produto direto de dois corpos. É claro que $\tau(Z_4[i])$ não é um grafo bipartido completo, de forma semelhante $\tau(Z_{q^2}[i])$ não é um grafo bipartido completo, já que é completo em mais de dois vértices. $\tau(Z_{p^2}[i])$ não é um grafo bipartido completo, uma vez que se $p = a^2 + b^2$, então temos o 3-ciclo $\bar{p}(\bar{a} + i\bar{b}) \dots (\bar{a} - i\bar{b}) \dots i\bar{p}(\bar{a} + i\bar{b}) \dots \bar{p}(\bar{a} + i\bar{b})$. Se a é um número primo, então, $\tau(Z_{a^3}[i])$ não é um grafo bipartido completo, uma vez que temos o 3-ciclo $\bar{a} \dots \bar{a}^2 \dots i\bar{a}^2 \dots \bar{a}$. Agora, pode-se concluir facilmente com o seguinte teorema.

Teorema 4.3.3.3: O grafo $\tau(Z_n[i])$ é bipartido completo se e somente se $n = p$ ou $n = q_1 q_1$.

Em [7]. Para um anel finito R, se $\tau(R)$ é um grafo de estrelas, então $R \cong Z_2 \times F$, onde F é um corpo finito com $|F| \geq 3$ ou R é local com ideal maximal M satisfazendo $\frac{R}{M} \cong Z_2, M^3 = \{0\}, e\ |M^2| \leq 2$.

Teorema 4.3.3.4: Para cada $n, \tau(Z_n[i])$ nunca é um grafo de estrelas.

Demonstração: Assumindo $\tau(Z_n[i])$ é um grafo de estrela. Se $Z_n[i] \cong Z_2 \times F$, então $n^2 = |Z_n[i]| = |Z_2 \times F| = 2 \times a^k$, para um número inteiro a. Portanto $n = 2^m, m > 1$. Se $Z_n[i]$ é local, então qualquer $n = 2^m\ ou\ n = q^m,\ m > 1$, Abu Osba [1], além disso, $2\ divide\ n$, então novamente $n = 2^m, m > 1$. Mas neste caso, temos o ciclo $\bar{2}^{m-1} \dots \bar{2} + i\bar{2} \dots i\bar{2}^{m-1} \dots \bar{2}^{m-1}$, uma contradição. Portanto $\tau(Z_n[i])$ nunca é um grafo de estrelas. ■

4.3.2 Quando o Número Dominante para $\boldsymbol{\tau(Z_n[i])}$ é **1 ou 2**?

Agora, é caracterizada quando o número dominante do grafo $\tau(Z_n[i])$ é um ou dois.

Teorema 4.3.2.1: O número dominante $\delta(\tau(Z_n[i])) = 1$ se e somente se $n = 2^m\ ou\ n = q^m$ onde $m > 1$.

Demonstração: Para $m > 1, se\ n = 2^m$, então, cada elemento em $\tau(Z_n[i])$ é adjacente a $(\bar{1} + i\bar{1})^{2n-1}\ e\ se\ n = q^m$, então cada elemento é adjacente a $\bar{q}^{m-1}$. Se houver um vértice

adjacente a qualquer outro vértice, então $Z_n[i]$ é local ou $Z_n[i] \cong Z_2 \times F$, onde F é um corpo finito, em [7] mas Z_n é local se e somente se $n = 2^m \; ou \; n = q^m \; e \; se \; Z_n[i] \cong Z_2 \times F, então \; n^2 = |Z_n[i]| = |Z_2 \times F| = 2 \times a^k$, para algum número primo a, portanto, $n = 2^m$. ■

Teorema 4.3.2.2: O número dominante $\delta(\tau(Z_n[i])) = 2$ se e somente se $n = p^m$ ou $n = a^m b^k \; com \; a \; e \; b$ são primos distintos e não congruentes com $1 \; módulo \; 4$.

Demonstração: Se $n = p^m$, com $p = a^2 + b^2$, então $\{(a+ib)^m, (a-ib)^m\}$ é o menor dominante o conjunto em $\tau(Z_n[i])$. Se $n = a^m b^k$, então $\tau(Z_{a^m}[i])$ contém um vértice α que é adjacente a qualquer outro vértice em $\tau(Z_{a^m}[i]) \; e \; \tau(Z_{b^k}[i])$ contém um vértice β que é adjacente a qualquer outro vértice em $\tau(Z_{b^k}[i])$. Assim, o conjunto $\{(\alpha, 0), (0, \beta)\}$ é um conjunto dominante em $\tau(Z_{a^m}[i]) \times \tau(Z_{b^k}[i]) \approx \tau(Z_n[i])$ de menor cardinalidade. Portanto $\delta(\tau(Z_n[i])) = 2$.

Assumindo $\delta(\tau(Z_n[i])) = 2, n = \prod_{j=1}^{k} {a_j}^{n_j} \; com \; k \geq 3$, e o conjunto dominante $\left\{(b_j)_{j=1}^{k}, (c_j)_{j=1}^{k}\right\}$ em $V\left(\tau\left(\prod_{j=1}^{k} {Z_{a_j}}^{n_j}\right)\right)$. Definimos $x_j = \begin{cases} \bar{1} \; j \neq k \\ \bar{0} \; j = k \end{cases}$ e assumindo que $(b_j)_{j=1}^{k} \times (x_j)_{j=1}^{k} = (\bar{0})_{j=1}^{k}$. Então $b_j = \bar{0} \; para \; todo \; j \neq k \; e \; b_j \neq \bar{0}$. Definimos

$$y_j = \begin{cases} \bar{1} \; j \neq 1 \\ \bar{0} \; j = 1 \end{cases}.$$

Então $(b_j)_{j=1}^{k} \times (y_j)_{j=1}^{k} \neq (\bar{0})_{j=1}^{k}$, o que implica que $(c_j)_{j=1}^{k} \times (x_j)_{j=1}^{k} = (\bar{0})_{j=1}^{k}$. Então $c_j = \bar{0} \; para \; todo \; j \neq 1 \; e \; c_1 \neq \bar{0}$. Agora definimos $z_j = \begin{cases} \bar{1} & j = 1 \\ \bar{1} & j = k \\ \bar{0} \; outros \; casos \end{cases}$.

Então $(b_j)_{j=1}^{k} \times (z_j)_{j=1}^{k} \neq (\bar{0})_{j=1}^{k} \; e \; (c_j)_{j=1}^{k} \times (z_j)_{j=1}^{k} \neq (\bar{0})_{j=1}^{k}$, uma contradição.

Assumindo que $n = p^m c^k, com \; p = a + ib$ e o conjunto dominante $\{(\alpha, \beta), (\gamma, \eta)\}$ em $\tau(Z_{p^m} \times Z_{c^k})$. Suponha que $(\bar{a} + i\bar{b}, 1) \times (\alpha, \beta) = (\bar{0}, \bar{0})$. Então $(\bar{a} + i\bar{b})^{m-1}(\bar{a} - i\bar{b})^m \; divide \; \alpha \; e \; \beta = \bar{0}$. Assim $\eta \neq 0$, caso contrário $(\bar{1}, \bar{0}) \times (\alpha, \bar{0}) \neq (\bar{0}, \bar{0})$ e $(\bar{1}, \bar{0}) \times (\gamma, \bar{0}) \neq (\bar{0}, \bar{0})$. Portanto $(\bar{a} - i\bar{b}, 1) \times (\gamma, \eta) \neq (\bar{0}, \bar{0})$ o que implica que $(\bar{a} - i\bar{b}, 1) \times (\alpha, 0) = (\bar{0}, \bar{0})$, assim $(\bar{a} + i\bar{b})^m (\bar{a} - i\bar{b})^{m-1} \; divide \; \alpha, \; portanto \; \bar{p}^m = (\bar{a} + i\bar{b})^m (\bar{a} - i\bar{b})^m \; divide \; \alpha, i.e., \alpha = \bar{0}$ uma contradição. Assim $= a^m b^k$ com $a \; e \; b$ são primos não congruentes com $1 \; módulo \; 4$.

Finalmente se n é divisível por apenas um primo, então $n = p^m$, caso contrário $\beta(\tau(Z_n)) = 1$.

■

4.3.3 Quando $\tau(\mathbf{Z_n}[\mathbf{i}])$ é planar?

Proposição 4.3.3.1: O grafo é planar se e somente não contém subgrafo homeomórfico para $K_5 \; ou \; K_{3,3}$.

Teorema 4.3.3.2: O grafo $\tau(Z_n[i])$ é planar se e só se $n = 2 \; ou \; 4$.

Demonstração: Se n é divisível por dois primos distintos $a \; e \; b$, então $Z_n[i]$ tem um fator direto da forma $Z_{a^n}[i] \times Z_{b^n}[i]$, e por isso contem um subgrafo homeomórfico para $K_{3,3}$, desde $|Z_n[i]| = n^2 \geq 4 \; para \; cada \; n > 1$. Então suponha que $n = a^m$ para algum primo inteiro a. Se $a = p = x^2 + y^2$, então $Z_n[i] \cong (Z[i]/\langle x + iy\rangle) \times (Z[i]/\langle x - iy\rangle)$ com $|(Z[i]/\langle x + iy\rangle)| = |(Z[i]/\langle x - iy\rangle)| = p^m \geq 5$, assim $\tau\left(Z_{p^m}[i]\right)$ não é planar Akbari [2]. Se $a = q$ então $m > 1$ e $\left|Z_{q^m}[i]/\langle \bar{q}\rangle\right| = \frac{q^{2m}}{q^{2m-2}} = q^2 \geq 9$ e $\left|Z_{q^m}[i]\right| \geq 9^2 = 81$, assim $\tau\left(Z_{q^m}[i]\right)$ não é planar. Se $a = 2 \; e \; m = 1$, então $\tau(Z_2[i])$ tem apenas um vértice e sem arestas o que mostra que $\tau(Z_2[i])$ é planar. Então suponha que $m > 2$, então $|Z_{2^m}[i]| = \frac{2^{2m}}{2^{2m-1}} = 2 \; e \; |Z_{2^m}[i]| \geq 64$, assim $\tau\left(Z_{q^m}[i]\right)$ não é planar Akbari [2]. Por isso acabamos com $n = 2^2 = 4$, e neste caso o grafo $\tau(Z_4[i])$ é planar. ■

4.3.4 Quando $\tau(\mathrm{Z_n[i]})$ *é regular?*

Agora, estudamos quando o grafo $\tau(Z_n[i])$ é regular. Mas primeiro, vamos provar o seguindo o teorema.

Teorema 4.3.4.1: Seja t um inteiro primo ímpar, $n > 1 \; e \; k$ um número inteiro.

a) Se $1 \leq k < \frac{n}{2}, então \; \tau(Z_{t^n}[i]) \; tem \; um \; vértice \; de \; grau \; t^{2k} - 1$.
b) Se $\frac{n}{2} \leq k < n, \; então \; \tau(Z_{t^n}[i]) \; tem \; um \; vértice \; de \; grau \; t^{2k} - 2$.

Demonstração: Seja $k \in \{1, 2, 3, \ldots, n-1\}$ e considere o vértice $v = (t^n - t^k)(\bar{1} + i\bar{1})$. Claramente, $t^{n-k}(\bar{1} + i\bar{1}) \in N(v)$. Para determinar $N(v)$, seja $\bar{a} + i\bar{b}$ ser um vértice em $\tau(Z_{t^n}[i])$ com $(\bar{0}, \bar{0}) \neq (\bar{a}, \bar{b}) \neq (\overline{t^n - t^k}, \overline{t^n - t^k})$. Então $\bar{a} + i\bar{b} \in N(v)$ se e somente se $(\bar{a} + i\bar{b})(t^n - t^k)(\bar{1} + i\bar{1}) = \bar{0}$.

(i) Se e somente se $(t^n - t^k)(\bar{a} - \bar{b}) = \bar{0} = (t^n - t^k)(\bar{a} + \bar{b})$
(ii) Se e somente se $(t^n - t^k)(a - b) \; e \; (t^n - t^k)(a + b)$ são múltiplos de t^n
(iii) Se e somente se $(t^{n-k} - 1)(a - b) \; e \; (t^{n-k} - 1)(a + b)$ são múltiplos de t^{n-k}
(iv) Se e somente se t^{n-k} divide ambos $a - b \; e \; a + b$, visto que $t^{n-k} \; e \; t^{n-k} - 1$ são relativamente primos.
(v) Se e somente se t^{n-k} divide ambos $2a \; e \; 2b$
(vi) Se e somente se t^{n-k} divide ambos $a \; e \; b, desde \; t \; é \; um \; primo \; ímpar$.

Isso implica que $N(v) = S\backslash\{(\bar{0}, v)\}$, onde $S = \left(t^{n-k}\left(\bar{c} + i\bar{d}\right)\right) : c, d \in \{1,2,3, \ldots t^k - 1\}$. Claramente, $\bar{0} \in S, mas\ v$ não precisa. De fato se $v \in S$, então $ct^{n-k} = dt^{n-k} = t^n - t^k$, o que implica que $c = t^k - t^{2k-n}$ e portanto, $2k - n \geq 0, i.e., k \geq \frac{n}{2}$.

Assim sendo, para $1 \leq k < \frac{n}{2}, v \notin S, enquanto\ para\ \frac{n}{2} \leq k < n$ temos $0 \leq 2k - n < n\ e\ temos\ v = (t^k - t^{2k-n})(\bar{t}^{n-k} + i\bar{t}^{n-k}) \in S$. Isso implica que

$$deg(v) = \begin{cases} |S| - 1 & 1 \leq k < \frac{n}{2} \\ |S| - 2 & \frac{n}{2} \leq k < n \end{cases} = \begin{cases} t^{2k} - 1 & 1 \leq k < \frac{n}{2} \\ t^{2k} - 2 & \frac{n}{2} \leq k < n \end{cases} \quad \blacksquare$$

Corolário 4.3.4.2: Seja t um inteiro primo ímpar e $n > 2$. Então, $\tau(Z_{t^n}[i])$ não é regular.

Para qualquer inteiro primo ímpar q tal que $q \equiv 3(mod4)$, $\tau\left(Z_q[i]\right)$ é vazio, enquanto $\tau\left(Z_{q^2}[i]\right)$ é completo. Para qualquer inteiro primo ímpar p tal que $p \equiv 1(mod4)$ e $p = a^2 + b^2$, $\tau\left(Z_p[i]\right)$ é um grafo bipartido completo, enquanto $\tau\left(Z_{p^2}[i]\right)$ não é regular, já que $N = \left(\bar{p}\left(\bar{a} + i\bar{b}\right)\right) = \langle\bar{a} - i\bar{b}\rangle\backslash\{\bar{0}\}$, mas $N\left(\bar{a} + i\bar{b}\right) = \langle\bar{p}\left(\bar{a} - i\bar{b}\right)\backslash\{\bar{0}\}\rangle \subsetneq N\left(p(a + ib)\right)$.

$\tau(Z_2[i])$ não tem arestas, $\tau(Z_4[i])$ não é regular, e para qualquer $n > 2$, $\tau(Z_{2^n}[i])$ é não regular, uma vez que $(\bar{1} + i\bar{1})^{2n-1}$ é adjacente a qualquer outro vértice, enquanto $\bar{1} + i\bar{1}$ não é.

Seja $n = \prod_{j=1}^{m} {t_j}^{n_j}, com\ t_k \neq t_s\ para\ k \neq s$. Definimos $x_j = \begin{cases} \bar{1}\ j = k \\ \bar{0}\ j \neq k \end{cases}$ e definimos $y_j = \begin{cases} \bar{1}\ j = s \\ \bar{0}\ j \neq s \end{cases}$.

Seja $\bar{x} = \left(x_j\right) \in \prod_{j=1}^{m} Z_{{t_j}^{n_j}}[i]\ e\ \bar{y} = \left(y_j\right) \in \prod_{j=1}^{m} Z_{{t_j}^{n_j}}[i]$. Então $deg(\bar{x}) = \frac{n}{{t_k}^{n_k}} \neq \frac{n}{{t_s}^{n_s}} - 1 = deg(\bar{y})$. Portanto $\tau(Z_n[i])$ não é regular. Então temos o seguinte teorema.

Teorema 4.3.4.3: O grafo $\tau(Z_n[i])$ é regular se e somente se $n = 2\ ou\ n = p\ ou\ n = q^2$.

4.3.5 Quando $\tau(\mathbf{Z_n}[\mathbf{i}])$ é Euleriano?

Agora é o momento de caracterizar, em termos de n, os casos em que o grafo $\tau(Z_n[i])$ é Euleriano, mas primeiro lembramos a seguinte proposição bem conhecida.

Proposição 4.3.5.1: O grafo conexo $\tau(R)$ é Euleriano se e somente se grau de cada vértice de $\tau(R)$ é par.

Segue-se pelo **Teorema 4.3.4.1** acima que para qualquer primo ímpar t e $n > 1$, o grafo $\tau(Z_{t^n})[i]$ contém um vértice de graus ímpar $= t^{2k} - 2$, e não é Euleriano. Se $n = 1$, $\tau\left(Z_p[i]\right)$ é o grafo bipartido completo $K_{p-1,p-1}$ e também é Euleriano. Para $t = 2$, é claro que $\tau(Z_2[i])$ é Euleriano. Para $n > 1$, O seguinte lema mostra que $\tau(Z_{2^n}[i])$ não poderia ser Euleriano.

Lema 4.3.5.2: Para $n > 1$, o grafo $\tau(Z_{2^n}[i])$ tem um vértice de grau 1.

Demonstração: Suponhamos que $(\bar{1} + i\bar{1})(\bar{x} + i\bar{y}) = \bar{0}$. Então $2^n \, divide \, (x - y) \, e \, (x + y)$ e então $2^n \, divide \, 2x \, e \, 2y$. Portanto $x = 2^{n-1}a \, e \, y = 2^{n-1}b$. Então, para obter uma solução diferente de zero para $\bar{x} + i\bar{y}$, devemos ter $a = 2m + 1 \, e \, b = 2k + 1$. Mas neste caso, $\bar{x} + i\bar{y} = 2^{n-1}\left(\overline{2m+1} + i\overline{(2k+1)}\right) = 2^{n-1}(\bar{1} + i\bar{1}). \; Assim \; deg(\bar{1} + i\bar{1}) = 1.$ ■

Reunindo os resultados acima, obtemos o seguinte Teorema.

Teorema 4.3.5.3: Para um primo inteiro $t \, e \, n \geq 1$. O grafo $\tau(Z_{t^n})[i]$ é Euleriano se e somente se $n = 1 \, e \, também \, t = 2 \, ou \, t = p \equiv 1(mod 4)$.

Para o caso geral, note primeiro que, se $n > 1$ e $(x_j)_{j=1}^n \in R = \prod_{j=1}^n R_j$, então $Ann\left((x_j)_{j=1}^n\right) = \prod_{j=1}^n Ann(x_j)$ e visto que $deg(x_j) = |Ann(x_j)| - 1$, segue que $deg\left((x_j)_{j=1}^n\right) = \left|Ann\left((x_j)_{j=1}^n\right)\right| - 1 = \left|\prod_{j=1}^n Ann(x_j)\right| - 1$, portanto $deg\left((x_j)_{j=1}^n\right)$ é mesmo se e somente se $|Ann(x_j)|$ é ímpar para todo j. Assim $\tau(R)$ é Euleriano se e somente se $|R_j|$ é ímpar para todo $j \, e \, se \, R_j$ não é um domínio de integridade, $\tau(R_j)$ é Euleriano.

Teorema 4.3.5.4: O grafo $\tau(Z_n[i])$ é Euleriano se e somente se $n = 2 \, ou \, n$ é um primo congruente com $1 \, módulo \, 4 \, ou \, n$ é um inteiro composto que é um produto distinto de primos.

4.3.6 Quando $\boldsymbol{\tau(\mathbf{Z_n}[\mathbf{i}])}$ *é local* **H**?

Um grafo em que todos os vértices tem o mesmo grau é chamado de grafo regular. Se todos os vértices em um grafo G tiverem vizinhança que sejam isomórficos para o mesmo grafo H, então G é dito ser localmente H. Um grafo G de diâmetro d é chamado de distância regular com parâmetros $\{p_{i,j}^k : 0 \leq i, j, k \leq d\}$ se para cada triplo (i, j, k) e para qualquer par (u, v) de vértices de G tal que $d(u, v) = k$, o número de vértices na distância i de u e a distância j de v é $p_{i,j}^k$, cada um desses números $p_{i,j}^k$ é independente da escolha particular de vértices. Uma classe especial de grafos regulares de distância é a dos grafos fortemente regulares. Um grafo G é chamado fortemente regular se for a distância regular do diâmetro 2.

Nesta seção, investigamos os casos em que o grafo $\tau(Z_n[i])$ é localmente H.

Teorema 4.3.6.1: O grafo $\tau(Z_n[i])$ é localmente H se e somente se $n = 2 \, ou \, n = p \, ou \, n = q^2$.

Demonstração: O grafo $\tau(Z_2[i])$ contém apenas um vértice; ou seja, $\bar{1} + i$ e assim $\tau(Z_2[i])$ é localmente $\emptyset$.

Se $n = p$, então $n = a^2 + b^2$ para alguns $a, b \in N$, e o conjunto de vértices de $\tau(Z_n[i])$ é $(\langle \bar{a} + i\bar{b} \rangle \cup \langle \bar{a} - i\bar{b} \rangle) - \{\bar{0}\}$. Nesse caso, $\tau(Z_n[i])$ é o grafo bipartido completo $K_{n-1,n-1}$. Daí o grafo $\tau(Z_n[i])$ é localmente $(n-1)\,K_1$.

Se $n = q^2$, o conjunto de vértices de $\tau(Z_n[i])$ é $\langle \bar{q} \rangle - \{\bar{0}\}$. Neste caso, $\tau(Z_n[i])$ é um grafo completo K_{n-1}. Portanto, o grafo $\tau(Z_n[i])$ é localmente K_{n-2}.

Foi mostrado em [1] que o grafo $\tau(Z_n[i])$ é regular se e somente se $n = 2\ ou\ n = p\ ou\ n = q^2$. Por isso $\tau(Z_n[i])$ não pode ser local H para qualquer outro caso. Como o caso regular. ■

Uma vez que o grafo bipartido completo regular $K_{n,n}, n \geq 2$ é fortemente regular e o grafo completo K_n é uma distância regular, pode-se deduzir o seguinte corolário.

Corolário 4.3.6.2: (a) O grafo $\tau(Z_n[i])$ é localmente H se e somente se for regular a distância se e somente se for regular.

(b) O grafo $\tau(Z_n[i])$ é fortemente regular se e somente se $n = p$.

4.3.7 Quando $\boldsymbol{\tau(Z_n[i])}$ é Halmitoniano?

Um componente de um grafo não dirigido é um subgrafo em que qualquer dois vértices são conexos uns aos outros por caminhos e ao qual não podem ser adicionados mais vértices ou arestas, preservando sua conexidade, ou seja, é um subgrafo subordinado máximo. Para um grafo G, seja $c(G)$ indicar o número de componentes. Um ciclo Hamiltoniano de um grafo G é um ciclo que contém todos os vértices de G. Um grafo é Hamiltoniano se ele contém um ciclo Hamiltoniano.

O nome "ciclo Hamiltoniano" decorre do fato de que Sir William Hamilton investigou sua existência no grafo do dodecaedro. Um dos principais problemas não resolvidos da teoria dos grafos são a obtenção de caracterizações simples para os grafos Hamiltonianos. A maioria dos teoremas existentes tem a forma, 'se G tiver limites suficientes, então G é Hamiltoniano'. Provavelmente, o mais famoso deles é o seguinte resultado.

Proposição 4.3.7.1: Se G é um grafo com $n(\geq 3)$ vértices, e se $deg(v) \geq \frac{n}{2}$ para cada vértice v, então G é Hamiltoniano.

Proposição 4.3.7.2: Se G é um grafo Hamiltoniano e S é qualquer subconjunto próprio não vazio de vértices em G, então $c(G - S) \leq |S|$.

Vamos usar essas duas proposições para caracterizar quando o grafo $\tau(Z_n[i])$ é Hamiltoniano. Vamos mostrar que $\tau(Z_n[i])$ é Hamiltoniano se e somente se $n = p\ ou\ n = q^2$.

Teorema 4.3.7.3: Para cada $m \geq 1$, o grafo $\tau(Z_{2^m}[i])$ não é Hamiltoniano.

Demonstração: O grafo $\tau(Z_2[i])$ é o grafo trivial K_1 que não é Hamiltoniano. Para $m > 1$, o vértice define $V(\tau(Z_{2^m}[i])) = \langle\bar{1} + i\rangle - \{\bar{0}\}$ e neste grafo $(\bar{1} + i)(\bar{1} - i) = \bar{2} \neq \bar{0}$ e todos os vértices são adjacentes a $(\bar{1} + i)^{2m-1}$. Também $\deg(\bar{1} + i) = 1 = \deg(\bar{1} - i)$, Em [1]. Seja $S = \{(\bar{1} + i)^{2m-1}\}$ e seja $H = \{\bar{1} + i, \bar{1} - i\}$. Então $c(\tau(Z_{2^m}[i])) - S) \geq |H| = 2 > 1 = |S|$. Portanto, segue pela **Proposição 4.3.7.2** que $\tau(Z_{2^m}[i])$ não é Hamiltoniano. ■

Teorema 4.3.7.4: O grafo $\tau(Z_{p^m}[i])$ é Hamiltoniano se e somente se $m = 1$.

Demonstração: Seja $p = a^2 + b^2$ para algum $a, b \in N$. $\tau(Z_p[i])$ é um grafo bipartido completo $K_{p-1,p-1}$ com os dois conjuntos de vértices $V_1 = \langle\bar{a} + i\bar{b}\rangle - \{\bar{0}\}$ e $V_2 = \langle\bar{a} + i\bar{b}\rangle - \{\bar{0}\}$. Portanto, é claro que $\tau(Z_{p^m}[i])$ é um grafo Hamiltoniano. Agora, seja $m > 1$, $Z_{p^m}[i] \simeq Z_{p^m} \times Z_{p^m}$, então, seja $S = \{(\bar{0}, \alpha p^{m-1}) \in Z_{p^m} \times Z_{p^m} : mdc\ (\alpha, p) = 1\}$, $H_1 = \{(\bar{1}, \alpha p) \in Z_{p^m} \times Z_{p^m} : mdc(\alpha, p) = 1\}$ e $H_2 = \{(\bar{2}, \alpha p) \in Z_{p^m} \times Z_{p^m} : mdc(\alpha, p) = 1\}$. Então $|H_1| = |H_2| \geq p - 1 = |S|$. Elementos de $H_1\ e\ H_2$ são adjacentes apenas aos elementos de S. Então $c(\tau(Z_{p^m} \times Z_{p^m}) - S) \geq |H_1| + |H_2| > |S|$. Por isso $\tau(Z_{p^m}[i])$ não é hamiltoniano. ■

Lema 4.3.7.5: Seja $m > 1$ e seja $\alpha, \beta \in \{0, q, 2q, 3q, \ldots, (q-1)q\} \subseteq Z_{q^m}[i]$ de tal modo que $(\alpha, \beta) \neq (0, 0)$. Então o conjunto $\{\bar{x} + i\bar{y} : (\bar{x} + i\bar{y})(\bar{\alpha} + i\bar{\beta}) = \bar{0}, \bar{x} + i\bar{y} \neq \bar{0}\} = \langle\bar{q}^{m-1}\rangle - \{\bar{0}\}$.

Demonstração: Suponha que $(\overline{aq} + \overline{bq}i)(\bar{x} + i\bar{y}) = \bar{0}$, onde $a, b \in \{0, 1, 2, \ldots, q-1\}$ mas nem ambos são zero. Então temos:

$ax - by = q^{m-1}l_1$.

$bx + ay = q^{m-1}l_2$.

Assim $(a^2 + b^2)x = q^{m-1}(al_1 + al_2)$ e $(a^2 + b^2)y = q^{m-1}(al_2 - bl_1)$ isso implica que $q^{m-1}|x$ e $q^{m-1}|y$, porque se $q|(a^2 + b^2)$, então $(a^{-1}b)^2 \equiv -1(mod q)$ uma contradição de fato que $q \equiv 3(mod 4)$. Portanto $\bar{x} + i\bar{y} \in \langle\bar{q}^{m-1}\rangle - \{\bar{0}\}$. ■

Teorema 4.3.7.6: O grafo $\tau(Z_{q^m}[i])$ é Hamiltoniano se e somente se $m = 2$.

Demonstração: $Z_q[i]$ é um corpo e assim $\tau(Z_q[i])$ é um grafo vazio. $\tau(Z_{q^2}[i])$ é o grafo completo K_{q^2-1}, em [1], que é um grafo Hamiltoniano. Agora seja $m > 2$. Então o conjunto de vértices de $\tau(Z_{q^m}[i]$ é $\langle\bar{q}\rangle - \{\bar{0}\})$. Seja $S = \langle\bar{q}^{m-1}\rangle\{\bar{0}\}$ e seja $H = \{\bar{\alpha} + i\bar{\beta} : \alpha, \beta \in \{0, q, 2q, 3q, \ldots, (q\ -\ 1)\ q\}, (\alpha, \beta) \neq (0, 0)\}$. Então, $H \subseteq V(\tau(Z_{q^m}[i])) - S$, e segue pelo **Lema 4.3.7.5** que $c(\tau(Z_{q^m}[i]) - S) > |H| = q^2 - 1 = |S|$. Assim, segue pela **Proposição 4.3.7.2** que $\tau(Z_{q^m}[i])$ não é Hamiltoniano. ■

Lema 4.3.7.7: Se $R = R_1 \times R_2\ com\ |reg(R_1)| > 1$ e $|Z^*(R_2)| > 1$, então $\tau(R)$ não é Hamiltoniano.

Demonstração: Seja $S = \{(0, v): v \in Z^*(R_2)\}$ e seja $H = \{(u, v): u \in reg(R_1)\ e\ v \in Z^*(R_2)\}$. Então, os elementos de H são adjacentes apenas aos elementos de S e $c(\tau(R) - S) \geq |H| = |reg(R_1)| \times |Z^*(R_2)| \geq 2|Z^*(R_2)| > |Z^*(R_2)| = |S|$. Assim $\tau(R)$ não é Hamiltoniano. ■

Teorema 4.3.7.8: Se um número inteiro n é divisível por pelo menos dois primos distintos, então $\tau(Z_n[i])$ não é Hamiltoniano.

Demonstração: Se $n = 2t$ com $mdc(2, t) = 1$, então $Z_n[i] \simeq Z_2[i] \times Z_t[i]$. Seja $S = \{(\bar{1} + i, \bar{0})\}\ e\ H = \{(\bar{1} + i, v): v \in U(Z_t[i])\}$. Então, os vértices de H são adjacentes apenas a $(\bar{1} + i, \bar{0})$ e, portanto, $c(\tau(Z_2[i] \times Z_t[i]) - S) \geq |H| > 1 = |S|$, então $\tau(Z_{2t}[i])$ não é Hamiltoniano. Para os outros casos, se $n = mk$ com $m, k > 2$ e $mdc(m, k) = 1$, então $Z_n[i] \simeq Z_m[i] \times Z_k[i]$. Se nem $Z_m[i]$ nem $Z_k[i]$ é um corpo, então o resultado segue imediatamente a partir do **Lema 4.3.7.7** Então, suponha que ambos $Z_m[i]$ e $Z_k[i]$ são corpos com $m < k$. seja $H = \{(\bar{0}, v): v \in (Z_m[i])^*\}$ e seja $S = \{(u, \bar{0}): u \in (Z_m[i])^*\}$. Então os elementos de H são adjacentes apenas aos elementos de S e $c(\tau(Z_n[i]) - S) = |H| = k^2 - 1 > m^2 - 1 = |S|$. Assim $\tau(Z_n[i])$ não é Hamiltoniano. ■

Combinando esses resultados em grafos Hamiltonianos juntamente com o **Teorema 4.3.6.1** e **Corolário 4.3.6.2**, podemos obter:

Corolário 4.3.7.9: Para $n > 2$, os seguintes são equivalentes:

1) $\tau(Z_n[i])$ é Hamiltoniano.
2) $\tau(Z_n[i])$ é localmente H.
3) $\tau(Z_n[i])$ é regular.
4) $\tau(Z_n[i])$ é a distância regular.
5) $n = p\ ou\ n = q^2$.

Teorema 4.3.7.10: Para qualquer número inteiro $n > 1$.

1) $rad(\tau(Z_n[i]) = 0$ se e somente se $n = 2$.
2) $rad(\tau(Z_n[i]) = 1$ se e somente se $n = 2^m\ ou\ q^m, onde\ m > 1$.

Foi mostrado em Anderson e Livingston [1, 2.3] que, para um anel comutativo R, o grafo $\tau(R)$ é conexo e tem diâmetro no máximo de 3. Portanto, em vista do **Teorema 4.3.7.10**, se $n \neq 2^m$ ou q^m, então $rad(\tau(Z_n[i]) \in \{2, 3\}$. Agora consideramos o caso $n = p^m$.

Teorema 4.3.7.11: Para qualquer número inteiro $m \geq 1, rad\left(\tau\left(Z_{p^m}[i]\right)\right) = 2$.

Demonstração: Seja $p = a^2 + b^2$. Conforme mostrado em [8, Teorema 20], o conjunto $\left\{(\bar{a} + \bar{b}i)^m(\bar{a} - \bar{b}i)^{m-1}, (\bar{a} + \bar{b}i)^{m-1}(\bar{a} - \bar{b}i)^m\right\}$ é um conjunto dominante mínimo de

$\tau(Z_{p^m}[i])$. Portanto $rad(\tau(Z_{p^m}[i]) > 1$. Sendo $(\bar{a} + \bar{b}i)^m(\bar{a} - \bar{b}i)^{m-1}$ é adjacente com $(\bar{a} + \bar{b}i)^{m-1}(\bar{a} - \bar{b}i)^m$, temos para qualquer vértice α de $\tau(Z_{p^m}[i])$ que não é adjacente a $(\bar{a} + \bar{b}i)^m(\bar{a} - \bar{b}i)^{m-1}$ o vértice $(\bar{a} + \bar{b}i)^{m-1}(\bar{a} - \bar{b}i)^m$, é um vizinho comum de $(\bar{a} + \bar{b}i)^m(\bar{a} - \bar{b}i)^{m-1}$ e α. Portanto, o vértice $(\bar{a} + \bar{b}i)^m(\bar{a} - \bar{b}i)^{m-1}$ tem excentricidade 2 e, portanto, $rad\left(\tau(Z_{p^m}[i])\right) = 2$. ■

O resultado a seguir determina o raio para o caso restante em que n possui pelo menos dois fatores primos distintos.

Teorema 4.3.7.12: Seja n um número inteiro positivo com pelo menos dois fatores primos distintos. Então $rad(\tau(Z_n[i]) = 2$.

Demonstração: Seja $n = t^m k$, onde t é um número primo e $mdc(t, k) = 1$. Pelo **Teorema 4.3.7.10**, $rad(\tau(Z_n[i]) > 1$. Então, seria suficiente encontrar um vértice em $\tau(Z_n[i])$ com excentricidade 2. Temos $\tau(Z_n[i]) \simeq \tau(Z_{t^m}[i] \times Z_k[i])$. Observe que o conjunto de vértices de $\tau(Z_{t^m}[i] \times Z_k[i])$ é $A_1 \cup A_2 \cup A_3 \cup A_4, onde$

$A_1 = \left\{(x, \bar{0}) : x \in Z_{t^m}[i] - \{\bar{0}\}\right\}$,

$A_2 = \left\{(\bar{0}, y) : y \in Z_k[i] - \{\bar{0}\}\right\}$,

$A_3 = \{(x, z) : x \in Z_{t^m}[i] - \{\bar{0}\}, Z^*(Z_k[i])\}$ e

$A_4 = \left\{(z, y) : z \in Z^*(Z_{t^m}[i]), y \in Z_k[i] - \{\bar{0}\}\right\}$,

onde A_3 é vazio quando $k = q_1$ para alguns q_1 e A_4 é vazio quando $t^m = q_2$ para alguns q_2. Considere o vértice $v = (a, \bar{0})$, onde a é um vértice de $\tau(Z_{t^m}[i])$ com o mínimo excentricidade. Mostraremos que v tem excentricidade 2 em $\tau(Z_{t^m}[i] \times Z_k[i])$. Como cada vértice em A_1 é adjacente a cada vértice em A_2, temos $d(v, \alpha) \leq 2$ para cada $\alpha \in A_1 \cup A_2$. Se $(x, z) \in A_3$, existe um elemento $z_1 \in Z^*(Z_k[i])\ tal\ que\ zz_1 = \bar{0}$ e, portanto, $(\bar{0}, z_1)$ é um vizinho comum de $(a, \bar{0})$ e (x, z). Assim $d(v, (x, z)) \leq 2$. Finalmente, se $(z, y) \in A_4$, então, pela escolha de a e de acordo com o **Teorema 4.3.7.10** ou o **Teorema 4.3.7.11**, temos $d(a, z) \leq 2$. Então, qualquer, $z = a$ ou $a\_z \in E(\tau(Z_{t^m}[i]))$ ou $a\ e\ z$ têm um comum vizinho z_1 em $\tau(Z_{t^m}[i])$. Portanto, se $z = a$, então $(a, \bar{0})$ é adjacente a (z, y) ou o vértice $(z_1, \bar{0})$ é um vizinho comum de $(a, \bar{0})\ e\ (z, y)$ e, portanto, em qualquer caso, temos $d(v, (z, y)) \leq 2$. Então suponha que $z = a$. Agora, se $t^m = 2$, então $a = \bar{1} + \bar{1}i = z\ e\ (a, \bar{0})$ é adjacente a (z, y), o que implica que $d(v, (z, y)) = 1$. Se $t^m \neq 2$, então a tem um vizinho x_1 em $\tau(Z_{t^m}[i])$. e, portanto $(x_1, \bar{0})$ é um vizinho comum de $(a, \bar{0})\ e\ (z, y)$, o que implica que $d(v, (z, y)) \leq 2$. Portanto, o vértice v tem excentricidade no máximo 2 e, portanto, sua excentricidade é 2. Assim $rad(\tau(Z_n[i]) = 2$.
■

Resumindo os resultados nos três teoremas desta seção, temos: para quaisquer inteiros $n > 1, m > 1\ com\ n \neq q\ para\ qualquer\ q$,

$$rad(\tau(Z_n[i]) = \begin{cases} 0 & n = 2 \\ 1 & n = 2^m ou\ q^m \\ 2 & outro\ caso \end{cases}$$

4.4 O Grafo de Linha do Grafo de Divisor de Zero para o Anel de Inteiros Gaussianos Modulo $\mathbf{n}$.

Definição 4.4.1: O grafo de Linha é denotado por $L(G)$ e representa a adjacência entre as arestas do grafo G.

Cada vértice de $L(G)$ representa uma aresta em G.

Dois vértices de $L(G)$ são adjacentes se e somente suas arestas correspondentes compartilham um mesmo vértice em G, ou seja, são adjacentes em G.

4.4.2 Quando $\mathbf{L}\big(\boldsymbol{\tau}(\mathbf{Z_n}[\mathbf{i}])\big)$ *é Euleriano?*

Agora, é caracterizada quando o grafo de linha $L\big(\tau(Z_n[i])\big)$ é Euleriano. Antes de prosseguir, provamos o seguinte Lema.

Lema 4.4.2.1: (i) Cada vértice de $\tau(Z_n[i])$ tem grau par se e somente se $n = 2, p\ ou\ n$ é um inteiro composto que é um produto de primos ímpares distintos.

(ii) Se $n = t^m, m > 2\ e\ n \neq q^2$ então $\tau(Z_n[i])$ tem um vértice de grau impar e outro de grau par.

(iii) Cada vértice de $\tau(Z_n[i])$ tem grau ímpar se e somente se $n = q^2$.

Demonstração: (i) Como o grafo G é Euleriano se e somente se cada vértice tiver um grau par. [1]

(ii) suponha que $n = t^m, t\ é\ primo, m \geq 2\ e\ n \neq q^2$. Então temos três casos.

Caso 1. $(t = 2)$ então $deg(1 + i) = 1$ e $deg(2^{m-1} + 2^{m-1}i) = 2^{2m-1} - 2$.

Caso 2. $(t\ é\ um\ primo\ ímpar\ e\ m > 2)$. Pelo **Teorema 23** [1], $\tau(Z_n[i])$ tem um vértice de grau $t^{2k-1} - 1, onde\ 1 \leq k < m/2$ e um vértice de grau $t^{2k} - 2, onde \frac{m}{2} \leq k < m$.

Caso 3. $(t = p = a^2 + b^2\ e\ m = 2)$. Já que $deg(a + ib) = |p\langle a - ib\rangle| - 1$ e $|p\langle a - ib\rangle|$ divide $\left|Z_{p^2}\right|, |p\langle a - ib\rangle|$ é ímpar e portanto $deg(a + ib)$ é mesmo.

(iii) (→) Seja $n = \prod_{j=1}^{k} {a_j}^{m_j}, k \geq 2, e\ \bar{x}_j = (x_t), onde$

$$x_t = \begin{cases} 1, & se\ t = j \\ 0, & de\ outra\ forma \end{cases}$$

Agora se todo $a_j^{'}s$ são primos ímpares, então $deg(\bar{x}_j) = \frac{n}{({a_j}^{m})} - 1$ e se $a_1 = 2$, então $deg(x_1) = (n/2^{m_1}) - 1$.

(←) Observe que, $\tau(Z_{q^2}[i]) \cong K_{q^2-1}$. Assim $deg(v) = q^2 - 2$ para cada vértice v em $\tau(Z_{q^2}[i])$.

Teorema 4.4.2.2: (i) $L(\tau(Z_n[i]))$ é grafo Euleriano se e somente se $n = 2, p, q^2\ ou\ n$, é um inteiro composto que é um produto de primos ímpares distintos. Em [16].

(ii) $L(\tau(Z_n[i]))$ o grafo Euleriano não implica necessariamente que $\tau(Z_n[i])$ é Euleriano.

4.4.3 Quando $\mathbf{L(\tau(Z_n[i]))}$ é Hamiltoniano ou Planar?

Teorema 4.4.3.1. (i) se G é um grafo de diâmetro no máximo de 2 com $|V(G)| \geq 4$, então $L(G)$ é Hamiltoniano.

(ii) O grafo de linha de um grafo Euleriano é Hamiltoniano e Euleriano.

Se $n = p, 2^m, ou\ q^m, onde\ m \geq 2, então\ diam(\tau(Z_n[i])) \leq 2$. Por outro lado, se $n = 2, p\ ou\ n$ é um inteiro ímpar composto que é um produto de primos distintos, então $\tau(Z_n[i])$ é Euleriano. Assim, obtém-se o seguinte corolário.

Corolário 4.4.3.2: (i) Se $n = p, 2^m, ou\ q^m, onde\ m \geq 2$, então $L(\tau(Z_n[i]))$ é Hamiltoniano.

(ii) Se n é um inteiro composto ímpar que é um produto de primos distintos, então $L(\tau(Z_n[i]))$ é Hamiltoniano e Euleriano.

Teorema 4.4.3.3: Um grafo não vazio G tem um grafo de linha do planar $L(G)$ se e somente se

(i) G é planar,

(ii) $\Delta(G) \leq 4$,

(iii) Se $deg_G(v) = 4, então\ v\ é\ um\ vértice\ cortado.$

Lembre-se de que $\tau(Z_n[i])$ é planar se e somente se $n = 2\ ou\ n = 4$. Mas $L(\tau(Z_4[i]))$ não é planar visto que $\Delta(\tau(Z_4[i])) = 7 > 4$. Portanto, obtemos o seguinte teorema.

Teorema 4.4.3.4: o grafo $L(\tau(Z_n[i]))$ nunca é planar.

4.4.4 Os números Cromático e Clique de $\mathbf{L(\tau(Z_n[i]))}$

Definição 4.4.4.1: Ao menor valor de k para o qual o grafo $\tau(R)$ admite uma $k-coloração$ chamamos número cromático de $\tau(R)$, e indicamos $\chi(\tau(R))$.

Definição 4.4.4.2: Dado um grafo $\tau(R)$, dizemos que $K \subseteq V(\tau(R))$ é uma clique de $\tau(R)$ se para quaisquer dois vértices $u, v \in K$ tivermos $uv \in E(V)$; ou seja, se o grafo induzido em $\tau(R)$ por K é um grafo completo. Dizemos que K é uma clique maximal se todo o $u \in V(\tau(R))\backslash K$ o conjunto $K \cup \{u\}$ não é uma clique. À clique de $\tau(R)$ com maior cardinalidade chamamos clique máxima e à sua cardinalidade número de clique de $\tau(R)$, que indicamos por $\omega(\tau(R))$.

Se R é um anel finito, então $\chi'\left(\tau(R) = \Delta(\tau(R))\right)$, a menos que $\tau(R)$ é um grafo completo de ordem ímpar. Observe que, o único grafo completo $\tau(Z_n[i])$ ocorre quando $n = q^2$. No entanto, neste caso, a ordem do grafo é $q^2 - 1$ que é uniforme, então $\chi'(\tau(Z_n[i])) = \Delta(\tau(Z_n[i]))$. Além disso, uma vez que a coloração de aresta de qualquer grafo leva a uma coloração de vértice do seu grafo de linha, obtemos $\chi\left(L(\tau(Z_n[i]))\right) = \Delta(\tau(Z_n[i]))$. Claramente, $\chi(G) \geq \omega(G)$. Por outro lado, o grafo de linha de G possui um subgrafo completo de ordem $\Delta(G)$. Assim $\omega\left(L(\tau(Z_n[i]))\right) \geq = \Delta(\tau(Z_n[i]))$. Observe que se $n = 2^m, ou\ q^m, onde\ m \geq 2$, então $\tau(Z_n[i])$ tem um vértice que é adjacente a qualquer outro vértice em $\tau(Z_n[i])$. Enquanto se $n = p^m, m \geq 1$, então $Z_{p^m}[i] \cong Z_{p^m} \times Z_{p^m}$. Assim $\Delta(Z_{p^m}[i]) = p^{2m-1} - 1$. Isso leva ao seguinte teorema.

Teorema 4.4.4.3:

$$\omega\left(L(\tau(Z_n[i]))\right) = \chi\left(L(\tau(Z_n[i]))\right)\begin{cases} 2^{2m-1} - 2, se\ n = 2^m, m \geq 2 \\ q^{2m-2} - 2, se\ n = q^m, m \geq 2, \\ p^{2m-1} - 1, se\ n = p^m, m \geq 1 \end{cases}$$

Finalmente, se $n = 2^m \prod_{j=1}^{r} {p_j}^{r_j} \prod_{j=1}^{l} q_j \prod_{j=1}^{s} {q_j}^{s_j}, onde\ s_j \geq 2\ e\ m, r_j \geq 1$, então o clique e o número cromático do grafo $L(\tau(Z_n[i]))$ é dado pelo seguinte Teorema.

Teorema 4.4.4.4: $n = 2^m \prod_{j=1}^{r} {p_j}^{r_j} \prod_{j=1}^{l} q_j \prod_{j=1}^{s} {q_j}^{s_j}, onde\ m, r_j \geq 1\ e\ s_j \geq 2$, então

$$\omega\left(L(\tau(Z_n[i]))\right) = \chi\left(L(\tau(Z_n[i]))\right) = (2^{2m-1} - 1) \prod_{j=1}^{r} \left({p_j}^{2r_{j-1}}\right) \prod_{j=1}^{s} \left({q_j}^{2s_{j-2}} - 1\right) - 1.$$

Demonstração: O resultado segue calculando $\Delta(\tau(Z_n[i]))$, uma vez que $\Delta(\tau(Z_n[i])) = \omega\left(L(\tau(Z_n[i]))\right) = \chi\left(L(\tau(Z_n[i]))\right)$. ■

Diâmetro de $L(\tau(Z_n[i]))$

Agora, encontraremos o diâmetro do grafo de linha $L(\tau(Z_n[i]))$. Primeiro, vamos provar que $diam\left(L(\tau(Z_n[i]))\right) = 2\ quando\ n = 2^m\ ou\ n = q^m$.

Lema 4.4.4.5: (i) Se $n = 2^m, m \geq 2$, então não há um $a + bi, c + di \in Z_n[i]$, onde a, b, c, d são inteiros ímpares, de modo que $(a + bi)(c + di) \equiv 0(mod4)$.

(ii) Se $n = 2^m, m \geq 2$, então não há um $a + bi, c + di \in Z_n[i]$, onde a, b, c, d são primos relativamente com q, modo que $(a + bi)(c + di) \equiv 0(modq)$.

Demonstração: (i) Suponha que $(a + bi)(c + di) \equiv 0(mod4)$. Então $ac - bd \equiv 0(mod4)$ e $ad + bc \equiv 0(mod4)$. Visto que a, b, c, d são inteiros ímpares, $a = 2a_1 + 1$,

$b = 2b_1 + 1, c = 2c_1 + 1\ e\ d = 2d_1 + 1$para algum $a_1, b_1, c_1, d_1 \in Z$. Assim $ac - bd \equiv a_1 + b_1 + c_1 + d_1 \equiv 0(mod2)$. E $ad + bc \equiv a_1 + b_1 + c_1 + d_1 \equiv 1(mod2)$, uma contradição.

(ii) Suponha que $(a + bi)(c + di) \equiv 0(modq)$. Então $ac - bd \equiv 0(modq)$ e $ad + bc \equiv 0(modq)$. Visto que a, b, c, d são primos relativamente com q, temos $a = qa_1 + a_2$, $b = qb_1 + b_2, c = qc_2 + c_2\ e\ d = qd_1 + d_2$, onde $0 < a_2, b_2, c_2, d_2 < q$. Assim

$$ac - bd \equiv a_2c_2 - b_2d_2 \equiv 0(modq) \qquad (I)$$

$$ad + bc \equiv a_2d_2 + b_2c_2 \equiv 0(modq) \qquad (II)$$

Multiplicando $(I)\ por\ c_2\ e\ (II)\ por\ d_2$ e adicionando dá $a_2\left({c_2}^2 + {d_2}^2\right) \equiv 0(modq)$. Então $q|a_2\ ou\ q|\left({c_2}^2 + {d_2}^2\right)$. Visto que $a_2 < q, q|\left({c_2}^2 + {d_2}^2\right)$. Assim sendo ${c_2}^2 + {d_2}^2 \equiv 0(modq)$, e portanto $c_2 \equiv d_2 \equiv 0(modq)$, uma contradição. ■

Então, concluímos o seguinte.

Teorema 4.4.4.6: Se $n = 2^m\ ou\ n = q^m, m \geq 2, então\ diam\left(L(\tau(Z_n[i]))\right) = 2$

Demonstração: (i) Suponha que $n = 2^m, m \geq 2$. Então,

1) $x = a2^t + b2^k i$ onde $a, b\ são\ ímpares\ e\ t \neq k\ ou\ t = k \geq \lceil m/2 \rceil$ implica que $ann(x) = \{c2^r + d2^s i : c\ e\ d\ são\ ímpares\ e\ r, s \geq m - min\{t, k\}\}$.
2) $x = a2^t(a + bi)$ onde $a, b\ são\ ímpares\ e\ t < \lceil m/2 \rceil$, então $ann(x) = \{c2^r + d2^s i : c\ e\ d\ são\ ímpares\ e\ r, s \geq m - t\} \cup \{2^{m-t-1}(c + di) : c\ e\ d\ são\ ímpares\}$.

Além disso, $d([2^t(a_1+b_1i), 2^{m-t-1}(c_1+d_1i)], [2^s(a_2+b_2i), 2^{m-s-1}(c_2+d_2i)]) = 2$, se $t \leq s < [m/2]$. Já que $[2^s(a_2+b_2i), 2^{m-t-1}(c_1+d_1i)\,] \in V\left(L(\tau(Z_n[i]))\right)$.

(ii) Suponha que $n = 2^m, m \geq 2$. Seja $x = aq^t + bq^k i \; e \; a, b \in U(Z_n)$. Então $ann(x) = \{cq^r + dq^s i : r, s \geq m - min\{t, k\}\}$. Além disso, $d([a_1q^{r_1} + b_1q^{s_1}i, c_1q^{t_1} + d_1q^{k_1}i], [a_2q^{r_2} + b_2q^{s_2}i, c_2q^{t_2} + d_2q^{k_2}i]\,) = 2$ visto que $r_1, s_1, t_2, k_2 \geq \left\lceil \frac{m}{2} \right\rceil$ o que implica $[a_1q^{r_1} + b_1q^{s_1}i, c_1q^{t_1} + d_1q^{k_1}i, a_2q^{r_2} + b_2q^{s_2}i, c_2q^{t_2} + d_2q^{k_2}i\,] \in V\left(L(\tau(Z_n[i]))\right)$. ■

Teorema 4.4.4.7: (i) Se $n = st, onde \; s \; e \; t \; são \; dois \; primos \; distintos \; e \; s \neq p \; ou \; p \neq t$, então $diam\left(L(\tau(Z_n[i]))\right) = 2$.

(ii) Se $n = st^2$ são dois primos distintos e $s, t \neq p$, então $diam\left(L(\tau(Z_n[i]))\right) = 2$.

Demonstração: Primeiro observe que $L(\tau(R)) \geq 2$, e para $n = n_1n_2$ com $mdc(n_1, n_2) = 1$, $Z_n[i] \cong Z_{n_1}[i] \times Z_{n_2}[i]$.

(i) **Caso 1:** Se $n = qp \; ou \; n = 2p$ onde $p = a^2 + b^2$, então $V\left(L(\tau(Z_n[i]))\right) = \{[(u, \alpha(a+bi)), (0, \beta(a-bi))]\} \cup \{[(0, \alpha(a+bi)), (u, \beta(a-bi))]\} \cup \{[(u, v), (0, v)]\}$.

Caso 2: Se $n = 2q \; ou \; n = q_1q_1$, então

$$V\left(L(\tau(Z_n[i]))\right) = \{[(u, v), (0, v)]\} : u, v \neq 0$$

(ii) Observe que $V\left(L(\tau(Z_n[i]))\right) = \{[(u, \alpha t), (0, \beta t)]\} \cup \{[(u, v), (0, v)]\} : u, v, \alpha, \beta \neq 0$. ■

Teorema 4.4.4.8: (i) Se $n = sp^2$, onde $s \; é \; primo \; e \; p = a^2 + b^2$, então $diam\left(L(\tau(Z_n[i]))\right) = 3$.

(ii) Se $n = {p_1}^m {p_2}^l$ onde ${p_1} = {a_1}^2 + {b_1}^2, {p_2} = {a_2}^2 + {b_2}^2$ e $m, l \geq 1$, então $diam\left(L(\tau(Z_n[i]))\right) = 3$.

(iii) Se $n = p^m t^l$, onde $p = a^2 + b^2, m \geq 1, l \geq 2$, e $mdc(p, t) = 1$, então $diam\left(L(\tau(Z_n[i]))\right) = 3$.

(iv) Se $n = s^m t^l$, onde s, t são primos distintos e $m, l \geq 2$, então $diam\left(L(\tau(Z_n[i]))\right) = 3$.

Demonstração: (i) Seja $v_1 = [(0, (a+bi)^2), (1(a-bi)^2)]$ e $v_2 = \left[\left(0, (a-bi)(a+bi)\right), \left(1(a-bi)(a+bi)\right)\right]$. Então $d(v_1, v_2) = 3$.

(ii) Seja $v = [((a_1 + b_1 i)^m, (a_2 + b_2 i)^l, (a_1 - b_1 i)^m, (a_2 + b_2 i)^l)]$. Então $d(v[(1,0)(0,1)]) = 3$.

(iii) Seja $v = [((a + bi)^m, t), ((a - bi)^m t^{l-1})]$. Então $d(v[(1,0)(0,1)]) = 3$.

(iv) Seja $v = [(s,t), (s^{m-1}, t^{l-1})]$. Então $d(v[(1,0)(0,1)]) = 3$. ■

Teorema 4.4.4.9: (i) Se R_1, R_2, R_3 são corpos e $R = R_1 \times R_2 \times R_3$, então $diam\left(L(\tau(R))\right) = 2$.

(ii) Se R_1, R_2, R_3 são anéis finitos e R_i não é corpo par algum $i \in \{1,2,3\}$ e $R = R_1 \times R_2 \times R_3$, então $diam\left(L(\tau(R))\right) = 3$.

(iii) Se $R = \prod_{i=1}^{k} R_i, onde\ k \geq 4, então\ diam\left(L(\tau(R))\right) = 3$.

Demonstração: (i) Seja $[(a_1, a_2, a_3), (b_1, b_2, b_3), (c_1, c_2, c_3), (d_1, d_2, d_3)] \in E\left(L(\tau(R))\right)$. Visto que R_1, R_2, R_3 são corpos, $(a_1, a_2, a_3)\ ou\ (b_1, b_2, b_3)$ tem exatamente duas componentes iguais a 0. Seja $(a_1, a_2, a_3) = (a_1, 0, 0)$ e $a_1 \neq 0$. Visto que $c_1 d_1 = 0, c_1 = 0\ ou\ d_1 = 0$. Sendo $c_1 = 0$, então $[(a_1, a_2, a_3), (c_1, c_2, c_3)] \in E\left(L(\tau(R))\right)$. Portanto $diam\left(L(\tau(R))\right) = 2$.

(ii) Suponha que R_1 não é corpo. Seja $x, y \in {R_1}^*$ de tal modo que $xy = 0$. Então $d([(x,0,1), (y,1,0)], [(0,1,1), (1,0,0)]) = 3$.

(iii) Seja $x = (x_j), onde\ x_j = 1\ se\ j = 1,2\ e\ 0$ de outra forma, $y = (y_j)$, onde $y_j = 1$ se $j = 3,4\ e\ 0$ de outra forma, $z = (z_j)$, onde $z_j = 1$ se $j = 2,3\ e\ 0$ de outra forma e $w = (w_j)$, onde $w_j = 1$ se $j = 1,4\ e\ 0$ de outra forma. Então $d([x,y],[z,w]) = 3$. ■

Teorema 4.4.4.10: (i) $diam\left(L(\tau(Z_n[i]))\right) = 2$ se e somente se $n = p, 2p, 2q, q_1, q_2, q_1 q_2 q_3, 2q_1 q_2, 4q,\ 2q^2, pq\ ou\ n = 2^m, q^m\ com\ m \geq 2$.
(ii) $diam\left(L(\tau(Z_n[i]))\right) = 3\ de\ outra\ forma$.

4.4.5 Cintura e Raio de $\mathrm{L}(\tau(\mathrm{Z_n}[\mathrm{i}]))$.

Teorema 4.4.5.1: $g\left(L(\tau(Z_n[i]))\right) = 3$.

Lema 4.4.5.2: Se existe um vértice $v \in L(\tau(Z_n[i]))$ com excentricidade 2, então $rad\left(L(\tau(Z_n[i]))\right) = 2$.

Demonstração: Observe que, $L(\tau(Z_n[i]))$ não tem grafo de estrelas abrangente, já que se $a, b \in V(\tau(Z_n[i]))$ de tal modo que $a \neq b\ e\ ab = 0, então\ d([a,b],[ai,bi]) > 1$. ■

Teorema 4.4.5.3: Se $n = 2^m, n = q^m, m \geq 2\ ou\ n = p^m, m \geq 1$, então $rad\left(L(\tau(Z_n[i]))\right) = 2$.

Demonstração: (1) Se $n = 2^m, m \geq 2$, então $d([2^{m-1} + 2^{m-1}i, 2][x, y]) \leq 2$ para todo $[x, y] \in V\left(L(\tau(Z_n[i]))\right)$.

(2) Se $n = q^m, m \geq 2$, então $d([q^{m-1}, q], [x, y]) \leq 2$ para todo $[x, y] \in V\left(L(\tau(Z_n[i]))\right)$.

(3) Se $n = p^m, m \geq 1$, então $d([(a + bi)^m(a - bi)^{m-1}, (a - bi)^m(a + bi)^{m-1}], [x, y]) \leq 2$ para todo $[x, y] \in V\left(L(\tau(Z_n[i]))\right)$. ■

Teorema 4.4.5.4: Se $n = r^m t$, onde $r = 2, q, ou\ p\ e\ m \geq 1, mdc(r, t) = 1$, então $rad\left(L(\tau(Z_n[i]))\right) = 2$.

Demonstração: (1) Se $r = 2, ou\ q$, então $d([(r^{m-1}, 0), (r, 1)], [(x, y), (t, s)]) \leq 2$ para todo $[(x, y), (t, s)] \in V\left(L(\tau(Z_n[i]))\right)$.

(2) Se $r = p = a^2 + b^2$, então $d = ([((a + bi)^m(a - bi)^{m-1}, 0), ((a - bi)^m(a + bi)^{m-1}, 0)\ ], [(x, y), (t, s)]) \leq 2$ para todo $[(x, y), (t, s)] \in V\left(L(\tau(Z_n[i]))\right)$. ■

Resumindo os resultados acima, obtemos o seguinte.

Teorema 4.18.5: O raio do grafo de linha $L(\tau(Z_n[i]))$ é igual a 2.

4.4.6 O Número de Dominação de $\mathrm{L}(\tau(\mathrm{Z_n}[\mathrm{i}]))$

Nesta seção, determinamos o número de dominação de $L(\tau(Z_n[i]))$ quando $n = t^m$ e t é primo.

O estudo do número de dominação do grafo de linha de G leva ao estudo do número de dominância de linha ou linha de G, isto é, $\gamma(L(G)) = \gamma'(G)$. Por outro lado, para qualquer grafo G, $\gamma_i'(G) = \gamma'(G)$. Além disso, se G é o grafo bipartido completo $K_{r,s}$, então $\gamma'(G) = \min(r, s)$, então temos o seguinte.

Lema 4.4.6.1: (i) $\gamma\left(L\left(\tau(Z_p[i])\right)\right) = \gamma_i'\left(\tau(Z_p[i])\right) = \gamma'\left(\tau(Z_p[i])\right) = p - 1$.

(ii) $\gamma\left(L\left(\tau(Z_{q_1q_2}[i])\right)\right) = \gamma_i'\left(\tau(Z_{q_1q_2}[i])\right) = \gamma'\left(\tau(Z_{q_1q_2}[i])\right) = q_1$ onde $q_1 < q_2$.

Agora, estudamos o número de dominação do grafo de linha de $\tau(Z_n[i])$ quando n é uma potência de um primo. O primeiro teorema trata o caso $n = 2^m, m \geq 2$. Aqui fazemos uso do fato de que $\tau(Z_{2^m}[i]) \cong \tau(Z_{2^{2m}}[i])$.

Teorema 4.4.6.2: Para $n = 2^m, m \geq 2$,

$$\gamma\left(L\left(\tau(Z_n[i])\right)\right) = \gamma_i'\left(\tau(Z_n[i])\right) = \gamma'\left(\tau(Z_n[i])\right) = \left\lfloor \frac{1}{2}(2^m - 1) \right\rfloor$$

Demonstração: Para $j = 1, 2, \ldots, 2m-1$, seja $A_1 = \left\{\alpha 2^{2m-j} : \alpha \in \{1, 3, \ldots, 2^j - 1\}\right\}$. Observe que os conjuntos A_j formam uma partição para os vértices de $\tau(Z_{2^{2m}})$. Seja $S = \cup_{j=1}^{m} A_j$ *e* $T = \cup_{j=m+1}^{2m-1} A_j$. Então, o conjunto S induz um subgrafo completo de $\tau(Z_{2^{2m}})$ e o conjunto T forma um conjunto independente dele. E cada vértice em A_k é adjacente a cada vértice em $\cup_{j=1}^{2m-k} A_j$. $\tau(Z_{2^{2m}})$ não tem outras arestas. Seja $D \subset E\left(\tau(Z_{2^{2m}})\right)$ ser um conjunto dominante de vértices para $L\left(\tau(Z_{2^{2m}})\right)$ com cardinalidade mínima. Como o conjunto S induz um subgrafo completo de $\tau(Z_{2^{2m}})$ da ordem $2^m - 1$, então $\gamma\left(L\left(\tau(Z_{2^m}[i])\right)\right) \geq \left\lfloor \frac{1}{2}(2^m - 1) \right\rfloor$. Por outro lado, uma vez que D domina todas as arestas no grafo completo $\langle S \rangle, D$ também domina todas as arestas juntando $S\ para\ T$, lembre-se de que T forma um conjunto independente e, portanto, $\gamma\left(L\left(\tau(Z_{2^m}[i])\right)\right) = \left\lfloor \frac{1}{2}(2^m - 1) \right\rfloor$. ■

A prova do **Teorema 4.4.6.2** mostra o conjunto T é um conjunto independente com cardinalidade máxima em $\tau(Z_{2^m}[i])$, enquanto o conjunto S induz um subgrafo completo com a ordem máxima.

Então, o seguinte corolário é obtido.

Corolário 4.4.6.3: Para $n = 2^m, m \geq 2$,

(i) $\omega\left(\tau(Z_n[i])\right) = 2^m - 1$
(ii) $\beta\left(\tau(Z_n[i])\right) = 2^m(2^m - 1)$

Como outra consequência para a prova do teorema anterior, obtém-se o seguinte corolário, que dá a sequência de grau para $\tau(Z_{2^m}[i])$.

Corolário 4.4.6.4: Para $j = 1, 2, \ldots, 2m-1$, o grafo $\tau(Z_{2^m}[i])$ tem exatamente 2^{j-1} vértices de grau $2^{2m-j} - 2$ se $1 \leq j \leq m$ e 2^{j-1} vértices de grau $2^{2m-j} - 1$ se $m + 1 \leq j \leq 2m - 1$.

Demonstração: Para cada $v \in A_j$, onde $1 \leq j \leq m, v^2 = 0$, assim $deg(v) = \left|\cup_{k=1}^{2m-j} A_k\right| - 1 = 2^{2m-j} - 1$. E para cada $v \in A_k$ onde $m + 1 \leq k \leq 2m - 1$, $v^2 \neq 0$, assim $deg(v) = \left|\cup_{k=1}^{2m-j} A_k\right| = 2^{2m-j} - 1$. ■

Além disso, a prova do teorema acima mostra que a excentricidade de 2^{2m-1} é 1 e a excentricidade de qualquer outro vértice em $\tau(Z_{2^{2m}})$ é 2, uma vez que o vértice 2 é adjacente apenas ao vértice 2^{2m-1}, e para qualquer $x \in V\left(\tau(Z_{2^m}[i])\right), 2 - 2^{2m-1} - x$, é um caminho do comprimento 2. Isso leva ao seguinte corolário.

Corolário 4.4.6.5: O centro do grafo $\tau(Z_{2^m}[i])$ é o conjunto $\{2^{m-1}(1 + i)\}$.

Em seguida, encontramos o número de dominação do grafo de linha $L(\tau(Z_n[i]))$ onde $n = q^m, m \geq 2$.

Lema 4.4.6.6: (i) Para $m \geq 2$,

1) Se $A_{kj} = \{aq^k + bq^j i : a \in U(Z_{q^{m-k}}), b \in U(Z_{q^{m-k}})\}, então\ |A_{kj}| = (q-1)^2 q^{2m-k-j-2}$ quando $1 \leq k, j \leq m-1$, $|A_{mj}| = q^{m-j} - q^{m-j-1}$ e $|A_{km}| = q^{m-k} - q^{m-k-1}$, onde $k, j \neq m$,
2) Se $S = (\cup_{\lceil m/2 \rceil \leq k, j \leq m} A_{kj}) - A_{m,n}, então\ |S| = q^{2\lceil m/2 \rceil} - 1$.

(ii) Para $m \geq 3$, se $T = \cup_{1 \leq k, j \leq \lceil \frac{m}{2} \rceil - 1} A_{kj}$, $então\ |T| = q^{2\lceil m/2 \rceil}(q^{\lceil m/2 \rceil} - 1)^2$.

Teorema 4.4.6.7: Se $n = q^m, m \geq 2$, então $\gamma\left(L(\tau(Z_n[i]))\right) = \gamma'(\tau(Z_n[i])) = \gamma_i'(\tau(Z_n[i])) = \left(\frac{1}{2}\right)(q^m - 1)$ se m é par e $\left(\frac{1}{2}\right)(q^{2\lfloor m/2 \rfloor} + 1)$ $se\ m$ é $ímpar$.

Demonstração: Seja A_{kj}, $S\ e\ T$ definidos como dados no **Lema 4.4.6.6.** Claramente, o conjunto S induz um subgrafo completo de $\tau(Z_n[i])$ com ordem máxima, se m for par e $S \cup \{q^{\lfloor m/2 \rfloor}\}$ induz um subgrafo completo de $\tau(Z_n[i])$ com ordem máxima, se m for ímpar. Por outro lado, se $m \geq 3$, então T formam um conjunto independente com cardinalidade máxima. Além disso, se um vértice v pertence ao conjunto $A_{r,s}$, então v é adjacente a cada elemento em A_{kj} onde $m - min\{r, s\} \leq k, j \leq m$ e $k, j \neq m$ ao mesmo tempo. $\tau(Z_n[i])$ não tem outras arestas. ■

Como consequência da prova do **Teorema 4.4.6.2**, concluímos o seguinte.

Corolário 4.4.6.8: Se $n = q^m, m \geq 2$, então

(i) $\omega(\tau(Z_n[i])) = q^m - 1\ se\ m$ é $par\ e\ q^{2\lfloor m/2 \rfloor}\ se\ m$ é $ímpar$,
(ii) $\beta\left(L(\tau(Z_n[i]))\right) = 1\ se\ m = 2\ e\ \beta\left(L(\tau(Z_n[i]))\right) = q^{2\lfloor m/2 \rfloor}(q^{\lceil m/2 \rceil} - 1)^2$ se $m \geq 3$.

Corolário 4.4.6.9: Seja $n = q^m, m \geq 2$ e $v = aq^r + bq^s i$ onde $a, b \in U(Z_n)$. Então

$$deg(v) = \begin{cases} q^{2min\{r,s\}} - 2, se\ r, s \geq \left\lceil \frac{m}{2} \right\rceil \\ q^{2min\{r,s\}} - 1, se\ r\ ou\ s < \left\lceil \frac{m}{2} \right\rceil \end{cases}$$

Corolário 4.4.6.10: Seja $n = q^m, m \geq 2$. Então

(i) A excentricidade de cada $v \in A_{(m-1)(m-1)}$ é 1 e a excentricidade de qualquer outro vértice $v \in \tau(Z_n[i])$ é 2,

(ii) O centro do grafo $\tau(Z_n[i])$ é o conjunto $A_{(m-1)(m-1)}$,

(iii) O raio do grafo $\tau(Z_n[i])$ é igual a 1,

(iv) O diâmetro do grafo $\tau(Z_n[i])$ é igual a 2, para $m \geq 3$.

Finalmente, encontramos o número de dominação do grafo de linha $L\big(\tau(Z_n[i])\big)$ onde $n = p^m, m \geq 2$.

Note que $Z_{p^m}[i] \cong Z_{p^m} \times Z_{p^m}$. Seja $A_{kj} = (ap^k, bp^j) : a \in U\big(Z_{p^{m-k}}\big),\ b \in U\big(Z_{p^{m-j}}\big)$. Claramente, o conjunto $A_{kj}, 0 \leq k, j \leq m$ e não ambos $k, j = m\ ou\ 0$, partição de vértices de $\tau\big(Z_{p^m} \times Z_{p^m}\big)$.

Lema 4.4.6.11: (i) Para $m \geq 2$;

1) Se $S = \big(\cup_{\lceil m/2 \rceil \leq k, j \leq m} A_{kj}\big) - A_{m,m}, então\ s = |S| = p^{2\lfloor m/2 \rfloor} - 1$,
2) Se $L_1 = \cup_{0 \leq k \leq \lceil m/2 \rceil - 1} A_{k,m}$ e $L_2 = \cup_{0 \leq k \leq \lceil m/2 \rceil - 1} A_{k,m}$, então $l = |L_1| = |L_2| = p^m - p^{\lfloor m/2 \rfloor}$,

(ii) Para $m \geq 3$,

1) Se $B = \cup_{k=1}^{\lceil m/2 \rceil - 1} \cup_{j=m-k}^{m-1} A_{kj}$, então $b = |B| = (p^m - p^{m-1})(\lceil m/2 \rceil - 1) - \big(p^{m-1} - p^{\lfloor m/2 \rfloor}\big)$,
2) Se $T = \cup_{0 \leq k \leq \lceil m/2 \rceil - 1} A_{kj} - A_{0,0}$, então $t = |T| = \big(p^{m-1} - p^{\lfloor m/2 \rfloor}\big)^2 + 2(p-1)\big(p^{2m-2} - p^{2m-\lceil m/2 \rceil - 1}\big)$,

(iii) Para $m \geq 4$;

Se $W_1 = \cup_{k=\lceil m/2 \rceil}^{m-1} \cup_{j=1}^{m-k-1} A_{kj}$, $W_2 = \cup_{j=\lceil m/2 \rceil}^{m-1} \cup_{k=1}^{m-k-1} A_{kj}$ e $W = W_1 \cup W_2$, então $w = |W| = 2p^{m-1}\Big(\big(p^{\lfloor m/2 \rfloor} - 1\big) - \lfloor m/2 \rfloor (p-1)\Big)$.

Teorema 4.4.6.12: Seja $n = p^m, m \geq 2$ e $s, l\ e\ b$ definidos no Lema 4.72., então $\gamma\Big(L\big(\tau(Z_n[i])\big)\Big) = \gamma'\big(\tau(Z_n[i])\big) = \gamma_i'\big(\tau(Z_n[i])\big) = (s/2) + l + b$ se m é par $(s/2) + l + b + 1$ se m é ímpar.

Demonstração: Usando algumas noções do **Lema 4.4.6.11**. Observe que o conjunto S induz um subgrafo completo de $\tau(Z_n[i])$, K_s. Assim, qualquer conjunto de dominação de aresta para $\tau\big(Z_{p^m} \times Z_{p^m}\big)$ deve conter $s/2$ arestas para dominar K_s. Se $m \geq 3$, o conjunto $L = L_1 \cup L_2$ induz um grafo bipartido completo $K_{l,l}$ com conjuntos bipartidos $L_1\ e\ L_2$. Isso contribui com as arestas na margem dominante definidas para $\tau\big(Z_{p^m} \times Z_{p^m}\big)$.

As arestas que juntam vértices em $K_{l,l}$ aos vértices em K_s são cobertos pelos mesmos conjuntos dominantes de aresta para $K_{l,l}$ e K_s. Além disso, os vértices em A_{k0} e A_{0k}, onde $1 \leq k \leq m-1$, são apenas adjacentes a alguns vértices em K_s e $K_{l,l}$.

Por outro lado, se $m \geq 3$, o conjunto T é um conjunto independente. Felizmente, os vértices em T são apenas adjacentes a vértices em S. Assim, qualquer conjunto de dominância de aresta para K_s também domina arestas entre $S\ e\ T$.

Agora, para cada $1 \leq k \leq \lceil m/2 \rceil - 1\ e\ m-k \leq j \leq m,$ o conjunto $A_{kj} \cup A_{jk}$ induz um grafo bipartido completo com conjuntos bipartidos $A_{kj}\ e\ A_{jk}$. Para dominar esta coleção de grafos bipartidos completos induzidos por $A_{kj} \cup A_{jk}$, precisamos de arestas b aresta no conjunto dominante de arestas para $\tau(Z_{p^m} \times Z_{p^m})$ Felizmente, esse conjunto dominante com elementos b também domina todas as arestas em $E\left(\tau(Z_{p^m} \times Z_{p^m})\right)$ que são incidentes de qualquer aresta nesta coleção.

Finalmente, observe que se $m \geq 4$, os vértices em W são apenas adjacentes a alguns vértices em K_s, bem como na coleção dos grafos bipartidos completos. O grafo $\tau(Z_{p^m} \times Z_{p^m})$ não tem outras arestas. ■

CAPÍTULO 5

GRAFO EQUILIBRADO DOS DIVISORES DE ZERO DE ANÉIS DE MATRIZ.

Neste último capítulo tratamos de anéis não comutativos. Neste caso em vez de um grafo simples, passamos a ter um grafo orientado.

Definição 5.1: Grafo Orientado, consiste em um grafo $G = (V, A)$ onde $V = \{v_1, \dots, v_n\}$ é um conjunto de vértices e $A = \{a_1, \dots, a_k\}$ é um conjunto de arcos tais que $a_k, k = 1, \dots, m$ é representado por um par ordenado (v_i, v_j) de vértices, $i, j = 1, \dots, n$.

Definição 5.2: O conjunto de arcos que saem de um vértice v é chamado de leque.

Definição 5.3: O grau de saída de um vértice v é número de arcos que saem de v, ou seja, o tamanho do leque de saída de v.

Definição 5.4: O grau de entrada de um vértice v é o número de arcos que terminam em v.

Definição 5.5: Um grafo diz-se equilibrado se para todos os vértices o grau de saída é igual ao grau de entrada.

Vamos revisar brevemente algumas definições e ferramentas que serão usadas posteriormente. Seja R um anel não comutativo. O grafo de divisores de zero dirigido de R é um grafo dirigido $\tau(R)$ com o conjunto de vértices $Z(R)^* = Z(R) - \{0\}$, onde para distintos vértices x e y de $Z(R)^*$ existe uma aresta dirigida $x \to y$ de x para y se e somente se $xy = 0$.

Se X é um subconjunto de um anel R, então o anulador esquerdo de X é $ann_l(X) = \{a \in R: aX = 0\}$ e o anulador direito de X é $ann_r(X) = \{a \in R: Xa = 0\}$. Se o anel R é comutativo, então obviamente, $ann_l(X) = ann_r(X)$. Neste caso, escrevemos simplesmente $ann(X)$. Observe que se R é um anel finito e $a \in \tau(R)$, então o grau de entrada de um vértice é $|ann_l(a)| - 1 \; se \; a^2 \neq 0 \; e \; |ann_l(a)| - 2 \; se \; a^2 = 0$, e de forma semelhante para o grau de saída. Além disso, o grau de a no grafo não dirigido $\bar{\tau}(R)$ é $|ann_l(a) \cup ann_r(a)| - 1 \; se \; a^2 \neq 0 \; e \; |ann_l(a) \cup ann_r(a)| - 2 \; se \; a^2 = 0$.

Em [3] Akabari e Mohammadian provaram que, para cada corpo finito $F \; e \; n \geq 2$, o grau de entrada e o grau de saída de um vértice $a \in \tau(M_n(F))$ são $|F|^{n(n-k)} - \varepsilon$, e o grau de $a \in \bar{\tau}(M_n(F))$ é $2|F|^{n(n-k)} - |F|^{(n-k)^2} - \varepsilon, onde \; \varepsilon = 1$, a menos que $a^2 = 0$ e neste caso $\varepsilon = 2$. Em particular, o grafo dirigido $\tau(M_n(F))$ é equilibrado. Vamos ver que este resultado pode ser estendido ao anel das matrizes sobre um anel comutativo com identidade e de ideais principais

5.1 Resultados auxiliares

Para provar os principais resultados, utilizamos a teoria de anel de divisão elementar. Esta teoria diz respeito a redução de matrizes para uma forma diagonal. Uma matriz n por m, $A = (a_{ij})$ é dita ser diagonal se $a_{ij} = 0\ para\ todos\ i \neq j$. Dizemos que uma matriz A sobre um anel R admite redução diagonal se existir as matrizes invertíveis P e $Q\ sobre\ R$, de modo que PAQ é uma matriz diagonal. Duas matrizes $A\ e\ B$ sobre um anel R dizem-se equivalentes (notação: $A \sim B$) se houver matrizes invertíveis $P\ e\ Q$ tal que $B = PAQ$. Seguindo Kaplansky [28], se toda matriz A sobre um anel R é equivalente a uma matriz diagonal $D_A = diag\ (d_1, \ldots, d_n)$, com a propriedade que d_i é um divisor total de d_{i+1}, então R é chamado de anel de divisão elementar. Os elementos $d_1, \ldots, d_n$ são chamados divisores elementares da matriz A. Os anéis de divisão elementar, foram estudados por muitos autores [24, 39, 40, 41]. O seguinte teorema fundamental, que é provado em [18], fazendo uso de dois teoremas de Kaplansky.

Teorema 5.1.1: Qualquer anel comutativo de ideais principais com identidade é um anel de divisão elementar.

Lembre-se de que um anel comutativo de ideal principal, é um anel comutativo em que todo ideal é um ideal principal.

No Lema seguinte, mostramos que em anéis finitos o tamanho dos anuladores é invariante sob multiplicação por unidades.

Lema 5.1.2: Seja R um anel finito com identidade. Se $u \in R$ é uma unidade, então, para qualquer $a \in R$, temos

$$|ann_l(ua)| = |ann_l(au)| = |ann_l(a)|.$$

Demonstração: Obviamente $ann_l(a) \subseteq ann_l(au)$. Suponha que $w \in ann_l(au)$. Como u é uma unidade, a equação $wau = 0$ implica que $wa = 0$. Portanto, $w \in ann_l(a)$, e depois $ann_l(au) = ann_l(a)$.

É fácil mostrar que se $\varphi: R \to R$ é um automorfismo e x é um elemento de R temos que $\varphi(ann_l(x)) = ann_l(\varphi(x))$, o que implica que $|ann_l(x)| = |ann_l(\varphi(x))|$. Como o mapa $\varphi: R \to R$ definido por $\varphi(r) = u^{-1}ru$ é um automorfismo e $\varphi(ua) = au$ segue que $|ann_l(ua)| = |ann_l(au)|$. Isso prova o lema. ■

Observação 1: É fácil verificar se um resultado semelhante é válido para anuladores direitos.

5.2 Resultados principais

O seguinte teorema é uma generalização do Lema 14 provado por Akabari e Mohammadian em [3].

Teorema 5.2.1: Seja R um anel comutativo de ideal principal finito com identidade e $n \geq 2$. Suponha que $A \in M_n(R)$ é um divisor de zero diferente de zero e $d_1, d_2, \ldots, d_n$ sejam divisores elementares de A. Então, o grau de entrada e o grau de saída de $A\ em\ \tau(M_n(R))$ são

$$2\prod_{i=1}^{n}|ann(d_i)|^n - \varepsilon$$

e o grau de $A\ em\ \bar{\tau}(M_n(R))$ é igual a

$$2\prod_{i=1}^{n}|ann(d_i)|^n - \prod_{i,j=1}^{n}\left|ann(d_i) \cap ann\left(d_j\right)\right| - \varepsilon$$

onde $\varepsilon = 1$, a menos que $A^2 = 0$ e neste caso $\varepsilon = 2$. Em particular, $\tau(M_n(R))$ é equilibrado.

Demonstração: Pelo **Teorema 5.1.1,** o anel R é um anel de divisão elementar. Então, suponha que $A \sim diag(d_1, \ldots, d_n) = D_A$. Resulta do **Lema 5.1.2** e da Observação 1 que $|ann_l(A)| = |ann_l(D_A)|\ e\ |ann_r(A)| = |ann_r(D_A)|$. Agora, para uma matriz $X = (x_{ij})$ no anel de matriz $M_n(R)$, temos

$$XD_A = 0 \leftrightarrow x_{ij}d_j = 0, para\ i, j\ =\ 1, \ldots n, \qquad (1)$$

$$D_AX = 0 \leftrightarrow d_jx_{ij} = 0, para\ i, i = 1, \ldots n. \qquad (2)$$

Como o anel R é comutativo, segue-se que

$$|ann_l(A)| = |ann_r(A)| = \prod_{i=1}^{n}|ann(d_i)|^n$$

Por isso, o grau de entrada e o grau de saída de A são ambos iguais a $\prod_{i=1}^{n}|ann_l(d_i)|^n - \varepsilon, onde\ \varepsilon = 1, a\ menos\ que\ A^2 = 0\ e\ neste\ caso\ \varepsilon = 2.$

Das equações (1) e (2), concluímos que uma matriz $X = (x_{ij})$ pertence a $ann_l(D_A) \cap ann_r(D_A)$ se e somente se $x_{ij} \in ann(d_i)\ \cap ann(d_j)$. Consequentemente,

$$|ann_l(A)| \cap |ann_r(A)| = \prod_{i,j=1}^{n}\left|ann(d_i) \cap ann\left(d_j\right)\right|$$

Assim sendo,

$$|ann_l(A)| \cup |ann_r(A)| = 2\prod_{i=1}^{n}|ann(d_i)|^n - \prod_{i,j=1}^{n}|ann(d_i) \cap ann(d_j)|$$

Assim, o grau de $A\ em\ \bar{\tau}(M_n(R))$ é $2\prod_{i=1}^{n}|ann(d_i)|^n - \prod_{i,j=1}^{n}|ann(d_i) \cap ann(d_j)| - \varepsilon$, onde $onde\ \varepsilon = 1, a\ menos\ que\ A^2 = 0\ e\ neste\ caso\ \varepsilon = 2$. Isso completa a prova. ■

Observação 2: Suponha que o anel R seja um corpo finito F. Então, na redução diagonal $D_A = diag(d_1, \ldots, d_n)$ da matriz A cada divisor elementar é zero ou uma unidade. Além disso, o número de divisores elementares diferentes de zero é igual ao rank de A. Note que $ann(d_i) = \{0\}$ se d_i é uma unidade e $ann(d_i) = F$ se d_i for zero. Assim, denotando por k o rank de A, temos

$$|ann_l(A)| = |ann_r(A)| = \prod_{i=1}^{n}|ann(d_i)|^n = |F|^{(n-k)}$$

e

$$|ann_l(A)| \cup |ann_r(A)| = 2\prod_{i=1}^{n}|F|^{n(n-k)} - |F|^{(n-k)^2}.$$

Então, obtemos os resultados de Akabari e Mohammadian provado em [1].

Um circuito num grafo dirigido é uma sequência $e_1, e_2, \ldots, e_r$ de arestas dirigidas distintas, de modo que o vértice final de e_i é o vértice inicial de e_{i+1} para todos $1 \leq i \leq r-1$, e o vértice final de e_r é o vértice inicial de e_1. Um circuito é Euleriano se incluir cada aresta exatamente uma vez e visitar todos os vértices. Um grafo dirigido é chamado Euleriano se contém um circuito Euleriano.

Teorema 5.2.2: Seja R um anel comutativo de ideal principal finito com identidade e $n \geq 2$. Então, o grafo do divisor de zero dirigido $\tau(M_n(R))$ é Euleriano.

Demonstração: Seja $Z_l(M_n(R))$ o conjunto de divisores de zero esquerdo de $M_n(R)$. Ou seja, $Z_l(M_n(R)) = \{X \in M_n(R): XA = 0,\ \text{para alguns}\ A \in M_n(R) - \{0\}\}$. Da mesma forma, seja $Z_r(M_n(R))$ o conjunto dos divisores de zero direito de $M_n(R)$. Em [31], foi mostrado que $Z_l(M_n(R)) = Z_r(M_n(R))$. Por outro lado, Redmond mostrou em [44] que, para um anel não comutativo, o grafo do divisor de zero dirigido é conexo se e somente se o conjunto de divisores de zero direito é igual ao conjunto de divisores de zero esquerdo. Portanto, $\tau(M_n(R))$ é conexo. Para completar a prova, observamos que um grafo dirigido conexo é Euleriano se for equilibrado, em [23]. ■

Em seguida, determinamos o menor anel comutativo finito com identidade tal que $\tau(M_n(R))$ não é equilibrado.

Teorema 5.2.3: Seja R um anel comutativo com identidade e $n \geq 2$. Se o grafo do divisor de zero dirigido $\tau(M_n(R))$ não é equilibrado, então $|R| \geq 8$. Além disso, existe um anel comutativo com identidade da ordem 8 tal que $\tau(M_n(R))$ não é equilibrado.

Demonstração: Para qualquer inteiro positivo n, seja $\gamma(n)$ o número de anéis, a menos de isomorfismo, da ordem n (incluindo anéis não-comutativos e anéis sem identidade). Usando a classificação de grupos abeliano finito e o fato de que quando se decompõe o grupo aditivo de um anel finito em suas componentes primárias os componentes são ideais de ordem de potência de um primo, concluímos que γ é multiplicativa. Se $n = {p_1}^{e_1} \dots {p_k}^{e_k}$ é a factorização prima de n, então $\gamma(n) = \gamma({p_1}^{e_1}) \dots \gamma({p_k}^{e_k})$.

O anel nulo é o único anel com um elemento e não tem identidade. Suponha que R é um anel finito da ordem p, onde $p \, é \, um \, número \, primo$. Lembre-se de que cada elemento em um anel finito é uma unidade ou um divisor de zero. Portanto, se R não possui divisores de zero diferentes de zero, então cada elemento diferente de zero é uma unidade. Por isso, R é um anel de divisão finita, e assim pelo pequeno teorema de Wedderburn R é isomorfo para o corpo primo F_p. Em seguida, suponha que R tem divisores de zero diferentes de zero. Seja $r \in R$ um divisor de zero diferente de zero. Uma vez que o grupo aditivo de R tem a ordem p pelo teorema de Lagrange não possui subgrupos não triviais. Como $ann_l(r)$ é um subgrupo do grupo aditivo de R devemos ter $ann_l(r) = R$. Portanto, todos os elementos de R são divisores de zero. Assim, para cada elemento $r \in R$ temos $ann_l(r) = ann_r(r) = R$. Isso implica claramente que R é o anel nulo da ordem p. Então, $\gamma(p) = 2$. Observe que o anel zero não possui identidade e $\tau(M_n(F_p))$ é equilibrado pelo **Teorema 5.2.1.**

Agora, sejam $p \, e \, q$ números primos distintos. Como γ é multiplicativo, $temos \, \gamma(pq) = 4$. Se R for um anel da ordem pq, então R tem um I_1 ideal de ordem p e um ideal I_2 de ordem q. Como $p \, e \, q$ são primos distintos, temos $R \cong I_2 \oplus I_2$. Portanto, se R tem identidade, devemos ter $R \cong F_p \oplus F_q$, onde $F_p \, e \, F_q$ são corpos primos de ordem $p \, e \, q$, respectivamente. Como $F_p \oplus F_q$ é um anel de ideal principal, o grafo $\tau(M_n(F_p \oplus F_q))$ é equilibrado pelo **Teorema 5.2.1.**

Agora suponha que R tenha ordem p^2, onde p é um número primo. Existem 11 anéis de ordem p^2 [14]. No entanto, se um anel R de ordem p^2 é comutativo com identidade, é necessariamente um anel de ideal principal. De fato, todo ideal próprio I diferente de zero, em particular, tem ordem p. Por isso, I é gerado como um grupo aditivo por qualquer elemento diferente de zero.

Uma vez que, para $1 < n < 8$, temos que n é primo, um quadrado de primo, ou o produto de dois primos, concluímos que $\tau(M_n(R))$ é equilibrado para $|R| < 8$.

Para completar a prova, deixe-nos dar um exemplo de um anel R de ordem 8, de modo que $M_n(R)$ não seja equilibrado. Seja R a álgebra tridimensional sobre o corpo F_2 com base $\{1, a, b\}$ e a seguinte multiplicação da tabela.

	1	a	b
1	1	a	b
a	a	0	0
b	b	0	0

Observe que o anel R não é um anel de ideal principal. Por exemplo, o ideal (a, b) não é principal. Uma simples computação mostra que para o vértice $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ no grafo $\tau(M_2(R))$ o grau de entrada é 254 e o grau de saída é 1022. Portanto, o grafo $\tau(M_2(R))$ não é equilibrado. ■

BIBLIOGRAFIA

[1] Abu Osba, E. A., Henrisken, M., Alkam, O., Smith, F. The maximal regular ideal of some commutative rings. *Comment. Math. Univ. Carolinea* **47(1):1-10**, (2006).

[2] Akbari, S., Maimani, H. R., Yassemi, S. When a zero divisor graph is planar or a complete r-partite graph. *J. Algebra* **270**:**169-180**, (2003).

[3] Akbari S., and A. Mohammadian, Zero-divisor graphs of non-commutative rings, *J. Algebra* **296** (2), 462-479, (2006).

[4] Akbari, S., and A. Mohammadian, On the zero-divisor graph of a commutative ring, *J. Algebra*, vol 274, **314** (1), **168,** (2004).

[5] Anderson, D. D., and M. Naseer, Beck´s coloring of a commutative ring, *J. Algebra* **159, 500-514,** (1993).

[6] Anderson,D. F., and P.S, Livingston, On the zero-divisor graph of a ring, *J. Algebra* **217**, 434, (1999).

[7] Anderson, D. F., Livingston, P.S. The zero-divisor graph of a commutative ring. *J. Algebra* **217**:434-447, (1999).

[8] Anderson, David F. Livingston, Philip S. The zero-divisor graph of a commutative ring. *J. Algebra* 217 $n^{\underline{o}}$ 2 $434 - 447$, (1999),.

[9] Atiyah, M. F., and I. G. McDonald, Introduction to Commutative Algebra, *Addison-Wesley, Reading*, MA, (1969).

[10] Axtell, M., Stickles, J., Warfel, J. Zero divisor graph for direct products of commutative rings. *Houston J. Math*. 32(4):985-994, (2006).

[11] Arumugam, S., and S. Velammal, Edge domination in graphs, Taiwanese Journal of Mathematics, vol. 2, no. 22, pp. 173-179, (1998).

[12] Beck, I., Coloring of commutative rings, *J. Algebra* **116 208-226,** (1988).

[13] Beck,I., Coloring of commutative rings, *J. Algebra* **116**, **208,** (1988).

[14] Benjamim Fine, Classification of finite rings of order p^2. *Math. Mag*. 66 **(4)**, 248-252 (1993).

[15] Bogdan Zabavsky, Nearly simple elementar divisor domains. *Bul. Acad. Stiinte Repub. Mold. Mat*. **3. 121-123,** (2006).

[16] Bhat, V. K., R. Raina, N. Nehra, and O. Prakash, A note on zero divisor graph over rings, *International Journal of contemporany Mathematical Sciences,* vol. 2, no. **13-16, pp. 667-671**, (2007).

[17] Bollabás, B. Graph Theory, An Introductory Course, *Springer-Verlag*, New York, (1979).

[18] Brown, W. C., Matrices over commutative rings (*Monographs and Textbooks in Pure and Applied Mathematics,* **169.** Marcel Dekker, Inc., New York, (1993).

[19] Cordova, N., C. Gholston, and H. Hauser, The Structure of Zero-Divisor Ghaphs, Summer *Undergraduate Mathematical Sciences research Institute, Miami Univesrity,* (2005).

[20] Cross, J. The Euler Φ-function in the Gaussian integers. *Amer. Math. Monthly* 90():518-528, (1983).

[21] Diestel, R., Graph Theory, *Springer-Verlag*, New York, (1997).

[22] Duane, A., Proper Coloring and p-partite structures of the zero-divisor graph, *Rose-Hilman Undergraduate Mathematical Journal,* vol. 7, no. **Pp.1-7**, (2006).

[23] Ganesan, N., Properties of rings with a finite number of zero-divisors, Math. Ann. **157 215-218** (1964).

[24] Ganesan, N., Properties of rings with a finite number of zero-divisors, Math. Ann. **161 241-246,** (1965).

[25] Gareth A. Jones and J. Mary Jones, Elementary Number Theory *(Springer).*

[26] Gatalevich, A. I., and B. V. Zabavs´kii, *Mat. Metodi Fiz.-Mekh.* Polya **40** (4), 86 (1997) (in Ukrainian); translation in J. Math. Sci. (New York) **96** (2), 3013-3016 (1999).

[27] Gibbons, A., Algorithmic graph theory (Cambridge University Press, Cambridge, 1985).

[28] Harary, F., Graph Theory, addison-*Wesley*. Reading, MA, (1972).

[29] http://www.Springer.com/978-0-387-95587-2

[30] http://pt.wikipedia.org/wiki/teoria_dos_aneis

[31] Ivana Boc ic and Zoran Petrovic, Zero-divisor graphs of matrices over commutative rings. *Comm. Algebra* **37** (4), **1186** (2009).

[32] KaplansKy, I., Elementary divisors and modules.*Trans. Amer. Math Soc*. **66**, 464-491, (1949).

[33] Kaplansky, I., Commutative Rings, *ver. Ed.*, Univ of Chicago Press, Chicago, (1974).

[34] Koh, K., On Properties of rings with a finite number of zero-divisors, Math. Ann **171 79-80,** (1967).

[35] Lee, P. F., Line graph of zero divisor graph in commutative rings, *M.S. thesis*, Colorado Christian University, (2004).

[36] Livingston, P. S., Structure in Zero-divisor Graphs of commutative Rings, *Masters Thesis*, The University of Tennessee, Knoxville, TN, December (1997).

[37] MANUELA, S. *Livro de Álgebra*, Universidade Aberta.

[38] MONTEIRO, A. J.; MATOS, I. T. *Álgebra-um Primeiro Curso, Escolar Editora*, Lisboa (1995).

[39] McCoy, N. H. The Theory of Rings. New York: Macmillan, (1964).

[40] Mulay, S.B. Cycles and symmetries of zero divisors. *Comm. Algebra* 30:3533-3558. (2002).

[41] McDonald, B. R., Finite Rings with Identity, Dekker, New York, (1974).

[42] Philips, A., J. Rogrers, K. Tolliver, and F. Worek, Uncharted Territory of Zero-Divisor Graphs and Their complements, Summer Undergraduate Mathematical Sciences research Institute, Miami Univesrity, (2004).

[43] Pinter, W. C., A Book of Abstract Algebra, *Second Edition*.

[44] Redmond, Shane P. The zero-divisor graph of a non-commutative rings. *Commutative rings, 39-47, Nova Sci. Publ., Hauppauge NY,* (2002).

[45] Robin J. Wilson, Introducción a la teoria de grafos. Alianza Universidad.

[46] Sedlácek, J., *Some properties of interchange graphs, in Theory of Graphs and its Application*, **pp. 145-150**, Academic Press, New York, NY, USA, (1962).

[47] Silverman, J. A Friendly Introduction to Number Theory. 3rd ed. New Jersey: Pearson Prentice Hall.(2006).

[48] Stillwell. J., Element of Number Theory, XII, **256p**., Hardcover, (2003).

[49] Skiena, S., Implemeting Discrete Mathematics*: Combinatorics and Graph Theory with Mathematica,* Addison-Wesley, Rdwood City, Calif, USA, (1990).

[50] Veldman, H. J., A result on Hamiltonian line graphs involving restrictions on induced subgraphs, *Journal of Ghaph Theory,* vol. **12, no.3, pp. 413-420**, (1988).

[51] Zabavsky, B. V., Diagonalization of matrices. *Mat. Stud.* ***23*****, 3-10,** (2005).

[52] Zabavsky, B. V., Diagonalizability theorems for matrices over rings with finite stable range. *Algebra Discrete Math.* ***1. 151-165*****,** (2005).