PROPIEDADES DE LOS GRAFOS DE LOS DIVISORES DE CERO DE ANILLOS CONMUTATIVOS

TANIA CAROLINA CALVACHE ROSERO
BYRON ALEXANDER PATIÑO DE LA CRUZ

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
2023

PROPIEDADES DE LOS GRAFOS DE LOS DIVISORES DE CERO DE ANILLOS CONMUTATIVOS

TANIA CAROLINA CALVACHE ROSERO
BYRON ALEXANDER PATIÑO DE LA CRUZ

Trabajo presentado como requisito parcial para optar al título de Licenciado en Matemáticas

Asesor:
John Hermes Castillo Gómez
Doctor en Matemáticas

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
2023

Nota de Responsabilidad

Todas las ideas y conclusiones aportadas en el siguiente trabajo son responsabilidad exclusiva de los autores.

Artículo 1^{ro} del Acuerdo No. 324 de octubre 11 de 1966 emanado por el Honorable Consejo Directivo de la Universidad de Nariño.

Nota de Aceptación

John Hermes Castillo Gómez

Director de Tesis

Viviana Carolina Guerrero

Jurado 1

Alexander Holguín Villa

Jurado 2

San Juan de Pasto, 18 de abril de 2023

Este trabajo está dedicado a:
Nuestros padres como reconocimiento a su amor y apoyo incondicional.
Como también, a nuestro compromiso y esfuerzo.
Tania y Byron

Agradecimientos

El que no arriesga, no gana. Cuando entre a la carrera no creí quedarme en ella, con el tiempo me di cuenta que internamente siempre soñé con enseñar, así que cuando llegaban estudiantes a mi amaba ayudar a descubrir el gran potencial que ellos tenían y la sensación de que si se estaba logrando me llenaba de orgullo. Para mi el estar culminando mi carrera hoy en día es mi mayor ganancia y quiero agradecer aquellas personas que han hecho parte de este proceso.

A mi familia, en especial a mi madre, por ser mi apoyo en todo momento, por el esfuerzo de hacer que estudie una carrera y por no dejarme rendir, por ella es quien soy hoy en día y he podido llegar hasta el lugar donde estoy. A mi hermana, por siempre impulsarme a ser una mujer valiente y no dejarme derrumbar ante los obstáculos. A mi novio, por ser esa voz de aliento y enseñarme que detrás de cada esfuerzo hay una gran recompensa.

A el docente Dr. John Castillo, por aceptar ser nuestro asesor y guiar cada parte de este trabajo; siendo el más disciplinado y paciente para que podamos lograr nuestro objetivo. Gracias a él y a sus enseñanzas me incliné por esta rama de las matemáticas y por amar de alguna u otra manera más esta carrera. Además, mi más profunda admiración y respeto, su metodología y el cómo trata a sus estudiantes es un claro ejemplo de lo que es ser un excelente docente.

A Byron, por ser mi compañero a lo largo de este trabajo, por el apoyo incondicional tanto académicamente como personalmente. Además, por ser un gran amigo, escucharme, tener paciencia con mi forma de llevar a cabo las cosas que era totalmente diferente a la suya y por supuesto por transmitir esa tranquilidad y paz que a pocas personas se les da.

A mis amigos, aquellos que estuvieron a lo largo de los años y pudimos compartir en la carrera, como aquellos que la universidad se dio el placer de hacerme conocer.

Y por último a mis docentes, con los que tuve el placer de escuchar sus clases y por los que conocí fuera de ellas, porque de cada uno de ellos me llevo un gran aprendizaje y espero llegar a ser una mejor persona.

Tania Carolina Calvache Rosero.

Agradecimientos

Cuando uno se encuentra en los primeros semestres de la carrera, visualiza muy lejano el hecho de hacer un trabajo de grado y más aún terminarlo. Ha sido un camino lleno de tropiezos, pero estoy orgulloso de todos mis logros académicos, donde me demostré a mi mismo que, con esfuerzo y dedicación puedo lograr lo que en ocasiones miraba imposible. Le agradezco a mi madre por darme un abrazo en los momentos donde estaba cansado, a mi padre por demostrarme con su historia de vida que uno siempre puede lograr lo imposible, a mis hermanos por llenarme de sueños que cumplir, a mis sobrinos por darme una razón por la cual luchar para ser un ejemplo a seguir, y le agradezco cada día a mi novia por darme el mejor consejo que cualquier persona me pudo haber dado, "La práctica hace al maestro", me hizo caer en cuenta que si quiero conseguir algo, se necesita de esfuerzos y sacrificios, que no basta con solo desearlo, sino que, también hace falta dedicarle el suficiente tiempo para poder ser como las personas que admiras.

Agradezco a mi asesor de tesis Doctor John Hermes Castillo por ser paciente, y darse el tiempo de explicar con detalle cada tema que se nos dificultaba, por impulsarnos a mejorar y acabar nuestra tesis. Le expreso mi profunda admiración y respeto, espero poder llegar tan alto como él.

Agradezco a mi compañera de tesis, Tania, que más que una compañera es una amiga, gracias por tenerme paciencia cuando se me dificultaba el entendimiento de algunos temas, por las risas en cada reunión, también por impulsarme académicamente y trabajar con dedicación en nuestro proyecto.

Agradezco a mis amigos por ser parte fundamental de mi carrera, por su apoyo y nunca dejarme caer, con sus chistes y salidas, siempre diciéndome palabras de aliento en momentos donde más los necesitaba.

Gracias a mis docentes que me hicieron amar la matemática con la misma pasión que hacían sus clases, gracias por la dedicación en hacer cada clase para que nosotros tengamos una educación de calidad.

Byron Alexander Patiño de la Cruz.

Resumen

En este trabajo se analizan los principales resultados del artículo "The zero-divisor graph of a commutative ring" de los autores David F. Anderson y Philip S. Livingston. Se estudian propiedades y características del grafo de los divisores de cero de anillos conmutativos R con identidad denotados por $\Gamma(R)$; donde su conjunto de vértices es $Z(R)$ y en el que dos vértices diferentes x, y son adyacentes si y solo si $xy = 0$. Se exponen los conceptos básicos de la teoría de anillos y grafos y se presentan ejemplos necesarios para mejorar el entendimiento de los posteriores capítulos. Se estudia el grupo de los automorfismos de $\Gamma(R)$; en particular se examina una caracterización de $\mathrm{Aut}(\Gamma(\mathbb{Z}_n))$. Por último, se presenta implementaciones en el software `SageMath` para calcular $\Gamma(\mathbb{Z}_n)$ y $\Gamma(\mathbb{Z}_{p^n q})$.

Abstract

In this manuscript, we analyze the main results of the paper "The zero-divisor graph of a commutative ring" written by David F. Anderson and Philip S. Livingston. We study the properties and characteristics of the zero-divisor graph of commutative rings R with identity denoted by $\Gamma(R)$; defined as the graph whose vertex set is $Z(R)$ and two different vertices x, y are adjacent if and only if $xy = 0$. The basic concepts of ring and graph theory are presented with examples that are necessary to handle the results in the following chapters. We study the automorphisms of $\Gamma(R)$, specifically $\mathrm{Aut}(\Gamma(\mathbb{Z}_n))$. Finally, we give implementations in `SageMath` to obtain $\Gamma(\mathbb{Z}_n)$ and $\Gamma(\mathbb{Z}_{p^n q})$.

Índice general

Índice de figuras ix

Introducción x

1. Preliminares 1
1.1. Conceptos básicos de la teoría de grafos 1
1.2. Conceptos básicos de la teoría de anillos 7

2. Propiedades de $\Gamma(R)$ 15
2.1. Grafos con un vértice adyacente a cualquier otro vértice 23
2.2. Grafos completos 25

3. Automorfismos de $\Gamma(R)$ 29

4. Representación de grafos divisores de cero de anillos $\mathbb{Z}_n$ 35

5. Conclusiones 44

Referencias 45

Índice de figuras

1.1. Grafo del Ejemplo 1.2. 2
1.2. Subgrafo del grafo del Ejemplo 1.2. 2
1.3. Ciclo C_4 en el Ejemplo 1.2. 3
1.4. Ciclo más corto C y camino P. 4
1.5. Ejemplo de un grafo conexo y un grafo no conexo. 5
1.6. Grafo del Ejemplo 1.18. 5
1.7. Grafo bipartito completo σ $K_{3,2}$ 6
1.8. Grafos isomorfos. 6

2.1. Grafo de los divisores de cero de algunos anillos. 16
2.2. Grafos $\Gamma(R)$. 16
2.3. Grafos con 4 vértices que no representan a $\Gamma(R)$. 17
2.4. Grafos bipartitos completos 18
2.5. Grafo ciclo C_5. 19
2.6. Subgrafo de $\Gamma(\mathbb{Z}_2 \times R_2)$. 26
2.7. $\Gamma(R_3) = \Gamma\left(\mathbb{Z}_2[x]/\langle x^4\rangle\right)$. 28

4.1. Grafo de los divisores de cero del anillo $\mathbb{Z}_{15}$. 37
4.2. Grafo del anillo $\mathbb{Z}_{3^2 2}$. 40
4.3. Grafo de los divisores de cero del anillo $\mathbb{Z}_{2^3 3}$. 41
4.4. Grafo bipartito de los divisores de cero del anillo $\mathbb{Z}_{2^2 5}$. 43

Introducción

En este trabajo se presentan de manera ordenada los conceptos y resultados básicos tanto de la teoría de anillos como de la teoría de grafos, necesarios para el estudio del artículo "The zero-divisor graph of a commutative ring" de los autores David F. Anderson y Philip S. Livingston, ver [3]. Se espera que esta presentación facilite la lectura de otros artículos relacionados con el tema y que surgieron a partir del trabajo de Anderson y Livingston. El estudio del conjunto de los divisores de cero en anillos es un tópico que ha llamado la atención de muchos investigadores en álgebra abstracta. En [3] se establece una interacción entre las propiedades del conjunto de divisores de cero de anillos conmutativos y la teoría de grafos. El estudio de este tema se originó en el trabajo de I. Beck en 1988, ver [9], quien estaba interesado en el problema del coloreo de grafos originados a partrir de anillos. Posteriormente, esta investigación continuó con D. Anderson y M. Naseer ver [5] aunque en su definición se consideran todos los elementos del anillo como vértices del grafo, lo que la hace en esencia diferente a la que se estudiará en este trabajo. La investigación sobre este tipo de grafos ha impulsado nuevas líneas de trabajo vigentes en la actualidad, ver [1, 2, 4, 6, 11, 12, 20, 22].

El objetivo en este trabajo consiste en representar mediante un grafo el conjunto de los divisores de cero de un anillo conmutativo y estudiar sus principales propiedades y características. Para ello, en el Capítulo 1, se presentan conceptos básicos de la teoría de anillos y grafos en dos secciones divididas, respectivamente, en cada una de estas se presentan diferentes definiciones con ejemplos para que sea de mayor entendimiento y dinámico para el lector; aunque es importante que el lector tenga conocimiento en conceptos básicos de la teoría de número y grupos.

En el Capítulo 2, se expone formalmente el concepto del grafo de los divisores de cero en anillos conmutativos denotados por $\Gamma(R)$ y se exponen las diferentes propiedades de estos. Se dan algunos ejemplos para previo entendimiento y se demuestran teoremas entre los que se resalta el hecho de que $\Gamma(R)$ es siempre conexo, su diámetro menor o igual a 3 y su cintura es menor o igual a 4. Luego, se divide en dos secciones el capítulo, en la primera de ellas se presenta cuando en $\Gamma(R)$ un vértice es adyacente a cualquier otro vértice, mientras que en la segunda, se especifica cuándo $\Gamma(R)$ se puede realizar como un grafo completo.

En el Capítulo 3, se estudia el grupo de los automorfismos de $\Gamma(R)$ denotados como $\mathrm{Aut}(\Gamma(R))$. Entre los principales resultados se encuentra cómo un automorfismo en un anillo induce a un automorfismo en $\Gamma(R)$. Seguidamente, se caracteriza el grupo de los

automorfismos de $\Gamma(\mathbb{Z}_n)$; en particular se dan algunos resultados importantes, entre ellos se destaca que $\Gamma(\mathbb{Z}_n)$ es isomorfo a un producto directo de grupos simétricos. A partir de este resultado se determinan los n para los que $\mathrm{Aut}(\Gamma(\mathbb{Z}_n))$ es abeliano.

Finalmente, en el Capítulo 4 se toma como referencia el artículo "Representación de grafos divisores de cero para anillos", ver [18]; el cual se enfoca en los grafos de los divisores de cero de anillos $\mathbb{Z}_n$ y en particular se presenta un algoritmo que permite representar el grafo divisor de cero de anillos de la forma $\mathbb{Z}_{p^nq}$. El objetivo, en este capítulo es implementar en el software `SageMath` este algoritmo. Por ello, primero se hace una función que determina el conjunto de los divisores de cero de cualquier anillo $\mathbb{Z}_n$. Adicionalmente, se construye una función que hace una representación general de grafos divisores de estos anillos. Luego, se realiza la función del algoritmo donde se utiliza la definición de conjuntos r-partitos y la construcción de estos. Como un caso especial se estudia cuándo $\mathbb{Z}_{p^nq}$ es un grafo bipartito.

Capítulo 1

Preliminares

En este capítulo se presentan los preliminares necesarios para comprender el artículo "The zero-divisor graph of a commutative ring". También se indica ejemplos relacionados con las definiciones para una interpretación mas dinámica.

1.1. Conceptos básicos de la teoría de grafos

A continuación se enunciarán algunos conceptos de la teoría de grafos que serán de utilidad para la compresión del artículo en cuanto a teoremas y demostraciones. El lector interesado puede consultar estos conceptos y resultados en los libros [10, 11, 13].

Definición 1.1 (Grafo)**.** Un grafo es un par $\Gamma = (V, E)$ de conjuntos tal que los elementos de E son subconjuntos de orden dos de V. Los elementos de V son los vértices del grafo Γ y los de E son sus aristas. Dos vértices u y v de Γ $(u, v \in V)$ son adyacentes si $\{u, v\} \in E$.

Cuando no sea claro el conjunto de vértices y aristas del grafo Γ se denotarán con $V(\Gamma)$ y $E(\Gamma)$, respectivamente.

En general, en un grafo se pueden considerar direcciones en las aristas, multiaristas (aristas con los mismos vértices extremos) y bucles o lazos (aristas que conectan al mismo vértice). Sin embargo, en este documento, únicamente se trabajará con grafos no dirigidos y sin bucles, este tipo de grafos se conoce como grafos simples.

Ejemplo 1.2. Considere el grafo $\Gamma = (V, E)$ tal que $V = \{a, b, c, d, e\}$ y $E = \{\{a, b\}, \{a, c\}, \{a, d\}, \{a, e\}, \{b, c\}, \{b, d\}, \{b, e\}, \{c, d\}, \{c, e\}, \{d, e\}\}$, ver Figura 1.2.

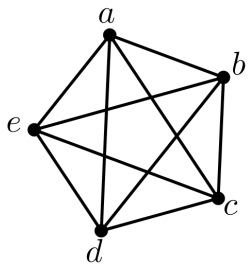


Figura 1.1: Grafo del Ejemplo 1.2.

Dado un grafo Γ, un subgrafo Δ de Γ es un grafo tal que $V(\Delta) \subseteq V(\Gamma)$ y $E(\Delta) \subseteq E(\Gamma)$.

Ejemplo 1.3. Del grafo del Ejemplo 1.2, se puede considerar el subgrafo Δ donde $V(\Delta) = \{a, b, c\}$ y $E(\Delta) = \{\{a, b\}, \{b, c\}\}$, ver Figura 1.2.

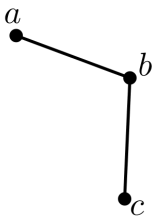


Figura 1.2: Subgrafo del grafo del Ejemplo 1.2.

En las siguientes definiciones se presentarán los conceptos de camino, sendero, trayectoria, ciclo y cintura.

Definición 1.4 (Camino o *walk*)**.** Sea Γ un grafo, un camino es una sucesión no vacía alternante

$$v_0 e_0 v_1 \dots e_{n-1} v_n \tag{1.1}$$

de vértices y aristas del grafo tal que $e_i = \{v_i, v_{i+1}\}$ para $0 \leq i \leq n-1$. Para abreviar la notación el camino (1.1) puede denotarse simplemente como: $v_0 v_1 \dots v_n$ o $v_0 - v_1 - \dots - v_n$. Si en (1.1) $v_0 = v_n$ el camino se denomina cerrado. La longitud de un camino es su número de aristas; de esta forma el camino en (1.1) es de longitud n.

Ejemplo 1.5. En el Ejemplo 1.2, los caminos *abec* y *aebc* unen los vértices a y c. Observe que en el grafo dado es lo mismo referirse al camino *abec* que al camino *ceba*.

Definición 1.6 (Sendero o *trail*)**.** Un sendero es un camino en el que las aristas son distintas, o lo que es lo mismo un camino donde no se repiten aristas.

Ejemplo 1.7. Se puede formar un sendero *abcde* en el grafo del Ejemplo 1.2. Un camino que no es sendero es el camino *cadeacb*.

Definición 1.8 (Trayectoria o *path*)**.** Una trayectoria de v a w es un sendero que no tiene ningún vértice repetido.

Observe que toda trayectoria es un sendero.

Ejemplo 1.9. El Ejemplo 1.7 de sendero es también una trayectoria y el contra ejemplo cumple que no es una trayectoria.

Definición 1.10 (Grafo camino)**.** El grafo camino con n vértices, que se denota con P_n, es el grafo en el que dos de sus vértices tienen grado 1 y los $n-2$ vértices restantes tienen grado 2. Si sus vértices son $v_1, v_2, \ldots, v_n$, entonces sus aristas están dadas por $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\}$.

Definición 1.11 (Grado de un vértice)**.** El grado de un vértice v en un grafo Ω es el número de aristas que son adyacentes al vértice v, y se denota así:

$$deg(v) = |\{x \in V(\Omega) : \{x, v\} \in E(\Omega)\}|.$$

Definición 1.12 (Ciclo)**.** Un ciclo es un camino cerrado que no tiene ningún otro vértice repetido excepto el primero y el último, ni tampoco tiene aristas repetidas. Para $n \geq 3$, el ciclo con n vértices se denota con C_n.

Ejemplo 1.13. Se puede formar un ciclo en el Ejemplo 1.2 si se selecciona el camino cerrado *abcda*.

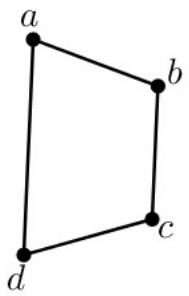


Figura 1.3: Ciclo C_4 en el Ejemplo 1.2.

Definición 1.14 (Cintura)**.** La cintura de un grafo Γ se denota con $\text{gr}(\Gamma)$, y se define como la longitud del ciclo más corto en Γ. Se dice que $\text{gr}(\Gamma) = \infty$ si el grafo Γ no contiene ciclos.

Ejemplo 1.15. Note que la longitud del ciclo que se indicó en el Ejemplo 1.13 no es la cintura del grafo del Ejemplo 1.2. En este grafo el ciclo más corto tiene 3 vértices; es decir su cintura es 3.

Dadas estas definiciones, se puede mencionar que la distancia entre dos vértices x, y en un grafo Γ, la cual se denota con $d(x, y)$, es la longitud de la trayectoria más corta de x a y en el grafo. Si dicha trayectoria no existe se dice que $d(x, y) = \infty$. En consecuencia se puede definir el diámetro de un grafo como la mayor distancia entre dos vértices cualesquiera; es decir

$$\operatorname{diam}(\Gamma) = \max\{d(u, v) : u, v \in V(\Gamma)\}.$$

El siguiente resultado relaciona la cintura de un grafo y su diámetro.

Proposición 1.16. *Sea Γ un grafo que contiene un ciclo. Entonces se tiene que* $\operatorname{gr}(\Gamma) \leq 2\operatorname{diam}(\Gamma) + 1$.

Demostración. Sea C uno de los ciclos más cortos en Γ. Supóngase que $\operatorname{gr}(\Gamma) \geq 2\operatorname{diam}(\Gamma) + 2$. Entonces existen dos vértices x, y en C cuya distancia en C es al menos $\operatorname{diam}(\Gamma) + 1$. En Γ, estos vértices tienen distancia menor, dado que cualquier camino más corto P en Γ debe tener una longitud como máximo $\operatorname{diam}(\Gamma)$. Entonces P no puede ser un subgrafo de C, esto es P debe contener aristas y vértices que no son parte de C.

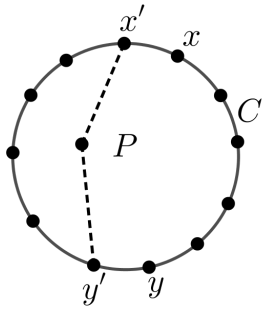


Figura 1.4: Ciclo más corto C y camino P.

Sea x' el último vértice en el cual C y P coinciden y y' el siguiente vértice de P en C. Entonces se forma el ciclo C' con las partes de P y C, así, entre x' y y' se forma un ciclo más corto que C, dado que la longitud de C' es menor o igual que $2\operatorname{diam}(\Gamma)$. Por lo que es una contradicción dado que el ciclo más corto era C. Por lo tanto, $\operatorname{gr}(\Gamma) \leq 2\operatorname{diam}(\Gamma) + 1$.

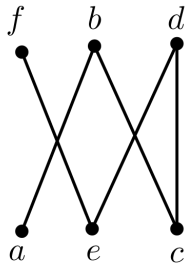
□

Los grafos se clasifican según algunas de sus características, las cuales van desde qué tipo son sus subgrafos, los ciclos que contienen, las particiones en sus conjuntos de vértices, entre otras. Algunos de los tipos de grafos que se mencionan en el artículo a estudiar son: grafos completos, grafos conexos, grafos libre de triángulos, entre otros.

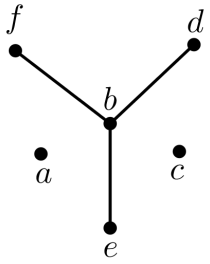
Un grafo completo es aquel en el que cada par de vértices son adyacentes. Se denota con K_n, al grafo completo con n vértices. Por ejemplo, el grafo de la Figura 1.1 es un grafo completo dado que todos sus vértices están conectados por una arista; este grafo

se denota con K_5. Un grafo es conexo si existe un camino entre cualquier par de vértices del grafo.

Ejemplo 1.17. El grafo de la Figura 1.5a es conexo, mientras que como en el grafo de la Figura 1.5b no existe un camino entre los vértices a y c, este es un grafo no conexo.



(a) Grafo conexo.



(b) Grafo no conexo.

Figura 1.5: Ejemplo de un grafo conexo y un grafo no conexo.

Un grafo que no contiene ciclos de longitud 3 se dice que es libre de triángulos.

Ejemplo 1.18. El grafo Γ con vértices $V(\Gamma) = \{x, y, z, w, u\}$ y aristas $E(\Gamma) = \{\{x, y\}, \{x, w\}, \{x, u\}, \{y, z\}, \{z, u\}\}$, es libre de triángulos.

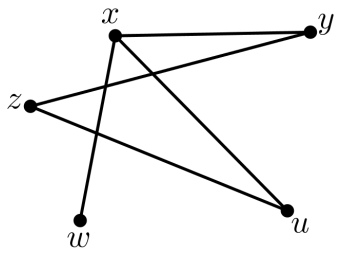


Figura 1.6: Grafo del Ejemplo 1.18.

Definición 1.19 (Grafo r-partito)**.** Un grafo $\Gamma = (V, E)$ se llama r-partito si V admite una partición en r conjuntos tal que cada arista tiene sus extremos en conjuntos diferentes: los vértices del mismo conjunto no pueden ser adyacentes; es decir, deben cumplir que:

1. $V_i \neq \emptyset, \forall i = 1, 2, \ldots, r$.
2. $V_i \cap V_j = \emptyset, \forall i, j = 1, 2, \ldots, r$.
3. $\bigcup_{i=1}^{r} V_i = V$.

Un grafo 2-partito es comúnmente llamado bipartito y en él V se divide en dos conjuntos disjuntos con relaciones de un vértice de un conjunto al otro y no entre ellos. Un grafo bipartito completo es aquel donde todos los vértices de las dos particiones son adyacentes y si los conjuntos de vértices tiene m y n elementos respectivamente, se denota por $K_{m,n}$. Al grafo bipartito completo $K_{1,n}$ ese le llama grafo estrella.

A continuación se presenta un ejemplo de grafo bipartito.

Ejemplo 1.20. Sea σ el grafo bipartito completo $K_{3,2}$ con vértices: $V(\sigma) = \{a, b, c, d, e\}$ y aristas $E(\sigma) = \{\{a, d\}, \{a, e\}, \{b, d\}, \{b, e\}, \{c, d\}, \{c, e\}\}$.

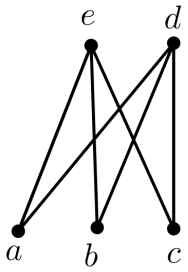
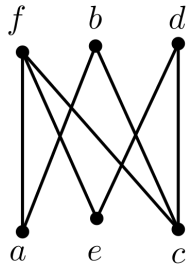


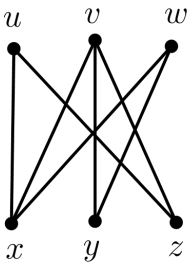
Figura 1.7: Grafo bipartito completo σ $K_{3,2}$.

Finalmente, dos grafos Γ y Δ son isomorfos si existe una biyección θ entre el conjunto de los vértices de Γ y los vértices de Δ de tal manera que $\{u, v\} \in E(\Gamma)$ si y sólo si $\{\theta(u), \theta(v)\} \in E(\Delta)$.

Ejemplo 1.21. Sea Θ el grafo cuyos vértices son $V(\Theta) = \{a, b, c, d, e, f\}$ y aristas $E(\Theta) = \{\{a, f\}, \{a, b\}, \{f, e\}, \{f, c\}, \{b, c\}, \{c, d\}, \{d, e\}\}$ y sea Λ el grafo cuyos vértices son $V(\Lambda) = \{x, y, z, w, v, u\}$ y aristas $E(\Lambda) = \{\{u, x\}, \{u, z\}, \{x, v\}, \{x, w\}, \{v, y\}, \{v, z\}, \{y, w\}\}$.



(a) Grafo Θ.



(b) Grafo Λ.

Figura 1.8: Grafos isomorfos.

Note que los grafos Θ y Λ son isomorfos puesto que se tiene la siguiente función biyectiva ψ dada por: $\psi(a) = u, \psi(f) = x, \psi(b) = z, \psi(c) = v, \psi(d) = y$ y $\psi(e) = w$.

Ahora, los grafos de las figuras 1.5a y 1.5b no son isomorfos, aunque los dos tienen el mismo número de vértices, el segundo tiene dos vértices que no tienen vecinos, mientras que en el primero todos sus vértices tienen al menos un vecino. Por último, un automorfismo de un grafo es un isomorfismo del grafo sobre si mismo.

1.2. Conceptos básicos de la teoría de anillos

En esta sección se definirán varios conceptos de teoría de anillos los cuales son necesarios para el entendimiento de los conceptos y resultados del artículo [3]. El lector interesado puede consultar los conceptos básicos y resultados que se presentan a continuación en los libros [7, 14, 15, 17].

Definición 1.22 (Anillo)**.** Un anillo R es un conjunto con dos operaciones binarias, adición (denotada con $a + b$) y multiplicación (denotado con ab), tal que para todo a, b, c en R se cumple:

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. Existe una identidad aditiva 0, es decir, existe un elemento $0 \in R$ tal que $a+0 = a$ para todo a en R.
4. Existe un elemento $-a \in R$ tal que $a + (-a) = 0$.
5. $a(bc) = (ab)c$.
6. $a(b + c) = ab + ac$ y $(b + c)a = ba + ca$.

Un anillo R se denomina conmutativo si para todo $a, b \in R$ se cumple que $ab = ba$. Se dice que R es un anillo con identidad si existe $1 \in R$ y $a \in R$, tal que $a1 = 1a = a$. Un elemento $a \in R$ en un anillo con identidad 1, se denomina unidad si existe $b \in R$ tal que $ab = ba = 1$ y se denota con $U(R)$ al conjunto de las unidades del anillo R. Los anillos que se estudiarán en este trabajo de grado son anillos conmutativos con identidad.

Ejemplo 1.23. El conjunto $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ bajo adición y multiplicación módulo n es un anillo conmutativo con identidad 1.

Definición 1.24 (Subanillo)**.** Un subconjunto no vacío S de un anillo R es un subanillo, si S es un anillo con las operaciones de R.

Ejemplo 1.25. El conjunto $A = \{0, 2, 4\}$ es un subanillo del anillo $\mathbb{Z}_6$.

Definición 1.26 (Divisores de cero)**.** Sea R un anillo conmutativo. Se dice que un elemento no nulo $a \in R$ es divisor de cero, si existe $0 \neq b \in R$ tal que $ab = 0$.

Con $Z(R)$ se denotará el *conjunto de los divisores de cero* del anillo R; esto es $x \in Z(R)$ si x es un divisor de cero de R.

Ejemplo 1.27. En el anillo $\mathbb{Z}_8$, el conjunto de los divisores de cero es

$$Z(\mathbb{Z}_8) = \{2, 4, 6\}.$$

En general, para el anillo $\mathbb{Z}_n$ con n compuesto, se tiene que existen $a, b \in \mathbb{Z}$ no nulos tales que $n = ab$, es decir $ab = 0$ en $\mathbb{Z}_n$. De esta forma, $a, b \in Z(\mathbb{Z}_n)$.

Dado un anillo R, se denotará con $D(R)$ el conjunto de los divisores de cero unido el elemento cero del anillo R; es decir, $D(R) = Z(R) \cup \{0\}$.

Aunque R sea un anillo conmutativo, $D(R)$ no necesariamente es un ideal de R. Para esto considere el anillo $R = \mathbb{R} \times \mathbb{R}$. Observe que aunque $(1, 0), (0, 1) \in D(R)$, el elemento $(1, 1) = (1, 0) + (0, 1) \notin D(R)$. Sin embargo, en casos especiales $D(R)$ es un ideal, inclusive puede ser un ideal primo, ver Teorema 2.13.

Definición 1.28 (Dominio entero)**.** Un dominio entero es un anillo conmutativo con identidad que no tiene divisores de cero. Es decir, en un dominio entero $ab = 0$ solo cuando $a = 0$ o $b = 0$.

Ejemplo 1.29. El anillo $\mathbb{Z}_p$ de los enteros módulo p primo, es un dominio entero.

Definición 1.30 (Cuerpo)**.** Un cuerpo es un anillo conmutativo con identidad tal que todo elemento diferente de cero es unidad.

Son ejemplos de cuerpos: $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$. Se puede demostrar que todo dominio entero finito es un cuerpo, ver [14, Thm. 13.2]. De esta forma, el anillo del Ejemplo 1.29 es un cuerpo.

Definición 1.31 (Suma directa)**.** Sean $R_1, R_2, \ldots R_n$ anillos conmutativos. Se le llama suma directa al anillo R dado por $R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$, si cumple que:

1. Para todo $r \in R$, $r = r_1 + r_2 + \cdots + r_n$ con $r_i \in R_i$.
2. $R_1 \cap R_2 \cap \cdots \cap R_n = \{0\}$.

Definición 1.32 (Producto directo)**.** Sean $R_1, R_2, \ldots R_n$ anillos. El anillo

$$R_1 \times R_2 \times \cdots \times R_n = \{(a_1, a_2, \ldots, a_n) : a_i \in R_i, 1 \leq i \leq n\},$$

donde la suma y la multiplicación se definen componente a componente.

Ejemplo 1.33. Para el anillo $\mathbb{Z}_3 \times \mathbb{Z}_3$, se puede verificar que

$$Z(\mathbb{Z}_3 \times \mathbb{Z}_3) = \{(0, 1), (1, 0), (0, 2), (2, 0)\}.$$

Definición 1.34 (Característica de un anillo)**.** La característica de un anillo R ($car(R)$) es el menor entero positivo n tal que $nx = 0$ para todo $x \in R$. Si este entero no existe, se dice que R tiene característica 0.

Ejemplo 1.35. Se puede demostrar que $car(\mathbb{Z}) = 0$ y que $car(\mathbb{Z}_n) = n$ para todo $n \in \mathbb{Z}^+$.

Definición 1.36 (Nilpotentes)**.** Un elemento x de un anillo R se dice que es nilpotente si existe algún entero positivo n tal que $x^n = 0$. Además, el conjunto de los elementos nilpotentes de un anillo se denota con $\text{nil}(R)$.

Ejemplo 1.37. La matriz $A = \begin{bmatrix} 2 & -4 \\ 1 & -2 \end{bmatrix}$ es nilpotente, puesto que $A^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Definición 1.38 (Ideal)**.** Un subanillo A de un anillo R es un ideal de R si para todo $r \in R$ y todo $a \in A$ se tiene que $ra \in A$ y $ar \in A$. Así A es un ideal siempre que

$$rA = \{ra : \forall a \in A\} \subseteq A \quad \text{y} \quad Ar = \{ar : \forall a \in A\} \subseteq A.$$

Ejemplo 1.39. Sea R un anillo conmutativo con identidad y $a \in R$. El conjunto

$$\langle a \rangle = \{ra : r \in R\}$$

es un ideal de R, el cual se denomina ideal principal generado por a.

Definición 1.40 (Anillo factor)**.** Sea R un anillo y A un ideal de R. El anillo factor formado por el conjunto de las clases laterales de A en R está dado por $R/A = \{r + A : r \in R\}$. Este conjunto tiene la estructura de anillo con las operaciones de adición y multiplicación dadas por

$$(r + A) + (s + A) = (r + s) + A,$$
$$(r + A)(s + A) = (rs) + A,$$

para todos $r, s \in R$.

Ejemplo 1.41. El anillo factor del ideal $4\mathbb{Z}$ en el anillo de los enteros es

$$\mathbb{Z}/4\mathbb{Z} = \{r + 4\mathbb{Z} : r \in \mathbb{Z}\} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}.$$

Definición 1.42 (Ideal primo)**.** Un ideal primo A de un anillo conmutativo R es un ideal propio de R si $a, b \in R$ y $ab \in A$ implica que $a \in A$ o $b \in A$.

Ejemplo 1.43. Sea n un entero mayor que 1. Entonces $n\mathbb{Z}$ es un ideal primo si y solo si n es primo, ver [14, Pag. 272].

Definición 1.44 (Ideal maximal)**.** Un ideal maximal M de un anillo conmutativo R es un ideal propio de R tal que, si B es un ideal de R y $M \subseteq B \subseteq R$, entonces $B = M$ o $B = R$.

Ejemplo 1.45. Considere el ideal $\langle 2 \rangle$ del anillo $\mathbb{Z}_{36}$. Si $ab \in \langle 2 \rangle$, entonces 2 divide a ab; lo que implica que 2 divide a a o 2 divide a b; es decir, $\langle 2 \rangle \subseteq \mathbb{Z}_{36}$ es primo. Así, puede demostrarse que el ideal $\langle 2 \rangle$ es maximal en $\mathbb{Z}_{36}$.

Definición 1.46 (Ideal anulador)**.** En un anillo R conmutativo, el ideal anulador de un elemento x, denotado con $\text{ann}(x)$, es el conjunto de los elementos $y \in R$ tal que $xy = 0$.

Ejemplo 1.47. En el anillo $\mathbb{Z}_{24}$, entonces $\text{ann}(2) = \{0, 12\}$.

Proposición 1.48. *Sean R un anillo y $x \in R$. Entonces* $\text{ann}(x)$ *es un ideal de R.*

Demostración. Sean $m, n \in \text{ann}(x)$, entonces $mx = 0$ y $nx = 0$. Luego, $mx - nx = x(m-n) = 0$, así $m-n \in \text{ann}(x)$. Por otro lado, sea $r \in R$. Entonces, $r(nx) = (rn)x = 0$ de ahí que $rn \in \text{ann}(x)$. Por lo tanto, $\text{ann}(x)$ es un ideal de R. □

Teorema 1.49. *Sea R un anillo conmutativo. Si Z es un ideal en R maximal entre todos los ideales anuladores de elementos diferentes de cero. Entonces Z es primo.*

Demostración. Suponga que Z es un ideal anulador de x en R, $Z = \text{ann}(x)$. Ahora, si $ab \in Z$, debemos probar que a o b están en Z. Sin pérdida de generalidad, suponga que $a \notin Z$. Entonces $ax \neq 0$. Notemos que $\text{ann}(ax) \supset Z$. Por la maximalidad de Z, $\text{ann}(ax) = Z$. Como b anula a ax, se sigue que $b \in Z$ y así Z es un ideal primo.

□

Definición 1.50 (Homomorfismo de anillos)**.** Un homomorfismo de anillos ϕ de un anillo R a un anillo S es una función de R a S que preserva las dos operaciones del anillo, es decir

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b), \\ \phi(ab) &= \phi(a)\phi(b), \end{aligned}$$

para cualquier pareja $a, b \in R$.

Ejemplo 1.51. Para cualquier entero positivo n la función

$$\begin{aligned} \phi : \langle \mathbb{Z}, +, \cdot \rangle &\longrightarrow \langle \mathbb{Z}_n, +, \cdot \rangle \\ k &\longmapsto k \text{ mód } n, \end{aligned}$$

es un homomorfismo sobreyectivo de $\mathbb{Z}$ en $\mathbb{Z}_n$.

Definición 1.52 (Isomorfismo y automorfismo)**.** Un isomorfismo es un homomorfismo biyectivo entre dos anillos R y S. Un automorfismo de R es un isomorfismo que va de R en el mismo.

Ejemplo 1.53. Para m y n enteros positivos primos relativos, la función

$$\phi : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n,$$

definida por $\phi(x) = (x \text{ mód } m, x \text{ mód } n)$ para todo $x \in \mathbb{Z}$ es un isomorfismo de $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

Definición 1.54 (Grupo simétrico S_n)**.** Sea $A = \{1, 2, \ldots, n\}$. El conjunto de todas las permutaciones de A es llamado el grupo simétrico de grado n y denotado por S_n. Los elementos de S_n son de la forma:

$$\alpha = \left[\begin{smallmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{smallmatrix} \right].$$

Observe que S_n tiene $n(n-1)\cdots 3 \cdot 2 \cdot 1 = n!$ elementos.

Teorema 1.55. *Sea R un anillo conmutativo y a un elemento idempotente de R. Entonces $R \cong R_1 \times R_2$, donde $R_1 = Ra$ y $R_2 = R(1-a)$.*

Demostración. Dado que $r = ra + r(1-a) \in R$, se tiene que $R = Ra + R(1-a)$. Además, si $x \in Ra \cap R(1-a)$, entonces $x = ra = s(1-a)$, para algunos $r, s \in R$. Así por un lado $xa = ra^2 = ra = x$, mientras que por otro $x = xa = s(1-a)a = s0 = 0$. Así $R = Ra \oplus R(1-a)$.

Sean $R_1 = Ra$ y $R_2 = R(1-a)$, entonces $R_1 \times R_2 = \{(ra, s(1-a)) : r, s \in R\}$. Considere la función ϕ tal que $\phi : R \longrightarrow R_1 \times R_2$, definida por $\phi(r) = \phi(ra + r(1-a)) = (ra, r(1-a))$, para cualquier $r \in R$. Primero se demuestra que ϕ es un homomorfismo de anillos. Sea $r, s \in R$.

1. Dado que $(ra)(sa) = rsa^2 = rsa$ y $(r(1-a))(s(1-a)) = rs(1-a)^2 = rs(1 - 2a + a^2) = rs(1 - 2a + a) = rs(1-a)$, entonces $\phi(rs) = (rsa, rs(1-a)) = (ra, r(1-a))(sa, s(1-a)) = \phi(r)\phi(s)$.

2. Además, $\phi(r+s) = ((r+s)a, (r+s)(1-a)) = (ra + sa, r(1-a) + s(1-a)) = (ra, r(1-a)) + (sa, s(1-a)) = \phi(r) + \phi(s)$.

Adicionalmente, se puede demostrar que ϕ es inyectiva y sobreyectiva. En efecto,

1. ϕ es inyectiva: Suponga que $\phi(r) = \phi(s)$ esto implica que $(ra, r(1-a)) = (sa, s(1-a))$ esto significa que $ra = sa$ y $r(1-a) = s(1-a)$, por lo tanto esto es $r = s$.

2. ϕ es sobreyectiva: Sea $(ra, s(1-a))$ un elemento cualquiera en $R_1 \times R_2$. Considere el elemento $x = ra + s(1-a) \in R$. Entonces $xa = (ra + s(1-a))a = ra^2 + s(1-a)a = ra + s(a - a^2) = ra + 0 = ra$. Por otro lado $x(1-a) = (ra + s(1-a))(1-a) = ra(1-a) + s(1-a)(1-a) = ra - ra^2 + s(1-a)^2 = 0 + s(1-a) = s(1-a)$. De esta forma, $\phi(x) = (xa, x(1-a)) = (ra, s(1-a))$.

□

Definición 1.56 (Anillo local)**.** Un anillo conmutativo R se denomina local si tiene un único ideal maximal.

Ejemplo 1.57. El anillo $\mathbb{Z}/p^n\mathbb{Z}$ es un anillo local (p primo, $n \geq 1$). El único ideal maximal consta de todos los múltiplos de p.

Teorema 1.58. *Todo cuerpo es un anillo local.*

Definición 1.59 (Anillo artiniano)**.** Un anillo conmutativo R es artinanio si toda cadena descendente de ideales $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_k \supseteq \cdots$, es estacionaria; es decir, que existe $m \in \mathbb{Z}^+$ tal que, para todo ideal, $I_n = I_m$, para todo $n \geq m$.

Ejemplo 1.60. Todo anillo finito es un anillo artiniano. Esto significa que $\mathbb{Z}/n\mathbb{Z}$ es un anillo artiniano para todo $n \in \mathbb{N}$.

Definición 1.61 (Anillo noetheriano)**.** Un anillo conmutativo R es noetheriano si toda cadena ascendente de ideales $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_k \subseteq \cdots$, es estacionaria.

Ejemplo 1.62. El anillo $\mathbb{Z}$ es noetheriano, sin embargo, no es artiniano, dado que al tomar la cadena ascendente de ideales: $(2) \subset (4) \subset (8) \subset \cdots \subset (2^n)$.

Definición 1.63 (Anillo R-módulo)**.** Sea R un anillo conmutativo. Un R-módulo es un grupo abeliano M (escrito de forma aditiva) sobre el que R actúa linealmente: más precisamente, es un par (M, μ), donde μ es una función de $R \times M$ en M, tal que para todo $m, n \in M$ y $a, b \in R$.

- $a(m + n) = am + an$.
- $(a + b)m = am + bm$.
- $(ab)m = a(bm)$.
- $1m = m$.

Ejemplo 1.64. Si K es un cuerpo y V un K-espacio vectorial, entonces V es un K-módulo unitario.

Proposición 1.65. *Si R es finito, entonces cada elemento de R es un divisor de cero o una unidad.*

Demostración. Sea $0 \neq a \in R$ no divisor de cero y considere la función $f(x) = ax$.

- Primero se prueba que la función f es inyectiva: Sean $x_1, x_2 \in R$ tal que $f(x_1) = f(x_2)$, entonces $ax_1 = ax_2$. Entonces $a(x_1 - x_2) = 0$ y como a no es un divisor de cero, entonces $x_1 = x_2$ Por lo tanto, f es inyectiva.
- Segundo, note que la función es sobreyectiva, esto se cumple por ser un anillo finito ya que es inyectiva sobre el mismo anillo.

De lo anterior se puede afirmar que existe $x \in R$ tal que $ax = 1$. Es decir a es una unidad. □

A continuación se presenta el siguiente resultado, cuya demostración no se incluye, pero que se puede en encontrar en [16, Prop. 4].

Proposición 1.66. *Si M es un ideal maximal en un anillo finito R, entonces $xM = 0$ para algún $0 \neq x \in M$.*

Proposición 1.67. *Sea R un anillo finito. Entonces,*

1. *Todo ideal primo es maximal.*
2. *Todo ideal primo es un ideal anulador.*

Demostración. Suponga que I es un ideal primo del anillo R, entonces R/I no tiene divisores de cero [14, Thm. 14.3, pág. 273]. Esto implica que R/I es un dominio entero finito, así R/I es un cuerpo, ver [14, Teorema 13.2, pág. 257]. Luego, I es un ideal maximal, ver [14, Teorema 14.4, pág. 273].

Para la segunda parte, sea I un ideal primo. Entonces por la primera parte I es un ideal maximal. Así de la Proposición 1.66 existe un $0 \neq x \in I$, tal que $xI = 0$. De esta forma, $I \subseteq \text{ann}(x)$. Por lo tanto, como I es maximal se sigue que $I = \text{ann}(x)$. □

Con $\text{nil}(R)$ se denota el conjunto de los elementos nilpotentes de R; es decir

$$\text{nil}(R) = \{x \in R : x^m = 0, \text{ para algún } m \in \mathbb{Z}^+\}.$$

Proposición 1.68. *Sea R un anillo conmutativo. Entonces $nil(R)$ es un ideal de R.*

Demostración. Sean $x, y \in nil(R)$. Luego, $x^n = 0 = y^m$, con $n, m \in \mathbb{Z}^*$. Así

$$(x+y)^{n+m} = \sum_{j=0}^{n+m} \binom{n+m}{j} x^j y^{m+n-j}.$$

Note que si $j < n$ entonces $m + n - j > n$ lo que implica que $y^{m+n-j} = 0$, ahora si $j \geq n$ entonces $x^j = 0$. Es decir que $nil(R)$ es cerrado bajo la suma.

Por otra parte. Sea $r \in R$, y considere el producto xr. Observe que si se eleva el producto a la n $(xr)^n = x^n r^n = 0$. Así, $nil(R)$ sería cerrado bajo la multiplicación. Por lo tanto $nil(R)$ es un ideal.

□

Proposición 1.69. *Sea R un anillo local finito con ideal maximal M. Entonces,*

1. *$M = D(R)$.*
2. *$\text{car}(R) = p^r$, para algún primo p y $r \in \mathbb{Z}^+$.*
3. *$|M| = p^m$, para algún $m \in \mathbb{Z}^+$.*

Demostración.

1. Como M es un ideal maximal, entonces M no contiene unidades, ver [14, Cap. 14, Ejer. 17, p. 275]. De la Proposición 1.65 se sabe que todos los elementos de M son divisores de cero. Así, $M \subseteq D(R)$. Pero como M es maximal, se sigue que $M = D(R)$.

2. Supóngase que $\text{car}(R) = n$. Dado que R/M es un cuerpo finito, se tiene que $\text{car}(R/M) = p$, con p un número primo. Como $n \cdot (1 + M) = n \cdot 1 + M = M$, se obtiene que el orden aditivo de $1 + M$ en $\langle R/M, + \rangle$ divide a n; es decir que p divide a n, ver [14, Cor. 2, p. 79]. Así $n = p^r s$ con s un entero positivo tal que $mcd(p, s) = 1$.

   Dado que p y s son primos relativos, se tiene $s(1 + M) \neq M$, lo cual implica que $s \cdot 1 \notin M$. Así por la Proposición 1.65 y el item anterior $s \cdot 1$ es una unidad en R. De esta forma, dado que $\text{car}(R) = n$, entonces el orden aditivo de $s \cdot 1$ en $\langle R, + \rangle$ es n. Ahora como $0 = n \cdot 1 = p^r(s \cdot 1)$, esto implica que el orden aditivo de $s \cdot 1$ en $\langle R, + \rangle$ divide a p^r. En consecuencia, $n = p^r s$ divide a p^r y así $s = 1$. Por lo tanto, $\text{car}(R) = p^r$.

3. Dado que $\langle M, + \rangle$ es un subgrupo de $\langle R, + \rangle$ y del item anterior se tiene que $|\langle R, + \rangle| = p^r$, por el Teorema de Lagrange, ver [14, pag. 147], se sigue que $|\langle M, + \rangle| = p^m$, con $m \leq r$.

□

El siguiente resultado es importante, porque se demuestra cuando el conjunto de los divisores de cero incluido el cero termina siendo igual a el conjunto de los elementos nilpotentes del anillo.

Proposición 1.70. *Sea R un anillo conmutativo. Entonces, $\{0\}$ es un ideal primario de R si y solo si $D(R) = \text{nil}(R)$.*

Demostración. Supóngase que $\{0\}$ es un ideal primario. Si $a \in \text{nil}(R)$, entonces $0 = a^n = a^{n-1}a$. Así, $a \in Z(R)$ y en consecuencia, $\text{nil}(R) \subseteq D(R)$. Por otro lado, sea $a \in Z(R)$, entonces existe $b \neq 0$ tal que $ab = 0$. De esta forma, $ab \in \{0\}$. Como $\{0\}$ es un ideal primario y $b \notin \{0\}$, entonces existe un $m \in \mathbb{Z}^+$ tal que $a^m = 0 \in \{0\}$. Así, $a \in \text{nil}(R)$ y luego $D(R) \subseteq \text{nil}(R)$. Por lo tanto, $D(R) = \text{nil}(R)$.

Recíprocamente, supóngase que $D(R) = \text{nil}(R)$. Sean $a, b \in R$ tales que $ab = 0$, con $a \notin \{0\}$. Es claro que si $b = 0$, entonces $b \in \{0\}$. Ahora si $b \neq 0$, entonces $b \in \text{nil}(R)$ y así existe $m \in \mathbb{Z}^+$, tal que $b^m \in \{0\}$. Por lo tanto, $\{0\}$ es un ideal primario. □

Capítulo 2

Propiedades de $\Gamma(R)$

En este capítulo se mostrará cuando un grafo de un anillo finito conmutativo se puede realizar como $\Gamma(R)$ y que siempre cumple con ser un grafo conexo. También, se determinará cuando $\Gamma(R)$ es un grafo completo o estrella.

Definición 2.1. Sean R un anillo conmutativo con identidad y $Z(R)$ el conjunto de los divisores de cero de R. Se asocia a R el grafo simple $\Gamma(R)$ cuyo conjunto de vértices es $Z(R)$, tal que para distintos $x, y \in Z(R)$, los elementos x y y son adyacentes si y solo si $xy = 0$. Es decir, $V(\Gamma(R)) = Z(R)$ y $\{x, y\} \in E(\Gamma(R))$ si y solo si $xy = 0$ y $x \neq y$.

Observe que $\Gamma(R)$ es un grafo vacío si y solo si R es un dominio entero.

En el siguiente teorema se muestra como dos anillos que son isomorfos implica que sus grafos también lo sean.

Teorema 2.2. *Sean R y S anillos conmutativos finitos. Si $R \cong S$, entonces $\Gamma(R) \cong \Gamma(S)$.*

Demostración. Supóngase que ϕ es un isomorfismo entre R y S. Entonces si $\{a, b\} \in E(\Gamma(R))$, se tiene que $ab = 0$. Así como ϕ es inyectiva y $\phi(a)\phi(b) = \phi(ab) = \phi(0) = 0$, entonces $\phi(a)$ y $\phi(b)$ son adyacentes en $\Gamma(S)$. Por lo tanto, los dos grafos tienen igual cantidad de vértices y las mismas conexiones; esto es, $\Gamma(R) \cong \Gamma(S)$. □

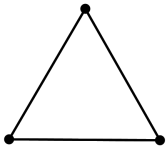
A continuación se presentan algunos ejemplos de grafos $\Gamma(R)$ para algunos anillos, estos ejemplos permiten observar algunas de las propiedades del grafo de los divisores de cero.

Ejemplo 2.3. En la Figura 2.1, se muestran los grafos de los divisores de cero para algunos anillos.

(a) $\mathbb{Z}_4$ o $\mathbb{Z}_2[X]/(X^2)$.

(b) $\mathbb{Z}_9$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ o $\mathbb{Z}_3[X]/(X^2)$.

(c) $\mathbb{Z}_6$, $\mathbb{Z}_8$ o $\mathbb{Z}_2[X]/(X^3)$.

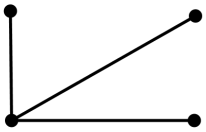


(d) $\mathbb{Z}_2[X,Y]/(X^2, XY, Y^2)$ o $F_4[X]/(X^2)$.

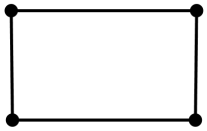
Figura 2.1: Grafo de los divisores de cero de algunos anillos.

Estos ejemplos muestran que anillos no isomorfos pueden tener el mismo grafo de los divisores de cero y que en el grafo no hay bucles, por lo cual no se evidencian los elementos nilpotentes.

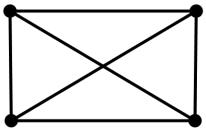
Ejemplo 2.4. Puede demostrarse que existen 11 grafos con cuatro vértices. Por el Teorema 2.8 el cual se demostrará posteriormente, en este trabajo únicamente son de interés 7 de ellos, los cuales son conexos. En realidad, de estos solo 3 son isomorfos a un grafo $\Gamma(R)$, para algún anillo R, ver Figura 2.2.



(a) $\mathbb{Z}_2 \times F_4$.



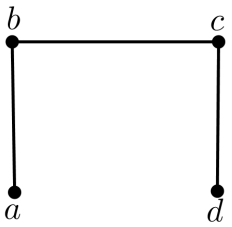
(b) $\mathbb{Z}_3 \times \mathbb{Z}_3$.



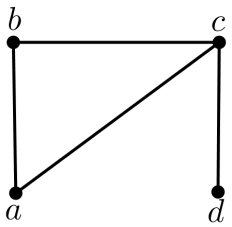
(c) $\mathbb{Z}_{25} \times \mathbb{Z}_5[X]/(X^2)$.

Figura 2.2: Grafos $\Gamma(R)$.

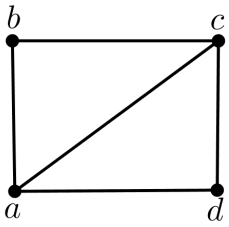
A continuación se demuestra que los 4 grafos con 4 vértices de la Figura 2.3, aunque son conexos no representan grafos $\Gamma(R)$.



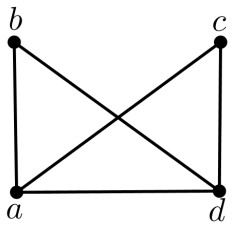
(a) Grafo Γ_1.



(b) Grafo Γ_2.



(c) Grafo Γ_3.



(d) Grafo Γ_4.

Figura 2.3: Grafos con 4 vértices que no representan a $\Gamma(R)$.

Primer grafo: Considere el grafo Γ_1 con vértices $V(\Gamma_1) = \{a, b, c, d\}$ y aristas $E(\Gamma_1) = \{\{a, b\}, \{b, c\}, \{c, d\}\}$, como se muestra en la Figura 2.3a.

Demostración. Sea R un anillo tal que $Z(R) = \{a, b, c, d\}$ y las relaciones de divisores dadas en la Figura 2.3a. Entonces $a + c \in \{0, a, b, c, d\}$, puesto que $(a + c)b = 0$.

- Caso 1: Supóngase que $a+c = 0$. Entonces $a = -c$. Multiplicando por d en ambos lados de esta igualdad se tiene que $ad = -cd$, así se tiene que $ad = 0$, lo cual es una contradicción.
- Caso 2: Supóngase que $a + c = a$. Entonces $c = 0$. Pero esto no puede ser, ya que los vértices están en el conjunto de divisores de cero. Lo mismo ocurre si se supone que $a + c = c$.
- Caso 3: Supóngase que $a + c = d$. Entonces $0 = (a + c)b = db$. Pero esto es una contradicción dado que $\{d, b\}$ no es una arista del grafo, ver Figura 2.3a.

De esta forma,

$$a + c = b. \tag{2.1}$$

Note que $b + d \in Z(R)$ ya que $(b + d)c = 0$, por lo tanto $b + d$ debe ser igual a $0, a, b, c$ o d. Así, realizando un análisis similar a los casos anteriores, se tiene que

$$b + d = c. \tag{2.2}$$

Por último, de las igualdades (2.1) y (2.2), se tiene que $b = a + c = a + (b + d)$, lo que implica que $a + d = 0$. Por lo tanto, $d = -a$ y $db = (-a)b = 0$, lo cual nuevamente es una contradicción.

Dado que en cualquier caso se obtiene una contradicción, la Figura 2.3a no representa el grafo de los divisores de cero de un anillo conmutativo. □

Segundo grafo: Considere el grafo Γ_2 con vértices $V(\Gamma_2) = \{a, b, c, d\}$ y aristas $E(\Gamma_2) = \{\{a, b\}, \{a, c\}, \{b, c\}, \{c, d\}\}$, ver Figura 2.3b.

Demostración. Sea $Z(R) = \{a, b, c, d\}$ el conjunto de los divisores de cero de un anillo conmutativo R. Entonces $b + d \in Z(R)$, dado que $(b + d)c = 0$. Por lo tanto, $b + d$ debe ser igual que $0, a, b, c$ o d. Si $b + d \in \{0, b, d\}$, en cualquier caso como se hizo anteriormente se puede obtener una contradicción.

Ahora supóngase que $b + d = c$. Entonces $0 = a(b + c) = ad$. Pero a y d no son vértices adyacentes.

En consecuencia, $b+d = a$. Dado que, $(a+c)b = 0$, se sigue que $a+c \in \{0, a, b, c, d\}$. Se puede verificar que $a + c$ debe ser igual a b. De esta forma, se tiene que $b = a + c = (b+d)+c$; entonces $d+c = 0$. Por lo tanto, $d = -c$ y $da = (-c)a = 0$, una contradicción. □

Usando ideas similares se puede demostrar que los grafos en las figuras 2.3c y 2.3d tampoco representan el grafo de los divisores de cero de ningún anillo conmutativo R.

El siguiente ejemplo muestra un grafo completo bipartito y un grafo completo bipartito estrella, a partir del producto de dos cuerpos finitos.

Ejemplo 2.5. Recordando la Definición 1.19 se sigue que $\Gamma(\mathbb{F}_p \times \mathbb{F}_q) = K_{p-1,q-1}$ y así, $\Gamma(\mathbb{Z}_2 \times \mathbb{Z}_7) = K_{1,6}$. Además, $\Gamma(\mathbb{Z}_2 \times \mathbb{F}_q) = K_{1,q-1}$ y en particular $\Gamma(\mathbb{Z}_3 \times \mathbb{Z}_5) = K_{2,4}$. Entonces,

(a) $\Gamma(\mathbb{Z}_2 \times \mathbb{Z}_7)$. (b) $\Gamma(\mathbb{Z}_3 \times \mathbb{Z}_5)$.

Figura 2.4: Grafos bipartitos completos

Como puede observarse en las figuras 2.1d y 2.2b, existen anillos para los que $\Gamma(R)$ es un triángulo o un cuadrado. Sin embargo, el siguiente resultado nos muestra que esto no es cierto para polígonos regulares con más lados. Los siguientes resultados se utilizarán en lo que sigue.

Proposición 2.6. *Para $n \geq 5$, no existe un anillo R tal que $\Gamma(R)$ sea isomorfo a C_n.*

Demostración. Supóngase que existe un anillo R tal que $\Gamma(R) \cong C_5$.

Así para este anillo se tiene que $Z(R) = \{a, b, c, d, e\}$ y $\Gamma(R)$ es como en la Figura 2.5. Considere las relaciones

$$ab = 0 \quad \text{y} \quad ae = 0. \tag{2.3}$$

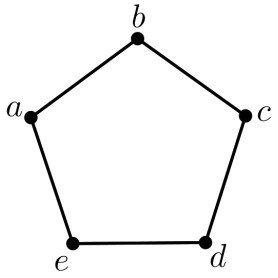


Figura 2.5: Grafo ciclo C_5.

Entonces, si se multiplica por -1 a cada lado de las igualdades en (2.3) se obtiene que $(-a)b = 0$ y $(-a)e = 0$. Por los vecinos que tiene b se deduce que $-a$ es a o c.

Si $-a = c$, entonces dado que $(-a)e = 0$ se tiene que $ce = 0$, lo cual es una contradicción, dado que c y e no son adyacentes, ver Figura 2.5. Por lo tanto, $-a = a$. Similarmente, se demuestra que $y = -y$ para todo $y \in D(R)$.

Ahora como $(b + e)a = ba + ea = 0$, esto implica que $b + e$ pertenece a $D(R) = \{0, a, b, c, d, e\}$.

- Si $b + e = 0$, entonces $b = -e$ pero esto es una contradicción, ya que $-e = e$.
- Si $b + e = b$, entonces $e = 0$ lo cual es absurdo. De manera similar pasa con el caso $b + e = e$.
- Si $b + e = c$, esto implica que $ac = 0$, lo que nuevamente es una contradicción; puesto que a y c no son adyacentes.
- Si $b + e = d$, esto quiere decir que $ad = 0$, y como a y d no son adyacentes, se obtiene una contradicción.

Por lo tanto, se concluye que $b + e = a$. Ahora como $(b + e)a = 0$, entonces $a^2 = 0$. Similarmente, se puede demostrar que esto sucede con todos los elementos de $Z(R)$; es decir $y^2 = 0$ para todo $y \in D(R)$; o de manera equivalente se tiene que $D(R) = \text{nil}(R)$ es un ideal de R, ver Proposición 1.68.

Además si $ab \in D(R)$, entonces $ab = 0$ o $(ab)z = 0$ para algún $0 \neq z \in R$. Si $ab = 0$, entonces $a, b \in D(R)$. Por otro lado, si $(ab)z = 0$, implica que si $bz = 0$, entonces $b \in D(R)$, mientras que si $bz \neq 0$, entonces $a \in D(R)$. De esta forma, en cualquier caso $a \in D(R)$ o $b \in D(R)$; es decir $D(R)$ es un ideal primo de R. Así por la Proposición 1.67, $D(R)$ es un ideal anulador; esto es $D(R) = \{0, a, b, c, d, e\} = \text{ann}(x)$, para algún $x \in D(R)$.

Sin embargo, como $|\text{ann}(x)| = 4$, ya que contiene sus dos vecinos, él mismo y al 0, se puede concluir que $D(R) \neq \text{ann}(x)$, puesto que $|D(R)| = 6$, lo que claramente es una contradicción a lo que se demostró en el párrafo anterior. Por lo tanto, $\Gamma(R)$ no puede ser isomorfo a C_5.

Supóngase que $\Gamma(R) \cong C_n$, con $n > 5$. Sea $Z(R) = \{a_1, a_2, a_3, ..., a_n\}$ el conjunto de vértices de $\Gamma(R)$ con aristas $E = \{\{a_1, a_2\}, \{a_2, a_3\}, \{a_3, a_4\}, \ldots, \{a_n, a_1\}\}$. Entonces,

$(-a_1)a_2 = 0$ y como a_1 y a_3 son los únicos vértices adyacentes a a_2, se tiene que $-a_1$ es igual a_1 o a_3. Ahora, si $-a_1 = a_3$, entonces $-a_1a_n = a_3a_n$, así $a_3a_n = 0$. Pero a_3 y a_n no son adyacentes, por lo tanto $-a_1 = a_1$. Similarmente, se demuestra que $y = -y$ para todo $y \in Z(R)$.

Además, $a_2+a_n \in D(R)$ ya que $(a_2+a_n)a_1 = 0$. Por lo tanto, $a_2+a_n \in \{0, a_1, a_2, a_n\}$.

- Si $a_2 + a_n = 0$, entonces $a_n = -a_2$ y multiplicando por a_3 se obtiene que $a_na_3 = -a_2a_3 = 0$, lo que es una contradicción, puesto que a_3 y a_n no son vértices adyacentes.
- Si $a_2 + a_n = a_2$, entonces $a_n = 0$, lo que es un absurdo. De manera similar pasa con el caso $a_2 + a_n = a_n$.
- Si $a_2 + a_n = a_i$ para $2 < i < n$, entonces $a_ia_1 = (a_2 + a_n)a_1 = 0$. Pero a_1 no es adyacente a ninguno de estos a_i.

Por lo tanto,

$$a_2 + a_n = a_1.$$

Esto implica que $a_1^2 = 0$. De manera similar se tiene que $y^2 = 0$ para todo $y \in Z(R)$. Como R es finito, igual que en el caso de C_5 se tiene que $D(R) = \operatorname{ann}(x)$ para algún $x \in Z(R)$. Sin embargo por un lado se tiene que $|\operatorname{ann}(x)| = 4$ mientras que $|D(R)| = n + 1 > 6$. Así nuevamente se obtiene una contradicción. Por lo tanto, $\Gamma(R)$ no puede ser isomorfo a C_n.

□

Ahora, cuando es un anillo conmutativo Artiniano la cintura del grafo se reduce y es menor o igual a 4.

Teorema 2.7. *Sea R un anillo conmutativo. Entonces $\Gamma(R)$ es finito si y solo si R es finito o es un dominio entero. En particular, si $1 \leq |\Gamma(R)| < \infty$, entonces R es finito y no es un cuerpo.*

Demostración. Si R es un dominio entero no tiene divisores de cero, por lo tanto $Z(R) = \emptyset$. Por otro lado, si R es un anillo finito y no es un dominio entero, entonces tendrá n elementos divisores de cero, es decir $|\Gamma(R)| = n$.

Recíprocamente, supóngase que R es infinito con un número finito de divisores de cero. Entonces $\Gamma(R)$ es finito y no vacío, pues de lo contrario R no tendría divisores de cero, lo cual significa que sería un dominio entero. Ahora, sean $x, y \in R$ tales que $xy = 0$ y considere $I = \operatorname{ann}(x)$. Entonces $y \in I$ y en consecuencia $ry \in I$, para todo $r \in R$. Observe que, $I \subseteq D(R)$ esto implica que I es finito. Luego, para un $i \in I$ el conjunto $N = \{r \in R : ry = i\}$ es infinito. Para cualesquiera $r, s \in N$ se tiene que $(r - s)y = ry - sy = i - i = 0$, esto implica que $r - s \in \operatorname{ann}(y)$ y así $\operatorname{ann}(y)$ es infinito. Ahora como $\operatorname{ann}(y) \subseteq D(R)$, se tiene que $D(R)$ es infinito lo cual es una contradicción. Por lo tanto, R debe ser finito. □

El siguiente resultado es uno de lo más relevantes, ya que demuestra que el grafo $\Gamma(R)$ para un anillo conmutativo finito siempre es un grafo conexo.

Teorema 2.8. *Sea R un anillo conmutativo. Entonces $\Gamma(R)$ es conexo y el diámetro* $\operatorname{diam}(\Gamma(R)) \leq 3$. *Además, si $\Gamma(R)$ contiene un ciclo, entonces* $\operatorname{gr}(\Gamma(R)) \leq 7$.

Demostración. Se buscarán todas las trayectorias posibles entre dos vértices cualesquiera en $\Gamma(R)$ y se demostrará que todas tienen longitud menor o igual a 7.

Considere dos elementos distintos $x, y \in Z(R)$. Se estudiarán los siguientes casos:

1. El caso trivial sucede cuando $xy = 0$, claramente $d(x, y) = 1$.

   Asúmase que $xy \neq 0$.

2. Supóngase que $x^2 = y^2 = 0$, esto significa que $x - xy - y$ es un camino de longitud 2 y así $d(x, y) = 2$.

3. Si $x^2 = 0$ y $y^2 \neq 0$, entonces existe $b \in Z(R) - \{x, y\}$ tal que $by = 0$. De esta forma, pueden ocurrir 2 casos; el primero es cuando $bx = 0$, entonces, se puede formar el camino $x - b - y$ el cual es de longitud 2. El segundo se presenta cuando $bx \neq 0$, entonces se forma el camino $x - bx - y$ cuya longitud es 2. De manera similar se estudia el caso cuando $y^2 = 0$ y $x^2 \neq 0$.

4. Finalmente, supóngase que y^2 y x^2 son diferentes de cero. Esto implica directamente que existen dos elementos $a, b \in Z(R) - \{x, y\}$ tales que $ax = by = 0$, de esta suposición se derivan tres casos cuando $a = b$, $ab = 0$ y $a \neq b$, los cuales se analizan a continuación:

   a) Si $a = b$, entonces se tiene el camino de longitud 2: $x - a - y$.

   b) Si $ab = 0$, se forma el camino de longitud 3: $x - a - b - y$.

   c) Si $a \neq b$, se puede considerar el camino de longitud 2: $x - ab - y$.

Por lo tanto, $d(x, y) \leq 3$, para cualquier x, y; así $\operatorname{diam}(\Gamma(R)) \leq 3$. En consecuencia, $\Gamma(R)$ es conexo y por la Proposición 1.16 se tiene que $\operatorname{gr}(\Gamma(R)) \leq 7$. □

En el siguiente resultado se demuestra que cuando el anillo es conmutativo Artiniano, se tiene que la cintura del grafo se reduce y es menor o igual a 4.

Teorema 2.9. *Sea R un anillo conmutativo Artiniano. Si $\Gamma(R)$ contiene un ciclo, entonces* $\operatorname{gr}(\Gamma(R)) \leq 4$.

Demostración. Supóngase que $\Gamma(R)$ contiene un ciclo. Del Teorema 8.7 en [7, pag. 90] se tiene que R es un producto directo finito de anillos locales artinianos. De esta forma, se demuestra el resultado cuando R es un anillo local y cuando R es el producto directo de dos anillos locales.

Supóngase que R es local con un ideal maximal no nulo M. Entonces por la Proposición 1.67, se tiene que $M = \operatorname{ann}(x)$ para algún $x \in M^*$. Si existen distintos

$y, z \in M^* - \{x\}$ con $yz = 0$, entonces $y - x - z - y$ es un triángulo. En este caso, $\text{gr}(\Gamma(R)) = 3$. De no ser así, $\Gamma(R)$ no contendría ciclos, lo cual sería una contradicción.

Supóngase que $R = R_1 \times R_2$. Si $|R_1| \geq 3$ y $|R_2| \geq 3$, entonces existe $a_i \in R_i - \{0, 1\}$. Así, $(1, 0) - (0, 1) - (a_1, 0) - (0, a_2) - (1, 0)$ es un cuadrado; es decir $\text{gr}(\Gamma(R)) \leq 4$. Ahora asúmase que $R_1 = \mathbb{Z}_2$. Si $|Z(R_2)| \leq 1$, entonces $\Gamma(R)$ no contiene ciclos, es una contradicción. Luego, $|Z(R_2)| \geq 2$. Dado que $\Gamma(R_2)$ es conexo, existen elementos distintos $x, y \in Z(R_2)$ con $xy = 0$. En consecuencia, $(0, x) - (1, 0) - (0, y) - (0, x)$ es un triángulo; es decir $\text{gr}(\Gamma(R_2)) = 3$. Por lo tanto, $\text{gr}(\Gamma(R)) \leq 4$ en todos los casos.

□

En el anterior teorema se demostró que el $\text{gr}(\Gamma(R))$ es menor o igual a 4. En los siguientes corolarios se demuestra específicamente cuando el $\text{gr}(\Gamma(R))$ es 4 e infinito.

Corolario 2.10. *Sea R un anillo conmutativo finito. Entonces,* $\text{gr}(\Gamma(R)) = 4$ *si y solo si*

1. $R \cong F \times K$, *para cuerpos finitos F y K, tales que* $|F| \geq 3$ *y* $|K| \geq 3$, *o*
2. $R \cong F \times A$, *con F un cuerpo finito tal que* $|F| \geq 3$ *y A un anillo finito tal que* $|D(A)| = 2$.

Demostración. Supóngase que $\text{gr}(\Gamma(R)) = 4$. Por la demostración del Teorema 2.9 se puede suponer que $R \cong R_1 \times R_2$ con $|R_1| \geq 3$ y $|R_2| \geq 3$. Si R_1 tiene divisores de cero, entonces existen $a, b \in Z(R_1)$ tales que $ab = 0$, con los cuales se puede formar un triángulo $(a, 0)-(b, 0)-(0, x)-(a, 0)$ lo cual es una contradicción ya que el $\text{gr}(\Gamma(R)) = 4$. Por lo tanto, ni R_1 ni R_2 tienen divisores de cero; es decir que son dominios enteros finitos, entonces son cuerpos finitos, ver [14, Thm. 13.2]. Ahora, si $|D(R_1)| = 2$ con $D(R_1) = \{0, a\}$ donde $a^2 = 0$ y $|D(R_2)| = 2$ con $D(R_2) = \{0, b\}$. Entonces $(a, 0) - (a, b)-(0, b)-(a, 0)$ forma un triángulo lo cual es una contradicción. Así que, $|D(R_1)| = 1$ y $|D(R_2)| \leq 2$; es decir cuando $|D(R_1)| = |D(R_2)| = 1$ entonces se llegaría a que R_1 y R_2 son cuerpos finitos. Cuando $|D(R_1)| = 1$ y $|D(R_2)| = 2$ entonces $R \cong F \times A$ donde F es un cuerpo finito y A es un anillo finito con $|D(A)| = 2$.

Recíprocamente, si $R \cong F \times K$ con F y K cuerpos finitos, $|F| \geq 3$ y $|K| \geq 3$. Suponga que $\text{gr}(\Gamma(R)) \neq 4$. Por el Teorema 2.9 el $\text{gr}(\Gamma(R)) = 3$ es decir que existen $a, b \in F$ y $x \in K$ que forman un triángulo $(a, 0) - (b, 0) - (0, x) - (a, 0)$. Note que $ab = 0$ lo cual es una contradicción ya que F es un cuerpo. Por lo tanto, $\text{gr}(\Gamma(R)) = 4$. De manera similar se demuestra que si $R \cong F \times A$ con F un cuerpo y con $|D(A)| = 2$, entonces $\text{gr}(\Gamma(R)) = 4$.

□

Corolario 2.11. *Sea R un anillo conmutativo finito. Entonces* $\text{gr}(\Gamma(R)) = \infty$ *si y solo si una de las siguientes afrimaciones es verdadera*

1. $|\Gamma(R)| \leq 2$,
2. $|\Gamma(R)| = 3$ *y* $\Gamma(R)$ *no es un grafo completo,*

3. $R \cong \mathbb{Z}_2 \times A$, donde A es un cuerpo finito o un anillo finito tal que $|D(A)| = 2$.

Demostración. Supóngase que $\text{gr}(\Gamma(R)) = \infty$. Si $|\Gamma(R)| > 3$, entonces existen $x, y, z, w \in Z(R)$ tal que $x - y - z - w - x$ forman un cuadrado en $\Gamma(R)$. Así, $\text{gr}(\Gamma(R)) = 4$, lo cual es una contradicción. De esta forma, $|\Gamma(R)| \leq 3$. Observe que si $|\Gamma(R)| = 3$, entonces por la hipótesis dada $\Gamma(R)$ no puede ser un grafo completo. Por último, asuma que $\text{gr}(\Gamma(R)) = \infty$ y $R \cong R_1 \times R_2$. De la demostración del Teorema 2.9 se tiene que $|R_1| \leq 2$ o $|R_2| \leq 2$. Suponga que $|R_1| = 2$, entonces $R_1 \cong \mathbb{Z}_2$. Si $|D(R_2)| \geq 3$, entonces por la demostración del Teorema 2.9, $\Gamma(R)$ contendría un triángulo, entonces $|D(R_2)| \leq 2$. Claramente si $|D(R_2)| = 1$, R_2 es un cuerpo finito.

Recíprocamente, claramente los dos primeros casos implican que $\text{gr}(\Gamma(R)) = \infty$. Ahora, si $R \cong \mathbb{Z}_2 \times A$, donde A es un cuerpo finito, entonces $Z(R) = \{(1,0), (0,x) : 0 \neq x \in A\}$. De esta forma, el vértice $(1,0)$ es adyacente a cualquier otro vértice, pero los demás vértices no son vecinos entre ellos. Así, $\Gamma(R)$ no contiene ciclos y por definición $\text{gr}(\Gamma(R)) = \infty$. Por otro lado, si A es un anillo con $|D(A)| = 2$, entonces el grafo $\Gamma(R)$ no contiene ciclos ya que solo tiene dos vértices: $(1,0)$ y $(0,a)$, con $0 \neq a \in D(R)$. Por lo tanto, $\text{gr}(\Gamma(R)) = \infty$. □

Finalmente se presenta la caracterización de cuando un grafo de los divisores de cero de un anillo es un grafo camino P_n, con $n \geq 1$.

Proposición 2.12. *Sea R un anillo conmutativo. Entonces $\Gamma(R) \cong P_n$ si y solo si $1 \leq n \leq 3$.*

Demostración. Por el Teorema 2.8 se tiene que el $\text{diam}(\Gamma(R))$ debe ser menor o igual que 3, para cualquier anillo R. De esta forma, $\Gamma(R)$ no puede ser isomorfo a P_n si $n \geq 4$. Ahora, de las figuras 2.1a, 2.1b y 2.1c se sigue el resultado. □

2.1. Grafos con un vértice adyacente a cualquier otro vértice

En esta sección se estudia el caso en el que existe un vértice que es adyacente a cualquier otro vértice en $\Gamma(R)$. A continuación, se demuestra como el hecho de que exista un vértice adyacente a cualquier otro vértice en $\Gamma(R)$ hace que el conjunto $D(R)$ termine siendo un ideal primo.

Teorema 2.13. *Sea R un anillo conmutativo. Entonces existe un vértice $\Gamma(R)$ que es adyacente a cualquier otro vértice si y solo si se da una de las siguientes opciones:*

1. $R \cong \mathbb{Z}_2 \times A$, donde A es un dominio entero, o

2. $D(R)$ es un ideal anulador de R. En este caso $D(R)$ es un ideal primo.

Demostración. Sea $a \in Z(R)$ adyacente a cualquier otro vértice en $\Gamma(R)$.

Si $D(R)$ es un ideal anulador, entonces $D(R) = \text{ann}(x)$ para algún $0 \neq x \in R$. Entonces si $z \in \text{ann}(y)$, para algún $0 \neq y \in R$, se tiene que $z \in D(R)$; es decir que $\text{ann}(y) \subseteq D(R)$. De esta forma, $D(R)$ es maximal entre todos los ideales anuladores de R, así por el Teorema 1.49 es un ideal primo.

Suponga que $D(R)$ no es un ideal anulador. Como a es adyacente a cualquier otro vértice se debe tener que $a \notin \text{ann}(a) = I$, pues de lo contrario $D(R) = I$. Nuevamente, como $ay = 0$, para todo $a \neq y \in D(R)$, se tiene que I es maximal entre todos los ideales anuladores de R; así por el Teorema 1.49 es un ideal primo de R. Si $a^2 \neq a$, entonces como $a^2 \in Z(R)$ y como a es adyacente a cualquier otro vértice se tiene que $a^3 = a^2a = 0$. Así, $a^2 \in I$ y como I es un ideal primo entonces $a \in I$, lo que es una contradicción. De esta forma, $a^2 = a$, entonces por el Teorema 1.55 se tiene que $R \cong R_1 \times R_2$. De este isomorfismo, se sigue que el vértice $(1, 0)$ es adyacente a cualquier otro vértice. Si $1 \neq c \in R_1$, el elemento $(c, 0) \in R_1 \times R_2$ es un divisor de cero, pero $(c, 0) = (c, 0)(1, 0) = (0, 0)$, entonces $c = 0$ lo que implica $R_1 \cong \mathbb{Z}_2$. Si R_2 no es un dominio entero, entonces existe un $b \in Z(R_2)$. Pero $(1, b)$ es un divisor de cero de R que no es adyacente a $(1, 0)$, una contradicción. Por lo tanto, R_2 es un dominio entero.

Si $R \cong \mathbb{Z}_2 \times A$ donde A es un dominio entero, entonces $Z(R) = \{(1, 0), (0, a) : 0 \neq a \in A\}$. En consecuencia, $(1, 0)$ es adyacente a cualquier otro vértice. Si $D(R) = \text{ann}(x)$ para algún $0 \neq x \in R$, entonces x es adyacente a cualquier otro vértice. □

Observe que el Ejemplo 2.1b muestra que los dos casos del Teorema 2.13 pueden darse incluso para el mismo grafo. En efecto, los grafos de los divisores de cero de $\mathbb{Z}_9$ y de $\mathbb{Z}_2 \times \mathbb{Z}_2$ son el mismo grafo estrella, donde $D(\mathbb{Z}_9) = \{0, 3, 6\} = \text{ann}(3)$. Un anillo R se denomina reducido, si no tiene elementos nilpotentes diferentes de cero. A continuación se presenta una implicación directa del Teorema 2.13 para este tipo de anillos.

Corolario 2.14. *Si R es reducido y $\Gamma(R)$ tiene un vértice adyacente a cualquier otro vértice, entonces $R \cong \mathbb{Z}_2 \times A$, con A un dominio entero.*

Demostración. Si $D(R) = \text{ann}(x)$ para algún $0 \neq x \in R$, entonces $x^2 = 0$. Esto contradice el hecho de que R sea reducido, es decir $D(R)$ no puede ser un ideal anulador. Por lo tanto, $R \cong \mathbb{Z}_2 \times A$, con A un dominio entero. □

Los siguientes corolarios de cuando un vértice es adyacente a cualquier otro vértice implican resultados muy interesantes.

Corolario 2.15. *Si un vértice x de $\Gamma(R)$ es adyacente a cualquier otro vértice de $\Gamma(R)$, entonces x es idempotente con $Rx = \{0, x\}$ un ideal primo de R o $D(R) = \text{ann}(x)$.*

Demostración. De la demostración del Teorema 2.13 se tiene que cuando $D(R)$ no es un ideal anulador, entonces $x^2 = x \neq 0$. Igualmente de los argumentos dados en esta demostración se tiene que $\{0, x\} \subseteq Rx \cong \mathbb{Z}_2$; es decir que $Rx = \{0, x\}$. Sean a, b elementos no nulos de R tales que $ab \in Rx$. Supóngase que $ab = x$. Entonces existe

$0 \neq y \in R$ tal que $xy = 0$. En consecuencia, $(ab)y = a(by) = 0$. Como $a \neq 0$, entonces $by \in D(R)$. En el caso de que $by = 0$, entonces $b \in Z(R)$ y así $bx = 0$. Entonces $x^2 = (ab)x = a(bx) = 0$, una contradicción. Esto implica que $a \in Z(R)$ y nuevamente $x^2 = (ax)b = 0$, se obtiene una contradicción. Por lo tanto, $ab = 0$.

Entonces a y b son vértices del grafo $\Gamma(R)$, entonces $ax = bx = 0$. De ahí que $a(b - x) = 0$. Si $b - x \neq 0$, entonces $x(b - x) = 0$, lo que implica que $x^2 = 0$, lo que es una contradicción. En consecuencia, $b = x$. Similarmente, se puede demostrar que $a = x$. Por lo tanto, $x^2 = 0$, lo que nuevamente es una contradicción. En consecuencia, si $ab \in Rx$, entonces $a = 0$ o $b = 0$.

□

Corolario 2.16. *Si $D(R)$ es un ideal anulador, entonces* $\operatorname{ann}(Z(R))^*$ *es precisamente el conjunto de vértices adyacentes a cualquier otro vértice.*

Demostración. Sea $D(R) = \operatorname{ann}(x)$, para algún $x \in R$. Sea $0 \neq s \in \operatorname{ann}(Z(R)) = \operatorname{ann}(\operatorname{ann}(x))$, entonces $st = 0$, para todo $t \in Z(R) = \operatorname{ann}(x)$. Entonces, todo elemento de $\operatorname{ann}(Z(R))^*$ es adayacente a todos los vértices del grafo. □

Adicionalmente, en los corolarios 2.6 y 2.7 en [3] se estudian casos particulares para anillos conmutativos R; cuando R es un anillo Noetheriano o finito.

Corolario 2.17. *Sea R un anillo conmutativo Noetheriano. Entonces existe un vértice en $\Gamma(R)$ que es adyacente a cualquier otro vértice si y solo si $R \cong \mathbb{Z}_2 \times A$, donde A es un dominio entero Noetheriano, o $D(R)$ es un ideal primo de R. Si adicionalmente,* $\dim(R) = 0$, *entonces $R \cong \mathbb{Z}_2 \times A$, donde A es un cuerpo o $\{0\}$ es un ideal primario de R; es decir, $D(R) = \operatorname{nil}(R)$.*

Corolario 2.18. *Sea R un anillo finito conmutativo. Entonces existe un vértice en $\Gamma(R)$ que es adyacente a cualquier otro vértice si y solo si $R \cong \mathbb{Z}_2 \times F$, donde F es un cuerpo finito, o R es local. Además, para algún primo p y un entero $n \geq 1$,*

$$|\Gamma(R)| = \begin{cases} |F| = p^n, & \text{si } R \cong \mathbb{Z}_2 \times F, \\ p^n - 1, & \text{si } R \text{ es local.} \end{cases}$$

2.2. Grafos completos

En esta sección se estudia el caso en el que $\Gamma(R)$ es un grafo completo. Por definición, $\Gamma(R)$ es completo si y solo si $xy = 0$ para todo par de elementos distintos $x, y \in Z(R)$. El caso para $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ merece atención. Si $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces $Z(R) = \{(0,1), (1,0)\}$. Así, en $\Gamma(R)$ tiene dos vértices y una arista y su grafo $\Gamma(R)$ es isomorfo a la Figura 2.1b. En consecuencia, $\Gamma(R)$ es completo.

En el siguiente resultado se demuestra que los dos casos mencionados en el párrafo anterior caracterizan completamente el hecho de que $\Gamma(R)$ sea completo.

Teorema 2.19. *Sea R un anillo conmutativo. Entonces $\Gamma(R)$ es completo si y solo si $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ o $xy = 0$ para todo $x, y \in Z(R)$.*

Demostración. Supóngase que $\Gamma(R)$ es completo y que existe $x \in Z(R)$ tal que $x^2 \neq 0$. Se demostrará que $x^2 = x$; esto es, que x es un elemento idempotente. Note que si no se cumple esta última afirmación, como $x \in Z(R)$, entonces existe $0 \neq y \in R$, tal que $xy = 0$. Entonces $x^2y = x(xy) = 0$, de esta forma $x \neq x^2 \in Z(R)$ y así $x^3 = x^2x = 0$. De ahí, $x^2(x + x^2) = x^3 + x^4 = 0$ y como $x^2 \neq 0$, entonces $x + x^2 \in Z(R)$. Si $x + x^2 = x$, entonces $x^2 = 0$, una contradicción. Por lo tanto, $x + x^2 \neq x$. Como $\Gamma(R)$ es completo se sigue que $x^2 = x^2 + x^3 = x(x + x^2) = 0$, lo cual es nuevamente una contradicción. En consecuencia $x^2 = x$.

Ahora de la demostración del Teorema 2.13 se tiene que $R \cong R_1 \times R_2$, donde $R_1 \cong \mathbb{Z}_2$ y R_2 es un dominio entero. Supóngase que $\{0, 1, a\} \subseteq R_2$, se tiene que $\{(1, 0), (0, 1), (0, a)\} \subseteq Z(R)$. De esta forma, el grafo en la Figura 2.6 es un subgrafo de $\Gamma(\mathbb{Z}_2 \times R_2)$.

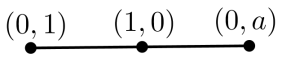


Figura 2.6: Subgrafo de $\Gamma(\mathbb{Z}_2 \times R_2)$.

Notése que como $(0, 1)(0, a) = (0, a) \neq (0, 0)$, entonces los vértices $(0, 1)$ y $(0, a)$ no son adyacentes en $\Gamma(R)$, por lo tanto $\Gamma(R)$ no sería completo. De esta forma, necesariamente $R_2 \cong \mathbb{Z}_2$ y así $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

Definición 2.20. Sea R un anillo conmutativo. Para $x, y \in Z(R)$ se dice que $x \sim y$ si $xy = 0$ o $x = y$ y que $x \sim^* y$ si $xy = 0$.

Es claro que para cualquier $x, y \in Z(R)$, se tiene que $x \sim x$ ($x \sim^* x$) y que si $x \sim y$ ($x \sim^* y$), entonces $y \sim x$ ($y \sim^* x$). Lo anterior implica que las relaciones $\sim$ y $\sim^*$ son relaciones reflexivas y simétricas. En el siguiente resultado se demuestra que estas dos relaciones son de equivalencia.

Corolario 2.21. *Sea R un anillo conmutativo. Entonces,*

1. *La relación $\sim$ es transitiva si y solo si $\Gamma(R)$ es completo,*
2. *La relación $\sim^*$ es transitiva si y solo si $\Gamma(R)$ es completo y $R \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

Demostración.

1. Supóngase que $\sim$ es transitiva. Sean $x, y \in Z(R)$ diferentes. Como $\Gamma(R)$ es conexo, ver Teorema 2.8, entonces existen $z_1, z_2, \ldots, z_r \in Z(R)$ tales que $\{\{x, z_1\}, \{z_1, z_2\}, \ldots, \{z_{r-1}, z_r\}, \{z_r, y\}\} \in E(\Gamma(R))$. De ahí que, $xz_1 = 0, z_1z_2 = 0, \ldots, z_{r-1}z_r = 0$ y $z_ry = 0$. Así, $x \sim z_1, z_1 \sim z_2, \ldots, z_{r-1} \sim z_r$ y $z_r \sim y$. Como $\sim$ es transitiva, entonces $x \sim y$ y por definición $xy = 0$; es decir $\{x, y\} \in E(\Gamma(R))$.

Recíprocamente, asúmase que $\Gamma(R)$ es completo y que $x \sim z$ y $z \sim y$. Si $x = z$ o $y = z$, entonces claramente $x \sim y$. Entonces se debe tener que $xz = 0$ y $zy = 0$, esto quiere decir que $x, y \in Z(R)$. Como $\Gamma(R)$ es completo, entonces $\{x, y\} \in E(\Gamma(R))$ y así $xy = 0$, es decir $x \sim y$. Por lo tanto, $\sim$ es transitiva.

2. De la demostración del item anterior se tiene que si $\sim^*$ es transitiva, entonces el grafo $\Gamma(R)$ es completo y se cumple que $xy = 0$ para toda pareja de elementos diferentes $x, y \in Z(R)$. Esto implica que $x \sim^* y$ y que $y \sim^* x$, esto es $x \sim^* x$; es decir que $x^2 = 0$; lo que implica por la demostración del Teorema 2.19 que $R \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.

   Por otro lado, suponga que $\Gamma(R)$ es completo y $R \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces por el Teorema 2.19 para todo $x, y \in Z(R)$, $xy = 0$. Así si $a \sim^* b$ y $b \sim^* c$, entonces $a, c \in Z(R)$ y así $ac = 0$, lo que es equivalente a decir que $a \sim^* c$. Por lo tanto, $\sim^*$ es transitiva.

□

Teorema 2.22. *Sea R un anillo conmutativo finito. Si $\Gamma(R)$ es completo, entonces*

1. *$R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, o*
2. *R es un anillo local con característica p o p^2 y $|\Gamma(R)| = p^n - 1$, donde p es primo y $n \in \mathbb{Z}^+$.*

Demostración. Para un cuerpo F, si $1 \neq a$, los vértices $(0, 1)$ y $(0, a)$ no son adyacentes, así el grafo $\Gamma(\mathbb{Z}_2 \times F)$ no es completo a menos que $F = \mathbb{Z}_2$, ver Teorema 2.19. Si este no es el caso, por el Corolario 2.18, R debe ser local con ideal maximal M y así por la Proposición 1.69, se tiene que $\text{car}(R) = p^m$, con p un número primo y $m \in \mathbb{Z}^+$. Si $m \geq 3$, existe λ primo relativo con p tal que $\lambda p < p^m$. Observe que si $p = 2$, basta tomar $\lambda = 3$, mientras que si $p > 2$ se puede considerar $\lambda = 2$. Entonces p y λp son dos divisores de cero que no son adyacentes. Así la $\text{car}(R) = p$ o p^2. Finalmente, de la tercera parte de la Proposición 1.69 se tiene que $|M| = p^n$, con $n \in \mathbb{Z}^+$ y así $|\Gamma(R)| = p^n - 1$.

□

Es importante resaltar que en el Ejemplo 2.11(a) en [3] se demuestra que para cada primo p y cualquier $n \in \mathbb{Z}^+$, existe un anillo R tal que $\Gamma(R)$ es completo y $|\Gamma(R)| = p^n - 1$. Así, $\Gamma(R) \cong K_m$ si y solo si $m = p^n - 1$, para algún p primo y $n \in \mathbb{Z}^+$.

Ejemplo 2.23. Sea p un primo y $R = \mathbb{Z}_{p^2}$. Entonces $Z(R) = \{p, 2p, \ldots, (p-1)p\}$. Entonces $\Gamma(R)$ es completo con $|\Gamma(R)| = p - 1$. Similarmente, se tiene que

$$Z\left(\frac{\mathbb{Z}_p[x]}{\langle x^2 \rangle}\right) = \left\{x + \langle x^2 \rangle, 2x + \langle x^2 \rangle, \ldots, (p-1)x + \langle x^2 \rangle\right\}.$$

De esta forma, $\Gamma\left(\dfrac{\mathbb{Z}_p[x]}{\langle x^2\rangle}\right) \cong K_{p-1}$; en consecuencia $\mathbb{Z}_{p^2}$ y $\dfrac{\mathbb{Z}_p[x]}{\langle x^2\rangle}$ no son anillos isomorfos pero tienen el mismo grafo de los divisores de cero; esto es K_{p-1}. En particular,

$$\Gamma(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \Gamma(\mathbb{Z}_9) \cong \Gamma\left(\frac{\mathbb{Z}_3[x]}{\langle x^2\rangle}\right) \cong K_2,$$

pero estos tres anillos no son isomorfos.

Adicionalmente en el Lema 2.12 y Teorema 2.13 en el articulo [3], los autores caracterizan completamente cuando el grafo $\Gamma(R)$ es un grafo estrella.

Lema 2.24 ([3, Lemma 2.12])**.** *Sea R un anillo conmutativo finito. Si $\Gamma(R)$ tiene exactamente un vértice adyacente a cualquier otro vértice, entonces*

1. *$R \cong \mathbb{Z}_2 \times F$, donde F es un cuerpo finito con $|F| \geq 3$, o*
2. *R es local con un ideal maximal M tal que $R/M \cong \mathbb{Z}_2$, $M^3 = 0$ y $|M^2| \leq 2$. Así, $|\Gamma(R)|$ es p^n o $2^n - 1$, para algún primo p y $n \in \mathbb{Z}^+$.*

Teorema 2.25 ([3, Thm. 2.13])**.** *Sea R un anillo conmutativo finito con $|\Gamma(R)| \geq 4$. Entonces $\Gamma(R)$ es un grafo estrella si y solo si $R \cong \mathbb{Z}_2 \times F$, donde F es un cuerpo finito. En particular, si $\Gamma(R)$ es un grafo estrella, entonces $|\Gamma(R)| = p^n$ para algún primo p y un entero $n \leq 0$. Recíprocamente, todo grafo estrella de orden p^n se puede obtener como $\Gamma(R)$ para algún anillo R.*

Ejemplo 2.26. Para un entero $n \geq 1$, sea $R_n = \dfrac{\mathbb{Z}_2[x]}{\langle x^{n+1}\rangle}$ un anillo local finito. Entonces

$$Z(R_n) = \{a_1x + a_2x^2 + \cdots + a_nx^n + \langle x^{n+1}\rangle : a_i \in \mathbb{Z}_2\},$$

donde no todos los a_i son simultáneamente iguales a cero. Así $|\Gamma(R_n)| = 2^n - 1$. Observe que x^n es el único vértice adyacente a cualquier otro vértice. Sin embargo, para $n \geq 3$, $\Gamma(R_n)$ no es un grafo estrella, ya que los vértices $x^{n-1} + x^n$ y x^{n-1} también son adyacentes.

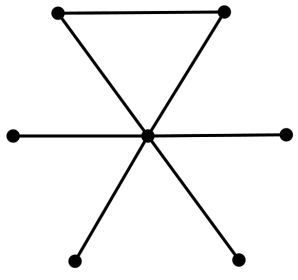


Figura 2.7: $\Gamma(R_3) = \Gamma\left(\mathbb{Z}_2[x]/\langle x^4\rangle\right)$.

Capítulo 3

Automorfismos de $\Gamma(R)$

En esta sección se estudia el grupo de los automorfismos del grafo $\Gamma(R)$ denotado por $\mathrm{Aut}(\Gamma(R))$.

Definición 3.1. Sean $G = (V, E)$ y $G' = (V', E')$ dos grafos. Una función $\varphi : V \longrightarrow V$ es un homomorfismo de G a G' si preserva la adyacencia de los vértices; es decir si $\{x, y\} \in E$, entonces $\{\varphi(x), \varphi(y)\} \in E'$. Si ϕ es biyectiva y su inversa φ^{-1} es también un homomorfismo; es decir $\{x, y\} \in E$ si y solo si $\{\varphi(x), \varphi(y)\} \in E'$, se dice que φ es un isomorfismo y que G y G' son isomorfos, lo que se denota con $G \cong G'$. Un isomorfismo de G a si mismo se denomina automorfismo de G.

El conjunto $\mathrm{Aut}(\Gamma)$ con la composición de funciones es un grupo. Si $|\Gamma| = n$, entonces $\mathrm{Aut}(\Gamma)$ es isomorfo a un subgrupo de S_n y claramente $\mathrm{Aut}(K_n) \cong S_n$. En efecto, para un grupo Γ de orden n, $\mathrm{Aut}(\Gamma) \cong S_n$ si y solo si $\Gamma \cong K_n$, ver [8, 19].

Proposición 3.2. *Cada automorfismo de un anillo R induce un automorfismo de $\Gamma(R)$. En particular, existe un homomorfismo de grupos $\phi : \mathrm{Aut}(R) \longrightarrow \mathrm{Aut}(\Gamma(R))$ dado por: si $f \in \mathrm{Aut}(R)$, entonces $f|_{Z(R)} \in \mathrm{Aut}(\Gamma(R))$.*

Demostración. Sean $f \in \mathrm{Aut}(R)$ y $x, y \in \Gamma(R)$ tal que $\{x, y\} \in E(\Gamma(R))$. Dado que $xy = 0$, entonces $0 = f(xy) = f(x)f(y)$, así $f(x)$ y $f(y)$ son adyacentes en $\Gamma(R)$. Esto implica que $f \in \mathrm{Aut}(\Gamma(R))$. Ahora, considere $\phi : \mathrm{Aut}(R) \longrightarrow \mathrm{Aut}(\Gamma(R))$, definido por $\phi(f) = f|_{Z(R)}$. Sean $f, g \in \mathrm{Aut}(R)$. Entonces $\phi(f \circ g) = (f \circ g)|_{Z(R)} = f|_{Z(R)}\,(g|_{Z(R)}) = \phi(f) \circ \phi(g)$. □

Teorema 3.3. *Sea R un anillo conmutativo finito el cual no es un cuerpo y $f \in \mathrm{Aut}(R)$. Si $f(x) = x$ para todo $x \in Z(R)$, entonces $f = Id_R$. Así $\phi : \mathrm{Aut}(R) \longrightarrow \mathrm{Aut}(\Gamma(R))$ es un monomorfismo.*

Demostración. Primero supóngase que R tiene dos ideales maximales M y N. Entonces como los elementos de M y N son divisores de cero, ver Proposición 1.69, se tiene que $M, N \subset D(R)$. Como $M \subset M + N$ y M es maximal, se tiene que $R = M + N$. Así, para todo $r \in R$

$$r = m + n, \text{ con } m \in M \text{ y } n \in N.$$

Es decir, $f(r) = f(m+n) = f(m) + f(n) = m + n = r$.

Ahora, supóngase que R es local, con ideal maximal M. Para cualquier $m \in M$ y $u \in U(R)$, se tiene

$$um = f(um) = f(u)m,$$

de ahí que $(f(u)-u)m = 0$, con $f(u)-u \in M$, entonces $f(u) = u+x$, para algún $x \in M$. Entonces, $xM = 0$. Por la Proposición 1.69 se tiene que $\text{car}(R) = p^n$ y así $|R/M| = p^m$, para algún primo p y enteros m, n mayores o iguales a 1, ver [14, Thm. 22.1]. Por lo anterior y el Corolario 4 en [14, Pág. 149] se tiene que $(u+M)^{p^m-1} = 1 + M$, luego $u^{p^m-1} + M = 1 + M$. En consecuencia, $u^{p^m-1} = 1 + y$ con $y \in M$. Entonces $f(u^{p^m-1}) = f(1+y) = f(1) + f(y) = 1 + y = u^{p^m-1}$, pero

$$u^{p^m-1} = f(u^{p^m-1}) = f(u)^{p^m-1} = (u+x)^{p^m-1} = \sum_{i=0}^{p^m-1} \binom{p^m-1}{i} u^{p^m-1-i}x^i$$

$$= u^{p^m-1} + \binom{p^m-1}{1} u^{p^m-2}x + \sum_{i=2}^{p^m-1} \binom{p^m-1}{i} u^{p^m-1-i}x^i.$$

Como $x \in M$ y $xM = 0$. Entonces $x^i = 0$ para todo i mayor igual que 2.

Así $u^{p^m-1} = u^{p^m-1} + (p^m-1)u^{p^m-2}x$, es decir $(p^m-1)u^{p^m-2}x = 0$. Dado que $p^m - 1$ y u^{p^m-2} son unidades en R ($\text{mcd}(p^m-1, p) = 1$) , se tiene que $x = 0$. Así $f(u) = u$ para todo $u \in U(R)$. Por lo tanto, $f = Id_R$. De esta forma, $\phi(Id_R) = Id_{\Gamma(R)}$ y así ϕ es un monomorfismo.

□

De la Definición 1.11, se tiene que el grado de un vértice x de $\Gamma(R)$, está dado por

$$\deg(x) = |\{y \in Z(R) : yx = 0 \text{ y } y \neq x\}|.$$

Proposición 3.4. *Sean $n \geq 4$ un entero compuesto y $X = \{d \in \mathbb{Z} : 1 < d < n \text{ y } d|n\}$; para cada $d \in X$ se forma el conjunto $V_d = \{x \in \mathbb{Z}_n : 1 < x < n \text{ y } \text{mcd}(x, n) = d\}$. Entonces se sastisfacen la siguientes propiedades:*

1. *El conjunto de los divisores de cero es igual a la unión disjunta de los conjuntos V_d; es decir*

$$Z(\mathbb{Z}_n) = \bigcup_{d \in X} V_d,$$

   con $V_d \cap V_e = \emptyset$, para $d \neq e$.

2. *Para $x \in V_d$, se tiene que el subgrupo $\text{ann}(x) = \text{ann}(d)$ tiene orden d en $\mathbb{Z}_n$.*

3. *Para cualesquiera $x, y \in V_d$ y $a \in \mathbb{Z}_n$, $ax = 0$ si y solo si $ay = 0$.*

4. *Si $x \in V_d$, entonces $\deg(x) = \deg(d)$.*

5. *Para $d \in X$, se tiene que*

$$\deg(d) = \begin{cases} d-1, & \text{si } n \nmid d^2, \\ d-2, & \text{si } n \mid d^2. \end{cases} \tag{3.1}$$

6. *Sean $d, e \in X$. Entonces $\deg(d) = \deg(e)$ si y solo si $d = e$.*

Demostración.

1. Supóngase que d y e son dos elementos distintos de X, tales que $V_d \cap V_e \neq \emptyset$. Entonces existe $u \in V_d \cap V_e$, en consecuencia $\mcd(u, n) = d$ y $\mcd(u, n) = e$, esto implica que $d = e$, lo cual es una contradicción. Por lo tanto, $\bigcap_{d\in X} V_d = \emptyset$. Sea $x \in Z(\mathbb{Z}_n)$ con $k = \mcd(x, n) > 1$, ver Proposición 1.65. Note que esto significa que $x \in V_k$, por lo tanto $Z(\mathbb{Z}_n) \subseteq \bigcup_{d\in X} V_d$. Por otro lado, sea $z \in \bigcup_{d\in X} V_d$, entonces $\mcd(z, n) = d$, para algún $d \in X$. Por el Lema de Bezout se puede afirmar que existen enteros a y b tales que $d = za + nb$. Luego, en $\mathbb{Z}_n$

$$d = za. \tag{3.2}$$

   Ahora, como $d \mid n$ entonces $dh = n$, para algún $h \in \mathbb{Z}^+$, si se multiplica por h en la igualdad (3.2), se tiene que $dh = 0 = zah$ en $\mathbb{Z}_n$; así $z \in Z(\mathbb{Z}_n)$. Entonces $\bigcup_{d\in X} V_d \subseteq Z(\mathbb{Z}_n)$. Por lo tanto, $\bigcup_{d\in X} V_d = Z(\mathbb{Z}_n)$.

2. Sea $a \in \operatorname{ann}(x)$. Como $d = \mcd(x, n)$; existen enteros m y k tales que $d = mx+nk$. Entonces en $\mathbb{Z}_n$, se tiene que $d = mx$, esto significa que $ad = a(mx) = 0$. En consecuencia $a \in \operatorname{ann}(d)$, es decir $\operatorname{ann}(x) \subseteq \operatorname{ann}(d)$. Ahora, sea $b \in \operatorname{ann}(d)$. Como $d \mid x$ se tiene que $x = dk$, con $k \in \mathbb{Z}$. Entonces en $\mathbb{Z}_n$, $bx = b(dk) = 0$. Así $b \in \operatorname{ann}(x)$. Por lo tanto, $\operatorname{ann}(x) = \operatorname{ann}(d)$. Luego, observe que $\operatorname{ann}(d) = \{z \in Z(\mathbb{Z}_n) : zd = 0\}$, como $d \mid n$, existe un entero positivo k tal que $dk = n$, es decir, $\operatorname{ann}(d) = \{0, k, 2k, \ldots, (d-1)k\}$, dado que al multiplicarlos por d son cero módulo n. De esta forma, $|\operatorname{ann}(d)| = d$.

   La demostraciones de los ítems (3) y (4), se siguen directamente de la afirmación del ítem (2).

5. Note que $\deg(d) = |\operatorname{ann}(d) - \{0, d\}|$. Entonces si $n \mid d^2$, $\deg(d) = |\operatorname{ann}(d) - \{0, d\}| = d-2$, porque $d \in \operatorname{ann}(d)$. Mientras que si $n \nmid d^2$, entonces $\deg(d) = d-1$.

6. Supóngase que $\deg(d) = \deg(e)$, con $d < e$. Entonces por el ítem (5), se tienen los siguientes casos.

   - $d - 1 = e - 1$.
   - $d - 2 = e - 1$.
   - $d - 2 = e - 2$.
   - $d - 1 = e - 2$.

Note que los tres primeros casos contradicen el hecho de que $d < e$, entonces $d - 1 = e - 2$. De ahí que $e = d + 1$. Como $n \mid e^2$, esto implica que $n \mid (d+1)^2$. Por otro lado, se tiene que $d \mid n$ y $e \mid n$, y como $\text{mcd}(d, e) = 1$, en consecuencia $de \mid n$ esto es $d(d+1) \mid n$, luego $d(d+1) \mid (d+1)^2$, es decir $d \mid d+1$, lo que es una contradicción. Por lo tanto, $\deg(d) = \deg(e)$, implica que $d = e$.

□

Teorema 3.5. *Sea $n \geq 4$ un entero compuesto. Entonces,* $\text{Aut}(\Gamma(\mathbb{Z}_n))$ *es un producto directo finito de grupos simétricos. Específicamente,*

$$\text{Aut}(\Gamma(\mathbb{Z}_n)) \cong \prod_{d \in X} S_{n_d},$$

donde $n_d = |V_d|$.

Demostración. Dado que dos vértices de $\Gamma(\mathbb{Z}_n)$ tienen el mismo grado si y solo si están en el mismo conjunto de V_d (ver ítems (4) y (6) en la Proposición 3.4) y un automorfismo de grafos preserva grados, se tiene que $f(V_d) = V_d$ para cada $f \in \text{Aut}(\Gamma(\mathbb{Z}_n))$ y $d \in X$. En consecuencia, dado que $Z(\mathbb{Z}_n) = \bigcup_{d \in X} V_d$ se puede definir una función

$$\phi : \text{Aut}(\Gamma(\mathbb{Z}_n)) \longrightarrow \prod_{d \in X} S_{n_d},$$

donde $\phi(f) = f|_{V_d}$, con $f|_{V_d}$ visto como un elemento de S_{n_d}. Ahora, ϕ es monomorfismo de grupos. En efecto,

$$\phi(f \circ g) = (f \circ g)\,|_{V_d} = f(g\,|_{V_d}) = \phi(f) \circ \phi(g).$$

Además, suponga que $\phi(f) = f|_{V_d} = Id|_{V_d}$; entonces $f(x) = x$, para todo $x \in V_d$ y para cada $d \in X$. Dado que

$$Z(\mathbb{Z}_n) = \bigcup_{d \in X} V_d,$$

esto implica que, $f(x) = x$ para todo $x \in Z(\mathbb{Z}_n)$. Entonces, por el Teorema 3.3, se tiene que $f(x) = Id_R$.

Para demostrar que ϕ es sobreyectiva basta probar que para cada $d \in X$ y cada permutación α de V_d, existe $f \in \text{Aut}(\Gamma(\mathbb{Z}_n))$ con $f|_{V_d} = \alpha$ y $f(y) = y$, para todo $y \in V_{d'}$, con $d' \neq d$ en X. Por lo tanto, $\text{Aut}(\Gamma(\mathbb{Z}_n))$ es isomorfo a $\prod_{d \in X} S_{n_d}$. □

Es bien conocido que el Teorema de Frucht afirma que cualquier grupo finito G es isomorfo a $\text{Aut}(\Gamma)$ para algún grafo Γ, ver [8, Thm. 4.1]. Por esta razón, es interesante conocer exactamente cuáles grupos se pueden realizar como $\text{Aut}(\Gamma(R))$, para cualquier anillo en general; o conocer la estructura del grupo $\text{Aut}(\Gamma(\mathbb{Z}_n))$ en particular. El siguiente corolario da una respuesta parcial para $\text{Aut}(\Gamma(\mathbb{Z}_n))$.

Corolario 3.6. *Sea $n \geq 4$ un entero compuesto. Entonces:*

1. $\mathrm{Aut}(\Gamma(\mathbb{Z}_n))$ *es trivial si y solo si* $n = 4$,

2. $\mathrm{Aut}(\Gamma(\mathbb{Z}_n))$ *es abeliano si y solo si* $n = 4, 6, 8, 9$ *o* 12.

Demostración.

1. Por el Teorema 3.5,
$$\mathrm{Aut}(\Gamma(\mathbb{Z}_n)) \cong \prod_{d \in X} S_{n_d},$$
donde para $n = 4$ se tiene que $X = \{d \in \mathbb{Z} : 1 < d < 4 \text{ y } d \mid 4\} = \{2\}$. Entonces, $V_2 = \{x \in \mathbb{Z}_4 : 1 < x < 4 \text{ y } \mathrm{mcd}(x, 4) = 2\} = \{2\}$. Así, $n_2 = 1$ y $S_{n_2} = S_1 = \{Id_1\}$ es el grupo trivial. Por lo tanto, $\mathrm{Aut}(\Gamma(\mathbb{Z}_4)) \cong S_1$.

2. - Para $n = 6$, se sabe que $X = \{d \in \mathbb{Z} : 1 < d < 6 \text{ y } d \mid 6\} = \{2, 3\}$. Entonces, $V_2 = \{x \in \mathbb{Z}_6 : 1 < x < 6 \text{ y } \mathrm{mcd}(x, 6) = 2\} = \{2, 4\}$ y $n_2 = |V_2| = 2$. Luego, $V_3 = \{x \in \mathbb{Z}_6 : 1 < x < 6 \text{ y } \mathrm{mcd}(x, 6) = 3\} = \{3\}$ y $n_3 = |V_3| = 1$. Así, $\mathrm{Aut}(\Gamma(\mathbb{Z}_6)) \cong S_{n_2} \times S_{n_3} = S_2 \times S_1 \cong S_2$.
   - Para $n = 8$, se tiene que $X = \{2, 4\}$. Entonces, $V_2 = \{x \in \mathbb{Z}_8 : 1 < x < 8 \text{ y } \mathrm{mcd}(x, 8) = 2\} = \{2, 6\}$ y $n_2 = 2$. Luego, $V_4 = \{x \in \mathbb{Z}_8 : 1 < x < 8 \text{ y } \mathrm{mcd}(x, 8) = 4\} = \{4\}$ y $n_4 = 1$. Así, $\mathrm{Aut}(\Gamma(\mathbb{Z}_8)) \cong S_{n_2} \times S_{n_4} = S_2 \times S_1 \cong S_2$.
   - Si $n = 9$, se tiene $X = \{3\}$. Entonces, $V_3 = \{x \in \mathbb{Z}_9 : 1 < x < 9 \text{ y } \mathrm{mcd}(x, 9) = 3\} = \{3, 6\}$ y $n_3 = 2$. Así, $\mathrm{Aut}(\Gamma(\mathbb{Z}_9)) = S_{n_3} = S_2$.
   - Finalmente, para $n = 12$, se tiene $X = \{2, 3, 4, 6\}$. Entonces,
$$\begin{aligned} V_2 &= \{2, 10\} \text{ y } n_2 = 2, \\ V_3 &= \{3, 9\} \text{ y } n_3 = 2, \\ V_4 &= \{4, 8\} \text{ y } n_4 = 2, \\ V_6 &= \{6\} \text{ y } n_6 = 1. \end{aligned}$$
   Así, $\mathrm{Aut}(\Gamma(\mathbb{Z}_{12})) \cong S_{n_2} \times S_{n_3} \times S_{n_4} \times S_{n_6} = S_2 \times S_2 \times S_2 \times S_1 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

   Por lo tanto, en todos los casos $\mathrm{Aut}(\Gamma(\mathbb{Z}_n))$ es abeliano.

   Recíprocamente, se muestra que $\mathrm{Aut}(\Gamma(\mathbb{Z}_n))$ es no abeliano para todos los otro enteros compuestos $n \geq 4$. Es suficiente mostrar que en cada caso, se puede encontrar un d, tal que $n_d \geq 3$ y de ahí que $\mathrm{Aut}(\Gamma(\mathbb{Z}_n))$ tiene entre uno de sus factores a S_m, para algún $m \geq 3$, por lo que no es abelliano.

   - Si $n = 2^r$, con $r \geq 4$. Entonces, $\{2, 6, 10\} \subseteq V_2$ ya que $\mathrm{mcd}(x, n) = 2$ para $x = 2, 6, 10, \ldots$
   - Si $n = 3^r$, con $r \geq 3$. Entonces, $\{3, 6, 15\} \subseteq V_3$ porque $\mathrm{mcd}(x, n) = 3$ para $x = 3, 6, 15, \ldots$
   - Si $n = p^r$, con p primo y $p \geq 5$. Como el $\mathrm{mcd}(x, n) = p$ para $x = p, 2p, 3p$, entonces $\{p, 2p, 3p\} \subseteq V_p$.

- Si $n = p_1^{r_1} \cdots p_k^{r_k}$ su factorización prima. Ahora, si $p_1 \leq 3$ y $k \leq 2$, entonces $\{p_1, 2p_1, 4p_1\} \subseteq V_{p_1}$. Así, se puede suponer que $p_1 = 2$ con $r = r_1 \leq 1$ y $k \leq 2$. Si $n > 2^r \cdot 3$, entonces $\{2^r, 2^{r+1}, 2^{r+2}\} \subseteq V_{2^r}$. De ahí que, se puede suponer que $n = 2^r \cdot 3$. Si $r \leq 3$, entonces $\{2, 10, 14\} \subset V_2$.

Por lo tanto, $\mathrm{Aut}(\Gamma(\mathbb{Z}_n))$ es abeliano si y solo si $n \in \{4, 6, 8, 9, 12\}$.

□

A continuación, se ejemplifica $\mathrm{Aut}(\Gamma(R))$.

Ejemplo 3.7. Sean F y K cuerpos finitos con distinto orden m y n, respectivamente. Como en el Ejemplo 2.5, $\Gamma(F \times K)$ es un grafo bipartito completo $K_{m-1,n-1}$. De ahí que, $\mathrm{Aut}(\Gamma(F \times K)) \cong S_{m-1} \times S_{n-1}$ y tiene orden $(m-1)!(n-1)!$. También, $\Gamma(F \times F)$ es un grafo bipartito completo $K_{m-1,m-1}$.

Para la comprensión del siguiente ejemplo y el como se caracteriza el conjunto X y el cardinal de cada conjunto V_d tenga en cuenta el enunciado de la Proposición 3.4.

Ejemplo 3.8. Sea $R = \mathbb{Z}_{1225}$ con $|\Gamma(R)| = 384$. Entonces, $X = \{5, 7, 25, 35, 49, 175, 245\}$ y se calcula $n_5 = 168$, $n_7 = 120$, $n_{25} = 42$, $n_{35} = 24$, $n_{49} = 20$, $n_{175} = 6$ y $n_{245} = 4$. Luego, $\mathrm{Aut}(\Gamma(R)) \cong S_{168} \times S_{120} \times S_{42} \times S_{24} \times S_{20} \times S_6 \times S_4$ y tiene orden $168! \cdot 120! \cdot 42! \cdot 24! \cdot 6! \cdot 4!$.

Capítulo 4

Representación de grafos divisores de cero de anillos $\mathbb{Z}_n$

En el artículo "Representación de grafos divisores de cero para anillos", ver [18]; se recopilan resultados relevantes de $\Gamma(R)$ y además, se presentan algunas caracterizaciones de los grafos divisores $\Gamma(\mathbb{Z}_m)$. En particular, se estudian estos grafos para anillos de la forma $\mathbb{Z}_{p^n q}$, donde p y q son primos y n un entero positivo mayor que 1; su principal enfoque es presentar el algoritmo para determinar el grafo de los divisores de cero en este tipo de anillos.

En este capítulo, se hará una implementación del algoritmo sugerido en el mencionado artículo en el software libre `SageMath` creado en 2005 por William Stein, ver este software está basado en el lenguaje de programación de Python.

En primer lugar, se crea el siguiente código en `SageMath` que encuentra una lista de los divisores de cero de anillos $\mathbb{Z}_n$.

```
def divisores_de_cero(n):
"Recibe un entero positivo n y retorna la lista de los divisores de
    cero de Z_n"
D=[]
for i in [1..n-1]:
    if gcd(i,n)!=1:
        D.append(i)
return(D)
```

A continuación se presenta un ejemplo de la aplicación de esta función para encontrar los divisores de cero de los anillos $\mathbb{Z}_{14}$ y $\mathbb{Z}_{30}$.

```
divisores_de_cero(14)
[2, 4, 6, 7, 8, 10, 12]
```

```
divisores_de_cero(30)
[2, 3, 4, 5, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24,
25, 26, 27, 28]
```

Uno de los métodos para determinar el grafo de los divisores de cero de un anillo $\mathbb{Z}_n$ de forma generalizada, es que se reciba el n, con ayuda de la función `Divisores_de_cero` se determine una lista de sus divisores de cero de $\mathbb{Z}_n$ y luego se establezcan cuáles de estos elementos son adyacentes. Logrando así, retornar el grafo del anillo.

```
def Grafo_divisores_de_cero_gen(n):
"Recibe n y calcula el grafo de los divisores de cero de Z_n"
D=Divisores_de_cero(n)
E={}
while len(D)!=0:
    d=D.pop(0)
    E[d]=[]
    for x in D:
        if mod(x*d,n)==0:
            E[d].append(x)
E1= {c:v for c,v in E.items() if v !=[]}
G=Graph(E1)
return(G.plot())
```

Ahora, se presenta un ejemplo de cómo se genera un grafo de los divisores de cero del anillo $\mathbb{Z}_{15}$ utilizando la función `Grafo_divisores_de_cero_gen`.

```
Grafo_divisores_de_cero_gen(15)
```

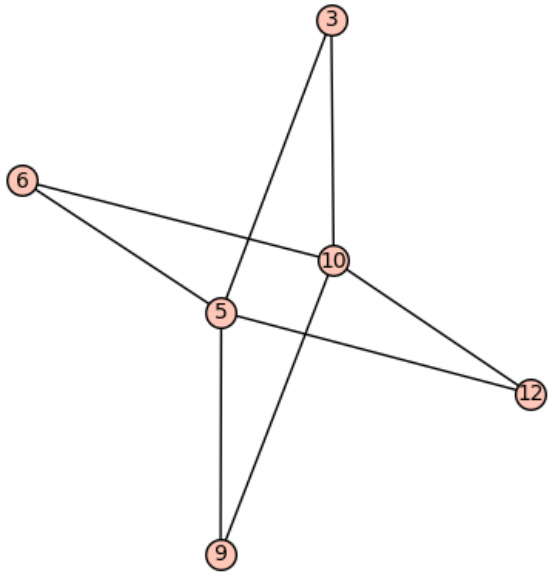


Figura 4.1: Grafo de los divisores de cero del anillo $\mathbb{Z}_{15}$.

N. H. Shuker, H. Q. Mohammad y A. M. Ali en [21, Thm. 2.2] establecen una caracterización de los grafos $\Gamma(Z(\mathbb{Z}_{p^nq}))$, donde p y q son primos diferentes y $n \in \mathbb{Z}^+$. Este resultado establece que se puede encontrar una partición de $Z(\mathbb{Z}_{p^nq})$ en conjuntos disjuntos independientes; esto es para cada conjunto en esta partición se tiene que sus elementos no son adyacentes entre sí. A continuación, se presenta este resultado sin demostración.

Teorema 4.1. *Si p y q son primos distintos y n es un entero positivo mayor que* 1. *Entonces:*

1. *Si n es par, $\Gamma(\mathbb{Z}_{p^nq})$ es $p^{\frac{n}{2}}$-partito,*

2. *Si n es impar, $\Gamma(\mathbb{Z}_{p^nq})$ es $(p^{\frac{n-1}{2}}+1)$-partito.*

La idea fundamental para la demostración del anterior resultado consiste en probar que dependiendo del valor de n, se puede calcular una partición de $Z(\mathbb{Z}_n)$. En particular, se demuestra que

- Si n es par, entonces
$$Z(\mathbb{Z}_n) = A_0 \cup A_1 \cup A_i,$$
donde

  1. $A_0 = \{x \in Z(\mathbb{Z}_{p^n \cdot q}) : p \mid x \text{ y } q \nmid x\}$. Como todos los vértices que son divisibles por p no son divisibles por q, entonces los vértices no son adyacentes en $\Gamma(\mathbb{Z}_{p^n \cdot q})$.

2. $A_1 = \{x \in Z(\mathbb{Z}_{p^n \cdot q}) : q \mid x \text{ y } p \nmid x\} \cup \{x \in Z(\mathbb{Z}_{p^n \cdot q}) : p^t q \mid x \text{ y } p^{\frac{n}{2}} q \nmid x\} \cup \{x \in Z(\mathbb{Z}_{p^n \cdot q}) : x = p^{\frac{n}{2}} q\}$, donde $1 \leq t \leq \frac{n}{2} - 1$. En este conjunto, los vértices tampoco son adyacentes entre ellos.
3. $A_i = \{x \in Z(\mathbb{Z}_{p^n \cdot q}) : x = ip^{\frac{n}{2}} q\}$, donde $2 \leq i \leq p^{\frac{n}{2}} - 1$. En este conjunto los vértices si son adyacentes entre ellos ya que todos son múltiplos de $p^{\frac{n}{2}} q$.

- Si n es impar, entonces

$$Z(\mathbb{Z}_n) = A_1 \cup A_2 \cup B_i,$$

donde

1. $A_1 = \{x \in Z(\mathbb{Z}_{p^n q}) : q \mid x \text{ y } p \nmid x\}$. Note que en este conjunto los vértices no son adyacentes por la misma razón que se indicó en la definición del conjunto A_0.
2. $A_2 = \{x \in Z(\mathbb{Z}_{p^n q}) : q \mid x \text{ y } p \nmid x\} \cup \{x \in Z(\mathbb{Z}_{p^n \cdot q}) : p^t q \mid x \text{ y } p^{\frac{n+1}{2}} q \nmid x\}$, donde $1 \leq t \leq \frac{n-1}{2}$. Se puede observar que no hay adyacencia entre los elementos de este conjunto.
3. $B_i = \{x \in Z(\mathbb{Z}_{p^n q}) : ip^{\frac{n+1}{2}} q\}$, donde $1 \leq i \leq p^{\frac{n-1}{2}} - 1$. En estos conjuntos se puede presentar una adyacencia, claramente si entre ellos su producto es cero módulo $p^m \cdot q$.

Estas ideas dadas en [21], fueron usadas por J. Otero y J. Salazar en [18] para proponer un algoritmo para encontrar $\Gamma(\mathbb{Z}_{p^n q})$, para p, q y n dados.

En este trabajo, se utilizaron las ideas de los dos artículos anteriormente mencionados para implementar en `SageMath` la función `Particion_divisores_de_cero`. Esta función calcula la partición propuesta en la demostración del Teorema 4.1 de $Z(\mathbb{Z}_{p^n q})$. A partir de esta representación se calculan las relaciones de adyacencia entre los vértices de conjuntos diferentes en la partición anteriormente calculada.

En la implementación que se presenta en este trabajo en `SageMath`, se ingresan p, n y q, y se construye el anillo $\mathbb{Z}_{p^n q}$. Entonces se determina el conjunto de los divisores de cero del anillo construido. Ahora, es importante identificar si n es par o impar, ya que en el Teorema 4.1 se deduce los conjuntos que ayudarán a obtener la partición del conjunto de los divisores de cero del anillo. Para conocer cómo serán estos conjuntos o que elementos se encuentran en cada uno de ellos, se utilizará la demostración del Teorema 4.1 que se puede ver en el artículo [21].

Posteriormente, se determina la adyacencia de los elementos entre los conjuntos, teniendo en cuenta que x y y estén conjuntos diferentes son adyacentes siempre y cuando $xy = 0$. Una vez calculadas estas conexiones se genera la representación del grafo del anillo ingresado con ayuda de las funciones `Graph` y `plot`. A continuación, se presenta la implementación realizada.

```
def Particion_divisores_de_cero(p,n,q):
"Recibe dos primos p,q y un entero n mayor que 1. Y, calcula el grafo
    de los divisores de cero de Z_{p^n*q}"
```

```
m=p^n*q
D=Divisores_de_cero(m)
if mod(n,2)==0:
    A0=[]
    for x in D:
        if mod(x,p)==0 and mod(x,q)!=0:
            A0.append(x)
    Ai=[]
    k=p^(n/2)
    for i in [2..k-1]:
        Ai.append(i*k*q)
    B=A0+Ai
    A1=[x for x in D if x not in B]
    E1={}
    for x in A0:
        E1[x]=[]
        for y in A1:
            if mod(x*y,m)==0:
                E1[x].append(y)
        for z in Ai:
            if mod(x*z,m)==0:
                E1[x].append(z)
    for x in A1:
        E1[x]=[]
        for z in Ai:
            if mod(x*z,m)==0:
                E1[x].append(z)
    while len(Ai)!=0:
        d=Ai.pop(0)
        E1[d]=[]
        for x in Ai:
            if mod(x*d,m)==0:
                E1[d].append(x)
    E2= {c:v for c,v in E1.items() if v !=[]}
    G=Graph(E2)
else:
    A2=[]
    for x in D:
        if mod(x,p)==0 and mod(x,q)!=0:
            A2.append(x)
    Bi=[]
    k=p^((n+1)/2)
    j=p^((n-1)/2)
    for i in [1..j-1]:
        Bi.append(i*k*q)
    B=A2+Bi
    A3=[x for x in D if x not in B]
    E3={}
    for x in A2:
        E3[x]=[]
        for y in A3:
            if mod(x*y,m)==0:
```

```
                    E3[x].append(y)
            for z in Bi:
                if mod(x*z,m)==0:
                    E3[x].append(z)
        for x in A3:
            E3[x]=[]
            for z in Bi:
                if mod(x*z,m)==0:
                    E3[x].append(z)
        while len(Bi)!=0:
            d=Bi.pop(0)
            E3[d]=[]
            for x in Bi:
                if mod(x*d,m)==0:
                    E3[d].append(x)
        E4= {c:v for c,v in E3.items() if v !=[]}
        G=Graph(E4)
    return(G.plot())
```

Ejemplo 4.2. A continuación, se muestra la utilización de la función `Particion_divisores_de_cero` para encontrar el grafo de los divisores de cero del anillo $\mathbb{Z}_{18}$ Observe que $18 = 3^2 2$; es decir, en este caso se tiene que n es par.

```
Particion_divisores_de_cero(3,2,2)
```

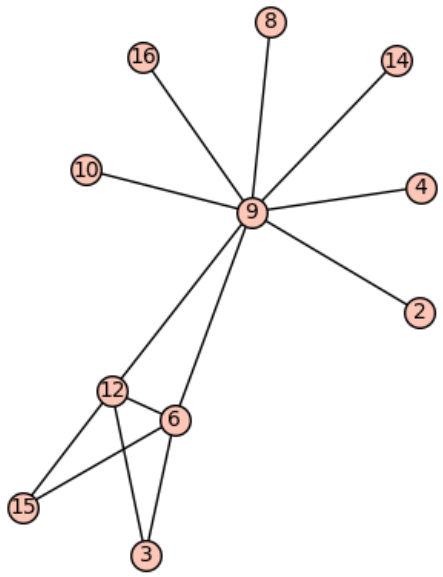


Figura 4.2: Grafo del anillo $\mathbb{Z}_{3^2 2}$.

Ejemplo 4.3. Ahora se encuentra el grafo $\Gamma(\mathbb{Z}_{24})$. Vale la pena anotar que $24 = 2^3 3$.

```
Particion_divisores_de_cero(2,3,3)
```

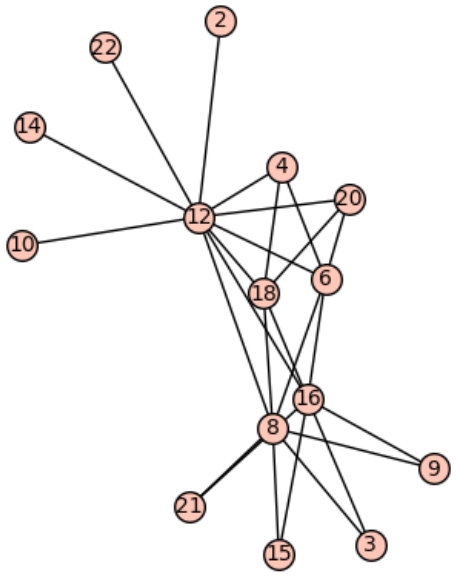


Figura 4.3: Grafo de los divisores de cero del anillo $\mathbb{Z}_{2^3 3}$.

Finalmente, se realiza un caso particular en base de la anterior función, donde se recibe un anillo de la forma $\mathbb{Z}_{p^n q}$ y regresa, un grafo bipartito o un mensaje diciendo que no es un grafo bipartito. El código recibe p, n y q, en seguida se calcula el conjunto de los divisores de cero. Después, determina si $p = 2$ y $n = 2$ ya que en este caso, según el Teorema 4.1, el grafo de los divisores de cero es un grafo bipartito. En la función `Grafos_bipartitos_divisores_de_cero` se utilizan ideas similares a las usadas en la función `Particion_divisores_de_cero` para cuando n es par. Por último, se genera el grafo de los divisores de cero del anillo usando la función `BipartiteGraph`. En caso contrario, si n o p no son iguales a 2, se regresa un mensaje diciendo: `No es un grafo bipartito`.

```
def Grafos_bipartitos_divisores_de_cero(p,n,q):
    "Recibe p,n igual a 2 y un primo q. Y, calcula el grafo bipartito de
       los divisores de cero de Z_{p^n*q}"
    m=p^n*q
    D=divisores_de_cero(m)
    A0=[]
    if n==2 and p==2:
        for x in D:
            if mod(x,p)==0 and mod(x,q)!=0:
```

```
                A0.append(x)
        Ai=[]
        k=p^(n/2)
        for i in [2..k-1]:
            Ai.append(i*k*q)
        B=A0+Ai
        A1=[x for x in D if x not in B]
        E={}
        for x in A0:
            E[x]=[]
            for y in A1:
                if mod(x*y,m)==0:
                    E[x].append(y)
            for z in Ai:
                if mod(x*z,m)==0:
                    E[x].append(z)
        for x in A1:
            E[x]=[]
            for z in Ai:
                if mod(x*z,m)==0:
                    E[x].append(z)
        while len(Ai)!=0:
            d=Ai.pop(0)
            E[d]=[]
            for x in Ai:
                #print([d,x])
                if mod(x*d,m)==0:
                    E[d].append(x)
        E1= {c:v for c,v in E.items() if v !=[]}
        G=BipartiteGraph(E1)
        return(G.plot())
    else:
        print('No es un grafo bipartito')
```

Ejemplo 4.4. Se calcula el grafo bipartito de los divisores de cero del anillo $\mathbb{Z}_{20}$.

```
Grafos_bipartitos_divisores_de_cero(2,2,5)
```

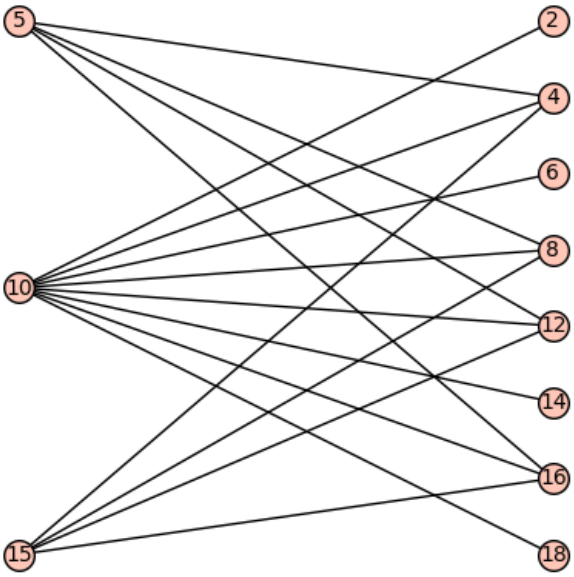


Figura 4.4: Grafo bipartito de los divisores de cero del anillo $\mathbb{Z}_{2^2 5}$.

Ejemplo 4.5. Además, se muestra que para el caso cuando $p \neq 2$, la función identifica que el grafo $\Gamma(\mathbb{Z}_{3^2 5})$ no es bipartito.

```
Grafos_bipartitos_divisores_de_cero(3,2,5)
 No es un grafo bipartito
```

Capítulo 5

Conclusiones

- El estudio desarrollado en este trabajo permite ver de manera precisa una conexión entre las propiedades de la estructura algebraica de un anillo y la estructura discreta de un grafo.
- Para adentrarse en el estudio de los grafos de los divisores de cero de anillos conmutativos es necesario tener un buen manejo de álgebra conmutativa. De hecho durante este trabajo se realizó una revisión de los conceptos básicos de la teoría de anillos para poder entender las demostraciones presentadas en el artículo [3]. Sin embargo, dado que en el programa de Licenciatura en Matemáticas no se profundizan en estos temas, no se pudo presentar todas la demostraciones de los resultados del citado artículo.
- Los ejemplos que se desarrollaron en este trabajo fueron fundamentales para el entendimiento de los principales resultados del artículo. Se espera que los mismos sean usados en futuros trabajos de grado e investigaciones.
- Las implementaciones desarrolladas en `SageMath` en el Capítulo 4 ayudaron comprender los resultados teóricos presentados en los artículos [18] y [21], y adicionalmente a presentar de manera más ágil y organizada ejemplos de $\Gamma(\mathbb{Z}_n)$. Se debe anotar que no se pretendía que estas implementaciones fueran eficientes desde el punto de vista computacional; sin embargo, en ellas se puede evidenciar el aprendizaje de los conceptos estudiados. Estas implementaciones podrán ser utilizadas en futuras investigaciones acerca del tema.

Referencias

[1] S. Akbari and A. Mohammadian. On the zero-divisor graph of a commutative ring. *Journal of algebra*, 274(2):847–855, 2004.

[2] D. F. Anderson and A. Badawi. On the zero-divisor graph of a ring. *Communications in Algebra*, 36(8):3073–3092, 2008.

[3] D. F. Anderson and P. S. Livingston. The zero-divisor graph of a commutative ring. *Journal of algebra*, 217(2):434–447, 1999.

[4] D. F. Anderson and S. B. Mulay. On the diameter and girth of a zero-divisor graph. *Journal of pure and applied algebra*, 210(2):543–550, 2007.

[5] D. F. Anderson and M. Naseer. Beck's coloring of a commutative ring. *Journal of algebra*, 159(2):500–514, 1993.

[6] T. Asir and T. T. Chelvam. On the total graph and its complement of a commutative ring. *Communications in algebra*, 41(10):3820–3835, 2013.

[7] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Company, 1969.

[8] L. Babai. Automorphism groups, isomorphism, reconstruction. In *Handbook of combinatorics (vol. 2)*, pages 1447–1540. 1996.

[9] I. Beck. Coloring of commutative rings. *Journal of algebra*, 116(1):208–226, 1988.

[10] B. Bollobás. *Graph theory: an introductory course*. Springer Verlag, 1979.

[11] G. Chartrand and P. Zhang. *A first course in graph theory*. Dover Publications, 2012.

[12] T. T. Chelvam and T. Asir. A note on total graph of $\mathbf{Z}_n$. *Journal of Discrete Mathematical Sciences and Cryptography*, 14(1):1–7, 2011.

[13] R. Diestel. *Graph Theory*. Springer, 5th edition, 2017.

[14] J. A. Gallian. *Contemporary Abstract Algebra*. Cengage Learning, 8th edition, 2013.

[15] I. Kaplansky. *Commutative rings*. The University of Chicago Press, revised edition, 1974.

[16] P. S. Livingston. Structure in zero-divisor graphs of commutative rings. Master's thesis, University of Tennessee, 1997.

[17] B. R. McDonald. *Finite rings with identity*. Marcel Dekker Incorporated, 1974.

[18] J. Otero, J. Salazar, and F. Villarroel. Representación de grafos divisores de cero para anillos. *Divulgaciones Matemáticas*, Vol. 19(No. 2):44–51, 2018.

[19] L. Rodriguez. Automorphism groups of simple graphs. https://www.whitman.edu/documents/Academics/Mathematics/2014/rodriglr.pdf, 2014.

[20] K. Samei. The zero-divisor graph of a reduced ring. *Journal of Pure and Applied Algebra*, 209(3):813–821, 2007.

[21] N. H. Shuker, H. Q. Mohammad, and A. M. Ali. The zero divisor graph of $\mathbb{Z}_{p^n q}$. *International Journal of Algebra*, 6(22):1049–1055, 2012.

[22] D. Weber. Zero-divisor graphs and lattices of finite commutative rings. *Rose-Hulman Undergraduate Mathematics Journal*, 12(1):4, 2011.