ANILLOS ISOMORFOS A SUS SUBANILLOS NO TRIVIALES

JESÚS DAVID ACERO RUEDA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
MATEMÁTICAS
BUCARAMANGA
2025

ANILLOS ISOMORFOS A SUS SUBANILLOS NO TRIVIALES

JESÚS DAVID ACERO RUEDA

Trabajo de grado para optar al título de Matemático

Director
Héctor Edonis Pinedo Tapia
Doctor en ciencias matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
MATEMÁTICAS
BUCARAMANGA
2025

DEDICATORIA

A mis padres, por ser el pilar fundamental de mi vida, por su amor incondicional, sus sacrificios incansables y por enseñarme con su ejemplo el verdadero significado de la perseverancia y la dedicación.

Gracias por creer en mí incluso cuando dudé de mí mismo; este logro no sería posible sin su apoyo y confianza constantes; este trabajo de grado está dedicado a ustedes con todo mi amor y gratitud.

AGRADECIMIENTOS

“A quienes con su amor, apoyo y ejemplo iluminaron mi camino, les dedico este logro con eterna gratitud...”.

A mi mamá, Luz Mery, por ser mi gran fortaleza y ejemplo de dedicación. Tus sacrificios, enseñanzas y amor infinito me han guiado en cada paso de este camino. Gracias por creer en mí y por enseñarme que los sueños se alcanzan con esfuerzo y perseverancia. A mis papás, Elías y Andrés, por ser pilares de mi vida. Su apoyo, consejos y confianza han sido esenciales para alcanzar este momento. Gracias por inspirarme con su sabiduría y por estar siempre presentes, brindándome su amor y su ejemplo. Finalmente a mi novia Isabela, por ser mi compañera incondicional, por su paciencia, amor y apoyo constante durante este camino. Tus palabras de aliento y tu fe en mí fueron fundamentales para superar cada obstáculo. Este logro también es tuyo.

CONTENIDO

RESUMEN

TÍTULO ANILLOS ISOMORFOS A SUS SUBANILLOS NO TRIVIALES. *

AUTOR: JESÚS DAVID ACERO RUEDA **

PALABRAS CLAVE: ANILLO, SUBANILLO, ANILLOS HOMOGÉNEOS, GRUPO, GRUPOS HOMOGÉNEOS, ISOMORFISMOS.

DESCRIPCIÓN:

En este trabajo se estudian los anillos que son isomorfos a todos sus subanillos no triviales, conocidos como anillos homogéneos. Se parte de la caracterización de subanillos y homomorfismos para analizar las restricciones que esta propiedad impone a la estructura del anillo. Se demuestra que si un anillo es isomorfo a cada uno de sus subanillos propios, entonces debe ser conmutativo y sin divisores de cero no nulos. Finalmente, se establece que los únicos anillos con esta propiedad son los enteros y los anillos de enteros módulo un número primo.

---

* Trabajo de grado

** Facultad de Ciencias. Escuela de Matemáticas. Director: Héctor Edonis Pinedo Tapia, Doctor en Matemáticas.

ABSTRACT

TITLE: RINGS ISOMORPHIC TO THEIR NONTRIVIAL SUBRINGS [*]

AUTOR: JESÚS DAVID ACERO RUEDA [**]

kEYWORDS: RING, SUBRING, HOMOGENEOUS RINGS, GROUP, HOMOGENEOUS GROUP, ISOMORPHISM.

DESCRIPTION:

In this written work, rings that are isomorphic to all their non-trivial subrings, known as homogeneous rings, are studied. The study begins with the characterization of subrings and homomorphisms to analyze the structural restrictions imposed by this property. It is shown that if a ring is isomorphic to each of its proper subrings, then it must be commutative and have no non-zero zero divisors. Finally, it is established that the only rings with this property are the integers and the rings of integers modulo a prime number.

---

[*] Bachelor Thesis

[**] Mathematics School. Sciences Faculty. Director: Ph.D Héctor Edonis Pinedo Tapia.

INTRODUCCIÓN

Durante los siglos XIX y XX, matemáticos como Galois, Hilbert y Cayley contribuyeron significativamente al desarrollo de la teoría de módulos y anillos. Sus aportaciones permitieron comprender mejor la estructura de los anillos mediante homomorfismos. Un resultado clave derivado de sus estudios es el **teorema de isomorfía** que establece que si $f : R \to S$ es un homomorfismo de anillos sobreyectivo, entonces $R/\ker(f) \cong S$, donde $\ker(f)$ denota el kernel de f, ver por ejemplo el *Colorario 4.1.2* en “Cuadernos de Álgebra, No. 1: Grupos”[1].

En el presente trabajo, se clasifica aquellos anillos R para los cuales $R \cong S$ para cada subanillo no trivial S de R. Este problema está relacionado con la estructura y propiedades algebraicas de los anillos, por ejemplo, los **anillos de Dedekind** definidos en "Álgebra"[2], son anillos son unitarios, conmutativos y sin divisores de cero, y tienen la propiedad de que todo ideal no trivial se descompone de manera única como producto de ideales primos. Los anillos de Dedekind son relevantes en la teoría de anillos de números, pues modelan los enteros algebraicos en extensiones finitas de $\mathbb{Q}$. Aunque los anillos homogéneos y los de Dedekind tienen propiedades estructurales diferentes, compararlos permite entender mejor el papel de la descomposición de ideales, la existencia de divisores de cero y el comportamiento de los subanillos en distintas clases de anillos. En particular, preguntarse si un anillo homogéneo puede compartir propiedades clave con un anillo de Dedekind como su control sobre los ideales motiva el estudio y revela nuevas perspectivas sobre la clasificación de anillos. En este trabajo, se asumirá que todos los anillos

---

[1] Lezama, O.: Cuadernos de Álgebra, No. 1: Grupos. Departamento de Matemáticas, Uni- versidad Nacional de Colombia, sede de Bogotá, s.f.

[2] Lang, S.: Algebra. 3.ª. Springer, 2002.

considerados son asociativos y no necesariamente conmutativos ni unitarios.

El trabajo se estructura de la siguiente manera: primero, se precisa sobre la definición de lo que es un grupo, anillo y anillo generado por un elemento, posteriormente, se define que es un homomorfismo de grupos y anillos. Seguido a esto se presenta la definición de ideales sobre un anillo, ideal generado, así como la noción de anillo cociente e ideal principal sobre un anillo, Finalmente, se aborda las propiedades sobre grupos y anillos, cómo lo es la noción de dominio, grupo cíclico entre otras. Estas herramientas proporcionan el marco necesario para comprender los resultados relevantes y apoyar la clasificación de los anillos objeto de estudio.

1. Preliminares

En este capítulo se presentan los conceptos necesarios para entender el concepto de isomorfismo entre un anillo y sus subanillos no triviales. Las definiciones y resultados aquí expuestos se tomaron de"Abstract algebra" [3], "Cuadernos de Álgebra, No.1:Grupos" [4],"Cuadernos de Álgebra, No. 2: Anillos" [5], "Cuadernos de Álgebra, No. 3: Módulos" [6], " Rings isomorphic to their nontrivial subrings" [7] Particularmente para introducir los conceptos de homomorfismo e isomorfismo entre anillos.

1.1. Grupos

Definición 1.1.1. *Sea G un conjunto no vacío. Una **operación binaria** en G es una función $\triangle : G \times G \to G$ del producto cartesiano de G con G en G.*

Ejemplo 1.1.2. *La operación binaria **adición** de números naturales es una ley de composición:*

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

$$(a, b) \mapsto a + b.$$

---

[3] Fraleigh, J.B.: Abstract Algebra. 7th. Addison-Wesley, 2004.

[4] Lezama, O.: Cuadernos de Álgebra, No. 1: Grupos. Departamento de Matemáticas, Uni- versidad Nacional de Colombia, sede de Bogotá, s.f.

[5] Lezama, O.: Cuadernos de Álgebra, No. 2: Anillos. Departamento de Matemáticas, Uni- versidad Nacional de Colombia, sede de Bogotá, s.f.

[6] Lezama, O.: Cuadernos de Álgebra, No. 3: Módulos. Departamento de Matemáticas, Uni- versidad Nacional de Colombia, sede de Bogotá, s.f.

[7] Lojewski, Jacob y Greg Oman: Rings isomorphic to their nontrivial subrings. En: Involve, a Journal of Mathematics 11.5 (2018).

Definición 1.1.3. *Sea $*$ una operación binaria definida sobre un conjunto G se dice que la operación binaria $*$ tiene la propiedad **asociativa** si para cualesquiera elementos $a, b, c \in G$ se cumple la igualdad :*

$$a * (b * c) = (a * b) * c.$$

Definición 1.1.4. *Un **semigrupo** es un conjunto G dotado de una operación binaria asociativa $*$, y se denota por $(G, *)$.*

Ejemplo 1.1.5. *$(\mathbb{N}, +)$ es un semigrupo.*

Definición 1.1.6. *Sea $*$ una operación binaria definida sobre un conjunto G. Se dice que la operación $*$ es **conmutativa** si para cualesquiera elementos a y b de G se tiene que:*

$$a * b = b * a.$$

Definición 1.1.7. *Sea G un conjunto en el cual se ha definido una operación binaria $*$. Se dice que el elemento e de G es **neutro** o también llamado una **identidad** de G con respecto a la operación binaria $*$ si para cualquier elemento de G se tiene que:*

$$e * a = a = a * e.$$

Ejemplo 1.1.8. *En el semigrupo $(\mathbb{Z}, +)$, donde $\mathbb{Z}$ es el conjunto de números enteros y $+$ es la adición habitual, 0 es una identidad.*

Proposición 1.1.9. *En un conjunto G con una operación binaria $*$ solo puede existir un elemento neutro respecto de $*$.*

Definición 1.1.10. *Sea G un conjunto dotado de una operación binaria interna $*$, la cual posee un elemento neutro e, se dice que $u \in G$ es **invertible**. Si existe $u' \in G$ tal que $u' * u = e = u * u'$, el elemento u' se denomina el **inverso** de u respecto a la operación $*$.*

Definición 1.1.11. *Sea G un conjunto no vacío y $*$ una operación binaria definida en G. Se dice que G es un **grupo** con respecto a la operación binaria $*$, si cumple con las siguientes propiedades:*

1. *$*$ es asociativa.*
2. *En G existe un elemento neutro e respecto de $*$.*
3. *Cada elemento de G es invertible.*

Denotaremos un grupo por $(G, *)$ o simplemente G.

Definición 1.1.12. *Sea G un grupo y $S \neq \emptyset$ un subconjunto de G. Se dice que S es un **subgrupo** de G si S bajo la operación $*$ tiene estructura de grupo. En tal caso se escribe $S \leq G$.*

Proposición 1.1.13. *Sea G un grupo y $\emptyset \neq S \subseteq G$. S es un subgrupo de G respecto de la operación $*$ si, y sólo si, se cumplen las siguientes condiciones:*

1. *Si $a, b \in S$ entonces $a * b \in S$.*
2. *Si $a \in S$ entonces $a^{'} \in S$.*

Definición 1.1.14. *Sea G un grupo y sean A y B subconjuntos no vacíos de G. Se denomina **producto de los conjuntos** A y B (en ese orden) al producto de conjuntos de la forma ab donde $a \in A$ y $b \in B$ y se denota por AB.*

$$AB = \{ab| \ a \in A, b \in B\}$$

Proposición 1.1.15. *Sea G un grupo y H un subgrupo de G. Entonces las siguientes condiciones son equivalentes:*

1. *para todo, $x \in G, h \in H : x^{-1}hx \in H$.*
2. *para todo, $x \in G : x^{-1}Hx = H$.*
3. *para todo, $x \in G : xH = Hx$.*
4. *para todo, $x, y \in G : xHyH = xyH$.*

Definición 1.1.16. *Sea G un grupo y $H \leq G$. Se dice que H es un **subgrupo normal** de G, lo cual denotamos por $H \trianglelefteq G$, si H cumple una de las condiciones de la proposición anterior.*

Proposición 1.1.17. *Sea G un grupo diferente de la identidad. Entonces G posee al menos dos subgrupos normales, llamados los **subgrupos normales triviales**: $\{1\}$ y G.*

Definición 1.1.18. *Sea G un grupo diferente de la identidad. Si G no posee otros subgrupos normales fuera de los triviales se dice que G es un **grupo simple**.*

Definición 1.1.19. *Un grupo G es abeliano, si la operación binaria $*$ es conmutativa.*

Definición 1.1.20. *Sea G un grupo y sea a un elemento cualquiera de G, se denota por $\langle a \rangle$ al conjunto de todos los elementos de G que son potencias enteras de a.*

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$$

*y será llamado **subgrupo cíclico** de G generado por a*

Definición 1.1.21. *Sea G un grupo, se dice que G es **cíclico**. Si existe un elemento $a \in G$ tal que el subgrupo cíclico generado por a, coincide con todo el grupo G, es decir, $G = \langle a \rangle$.*

Proposición 1.1.22. *Sea G un grupo y H un subgrupo de G. Si G es un grupo cíclico, entonces H es un grupo cíclico.*

Demostración. Sea G un grupo cíclico generado por a y sea H un subgrupo de G. Si $H = \{e\}$, entonces $H = \langle e \rangle$ es cíclico. Si $H \neq \{e\}$, entonces existe un entero positivo m tal que $a^m \in H$ y m es el menor entero positivo con esta propiedad.

Afirmamos que $c = a^m$ genera a H, es decir,

$$H = \langle a^m \rangle = \langle c \rangle.$$

Se quiere ver que dado cualquier $b \in H$ es una potencia de c. Como $b \in H$ y $H \subseteq G$, existe un entero n tal que

$$b = a^n.$$

Aplicamos el algoritmo de la división para escribir $n = mq + r,$ con $0 \leq r < m.$ Entonces,

$$a^n = a^{mq+r} = (a^m)^q a^r,$$

por lo que,

$$a^r = (a^m)^{-q} a^n.$$

Dado que $a^n \in H$ y $a^m \in H$, y como H es un grupo, tanto $(a^m)^{-q}$ como a^n pertenecen a H. Así,

$$(a^m)^{-q} a^n \in H, \quad \text{es decir,} \quad a^r \in H.$$

Como m es el menor entero positivo tal que $a^m \in H$ y $0 \leq r < m$, necesariamente $r = 0$. Por lo tanto, $n = qm$ y $b = a^n = (a^m)^q = c^q$.

Así, b es una potencia de c. □

Ejemplo 1.1.23. *El grupo $\mathbb{Z}$ con la suma habitual es un grupo cíclico y todos sus subgrupos son cíclicos.*

Sea $H \leq \mathbb{Z}$, si $H = \{0\}$ es el subgrupo trivial nulo, entonces claramente $\langle 0 \rangle = \{0\}$ y H es cíclico. Suponga que $H \neq \{0\}$. Entonces existe $k \neq 0$, $k \in \mathbb{Z}$, $k \in H$. Si $k \in \mathbb{Z}$, entonces $-k \in \mathbb{Z}^+$ y $-k \in H$. Así pues, el conjunto

$$H^+ := \{x \in H \mid x \in \mathbb{Z}^+\} \neq \emptyset.$$

Ya que $(\mathbb{Z}^+, \leq)$ es bien ordenado, existe un entero positivo mínimo n en H. Se quiere probar que H coincide con el subgrupo cíclico generado por n, es decir, $H = \langle n \rangle$. En efecto, sea $p \in H$. Existen enteros q, r tales que $p = q \cdot n + r$, $0 \leq r < n$, luego $r = p + [-(q \cdot n)]$. Si $q \in \mathbb{Z}^+$, entonces $r = p + q \cdot (-n)$.

Como $-n \in H$ y $p \in H$ se tiene que $r \in H$. Por la escogencia de n, $r = 0$ y así $p = q \cdot n \in \langle n \rangle$. Si $q \in \mathbb{Z}^-$, entonces $-q \in \mathbb{Z}^+$ y $r = p + [-(q) \cdot n]$. Como $p, n \in H$, entonces $r \in H$ y nuevamente $r = 0$, con lo cual $p = q \cdot n \in \langle n \rangle$. Si $q = 0$, entonces $p = r \in H$, luego $r = 0$ y así $p = 0 \in \langle n \rangle$. En los tres casos se ha probado que $H \subseteq \langle n \rangle$. Puesto que $n \in H$, la otra inclusión es obvia. Se ha demostrado que cada subgrupo H de $\mathbb{Z}$ es cíclico y generado por el menor entero positivo n contenido en H. Además, $\langle n \rangle = \langle -n \rangle$. Así pues, los subgrupos de $\mathbb{Z}$ son: $\langle n \rangle$, $n \geq 0$.

1.2. Anillos y Módulos

Definición 1.2.1. *Sea R un conjunto no vacío. Se dice que R es un **anillo**, si R tiene dos operaciones binarias notadas $+$ y $\cdot$ tales que,*

1. *$(R, +)$ es un grupo abeliano.*
2. *$(R, \cdot)$ es un semigrupo con identidad 1.*

3. *La multiplicación es distributiva con respecto a la adición, es decir, para cualesquiera* $a, b, c, d \in R$*,*

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$
$$(b + c) \cdot d = b \cdot d + c \cdot d.$$

Si además la multiplicación es conmutativa, es decir para cualesquiera $a, b \in R$*,*

$$a \cdot b = b \cdot a,$$

se dice entonces que $(R, +, \cdot)$ *es un* ***anillo conmutativo****.*

Definición 1.2.2. *Sea* R *un anillo y* $S \subseteq R$*. Se dice que* S *es un* ***subanillo*** *de* R *si cumple las siguientes condiciones:*

1. S *es cerrado bajo la adición y la multiplicación, es decir, para cualesquiera* $a, b \in S$*, se tiene que* $a + b \in S$ *y* $a \cdot b \in S$*.*
2. S *contiene al elemento neutro aditivo de* R*.*
3. S *es cerrado bajo la operación inversa aditiva.*

Ejemplo 1.2.3. *Sea* R *es un anillo, es claro que la intersección de cualquier colección no vacía de subanillos de* R *es un subanillo de* R*. Sea* $r \in R$*. La intersección de todos los subanillos de* R *que contienen a* r *se denomina* ***subanillo generado por*** r*, el cual denotamos por* $\mathbb{Z}[r]$*, y es el subanillo más pequeño de* R *que contiene a* r*. Queremos presentar los elementos de* $\mathbb{Z}[r]$ *de una manera explícita. Supongamos inicialmente que*

$r \neq 0$. *Puesto que* $0, 1 \in \mathbb{Z}[r]$*, entonces en el grupo* $(\mathbb{Z}[r], +, 0)$ *se tiene*

$$\left.\begin{array}{r} k \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{k\text{-veces}} := k \in \mathbb{Z}[r] \\ 0 \cdot 1 = 0 := 0 \in \mathbb{Z}[r]; \quad 0 \in \mathbb{Z} \\ (-k) \cdot 1 = -(k \cdot 1) := -k \in \mathbb{Z}[r] \end{array}\right\} \quad k \in \mathbb{Z}^+,\ 1, 0 \in R.$$

Además, como las potencias enteras no negativas de r *están en* $\mathbb{Z}[r]$*, entonces estarán las combinaciones enteras de estas potencias, es decir, el conjunto*

$$S := \left\{ \sum_{i=0}^{n} k_i r^i \;\middle|\; k_i \in \mathbb{Z},\ n \geq 1 \right\} \subseteq \mathbb{Z}[r].$$

De otra parte, S *es un subanillo de* R *que contiene a* r*. En efecto, la suma de dos elementos de* S *está en* S*,* $1 = 1 \cdot 1 \in S$*, y la propiedad distributiva en* R *junto con la relación*

$$(k_i a^i)(k_j a^j) = k_i k_j a^{i+j}$$

da que el producto de dos elementos de S *está en* S*. Obviamente* $r \in S$*. De lo anterior se desprende que*

$$\mathbb{Z}[r] = \left\{ \sum_{i=0}^{n} k_i r^i \;\middle|\; k_i \in \mathbb{Z},\ n \geq 1 \right\}, \quad a \neq 0. \tag{1}$$

En adelante 0 se denota cómo el elemento neutro de la adición de un anillo R, también denominado el **cero** de R, $-a$ el **opuesto aditivo** de $a \in R$. El elemento identidad 1 también se denomina el **uno** de R.

Definición 1.2.4. *Se dice que un anillo* R *es un anillo* ***sin divisores de cero*** *si para cualesquiera elementos* $a, b \in R$ *se cumple,*

$$ab = 0, \textit{entonces}, a = 0 \quad \textit{o} \quad b = 0.$$

Definición 1.2.5. *Sea R un anillo, si R no tiene divisores de cero será llamado **dominio**, si además es conmutativo se le dirá **dominio de integridad**.*

Definición 1.2.6. *Sea R un anillo. Un elemento $r \in R$ es una **unidad** de R si tiene un inverso múltiplicativo en R. Además si todo elemento no nulo de R es unidad se dice que R es un **anillo de división**.*

Definición 1.2.7. *Sea R un anillo con $1 \neq 0$, se dice que R es un **campo**. Si R es un anillo de división conmutativo.*

Ejemplo 1.2.8. *$\mathbb{Z}$ no es un campo porque 2, por ejemplo, no tiene inverso multiplicativo, así que 2 no es una unidad en $\mathbb{Z}$. Las unidades en $\mathbb{Z}$ son -1 y 1.*

Definición 1.2.9. *Sea R un anillo conmutativo, se dice que R es **reducido**. si R no tiene elementos nilpotentes distintos de cero, esto es*

$$a^n = 0 \quad \textit{entonces} \quad a = 0$$

para cualquier $a \in R$ y n arbitrario.

Definición 1.2.10. *Sean $(G, +)$ un grupo abeliano y $(R, +, \cdot, 1)$ un anillo. Se dice que G es un módulo a la derecha sobre el anillo R, si se ha definido un producto entre elementos de G y de R*

$$G \times R \longrightarrow G$$

$$(g, r) \longmapsto g \cdot r$$

para el cual se cumplen las siguientes condiciones:

1. $(g_1 + g_2) \cdot r = g_1 \cdot r + g_2 \cdot r$.

2. $g \cdot (r_1 + r_2) = g \cdot r_1 + g \cdot r_2$.

3. $g \cdot (r_1 \cdot r_2) = (g \cdot r_1) \cdot r_2$.

4. $g \cdot 1 = g$.

con $g, g_1, g_2 \in G$, $r, r_1, r_2 \in R$.

De manera similar se definen los ***módulos a la izquiera*** *sobre el anillo* R.

Ejemplo 1.2.11. *Sea* $(G, +, 0)$ *un grupo abeliano. Los múltiplos enteros de elementos de* G *se definen inductivamente*

$$\begin{cases} g \cdot 1 & := g, \\ g \cdot k & := g \cdot (k-1) + g, \quad k \geq 2, \\ g \cdot 0 & := 0, \\ g \cdot (-k) & := (-g) \cdot k, \quad k \in \mathbb{Z}^+, \end{cases} \qquad g \in G,\ k \in \mathbb{Z}^+;$$

G *es un* $\mathbb{Z}$*-módulo. De ahí, cada grupo abeliano es un* $\mathbb{Z}$*-módulo.*

Definición 1.2.12. *Sea* G *un* R*-módulo y* N *un subconjunto no vacío de* G*. Se tiene que* N *es un* R*-****submódulo*** *de* G *o, simplemente, un submódulo de* G*, si* N *es un subgrupo del grupo* $(G, +)$*, y además*

$$n \cdot r \in N, \text{ para cada } n \in N \text{ y cada } r \in R.$$

esto se denota por $N \leq G$.

Ejemplo 1.2.13. *Los submódulos de un grupo abeliano son sus subgrupos. Así que, los submódulos de $\mathbb{Z}$ son de la forma $\langle n \rangle$, con $n \geq 0$. Es decir, coinciden con sus subgrupos y con sus ideales.*

Definición 1.2.14. *Sea G un R-módulo y $\{G_i\}_{i \in I}$ una familia de submódulos de G. G es* ***suma directa interna*** *de la familia si,*

1. $G = \sum_{i \in I} G_i$,
2. $\left(\sum_{i \neq j} G_i\right) \cap G_j = 0$, *para cada* $j \in I$.

En tal caso se denota;

$$G = \bigoplus G_i.$$

Si $I = I_n$ es finito se escribe $G = G_1 \oplus \cdots \oplus G_n$.

1.3. Homomorfismos e Isomorfimos

Definición 1.3.1. *Dado dos grupos $(G, *)$ y $(H, \circ)$, una aplicación $f : G \to H$ es un* ***homomorfismo de grupos*** *si satisface:*

$$f(a * b) = f(a) \circ f(b), \quad \text{para cualesquiera } a, b \in G.$$

Ejemplo 1.3.2. *Sea $(\mathbb{Z}, +)$ el grupo de los enteros bajo la suma y $(\mathbb{Z}_n, +)$ el grupo de los enteros módulo n bajo la suma, así $f : \mathbb{Z} \to \mathbb{Z}_n$ dado por $f(k) = [k]_n$ es un homomorfismo de grupos. Donde $[k]_n$ denota las clases de los elementos de $\mathbb{Z}_n$, esto es,*

$$[k]_n = \{a \in \mathbb{Z} \mid a \equiv k \pmod{n}\}.$$

Definición 1.3.3. *Sean R y S anillos, una aplicación $f : R \to S$ se denomina un **homomorfismo de anillos**, si satisface las siguientes propiedades para todo $a, b \in R$:*

1. $f(a + b) = f(a) + f(b)$,
2. $f(a \cdot b) = f(a) \cdot f(b)$.

Ejemplo 1.3.4. *Sea $(\mathbb{Z}, +, \cdot)$ el anillo de los enteros con la suma y multiplicación habitual y $(\mathbb{Z}_n, +, \cdot)$ el anillo de los enteros módulo n con la suma y multiplicación habitual, así $f : \mathbb{Z} \to \mathbb{Z}_n$ dado por $f(k) = [k]_n$ es un homomorfismo de anillos.*

Definición 1.3.5. *Sean G y H grupos (o R y S anillos). Se dirá que:*

1. *G es **isomorfo** a H, y se escribe $G \cong H$, si existe un homomorfismo biyectivo $f : G \to H$.*
2. *R es **isomorfo** a S, y se escribe $R \cong S$, si $f : R \to S$ es un homomorfismo biyectivo, su inverso $f^{-1} : S \to R$ también lo será.*

Definición 1.3.6. *Sea $f : R \to R_1$ un homomorfismo de anillos, el conjunto,*

$$\ker(f) := \{r \in R \mid f(r) = 0\},$$

*se llama el **núcleo** de f.*

Ejemplo 1.3.7. *Sea $\mathbb{Z}$ el conjunto de los enteros y $\mathbb{Z}_6$ los enteros modulo 6, se considera $f : \mathbb{Z} \to \mathbb{Z}_6$ dada por $f(n) = [n]_6$ y se tiene que:*

$$\ker(f) := 6\mathbb{Z}$$

Definición 1.3.8. *Sea R un anilllo se dice que R es **homogéneo**, si R es no trivial y $R \cong S$ para cada subanillo propio S de R.*

Definición 1.3.9. *Sea G un grupo se dice que G es **homogéneo**, Si G es no trivial y $G \cong H$ para cada subgrupo no trivial H de G.*

Ejemplo 1.3.10. *Considere el conjunto de los números enteros $\mathbb{Z}$. Los subanillos propios de $\mathbb{Z}$ son aquellos de la forma $n\mathbb{Z}$, donde n es un entero distinto de cero. Del ejemplo 1.1.23 se establece que estos subanillos son subgrupos cíclicos del grupo aditivo $\mathbb{Z}$ y además son isomorfos entre sí como grupos aditivos.*

En efecto, se define $f : \mathbb{Z} \to n\mathbb{Z}$ como :

$$f(k) = nk.$$

f es un homomorfismo de grupos. Sean $k_1, k_2 \in \mathbb{Z}$

$$f(k_1 + k_2) = n(k_1 + k_2) = nk_1 + nk_2 = f(k_1) + f(k_2).$$

Vea que f es inyectivo. Suponga $f(k_1) = f(k_2)$, esto implica que:

$$nk_1 = nk_2.$$

Por eso $k_1 = k_2$. Finalmenté se muestra que f es sobreyectivo.
Sea $m \in n\mathbb{Z}$, se tiene que $m = nk$ para algún $k \in \mathbb{Z}$, entonces $f(k) = m$. Con esto, se tiene que $\mathbb{Z}$ es hómogeneo como grupo.
Sin embargo, aunque los subanillos propios de $\mathbb{Z}$ son isomorfos como grupos aditivos, no necesariamente lo son como anillos, en efecto.

suponga que existe un isomorfismo de anillos $f : n\mathbb{Z} \to m\mathbb{Z}$*.*

$$f(nk) = ck, \quad \textit{para algún } c \in \mathbb{Z}.$$

la función f *se asume de esta forma pues en* $\mathbb{Z}$ *los subanillos son precisamente sus ideales. En la siguiente sección se aborda con mayor precisión esta afirmación. Dicho esto, dado que* f *es un homomorfismo de anillos, debe preservar la multiplicación. Sea* $k_1, k_2 \in \mathbb{Z}$ *con* $k_1 \neq 0$ *y* $k_2 \neq 0$*, entonces*

$$f(nk_1 \cdot nk_2) = f(n^2 k_1 k_2) = cnk_1 k_2.$$

Por otro lado, evaluamos la multiplicación en la imagen de f*:*

$$f(nk_1) \cdot f(nk_2) = (ck_1) \cdot (ck_2) = c^2 k_1 k_2.$$

Para que f *sea un homomorfismo de anillos, ambas expresiones deben ser iguales, es decir,*

$$cnk_1 k_2 = c^2 k_1 k_2.$$

Como $k_1 k_2 \neq 0$*, se puede dividir por* $k_1 k_2$ *y se obtiene,* $cn = c^2$*. En consecuencia*

$$c(n - c) = 0,$$

Por lo tanto, $c = 0$ *ó* $c = n$*.*

Si $c = 0$*, entonces* f *es la función trivial y no es un isomorfismo. Si* $c = n$*, entonces* $f(nk) = nk$*, lo que implica que* $m = n$*. Así, si* $n \neq m$*, no puede existir un isomorfismo de anillos entre* $n\mathbb{Z}$ *y* $m\mathbb{Z}$*. Se mostró que los subanillos propios de* $\mathbb{Z}$ *son isomorfos como grupos aditivos, pero no necesariamente como anillos.*

1.4. Ideales y Anillo cociente

Definición 1.4.1. *Sea R un anillo e I un subconjunto no vacío de R, se dice que,*

1. *I es un **ideal izquierdo** de R, si $x - y \in I$ para todo $x, y \in I$, y además $rx \in I$ para todo $r \in R$ y todo $x \in I$.*
2. *I es un **ideal derecho** de R, si $x - y \in I$ para todo $x, y \in I$, y además $xr \in I$ para todo $x \in I$ y todo $a \in R$.*
3. *I es un **ideal bilátero** de R, si I es un ideal izquierdo y derecho de R.*

Ejemplo 1.4.2. *Para todo entero k en $\mathbb{Z}$, $k\mathbb{Z}$ es un ideal de $\mathbb{Z}$.*

Definición 1.4.3. *Si R es un anillo e $\{I_i\}_{i\in I}$ es una familia de ideales de R, la intersección $\bigcap_{i\in I} I_i$ es un ideal de R, el cual se denomina **ideal intersección**.*

Proposición 1.4.4. *Sean R un anillo, $S \subseteq R$, $S \neq \emptyset$,el menor ideal de R que contiene al subconjunto S es la intersección de todos los ideales de R que contienen a S, y se denota por $\langle S\rangle$, es decir,*

$$\langle S\rangle := \bigcap_{\substack{S\subseteq I \\ I \text{ ideal de } R}} I.$$

Demostración. Considere el conjunto $F = \{I \subseteq R|\ I$ ideal de R y $S \subseteq I\}$, el cual es no vacío, puesto que $S \subseteq R$, por consiguiente $R \in F$. Note que $\langle S\rangle$ contiene a S y además es el menor ideal que contiene a S, en efecto, como cada I contiene a S su intersección también lo contiene y sea J un ideal de R tal que $S \subseteq J$. Entonces $J \in F$, por lo que,

$$\langle S\rangle := \bigcap_{I\in F} I \subseteq J.$$

□

Definición 1.4.5. *Dados R un anillo, $S \subseteq R$, $S \neq \emptyset$, al ideal $\langle S\rangle$ se le denomina el **ideal generado por** S. Un ideal bilateral I de R se dice que es **finitamente generado**, si existe un subconjunto finito S en R tal que $\langle S\rangle = I$.*

Ejemplo 1.4.6. *Sea $\mathbb{Z}$ el conjunto de los números enteros y $S = \{6\} \subseteq \mathbb{Z}$, entonces, $\langle S\rangle = 6\mathbb{Z}$.*

Definición 1.4.7. *Sea R un anillo y $x \in R$, definimos.*

$$\langle x\} = Rx = \{rx| \quad r \in R\},$$

$$\{x\rangle = xR = \{xr| \quad r \in R\},$$

$$\langle x\rangle = \{\textstyle\sum_{k=1}^{n} a_k x a'_k : | \quad a_k, a'_k \in R, n \in \mathbb{Z}^+\}.$$

*Que son llamados **ideal principal por izquierda, derecha y bilateral**, respectivamente.*

Definición 1.4.8. *Sea R un anillo se dice que es de **ideales principales**, si todo ideal de R es principal.*

Ejemplo 1.4.9. *El anillo $\mathbb{Q}[x]$ de polinomios con coeficientes racionales es un anillo de ideales principales.*

Definición 1.4.10. *Sea R un anillo e I un ideal bilateral propio de R, se define al grupo cociente R/I cuyos elementos son las clases :*

$$\bar{r} := r + I = \{r + i \mid \quad i \in I\}, r \in R.$$

A continuación se definen dos operaciones sobre R/I, de tal que se le dota una estructura de anillo.

Proposición 1.4.11. *Dado un anillo R y un ideal I bilateral propio de R, las operaciones + y · definidas a continuación dotan al conjunto R/I de estructura de anillo.*

$$\left.\begin{array}{rcl} \bar{r_1} \ + \ \bar{r_2} & := & \overline{r_1 + r_2} \\ \bar{r_1} \ \cdot \ \bar{r_2} & := & \overline{r_1 \cdot r_2} \end{array}\right\} \forall\, r_1, r_2 \in R.$$

Además si R es un anillo conmutativo, entonces R/I es un anillo conmutativo. El anillo $(R/I, +, \cdot)$ se denomina ***anillo cociente*** *de R por I.*

2. Anillos isomorfos a sus subanillos no triviales

En el estudio de la teoría de anillos, uno de los temas importantes es la relación entre un anillo y sus subanillos, especialmente al establecer condiciones bajo las cuales un anillo puede ser isomorfo a uno de sus subanillos no triviales. Estos resultados tienen importantes implicaciones para la estructura interna de los anillos y permiten comprender cómo se pueden construir anillos con más propiedades a partir de sus subanillos.

Este tema ha sido investigado por autores como Israel Halperin en "Subrings and Their Isomorphisms" [8], quien exploró las condiciones necesarias para generar dicho isomorfismo. Las implicaciones de este resultado son vastas porque permiten una nueva perspectiva sobre las propiedades estructurales de los anillos y sus subanillos, útil en el contexto de los anillos no conmutativos.

2.1. Clasificación de Anillos y Grupos Homogéneos

En esta sección se presentan los resultados más representativos relacionados con la clasificación de los grupos y anillos homogéneos. Inicialmente, se introduce un resultado clave para clasificar los grupos homogéneos. Posteriormente, se enuncian una serie de consecuencias que serán útiles para comprender el resultado principal expuesto en "Rings isomorphic to their nontrivial subrings" [9].

Proposición 2.1.1. *Sea G un grupo. Entonces, G es homogéneo si, y solo si, $G \cong \mathbb{Z}/\langle p\rangle$ para algún primo p, o $G \cong \mathbb{Z}$.*

---

[8] Halperin, I.: Subrings and Their Isomorphisms. En: Transactions of the American Mathe- matical Society 101.3 (1964).

[9] Lojewski, Jacob y Greg Oman: Rings isomorphic to their nontrivial subrings. En: Involve, a Journal of Mathematics 11.5 (2018).

Demostración. Suponga que G es homogéneo. Si G es infinito, sea $g \in G$, $g \neq e$, donde e es la identidad de G. Como G es homogéneo, se tiene que $G \cong \langle g \rangle$, dado que $\langle g \rangle$ es un grupo cíclico, se concluye que G es cíclico. Ahora, note que $\mathbb{Z}$ es un grupo cíclico infinito generado por 1 . Como G también es cíclico e infinito, se define la función:

$$\phi : \mathbb{Z} \to G \quad \text{dada por} \quad \phi(n) = g^n, \text{ con } g \in G,\ g \neq e.$$

Es claro que ϕ es un isomorfismo ya que, para $m, n \in \mathbb{Z}$, se tiene que $\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n)$.

Ahora, si $\phi(m) = \phi(n)$ para $m, n \in \mathbb{Z}$, entonces, $g^m = g^n$, por consiguiente $g^m g^{-n} = e$, por lo que $g^{m-n} = e$, dado que G es infinito $m - n = 0$. Así, $m = n$, finalmente note que ϕ es sobreyectiva.

En efecto,sea $h \in G$. Como G es cíclico, existe $k \in \mathbb{Z}$ tal que $h = g^k$. Por tanto, $h = \phi(k)$.

Se ha demostrado que ϕ es un isomorfismo, por lo que $G \cong \mathbb{Z}$.

Si G es finito, $n = |G|$, para algún $n \in \mathbb{Z}^+$. Note que G es cíclico, en efecto.

Como G es homogéneo, G es simple. Si no lo fuera, existe un subgrupo normal N de G tal que N es propio, es decir:

$$\{e\} \subsetneq N \subsetneq G.$$

Por ser G homogéneo se tiene que $G \cong N$, dado que G es finito, N también lo es, por lo que tienen el mismo orden. $n = |G| = |N| = |m|$, pero N es un subgrupo propio de G, así que $|m| < |n|$.

Se sabe que G es simple y finito $n = |G|$. Por la simplicidad sabemos que G no tiene subgrupos normales propios, así G es cíclico, pues caso contrario, $n = |G|$ sería compuesto, lo que contradice la simplicidad, por esto, existe $g \in G$ tal que $G = \langle g \rangle$. Se define la función

$$\phi : G \to \mathbb{Z}/\langle n \rangle \quad \text{dada por} \quad \phi(g^k) = [k]_n, \text{ con } k \in \mathbb{Z}.$$

Vea que ϕ esta bien definida. Para esto, se mostrará que si $g^m = g^n$ en G, entonces $\phi(g^m) = \phi(g^n)$.

En efecto, si g^m y $g^t \in G$ tal que $g^m = g^t$, de ahí que $g^{m-t} = e$, dado que G tiene orden n, vale que $g^n = e$, entonces $m - t$, es múltiplo de n:

$$m - t = nk, \quad \text{para algún } k \in \mathbb{Z}.$$

De ahí que $m \equiv t \pmod{n}$, es decir $[m]_n = [t]_n$, por lo tanto $\phi(g^m) = \phi(g^t)$.

Vea que ϕ es un isomorfismo, en efecto, para $g^a, g^b \in G$,

$$\phi(g^a g^b) = \phi(g^{a+b}) = [a + b] = [a] + [b] = \phi(g^a) + \phi(g^b).$$

Si $\phi(g^a) = \phi(g^b)$. Entonces, $[a]_n = [b]_n$, es decir, $a \equiv b \pmod{n}$. Por tanto, $a = b + kn$ para algún $k \in \mathbb{Z}$, lo que implica que $g^a = g^b(g^n)^k = g^b$, ya que $g^n = e$. Finalmente vea ϕ es sobreyectiva.

Sea $[m]_n \in \mathbb{Z}/\langle n \rangle$, dado que G es cíclico y $G = \langle g \rangle$ los elementos de G tienen la forma de g^k, con $k \in \mathbb{Z}$. Además como $|G| = n$, los valores de k se reducen *módulo n*. Por esto,

considere $k \in \mathbb{Z}$ tal que $k \equiv m \pmod{n}$, es decir k es un entero de la forma,

$$k = m + tn \quad \text{para algún } t \in \mathbb{Z}.$$

Sea $g^k \in G$ al aplicar la función ϕ sobre g^k, se tiene que $\phi(g^k) = [k]_n$, por la elección de k, se sabe que $[k]_n = [m]_n$, de ahí que $\phi(g^k) = [m]_n$. Se ha probado que $G \cong \mathbb{Z}/\langle n \rangle$.

Ahora bien, sea H un subgrupo de G con $|H| = d$ y $|G| = n$, donde d es un divisor de n con $d < n$. Como G es cíclico, H también lo es, y por lo anterior, $H \cong \mathbb{Z}/\langle d \rangle$. Dado que G es homogéneo, se tiene que $G \cong H$, es decir, $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}/\langle d \rangle$. Esto no es posible si $d \neq n$, por lo que n debe ser primo.

Suponga ahora que $G \cong \mathbb{Z}/\langle p \rangle$ para algún primo p, es claro que G es homogéneo, en efecto, si $G \cong \mathbb{Z}/\langle p \rangle$ por el Teorema de Lagrange el orden de los subgrupos de $\mathbb{Z}/\langle p \rangle$ deben dividir al orden del grupo. Dado que $\mathbb{Z}/\langle p \rangle$ tiene p elementos (y p es primo) los únicos divisores son 1 y p. Así $\mathbb{Z}/\langle p \rangle$ es simple, por lo que $\mathbb{Z}/\langle p \rangle$ es trivialmente homogéneo.

Sea H un subgrupo no trivial de $\mathbb{Z}$, por lo mostrado en el Ejemplo 1.1.23, H es un grupo cíclico infinito, así existe $n \in \mathbb{Z}^+$ tal que,

$$H = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}.$$

Considere $f : \mathbb{Z} \to H$ definida como,

$$f(k) = nk.$$

f es trivialmente un homomorfismo de grupos. Sean $a, b \in \mathbb{Z}$ tal que $f(a) = f(b)$, entonces, $na = nb$, dado que $n \neq 0$ ya que $H \neq \{0\}$, se tiene que $a = b$. Finalmente note que f es sobreyectiva. Sea $h \in H$, entonces $h = nk$ para algún $k \in \mathbb{Z}$, lo que implica que $f(k) = h$. Así $\mathbb{Z}$ es homogéneo.

□

La siguiente proposición sirve para establecer el resultado principal. Pues nos da una caracteristica de los anillos homogéneos.

Proposición 2.1.2. *Sea R un anillo y $\mathbb{Z}$ el anillo de los enteros, considere $r \in R/\{0\}$ y $r\mathbb{Z}[r] := \{rp(r)|p(x) \in \mathbb{Z}[r]\}$ el subanillo de R generado por r. Suponga además que existe un isomorfismo de anillos, $f : r\mathbb{Z}[r] \to R$, entonces,*

1. $R = f(r)\mathbb{Z}[f(r)]$,
2. *Si además R es homogéneo, $R = r\mathbb{Z}[r]$ para algún r $\in R \setminus \{0\}$. En particular R es conmutativo.*

Demostración.

Es claro que $R = f(r)\mathbb{Z}[f(r)]$, en efecto, sean $f : r\mathbb{Z}[r] \to R$ un isomorfismo de anillos y $a = f(r)$, note que la imagen de $r\mathbb{Z}[r]$ bajo f será el subanillo generado por a, es decir, $a\mathbb{Z}[a]$. En efecto, sea $x \in r\mathbb{Z}[r]$, entonces,

$$x = m_1 r + m_2 r^2 + \cdots + m_k r^k; \quad m_i \in \mathbb{Z}.$$

Aplicando f sobre x, se concluye que,

$$f(x) = f(m_1 r + m_2 r^2 + \cdots + m_k r^k),$$

dado que f es un homomorfismo, se descompone como,

$$f(x) = f(m_1 r) + f(m_2 r^2) + \cdots + f(m_k r^k),$$

ahora por la linealidad de f , se tiene que,

$$f(m_k r^k) = m_k f(r^k),$$

además, como f preserva las potencias,

$$f(r^k) = f(r)^k = a^k,$$

por tanto,

$$f(x) = m_1 a + m_2 a^2 + \cdots + m_k a^k.$$

Esto muestra que dado cualquier elemento x en $r\mathbb{Z}[r]$ es enviado bajo f a un elemento del subanillo generado por a en R,

$$f(r\mathbb{Z}[r]) = a\mathbb{Z}[a] = \{m_1 + m_2 a^2 + \cdots + m_k a^k | k \in \mathbb{N}, m_i \in \mathbb{Z}, \text{ con } 1 \leq i \leq k\}.$$

Dado que la aplicación f es un isomorfismo, en particular es sobreyectiva, para cualquier $x \in R$, existe $y \in r\mathbb{Z}[r]$ tal que $f(y) = x$, como $f(r\mathbb{Z}[r]) = R$, se sigue que $R = a\mathbb{Z}[a]$. En consecuencia, $R = f(r)\mathbb{Z}[f(r)]$.

2. *Si R es homogéneo, entonces, $R = r\mathbb{Z}[r]$ y R es conmutativo*.

Sea $S = rR = \{r \cdot x : x \in R\}$, se tiene que S es un subanillo de R. En efecto:

- S es cerrado bajo la adición, si $r \cdot x$, $r \cdot y \in S$, entonces $(r \cdot x) + (r \cdot y) = r(x + y) \in S$.
- S es cerrado bajo la multiplicación, si $r \cdot x$, $r \cdot y \in S$, entonces $(r \cdot x) \cdot (r \cdot y) = r(\cdot r \cdot (x \cdot y)) \in S$.
- S contiene al neutro aditivo de R, dado $r \in R$, se tiene que $r \cdot 0 = 0 \in S$.
- S es cerrado bajo la operación inversa aditiva, sea $a \in S$, entonces $a = r \cdot x$ para algún $x \in R$, ahora $-a = -(r \cdot x) = (r)(-x) \in S$, pues $-x \in R$.

Dado que R es homogéneo, $R \cong S$, considere $f : R \to S$ un isomorfismo con inverso,

$$f^{-1} : S \to R.$$

Para cada $x \in R$, se define $y = f^{-1}(x)$, por definición de isomorfismo, $y \in R$ y $f(y) = x$. Como la imagen de f es precisamente S; se sigue que $x \in S$, de ahí que $R = S = rR$.

Sea $x \in R$, entonces,

$$x = r \cdot y \quad \text{con} \quad y \in R,$$

repitiendo este proceso para $y \in R$, se tiene que,

$$y = r \cdot t \quad \text{con} \quad t \in R$$

Así que:

$$x = r \cdot (r \cdot t)$$

Por esto, para $x \in R$ arbitrario, se tiene que dado cualquier $x \in R$, se puede escribir de la forma,

$$x = r \cdot p(r),$$

donde $p(r)$ es un polinomio con coeficientes en $\mathbb{Z}$, por tanto cada $x \in R$, cumple que $x \in r\mathbb{Z}[r]$. Por lo tanto, $R \subseteq r\mathbb{Z}[r]$. Además por hipótesis $r\mathbb{Z}[r]$ es un subanillo de R generado por r, entonces $r\mathbb{Z}[r] \subseteq R$, por lo que $R = r\mathbb{Z}[r]$.

Finalmente, vea que R es conmutativo, se tiene que $r\mathbb{Z}[r]$ hereda la conmutatividad de $\mathbb{Z}$. Sean $a, b \in R$ por lo que $a, b \in r\mathbb{Z}[r]$ así que,

$$a \cdot b = b \cdot a,$$

por lo tanto, se concluye que R es conmutativo.

□

El resultado principal de este trabajo busca establecer condiciones para las cuales un anillo es homogéneo, las proposiciones que resultan a continuación ayudan a delimitar la estructura que puede tener un anillo homogéneo.

Proposición 2.1.3. *Sea D un dominio conmutativo con identidad* $1 \neq 0$*, y sea* $D[X^2, X^3]$ *el anillo generado por* D, X^2, X^3*, donde* X *es un elemento arbitrario que conmuta con los elementos de* D*; considere el ideal* $\langle X^2, X^3 \rangle$ *de* $D[X^2, X^3]$ *generado por* X^2*,* X^3*, entonces* $\langle X^2, X^3 \rangle$ *no es un ideal principal de* $D[X^2, X^3]$*.*

Demostración.

Note que,

$$X \notin D[X^2, X^3]. \tag{1}$$

En efecto, suponga que $X \in D[X^2, X^3]$, es decir X puede escribirse cómo una combinación de potencias de X^2 Y X^3,

$$X = f(X^2, X^3)$$

Para algún $f(X) \in D[X^2, X^3]$, evidentemente $D[X^2, X^3]$ es un subanillo de $D[X]$ que por definición de anillo es cerrado bajo suma y multiplicación, por definición de subanillo si $X \in D[X^2, X^3]$ su inverso X^{-1} también pertenece a $D[X^2, X^3]$, así que X sería una unidad de $D[X]$.

Si X es una unidad de $D[X]$ existe un polinomio $g(X) \in D[X]$ tal que :

$$X \cdot g(X) = 1$$

Como $g(X) \in D[X]$, tiene la forma:

$$g(X) = b_0 + b_1X + b_2X^2 + \cdots + b_nX^n$$

Donde $b_i \in D$. Multiplicando X por $g(X)$:

$$Xg(X) = Xb_0 + b_1X^2 + b_2X^3 + \cdots + b_nX^{n+1}$$

Por un lado tenemos que $Xb_0 + b_1X^2 + b_2X^3 + \cdots + b_nX^{n+1}$ es un polinomio sin termino constante.

Por otra parte se tiene que $X \cdot g(X) = 1$, por lo tanto el término constante de $X \cdot g(X)$ es 1. Pero en $Xb_0 + b_1X^2 + b_2X^3 + \cdots + b_nX^{n+1} = Xg(X)$ el término constante en 0. Así $X \notin D[X^2, X^3]$.

Note que $\langle X^2, X^3\rangle$ no es un ideal principal de $D[X^2, X^3]$.En efecto, suponga que $\langle X^2, X^3\rangle$ es un ideal principal de $D[X^2, X^3]$, así existe $f(X) \in D[X^2, X^3]$ tal que $\langle f(X)\rangle = \langle X^2, X^3\rangle$.

Usando que $\langle f\rangle = \langle X^2, X^3\rangle$. Se sabe que cada elemento de $\langle X^2, X^3\rangle$ puede escribirse como un múltiplo de f, es decir, para todo $g \in \langle X^2, X^3\rangle$ existe $r \in D[X^2, X^3]$ tal que $g = rf$.

En particular $X^2 \in \langle X^2, X^3\rangle$ y $X^3 \in \langle X^2, X^3\rangle$, por lo tanto existen $r_1, r_2 \in D[X^2, X^3]$ tales que,

$$X^2 = r_1 f \quad y \quad X^3 = r_2 f.$$

Por esto f divide a X^2 Y X^3 en $D[X^2, X^3]$, dado que $D[X^2, X^3]$ es subanillo de $D[X]$ particularmente f divide a X^2 en $D[X]$.

Usando nuevamente que $\langle f\rangle = \langle X^2, X^3\rangle$, se tiene que existen $a, b \in D[X^2, X^3]$ tales que,

$$f(X) = aX^2 + bX^3 = X^2(a + bX).$$

De ahí que todo polinomio en $D[X^2, X^3]$ es un polinomio en la variable X, así $a + bX = h$ para algún $h \in D[X]$, entonces $f(X) = X^2h$ y cumple que $X^2|f(X)$.

Ahora si, $X^2|f(X)$ y $f(X)|X^2$ en el anillo $D[X]$. se tiene que $f(X) = uX^2$ para alguna unidad $u \in D$. como $f(X)|X^3$, en $D[X^2, X^3]$, entonces $uX^2g = X^3$ para algún $g \in D[X^2, X^3]$, de ahí que $X = u \cdot g \in D[X^2, X^3]$, lo que contradice (1). Se concluye que $\langle X^2, X^3\rangle$ no es un ideal principal de $D[X^2, X^3]$.

□

Proposición 2.1.4. *Sea D un dominio entero conmutativo y $XD[X]$ el subanillo de $D[X]$ que consta de todos los $f(x) \in D[X]$, para el cual $f(0) = 0$, entonces, $XD[X]$ no es homogéneo.*

Demostración. Suponga que $XD[X]$ es homogéneo, sea R el subanillo de $XD[X]$ generado por X^2 Y X^3, dado que $XD[X]$ es homogéneo y R es un subanillo de $XD[X]$, entonces R es homogéneo.
Usando lo mostrado en la Proposición 2.1.2, se tiene que existe $f(x) \in R$ tal que $R = f(x)\mathbb{Z}[f(x)]$, considere el ideal I de $D[X^2, X^3]$ generado por R, por lo mostrado en la Proposición 2.1.3 $I = \langle X^2, X^3\rangle = \langle f(x)\rangle$, entonces $\langle X^2, X^3\rangle$ es un ideal principal de $D[X^2, X^3]$ lo cual es contradictorio. □

La siguiente proposición servira para clasificar los anillos homogéneos.

Proposición 2.1.5. *Sea R un anillo reducido y homogéneo, entonces R no tiene divisores de cero no nulos.*

Demostración. Suponga por contradicción, que existe $r_0 \in R \setminus \{0\}$ que es un divisor de cero, entonces,

$$r_0 \cdot s = 0 \quad \text{para algún} \quad s \in R \setminus \{0\},$$

considere el subanillo no nulo $T_1 = r_0\mathbb{Z}[r_0]$ de R, definido según la Proposición 2.1.2, y el subconjunto $S_1 = \{r \in R : rT_1 = \{0\}\}$. Note que S_1 es un subanillo no nulo de R. En

efecto, como R es reducido, se cumple que,

$$S_1 \cap T_1 = \{0\}, \quad xy = 0 \quad \text{para } x \in S_1,\, y \in T_1. \tag{2}$$

para demostrar esta afirmación, suponga que existe $x \in S_1 \cap T_1$. Dado que $x \in T_1$, se escribe como,

$$x = r_0 g(r_0),$$

donde $g(r_0) \in \mathbb{Z}[r_0]$. (Ver Ejemplo 1.2.3), por otro lado, como $x \in S_1$, se tiene que $xT_1 = \{0\}$. Así, tomando $x = r_0 g(r_0)$, se obtiene de forma recursiva $x^n = r_0^n g(r_0)^n = 0$.

Como R es reducido, esto implica que $x = 0$, lo que prueba (2).

Dado que T_1 y S_1 son subanillos no nulos de R, y que $R \cong S_1$ por ser homogéneo, existen dos subanillos no nulos S_2 y T_2 de S_1 que cumplen una relación similar a (2), es decir,

$$S_2 \cap T_2 = \{0\}, \quad xy = 0 \quad \text{para } x \in S_2,\, y \in T_2. \tag{3}$$

Mediante un procedimiento recursivo, se construyen sucesiones $\{S_n : n \geq 0\}$ y $\{T_n : n \geq 0\}$ de subanillos no nulos de R, donde $S_0 = T_0 = R$, y para cada $n \geq 1$, S_{n+1} y T_{n+1} son subanillos no nulos de S_n tales que:

$$S_{n+1} \cap T_{n+1} = \{0\}, \quad xy = 0 \quad \text{para } x \in S_{n+1},\, y \in T_{n+1}. \tag{4}$$

La demostración de (3) y (4) es análoga a la de (2).

A continuación, se muestra por inducción que, para todo entero positivo k, si $t_1, \ldots, t_k \in T_n$ con $t_1 + \cdots + t_k = 0$, entonces $t_i = 0$ para todo i. Si $t_1 \in T_{n_1}$ y $t_1 = 0$, el resultado es

inmediato. Ahora, suponga que el resultado es válido para k, y se prueba para $k+1$. Sean $0 < n_1 < n_2 < \cdots < n_{k+1}$ y $t_1 + \cdots + t_{k+1} = 0$, donde $t_i \in T_{n_i}$. Entonces $t_2, \ldots, t_{k+1} \in S_{n_1}$. Definamos $\alpha = t_2 + \cdots + t_{k+1}$. Como $t_1 + \alpha = 0$ y $S_{n_1} \cap T_{n_1} = \{0\}$, se tiene que $t_1 = \alpha = 0$. Por hipótesis inductiva, $t_2 = \cdots = t_{k+1} = 0$.

De lo anterior, como cada T_n es un subanillo no nulo de R, se tiene que R es isomorfo a la suma directa interna de los subanillos T_n,

$$R \cong \bigoplus_{n>0} T_n.$$

En efecto, sabemos por la forma que se han definido los subanillos T_n que cualquier elemento $r \in R$ se puede describir de forma unica cómo,

$$r = t_1 + t_2 + \cdots + t_i,$$

donde cada t_n pertence a su respectivo subanillo T_n. Así considere la función,

$$\phi : R \to \bigoplus_{n>0} T_n \quad \phi(r) = (t_1, t_2, t_3, ...).$$

Donde t_1 es el componente de r que pertenece a T_1. t_2 el componente de r que pertenece a T_2 y así inductivamente; esta descomposición es única por la propiedad de intersección trivial de los T_n.

Note que ϕ es un isomorfismo.

1.) ϕ *es un homomorfimo de anillos*:

Sean $r, s \in R$ con descomposición:

$$r = t_1 + t_2 + t_3 + \cdots + t_n,$$
$$s = u_1 + u_2 + u_3 + \cdots + u_n,$$

con $t_n, u_n \in T_n$, entonces,

$$\begin{aligned}\phi(r+s) &= \phi((t_1+u_1)+(t_2+u_2)+(t_3+u_3)+\dots) \\ &= (t_1+u_1, t_2+u_2, t_3+u_3, \dots, t_n+u_n).\end{aligned}$$

Esto corresponde con la suma en $\bigoplus_{n>0} T_n$.
Por la construcción de los T_n, los productos entre términos de distintos subanillos son cero,

$$t_i u_j = 0 \quad \text{si } i \neq j. \tag{2}$$

Así, el producto en R se distribuye como,

$$\begin{aligned}rs &= (t_1 + t_2 + \cdots + t_n)(u_1 + u_2 + \cdots + u_n), \\ &= t_1u_1 + t_2u_2 + \dots t_nu_n,\end{aligned}$$

esto coincide con la multiplicación componente a componente en $\bigoplus_{n>0} T_n$, por lo que ϕ es un homomorfismo de anillos.

2.) ϕ *es un isomorfismo de anillos*

Si $\phi(r) = 0$, entonces cada coordenada es cero, es decir,

$$(t_1, t_2, t_3, \ldots, t_n) = (0, 0, 0, \ldots, 0), \tag{3}$$

por la unicidad de la descomposición, esto implica que $r = 0$, por lo tanto, $\ker(\phi) = \{0\}$ y ϕ es inyectiva. Por ultimo vea que ϕ es sobreyectiva, sea $(t_1, t_2, t_3, \ldots) \in \bigoplus_{n>0} T_n$. Definimos,

$$r = t_1 + t_2 + t_3 + \cdots + t_n \in R, \tag{4}$$

por la definición de ϕ se tiene que

$$\phi(r) = (t_1, t_2, t_3, \ldots), \tag{5}$$

así ϕ es sobreyectiva. por esto R es isomorfo a la suma directa interna de los subanillos T_n,

$$R \cong \bigoplus_{n>0} T_n,$$

lo que implica que $\bigoplus_{n>0} T_n$ es homogéneo, y por lo mostrado en la Proposición 2.1.2 se tiene que,

$$\bigoplus_{n>0} T_n = r\mathbb{Z}[r] \quad \text{para algún} \quad r \in \bigoplus_{n>0} T_n.$$

lo que es una contradicción.

Si $R \cong \bigoplus_{n>0} T_n$, se tiene que para $r \in R$,

$$r = t_1 + t_2 + t_3 + \cdots t_n,$$

donde $t_i \in T_i$ para cada $i > 0$, se pueden construir elementos de $\bigoplus_{n>0} T_n$, que involucren cualquier número finito de términos en distintos T_n por ejemplo, se toma,

$$r_1 \in T_1, \;\; r_2 \in T_2, \cdots \;\; r_k \in T_k,$$

y al sumar,

$$r = r_1 + r_2 + \cdots + r_k,$$

Donde k es arbitrario. La contradicción surge pues si $R = r\mathbb{Z}[r]$ todos los elementos son simplemente polinomios en r lo que no permite la existencia de una descomposición en partes disjuntas como la que se construyó con los T_n.

□

Las proporsiciones que se presentan a continuación, junto con la suposición de que R no tiene elementos nilpotentes no nulos, permitiran mostrar el resultado principal *Teorema* 2.1.10

Proposición 2.1.6. *Sean R un dominio conmutativo y $K := \left\{ \frac{a}{b} : a \in R, b \in R \setminus \{0\} \right\}$ el campo cociente de R, considere D el subanillo de K generado por 1; entonces $rD[r]$ es un subanillo no nulo de R, para algún $r \neq 0 \in R$ y $R \cong rD[r]$.*

Demostración. Note que $rD[r]$ es el conjunto de elementos de la forma $r \cdot f(r)$, donde $f(r)$ es un polinomio en D con coeficientes en r.

Es claro que $rD[r]$ es un subanillo de R, en efecto

1.) $rD[r]$ *contiene al elemento neutro* (0).

Pues el polinomio $f(r) = 0$ es un elemento de $D[r]$ (ya que $D[r]$ contiene el polinomio cero), además.

$$r \cdot f(r) = r \cdot 0 = 0.$$

2.) $rD[r]$ *es cerrado bajo la adición y multiplicación.*

Sean $(r \cdot f_1(r)), (r \cdot f_2(r)) \in rD[r]$, la suma de estos dos elementos es,

$$r \cdot f_1(r) + r \cdot f_2(r) = r \cdot (f_1(r) + f_2(r)).$$

Dado que $f_1(r) + f_2(r) \in D[r]$(ya que $D[r]$ es cerrado bajo la suma), esto implica que $r \cdot (f_1(r) + f_2(r)) \in rD[r]$.
Su producto es,

$$(r \cdot f_1(r)) \cdot (r \cdot f_2(r)) = r^2 \cdot f_1(r) \cdot f_2(r).$$

De igual forma, dado que $f_1(r) \cdot f_2(r) \subset D[r]$($D[r]$ es cerrado bajo el producto) y r^2 es un múltiplo de r, se puede escribir $r^2 \cdot f_1(r) \cdot f_2(r) = r \cdot (r \cdot f_1(r) \cdot f_2(r))$, claramente $r \cdot f_1(r) \cdot f_2(r) \in D[r]$, por lo tanto $r^2 \cdot f_1(r) \cdot f_2(r) \in rD[r]$.

3.)$rD[r]$ *es cerrado bajo el inverso aditivo*.

Sea $r \cdot f(r) \in rD[r]$, note que,

$$-(r \cdot f(r)) = r \cdot (-f(r)) \in rD[r],$$

así $rD[r]$ es un subanillo no trivial de R pues $r \neq 0 \in R$, por lo que podemos asegurar que $rD[r]$ contiene elementos no nulos, además como R es homogéneo y $rD[r]$ es un subanillo de R, $R \cong rD[r]$. □

Proposición 2.1.7. *Sea $\phi : XD[X] \to rD[r]$ dado por $\phi(Xg(X)) = rg(r)$ un homomorfismo de anillos sobreyectivo y considere un polinomio no nulo $Xf(X) = d_1X + d_2X^2 + \cdots d_nX^n \in XD[X]$ de grado mínimo n tal que $rf(r) = 0$, entonces $d_1 \in R\backslash\{0\}$.*

Demostración. Se sabe que $rD[r]$ es homogéneo según la Proposición 2.1.6. Por otro lado se mostró que $XD[X]$ no es homogéneo (Proposición 2.1.4), por esto el kernel de ϕ es no nulo.

Pues caso contrario si el $ker(\phi) = 0$, ϕ es inyectiva. Así, $XD[X] \cong rD[r]$. Lo que sería contradictorio.
Vea que $d_1 \neq 0$. Si $n = 1$, ya esta, pues $Xf(X) \neq 0.$ suponga que $n > 1$. si $d_1 = 0$, se tiene que $rf(r) = d_2r^2 + \cdots d_nr^n = 0$ dado que R es un dominio y $r \neq 0$, se tiene que $d_2r^2 + \cdots d_nr^{n-1} = 0$ que contradice la minimalidad de n.
Note que $d_1 \in R$, en efecto.

$$d_1r + d_2r^2 + \cdots d_nr^n = 0 \quad d_1 \neq 0, \tag{7}$$

donde r es un elemento no nulo de R, esto implica que los coeficientes d_i estan en el

subanillo D de K generado por $f(1)$, donde,

$$K := \left\{ \frac{a}{b} : a \in R, b \in R \setminus \{0\} \right\},$$

es el campo cociente de R y D el subanillo de K generado por 1. Al dividir por r en (7) se tiene,

$$d_1 + d_2 r^2 + \cdots d_n r^{n-1} = 0.$$

Por tal motivo d_1 se escribe cómo una combinación de elementos de D y potencias de R dado que $R \cong rD[r]$ por lo mostrado en la proposición 2.1.6, por consiguiente $d_1 \in R$.

□

Proposición 2.1.8. *Sea R un anillo homogéneo y $rf(r) = d_1 r + d_2 r^2 + \cdots + d_n r^n$ un polinomio en el campo cociente K de R, entonces, $R \cong \mathbb{F}_p$ para algún primo p, donde K está definido en la Proposición 2.1.6.*

Demostración.

Se usará que $R \cong rD[r]$ para mostrar que el subanillo D de K generado por $f(1)$, Es isomorfo a $\mathbb{Z}$ o $\mathbb{Z}\backslash\langle p\rangle$, donde K se define como en la proposición 2.1.6 dado que $d_1 \in D$ el cual está generado por $f(1)$ se tiene que ,

$$d = m \cdot f(1).$$

Dado que K es un campo y D es un subanillo de K generado por $f(1)$, entonce, D debe ser isomorfo a $\mathbb{Z}$ o $\mathbb{Z}/\langle p\rangle$.
Si $D \cong \mathbb{Z}$ genera una contradicción, en efecto, recordando que $R \cong rD[r]$, se tendria que $R \cong m\mathbb{Z}$, se vió en el Ejemplo 1.3.10 que los anillos de la forma $m\mathbb{Z}$ no son homogéneos.

Si $D \cong \mathbb{Z}/\langle p \rangle$ se tiene que $D \cong \mathcal{F}_p$. Donde $\mathcal{F}_p$ es el campo de p elementos para algún primo p, además como $d_1 \in R\backslash\{0\}$ y $D \cong \mathcal{F}_p$ se tiene que $d_1 \in (\mathcal{F}_p \cap R\backslash\{0\})$ aplicando homogeneidad, se observa que R es isomorfo a el anillo generado por d_1, $\mathbb{Z}[d_1]$.

Como $D \cong \mathbb{Z}/\langle p \rangle$ los unicos valores que puede tomar d_1 estan en el conjunto $\{0, 1, 2, ..., p-1\}$ con operaciones *módulo p*, esto implica que el subanillo generado por d_1 es simplemente D, Así $R \cong D$ y como $d_1 \neq 0$ $R \cong \mathcal{F}_p$.

□

Definición 2.1.9. *Se dice que un anillo R tiene **multiplicación o producto trivial**, si $x \cdot y = 0$ para todo $x, y \in R$.*

Para realizar la demostración del siguiente teorema, se utilizan las proposiciones anteriormente demostradas, las cuales son expuestas por Jacob Lojewski y Greg Oman en Jacob Lojewski y Greg Oman: *Rings isomorphic to their nontrivial subrings*. En: *Involve, a Journal of Mathematics* 11.5 (2018)

Teorema 2.1.10. *Sea R un anillo. Se tiene que R es homogéneo si y solo si se cumple una de las siguientes condiciones:*

1. $R \cong \mathbb{F}_p$*, donde $\mathbb{F}_p$ es el campo de p elementos y p es un número primo.*
2. $R \cong \mathbb{Z}/\langle p \rangle$ *con multiplicación trivial.*
3. $R \cong \mathbb{Z}$ *con multiplicación trivial.*

Demostración.

Inicialmente, se muestra que $\mathbb{F}_p$, $\mathbb{Z}/\langle p \rangle$ y $\mathbb{Z}$ con multiplicación trivial, son homogéneos.

De manera trivial, si S es un subanillo no trivial del campo finito $\mathbb{F}_p$, por el teorema de Lagrange, $S = \mathbb{F}_p$, por lo que $\mathbb{F}_p \cong S$. De manera similar, se muestra que $\mathbb{Z}/\langle p\rangle$ con multiplicación trivial es homogéneo.

Es claro que $\mathbb{Z}$ es homogéneo, en efecto, sea S un subanillo no trivial de $\mathbb{Z}$ (con multiplicación trivial), entonces, aditivamente, S es un subgrupo no trivial de $(\mathbb{Z}, +)$; por la proposición 2.1.1, tenemos que $(S, +) \cong (\mathbb{Z}, +)$. Sea $f : S \to \mathbb{Z}$ un isomorfismo aditivo, dado que la multiplicación en $\mathbb{Z}$ es trivial, se sigue que f es un isomorfismo de anillos.

Lo que muestra que si se cumple (1), (2), o (3), entonces R es homogéneo.
Para la otra parte de la demostración se dividirá la prueba en dos casos, el caso en que R posee elementos nilpotentes no nulos, y el caso en que no posee elementos nilpotentes no nulos.
Sea R es un anillo homogéneo que posee un elemento nilpotente no nulo α.
Fije $n > 1$ el menor número tal que $\alpha^n = 0$, y defina $\beta = \alpha^{n-1}$. Entonces, $\beta \neq 0$, pero $\beta^2 = 0$. Sea $S = \{m\beta : m \in \mathbb{Z}\}$, entonces S es un subanillo no nulo de R con multiplicación trivial. Dado que R es homogéneo, $R \cong S$, Por lo tanto, R es un anillo no trivial con multiplicación trivial, dado que cada subgrupo de R es un subanillo de R, y R es homogéneo, $H \cong K$ para cualquier subgrupo no trivial H y K de $(R, +)$ (por la Proposición 2.1.1), se observa que se cumple (2) o (3) .
Suponga ahora que R no tiene elementos nilpotentes no nulos, con esto y la Proposición 2.1.5, concluimos que R es un dominio y usando la Proposición 2.1.2 se concluye además que R es conmutativo. Es necesario mostrar que R es un dominio conmutativo para evitar que R contenga divisores de cero y así genere subanillos diferentes a R, lo que contradice la homogeneidad. Ahora bien por la Proposición 2.1.6, R posee una identidad multiplicativa, y $R \cong rD[r]$.

Considere $\phi : XD[X] \to rD[r]$ un homomorfismo de anillos sobreyectivo y el polinomio no nulo $Xf(X) = d_1X + d_2X^2 + \cdots + d_nX^n$ de grado mínimo n tal que $rf(r) = 0$, lo que concluye que $d_1 \neq 0$ y $d_1 \in R$ gracias a la proposición 2.1.7. Considerando finalmente la función,

$$rf(r) = d_1r + d_2r^2 + \cdots + d_nr^n,$$

En el campo cociente K de R, se concluye que $R \cong \mathbb{F}_p$ por la proposicón 2.1.8. Lo que termina la demostración.

□ En esta última parte del proyecto, se presenta un resultado que permite caracterizar los campos de orden primo.

Observación 2.1.11. *Sea R un anillo con multiplicación no trivial. R es un campo con p elementos $primos$ si y solo si, dos subanillos no triviales de R son isomorfos.*

BIBLIOGRAFÍA

Corry, L.: *Modern Algebra and the Rise of Mathematical Structures*. Springer, 2003.

Fraleigh, J.B.: *Abstract Algebra*. 7th. Addison-Wesley, 2004.

Halperin, I.: *Subrings and Their Isomorphisms*. En: *Transactions of the American Mathematical Society* 101.3 (1964).

Lang, S.: *Algebra*. 3.ª. Springer, 2002.

Lezama, O.: *Cuadernos de Álgebra, No. 1: Grupos*. Departamento de Matemáticas, Universidad Nacional de Colombia, sede de Bogotá, s.f.

Lezama, O.: *Cuadernos de Álgebra, No. 2: Anillos*. Departamento de Matemáticas, Universidad Nacional de Colombia, sede de Bogotá, s.f.

Lezama, O.: *Cuadernos de Álgebra, No. 3: Módulos*. Departamento de Matemáticas, Universidad Nacional de Colombia, sede de Bogotá, s.f.

Lojewski, Jacob y Greg Oman: *Rings isomorphic to their nontrivial subrings*. En: *Involve, a Journal of Mathematics* 11.5 (2018).

Van Der Waerden, B.: *A History of Algebra*. Springer, 1985.