UNIVERSIDAD NACIONAL DE EDUCACIÓN

Enrique Guzmán y Valle

Alma Máter del Magisterio Nacional

FACULTAD DE CIENCIAS
Escuela Profesional de Matemática e Informática

MONOGRAFÍA

ESTRUCTURA DE ANILLO

Anillos. Dominio de Integridad. Subanillos. Ideales. Ideales Maximales y Primos. Anillo Cociente. Características de Anillos. Homomorfismo de anillos. Descomposición de homomorfismos de anillos.

Examen de Suficiencia Profesional Res. Nº1249-2018-D-FAC

Presentada por:

Enrique Clemente Yacolca Paniura

Para optar al Título Profesional de Licenciado en Educación

Especialidad: Matemática e Informática

Lima, Perú
2018

Monografía

ESTRUCTURA DE ANILLO

Anillos. Dominio de Integridad. Subanillos. Ideales. Ideales Maximales y Primos. Anillo Cociente. Características de Anillos. Homomorfismo de anillos. Descomposición de homomorfismos de anillos.

Designación de Jurado Resolución N°1249-2018-D-FAC

Lic. Leonidas TORRES ANAYA

Mg. José Carlos RAMÍREZ GAMARRA
Secretario

Lic. Modesto Isidoro GILES NONALAYA
Vocal

Linea de Investigación: Curriculum y formación profesional en educación

Dedicatoria

A mis padres Dora María y Enrique Clemente por su apoyo y motivación para seguir mis estudios.

A mis familiares y amigos que me motivaron a seguir persistiendo en mis metas.

A Milagros Laqui por su apoyo incondicional.

Tabla de contenido

Dedicatoria iii

Introducción vii

Capítulo I : Conceptos preliminares 9

1.1 Ley de composición interna 9

1.2 Estructura algebraica 11

1.3 Monoides y semigrupos 11

1.4 Elementos distinguidos 13

1.4.1 Elementos permutables 13

1.4.2 Elemento neutro 14

1.4.3 Elemento simétrico 15

1.5 Grupos y subgrupos 17

1.5.1 Grupos 17

1.5.2 Subgrupos 21

1.5.3 Condición suficiente para la existencia de subgrupos 22

Capítulo II: Estructura de anillo 24

2.1 Anillo 24

2.2 Tipos de anillos 26

2.2.1 Anillo conmutativo 26

2.2.2 Anillo con identidad 26

2.3 Propiedades de los anillos 32

2.4 Anillo con divisores de cero 35

2.5 Dominio de integridad 37

2.5.1 Característica de un anillo 38

2.6 Subanillos 40

2.7 Ideales 46

2.8 Anillo cociente 52

2.9 Homomorfismo de anillos 57

2.10 Isomorfismo de anillos 63

Aplicación didáctica 66

Sesion de aprendizaje 67

Síntesis 70

Apreciación crítica y sugerencias 75

Concluciones 77

Referencias 78

Lista de figuras

Figura 1. Subgrupos 21

Figura 2. Condición suficiente para la existencia de subgrupos 22

Introducción

En términos generales, las estructuras algebraicas son conjuntos no vacíos provistos de una o más leyes de composición que verifican determinadas propiedades. Entre éstas tenemos la estructura de semigrupos, grupos, anillos, cuerpos o campos, entre otros.

Como se ve, la ***estructura de anillos*** que es el tema que se aborda en la presente monografía, es una estructura algebraica, que se construye sobre la base de la estructura de grupos y semigrupos. Por esta razón, el primer capítulo se ha destinado a realizar una breve revisión de dichas estructuras en base al concepto de leyes de composición interna y sus propiedades.

Sobre estos conceptos básicos, en el segundo capítulo se realiza en sí mismo el estudio de la estructura de anillos, basado principalmente en la familiaridad que casi todos tenemos con el estudio de las operaciones de adición y multiplicación en el conjunto de los números enteros. Se precisa asimismo las propiedades que la caracterizan, diferenciando algunos tipos de anillos, y señalando otras propiedades complementarias. Así mismo se incluyen los dominios de integridad, los ideales, el anillo cociente, concluyendo con el homomorfismo e isomorfismo de anillos.

Luego, se presenta la aplicación didáctica, la síntesis, así como una apreciación crítica; terminando con algunas conclusiones y sugerencias.

Considerando la importancia que tiene la comprensión de las estructuras algebraicas por parte de los docentes de educación básica, hemos intentado presentar el tema de los anillos de la manera más comprensible posible mostrando en todos los casos ejemplos y contraejemplos que ayudan a comprender mejor los conceptos que por su nivel de abstracción resultan difíciles para muchos.

Es necesario señalar que las estructuras algebraicas están presentes en diversos objetos matemáticos, empezando como es evidente en los conjuntos numéricos con los que los estudiantes desde la primaria están en contacto, los polinomios, las funciones, las matrices, hasta con temas de la geometría.

Por lo que sería conveniente que de manera progresiva se vayan abordando desde la educación primaria para que después no generen tanta dificultad. Es posible asimismo encontrar analogías o isomorfismos en conjuntos de diversa naturaleza, inclusive con situaciones de la vida cotidiana, y siendo así ayudaría aún más a entender la matemática de manera más integrada e interconectada.

Cabe recordar que entre los principales gestores de las estructuras algebraicas están Evariste Galois, Niels H. Abel y otros matemáticos importantes de la época moderna y contemporánea.

Finalmente, quiero manifestar que durante mi formación como docente de matemática e informática no he tenido la oportunidad de desarrollar estos conceptos; puesto que nunca llevamos estos cursos en las sedes itinerantes; por lo que en la elaboración de esta monografía he tenido serias dificultades para comprender estos conceptos por ser muy abstractos, pero gracias al esfuerzo realizado he logrado comprender medianamente, por lo que espero ser comprendido. Sin embargo, la calidad del trabajo realizado será de mucha utilidad en la formación de otros estudiantes o docentes.

El autor

Capítulo I : Conceptos preliminares

1.1 Ley de composición interna

Definición.-

Sea A un conjunto no vacío. Llamamos ley de composición interna (LCI) a toda función "$*$" de $A \times A$ en A.

Es decir:

$*$ es una LCI en A, si $*: A \times A \to A$

$(a;b) \to a * b$ y se lee "a compuesta con b"

Ejemplo 1:

La adición es una ley de composición interna en el conjunto de los números naturales; pues, la suma de dos números naturales es otro número natural.

$$+ : \mathbb{N} \text{ x } \mathbb{N} \to \mathbb{N}$$

$$(a;b) \to a + b$$

Como, $(3;5) \to 3 + 5 = 8 \in \mathbb{N}$

En general la adición es una ley de composición interna en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{I}$ y $\mathbb{R}$.

Ejemplo 2:

La multiplicación es una ley de composición interna en $\mathbb{Z}$; pues el producto de cualquier par de números enteros es siempre un número entero.

$\cdot : \mathbb{Z} \text{ x } \mathbb{Z} \rightarrow \mathbb{Z}$

$(a;b) \rightarrow a \cdot b$

$(-5;4) \rightarrow (-5) \cdot 4 = -20 \in \mathbb{Z}$

En general la multiplicación es una ley de composición interna en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$.

Contraejemplo 1:

La sustracción no es una ley de composición interna en $\mathbb{N}$; pues la diferencia de dos números naturales no siempre es un número natural.

Así:

$(5;2) \rightarrow 5 - 2 = 3 \in \mathbb{N}$

$(5;5) \rightarrow 5 - 5 = 0 \in \mathbb{N}$

$(2;5) \rightarrow 2 - 5 = -3 \notin \mathbb{N}$

Como se observa, la diferencia de dos números naturales es otro número natural, solo cuando el minuendo es mayor o igual que el sustraendo; si el minuendo es menor que el sustraendo no es un número natural.

Contraejemplo 2:

La multiplicación no es una LCI en el conjunto de los números irracionales; puesto que el producto de dos números irracionales no siempre es un número irracional.

$+ : \mathbb{I} \, x \, \mathbb{I} \rightarrow \mathbb{I}$

$(a;b) \rightarrow a \cdot b$

$(\sqrt{3};\sqrt{5}) \rightarrow \sqrt{3} \cdot \sqrt{5} = \sqrt{15} \in \mathbb{I}$

$(\sqrt{2};\sqrt{8}) \rightarrow \sqrt{2} \cdot \sqrt{8} = \sqrt{16} = 4 \notin \mathbb{I}$

1.2 Estructura algebraica

Definición

Una estructura algebraica es un conjunto $A \neq \Phi$ provisto de una o más leyes de composición interna y/o externa o sus combinaciones.

Notación

Las estructuras algebraicas se denotan como: $(A, *, \circ, \otimes, T, ...)$, donde A es el conjunto no vacío, y $, *, \circ, \otimes, T, ...$, son las leyes definidas en dicho conjunto.

1.3 Monoides y semigrupos

Definición

Un conjunto $A \neq \Phi$, provisto de una LCI "$*$" se llama monoide.

Notación: Un monoide se representa como: $(A; *)$

Ejemplos:

1. $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{I}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$, son monoides porque "+" y "$\cdot$" son leyes de composición interna en cada uno de los conjuntos.

2. Si A = F($\mathbb{R}$) = { f / f: $\mathbb{R}$ x $\mathbb{R}$ $\rightarrow$ $\mathbb{R}$ } **y** "$\circ$" la composición de funciones, definida como:

   $\circ$: F($\mathbb{R}$) x F($\mathbb{R}$) $\rightarrow F(\mathbb{R})$

   $(f; g) \rightarrow f \circ g$

   Entonces, $(F(R); \circ)$ es un monoide, pues la composición de dos funciones reales es otra función real.

Definición

Un conjunto $A \neq \Phi$, provisto de una LCI "$*$" que es asociativa se llama ***semigrupo***.
Es decir:

$$(x*y)*z = x*(y*z); \quad \forall x, y, z \in A$$

Ejemplos:

1. $(\mathbb{N}, +)$, es un semigrupo, pues:

$$(x+y)+z = x+(y+z); \quad \forall x, y, z \in \mathbb{N}$$

Así:

$$(2+3)+7 = 2+(3+7)$$
$$5+7 = 2+10$$
$$10 = 10$$

2. Sea $A = \{a;b\}$ y "$*$" definida por:

$*$	a	b
a	a	b
b	b	a

Se verifica que:

$$(x*y)*z = x*(y*z); \quad \forall x, y, z \in A$$

Por ejemplo:

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

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

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

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

Por lo tanto $(A;*)$ es un semigrupo.

1.4 Elementos distinguidos

1.4.1 Elementos permutables

Sea $(A;*)$ un monoide, decimos que $a \in A$ y $b \in A$ son permutables si: $a * b = b * a$.

Ejemplo 1:

En ($\mathbb{N}, +$) 3 y 5 son permutables,
Pues 3 + 5 = 5 + 3.

Ejemplo 2:

Sea $A = \{1;2;3\}$ y "$*$" definido por:

$*$	1	2	3
1	1	2	3
2	3	3	1
3	2	1	2

2 y 3 son permutables pues: $2 * 3 = 3 * 2$

$1 = 1$

Ejemplo 3:

En ($\mathbb{Q} - \{0\}, \div$) 1 y -1 son permutables pues: $\frac{1}{-1} = \frac{-1}{1}$

Definición.-

La ley de composición interna "$*$" es conmutativa**, s**i todos los elementos son permutables; es decir:

$$x * y = y * x, \forall x; y \in A.$$

Ejemplo 1

Sea $A = \{a;b;c\}$ y $*$ definido por:

$*$	a	b	c
a	a	a	b
b	a	b	c
c	b	c	c

$a * b = b * a$

$a * c = c * a$

$b * c = c * b$

Ejemplo 2:

En $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, la adición es una ley conmutativa, pues: a + b = b + a.

Así, ($\mathbb{N}$, +), $(\mathbb{Z},+)$, $(\mathbb{Q},+)$ y $(\mathbb{R},+)$ son monoides conmutativos.

1.4.2 Elemento neutro

Definición

Sea $(A;*)$ un monoide, un elemento $e \in A$ se llama neutro, si;

$$e * a = a \quad \wedge \quad a * e = a, \ \forall a \in A$$

Ejemplo 1:

En ($\mathbb{N}$, +), $(\mathbb{Z},+)$, $(\mathbb{Q},+)$ y $(\mathbb{R},+)$ y $(\mathbb{C},+)$, el "0" es elemento neutro, pues:

$$0 + a = a + 0 = a, \ \forall a$$

Ejemplo 2:

En $(\mathbb{N},\cdot)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Q},\cdot)$ y $(\mathbb{R},\cdot)$ y $(\mathbb{C},\cdot)$, el "1" es elemento neutro, pues:

$$1 \cdot a = a \cdot 1 = 1, \ \forall a \in \mathbb{N}, \ \mathbb{Z}, \ \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

Ejemplo 3:

En $\mathbb{Q}$, se define la LCI $a * b = \frac{a \cdot b}{4}$. Hallar el neutro si existe.

Solución:

Supongamos que el neutro es "*e*"; entonces:

$$e * a = a \quad \wedge \quad a * e = a$$

$$\frac{e \cdot a}{4} = a \qquad \frac{a \cdot e}{4} = a$$

$$e \cdot a = 4 \cdot a \qquad a \cdot e = 4 \cdot a$$

$$e = 4 \qquad e = 4$$

1.4.3 Elemento simétrico

Definición.-

Sea $(A;*)$ un semigrupo con elemento neutro *e*; un elemento $a \in A$ es simetrizable, si existe $a' \in A$, tal que: $a' * a = e$ y $a * a' = e$ o $a' * a = a * a' = e$.

Ejemplo 1:

En ($\mathbb{Z}$; $+$) el opuesto de 5 es -5, pues $(-5) + 5 = 0 \ \wedge \ 5 + (-5) = 0$.

En general el opuesto de $a \in \mathbb{Z}$ es $-a \in \mathbb{Z}$, puesto que: $(-a) + (a) = (a) + (-a) = 0$.

Ejemplo 2:

En ($\mathbb{R}$- {0}; $\cdot$)

- El inverso de 3 es 1/3, pues $3 \cdot \frac{1}{3} = \frac{1}{3} \cdot 3 = 1$
- El inverso de 2/5 es 5/2, pues $\frac{2}{5} \cdot \frac{5}{2} = \frac{5}{2} \cdot \frac{2}{5} = 1$.
- En general:

El inverso de $a \in R^{-\{0\}}$, será $\frac{1}{a}^{'}$ pues $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$.

Ejemplo 3:

En $\mathbb{R}$ se define la operación $a * b = \sqrt{a^2 + b^2}$.

Hallar el neutro y simétrico, si existen.

Solución:

a. Para hallar el elemento neutro, supongamos que el neutro es $e \in \mathbb{R}$.

Entonces se debe verificar que:

$$e * a = a \quad \wedge \quad a * e = a$$

$$\sqrt{e^2 + a^2} = a \qquad \sqrt{a^2 + e^2} = a$$

$$e^2 + a^2 = a^2 \qquad a^2 + e^2 = a^2$$

$$e^2 = 0 \qquad e^2 = 0$$

$$e = 0 \qquad e = 0$$

Por lo tanto el elemento neutro de $(\mathbb{R}\ ,\ *)$ es $e = 0$.

b. Para hallar el elemento simétrico:

$$a^{'} * a = e \quad \wedge \quad a * a^{'} = e$$

$$\sqrt{(a')^2 + a^2} = 0 \qquad \sqrt{a^2 + (a')^2} = 0$$

$$(a')^2 + a^2 = 0 \qquad a^2 + (a')^2 = 0$$

$$(a')^2 = 0 \qquad (a')^2 = 0$$

$$a' = 0 \qquad a' = 0$$

Luego, en $(\mathbb{R}\ ,\ *)$ el elemento simétrico de a es $a' = 0$.

1.5 Grupos y subgrupos

1.5.1 Grupos

Definición.-

Sea el conjunto $G \neq \Phi$, "$*$" una L.C.I. definida sobre G; se dice que el monoide $(G;*)$ tiene la estructura de ***grupo*** si y solo si verifica los siguientes axiomas:

G_1. Asociativa: $(x*y)*z = x*(y*z)$, $\forall x, y, z \in G$.

G_2. Existencia del elemento neutro: $\exists e \in G / e*x = x*e = x$, $\forall x \in G$.

G_3. Existencia del elemento simétrico: $\exists x' \in G$, $x'*x = x*x' = e$, $\forall x \in G$.

Si además se cumple:

G_4. Conmutativa: $x*y = y*x$, $\forall x, y \in G$, el grupo $(G,*)$ es un ***grupo abeliano.***

Ejemplos:

El conjunto de los números enteros provisto de la operación de adición $(\mathbb{Z}, +)$, es un grupo conmutativo o grupo abeliano.

En efecto:

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

$$(a;b) \to a+b$$

Además cumple:

G_1: $\forall x, y, z \in \mathbb{Z}$; $(x+y)+z = x+(y+z)$

Ejemplo:

$$(1+3)+5 = 1+(3+5)$$

$$4+5 = 1+8$$

$$9 = 9$$

G_2: Existe e = $0 \in \mathbb{Z}, / 0+x = x+0 = x, \ \forall x \in \mathbb{Z}$

Ejemplo:

$$0+5 = 5+0$$

$$5 = 5$$

G3: $\forall x \in \mathbb{Z},\ \exists -x \in \mathbb{Z}\ /\ \ (-x) + x = x + (-x) = 0$

Ejemplo:

$$(-5) + 5 = 5 + (-5)$$
$$0 = 0$$

G4: $x + y = y + x,\ \forall x, y \in \mathbb{Z}$

Ejemplo:

$$8 + 10 = 10 + 8$$
$$18 = 18$$

1. Sea $A = \{a;b\}$ y la operación $*$ definida por:

$*$	a	b
a	a	b
b	b	a

¿Será $(A;*)$ un grupo abeliano?

Veamos:

G1: Asociativa: $\forall a,b \in A,\ (x * y) * z = x * (y * z)$

Ejemplos:

$(a * b) * a = a * (b * a)$ $\qquad$ $(a * a) * b = a * (a * b)$

$b * a = a * b$ $\qquad$ $a * b = a * b$

$b = b$ $\qquad$ $b = b$

G2: Existencia del elemento neutro:

Así:

i. $\begin{matrix} a*e=a \\ e=a \end{matrix} \quad \wedge \quad \begin{matrix} e*a=a \\ e=a \end{matrix}$

ii. $\begin{matrix} b*e=b \\ e=a \end{matrix} \quad \wedge \quad \begin{matrix} e*b=b \\ e=a \end{matrix}$

G_3: Existencia del elemento simétrico: $\forall x \in A, \exists x' \in A / x'*x = x*x' = e$

Para a, $a*a=a*a=a$; luego $a'=a$

Para a, $b*b=b*b=a$; luego $b'=b$

G_4: Conmutativa: $a*b=b*a$

$b=b$

Por G_1, G_2, G_3 y G_4, $(A;*)$ es un grupo abeliano.

3. ¿Será $\mathbb{Z}$ provisto de la multiplicación "$\cdot$", un grupo?

Prueba:

En efecto la multiplicación es una LCI, pues:

$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

$$(a;b) \to a \cdot b$$

Además cumple:

G_1: $\forall x, y, z \in \mathbb{Z};\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$

$(1 \cdot 3) \cdot 5 = 1 \cdot (3 \cdot 5)$

$3 \cdot 5 = 1 \cdot 15$

$15 = 15$

G_2: Existe e = 1 $\in \mathbb{Z}$ $/ 1 \cdot x = x \cdot 1 = x$; $\forall x \in \mathbb{Z}$

$$1 \cdot 5 = 5 \cdot 1$$

$$5 = 5$$

G_3: Existencia del elemento simétrico:

Para cualquier número entero x debería existir otro entero x' tal que:

$$x' \cdot x = x \cdot x' = e$$

Pero por ejemplo para $8 \in \mathbb{Z}$, $8^{-1} = \frac{1}{8} \notin \mathbb{Z}$

Es decir, no existe un entero que multiplicado por 8 sea igual a 1

Por lo que, $(\mathbb{Z}, \cdot)$ no es un grupo

4. El par **($\mathbb{Z}$, $*$)** donde $\mathbb{Z}$ es el conjunto de los números enteros y $*$ es una LCI definida como a $*$ b = a + b + 3, es un grupo abeliano.

Verifiquemos:

- $*$ es una LCI en $\mathbb{Z}$ **,** pues:

  Si a y b $\in \mathbb{Z}$, (a + b + 3) $\in \mathbb{Z}$ puesto que la adición es LCI en $\mathbb{Z}$.

- $*$ es asociativa, pues

  (a $*$ b) $*$ c = (a + b +3) $*$ c = a + b +3 + c +3 = a + b + c + 6

  y

  a $*$ (b $*$ c) = a $*$ (b + c + 3) = a + b + c + 3 + 3 = a + b + c + 6

- Existe un elemento neutro, puesto que, $\forall$a $\in \mathbb{Z}$:

  a $*$ e = a implica que: a + e +3 = a, de donde: e = –3 ; y,

  e $*$ a = a implica que: e + a + 3 = a, de donde: e = –3

- Todo elemento a $\in \mathbb{Z}$ tiene inverso, ya que:

$a * a' = -3 \Rightarrow a + a' + 3 = -3$ luego $a' = -a - 6$ es inverso a derecha

$a' * a' = -3 \Rightarrow a' + a + 3 = -3$ luego $a' = -a - 6$ es inverso a izquierda

- Finalmente, $*$ es conmutativa pues, $a * b = a + b + 3 = b + a + 3 = b * a$

1.5.2 Subgrupos

Definición.-

Sea $(G;*)$ un grupo, y un subconjunto no vacío H del conjunto G; decimos que H es un subgrupo de G; si $(H;*)$ es grupo.

$$*: H \times H \to H$$
$$(a;b) \to a * b$$

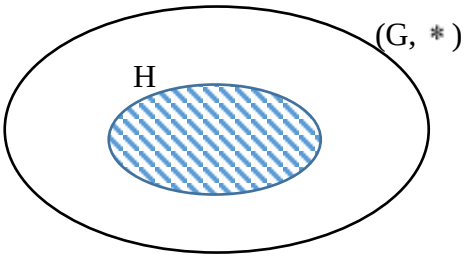

Figura 1. Subgrupos

Es decir:

Dado el grupo $(G;*)$ y $\emptyset \neq H \subset G$;

$(H;*)$ es un subgrupo de $(G;*) \Leftrightarrow (H;*)$ es un grupo.

Ejemplo 1:

1. **($\mathbb{Z}$, +)** es un subgrupo de **($\mathbb{Q}$, +)**.

Ejemplo 2:

Dado el grupo abeliano $(\mathbb{Z}, +)$;

$2\,\mathbb{Z} \subset \mathbb{Z}$, $3\mathbb{Z} \subset \mathbb{Z}$, $4\,\mathbb{Z} \subset \mathbb{Z}$, $5\,\mathbb{Z} \subset \mathbb{Z}$, $\ldots, n\,\mathbb{Z} \subset \mathbb{Z}$

Además se sabe que: $(2\,\mathbb{Z}, +)$, $(3\,\mathbb{Z}, +)$, $(4\,\mathbb{Z}, +)$, $(5\mathbb{Z}, +)$, $\ldots, n\,\mathbb{Z}$ son grupos.

Entonces:

$(2\,\mathbb{Z}, +)$, $(3\,\mathbb{Z}, +)$, $(4\,\mathbb{Z}, +)$, $(5\mathbb{Z}, +)$, $\cdots$ son subgrupos de $\mathbb{Z}$.

Ejemplo 3:

Se sabe que $\mathbb{Z} \subset \mathbb{Q}$ y $\mathbb{Q} \subset \mathbb{R}$

Por lo que **($\mathbb{Z}$, +)** **e**s subgrupo de **($\mathbb{Q}$, +), ($\mathbb{Q}$, +)** es subgrupo de **($\mathbb{R}$, +)**

Además **($\mathbb{Z}$, +)** es subgrupo de **($\mathbb{R}$, +)**.

1.5.3 Condición suficiente para la existencia de subgrupos

Sea $(G;*)$ un grupo; un subconjunto $\emptyset \neq H \subset G$ es un subgrupo de G si y solo si $\forall x; y \in H$: $x * y \in H$.

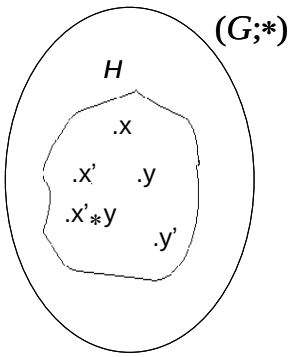

Figura 2. Condición suficiente para la existencia de subgrupos

Teorema:

Sea **($\mathbb{Z}$, +)** el grupo de los enteros en la adición, $(n\mathbb{Z}, +)$ es subgrupo de $(\mathbb{Z}, +)$.

Demostración:

Debemos probar que: $\forall x; y \in \mathbb{Z};\ (-x) + y \in\ n\mathbb{Z}.$

Si $x \in n\mathbb{Z};\ \ -x = n(-t)\,,\ \ t \in\ \mathbb{Z}.$

Si $y \in n\mathbb{Z};\ -x = n(t')\,,\ \ t' \in\ \mathbb{Z}.$

$$(-x) + y = n(-t) + nt'$$

$$(-x) + y = n(-t + t')$$

$$(-x) + y = nt'' \in n\mathbb{Z}$$

$\therefore$ $(n\mathbb{Z}\ ,\ +)$ es subgrupo de $(\mathbb{Z},\ +\ )$.

Capítulo II: Estructura de anillo

2.1 Anillo

La estructura de anillo es una estructura más compleja que la estructura de grupo. Mientras que en la estructura de grupo se tiene un conjunto no vacío provisto de una LCI, la estructura de anillo está conformada por un conjunto no vacío y dos leyes de composición interna, en la que cada una de ellas verifica ciertas propiedades.

El anillo más conocido o más sencillo es el de los números enteros, donde están definidas un par de operaciones, la adición y la multiplicación, relacionadas entre sí por una ley de distributividad. Sobre esta base es más fácil entender la generalización de esta estructura algebraica.

Definición:

Sean un conjunto no vacío A, y dos leyes de composición interna " $*$ " y " $\circ$ "; la terna $(A;\ *;\ \circ)$ es un **anillo**, si y solo si:

1. $(A;\ *)$ es un grupo abeliano
2. $(A;\ \circ)$ *es un semigrupo*

3. *La segunda LCI* $(\circ)$ *es distributiva respecto a la primera* $(*)$.

Identificando estas dos leyes de composición con las leyes aditiva (+) y multiplicativa $(\cdot)$ respectivamente, podemos reformular esta definición, de la siguiente manera.

La terna $(A,\ +,\ \cdot)$ es un **anillo** si y solo si:

1. $(A;\ +)$ es un grupo abeliano
2. $(A;\ \cdot)$ *es un semigrupo*
3. *El producto es distributivo respecto a la adición.*

En otras palabras, $(A,\ +,\ \cdot)$ es un **anillo** si y solo si:

$A_1\ :\ \forall\ a \in A, \forall\ b \in A, \forall\ c \in A:\ a + (b + c) = (a + b) + c$

Ley asociativa respecto a " $+$ "

$A_2\ :\ \exists\ 0 \in A\ /\ a\ + 0 = 0 +\ a\ ;\quad \forall\ a \in A$

Existencia del elemento neutro respecto a " $+$ "

$A_3\ :\ \forall\ a \in A,\ \exists - a \in A\ /\ a\ + (-a) = (-a) + a = 0$

Ley del opuesto aditivo.

$A_4\ :\ \forall\ a \in A, \forall\ b \in A:\ a\ + b\ =\ b + a$

Ley conmutativa respecto de " $+$ "

$A_5\ :\ \forall\ a \in A, \forall\ b \in A, \forall\ c \in A:\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Ley asociativa respecto a " $\cdot$ "

$$A_6 \ : \ \forall \ a,b,c \ \in \ A; \qquad \begin{cases} a \cdot (b+c) = a \cdot b + a \cdot c \\ (b+c) \cdot a = b \cdot a + c \cdot a \end{cases}$$

Ley distributiva de la $" \cdot "$ respecto a la $" + "$

2.2 Tipos de anillos

2.2.1 Anillo conmutativo

Definición.-

Si además, la ley multiplicativa ($\cdot$) es conmutativa, decimos que $(A, \ +, \ \cdot)$ es un ***anillo conmutativo***.

2.2.2 Anillo con identidad

Definición.-

Si existe elemento neutro o identidad respecto a la ley multiplicativa $(\cdot)$, entonces $(A, \ +, \ \cdot)$ se llama ***anillo con identidad*** o con unidad.

Es decir, se cumple que:

$$\forall \ a \in A, \qquad \exists \ 1 \in A \ / \ \ a \cdot 1 = 1 \cdot a = a$$

Ejemplo 1:

$(\mathbb{Z}, +, \ \cdot)$ es un anillo conmutativo con unidad.

Puesto que:

1. $(\mathbb{Z}, +)$ es un grupo.
2. $(\mathbb{Z}, \ \cdot)$ es asociativa, conmutativa y tiene elemento neutro (1).
3. Además $" \cdot "$ es distributiva respecto a “+”.

Ejemplo 2:

$(\mathbb{Q}, +, \cdot)$ es un anillo conmutativo con unidad.

Puesto que:

1. $(\mathbb{Q}, +)$ es un grupo.
2. $(\mathbb{Q}, \cdot)$ es asociativa, conmutativa y tiene elemento neutro (1).
3. Además "$\cdot$" es distributiva respecto a "+".

Ejemplo 3:

$(\mathbb{R}, +, \cdot)$ es un anillo conmutativo con unidad.

Puesto que:

1. $(\mathbb{R}, +)$ es un grupo.
1. $(\mathbb{R}, \cdot)$ es asociativa, conmutativa y tiene elemento neutro (1).
2. Además "$\cdot$" es distributiva respecto a "+".

Ejemplo 4:

$(\mathbb{N}, +, \cdot)$ no es un anillo, puesto que los elementos no nulos carecen de opuesto aditivo.

Ejemplo 5:

Sea M el conjunto de matrices de la forma:

$$M = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \ / \ a, b \in \mathbb{Z} \right\}$$

Verifique que $(M, +, \cdot)$ es un anillo.

En efecto:

En primer lugar, dados,

$A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ y $B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$, $A + B = \begin{pmatrix} a+c & 0 \\ 0 & b+d \end{pmatrix} \in$ M

A_1 : $A + (B + C) = (A + B) + C$, $\forall\ A, B, C \in M$

Se justifica por la asociatividad de " $+$ " en $\mathbb{Z}$

A_2 : Existe $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M$ / $A + 0 = 0 + A$; $\forall\ a \in M$

A_3 : $\forall\ A \in M$, existe $-A = \begin{pmatrix} -a & 0 \\ 0 & -b \end{pmatrix} \in M$ / $A + (-A) = (-A) + A = 0$

A_4 : $\forall\ A, B \in M$: $A + B = B + A$

Se justifica por la conmutatividad de " $+$ " en $\mathbb{Z}$

A_5 : $\forall\ A,\ B,\ C \in M$: $A \cdot (B \cdot C) = (A \cdot B) \cdot C$

Se justifica por la asociatividad de " $\cdot$ " en $\mathbb{Z}$

A_6 : $\forall\ A, B, C \in M$; $\begin{cases} A \cdot (B + C) = A \cdot B + A \cdot C \\ (B + C) \cdot A = B \cdot A + C \cdot A \end{cases}$

Se justifica por la distributividad de " $\cdot$ " respecto a " $+$ " en $\mathbb{Z}$.

Luego, $(M, +, \cdot)$ es un anillo.

Además se verifica que:

- $(M, \cdot)$ es conmutativo, basado en la conmutatividad de la multiplicación en $\mathbb{Z}$.
- Existe $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$ / $A \cdot I = I \cdot A = A, \forall\ A \in M$.

Por lo que, $(M, +, \cdot)$ es un anillo conmutativo con unidad.

Ejemplo 6:

Sea $(\mathrm{M},+,\cdot)$ el conjunto de matrices cuadradas de orden 2×2 con coeficientes reales. Si A y B son dos elementos de M, la suma y el producto están dadas por:

$$A + B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$
$$= \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$A \cdot B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$
$$= \begin{pmatrix} a.e + b.g & a.f + b.h \\ c.e + d.g & c.f + d.h \end{pmatrix}$$

M con estas dos leyes de composición interna es un anillo con unidad.

Pues, para cualquier $X \epsilon$ M, existe la matriz $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \epsilon$ M , tal que:

$X \cdot I = I \cdot X = X$.

Pero, $(\mathrm{M},+,\cdot)$ no es un anillo conmutativo.

Por ejemplo, si tomamos las matrices:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad y \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

Operando A por B, se tiene: $AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

Mientras que B por A es:

$$BA = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

Es decir, $AB \neq BA$, por lo que el anillo $(\mathrm{M},+,\cdot)$ no es conmutativo.

Ejemplo 7:

En el conjunto $\mathbb{Z}$ se definen las siguientes LCI:

$$a * b = a + b - 1$$
$$a \circ b = a + b - ab$$

Demostrar que $(\mathbb{Z}, *, \circ)$ es un anillo conmutativo con unidad.

Prueba

1. En primer lugar, veamos que $(\mathbb{Z}, *)$ es un grupo abeliano.

- Se verifica que es una LCI, pues la suma de números enteros es un número entero.
- Es asociativa.

  Pues, se verifica que para todo $a, b, c \in \mathbb{Z}$:

$$a * (b * c) = a * (b + c - 1) = a + b + c - 2.$$
$$(a * b) * c = (a + b - 1) * c = a + b + c - 2.$$

- Es conmutativa

  Pues se verifica que para todo $a, b \in \mathbb{Z}$:

$$a * b = a + b - 1 = b + a - 1 = b * a.$$

- Existe elemento neutro

  Porque, para cualquier número entero, el número 1 satisface:

$$a * 1 = 1 * a = a + 1 - 1 = a$$

  Luego, $1 \in \mathbb{Z}$ es el elemento neutro para la operación $*$.

- Existencia del elemento simétrico

  Para todo $a \in \mathbb{Z}$, el número entero $2 - a$ satisface:

$$a * (2-a) = (2-a) * a = a + 2 - a - 1 = 1$$

Por tanto, todo número entero tiene simétrico, que es: $2-a$

Por lo que se concluye que, $(\mathbb{Z}, *, \circ)$ es un grupo abeliano.

2. Ahora, veamos que $(\mathbb{Z}, \circ)$ es un semigrupo.

- Se verifica que la ley $\circ$ es de composición interna, pues la suma y producto de números enteros es un número entero.
- Asociativa.

  Se verifica, pues para todo $a, b, c \in \mathbb{Z}$:

$$\begin{aligned} a \circ (b \circ c) &= a \circ (b + c - bc) \\ &= a + b + c - bc - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc \end{aligned}$$

$$\begin{aligned} (a \circ b) \circ c &= (a + b - ab) \circ c \\ &= a + b - ab + c - (a - b - ab)c \\ &= a + b - ab + c - ac - bc + abc. \end{aligned}$$

Luego, $(\mathbb{Z}, \circ)$ es un semigrupo conmutativo, pues además:

$$a \circ b = a + b - ab = b + a - ba = b \circ a$$

3. Por último, veamos que $\circ$ es distributiva respecto $*$:
4.

Dado que $\circ$ es conmutativa, bastará demostrar que para todo $a, b, c \in \mathbb{Z}$ se verifica $a \circ (b * c) = (a \circ b) * (a \circ c)$

En efecto:

$$a \circ (b * c) = a \circ (b + c - 1)$$

$$= a + b + c - 1 - a(b + c - 1)$$
$$= 2a + b + c - ab - ac - 1.$$

$$(a \circ b) * (a \circ c) = (a + b - ab) * (a + c - ac)$$
$$= (a + b - ab) + (a + c - ac) - 1$$
$$= 2a + b + c - ab - ac - 1.$$

Por (1), (2) y (3), se concluye que $(\mathbb{Z}, *, \circ)$ es un anillo conmutativo.

Además es unitario, pues el número $0 \in \mathbb{Z}$ satisface para todo $a \in \mathbb{Z}$:

$$a \circ 0 = 0 \circ a = a + 0 - 0a = a$$

Es decir $0 \in \mathbb{Z}$ es el elemento unidad del anillo.

Observaciones:

- Un anillo $(A, +, \cdot)$ siempre contiene al elemento 0.
- Si este es el único elemento de $(A, +, \cdot)$ entonces $(A, +, \cdot)$ se llama el ***anillo nulo*** o anillo cero.

2.3 Propiedades de los anillos

Teorema:

Sea $(A, +, \cdot)$ un anillo, y a, b, c elementos de A.

1) $Si\ a + b = a + c, entonces\ b = c$
2) $Si\ a + a = a,\ entonces\ a = 0$
3) $-(-a) = a$
4) $(-a)(-b) = ab$
5) $-(a + b) = -a - b$

Demostración

1) $a + b = a + c \Rightarrow -a + a + b = -a + a + c \Rightarrow 0 + b = 0 + c \Rightarrow b = c$
2) $a + a = a \Rightarrow a + a = a + 0 \Rightarrow a = 0$
3) $-a + a = 0 = -a + (-(-a)) \Rightarrow a = -(-a)$
4) $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$
5) $(-a - b) + (a + b) = a - a + b - b = 0 \Rightarrow (-a - b) = -(a + b)$

Proposición:

Sea $(A, +, \cdot)$ un anillo, entonces, $\forall\, a, b \in A$, se tiene:

$i)\ a \cdot 0 = 0 \cdot a = 0$
$ii)\ a(-b) = (-a)b = -(ab)$

Demostración

i) Usando la propiedad distributiva de la definición para $(A, +, \cdot)$, se obtiene:

$$a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$$
$$a.0 + 0 = a \cdot 0 + a \cdot 0$$

Luego, al aplicar la propiedad de cancelación en el grupo aditivo A, se tiene:

$$a \cdot 0 = 0$$

Del mismo modo se demuestra que:

$$0 \cdot a = 0$$

ii) De acuerdo a i) se tiene

$$\begin{aligned} 0 &= a \cdot 0 \\ &= a(b-b) \\ &= ab + a(-b) \end{aligned}$$

Por lo tanto el inverso de ab bajo la adición en A (el cual es único) es $a(-b)$ es decir:

$$-(ab) = a(-b)$$

De la misma forma se demuestra que:

$$-(ab) = (-a)b$$

Corolario:

Sea $(A, +, \cdot)$ anillo con identidad; entonces:

i) $(-1)a = -a \quad \forall\, a \in A$

ii) $(-1)(-1) = 1$

Demostración

i) Sea $a \in A$, luego por la proposición se tiene:

$$(-1)a = -(1a) = -a$$

ii) Aplicando la proposición dos veces, se tiene:

$$\begin{aligned} (-1)(-1) &= -(1(-1)) \\ &= -(-(1.1)) \\ &= 1 \end{aligned}$$

Nota:

Se ha usado la propiedad $-(-a) = a$; que se cumple porque A es un grupo bajo la adición.

2.4 Anillo con divisores de cero

Definición.-

El anillo $(A, +, \cdot)$ tiene **divisores de cero**, si y solo si, elementos no nulos dan producto nulo. Es decir:

$$A\ tiene\ divisores\ de\ cero \Leftrightarrow \forall\, x, y: \ x \neq 0 \wedge \ y \neq 0 \Rightarrow x.y = 0$$

Definición.-

El anillo $(A, +, \cdot)$ no tiene divisores de cero, si y solo si, elementos no nulos dan producto diferente de cero.

Ejemplo 1:

Determinar los divisores de cero del anillo $\mathbb{Z}_6$:

Solución

Sea $\mathbb{Z}_6$ el anillo de los enteros módulo 6.

La tabla de Cayley del producto es:

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Luego

$$[2] \neq [0] \quad y \quad [3] \neq [0],$$

Pero

$$\begin{aligned} [2][3] &= [2 \cdot 3] \\ &= [6] \\ &= [0] \end{aligned}$$

De manera que los divisores de cero son 2, 3 y 4.

Ejemplo 2:

Sea $(\mathbb{Z}, +, \cdot)$ el anillo de los enteros. Por las propiedades de los números enteros, se sabe $(\mathbb{Z}, +, \cdot)$ no tiene divisores de cero. Para probar, basta aplicar la ley de cancelación para el producto en $(\mathbb{Z}, +, \cdot)$.

En efecto:

Dados los enteros $a \neq 0 \;\; y \;\; b \neq 0 \;\; con \; ab = 0$

Se tiene: $a0 = 0 = ab$

De donde $b = 0$, lo cual es una contradicción.

Definición:

Un anillo $(A;\ *;\ \circ)$ se dice que es un ***cuerpo o campo*** si:

1°) $(A;\ *)$ es un grupo abeliano

2) $(A';\ \circ)$ es un grupo abeliano, donde $A' = A - \{0\}$

Ejemplos:

$(\mathbb{Q}, +,\ \cdot)$, $(\mathbb{R}, +,\ \cdot)$ y $(\mathbb{C}, +,\ \cdot)$ son cuerpos.

2.5 Dominio de integridad

Definición:

Un anillo conmutativo con identidad que no posee divisores de cero se llama dominio de integridad.

Observación:

En un dominio de integridad, el producto de dos elementos no nulos, es distinto de cero.

Ejemplos:

1. $(\mathbb{Z}, +,\ \cdot)$ es dominio de Integridad
2. $(\mathbb{Q}, +,\ \cdot)$ es dominio de Integridad
3. $(\mathbb{R}, +,\ \cdot)$ es dominio de Integridad
4. $(A, +,\ \cdot)$ un anillo, $A = M_{2\times 2}(\mathbb{R})$ no es ***dominio de integridad***.

Por ejemplo:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Definición:

Dado $(A, +, \cdot)$ dominio de integridad con elemento identidad (1) un elemento $a \in A,\ a \neq \emptyset$ se dice que es una **unidad** de A, si $\exists\ b \in A\ /\ a.b = 1$.

Ejemplo 1:

En los enteros $(\mathbb{Z},\ +,\ \cdot)$

Para $1 \neq 0 \quad \exists\ 1 \in \mathbb{Z}\ /\ (1)(1) = 1$

$-1 \neq 0 \quad \exists\ -1 \in \mathbb{Z}\ —\ (-1)(-1) = 1$

Entonces $\{-1, 1\}$ son unidades del anillo $(\mathbb{Z},\ +,\ \cdot)$.

Ejemplo 2:

En el anillo $(\mathbb{Z}_p, +,\ \cdot)$ donde p es primo

Como $\mathbb{Z}_p$ es un cuerpo $\forall\ \bar{a} \neq 0,\ \exists\ \bar{a}^{-1} \in \mathbb{Z}_p\ /\ \bar{a}.\bar{a}^{-1} = 1$

$\Rightarrow \forall\ \bar{a} \neq 0\ , \exists\ \bar{a}^{-1} \in \mathbb{Z}_p\ /\ \bar{a}.\bar{a}^{-1} = 1$

$\Rightarrow \quad \mathbb{Z}_p - \{0\}$ Son las unidades de $\mathbb{Z}_p$.

2.5.1 Característica de un anillo

Definición.-

Sea A un dominio de integridad: entonces, el menor entero positivo n (si existe) tal que $na = 0$ para todo $a \in A$ se llama la característica del anillo. Si no existe dicho entero, entonces se dice que A es de característica 0.

Ejemplo 1:

El anillo $(\mathbb{Q}, +,\ \cdot)$ de los números racionales con la suma y el producto habituales, es un anillo de característica 0.

Ejemplo 2:

El anillo $\mathbb{Z}_7$ de los enteros módulo 7 es de característica 7, pues si $\bar{a} = [a] \in \mathbb{Z}_7$ se tiene que

$$7[a] = [7a] = [0]$$

Además no existe un entero positivo menor con dicha propiedad.

Teorema:

El anillo $(\mathbb{Z}_m, +, \cdot)$ es dominio de integridad de característica $m > 1 \Leftrightarrow m$ es primo.

Demostración

$\Rightarrow$)

Si m no fuera primo, entonces, $m = rs$ con r, s enteros tales que $1 < r < m$ y $1 < s < m$.

Esto implicaría $\bar{r} \cdot \bar{s} = \overline{m} = \bar{0}$ siendo $\bar{r} \neq \bar{0}$ y $\bar{s} \neq \bar{0}$.

Existirían divisores de cero, lo que contradice la hipótesis de ser $\mathbb{Z}_m$ de integridad.

$\Leftarrow$)

Supongamos que $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$ tuviera divisores de cero, es decir que existieran elementos $\bar{r}$ y $\bar{s}$ de $\mathbb{Z}_m$ no nulos tales que $\bar{r} \cdot \bar{s} = \bar{0}$.

Esto implicaría que m divide a rs.

Ahora bien, dado que $r < m$ y m es primo, r y m son primos entre sí, y al dividir m a rs y ser primo con r, m divide a s (por tanto $\bar{s} = \bar{0}$), lo cual es absurdo pues se ha supuesto que $\bar{s} \neq \bar{0}$.

Ejemplo 1:

$\mathbb{Z}_4 = \{\,\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\bar{2}.\bar{2} = \bar{4} = \bar{0} \quad \nRightarrow \quad \bar{2} = \bar{0}$

$\bar{2}$ es un divisor de cero

Luego, $\mathbb{Z}_4$ no es dominio de Integridad.

Ejemplo 2:

$\mathbb{Z}_5 = \{\,\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$\nexists \;\; a \; y \; b \in \mathbb{Z}_5\,, \;\; a \neq 0, \qquad b \neq 0 \;\; / \;\; \bar{a}.\bar{b} = \bar{5} = \bar{0}$

$\mathbb{Z}_5$ no tiene divisores de cero; $m = 5$ es primo.

$\Longrightarrow \;\; \mathbb{Z}_5$ es dominio de Integridad,

2.6 Subanillos

Definición:

Sea $(A, +, \cdot)$ un anillo; un subconjunto $S \subset A$ es un **subanillo** de $(A, +, \cdot)$; si $(S, +, \cdot)$ es un anillo.

Observación:

- Sea $(\mathbb{Z}, +, \cdot)$ el anillo de los enteros, como $2\mathbb{Z}$, $3\mathbb{Z}$, $5\mathbb{Z}$, $6\mathbb{Z}$, ... están contenidos en $\mathbb{Z}$; entonces se tiene que $(2\mathbb{Z}, +, \cdot)$, $(3\mathbb{Z}, +, \cdot)$, $(5\mathbb{Z}, +, \cdot)$, …. son subanillos de $(\mathbb{Z}, +, \cdot)$.

- Para probar que un subconjunto es un subanillo de un anillo, es condición suficiente:

$$i) \;\; \forall \;\; a, b \in A \;\; ; \quad a - b \in A$$

$$ii) \quad \forall \ a, b \ \in A \ ; \quad a \cdot b \in A$$

Con esta definición probemos el siguiente ejemplo.

Ejemplo 1:

El conjunto de los enteros pares $(2\mathbb{Z}, +, \cdot)$ es un subanillo del anillo $(\mathbb{Z}, +, \cdot)$ de los números enteros.

Prueba

En efecto:

i) Si $a \in 2\mathbb{Z}, \quad b \in 2\mathbb{Z} \ \Rightarrow \ a - b \ \in \ 2\mathbb{Z}$

Pero,

$$si \quad a \in 2\mathbb{Z}; \quad a = 2n, \quad n \in \mathbb{Z}$$
$$si \quad b \in 2\mathbb{Z}; \quad b = 2m, \quad m \in \mathbb{Z}$$

Entonces,

$$\begin{aligned} a - b &= 2n - 2m \\ &= 2(n - m) \\ &= 2t \quad \in \quad 2\mathbb{Z} \end{aligned}$$

ii) Si $a \in 2\mathbb{Z}, \quad b \in 2\mathbb{Z} \ \Rightarrow \ a \cdot b \ \in \ 2\mathbb{Z}$

De manera similar al caso anterior.

$$si \quad a \in 2\mathbb{Z}; \quad a = 2n, \quad n \in \mathbb{Z}$$
$$si \quad b \in 2\mathbb{Z}; \quad b = 2m, \quad m \in \mathbb{Z}$$

Entonces:

$$\begin{aligned} a - b &= (2n)(2m) \\ &= 2(2nm) \\ &= 2p \quad \in \quad 2\mathbb{Z} \end{aligned}$$

$\therefore \quad (2\mathbb{Z}, +, \cdot)$ es un subanillo de $(\mathbb{Z}, +, \cdot)$

Observación:

De manera análoga se puede probar en general que: $(n\mathbb{Z}, +, \cdot)$ es un subanillo de $(\mathbb{Z}, +, \cdot)$, $\forall\ n \geq 1$.

Proposición:

Sea $(A, +, \cdot)$ un anillo y sea B un subconjunto no vacío de A

$$B \text{ es subanillo de } A \iff \begin{cases} \text{i)} & \forall\, a, b \in B \Rightarrow a - b \in B \\ \text{ii)} & \forall\, a, b \in B \Rightarrow a.b \in B \end{cases}$$

Demostración:

$\Rightarrow)$

Si B es subanillo de A, entonces $B \neq \emptyset$, pues $0 \in B$.

Además, B es subgrupo aditivo de A , luego se cumple (i).

Como la operación producto es una LCI en B , se cumple (ii).

$\Leftarrow)$

De $B \neq \emptyset$ y (i), se deduce que $(B, +)$ es subgrupo de $(A, +)$ y además como $(A, +)$ es abeliano, $(B, +)$ es grupo abeliano.

De (ii) se deduce que la operación producto es cerrada en B, y además, es asociativa en B porque A es asociativa, lo que implica que $(B, \cdot)$ es un semigrupo.

Por último, se cumple la propiedad distributiva en B puesto que se cumple en A. Luego, se concluye que $(B,+,\cdot)$ es anillo, por lo que B es subanillo de A.

Ejemplo:

Verifique si el conjunto $B=\{\overline{0},\overline{5},\overline{10}\}$ es un subanillo del anillo $(\mathbb{Z}_{15},+,\ \cdot)$.

Prueba

$$B=\{\overline{0},\overline{5},\overline{10}\}\subset(\mathbb{Z}_{15},+,\cdot)\ \text{ es subanillo si: } \begin{cases}\forall\, x,y\ \in B\ \ ,\ \ x-y\in B\\ \forall\, x,y\ \in B\ \ ,\ \ x\cdot y\in B\end{cases}$$

Operando cada elemento con su opuesto en $(\mathbb{Z}_{15},+,\cdot)$ se tiene:

$\forall\, x,y\ \in B\ \ ,\ \ x-y\in B$	$\forall\, x,y\ \in B\ \ ,\ \ x\cdot y\in B$
$0-0=0+0=\overline{0}\in B$	$0\cdot 0=\overline{0}\in B$
$0-5=0+10=\overline{10}\in B$	$0\cdot 5=\overline{0}\in B$
$0-10=0+5=\overline{5}\in B$	$0\cdot 10=\overline{0}\in B$
$5-0=5+0=\overline{5}\in B$	$5\cdot 0=\overline{0}\in B$
$5-5=5+10=\overline{0}\in B$	$5\cdot 5=\overline{10}\in B$
$5-10=5+5=\overline{10}\in B$	$5\cdot 10=\overline{5}\in B$
$10-0=10+0=\overline{10}\in B$	$10\cdot 0=\overline{0}\in B$
$10-5=10+10=\overline{5}\in B$	$10\cdot 5=\overline{5}\in B$
$10-10=10+5=\overline{0}\in B$	$10\cdot 10=\overline{10}\in B$

Luego $B=\{\overline{0},\overline{5},\overline{10}\}$ es un Subanillo de $(\mathbb{Z}_{15},+,\ \cdot)$.

Observaciones:

- Los subanillos pueden contener o no a la unidad.
- Puede ocurrir que un subanillo de un anillo no conmutativo, sea conmutativo.

Definición:

Un subconjunto $S \subset A$ (anillo) tal que $S \neq \emptyset$ se dice que es un subanillo de A si S con las operaciones de A posee estructura de anillo.

Ejemplo 1:

$A = M_{2\times 2}(\mathbb{R}), \quad (A, +, \cdot)$ es anillo

$B = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \ / \ a \in \mathbb{R} \right\}$ es subanillo.

Ejemplo 2:

$(\mathbb{Z}, +, \cdot)$ es subanillo de $(\mathbb{Q}, +, \cdot)$ y de $(\mathbb{R}, +, \cdot)$.

Observaciones:

- Si $1 \in A$, diremos que A es un subanillo con unidad.
- En todo anillo A, el conjunto A y el 0 son subanillos, llamados subanillos triviales. Los demás subanillos se llaman propios.

Teorema:

Si $\{S_i\}_{i\in I}$ es una familia cualquiera de subanillos de un anillo $(A, +, \cdot)$; entonces la intersección $\bigcap_{i\in I} S_i$ es un subanillo de $(A, +, \cdot)$.

Demostración

Debemos probar que:

$$\forall\, a, b \in \bigcap_{i\in I} S_i \ ; \quad a + (-b) \in \bigcap_{i\in I} S_i$$

$$\forall\, a, b \in \bigcap_{i\in I} S_i \;\; ; \quad a.b \in \bigcap_{i\in I} S_i$$

Entonces, si:

$$a \in \bigcap_{i\in I} S_i \;\; ; \;\; a \in S_i \;\; ; \quad \forall\; i \in I$$

$$b \in \bigcap_{i\in I} S_i \;\; ; \;\; b \in S_i \;\; ; \quad \forall\; i \in I$$

Como los S_i son subanillos, también son anillos.

Entonces:

$$-b \in S_i \;\; ; \quad \forall\; i \in I$$

$$a + (-b) \in S_i \;\; ; \quad \forall\; i \in I$$

$$\Rightarrow \;\; a + (-b) \in \bigcap_{i\in I} S_i$$

También:

$$a.b \in S_i \;\; ; \quad \forall\; i \in I$$

$$\Rightarrow \;\; a.b \in \bigcap_{i\in I} S_i$$

$\therefore$ La $(\bigcap_{i\in I} S_i \;, +, \; .)$ es subanillo de $(A, +, \cdot)$.

Definición:

Sea S un subconjunto de A. A la intersección de todos los subanillos que contienen a S se le llama subanillo generado por el subconjunto S.

Observación:

La unión de subanillos no siempre es un subanillo.

Verificaremos con un ejemplo,

Sea $(\mathbb{Z}, +, \cdot)$ un anillo y $(n\mathbb{Z}, +, \cdot)$ $\forall\ n \geq 1$ subanillos de $(\mathbb{Z}, +, \cdot)$.

Tenemos que:

$2\mathbb{Z} \cup 8\mathbb{Z} = 2\mathbb{Z}$, es un subanillo de $(\mathbb{Z}, +, \cdot)$

pero $2\mathbb{Z} \cup 3\mathbb{Z} \neq n\mathbb{Z}$, no es subanillo de $(\mathbb{Z}, +, \cdot)$.

2.7 Ideales

El concepto de ideal juega un papel importante; pues mediante el uso de ideales es posible definir los anillos cocientes.

Definición:

Sea A un anillo. Un subconjunto I de A se dice ideal a la derecha, *si se tiene:*

i) $a + b \in I$, *para todo* $a, b \in I$

ii) $\gamma a \in I$, *para todo* $\gamma \in A$ *y* $a \in I$.

Definición:

Sea A un anillo. Un subconjunto I de A se dice ideal a la izquierda, *si satisface*

i) $a + b \in I$, *para todo* $a, b \in I$

ii) $a\gamma \in I$, *para todo* $\gamma \in A$ *y* $a \in I$.

A partir de ambas definiciones se tiene:

Definición:

Sea A un anillo. Un subconjunto I de R se dice ideal de A, *si I es un ideal a la derecha y a la izquierda.*

***Definición**:*

Sea $(A,+,\cdot)$ un anillo. Un subanillo $I \subset A$ es un **ideal** de A, si para todo $r \in A$ y $m \in I$ se tiene que $rm,\ mr \in I$.

Ejemplo:

Sea $(\mathbb{Z},+,\cdot)$ el anillo de los enteros y considere que $I = (2\mathbb{Z},+,\cdot)$ el conjunto de los enteros pares. Verificar que $\boldsymbol{I}$ es un ideal de $\mathbb{Z}$.

Solución:

Veamos,

$$\langle 2 \rangle = 2\mathbb{Z} = \{\, 2n\,;\ \ n \in \mathbb{Z}\}$$
$$\forall\ z \in 2\mathbb{Z}\ ,\ \forall\ a \in \mathbb{Z}\ :\ z.a \in 2\mathbb{Z}$$
$$z \in 2\mathbb{Z}:\quad z = 2m\ ,\ m \in \mathbb{Z}$$
$$z.a = 2m.a = 2(ma)\ \in\ \mathbb{Z}$$

Por lo tanto, $I = 2\mathbb{Z}$ es ideal de $(\mathbb{Z},+,\cdot)$.

Proposición:

Sea $(A,+,\cdot)$ un anillo. La intersección de ideales de $(A,+,\cdot)$ es un ideal de $(A,+,\cdot)$.

Demostración

Sea $J = \bigcap_{i\in I} J_i$, donde J_i $(i \in I)$ es un conjunto de ideales.

$i)$ Veamos que J es un subanillo.

$Sea \;\; x,y \in J \;\; \Rightarrow \;\; x,y \in \bigcap_{i\in I} J_i$

$\Rightarrow \;\; x,y \in J_i \,, \quad \forall \; i \in I \quad (J_i \; son \; subanillos)$

$\Rightarrow \;\; x-y \in J_i \,, \quad \forall \; i \in I$

$\Rightarrow \;\; x-y \in \bigcap_{i\in I} J_i = J$

$\Rightarrow \;\; J$ es subgrupo con la adición.

Sea $x,y \in J \Rightarrow x,y \in J_i \,, \quad \forall \; i \in I$

$\Rightarrow \;\; x.y \in J_i \,, \quad \forall \; i \in I$

$\Rightarrow \;\; x.y \in \bigcap_{i\in I} J_i = J$

$\Rightarrow \;\; J$ es cerrado bajo la multiplicación

$\therefore \;\; J$ es Subanillo.

$ii)$ Veamos que J es Ideal.

$Sea \;\; x \in J \;\; \Rightarrow \;\; x \in J_i \,, \quad \forall \; i \in I$

$\Rightarrow \;\; r.x \in J_i \,, \quad \forall \; i \in I \,, \quad \forall \; r \in R \quad (J_i \; son \; ideales)$

$\Rightarrow \;\; r.x \in \bigcap_{i\in I} J_i = J \,, \quad \forall \; r \in R$

$\Rightarrow \;\; J$ es ideal la izquierda.

Análogamente,

$\Rightarrow \;\; J$ es ideal a la derecha.

Luego, J es un Ideal.

Ejemplo:

Si $I = \{\,\bar{0},\ \bar{2}\,\} \subset (\mathbb{Z}_4, +, \cdot)$. Verifique que I es ideal.

Prueba

$$\forall\ z \in I\,, \qquad \forall\ a \in \mathbb{Z}_4\ : \qquad z.a \in I\,, \qquad \mathbb{Z}_4 = \{\,\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$

$$x = 0 \quad \Rightarrow \quad \begin{array}{l} 0.0 = 0\ \in I \\ 0.1 = 0\ \in I \\ 0.2 = 0\ \in I \\ 0.3 = 0\ \in I \end{array}$$

$$x = 2 \quad \Rightarrow \quad \begin{array}{l} 2.0 = 0\ \in I \\ 2.1 = 2\ \in I \\ 2.2 = 0\ \in I \\ 2.3 = 2\ \in I \end{array}$$

Luego $\{\,\bar{0},\ \bar{2}\,\}$ es Ideal de $(\mathbb{Z}_4, +, \cdot)$.

Ejemplo:

Probar que $(\mathbb{Q}, +, \cdot)$ es subanillo de $(\mathbb{R}, +, \cdot)$, pero $(\mathbb{Q}, +, \cdot)$ no es ideal de $(\mathbb{R}, +, \cdot)$.

Prueba

$(\mathbb{Q}, +, \cdot) \subset (\mathbb{R}, +, \cdot)$, además $(\mathbb{Q}, +, \cdot)$ es un Anillo.

Por definición de subanillo, tenemos que,

$(\mathbb{Q}, +, \cdot)$ es Subanillo de $(\mathbb{R}, +, \cdot)$

Sea: $\begin{array}{c} z = 2\ \in \mathbb{Q} \\ a = -10 \in \mathbb{R} \end{array} \quad \Rightarrow \quad \begin{cases} z.a = 2(-10) \\ \ \ = -20 \in \mathbb{Q} \end{cases}$

Sea: $\begin{matrix} z = 2 \ \in \mathbb{Q} \\ a = \sqrt{2} \in \mathbb{R} \end{matrix} \quad \Rightarrow \quad \begin{cases} z.a = 2.\sqrt{2} \\ = 2\sqrt{2} \notin \mathbb{Q} \end{cases}$

Luego, $(\mathbb{Q}, +, \cdot)$ no es Ideal de $(\mathbb{R}, +, \cdot)$.

Teorema (correspondencia):

Sea $\pi : A \longrightarrow A/I$ la proyección canónica.

Existe una correspondencia biunívoca entre ideales de $\frac{A}{I}$ e ideales de A que contienen a I.

Demostración

Sea J un ideal del cociente.

$\Rightarrow \ \pi^{-1}(J)$ es un ideal de A que contiene a I.

Del mismo modo

$\pi\left(\pi^{-1}(J)\right) = J$ es un ideal (proyección canónica epiyectiva)

Esto prueba que la correspondencia es biunívoca.

Teorema:

Sea $(A, +, \cdot)$ un anillo e I un ideal de A.

1. Si J es un ideal de A con $I \subseteq J$ definamos

   $J/I = \{x + I \mid x \in J\}$. Entonces, $\frac{J}{I}$ es un ideal de $\frac{A}{I}$.

   Además, si K es otro ideal de con $I \subseteq K$, tenemos que:

   $K = J$ si y solo si $K/I = J/I$

2. Sea L un ideal de A/I y sea $J = \{x \in A \mid x + I \in L\}$.
   Entonces, J es un ideal de A que contiene a I y $J/I = L$.

Demostración

1. Primero comprobamos que J/I es un ideal de A/I.
   Como J e I son subgrupos de $(A, +)$, J/I es un subgrupo de R/I.

   Ahora, sea $r \in A$ y $a \in J$. Entonces

$$(r + I)(a + I) = ra + I \in J/I.$$

   De la misma forma $(a + I)(r + I) \in J/I$. Entonces J/I es un ideal de A/I. Supongamos ahora que $K/I = J/I$.

   Queremos ver que $K = J$. Sea $k \in K$.
   Entonces existe $j \in J$ tal que $k + I = j + I$.
   Luego, $k - j \in I$, y como $I \subseteq J$, $k \in J$.
   Lo que prueba que $K \subseteq J$.

   De la misma manera obtenemos que $J \subseteq K$.

2. Veamos que J es un ideal de A.
   Demostremos uno de los axiomas de ideales como ejemplo.
   Sean $a \in J$ y $r \in A$.
   Como $a + I \in L, (ra + I) = (r + I)(a + I) \in L$;
   Entonces $ra \in J$.

Si $a \in I, a + I = 0 + I \in L$. Entonces $I \subseteq J$.

Ahora $J/I = L$ por las definiciones de J y J/I.

Así pues, existe una biyección entre los ideales de un anillo cociente A/I y los ideales de A que contienen a I.

2.8 Anillo cociente

Los ideales son importantes porque sirven para definir anillos cocientes.

Definición:

Si I es un ideal del anillo $(A, +, \cdot)$, al conjunto cociente formado por las clases laterales se le llama *anillo cociente*.

$$R/_I = \{a + I \mid a \in A\}$$

Donde el anillo A/I es ***el anillo cociente*** de A módulo I.

Teorema:

Sea $(A, +, \cdot)$ un anillo, e I un ideal de A. Entonces

$$A/_I = \{ a + I \ : \ a \in A\}$$

es un anillo con las operaciones:

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I) \cdot (b + I) = ab + I.$$

Además si A es conmutativo (unitario), entonces A/I es conmutativo (unitario).

Demostración

1) $(A/I, +, \cdot)$ es grupo abeliano.

En efecto, como I es un subgrupo aditivo de A, y la operación $+$ es conmutativa, I es subgrupo normal de A, y según sabemos $A/I = \{a + I : a \in A\}$ es un grupo (además abeliano) con la operación $+$, $(a + I) + (b + I) = (a + b) + I$.

2) $(A/I, \cdot)$ es semigrupo.

Lo primero que tenemos que demostrar es que la operación producto está bien definida en A/I, es decir que el producto depende de las clases en sí, y no del representante que elijamos. Equivalentemente, tenemos que demostrar que:

$$a + I = a' + I \quad y \quad b + I = b' + I \quad \Longrightarrow \quad ab + I = a'b' + I.$$

En efecto,

Si $a + I = a' + I \quad y \quad b + I = b' + I$,

entonces $a' \in a + I \quad y \quad b' \in b + I$,

o sea $a' = a + x, \quad b' = b + y$ para ciertos $x, y \in I$.

Ahora bien,

$$a'b' = (a + x)(b + y) = ab + xb + ay + xy.$$

Como I es ideal, la suma $xb + ay + xy$ pertenece a I, y por tanto $a'b' \in ab + I$, luego $a'b' + I = ab + I$.

Queda demostrado que la operación producto está bien definida en A/I.

LCI:

Por la propia definición, el producto de dos elementos de A/I es un elemento de A/I.

Asociativa:

Para $a+I,\ b+I,\ c+I$ elementos cualesquiera de A/I, y usando la propiedad asociativa del producto en A:

$$[(a+I)(b+I)](c+I)=(ab+I)(c+I)=(ab)c+I.$$

$$=a(bc)+I=(a+I)(bc+I)=(a+I)[(b+I)(c+I)].$$

3) En A/I la multiplicación es distributiva respecto la adición.

En efecto, para $a+I,\ b+I,\ c+I$ elementos cualesquiera de A/I, y usando la propiedad distributiva en A, se tiene:

$$(a+I)[(b+I)+(c+I)]=(a+I)[(b+c)+I]=a(b+c)+I=$$

$$(ab+ac)+I=(ab+I)+(ac+I)=(a+I)(b+I)+(a+I)(c+I).$$

$$[(a+I)+(b+I)](c+I)=[(a+b)+I](c+I)=(a+b)c+I=(ac+bc)+I$$

$$=(ac+I)+(bc+I)=(a+I)(c+I)+(b+I)(c+I).$$

Del que se concluye que $(A/I,+,\cdot)$ es anillo.

Por último, si A es conmutativo, para $a+I,\ \ b+I$, elementos cualesquiera de $\frac{A}{I}$:

$$(a+I)(b+I)=ab+I=ba+I=(b+I)(a+I)$$

Luego A/I es conmutativo.

Si A es unitario con elemento unidad 1, para todo elemento $a+I$ de A/I:

$$(a+I)(1+I)=a\cdot 1+I=a+I$$

$$(1+I)(a+I) = 1 \cdot a + I = a + I,$$

Es decir A/I es unitario con elemento unidad $1+I$.

Ejemplo:

Consideremos el ideal $(n\mathbb{Z}, +, \cdot)$ de $(\mathbb{Z}, +, \cdot)$.

El anillo cociente se denota en este caso por $(\mathbb{Z}_n, +, \cdot)$.

El estudio clásico de las congruencias es el estudio de este anillo.

$$\mathbb{Z}_n = {}^{\mathbb{Z}}/_{n\mathbb{Z}}$$

Proposición:

A/I es un anillo (llamado anillo cociente), que hace de la proyección $\pi : A \rightarrow A/I$ un homomorfismo de anillos, sí y sólo si I es un ideal de R.

Demostración

De lo anterior vemos que el equivalente, en la teoría de anillos, de los subgrupos normales son los ideales.

También, nos damos cuenta que podemos ver cada subgrupo normal de un grupo como el núcleo de algún homomorfismo y que todo núcleo de un homomorfismo de grupos es subgrupo normal.

Para los anillos tenemos la situación similar.

Lo anterior nos permite ver cada ideal como el núcleo de algún homomorfismo de anillos.

Por otro lado, si $h : A \rightarrow S$ es un homomorfismo de anillos, entonces $Ker(h)$ es un ideal de A.

En efecto, si $r_1, r_2 \in Ker(h)$,

$\Rightarrow \quad h(r_1 r_2) = h(r_1)h(r_2) = 0,$

luego $r_1\, r_2 \in Ker(h)$, obteniendo que h es subanillo.

Por otro lado, si $r \in A$ y $s \in Ker(h)$,

$\Rightarrow \quad h(rs) = h(r)h(s) = 0, \quad h(sr) = h(s)h(r) = 0$

decimos que $rs, sr \in Ker(h)$, es decir, $Ker(h)$ es ideal.

Teorema:

Sea I un ideal de $(A, +, \cdot)$. En el grupo cociente A/I se puede introducir una estructura única de anillo que hace que la proyección canónica sea un homomorfismo de anillos. Si A tiene unidad también la tendrá A/I.

Demostración

Sabemos que en A/I se puede introducir una estructura de grupo abeliano con las condiciones pedidas.

Para que la proyección canónica $\pi : A \longrightarrow A/I$ sea homomorfismo de anillos, la única definición posible de producto en A/I es:

$$\pi(a).\pi(b) = \pi(ab)$$

Si I es un ideal esta definición no depende de los representantes elegidos.

En efecto si:

$$\pi(a) = \pi(a') \Rightarrow \; a = a' + r, \quad r \in I$$
$$\pi(b) = \pi(b') \Rightarrow \; b = b' + s, \quad s \in I$$

De esto concluimos que $ab = a'b' + a's + rb' + rs$.

Entonces $\pi(ab) = \pi(a'b')$ puesto que $a's + rb' + rs \in I$.

2.9 Homomorfismo de anillos

Definición:

Dados $(A, +, \cdot)$ y $(A', +', \cdot')$ dos anillos, diremos que: $\varphi : A \xrightarrow{ds} A'$ es un homomorfismo de anillos si:

i) $\varphi(a + b) = \varphi(a) +' \varphi(b)$, $para\ todo\ a,\ b\ en\ A$.

ii) $\varphi(a.b) = \varphi(a) \cdot' \varphi(b)$, $para\ todo\ a, b\ en\ A$.

Observación:

De acuerdo a la condición *i*) todo homomorfismo de anillos es un homomorfismo de grupos; por lo tanto son válidos todos los resultados sobre homomorfismos de grupos.

Ejemplo 1:

Sean $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_m, +', \cdot')$ anillos y

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$$
$$z \longrightarrow \bar{z}$$

Veamos:

i) $\varphi(z_1 + z_2) = \overline{z_1 + z_2} = \overline{z_1} +' \overline{z_2} = \varphi(z_1) +' \varphi(z_2)$

ii) $\varphi(z_1 . z_2) = \overline{z_1 \cdot z_2} = \overline{z_1} \cdot' \overline{z_2} = \varphi(z_1) \cdot' \varphi(z_2)$

$\therefore$ φ es un homomorfismo.

Ejemplo 2:

Sea $M_{2\times 2}(\mathbb{R})$ y $B = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \ / \ a \in \mathbb{R} \right\}$

donde B es Subanillo.

$\varphi : B \longrightarrow \mathbb{R}$

$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \longrightarrow a$

Veamos:

$$i) \qquad \varphi\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} a+b & 0 \\ 0 & a+b \end{pmatrix}\right)$$
$$= a + b$$
$$= \varphi\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}\right)$$

$$ii) \qquad \varphi\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix}\right)$$
$$= a \cdot b$$
$$= \varphi\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right) \cdot \varphi\left(\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}\right)$$

$\therefore$ φ es un homomorfismo

Proposición:

Si $\varphi : (A, +, \cdot) \longrightarrow (S, +, \cdot)$ es un homomorfismo de anillos, entonces:

i) $\varphi(0) = 0$

ii) $\varphi(-a) = -\varphi(a) \quad para\ todo \quad a \in A.$

Demostración

i) En , se cumple,

$$a + 0 = a \ , \quad \forall \ a \in A$$
$$si \quad a = 0 : \quad 0 + 0 = 0$$

Aplicando ϕ , $\phi(0 + 0) = \phi(0)$

Se tiene, $\phi(0) + \phi(0) = \phi(0)$, ϕ es homomorfismo.

$\phi(0) \in S \ : \ \phi(0) = r \ , \ r + r = r \implies r = 0$

$\therefore \ \phi(0) = 0$

ii) Haciendo uso de i) :

$a \in A \ : \ \phi(a) \in S \ , \ \exists \ -\phi(a) \in S \ /$
$\phi(a) + [-\phi(a)] = 0 \in S$

$-\phi(a)$: inverso de $\phi(a)$.

Sumando,

$$\phi(a) + \phi(-a) = \phi[a + (-a)] = \phi(0) = 0$$

$\therefore \ \phi(-a)$ es también inverso de $\phi(a)$.

De la unicidad del mismo es:

$$\phi(-a) = -\phi(a)$$

El caso en que: $A = (A, +, \cdot, 1)$

$S = (S, +, \cdot, 1')$

No es cierto que,

$$\phi(1) = 1' \ \ldots\ldots \quad (*)$$

Sin embargo, si S es un Dominio de Integridad y ϕ es epiyectivo, entonces $(*)$ es cierto.

Proposición:

Sea $f : A \longrightarrow A'$ un homomorfismo de anillos, entonces se tienen las siguientes propiedades:

1) $f(0_A) = 0_{A'}$ *y* $f(-x) = -f(x)$, *donde* 0_A *y* $0_{A'}$ *son los elementos neutros de* A *y* A', *respectivamente, con respecto a la primera LCI.*
2) *Si S es un subanillo de A,* $f(S) = \{f(s) : s \in S\}$ *es un subanillo de* A'.
3) *Si* S' *es un subanillo de* A', $f^{-1}(S') = \{s \in A : f(s) \in S'\}$ *es un subanillo de A.*
4) *Si* I' *es un ideal de* A', $f^{-1}(I')$ *es un ideal de A.*
5) *Si f es sobreyectiva e I es un ideal de A,* $f(I)$ *es un ideal de* A'.
6) *Si A es un anillo con unidad* 1_A *y* f *es sobreyectiva, entonces* A' *es un anillo con unidad* $1_{A'} = f(1_A)$.

Demostración

1) Si $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A)$, entonces
$f(0_A) = 0_{A'}$ ya que el elemento neutro del grupo $(A', +)$ es único.
Si $f(0_A) = f(x + (-x)) = f(x) + f(-x)$,

entonces

$$f(x) + f(-x) = 0_{A'}.$$

Por tanto

$$f(-x) = -f(x).$$

2) Si S es un Subanillo de A, entonces $(S; +)$ es un subgrupo de $(A; +)$.
Como f es un homomorfismo entre grupos $(A, +)$ y $(A', +)$, entonces $(f(S), +)$ es un subgrupo de $(A', +)$.

Demostramos que el producto es una LCI en $f(S)$:

Sean $x;\ y\ \in S$, tenemos que

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

por ser un homomorfismo.
Como $x\ e\ y$ son elementos del subanillo S, entonces $x \cdot y\ \in\ S$, por lo tanto

$$f(x \cdot y) \in\ f(S).$$

Luego $f(S)$ es subanillo de A'.

3) Por la proposición de homomorfismo de grupos se tiene que, si S' es subgrupo de $(S';\ +)$, entonces $f^{-1}(S')$ es subgrupo de $(A;\ +)$.

Por lo tanto, para demostrar que $f^{-1}(S')$ es subanillo de A, sólo tenemos que demostrar que en $f^{-1}(S')$ el producto es una operación cerrada.

Para ello consideremos $x;\ y \in f^{-1}(S')$ entonces existen $x',\ y' \in\ S'$ tales que

$$f(x) =\ x'\ \ ,\ \ f(y) =\ y'\ .$$

Por lo tanto,

$$f(x).f(y) = f(x.y) = x'.y'\ \in\ S'\ ,$$

ya que S' es un Subanillo, así que $x.y \in f^{-1}(S')$

Esto significa que $f^{-1}(S')$ es Subanillo de A.

4) Hemos demostrado antes que la contraimagen de un subanillo de A' es un subanillo de A, así que solo queda demostrar que la contraimagen de un ideal cumple la propiedad de absorción con el producto.

Tomemos $x \in f^{-1}(I')$, por lo tanto existe $x' \in I'$ tal que

$$f(x) = x' .$$

Sea $a \in A$ tenemos que $f(a) \in A'$, entonces

$$f(a) . x' = f(a). f(x) \in I' ,$$

Ya que I' es un ideal de A' .

Como f es un homomorfismo, se tiene que

$$f(a). f(x) = f(a. x) \in I',$$

Por lo tanto $a. x \in f^{-1}(I')$, así que $f^{-1}(I')$ es un ideal de A.

5) Nuevamente, para demostrar que la imagen de un ideal I de A es un ideal de A' si f es sobreyectiva, basta demostrar que en $f(I)$ el producto cumple la propiedad de absorción.

Como f es sobreyectiva, entonces

$$\forall \ b \in A', \qquad \exists \ a \in A \quad tal\ que \quad f(a) = b .$$

Por lo tanto, $\forall \ y \in f(I), \quad \exists \ x \in I \quad tal\ que \quad y = f(x)$

Así que,

$$b. y = f(a). f(x) = f(a. x)$$

Como I es un ideal $a. x \in I$, así $f(a. x) \in f(I)$

Por lo que $f(I)$ es un ideal de A' .

6) Si $a' \in A'$, $\exists\ a \in A \quad tal\ que \quad a' = f(a)$

Por tanto

$$a'.f(1_A) = f(a).f(1_A) = f(a.1_A) = f(a) = a'$$

También $f(1_A).a' = a'$, lo que prueba que

$A' \quad = f(1_A)$.

2.10 Isomorfismo de anillos

Definición:

Un homomorfismo $\varphi : A \longrightarrow A'$ se dice que es:

i) Monomorfismo si y sólo si φ es inyectiva

ii) Epimorfismo si y sólo si φ es sobreyectiva

iii) Isomorfismo si y sólo si se cumple i) y ii).

Definición:

Sea $(A,+,\cdot)$ y $(A',+,\cdot)$ dos anillos. Un homomorfismo $\varphi : A \longrightarrow A'$, *el cual es biyectivo, se dice que es un* isomorfismo de anillo.

En tal caso, se dice que los anillos A y A' **son isomorfos** y lo simbolizamos por $A \approx A'$.

Ejemplo:

Se considera el anillo $A = \left\{ \begin{bmatrix} x & y \\ -y & x \end{bmatrix} : x, y \in \mathbb{R} \right\}$. Demostrar que es un isomorfismo entre anillos, la aplicación $f : \mathbb{C} \longrightarrow A$ dada por

$$f(x+iy) = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}.$$

Prueba

Para cualquier par de números complejos $x + iy,\ x' + iy'$:

$$f[(x+iy)+(x'+iy')] = f[(x+x')+(y+y')i] = \begin{bmatrix} x+x' & y+y' \\ -(y+y') & x+x' \end{bmatrix}$$
$$= \begin{bmatrix} x & y \\ -y & x \end{bmatrix} + \begin{bmatrix} x' & y' \\ -y' & x' \end{bmatrix} = f(x+iy) + f(x'+iy').$$

$$f[(x+iy).(x'+iy')] = f[(xx' - yy') + (xy' + yx')i]$$
$$= \begin{bmatrix} xx' - yy' & xy' + yx' \\ -(xy' + yx') & xx' - yy' \end{bmatrix} = \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \begin{bmatrix} x' & y' \\ -y' & x' \end{bmatrix}$$
$$= f(x+iy).f(x'+iy').$$

Concluimos que f es homomorfismo entre los anillos $\mathbb{C}\ y\ A$.

Su núcleo es:

$$kerf = \left\{ x+iy \in \mathbb{C} \ :\ f(x+iy) = \begin{bmatrix} x & y \\ -y & x \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\} = \{0+0i\} = \{0\},$$

Por tanto f es inyectiva.

Por último, cualquier elemento de A se puede expresar en la forma:

$$\begin{bmatrix} x & y \\ -y & x \end{bmatrix} = f(x+iy),$$

Es decir f es sobreyectiva.

Lo que demuestra que f es un isomorfismo entre los anillos $\mathbb{C}\ y\ A$.

Proposición:

Sea $f\ :\ A \longrightarrow B$ un homomorfismo de anillos.

Entonces $A/\ker(f)$ es isomorfo a $Im\ (f)$.

Teorema:

S*ea* $\varphi : A \longrightarrow S$ un homomorfismo de anillos sobreyectivo con $K = ker\,\varphi$, y supongamos que I es un ideal de A que contiene a K. Sea L el ideal de S, dado por $L = \varphi(I)$. Entonces

$$A/K \approx S/L$$

Aplicación didáctica

Sesion de aprendizaje

Nivel: Educación Superior Tiempo:50 min

I. OBJETIVOS

1.1 Objetivo general

- Define y caracteriza la estructura de anillo.

1.2 Objetivos especificos

- Define anillos, mostrando ejemplos.
- Reconoce los diferentes tipos de anillos, mostrando ejemplos.
- Determina subanillos.
- Establece homorfismo entre anillos.

II. ORGANIZACIÓN DE LOS APRENDIZAJES

CONCEPTOS	APRENDIZAJE(S) ESPERADOS	ACTITUDES
▪ Conceptos previos: estructura algebraica, LCI, monoide, semigrupo, grupos y subgrupos. ▪ Anillo: tipo de anillos, propiedades. ▪ Subanillo ▪ Homomorfismo.	**COMUNICACIÓN MATEMÁTICA:** ▪ Propone LCI. ▪ Explica las condiciones que definen una LCI, monoides y semigrupos y grupos . ▪ Define anillos y subanillos. RAZONAMIENTO Y DEMOSTRACIÓN ▪ Establece analogías entre semigrupos, grupos y anillos. ▪ Relaciona los conceptos de anillos y subanillos. ▪ Prueba las propiedades de los anillos. ▪ Prueba el homorfismo de los anillos.	▪ Muestra deseos de superación personal y profesional. ▪ Muestra rigurosidad en el manejo conceptual. ▪ Muestra perseverancia en la solución de la guía de práctica.

	RESOLUCIÓN DE PROBLEMAS ▪ Resuelve problemas aplicando los conceptos de anillos.	

III. SECUENCIA DIDÁCTICA

SITUACIONES DE APRENDIZAJE	ESTRATEGIAS	RECURSOS	EVALUACIÓN			TIEMPO
			Criterio	Indicadores	Instrumentos	
INICIO	▪ Presentación. ▪ Explica sobre la importancia de la estructura de anillos. ▪ Precisa los conceptos previos: LCI, monoide, semigrupo y grupo.	▪ Exposición oral. ▪ Equipo multimedia. ▪ PPT ▪ Pizarra, plumones y mota.	C.M.			10’
PROCESO	▪ Define un anillo presentando ejemplos y contraejemplos. ▪ Identifica clases de anillos, mostrando ejemplos. ▪ Define subanillos. Muestra ejemplos. ▪ Verifica homorfismos entre anillos.	▪ Exposición oral. ▪ Equipo multimedia. ▪ PPT ▪ Pizarra, plumones y mota.	C.M. R.D. R.P.			30’
SALIDA	▪ Resuelve la guía práctica.	▪ Guía práctica.	R.M. R.P.			10’

IV. REFERENCIAS

Fraleigh, J. (1987). Álgebra abstracta. México: Addison-wesley.

Herstein, I. (1985). Álgebra Moderna. México: Editorial Trillas.

Queysanne, M. (1989). Álgebra Básica. Buenos Aires: Talleres gráficos.

Rojo, A. (1985). Álgebra I. Buenos Aires: editorial atenea.

Trejo, C. (1969). Matemática elemental moderna. Estructura y método. Buenos Aires: Talleres gráficos.

Trujillo, F. y otros. (2014). Introducción a las estructuras algebraicas. Lima: UNE EGV.

GUÍA DE PRÁCTICA

1. Dado el anillo $(A, *, \circ)$, identifique si las siguientes afirmaciones son verdaderas o falsas. Explique sus respuestas
   a. $(A, *)$ es un grupo abeliano.
   b. $(A, \circ)$ es un semigrupo conmutativo.
   c. $(A, \circ)$ tiene elemento neutro.

2. Verifique si $(\mathbb{Q}, +, \cdot)$ es un anillo.

3. Explique por qué el anillo $(\mathcal{M}^{2x2}, +, \cdot)$ no es conmutativo.

4. Pruebe que $(2\mathbb{Z}, +, \cdot)$ es un subanillo de $(\mathbb{Z}, +, \cdot)$.

5. Identifique qué tipo de anillo es $(\mathbb{Z}_3, +, \cdot)$.

Síntesis

Estructura de anillo

Anillo

Definición:

Sean un conjunto no vacío A, y dos leyes de composición interna " $*$ " y " $\circ$ "; la terna $(A;\ *;\ \circ)$ es un **anillo**, si y solo si:

1. $(A;\ *)$ es un grupo abeliano
2. $(A;\ \circ)$ *es un semigrupo*
3. *La segunda LCI* $(\circ)$ *es distributiva respecto a la primera* $(*)$.

Identificando estas dos leyes de composición con las leyes aditiva (+) y multiplicativa ($\cdot$) respectivamente, podemos reformular esta definición, de la siguiente manera.

La terna $(A,\ +,\ \cdot)$ es un **anillo** si y solo si:

1. $(A;\ +)$ es un grupo abeliano
2. $(\mathrm{A};\ \cdot)$ es un semigrupo
3. El producto es distributivo respecto a la adición.

Tipos de anillos

Anillo conmutativo.-

Si además, la ley multiplicativa (·) es conmutativa, decimos que (A, +, ·) es un anillo conmutativo.

Anillo con unidad.-

Si existe elemento neutro o identidad respecto a la ley multiplicativa (·), entonces $(A, +, \cdot)$ se llama ***anillo con identidad*** o con unidad.

Es decir, se cumple que:

$$\forall\ a \in A, \qquad \exists\ 1 \in A\ /\ \ a \cdot 1 = 1 \cdot a = a$$

Propiedades de los anillos

Sea (A, +, ·) un anillo, y a, b, c elementos de A.

1) $Si\ a + b = a + c, entonces\ b = c$
2) $Si\ a + a = a,\ entonces\ a = 0$
3) $-(-a) = a$
4) $(-a)(-b) = ab$
5) $-(a + b) = -a - b$
6) $a \cdot 0 = 0 \cdot a = 0$
7) $a(-b) = (-a)b = -(ab)$

Si (A, +,·) es un anillo con identidad:

8) $(-1)a = -a \qquad \forall\ a \in A$
9) $(-1)(-1) = 1$

Anillo con divisores de cero

El anillo $(A,+,\cdot)$ tiene **divisores de cero**, si y solo si, elementos no nulos dan producto nulo. Es decir:

$$A\ tiene\ divisores\ de\ cero \Leftrightarrow \forall\, x,y:\ x \neq 0 \wedge\ y \neq 0 \Rightarrow x.y = 0$$

Anillo sin divisores de cero

El anillo $(A,+,\cdot)$ no tiene divisores de cero, si y solo si, elementos no nulos dan producto diferente de cero.

Dominio de integridad

Un anillo conmutativo con identidad que no posee divisores de cero se llama d**ominio de integridad**.

Característica de un anillo

Sea A un dominio de integridad: entonces, el menor entero positivo n (si existe) tal que $na = 0$ para todo $a \in A$ se llama la **característica** del anillo. Si no existe dicho entero, entonces se dice que A es de **característica** 0.

Subanillos

Sea $(A,+,\cdot)$ un anillo; un subconjunto $S \subset A$ es un **subanillo** de $(A,+,\cdot)$; si $(S,+,\cdot)$ es un anillo.

Ideales

Definición:

Sea A un anillo. Un subconjunto **I** de A se dice ideal a la derecha, si se tiene:

iii) $a + b \in I$, *para todo* $a, b \in I$

iv) $\gamma a \in I$, *para todo* $\gamma \in A$ *y* $a \in I$.

Definición:

Sea A un anillo. Un subconjunto I de A se dice ideal a la izquierda, si satisface

iii) $a + b \in I$, para todo $a, b \in I$

iv) $a\gamma \in I$, para todo $\gamma \in A$ y $a \in I$.

Definición:

Sea A un anillo. Un subconjunto I de R se dice ideal de A, si I es un ideal a la derecha y a la izquierda.

Definición:

Sea $(A, +, \cdot)$ un anillo. Un subanillo $I \subset A$ es un ideal de A, si para todo $r \in A$ y $m \in I$ se tiene que $rm, mr \in I$.

Anillo cociente

Si I es un ideal del anillo $(A, +, \cdot)$, al conjunto cociente formado por las clases laterales se le llama anillo cociente.

$$R/_I = \{a + I \mid a \in A\}$$

Donde el anillo A/I es el anillo cociente de A módulo I.

Homomorfismo de anillos

Dados $(A, +, \cdot)$ y $(A', +', \cdot')$ dos anillos, diremos que: $\varphi : A \xrightarrow{ds} A'$ es un homomorfismo de anillos si:

i) $\varphi(a+b) = \varphi(a) +' \varphi(b)$, para todo a, b en A.

ii) $\varphi(a.b) = \varphi(a) \cdot' \varphi(b)$, para todo a, b en A.

Isomorfismo de anillos

Un homomorfismo $\varphi : A \longrightarrow A'$ se dice que es:

i) Monomorfismo si y sólo si φ es inyectiva

ii) Epimorfismo si y sólo si φ es sobreyectiva

iii) Isomorfismo si y sólo si se cumple i) y ii).

Definición:

Sea $(A, +, \cdot)$ y $(A', +, \cdot)$ dos anillos. Un homomorfismo $\varphi : A \longrightarrow A'$, el cual es biyectivo, se dice que es un isomorfismo de anillo.

En tal caso, se dice que los anillos A y A' son isomorfos y lo simbolizamos por $A \approx A'$.

Apreciación crítica y sugerencias

Los anillos, así como las demás estructuras algebraicas, nos permiten comprender mejor los diferentes conjuntos, numéricos y de otro tipo, profundizando en la comprensión de sus propiedades al margen de la naturaleza de sus elementos.

El conocimiento que la mayoría tiene acerca de las operaciones con números enteros, es una gran ventaja para iniciar el estudio de los anillos, y así lograr una adecuada comprensión.

Sin embargo, es preocupante que dada la facilidad que existe para desarrollar estos temas en la educación básica, se deje de lado, pudiendo ser un tema motivante para los estudiantes, los que a la vez de desarrollar sus capacidades operativas podrían también desarrollar la capacidad para encontrar patrones, regularidades, y familiarizarse con las propiedades verificando de manera lúdica diversas LCI u operaciones que ellos mismos podrían proponer.

De igual manera, es necesario reiterar la preocupación respecto a que se revise la malla curricular de la Facultad, a fin de considerar cursos sobre estructuras algebraicas en la formación de los docentes de matemática de todos los programas y en todas las sedes.

Sistematizar las propiedades de las diferentes operaciones en los conjuntos numéricos N,Z,Q,R, asi como el conjunto de los polinomios, las matrices y las funciones, de manera progresiva desde la educación básica, y asi introducir la nocion de estructuras algebraicas de manera sencilla y comprensible.

Analizar las propiedades de las diversas operaciones (leyes de composición interna) cuando se desarrollan los “operadores”. Elaborar una secuencia didáctica incorporando casos extra matemáticos para ayudar a la comprensión de las diferentes estructuras matemáticas (no solo algebraicas).

Revisar la malla curricular de la facultad, para que todos los futuros docentes de los diversos programas lleven cursos que desarrollen las estructuras algebraicas y muchos otros que son fundamentales para mejorar nuestro desempeño profesional.

Concluciones

1. Una estructura algebraica es un conjunto de elementos provisto de una o más LCI que verifican una serie de propiedades, cada una de las cuales caracteriza una estructura distinta.

2. Las estructuras algebraicas se desarrollaron al tratar de encontrar fórmulas que contengan radicales y que sirvan para la resolución de ecuaciones de 5º o mayor grado, cuyos gestores fueron los matemáticos Evariste Galois y Niels H. Abel.

3. Un anillo es un conjunto no vacio, provisto de dos leyes de composición interna, donde con la primera ley, tiene una estructura de grupo abeliano y con la segunda tiene la estructura de semigrupo, además se verifica la ley distributiva a izquierda y derecha de la segunda ley respecto a la primera.

4. Si en dicho anillo, la segunda ley es conmutativa entonces se tiene un anillon conmutativo, y si en la segunda ley existe un elemento neutro es un anillo con unidad.

5. Se pueden definir diversas relaciones importantes entre semigrupos, grupos u otras estructuras, como las de homomorfismo.

6. Tanto en educación como en educación secundaria, la enseñanza de la matemática está centrada principalmente en los conjuntos numéricos $(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R})$ provistos de diversas operaciones, por lo que sería solo asunto de decisión de los maestros, el hecho de incorporar el conocimiento de las estructuras algebraicas, que dicho sea de paso es mucho más fácil de comprender cuando se realiza de manera progresiva.

Referencias

Fraleigh, J. (1987). Álgebra abstracta. México: Addison-wesley.

Herstein, I. (1985). Álgebra Moderna. México: Editorial Trillas.

Queysanne, M. (1989). Álgebra Básica. Buenos Aires: Talleres gráficos.

Rojo, A. (1985). Álgebra I. Buenos Aires: editorial atenea.

Trejo, C. (1969). Matemática elemental moderna. Estructura y método. Buenos Aires: Talleres gráficos.

Trujillo, F. y otros. (2014). Introducción a las estructuras algebraicas. Lima: UNE EGV.