Sebastián Castañeda Hernández
Ismael Gutiérrez García

Anillos y cuerpos

UNIVERSIDAD DEL NORTE
Editorial

ANILLOS Y CUERPOS

ANILLOS Y CUERPOS

Sebastián Castañeda Hernández
Ismael Gutiérrez García

Área metropolitana
de Barranquilla (Colombia), 2019

UNIVERSIDAD DEL NORTE
Editorial

Castañeda Hernández, Sebastián.
Anillos y cuerpos / Sebastián Castañeda Hernández, Ismael Gutiérrez García. – Barranquilla, Colombia: Editorial Universidad del Norte, 2019.

205 p. 28 cm
Incluye referencias bibliográficas (p. 201-202) e índice.
ISBN 978-958-789-098-3 (PDF)

1. Anillos (Álgebra). 2. Álgebra. 3. Polinomios I. Gutiérrez García, Ismael. II. Tít.

(512.4 C346 ed. 23) (CO-BrUNB)

UNIVERSIDAD DEL NORTE
Vigilada Mineducación
www.uninorte.edu.co
Km 5, vía a Puerto Colombia, A.A. 1569
Área metropolitana de Barranquilla (Colombia)

Coordinación editoral
Zoila Sotomayor O.

Diseño y diagramación
Ismael Gutiérrez García

Procesos técnicos
Munir Kharfan de los Reyes

Corrección de textos
Henry Stein

Diseño de portada
Joaquín Camargo Valle

Hecho en Colombia
Made in Colombia

A Elena y Matthias

LOS AUTORES

Ismael Gutierrez García

Doctor en Ciencias Naturales de la Universidad Johannes Gutenberg de Mainz (Alemania). Magíster en Matemáticas de la Universidad del Valle (Colombia) y licenciado en Matemáticas y Física de la Universidad del Atlántico (Colombia). Está vinculado a la Universidad del Norte (Colombia) como profesor titular del departamento de Matemáticas y Estadística. Posee una amplia experiencia como docente universitario y además ha liderado proyectos de investigación en el área de matemáticas discretas y sus aplicaciones, concretamente en teoría clásica de códigos y en códigos de subespacios. Es autor del libro *Matemáticas para informática*, y coautor de *Álgebra lineal* y *Matemáticas básicas con trigonometría*.

Sebastián Castañeda Hernández

Magíster en Ciencias matemáticas de la Universidad del Valle, en convenio con la Universidad del Norte (Colombia). Licenciado en Matemáticas de la Universidad del Atlántico (Colombia). Es profesor del departamento de Matemáticas y Estadística de la Universidad del Norte (Colombia) desde 1988. Es autor de los libros *Matemáticas fundamentales para estudiantes de ciencias* y *Curso básico de teoría de números*, y coautor del *Manual de álgebra lineal*.

ÍNDICE GENERAL

PRÓLOGO

En el presente texto, diseñado inicialmente para estudiantes no graduados en Matemáticas, se consideran dos partes importantes del álgebra: una introducción a los resultados básicos de la teoría de anillos y los primeros elementos de la teoría de extensiones de cuerpos con característica cero o característica prima.

En el primer capítulo se presenta la definición de anillo y un gran número de ejemplos inspirados en el álgebra lineal, el cálculo diferencial y la teoría de grupos. Seguidamente se consideran subestructuras especiales: los subanillos y los ideales. Estos últimos juegan el mismo papel que los subgrupos normales, son los necesarios para construir la estructura cociente de un anillo. Posteriormente se presentan unos resultados elementales sobre anillos de ideales principales, anillos noetherianos y anillos euclidianos.

El segundo capítulo está dedicado a funciones entre anillos que preservan la estructura: los homomorfismos de anillos. Los resultados relevantes que se presentan son los tres teoremas de isomorfía y la construcción del cuerpo cociente de un dominio entero, con la conocida propiedad universal.

En el capítulo tres se presentan definiciones y caracterizaciones de ideales maximales e ideales primos. Especialmente se indagan condiciones que permitan establecer relaciones entre estos. Seguidamente consideramos el concepto de elemento e ideal nilpotente. Nuevamente se consideran ejemplos importantes para fijar los diferentes resultados.

El cuarto y último capítulo de esta primera parte está dedicado al estudio de cier-tas propiedades de los anillos conmutativos. Concretamente se presentan resultados sobre divisibilidad, elementos primos y elementos irreducibles y las relaciones entre estos conceptos. Luego presentamos los anillos de factorización única y el anillo de polinomios con coeficientes en esta clase de anillos.

El segundo tema de este libro lo constituyen las extensiones de cuerpos. En el capítulo quinto se muestran resultados básicos sobre extensiones, por ejemplo, la fórmula del grado. Seguidamente se describen la extensiones algebraicas y se demuestra la existencia y unicidad de la clausura algebraica de un cuerpo. Posteriormente se presenta el cuerpo de descomposición de un polinomio con coeficientes en un cuerpo, así como los resultados más importantes sobre extensiones normales, separables y de Galois. Para finalizar este capítulo se demuestra el teorema fundamental de la teoría de Galois acompañado de un considerable número de ejemplos.

En el capítulo sexto se presenta de manera sucinta los cuerpos finitos. Esta parte está inspirada en la necesidad de este tipo de estructuras para el estudio de estructuras discretas, y en especial la teoría de códigos de bloques o códigos con la métrica del rango.

El capítulo final del libro está dedicado a la construcción con regla y compás y especialmente a presentar tres problemas clásicos: la duplicación del cubo, la cuadratura del círculo y la trisección de un ángulo. Al final del texto se presenta un pequeño anexo sobre el anillo de los polinomios en una indeterminada.

De antemano damos gracias a los lectores por cualquier sugerencia que conduzca a mejorar la presente propuesta, la cual es fruto de los cursos dictados por los autores a lo largo de los últimos diez años, tanto en la carrera de Matemáticas como en la maestría en Matemáticas de la Universidad del Norte.

Parte I

Anillos

CAPÍTULO 1

GENERALIDADES SOBRE ANILLOS

1.1 Definiciones y propiedades básicas

1.1.1 Definición. Un conjunto no vacío R sobre el cual están definidas dos operaciones binarias " $+$ " (suma) y " $\cdot$ " (multiplicación) se denomina un `anillo` si se satisfacen las siguientes propiedades:

(1) Para todo $x, y, z \in R \;\; x + (y + z) = (x + y) + z$.

(2) Existe un elemento $0 \in R$ tal que para todo $x \in R \;\; 0 + x = x$.

(3) Para todo $x \in R$ existe $y \in R$ tal que $y + x = 0$.

(4) Para todo $x, y \in R \;\; x + y = y + x$.

(5) Para todo $x, y, z \in R \;\; x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

(6) Para todo $x, y, z \in R \;\; x(y + z) = xy + xz$ y $(y + z)x = yx + zx$.

1.1.2 Observaciones. Los axiomas del (1) al (4) de la definición anterior indican que $(R, +)$ es un grupo abeliano con elemento neutro 0_R o simplemente 0, si no hay lugar a confusión (llamado `cero` o elemento `nulo` de R), el axioma (5) dice que $(R, \cdot)$ es un semigrupo. Si R admite un elemento neutro para la multiplicación (un uno), entonces $(R, \cdot)$ es un semigrupo con `elemento identidad` o simplemente un semigrupo con `uno` y finalmente el axioma (6) establece que la multiplicación distribuye con respecto a la adición. En adelante, en lugar de $x \cdot y$ escribimos simplemente xy.

1.1.3 Observaciones. Sea R un anillo. Escribimos $-x$ para referirnos al único inverso de un elemento x en el grupo aditivo de R. Si R tiene elemento identidad, entonces este se nota con 1_R o simplemente con 1. Si un elemento $x \in R$ es invertible multiplicativamente notaremos por x^{-1} a su único inverso.

1.1.4 Definición. Sea R un anillo.

(1) Decimos que R es `conmutativo` si para todo $x, y \in R$ se verifica que $x \cdot y = y \cdot x$.

(2) $0 \neq a \in R$ se denomina un `divisor de cero` si existe $0 \neq b \in R$ tal que $ab = 0$ o $ba = 0$.

(3) Si R es conmutativo y no tiene divisores de cero, entonces R se llama un `dominio entero`.

(4) $a \in R$ se llama `invertible`, o una `unidad` si existe $b \in R$ tal que $ab = ba = 1$. El conjunto de todas las unidades de R lo notamos con $U(R)$ o también con $R^\times$.

(5) Si todo elemento no nulo de R es invertible, entonces se dice que R es un `anillo con división`. Claramente, si R es un anillo con división, entonces $|R|$, la cardinalidad de R, es mayor o igual a dos.

(6) Si R es un anillo conmutativo con división, entonces R se denomina un `cuerpo` o un `campo`.

1.1.5 Observación. Si R es una anillo con identidad y tiene al menos dos elementos, claramente $1 \neq 0$ ya que si $1 = 0$ se tendría para todo $x \in R$ que

$$x = x1 = x0 = 0$$

lo que implicaría que $R = \{0\}$.

1.1.6 Ejemplo. Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_p$ (p primo) con las sumas y multiplicaciones usuales son anillos conmutativos. En particular $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_p$ son cuerpos.

1.1.7 Ejemplo. Sean $n \in \mathbb{N}$ con $n \geq 2$ y R un anillo. El conjunto de todas las matrices de tamaño $n \times n$ con entradas en R es un anillo no conmutativo. Este es denotado en lo que sigue con $\mathrm{Mat}(n, R)$. En particular, en $\mathrm{Mat}(n, \mathbb{R})$ existen divisores de cero. Consideremos por ejemplo:

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{y} \quad b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Note que $a \neq 0$ y $b \neq 0$ y, sin embargo, $ab = 0$.

1.1.8 Ejemplo. Sea $n \in \mathbb{N}$. El conjunto $\mathbb{Z}_n$ de las clases residuales módulo n con las operaciones usuales es un anillo conmutativo. Si $n = ab$ con $a, b \neq 1$, entonces $\mathbb{Z}_n$ no es un dominio entero, ya que $[a][b] = [n] = [0]$, sin embargo $[a] \neq [0]$ y $[b] \neq [0]$.

1.1.9 Ejemplo. Si $(G, +)$ es un grupo abeliano, entonces $\mathrm{End}(G)$ es un grupo abeliano con respecto a la suma definida por:

$$(\alpha + \beta)(g) := \alpha(g) + \beta(g),$$

para todo $g \in G$. Si consideramos sobre $\mathrm{End}(G)$ la composición de funciones como la multiplicación, se verifica que $\mathrm{End}(G)$ es un anillo.

1.1.10 Ejemplo. Sean $X \neq \varnothing$ y R un anillo. El conjunto $\mathrm{Fun}(X, R)$ de todas las funciones $f : X \longrightarrow R$ con las operaciones usuales (puntuales)

$$(f + g)(x) = f(x) + g(x)$$
$$(f \cdot g)(x) = f(x) \cdot g(x),$$

para todo $f, g \in \mathrm{Fun}(X, R)$ y todo $x \in X$, es un anillo. Si R es conmutativo, entonces $\mathrm{Fun}(X, R)$ también lo es.

Como caso particular, $R = \mathrm{Fun}([a, b], \mathbb{R})$ es un anillo conmutativo con elemento identidad $f(x) = 1$ para todo $x \in [a, b]$. R no es un dominio entero. En efecto, consideremos las funciones no nulas

$$f(x) = \begin{cases} \frac{1}{2} - x, & \text{si } 0 \leq x < \frac{1}{2} \\ 0, & \text{si } \frac{1}{2} \leq x \leq 1 \end{cases}$$

$$g(x) = \begin{cases} 0, & \text{si } 0 \leq x < \frac{1}{2} \\ x - \frac{1}{2}, & \text{si } \frac{1}{2} \leq x \leq 1 \end{cases}$$

Note que $f(x)g(x) = 0$, $\forall x \in [0, 1]$ y ni f ni g son la función nula.

1.1.11 Ejemplo. El conjunto $\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}$ con las operaciones usuales entre números complejos es un anillo conmutativo, denominado el anillo de los `números Gaussianos`. Es claro que $\mathbb{Z}[\mathrm{i}]$ es conmutativo y sin divisores de cero. No obstante, note que

$$(1 - \mathrm{i})^{-1} = \tfrac{1}{2} + \tfrac{1}{2}\mathrm{i} \notin \mathbb{Z}[\mathrm{i}].$$

Por lo tanto, $\mathbb{Z}[\mathrm{i}]$ no es un cuerpo.

1.1.12 Ejemplo. Si $R_1, \ldots, R_n$ son anillos, entonces el producto cartesiano

$$R := R_1 \times \cdots \times R_n$$

también lo es con respecto a las siguientes operaciones:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 + b_1, \ldots, a_n + b_n)$$

y

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) := (a_1 b_1, \ldots, a_n b_n).$$

1.1.13 Ejemplo. Sea R un anillo y notemos con $R[[x]]$ el conjunto de todas las `series de potencias` en la indeterminada x con coeficientes en R. Esto es:

$$R[[x]] := \left\{ \sum_{j=0}^{\infty} c_j x^j \mid c_j \in R \right\}.$$

Para dos series de potencias $f = \sum_{j=0}^{\infty} a_j x^j$ y $g = \sum_{j=0}^{\infty} b_j x^j$ definimos

$$f = g \Leftrightarrow a_j = b_j, \quad \forall j \in \mathbb{N}_0$$
$$f + g = \sum_{j=0}^{\infty} (a_j + b_j) x^j$$
$$f \cdot g = \sum_{j=0}^{\infty} \Big(\sum_{i+k=j} a_i b_k \Big) x^j.$$

Se deja como ejercicio verificar que $R[[x]]$ es un anillo. Si R es conmutativo, entonces $R[[x]]$ también lo es.

1.1.14 Ejemplo. Sea R un anillo y notemos con $R[x]$ el conjunto de todos los `polinomios` en la indeterminada x con coeficientes en R. Esto es:

$$R[x] := \left\{ \sum_{j=0}^{m} c_j x^j \mid m \in \mathbb{N}_0,\ c_j \in R \right\}.$$

Para dos polinomios $f = \sum_{j=0}^{m} a_j x^j$ y $g = \sum_{j=0}^{n} b_j x^j$ definimos

$$f = g \Leftrightarrow m = n \ \wedge \ a_j = b_j, \quad \forall j$$
$$f + g = \sum_{j=0}^{\max\{m,n\}} (a_j + b_j) x^j$$
$$f \cdot g = \sum_{j=0}^{mn} \Big(\sum_{i+k=j} a_i b_k \Big) x^j.$$

Se deja como ejercicio verificar que $R[x]$ es un anillo. Si R es conmutativo, entonces $R[x]$ también lo es.

1.1.15 Ejemplo. (`Los cuaterniones de Hamilton`) Sea $\mathbb{H} \subseteq \mathrm{Mat}(2,\mathbb{C})$ definido por

$$\mathbb{H} := \left\{ \begin{pmatrix} z & -\overline{w} \\ w & \overline{z} \end{pmatrix} \middle| \; z, w \in \mathbb{C} \right\},$$

donde $\overline{z}$ y $\overline{w}$ denotan respectivamente los complejos conjugados de z y w. Si $z = a + b\mathrm{i}$ y $w = c + d\mathrm{i}$ con $a, b, c, d \in \mathbb{R}$, entonces

$$\begin{pmatrix} z & -\overline{w} \\ w & \overline{z} \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix} + c \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}.$$

Si definimos

$$1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \imath := \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix},\ \jmath := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ k := \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix},$$

entonces cada elemento de $\mathbb{H}$ puede expresarse en la forma

$$a1 + b\imath + c\jmath + dk,$$

con $a, b, c, d \in \mathbb{R}$. Se puede verificar sin dificultades los resultados de la siguiente tabla,

$\cdot$	1	$\imath$	$\jmath$	k
1	1	$\imath$	$\jmath$	k
$\imath$	$\imath$	-1	k	$-\jmath$
$\jmath$	$\jmath$	$-k$	-1	$\imath$
k	k	$\jmath$	$-\imath$	-1

en la cual se puede también observar que $\mathbb{H}$ es un anillo no conmutativo. Por otro lado, si para $z = a1 + b\imath + c\jmath + dk$, definimos $\overline{z} = a1 - b\imath - c\jmath - dk$, entonces se tiene que

$$z\overline{z} = \overline{z}z = (a^2 + b^2 + c^2 + d^2) \cdot 1.$$

En consecuencia, si $z \neq 0$, se tiene que

$$z^{-1} = \frac{\overline{z}}{z\overline{z}}.$$

Por lo tanto, $\mathbb{H}$ es un anillo con división, no conmutativo.

1.1.16 Ejemplos. Algunas unidades.

(1) $U(\mathbb{Z}) = \{1, -1\}$,

(2) $U(\mathbb{Z}_6) = \{[1], [5]\}$,

(3) $U(\mathbb{Z}_7) = \{[1],[2],[3],[4],[5],[6]\}$,

(4) Si $R = \mathrm{Mat}(n,K)$, entonces $U(R) = \mathrm{GL}(n,K)$.

El siguiente teorema presenta algunos resultados básicos sobre anillos. Como es usual, al decir que R es un anillo nos referimos no solamente al conjunto, sino a la estructura formada por el conjunto y las dos operaciones.

1.1.17 Teorema. Sea R un anillo.

(1) Para todo $x \in R$ se tiene $x0_R = 0_R x = 0_R$.

(2) Si $x, y \in R$, entonces:

$$-(-x) = x \tag{1.1}$$
$$-(x+y) = -x + (-y) \tag{1.2}$$
$$x(-y) = (-x)y = -(xy) \tag{1.3}$$
$$(-x)(-y) = xy \tag{1.4}$$

Demostración. (1) Se deja como ejercicio.

(2) Las propiedades (1.1) y (1.2) son casos particulares de

$$(x^{-1})^{-1} = x \quad \text{y} \quad (xy)^{-1} = y^{-1}x^{-1},$$

las cuales son válidas en un monoide para elementos invertibles, x e y. En particular, son válidas para la estructura multiplicativa de un anillo con identidad y elementos no singulares x, y (ver, por ejemplo, [3], teorema 2.1.1, página 50). □

De igual manera se tiene que $U(R)$, el conjunto de las unidades en un anillo con identidad, es un grupo multiplicativo, ya que en todo monoide el conjunto de los elementos invertibles lo es.

Similar como en los grupos, si R es un anillo podemos definir potencias enteras nx de un elemento x en el grupo aditivo $(R,+)$.

1.1.18 Definición. Sean R un anillo, $x \in R$ y $n \in \mathbb{Z}$. Definimos

$$nx = \begin{cases} 0_R, & \text{si } n = 0; \\ (n-1)x + x, & \text{si } n > 0; \\ -((-n)x), & \text{si } n < 0. \end{cases} \tag{1.5}$$

La notación x^n se utiliza para potencias multiplicativas con $n > 0$. Así tenemos

$$x^n = \begin{cases} x & \text{si } n = 1; \\ x^{n-1}x, & \text{si } n > 1. \end{cases} \tag{1.6}$$

Las propiedades de la potenciación entera en grupos y en grupos abelianos adoptan entonces las siguientes formas específicas en la estructura aditiva de grupo abeliano de un anillo R.

1.1.19 Teorema. Sean R un anillo, $x, y \in R$ y $n, m \in \mathbb{Z}$. Entonces:

$$m(nx) = (mn)x = n(mx) \tag{1.7}$$
$$mx + nx = (n+m)x \tag{1.8}$$
$$n(x+y) = nx + ny \tag{1.9}$$
$$(nx)y = x(ny) = n(xy) \tag{1.10}$$
$$(nx)(my) = (nm)(xy) \tag{1.11}$$

Demostración. Es claro que (1.11) es consecuencia de (1.10). Demostremos esta última inicialmente para $n \geq 0$, utilizando inducción.

El caso $n = 0$ es trivial. Supongamos entonces que los resultados son válidos para un cardinal n. Tenemos entonces:

$$\begin{aligned} ((n+1)x)y &= (nx+x)y \\ &= (nx)y + (xy) \\ &= n(xy) + (xy) \\ &= (n+1)(xy). \end{aligned}$$

También

$$\begin{aligned} ((n+1)x)y &= (nx)y + (xy) \\ &= x(ny) + xy \\ &= x(ny+y) \\ &= x((n+1)y), \end{aligned}$$

lo que concluye la demostración para el caso $n \geq 0$. Si $n < 0$, tenemos

$$\begin{aligned} (nx)y &= (-((-n)x))y \\ &= -(((-n)x)y) \\ &= -(x((-n)y)) \\ &= x(-((-n)y)) \\ &= x(ny). \end{aligned}$$

De manera similar, para el caso $n < 0$, se demuestra $(nx)y = n(xy)$.

El resto se deja como ejercicio. □