

UNIDAD 2: ANILLOS

En la unidad precedente se han tratado diversos aspectos de la *teoría de grupos*. Uno de los primeros ejemplos, fue \mathbb{Z} con la operación *suma*. Sin embargo en \mathbb{Z} hay otra operación, el *producto*. (\mathbb{Z}, \cdot) no es grupo, pues elementos como 2,3 y 4 carecen de inversos multiplicativos dentro de \mathbb{Z} ($\frac{1}{2}, \frac{1}{3}, \frac{1}{4}$ pertenecen a \mathbb{Q} y no a \mathbb{Z}); pero el producto no está desprovisto de propiedades: es asociativo, conmutativo, tiene a 1 como elemento identidad y está relacionado con la suma mediante la propiedad distributiva; de hecho es la interrelación entre la suma y el producto lo que le da a \mathbb{Z} su riqueza de propiedades. Esta situación de un conjunto con dos operaciones de propiedades paralelas a las de la suma y el producto en \mathbb{Z} surge muy frecuentemente en *matemática*, y la importancia de sus ejemplos da lugar al concepto abstracto de **anillo**.

Con el agregado de una ley de composición interna sujeta a ciertas condiciones, se enriquece la estructura de *grupo abeliano* y la terna así obtenida, constituye otro *sistema axiomático*. Se definirán aquí, la estructura de **anillo** y el caso particular de **cuerpo**. Lo mismo que en el caso de la estructura de *grupo*, se estudian sus propiedades básicas y se introduce el concepto de *ideal*.

Comentarios históricos

Al igual que sucedió con el concepto abstracto de *grupo*, la idea de *anillo* tuvo su definición abstracta a comienzos del siglo XX; con ella se pretendía englobar las propiedades de las numerosas estructuras que habían aparecido en el siglo XIX: *cuaterniones, matrices,...* y otras más antiguas como los *números enteros* y los *polinomios*.

Un gran impulsor de esta teoría fue el matemático alemán *Ernst Eduard Kummer* (1810-1893) y el causante indirecto de ello fue *Pierre de Fermat*.

La conjetura, recientemente demostrada, conocida actualmente con el nombre de *El último teorema de Fermat*, dice que es imposible encontrar números enteros positivos x, y, z tales que $x^n + y^n = z^n$ si $n > 2$.

A *Pierre de Fermat* se le atribuye la demostración para $n = 4$, porque la esbozó en una de sus cartas, por un método que se conoce con el nombre de *método del descenso infinito*.

Este método consiste en suponer que $x^4 + y^4 = z^4$ tiene una solución entera x_0, y_0, z_0 y fabricar otra $(x_1)^4 + (y_1)^4 = (z_1)^4$ en la que z_1 es menor que z_0 ; aplicando repetidas veces, pero una cantidad finita, este proceso, se llega a que 1 es una suma de cuartas potencias de números positivos, lo que es contrario a la lógica.

Leonhard Euler (1707-1783) demostró el resultado conjeturado por *Fermat* para $n=3$. En 1823, *Adrien-Marie Legendre* (1752-1833) lo probó para $n = 5$. En 1832, *Peter Gustav Lejeune Dirichlet* (1805-1859) lo probó para $n = 14$ después de intentarlo sin éxito para $n = 7$.

A pesar de todos estos esfuerzos nadie había logrado inventar una vía que permitiera vislumbrar la posibilidad de probar el resultado para todos los valores de n . Fueron los trabajos de *Ernst Eduard Kummer* los que permitieron alumbrar esperanzas.

La idea es escribir $x^n = z^n - y^n$ y factorizar la parte derecha de esta ecuación. Como había hecho *Euler* para $n = 3$, si $\xi = e^{\frac{2\pi i}{n}}$ es una raíz n -ésima de la unidad, podemos escribir

$$x^n = z^n - y^n = (z - y)(z - \xi y)(z - \xi^2 y) \dots (z - \xi^{n-1} y)$$

Kummer hizo uso del anillo $\mathbb{Z}[\xi]$, que es el menor anillo contenido en el cuerpo de los números complejos y que contiene a todos los números enteros y a los elementos $1, \xi, \xi^2, \dots, \xi^{n-1}$, para demostrar el *último teorema de Fermat*. En el proceso necesitó estudiar la *unidad de la factorización* de estos anillos en *elementos irreducibles*, encontrando que no era cierto en general: para $n = 23$ el anillo anterior no es un *dominio de factorización única*.

Kummer trató de solucionar este escollo que le impedía demostrar el ansiado teorema. Para ello inventó lo que él llamó *números ideales*, precursores de la noción de *ideal* de un anillo. En sus trabajos, *Kummer*, logró demostrar que la conjetura de *Fermat* es cierta para infinitos *primos* que llamó *regulares*, de los cuales solamente 37, 59 y 67 no lo son entre los primos menores que 100.

Ernst Eduard Kummer comenzó a estudiar en la Universidad de Halle en 1828 la carrera de *teología*, pero rápidamente se cambió a las *matemáticas*; sus estudios los realizó de manera brillante ya que en 1831 la universidad le concedió el doctorado por uno de sus trabajos sobre series de senos y cosenos. Desde 1832 a 1842 enseñó matemática en un colegio de Liegnitz (actualmente en Polonia), desde 1842 hasta 1855 trabajó en la Universidad de Breslau y a partir de 1855 fue Profesor en la Universidad de Berlín. Aunque no fue capaz de demostrar el *último teorema de Fermat*, la Academia Francesa retiró el premio que había establecido para

quien lo demostrara y concedió a *Kummer* la Gran Medalla de la Academia, en reconocimiento de su esfuerzo para avanzar en la demostración.

Los trabajos de Kummer fueron continuados por el matemático alemán *Julius Wilhelm Richard Dedekind* (1831-1916) quien introdujo la noción de *ideal* tal como nosotros la expondremos, pero sólo para los anillos $\mathbb{Z}[\xi]$, y fue capaz de construir una teoría que contenía los trabajos de *Kummer* sobre los números ideales.

La teoría abstracta de anillos es un producto del siglo XX. *David Hilbert* (1862-1943) fue quien primero usó la palabra *anillo*. El trabajo de sistematizar todos los resultados conocidos sobre anillos e ideales particulares y de incluirlos todos ellos en una teoría abstracta lo realizó la matemática alemana *Amalie (Emmy) Noether* (1882-1935), quien durante gran parte de su vida tuvo que luchar contra la prohibición de admitir profesoras en las universidades alemanas; finalmente, después de haberle concedido una plaza de *profesor asociado no oficial*, fue nombrada Profesora en la Universidad de Göttingen en 1922.

Definiciones

- Un **anillo** es un conjunto no vacío R con dos operaciones, $+$ y \cdot , tal que:

1. $(R, +)$ es grupo abeliano
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in R$
3. $a \cdot (b + c) = a \cdot b + a \cdot c, \forall a, b, c \in R$
 $(a + b) \cdot c = a \cdot c + b \cdot c, \forall a, b, c \in R$

- Si

$$a \cdot b = b \cdot a, \forall a, b \in R,$$

R se dice **anillo conmutativo**.

- Si R contiene $1_R \in R$ tal que

$$1_R \cdot a = a \cdot 1_R = a, \forall a \in R,$$

R se dice **anillo con identidad**.

- Un elemento no nulo se dice **divisor de cero** a izquierda (*a derecha*) si $\exists b \in R, b \neq 0$ tal que $a \cdot b = 0$ ($b \cdot a = 0$).

- Sea R anillo con identidad, $a \in R$ se dice **invertible a izquierda** (*a derecha*) si $\exists c \in R : c \cdot a = 1_R$ ($a \cdot c = 1_R$).

Un elemento $a \in R$ que es invertible a izquierda y a derecha, se dice, simplemente, **invertible** o **unidad**.

- **Dominio de integridad (o dominio íntegro, o dominio entero):** es un anillo conmutativo con identidad $1_R \neq 0$ y sin divisores de cero.
- **Anillo de división:** es un anillo D con identidad $1_D \neq 0$, en el cual, cualquier elemento no nulo es unidad.
- **Cuerpo:** es un anillo de división conmutativo.

Ejemplos

1. \mathbb{Z} es dominio de integridad. (Ejercicio)
2. $2\mathbb{Z}$ es anillo conmutativo sin identidad. (Ejercicio)
3. $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ son cuerpos. (Ejercicio)
4. $M(n, \mathbb{K})$ con $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ o \mathbb{C} , es anillo con identidad ($\neq 0$). ¿Quiénes son las unidades? (Ejercicio)
5. $M(2, \mathbb{Z}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_2 \right\}$ ¿Qué es? (Ejercicio)
6. \mathbb{Z}_m es anillo conmutativo, $\forall m$. (Ejercicio)
 \mathbb{Z}_p es cuerpo, $\forall p$ primo. (Ejercicio)
7. **Los cuaterniones reales**

Sea $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ grupo. Elegimos símbolos $1, i, j, k$ de modo que identificamos

$$(a_0, a_1, a_2, a_3) \longleftrightarrow a_0 1 + a_1 i + a_2 j + a_3 k$$

y convenimos

$$a_0 1 \longleftrightarrow a_0$$

Sea $Q = \{a_0 1 + a_1 i + a_2 j + a_3 k / a_i \in \mathbb{R}, i = 0, 1, 2, 3\}$. Se define la *multiplicación* por la multiplicación de sumas formales término a término, sujeta a:

- (a) la *asociatividad*, y
- (b) las relaciones

$$\begin{aligned} i^2 &= j^2 = k^2 = -1 \\ ri &= ir, rj = jr, rk = kr \text{ para } r \in \mathbb{R} \\ ij &= -ji = k \\ ki &= -ik = j \\ jk &= -kj = i \end{aligned}$$

Q es un anillo de división, llamado **los cuaterniones reales**.

(Ejercicio)

Definición

Sean R y S anillos. $f : R \rightarrow S$ es un **homomorfismo de anillos** si:

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

(Ejercicio: definir *monomorfismo*, *epimorfismo*, *isomorfismo*, *endomorfismo*, *automorfismo*.)

Ejemplos

1. Sean R y S anillos. $f : R \rightarrow S$ es monomorfismo de anillos $\Leftrightarrow \ker f = \{0_R\}$ donde $\ker f = \{x \in R / f(x) = 0_S\}$.
(Ejercicio)
2. La función

$$\pi : \mathbb{Z} \rightarrow \mathbb{Z}_m / x \mapsto \bar{x}$$

es un epimorfismo de anillos.

3. La función

$$\phi : \mathbb{Z} \rightarrow \mathbb{R}/m \mapsto m \cdot 1_R$$

es un homomorfismo de anillos.

Definición

Sea R anillo, R se dice de **característica** \tilde{n} , si \tilde{n} es el menor de los n naturales, tales que $n \cdot a = 0, \forall a \in R$. Si tal n no existe, R se dice de *característica cero*.

Ejemplos

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ son de característica cero.
- \mathbb{Z}_m es de característica m .

Definición

Sea R un anillo, $\emptyset \neq S \subset R$ cerrado por la suma y la multiplicación. Si S es él mismo un anillo con esas operaciones, entonces S es un **subanillo**.

Definición

Un subanillo I , de R , es un **ideal a izquierda** si

$$r \in R, x \in I \Rightarrow r \cdot x \in I,$$

y es un **ideal a derecha** si

$$r \in R, x \in I \Rightarrow x \cdot r \in I.$$

Un **ideal bilátero** es un ideal a izquierda y a derecha.

Un ideal se dice **propio** si $I \neq \{0\}$ e $I \neq R$

Ejemplos

1. $\{0\}$ y R son ideales de cualquier anillo. (Ejercicio)
2. El **centro de un anillo** R ,

$$Z(R) = \{x \in R : x \cdot y = y \cdot x, \forall y \in R\}$$

es un subanillo pero no, necesariamente, un ideal. (Ejercicio)

Proposición

$\emptyset \neq I \subset R$ es ideal a izquierda (*derecha*) sii $\forall a, b \in I, r \in R$:

1. $a - b \in I$
2. $r \cdot a \in I$ ($a \cdot r \in I$)

Dem.: (Ejercicio)

Corolario

Si $\{A_i\}_{i \in I}$ es una familia de ideales a izquierda (*derecha*), entonces $\bigcap_{i \in I} A_i$ es ideal a izquierda (*derecha*).

Dem.: (Ejercicio)

Definición

Sea R anillo y $X \subset R$. El **ideal a izquierda (*derecha*) generado por X** es:

$$(X) = \bigcap_{i \in I} A_i \text{ donde } A_i \text{ es ideal a izquierda (*derecha*)/} X \subset A_i, \forall i \in I.$$

Los elementos de X se llaman **generadores** de (X) .

Si $|X| < \infty$, entonces (X) se dice **finitamente generado**.

Un **ideal** se dice **principal** si está generado por un solo elemento.

Un **anillo a ideales principales** es un anillo en el cual todo ideal es principal.

Proposición

Sea R un anillo conmutativo con identidad y $X \subset R$. Entonces,

$$(X) = \{r_1 \cdot x_1 + r_2 \cdot x_2 + \dots + r_n \cdot x_n : r_i \in R, x_i \in X, n \in \mathbb{N}\}$$

Dem.: (No la haremos).

Teorema

Sea R anillo e $I \subset R$, un ideal de R . Entonces,

$$\frac{R}{I} = \{a + I : a \in R\}$$

es un anillo con las siguientes operaciones:

- *Suma:* $(a + I) + (b + I) = (a + b) + I$
- *Multiplicación:* $(a + I) \cdot (b + I) = (a \cdot b) + I$

$\frac{R}{I}$ se llama **anillo cociente**.

Dem.:

Asumamos que las operaciones están bien definidas.

- Asociatividad de la multiplicación:

Sean $r + I, s + I, t + I \in \frac{R}{I}$

$$[(r + I) \cdot (s + I)] \cdot (t + I) = (r \cdot s + I) \cdot (t + I) = (r \cdot s) \cdot t + I = r \cdot (s \cdot t) + I = (r + I) \cdot (s \cdot t + I) = (r + I) \cdot [(s + I) \cdot (t + I)].$$

(Ejercicio: completar la demostración)

Observaciones

- Si R es conmutativo, entonces $\frac{R}{I}$ es conmutativo. (Ejercicio)
- Si R tiene identidad 1_R , entonces $\frac{R}{I}$ tiene identidad $1_R + I$ (Ejercicio)

Definición

Un ideal P en un anillo R se dice **primo** si $P \neq R$ y si A, B son ideales de R tales que:

$$A \cdot B \subset P \Rightarrow A \subset P \vee B \subset P$$

Teorema

Sea P un ideal en un anillo R , $P \neq R$, y supongamos que si $a, b \in R$:

$$a \cdot b \in P \Rightarrow a \in P \vee b \in P,$$

entonces, P es primo.

Dem.: (No la haremos)

Ejemplos

1. Sea $p \in \mathbb{Z}^+$ tal que p es primo. $p\mathbb{Z}$ es ideal de \mathbb{Z} .

Sean $a, b \in \mathbb{Z}/a \cdot b \in p\mathbb{Z} \Rightarrow p | (a \cdot b) \underbrace{\Rightarrow}_{p \text{ primo}} p | a \vee p | b \Rightarrow a \in p\mathbb{Z} \vee b \in p\mathbb{Z}$. Luego, $p\mathbb{Z}$ es ideal primo de \mathbb{Z} .

2. $6\mathbb{Z}$ no es primo en \mathbb{Z} . ¿Por qué?

FIN

PRÁCTICA 2: Anillos

1. Completar los ejercicios de la teoría.
2. Sea $(A, +, \cdot)$ un anillo. Demostrar que:

- (a) $a \cdot 0 = 0 \cdot a = 0$
- (b) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
- (c) $(-a) \cdot (-b) = a \cdot b$
- (d) $(a - b) \cdot c = a \cdot c - b \cdot c$

3. Sea $(A, +, \cdot)$ un anillo con identidad. Probar que:

- (a) Si $a, b \in A$ son dos unidades del anillo, entonces también lo es $a \cdot b$ y

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

- (b) El conjunto $A^* = \{a \in A / \exists a^{-1} \in A\}$ es un grupo respecto del producto, al que se llama **grupo multiplicativo del anillo A** .

4. Probar que *un anillo no tiene divisores de cero si vale la ley cancelativa del producto para todo elemento no nulo del mismo*.
5. Sea $R = \{x \in \mathbb{R} / x = a + b \cdot \sqrt{2} \wedge a, b \in \mathbb{Z}\}$. Comprobar que R es un anillo conmutativo con identidad, con la suma y el producto usual en \mathbb{R} . Investigar si admite divisores de cero.
6. Sea R un anillo. Demostrar que $I = \{x \in R / n \cdot x = 0 \wedge n \in \mathbb{Z}\}$ es un ideal de R .
7. Con relación al anillo del ejercicio 4., verificar que:

$$f : R \longrightarrow R/f(a + b \cdot \sqrt{2}) = a - b\sqrt{2}$$

es un isomorfismo de R en R , respecto de la suma y el producto.

8. Sea $f : A \longrightarrow B$ un homomorfismo del anillo $(A, +, \cdot)$ en el anillo $(B, +, \cdot)$. Probar que:

$$\tilde{A} \text{ es subanillo de } A \Rightarrow f(\tilde{A}) \text{ es subanillo de } B$$

9. Probar que \mathbb{Z}^+ y \mathbb{N} son isomorfos. En consecuencia, ambos conjuntos son indistinguibles algebraicamente y pueden identificarse.
10. Sea \mathbb{Q}_1 el conjunto de los racionales de denominador 1. Probar que \mathbb{Q}_1 es isomorfo a \mathbb{Z} . En virtud del isomorfismo, escribimos $\frac{a}{1} = a$.
11. Sea $(\mathbb{K}, +, \cdot)$ cuerpo. Probar que:
 - (a) No admite divisores de cero.
 - (b) Vale la ley cancelativa del producto para todo elemento no nulo del mismo.
 - (c) Si $b \neq 0$, entonces la ecuación $b \cdot x = a$ admite solución única en \mathbb{K} .
 - (d) El recíproco del opuesto de todo elemento no nulo es igual al opuesto de su recíproco.
 - (e) Se verifica:

$$\frac{x}{y} = \frac{x'}{y'} \Leftrightarrow x \cdot y' = y \cdot x'$$

12. Resolver el siguiente sistema de ecuaciones en $(\mathbb{Z}_5, +, \cdot)$:

$$\begin{cases} \bar{2}x + \bar{1}y = \bar{2} \\ \bar{3}x + \bar{4}y = \bar{3} \end{cases}$$

13. Un cuerpo \mathbb{K} es denso respecto de la relación $<$ sii

$$x < y \Rightarrow \exists z \in \mathbb{K}/x < z < y$$

Probar que el conjunto \mathbb{Q} es denso con la relación $<$. Como consecuencia de ello, entre dos racionales distintos se pueden intercalar infinitos racionales, si el orden está dado por la relación $<$.