

# Álgebra

## Anillos

### Generalidades

**Definición 1.1 (Anillo)** Un **anillo** es una estructura  $(A, +, \cdot)$  con las propiedades:

- $(A, +)$  es un grupo conmutativo
- Asociatividad:  $(xy)z = x(yz)$
- Distributividad:  $(x + y)z = xz + yz$        $x(y + z) = xy + xz$

Se denota al elemento unitario de  $(A, +)$  por  $0_A$  y al unitario de  $(A, +, \cdot)$ , si existe, por  $1_A$ .  $A^* = A \setminus \{0\}$ .  $0_A = 1_A \iff A = \{0\}$ .

**Definición 1.6** Si  $1_A \in A$ , entonces  $A$  es un **anillo unitario**. Una **unidad** de  $A$  es un elemento  $x$  que tiene su inverso  $y$ :  $xy = 1$ . El conjunto de unidades es  $U(A)$ . El inverso, si existe, se puede denotar por  $x^{-1}$  y  $x/y = xy^{-1}$ .

**Definición 1.8** Un **cuerpo** es un anillo  $K$  tal que  $K^*$  es un grupo. O, un anillo unitario con inverso.

**Definición 1.10** Un **divisor de cero** es un elemento  $x \in A^*$  tal que, para algún  $y \in A^*$ ,  $xy = 0_A$ . Un cuerpo nunca tiene divisores de cero:  $x = x(yy^{-1}) = (xy)y^{-1} = 0y^{-1} = 0$

**Definición 1.11** Se denomina **dominio de integridad** a un anillo unitario sin divisores de cero. El producto de dos anillos conmutativos  $C = A \times B$  nunca es un dominio de integridad, pues  $(a, 0) \neq 1_A, (0, b) \neq 1_B$  y  $(a, 0) \times (0, b) = (0, 0) = 0_C$ .

A un dominio de integridad se le puede asociar un cuerpo mediante el **cuerpo de fracciones de un dominio**. Dada la relación  $(x, y)R(x', y') \iff xy' = x'y$ , para el producto de dominios  $A \times A^*$  entonces para la clase de equivalencia  $[x, y]$ , las operaciones  $[x, y] + [x', y'] = [xy' + y'x, yy']$ ,  $[x, y] \cdot [x', y'] = [xx', yy']$  forman un cuerpo,  $K$ , con  $0_K = [0, 1]$ ,  $1_K = [1, 1]$ , y  $[x, y]^{-1} = [y, x]$ .

**Definición 1.14 (Ideal)** Un **ideal** es un subconjunto  $I \subset A$  tal que

- $I$  es subgrupo de  $A$
- $\forall i \in I, a \in A, ia \in I$ .

$A, \{0\}$  son los **ideales triviales**, y si  $I \neq A$ ,  $I$  es un **ideal propio**. Si  $1_A \in I$ ,  $I = A$ :  $\forall a \in A, a = a \cdot 1$ , y como  $1 \in I, a \in I$ .

**Definición 1.16** Dado un ideal  $I$  de  $A$ , dada la relación  $xRy \iff x - y \in I$ , se forma el **anillo cociente**  $A/I$  con las clases de equivalencia  $[x] = x + I = \{x + a \mid a \in I\}$ . Las operaciones suma y producto definidas por  $(x + I) + (y + I) = (x + y) + I$ ,  $(x + I)(y + I) = xy + I$ , son inyectivas.

**Definición 1.17 - 1.19** Sea  $A$  un anillo conmutativo y  $L$  un subconjunto de  $A$ . El conjunto  $I$  de sumas finitas  $a_1x_1 + \dots + a_lx_l$ ,  $a_i \in A, l_i \in L$  es un **ideal generado por  $L$** . Además,  $I$  es el mínimo ideal que contiene a  $L$ . Si  $L$  es finito,  $I$  es **finitamente generado**; y si  $L$  tiene un solo elemento, es decir,  $I = Al$ , el ideal es **principal**.

En los ideales se definen la (1) suma:  $I + J$  está dado por  $a_1, \dots, a_r, b_1, \dots, b_s \in A, x_1, \dots, x_r \in I$

$I, y_1, \dots, y_s \in J, a_1x_1 + \dots + a_rx_r + b_1y_1 + \dots + b_sy_s = x + y$ ; (2) producto:  $IJ = x_1y_1 + \dots + x_ry_r, x_1, \dots, x_r \in I, y_1, \dots, y_r \in J$ , (3) intersección  $I \cap J$ .

**Definición 1.21** Un ideal es **maximal** si (1)  $A/I$  es un cuerpo y (2)  $I$  es propio y ningún otro ideal propio lo contiene. (1)  $\iff$  (2). Si  $A/I$  es un cuerpo, luego contiene una unidad. Ninguna unidad  $i$  de  $A/I$  puede estar en  $I^* = I + i$  porque entonces  $I^* = A$ .

**Definición 1.22** Sean  $A$  unitario e  $I$  un ideal. Se dice que  $I$  es **primo** si (1)  $A/I$  es un dominio de integridad y (2)  $I$  es propio, y  $\forall x, y \in A$ , si  $xy \in I, x \in I$  o  $y \in I$ . (1)  $\iff$  (2). Demostración. Si  $xy \in I, 0 + I = xy + I = (x + I)(y + I)$ . Como  $A/I$  es dominio,  $x + I = 0 + I \rightarrow x \in I$  o  $y + I = 0 + I \rightarrow y \in I$ .

**Definición 1.24** Un **homomorfismo** de los anillos  $A, B$  es una aplicación  $f : A \rightarrow B$  definida por:

- $f(x + y) = f(x) + f(y)$
- $f(xy) = f(x)f(y)$
- $f(1_A) = 1_B$

$f(x)(f(1_A) - 1_B) = f(x)f(1_A) - f(x)1_B = f(x \cdot 1_A) - f(x) = 0$ . Si  $f(1_A) \neq 1_B$ ,  $f(A)$  son divisores de 0. La aplicación composición  $\phi : A \rightarrow A : g \mapsto g \circ f$  es homeomorfismo.

**Definición 1.26 (Núcleo e imagen)** Se define el **núcleo** de  $f$  al ideal:  $\ker f = \{x \in A \mid f(x) = 0\}$ , y se define la **imagen** de  $f$  al anillo  $\text{im } f = \{y \in B \mid \exists x \in A, f(x) = y\}$ .

**Proposición 1.27 / 1.30 Teorema de isomorfía.** Dado un homomorfismo  $f$ , el diagrama

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow p & & \uparrow j \\ A/\ker f & \xrightarrow{\bar{f}} & \text{im } f \end{array}$$

Con  $p : x \mapsto x + \ker f$  sobreyectiva / **epimorfismo**,  $f : x + \ker f \mapsto f(x)$  biyectiva / **isomorfismo**,  $j : y \mapsto y$  inyectiva / **monomorfismo**; es conmutativo. Si  $f$  es monomorfismo entonces  $\ker f = \{0\}$ . Dos anillos conmutativos son **isomorfos** ( $A \simeq B$ ) si existe un isomorfismo entre ellos.

## Divisibilidad

**Definición 2.1**  $x$  es un divisor de  $y$  o  $y$  es un múltiplo de  $x, x|y$  si existe  $a \in A, y = ax$ . Si  $(x) = \{kx \mid k \in \mathbb{Z}\}$ , entonces  $x|y \iff (y) \subset (x)$ .  $x$  está relacionado con  $y$  si  $(x) = (y) \iff x|y, y|x$ . En ese caso, existe una unidad  $a \in U(A)$  tal que  $y = ax$ . Si  $(y) = (x), y \in (x), x \in (y); y = ax, x = by, y = aby \iff 1 = ab$ .

Denotamos  $\text{div}(y)$  al conjunto de divisores de  $y$ . Si  $y$  genera un ideal primo, entonces decimos que  $y$  es **primo**.  $y$  es **irreducible** si sus divisores son las unidades y productos de  $y$  por unidades. **Todo primo es irreducible, pero NO TODO irreducible es primo** (hay irreducibles que no generan ideales primos).

**Definición 2.6** Se dice que  $A$  es un **dominio euclídeo** **DE** si existe una aplicación  $\|\cdot\| : A \rightarrow \mathbb{N}$  tal que

- $\|x\| = 0 \iff x = 0$
- $\|xy\| = \|x\| \cdot \|y\|$
- Si  $x, y \in A^*$  existe  $r \in A$  tal que  $y|(x - r)$  y  $\|r\| < \|y\|$

$\mathbb{Z}$  es DE porque el valor absoluto cumple la función. En  $\mathbb{Z}[i]$  la función  $\|a + bi\| = a^2 + b^2$  cumple las propiedades y  $\mathbb{Z}[i]$  es DE.

**Proposición 2.8** Si  $A$  es DE, entonces  $U(A) = \{x \in A \mid \|x\| = 1\}$ .  $\rightarrow \|1_A\| = 1$  porque  $\|1_A\| = \|1_A \cdot 1_A\| =$

$\|1_A\| \|1_A\|$ , y como  $\|1_A\| \neq 0$ ,  $\|1_A\| = 1$ . Si  $x \in A$ , existe  $x^{-1}$  y  $\|x\| \|x^{-1}\| = \|xx^{-1}\| = 1$  y como  $\|x\| \in \mathbb{N}$ ,  $\|x\| = \|x^{-1}\| = 1$

**Proposición 2.10/Definición 2.11** En un dominio de ideales principales **DPI** todos los ideales son principales. Un DE es un DIP. Elegimos  $x$  tal que  $\|x\| = \min\{\|y\| \mid 0 \neq y \in I\}$ . Entonces  $x > 0$  y  $I$  está generado por  $x$ , ya que si  $y \neq 0$ ,  $y \in I$ , existe  $r \in A$  tal que  $x|(y-r)$ ,  $\|r\| < \|x\|$ . Entonces  $y-r \in I$  y como  $y \in I$ ,  $r \in I$ , pero como  $\|r\| < \|x\|$ , y  $\|x\|$  es el mínimo en  $I$ ,  $r=0$  y  $y \in (x)$ .

**Proposición 2.12** Si  $A$  es un DIP, todo elemento irreducible  $a \in A^*$  genera un ideal maximal. Sea  $I$ ,  $(a) \subset I$ . Entonces  $I = (a)$  o  $I = A$ . Sea  $b \in A$  tal que  $I = (b)$ . Entonces  $(a) \subset I = (b)$ ,  $b|a$ . Como  $a$  es irreducible, o bien  $b = ua$ ,  $u \in U(A)$ , y  $(a) = (b) = I$  o  $b \in U(A)$ , y  $I = (b) = A$ .

**Definición 2.13 (Característica de un dominio de integridad)** Definimos  $\phi = \phi_A : \mathbb{Z} \rightarrow A : k \mapsto k \cdot 1_A = 1_A + \dots + 1_A$  ( $k > 0$ ),  $0$  ( $k = 0$ ),  $-((-k) \cdot 1_A)$  ( $k < 0$ ).  $\phi$  es un homomorfismo. Si  $\ker \phi = \{0\}$ ,  $\mathbb{Z} \subset A$ , y tiene característica 0; y si  $\ker \phi \neq \{0\}$ ,  $A$  tiene característica positiva. En este caso, como  $A$  es dominio de integridad y  $\mathbb{Z}/\ker \phi \simeq \text{im } \phi \subset A$ ,  $\mathbb{Z}/\ker \phi$  también es dominio y  $\ker \phi = (p)$  es un ideal primo.

**Definición 2.14** Sean  $x, y \in A^*$ ,  $z \in A$ .  $z$  es un **máximo común divisor** si  $z|x$ ,  $z|y$ , y  $z$  divide cualquier otro divisor de ambos.  $z$  es un **mínimo común múltiplo** si  $x|z$ ,  $y|z$  y  $z$  divide a cualquier otro múltiplo de ambos. Estos elementos son únicos.

**Proposición 2.17 / 2.18 / 2.19.** Para un dominio de integridad  $A^*$ :

- $\forall x, y \in A^*$  tiene mcd:  $(x) + (y) \subset (mcd)$ .
- $\forall x, y \in A^*$  tiene mcm:  $(x) \cap (y) = (mcm)$ .
- $xy = mcm \cdot mcd$ .

Si se cumple cualquiera de los dos primeros puntos **MC**, todo elemento irreducible es primo **P**.

**Proposición 2.20 (Identidad de Bezout B).** Si  $x, y \in A^*$  generan un ideal principal, existe  $z = mcd(x, y)$  y existen  $a, b \in A$  tales que  $z = ax + by$ .

**Definición 2.21** Dos elementos  $x, y \in A^*$  son primos entre sí si no comparten más divisores que las unidades, es decir,  $mcd(x, y) = 1_A$ .

El esquema de todas las relaciones queda así.

$$\begin{array}{ccccccc} DE & \longrightarrow & DIP & \longrightarrow & DFU & \longrightarrow & F \\ & & \downarrow & & \downarrow & & \\ & & B & \longrightarrow & MC & \longrightarrow & P \end{array}$$

**Proposición 2.26 Ecuaciones diofánticas lineales con dos incógnitas.** Las ecuaciones son de la forma  $c = aX + bY$ , de un dominio. Si se cumple la identidad de Bezout, y  $d = mcd(a, b)$ , entonces se cumple que  $d = \alpha a + \beta b$ . Por tanto, existen  $a_0, b_0, c_0 \in A$  tales que  $c = c_0 d$ ,  $a = a_0 d$ ,  $b = b_0 d$ , y  $1 = \alpha a_0 + \beta b_0$ , de modo que la nueva ecuación a resolver es

Multiplicando por  $\alpha$  y sustituyendo  $\alpha a_0 = 1 - \beta b_0$  tenemos  $X = \alpha c_0 + b_0(\beta X - \alpha Y)$ . Igualmente, multiplicando por  $\beta$  y sustituyendo  $\alpha a_0 = 1 - \beta b_0$  tenemos  $Y = \beta c_0 - a_0(\beta X - \alpha Y)$ . Así, si  $t = \beta X - \alpha Y$ , para algunos  $x, y$ , tenemos las ecuaciones  $x = \alpha c_0 + b_0 t$ ;  $y = \beta c_0 - a_0 t$ .

Así, primero hallamos  $d = \alpha a + \beta b$ , con lo cual obtenemos  $\alpha, \beta, a, b$ , y de ahí sacamos  $a_0 = a/mcd$ ,  $b_0 = b/mcd$ ,  $c_0 = c/mcd$ . Para obtener  $d = \alpha a + \beta b$  empleamos el algoritmo de Euclides.

**Proposición 2.27 Algoritmo de Euclides.** Este algoritmo sólo es válido en DIPs, ya que en ellos se da B y MC. Ponemos un ejemplo práctico con 4329/132:

$$4329 = 132 \cdot 32 + 105, \quad 132 = 105 \cdot 1 + 27, \quad 105 = 27 \cdot 3 + 24, \quad 27 = 24 \cdot 1 + 3, \quad 24 = 8 \cdot 3$$

Si tenemos la ecuación diofántica  $4329X + 132Y = 33$ , vemos que tiene solución pues  $\text{mcd}(4329, 132) = 3$  y  $3|33$ . Para encontrar las soluciones primero necesitamos reconstruir la ecuación  $d = \alpha a + \beta b$ , con  $a = 4329, b = 132$ . Para ello vamos sustituyendo el cociente de cada una de las ecuaciones por la siguiente.

$$a = 32b + x_2 \iff x_2 = a - 32b \quad || \quad b = x_2 + x_3 \iff x_3 = b - x_2 \quad || \quad x_2 = 3x_3 + x_4 \iff x_4 = x_2 - 3x_3$$

Finalmente,  $3 = x_3 - x_4$ . De aquí empezamos a sustituir todas las secuencias, al revés, hasta llegar con  $a, b$ .  $3 = x_3 - x_4 = 4x_3 - x_2 = 4b - 5x_2 = 164b - 5a$ . Luego  $3 = 164b - 5a = \beta b + \alpha a$ . Así,  $\beta = 164, \alpha = -5$ . Si, además,  $a_0 = a/\text{mcd} = 4329/3 = 1443, b_0 = b/\text{mcd} = 132/3 = 44, c_0 = c/\text{mcd} = 33/3 = 11$ , tenemos las ecuaciones  $x = -5 \cdot 11 + 44t; y = 164 \cdot 11 - 1443t$ .