

# Álgebra Conmutativa Computacional

F. J. Lobillo

2019/2020



# Anillos e ideales

1.1

## Anillos conmutativos

**Definición 1.1.** Un *anillo* es un conjunto  $R$  sobre el que hay definidas dos operaciones  $+: R \times R \rightarrow R$  y  $\cdot: R \times R \rightarrow R$  (denominadas suma y producto) que satisfacen las siguientes propiedades:

**Asociativa de la suma.** Para cualesquiera  $r, s, t \in R$ ,

$$r + (s + t) = (r + s) + t.$$

**Conmutativa de la suma.** Para cualesquiera  $r, s \in R$ ,

$$r + s = s + r.$$

**Elemento neutro para la suma.** Existe un elemento  $0 \in R$  tal que

$$r + 0 = r$$

para cualquier  $r \in R$ .

**Elemento opuesto para la suma.** Para cualquier  $r \in R$ , existe  $-r \in R$  tal que

$$r + (-r) = 0.$$

**Asociativa del producto.** Para cualesquiera  $r, s, t \in R$ ,

$$r(st) = (rs)t.$$

**Elemento neutro para el producto.** Existe  $1 \in R$ , tal que

$$r1 = 1r = r$$

para todo  $r \in R$ .

**Distributiva de la suma respecto del producto.** Para todos  $r, s, t \in R$ ,

$$r(s + t) = rs + rt$$

y

$$(r + s)t = rt + st.$$

Un anillo se dice *conmutativo* si satisface la propiedad

**Conmutativa del producto.** Para cualesquiera  $r, s \in R$ ,

$$rs = sr.$$

**Proposición 1.2.** *Los elementos neutros para la suma y el producto son únicos. El opuesto de un elemento es único.*

**Demostración.** Si  $0, 0' \in R$  son elementos neutros para la suma

$$0 = 0 + 0' = 0'.$$

La unicidad del elemento neutro para el producto es análoga. Si  $-r, r'$  son opuestos para  $r$ ,

$$-r = -r + 0 = -r + (r + r') = (-r + r) + r' = 0 + r' = r'.$$

□

**Definición 1.3.** Dado un anillo conmutativo  $R$ , un elemento  $r$  es una *unidad* si tiene inverso para el producto, es decir, si existe  $r^{-1} \in R$  tal que

$$rr^{-1} = 1.$$

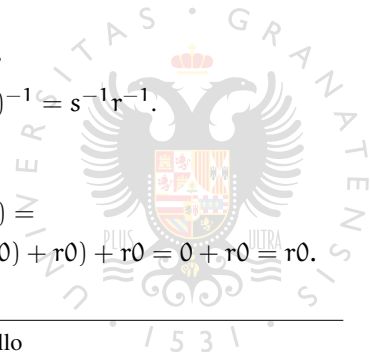
El conjunto de la unidades se denota  $\mathcal{U}(R)$ . Se dice que  $r \in R$  es un *divisor de cero* si existe  $s \in R \setminus \{0\}$  tal que  $rs = 0$ .

**Proposición 1.4.** Sea  $R$  un anillo. Para cualesquiera  $r, s \in R$ ,

1.  $r0 = 0$ ,
2.  $(-r)s = -(rs) = r(-s)$ ,
3. si  $r \in \mathcal{U}(R)$ , su inverso es único,
4. si  $r, s \in \mathcal{U}(R)$ ,  $rs \in \mathcal{U}(R)$  y  $(rs)^{-1} = s^{-1}r^{-1}$ .

**Demostración.** Para cualquier  $r \in R$ ,

$$\begin{aligned} 0 &= -(r0) + r0 = -(r0) + r(0 + 0) = \\ &= -(r0) + (r0 + r0) = (-r0) + r0 = 0 + r0 = r0. \end{aligned}$$



Dado que

$$(-r)s + rs = (-r + r)s = 0s = 0,$$

se tiene que  $(-r)s = -(rs)$  por la unicidad del opuesto. La unicidad del inverso es análoga a la unicidad del opuesto. Finalmente

$$rs(s^{-1}r^{-1}) = r(ss^{-1})r^{-1} = r1r^{-1} = rr^{-1} = 1,$$

de donde  $s^{-1}r^{-1} = (rs)^{-1}$  y  $rs \in \mathcal{U}(R)$ . □

**Definición 1.5.** Un anillo conmutativo en el que 0 es el único divisor de cero recibe el nombre de *dominio de integridad*. Observemos que  $R$  es dominio de integridad si y solo si para cualesquiera  $r, s \in R$ , si  $rs = 0$  entonces  $r = 0$  o  $s = 0$ .

Un *cuerpo* es un anillo conmutativo en el que todo elemento no nulo es una unidad, es decir,  $\mathcal{U}(R) = R \setminus \{0\}$ .

*Ejemplo 1.6.* Son anillos conmutativos  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, R[x]$  donde  $R$  es un anillo conmutativo,  $\mathbb{Z}_n, \mathbb{F}_q$ . De los anteriores,  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q$  son cuerpos.

*Ejemplo 1.7.* Sean  $A_1, A_2$  dos anillos. Es un ejercicio rutinario comprobar que  $A_1 \times A_2$  es un nuevo anillo en el que las operaciones se realizan componente a componente, es decir,

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

y

$$(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2).$$

El cero y el uno de este nuevo anillo son, respectivamente,  $(0_1, 0_2)$  y  $(1_1, 1_2)$ , y el opuesto se calcula

$$-(a_1, a_2) = (-a_1, -a_2).$$

**Subanillos e ideales**

**Definición 1.8.** Dado un anillo  $A$ , un subconjunto  $B \subseteq A$  es un subanillo si

- $0 \in B$  y  $1 \in B$ ;
- dados  $a, b \in B$ ,  $a - b \in B$ ;
- dados  $a, b \in B$ ,  $ab \in B$ .

Es inmediato comprobar que un subanillo vuelve a ser un anillo con las operaciones heredadas. Pero no todo subconjunto que sea un anillo con las operaciones heredadas es un subanillo, como vamos a comprobar con el siguiente ejemplo.

*Ejemplo 1.9.* En  $\mathbb{Z}_6$  consideramos el subconjunto  $\{0, 2, 4\}$ . Es sencillo verificar que  $\{0, 2, 4\}$  es cerrado para la suma, opuesto y producto. Como

$$4 \times 0 = 0, 4 \times 2 = 2, 4 \times 4 = 4,$$

tenemos que  $\{0, 2, 4\}$  es un anillo en el que el elemento neutro para el producto es 4.

En adelante, y salvo que específicamente se indique lo contrario, todos los anillos tratados en este curso son anillos conmutativos.

**Definición 1.10.** Dado un anillo conmutativo  $A$ , un subconjunto no vacío  $I \subseteq A$  es un ideal si

- dados  $a, b \in I$ ,  $a + b \in I$ ;

- dados  $a \in I$  y  $b \in A$ ,  $ab \in I$ .

Se denota por  $I \leq A$ .

*Observación 1.11.* Si  $a, b \in I$ , entonces  $a - b = a + (-1)b \in I$ , por lo que  $I$  es un subgrupo abeliano de  $A$ .

**Proposición 1.12.** Sea  $A$  un anillo conmutativo y sea  $I \subseteq A$  un subgrupo abeliano.  $I$  es un ideal de  $A$  si y sólo si  $A/I$  es un anillo conmutativo con respecto a las operaciones  $(a + I) + (b + I) = (a + b) + I$  y  $(a + I)(b + I) = ab + I$ .

*Demostración.* Por ser  $I$  un subgrupo abeliano sólo tenemos que ocuparnos de que el producto está bien definido. Supongamos que  $a + I = a' + I$ , es decir,  $a - a' \in I$ . Si  $I$  es ideal,  $a + I = a' + I$  y  $b + I = b' + I$  tenemos que

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I,$$

luego el producto está bien definido. Recíprocamente, si el producto está bien definido tenemos que  $(0 + I)(b + I) = 0 + I$ , por tanto, si  $a \in I$

$$ab + I = (a + I)(b + I) = (0 + I)(b + I) = 0 + I,$$

es decir,  $ab \in I$ , lo que implica que  $I$  es un ideal. □

Dados ideales  $I, J \leq A$ , se define

$$I + J = \{x + y \mid x \in I, y \in J\}$$

y

$$IJ = \{x_1 y_1 + \cdots + x_t y_t \mid x_i \in I, y_i \in J, 1 \leq i \leq t\}$$

**Proposición 1.13.**  $I + J$ ,  $I \cap J$  e  $IJ$  son ideales de  $A$ .  $I + J$  es el menor ideal que contiene tanto a  $I$  como a  $J$ .  $IJ \subseteq I \cap J$ .

*Demostración.* Ejercicio. □

Dado  $F \subseteq A$ , definimos

$$\langle F \rangle = \{a_1 f_1 + \cdots + a_s f_s \mid a_1, \dots, a_s \in A, f_1, \dots, f_s \in F\}.$$

**Proposición 1.14.**  $\langle F \rangle$  es el menor ideal de  $A$  que contiene a  $F$ .

*Demostración.* Es inmediato comprobar que si un ideal contiene a  $F$ , debe contener a  $\langle F \rangle$ . Comprobemos que es un ideal. Sean  $a_1 f_1 + \cdots + a_s f_s, b_1 g_1 + \cdots + b_t g_t \in \langle F \rangle$ . Tenemos que

$$\begin{aligned} (a_1 f_1 + \cdots + a_s f_s) + (b_1 g_1 + \cdots + b_t g_t) = \\ a_1 f_1 + \cdots + a_s f_s + b_1 g_1 + \cdots + b_t g_t \in \langle F \rangle. \end{aligned}$$

Por otra parte, si  $a \in A$  y  $a_1 f_1 + \cdots + a_s f_s \in \langle F \rangle$ ,

$$a(a_1 f_1 + \cdots + a_s f_s) = (aa_1)f_1 + \cdots + (aa_s)f_s \in \langle F \rangle,$$

lo que demuestra que  $\langle F \rangle$  es un ideal. □

**Definición 1.15.**  $\langle F \rangle$  recibe el nombre de ideal generado por  $F$ . Por convenio,  $0 = \langle \emptyset \rangle$ . Un ideal  $I$  se dice finitamente generado si existen  $f_1, \dots, f_s \in I$  tales que  $I = \langle f_1, \dots, f_s \rangle$ .

**Proposición 1.16.** Sean  $I = \langle F \rangle$  y  $J = \langle G \rangle$ . Entonces  $I + J = \langle F \cup G \rangle$  y  $IJ = \langle fg \mid f \in F, g \in G \rangle$ .

*Demostración.* Ejercicio. □



**Morfismos de anillos**

**Definición 1.17.** Sean  $A$  y  $B$  dos anillos. Una aplicación  $f : A \rightarrow B$  es un morfismo de anillos si  $f(0) = 0$ ,  $f(1) = 1$ ,  $f(a + b) = f(a) + f(b)$  y  $f(ab) = f(a)f(b)$ .

*Observación 1.18.* Como consecuencia de la definición, si  $f : A \rightarrow B$  es un morfismo de anillos tenemos que

$$0 = f(0) = f(b + (-b)) = f(b) + f(-b),$$

luego  $f(-b) = -f(b)$  para cualquier  $b \in A$ . En consecuencia,

$$f(a - b) = f(a + (-b)) = f(a) + f(-b) = f(a) - f(b),$$

luego  $f$  es morfismo de grupos abelianos.

**Proposición 1.19.** Sea  $f : A \rightarrow B$  un morfismo de anillos. Entonces  $\text{im}(f)$  es un subanillo de  $B$  y  $\ker(f)$  un ideal de  $A$ . Además  $\text{im}(f) \cong A/\ker(f)$ .

*Demostración.* Es sencillo comprobar que  $\text{im}(f)$  es un subanillo. Como  $f$  es un morfismo de grupos abelianos, es también inmediato que  $\ker(f)$  es un subgrupo abeliano de  $A$ . Si  $a \in \ker(f)$  y  $b \in A$ ,

$$f(ab) = f(a)f(b) = 0f(b) = 0,$$

luego  $ab \in \ker(f)$ , i.e.  $\ker(f)$  es un ideal de  $A$ . Por último definimos  $\phi : A/\ker(f) \rightarrow \text{im}(f)$  mediante  $\phi(a + \ker(f)) = f(a)$ . Esta aplicación

está bien definida porque si  $a + \ker(f) = a' + \ker(f)$ ,

$$\begin{aligned}\phi(a + \ker(f)) &= f(a) = f(a - a' + a') \\ &= f(a - a') + f(a') = f(a') = \phi(a' + \ker(f)).\end{aligned}$$

Es sencillo comprobar que  $\phi$  es un morfismo de anillos biyectivo.  $\square$

Dos ideales  $I, J \leq A$  se dicen coprimos si  $A = I + J$ .

**Lema 1.20.** Sean  $I, J, K$  ideales de  $A$ . Entonces  $I + J = A$  e  $I + K = A$  si y sólo si  $I + (J \cap K) = A$ .

*Demostración.* Es inmediato que si  $I + (J \cap K) = A$  tenemos que  $I + J = A$  e  $I + K = A$ . Supongamos por tanto que  $I + J = A$  e  $I + K = A$ . Existen  $a, a' \in I$   $b \in J$  y  $c \in K$  tales que  $1 = a + b$  y  $1 = a' + c$ . Por tanto

$$1 = a + b = a + b(a' + c) = a + ba' + bc = (a + ba') + bc \in I + (J \cap K),$$

luego  $I + (J \cap K) = A$ .  $\square$

**Teorema 1.21** (Teorema Chino del Resto). Sean  $I_1, \dots, I_t$  ideales de  $A$  coprimos dos a dos, es decir  $I_i + I_j = A$  para cualesquiera  $i \neq j$ . Entonces  $A/(I_1 \cap \dots \cap I_t) \cong (A/I_1) \times \dots \times (A/I_t)$ .

*Demostración.* Sea  $f : A \rightarrow (A/I_1) \times \dots \times (A/I_t)$  el morfismo de anillos definido por  $f(a) = (a + I_1, \dots, a + I_t)$ . Veamos que es sobreyectivo. Para ello, dados  $a_1, \dots, a_t \in A$  tenemos que encontrar un  $x \in A$  tal que  $x + I_i = a_i + I_i$  para cada  $1 \leq i \leq t$ . Aplicando iteradamente el Lema 1.20, tenemos que  $A = I_i + \bigcap_{j \neq i} I_j$ , por lo que existen

$b_i \in I_i$  y  $c_i \in \bigcap_{j \neq i} I_j$  tales que  $1 = b_i + c_i$ . Sea  $x = a_1 c_1 + \cdots + a_t c_t$ . Dado que

$$\begin{aligned}x + I_i &= a_1 c_1 + \cdots + a_t c_t + I_i = a_i c_i + I_i \\&= a_i(1 - b_i) + I_i = a_i - a_i b_i + I_i = a_i + I_i,\end{aligned}$$

tenemos que  $f$  es sobreyectiva. Por otra parte,  $f(a) = 0$  si y solo si  $a \in I_i$  para cualquier  $1 \leq i \leq t$ , de donde  $\ker(f) = I_1 \cap \cdots \cap I_t$ . El teorema se sigue por tanto de la Proposición 1.19.  $\square$



---

## Ejercicios sobre Anillos

Todos los anillos considerados en esta relación de ejercicios son conmutativos salvo que se especifique lo contrario.

**Ejercicio 1.1.** Dados anillos  $A_1$  y  $A_2$ , comprueba que  $A_1 \times A_2$  con las operaciones definidas en el Ejemplo 1.7 es un anillo. Calcula sus unidades  $\mathcal{U}(A_1 \times A_2)$ .

**Ejercicio 1.2.** Un elemento  $e \in A$  se dice idempotente si  $e^2 = e$ . Demuestra que si  $e$  es idempotente,  $1 - e$  también lo es. Demuestra que  $A = \langle e \rangle \oplus \langle 1 - e \rangle$ , es decir,  $A = \langle e \rangle + \langle 1 - e \rangle$  y  $\{0\} = \langle e \rangle \cap \langle 1 - e \rangle$ .

**Ejercicio 1.3.** Un elemento  $x \in A$  se dice nilpotente si  $x^n = 0$  para algún  $n \in \mathbb{N}$ . Demuestra que si  $x$  es nilpotente,  $1 - x$  y  $1 + x$  son unidades de  $A$ .

**Ejercicio 1.4.** Demuestra que el conjunto de los elementos nilpotentes de un anillo conmutativo  $A$  es un ideal.

**Ejercicio 1.5.** Sea  $p \in \mathbb{Z}$  primo y sea  $R = \left\{ \frac{m}{n} \in \mathbb{Q} \mid p \nmid n \right\}$ . Demuestra que  $R$  es un subanillo.

**Ejercicio 1.6.** Demuestra la Proposición 1.13.

**Ejercicio 1.7.** Demuestra la Proposición 1.16.

**Ejercicio 1.8.** Demuestra que  $I(J + K) = IJ + IK$  para ideales  $I, J, K \leq A$ . ¿Es cierta la identidad  $I \cap (J + K) = (I \cap J) + (I \cap K)$ ?

**Ejercicio 1.9.** Demuestra que si  $I + J = A$ , entonces  $IJ = I \cap J$ .

**Ejercicio 1.10.** Un ideal  $P \leq A$  en un anillo conmutativo se dice primo si, para cualesquiera  $a, b \in A$ , si  $ab \in P$  entonces  $a \in P$  o  $b \in P$ . Demuestra que  $\langle p \rangle \subseteq \mathbb{Z}$  es un ideal primo si y solo si  $p$  es un número primo.

**Ejercicio 1.11.** Un ideal  $M \leq A$  de un anillo conmutativo se dice maximal si no existe otro ideal  $J \leq A$  tal que  $M \subsetneq J \subsetneq A$ . Demuestra que todo ideal maximal es primo.

**Ejercicio 1.12.** Demuestra que  $P \leq A$  es primo si y solo si  $A/P$  es un dominio de integridad. Demuestra que  $M \leq A$  es maximal si y solo si  $A/M$  es un cuerpo.



## Bibliografía

- [1] David A. Cox, John Little, and Donald O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Text in Mathematics. Springer, fourth edition, 2015.
- [2] Serge Lang. *Undergraduate Algebra*. Undergraduate Text in Mathematics. Springer, second edition, 1990.

