Álgebra Conmutativa Computacional

F. J. Lobillo

2022/2023

Índice general

Capítulo 1

Anillos e Ideales

1.1 Anillos conmutativos

Definición 1.1. Un *anillo* es un conjunto R sobre el que hay definidas dos operaciones $+ : R \times R \to R$ y $\cdot : R \times R \to R$ (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 $r, s, t \in R$,

$$r(s+t) = rs + rt \quad \text{y} \quad (r+s)t = rt + st.$$

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 $r \in R$,

$$0 = -(r0) + r0 = -(r0) + r(0+0) = \\ -(r0) + (r0 + r0) = (-(r0) + r0) + r0 = 0 + r0 = r0.$$

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

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

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

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

1.2 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 aditivo de A.

Proposición 1.12. *Sea A un anillo conmutativo y sea $I \subseteq A$ un subgrupo aditivo. 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 aditivo 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. □

Definición 1.13. Un ideal $P \lneq A$ en un anillo conmutativo se dice primo si, para cualesquiera $a, b \in A$, si $ab \in P$ entonces $a \in P$ o $b \in P$. Un ideal $M \lneq A$ de un anillo conmutativo se dice maximal si no existe otro ideal $J \leq A$ tal que $M \subsetneq J \subsetneq A$.

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

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

y

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

Proposición 1.14. *$I+J$, $I \cap J$ 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

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

Proposición 1.15. *$\langle F\rangle$ 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 $a_1f_1 + \cdots + a_sf_s, b_1g_1 + \cdots + b_tg_t \in \langle F\rangle$. Tenemos que

$$(a_1f_1 + \cdots + a_sf_s) + (b_1g_1 + \cdots + b_tg_t) = \\ a_1f_1 + \cdots + a_sf_s + b_1g_1 + \cdots + b_tg_t \in \langle F\rangle.$$

Por otra parte, si $a \in A$ y $a_1f_1 + \cdots + a_sf_s \in \langle F\rangle$,

$$a(a_1f_1 + \cdots + a_sf_s) = (aa_1)f_1 + \cdots + (aa_s)f_s \in \langle F\rangle,$$

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

Definición 1.16. $\langle F\rangle$ recibe el nombre de ideal generado por F. Por convenio, $0 = \langle\varnothing\rangle$. Un ideal I se dice finitamente generado si existen $f_1, \ldots, f_s \in I$ tales que $I = \langle f_1, \ldots, f_s\rangle$.
Si es necesario hacer referencia al anillo, también se emplean las siguientes notaciones:

$$\langle F\rangle = {}_R\langle F\rangle = \langle F\rangle_R = RF = Rf_1 + \cdots + Rf_s,$$

la última en el caso $F = \{f_1, \ldots, f_s\}$.

Proposición 1.17. *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. □

Teorema 1.18. *Para un anillo R las siguientes afirmaciones son equivalentes:*

1. *R satisface la Condición de Cadena Ascendente, es decir, dada una cadena de ideales $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_k \subseteq \cdots$, existe n tal que $I_n = I_m$ para todo $m \geq n$.*

2. *Todo ideal de R es finitamente generado.*

Demostración. Ejercicio. □

Recordemos que un anillo R es Noetheriano si satisface las condiciones equivalentes del Teorema 1.18.

1.3 Morfismos de anillos

Definición 1.19. Sean A y B dos anillos. Una aplicación $f : A \to B$ 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 1.20. Como consecuencia de la definición, si $f : A \to B$ 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 1.21. *Sea $f : A \to B$ un morfismo de anillos. Entonces* $\operatorname{im}(f)$ *es un subanillo de B y* $\ker(f)$ *un ideal de A. Además* $\operatorname{im}(f) \cong A/\ker(f)$.

Demostración. Es sencillo comprobar que $\mathrm{im}(f)$ 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 $ab \in \ker(f)$, lo que implica que $\ker(f)$ es un ideal de A. Por último definimos $\phi : A/\ker(f) \to \mathrm{im}(f)$ 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 ϕ es un morfismo de anillos biyectivo. □

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

Lema 1.22. *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 $I + (J \cap K) = A$. □

Teorema 1.23 (Teorema Chino del Resto)**.** *Sean $I_1, \ldots, I_t$ ideales de A coprimos dos a dos, es decir $I_i + I_j = A$ para cualesquiera $i \neq j$. Entonces $A/(I_1 \cap \cdots \cap I_t) \cong (A/I_1) \times \cdots \times (A/I_t)$.*

Demostración. Sea $f : A \to (A/I_1) \times \cdots \times (A/I_t)$ el morfismo de anillos definido por $f(a) = (a + I_1, \ldots, a + I_t)$. Veamos que es sobreyectivo. Para ello, dados $a_1, \ldots, a_t \in A$ 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 1.22, 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 $x = a_1c_1 + \cdots + a_tc_t$. Dado que

$$\begin{aligned} x + I_i = a_1c_1 + \cdots + a_tc_t + I_i &= a_ic_i + I_i \\ &= a_i(1 - b_i) + I_i = a_i - a_ib_i + I_i = a_i + I_i, \end{aligned}$$

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 1.21. □

1.4 Anillo de fracciones

Sea R un dominio de integridad conmutativo y $S \subseteq R$ un conjunto multiplicativamente cerrado, es decir, $1 \in S$ y $s, t \in S \Rightarrow st \in S$. En $R \times S$ definimos la siguiente relación binaria:

$$(r, s) \sim (r', s') \iff rs' = r's.$$

Lema 1.24. *La relación $\sim$ es una relación de equivalencia.*

Demostración. Ejercicio. □

Denotamos por $r/s = \frac{r}{s}$ a la clase de equivalencia de $(r, s) \in R \times S$ mediante la relación $\sim$. El conjunto cociente $(R \times S)/\sim$ se denota $Q_S(R)$ o RS^{-1}.

En $R \times S$ definimos la siguiente aritmética

$$(a,b) + (c,d) = (ad + bc, bd), \quad (a,b)(c,d) = (ac, bd).$$

Lema 1.25. *Si* $(a,b) \sim (a',b')$ *y* $(c,d) \sim (c',d')$, *entonces* $(a,b) + (c,d) \sim (a',b') + (c',d')$ *y* $(a,b)(c,d) \sim (a',b')(c',d')$.

Demostración. De las siguientes identidades, $ab' = a'b$, $cd' = c'd$, deducimos que

$$\begin{aligned}(ad + bc)b'd' &= adb'd' + bcb'd' \\ &= a'bdd' + bb'c'd = (a'd' + b'c')bd,\end{aligned}$$

luego $(ad + bc, bd) \sim (a'd' + b'c', b'd')$. Además

$$(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd),$$

luego $(ac, bd) \sim (a'c', b'd')$. □

Como consecuencia del lema anterior, las operaciones definidas en $R \times S$ pueden extenderse a $Q_S(R)$.

Proposición 1.26. $(Q_S(R), +, \cdot)$ *es un dominio conmutativo.*

Demostración. Ejercicio. □

El morfismo

$$R \to Q_S(R), \quad \left[r \mapsto \frac{r}{1}\right]$$

es un morfismo inyectivo de anillos, por lo que podemos identificar R como subanillo de $Q_S(R)$. Bajo esta identificación tenemos la siguiente proposición.

Proposición 1.27. $\mathcal{U}(R) \cup S \subseteq \mathcal{U}(Q_S(R))$.

Demostración. Ejercicio. □

Teorema 1.28. *Sea $f : R \to T$ un morfismo de anillos tal que $f(S) \subseteq \mathcal{U}(T)$. Existe un único morfismo de anillos $\overline{f} : Q_S(R) \to T$ tal que $\overline{f}(r) = f(r)$ para cualquier $r \in R$.*

Demostración. Como f es un morfismo de anillos, si $rs' = r's$ tenemos que $f(r)f(s') = f(r')f(s)$, por tanto $f(r)f(s)^{-1} = f(r')f(s')^{-1}$ dado que $f(S) \subseteq \mathcal{U}(T)$. En consecuencia el morfismo $\overline{f} : Q_S(R) \to T$ definido por $\overline{f}(\frac{r}{s}) = f(r)f(s)^{-1}$ está bien definido. Es sencillo comprobar que $\overline{f}$ es morfismo de anillos. Supongamos que $g : Q_S(R) \to T$ satisface también que $g(r) = f(r)$ para cualquier $r \in R$. Si $s \in S$, $1 = g\left(\frac{s}{s}\right) = g(s)g\left(\frac{1}{s}\right) = f(s)g\left(\frac{1}{s}\right)$, por lo que $f(s)^{-1} = g\left(\frac{1}{s}\right)$. En consecuencia $g\left(\frac{r}{s}\right) = g(r)g\left(\frac{1}{s}\right) = f(r)f(s)^{-1} = \overline{f}\left(\frac{r}{s}\right)$. □

Sea $P \leq R$ un ideal primo. Observemos que $R \setminus P$ es multiplicativamente cerrado. En este caso, el anillo de fracciones se denota $Q_{R\setminus P}(R) = Q_P(R)$. Dado que R es un dominio, $\{0\}$ es un ideal primo. Se emplea la notación $Q_{cl}(R) = Q_{\{0\}}(R)$.

Corolario 1.29. *$Q_{cl}(R)$ es un cuerpo.*

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 $A = Ae \oplus A(1-e)$, es decir, $A = Ae + A(1-e)$ y $\{0\} = Ae \cap A(1-e)$.

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 1.14.

Ejercicio 1.7. Demuestra la Proposición 1.17.

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. Demuestra el Teorema 1.18.

Ejercicio 1.11. Demuestra que $\langle p \rangle \subseteq \mathbb{Z}$ es un ideal primo si y solo si p es un número 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.

Ejercicio 1.13. Demuestra el Lema 1.24.

Ejercicio 1.14. Demuestra la Proposición 1.26.

Ejercicio 1.15. Demuestra la Proposición 1.27.

Bibliografía

[1] Thomas Becker, Volker Weispfenning, and Heinz Kredel. *Gröbner Bases. A Computational Approach to Commutative Algebra.* Number 141 in Graduate Texts in Mathematics. Springer Science+Business Media, 1993.

[2] David A. Cox, John Little, and Donald O'Shea. *Ideals, Varieties, and Algorithms.* Undergraduate Text in Mathematics. Springer, fourth edition, 2015.

[3] Ernst Kunz. *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, 1985.

[4] Serge Lang. *Undergraduate Algebra.* Undergraduate Text in Mathematics. Springer, second edition, 1990.