DOMINIOS DE DEDEKIND

MARIANO SUÁREZ-ALVAREZ

1. Estas notas siguen esencialmente la exposición del libro [1].

2. Sea A un dominio conmutativo y sea F su cuerpo de fracciones.

3. Un *ideal fraccionario* de A es un sub-A-módulo $I \subset F$ no nulo para el cual existe $a \in A$ tal que $aI \subset A$. Sea $\mathsf{Id}(A)$ el conjunto de ideales fraccionarios de A.

4. Es claro que todo ideal de A es un ideal fraccionario. En este contexto, llamamos a estos ideales *ideales enteros*.

5. Un ideal fraccionario $I \in \mathsf{Id}(A)$ es *principal* si existe $x \in F$ tal que $I = Ax$. Si I es entero, entonces es principal como ideal fraccionario sii es principal como ideal de A. Notamos $\mathsf{Prid}(A)$ al conjunto de los ideales principales de A.

6. Si $I, J \in \mathsf{Id}(A)$, entonces $IJ \in \mathsf{Id}(A)$. Dotado de esta operación, $\mathsf{Id}(A)$ es un semigrupo abeliano. Su elemento neutro es R. Es fácil ver que $\mathsf{Prid}(A)$ es un subgrupo de $\mathsf{Id}(A)$.

7. Decimos que A es un dominio de Dedekind si $\mathsf{Id}(A)$ es un grupo. Explícitamente, esta condición dice que para cada ideal fraccionario $I \in \mathsf{Id}(A)$, existe $I^{-1} \in \mathsf{Id}(A)$ tal que $II^{-1} = A$. Si ponemos $J = \{a \in A : aI \subset R\}$, entonces es $I^{-1} \subset J$ y $R = II^{-1} \subset IJ \subset R$, de manera que $IJ = R$. Usando esto, vemos que

$$I^{-1} = I^{-1}II^{-1} = I^{-1}IJ = J.$$

8. Supongamos desde ahora que A es un dominio de Dedekind.

9. Proposición. *Hay un isomorfismo de grupos* $\mathsf{Prid}(A) \cong F^\times / A^\times$.

Demostración. Si $I \in \mathsf{Prid}(A)$, existe $x \in F$ tal que $I = Ax$. Definimos $\phi : \mathsf{Prid}(A) \to F^\times / A^\times$ poniendo $\phi(I) = [x]$. □

10. El *grupo de clases de ideales* de A es el cociente $C(A) = \mathsf{Id}(A) / \mathsf{Prid}(A)$.

11. El uso de ideales fraccionarios es, en cierta forma, un recurso técnico:

Proposición. *Sea $\mathscr{I}(A)$ el conjunto de clases de isomorfismo de ideales de A. Entonces hay una biyección $C(A) \to \mathscr{I}(A)$.*

Demostración. Si $I \in \mathsf{Id}(A)$ y $a \in A$ son tales que $aI \subset A$, entonces el tipo de isomorfismo de aI depende únicamente de I: en efecto, $I \cong aI$ como A-módulo. Más aún, si $x \in F$ y $J = Rx$ es el ideal fraccionario principal correspondiente a x, entonces $I \cong IJ$. Esto nos dice que la aplicación $\phi : C(R) \to \mathscr{I}(A)$ tal que $\phi([I]) = [aI]$ está bien definida. Como todo ideal entero es un ideal fraccionario, ϕ es sobreyectiva. Veamos que es inyectiva.

Sean $I, J \in \mathsf{Id}(A)$ tales que $\phi([I]) = \phi([J])$. Entonces en particular es $I \cong J$ como A-módulos y existe un isomorfismo $f : I \to J$. Sea $x_0 \in I \setminus 0$. Si $x \in I$, entonces $xf(x_0) = f(xx_0) = x_0 f(x)$ en F. Luego $f(x) = xf(x_0)/x_0$ y vemos que $J = Iy$ con $y = f(x_0)/x_0$. Esto nos dice que $[I] = [J]$ en $C(A)$. □

Fecha: 11 de junio, 2007; compilado: 4 de julio de 2007.

12. Corolario. *Un dominio de Dedekind A es un dominio de ideales principales sii $C(A) = 1$.*

Demostración. En efecto, A es un dominio de ideales principales sii todos sus ideales enteros son isomorfismos a A. □ □

13. Proposición. *Si A es un dominio de Dedekind, todo ideal fraccionario de A es finitamente generado y proyectivo.*

Demostración. Sea $I \in \mathsf{Id}(A)$. Como $I^{-1}I = R$, existen $n \in \mathbb{N}$, $x_1, \dots, x_n \in I^{-1}$ e $y_1, \dots, y_n \in I$ tales que $\sum_{i=1}^n x_i y_i = 1$.

Consideremos el morfismo de A-módulos $\pi : (a_i)_{i=1}^n \in A^n \mapsto \sum_{i=1}^n a_i y_i \in I$. Si $a \in I$, entonces $ax_i \in R$ para todo $i \in \{1, \dots, n\}$ y $\pi((ax_i)_{i=1}^n) = \sum_{i=1}^n ax_i y_u = a\sum_{i=1}^n x_i y_i = a$. Esto nos dice que π es sobreyectivo. Más aun, π se parte: el morfismo $s : a \in I \mapsto (ax_i)_{i=1}^n \in A^n$ es una sección para π. □

14. Corolario. *Un dominio de Dedekind es nötheriano.* □

15. Teorema. *Sea A un dominio de Dedekind. Todo A-módulo proyectivo finitamente generado es isomorfo a una suma directa de ideales de A.*

Demostración. Basta mostrar, haciendo inducción sobre n, que

> Si $M \subset A^n$ es un sumando directo, entonces M es isomorfo a una suma directa de k ideales para cierto $k \leq n$.

Es claro que cuando $n = 0$ no hay nada que probar.

Sea entonces $M \subset A^n$ un sumando directo. Sea además $\pi : A^n \to A$ la última proyección. Si $M \subset \ker \pi$, entonces M es un sumando directo de $\ker \pi \cong A^{n-1}$ y podemos usar la hipótesis inductiva. Supongamos entonces que el ideal $I = \pi(M)$ es no nulo. Como I es proyectivo y $\pi|M : M \to I$ es sobreyectiva, vemos que $M \cong \ker \pi|_M \oplus I$. Además, $\ker \pi|_M$ es un sumando directo de A^{n-1}. Usando la hipótesis de inducción otra vez, vemos que $\ker \pi|_M$ es isomorfo a una suma directa de a lo sumo $n-1$ ideales de A. Esto implica que M mismo es suma directa de a lo sumo n ideales. □

16. Teorema. *Sea A un dominio de Dedekind.*

(a) Todo ideal primo no nulo de A es maximal.
(b) Todo ideal entero es producto de ideales primos de forma única (a menos de permutaciones entre los factores)
(c) El grupo abeliano $\mathsf{Id}(A)$ de ideales fraccionarios es libre. Una base es el conjunto de ideales primos.

Demostración. Sea I un ideal primo propio y no nulo. Supongamos que no es maximal, de manera que existe otro ideal J tal que $I \subsetneq J \subsetneq A$. Pongamos $K = J^{-1}I$. Es $K = J^{-1}I \subsetneq J^{-1}J = A$, así que K es propio. Por otro lado, como $JK = I$, I es primo y $J \not\subset I$, es $K \subset I$. Usando esto, vemos que

$$I = JK \subset JI \subsetneq AI = I$$

y esto es absurdo. Esta contradicción prueba la primera parte del teorema.

Para ver la existencia afirmada en la segunda parte, tenemos que mostrar que el conjunto $\mathscr{C}$ de los ideales enteros propios de A que no son productos finitos de ideales primos es vacío. Supongamos que este no es el caso.

Como A es nötheriano, existe entonces un elemento $I \in \mathscr{C}$ maximal. Como I mismo no puede ser primo, no es un ideal maximal, y entonces existe un ideal I_1 en A tal que $I \subsetneq I_1 \subsetneq A$. Pongamos $I_2 = II_1^{-1}$. Como $I \subsetneq I_1$, $I_1^{-1} \subsetneq I^{-1}$ y entonces $I_2 = II_1^{-1} \subsetneq II^{-1} = A$. Esto es, I_2 es un ideal entero propio. Por otro lado, como $I_1 \subsetneq A$, $I_1 I \subsetneq AI = I$, así que $I \subsetneq I_1^{-1}I = I_2$. La maximalidad de I

nos dice entonces que tanto I_1 como I_2 son productos finitos de ideales primos. Como $I = I_1 I_2$, esto es absurdo.

Para ver la unicidad, supongamos que m, $n \in \mathbb{N}$ son tales que $m \leq n$ y que $P_1, \dots, P_m$, $Q_1, \dots, Q_n$ son ideales primos propios no nulos de A tales que $P_1 \cdots P_m = Q_1 \cdots Q_n$. Multiplicando por inversos, podemos suponer que

$$\{P_i : 1 \leq i \leq m\} \cap \{Q_j : 1 \leq j \leq n\} = \varnothing.$$

Si $n > 1$, como $P_1 \supset P_1 \cdots P_m = Q_1 \cdots Q_n$ y P_1 es primo, podemos suponer sin pérdida de generalidad que $P_1 \supset Q_1$. Pero Q_1 es maximal y P_1 es propio, así que $P_1 = Q_1$, contra la hipótesis. Luego debe ser $n = m = 1$. Pero entonces $P_1 = Q_1$, lo que otra vez contradice la hipótesis.

Sea L el grupo abeliano libre con base en el conjunto de ideales primos propios y no nulos de A y sea $\phi : L \to \mathsf{Id}(A)$ el único morfismo de grupos tal que $\phi(P) = P$ para todo ideal primo P propio y no nulo.

Si $I \in \mathsf{Id}(A)$, existe $a \in A$ tal que $aI \subset A$ y entonces, usando la existencia de factorizaciones, existen ideales primos no nulos $P_1, \dots, P_n$ en A tales que $aI = P_1 \cdots P_n$. Además, existen ideales primos no nulos $Q_1, \dots, Q_m$ tales que $Aa = Q_1 \cdots Q_m$. Como

$$I = P_1 \cdots P_n Q_1^{-1} \cdots Q_m^{-1},$$

vemos que $I \in \operatorname{im} \phi$, esto es, que ϕ es sobreyectiva.

Supongamos finalmente que $x = \sum_{i=1}^n x_i P_i \in L$ es una combinación lineal finita con coeficientes enteros tal que $\phi(x) = A$. Entonces $\prod_{i=1}^n P_i^{x_i} = R$ y

$$\prod_{\substack{1 \leq i \leq n \\ x_i > 0}} P_i^{x_i} = \prod_{\substack{1 \leq i \leq n \\ x_i < 0}} P_i^{-x_i}.$$

Esto contradice la unicidad de la factorización en producto de primos. □

17. Lema.

(a) Si A es un anillo conmutativo arbitrario e I_1, $I_2 \subset A$ son ideales tales que $I_1 + I_2 = A$, entonces $I_1 I_2 = I_1 \cap I_2$.

(b) Si A es un dominio de Dedekind e I y J son un ideal fraccionario y un ideal entero de A, respectivamente, entonces existe $a \in I$ tal que $I^{-1}a + J = A$.

Demostración. (a) Evidentemente $I_1 I_2 \subset I_1 \cap I_2$. Si $a_1 \in I_1$ y $a_2 \in I_2$ son tales que $a_1 + a_2 = 1$, entonces para cada $x \in I_2 \cap I_2$, tenemos que $x = xa_1 + xa_2 \in I_2 I_1 + I_1 I_2 = I_1 I_2$.

(b) Supongamos que $P_1, \dots, P_n$ son ideales primos no nulos y distintos tales que existen $n_1, \dots, n_r \in \mathbb{N}$ con $J = P_1^{n_1} \cdots P_r^{n_r}$.

Sea $i \in \{1, \dots, r\}$. Como $IP_1 \cdots \hat{P}_i \cdots IP_r \subsetneq IP_1 \cdots P_r$, existe un elemento $a_i \in IP_1 \cdots \hat{P}_i \cdots IP_r \setminus IP_1 \cdots P_r$. Pongamos $a = \sum_{i=1}^r a_i$.

Es $a_i I^{-1} \subset P_j$ si $i \neq j$. Por otro lado, supongamos que $a_i I^{-1} \subset P_i$. Esto implica que

$$a_i I^{-1} \subset P_i \cap P_1 \cdots \hat{P}_i \cdots P_r = P_1 \cdots P_r,$$

lo que es absurdo. Luego $a_i I^{-1} \not\subset P_i$.

Esto nos dice que $aI^{-1} \not\subset P_i$ para ningún $i \in \{1, \dots, r\}$. Como $a \in I$, aI^{-1} es un ideal entero. Sea $aI^{-1} + J = Q_1 \dots Q_s$ la factorización como producto de ideales primos de $aI^{-1} + J$. Si $Q_1 = P_i$ para algún $i \in \{1, \dots, r\}$, entonces $aI^{-1} \subset aI^{-1} + J \subset P_i$, lo que es imposible. Por otro lado, $P_1^{n_1} \cdots P_r^{n_r} = J \subset aI^{-1} + J \subset Q_1$ así que existe $i \in \{1, \dots, r\}$ tal que $P_i \subset Q_1$. Como P_i es maximal, esto implica que $P_i = Q_1$, lo que otra vez es imposible.

Vemos así que en la factorización de $aI^{-1}+J$ no puede haber ningún factor. Esto es, $aI^{-1}+J=A$. □

18. Corolario. *Sea A un dominio de Dedekind. Entonces todo ideal fraccionario de A puede ser generado por dos elementos.*

Demostración. Sea $I \in \mathsf{Id}(A)$ y sea $a \in I \setminus 0$. Entonces aI^{-1} es un ideal entero y, por la segunda parte del lema, existe $b \in I$ tal que $aI^{-1}+bI^{-1}=A$. Multiplicando por I, vemos que $I = Aa + Ab$. □

19. Proposición. *Sea A un dominio de Dedekind y sean I_1, $I_2 \in \mathsf{Id}(A)$. Entonces hay un isomorfismo de A-módulos $I_1 \oplus I_2 \cong A \oplus I_1 I_2$.*

Demostración. Sea $a_1 \in I_1 \setminus 0$, de manera que $a_1 I_1^{-1}$ es un ideal entero. La segunda parte del lema muestra que existe $a_2 \in I_2$ tal que $a1I_1^{-1}+a_2I_2^{-1}=A$. Sean $b_1 \in I_1^{-1}$ y $b_2 \in I_2^{-1}$ tales que $1 = a_1b_1 + a_2b_2$. Entonces el morfismo

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in I_1 \oplus I_2 \mapsto \begin{pmatrix} b_1 & b_2 \\ -a_2 & a_1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in A \oplus I_1 I_2$$

tiene como inverso al morfismo

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in A \oplus I_1 I_2 \mapsto \begin{pmatrix} a_1 & -b_2 \\ a_2 & b_1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in I_1 \oplus I_2.$$

□

20. Teorema. *Sea A un dominio de Dedekind. Si M es un A-módulo proyectivo finitamente generado de rango k, entonces existe un ideal I tal que $M \cong A^{k-1} \oplus I$.*

Demostración. Sea M un A-módulo proyectivo finitamente generado de rango k. Usando **15** vemos que existen ideales $I_1, \dots, I_l$ tales que $M \cong I_1 \oplus \cdots \oplus I_l$. En particular, $k = \sum_{i=1}^{l} \mathsf{rk}_A I$. Pero $\mathsf{rk}_A I = \mathsf{dim}_F I \otimes_A F$ y $I \otimes_A F$ es un sub-F-espacio vectorial no nulo de $A \otimes_A F \cong F$, así que $\mathsf{rk}_A I = 1$. Esto nos dice que $l = k$.

Usando ahora **19**, vemos que $M \cong A^{k-1} \oplus I_1 \cdots I_k$. □

21. Lema. *Sea A un dominio nötheriano íntegramente cerrado en su cuerpo de fracciones F. Si $I \in \mathsf{Id}(A)$, entonces $\{a \in F : aI \subset I\} = A$.*

Demostración. Pongamos $B = \{a \in F : aI \subset I\}$. Claramente $A \subset B$. Sea $b \in B$. Como A es nötheriano, existe un conjunto finito $\{a_1, \dots, a_n\}$ que genera a I. Como $b \in B$, para cada $i \in \{1, \dots, n\}$ existen $b_{i,1}, \dots, b_{i,n} \in A$ tales que $ba_i = \sum_{j=1}^{n} b_{i,j} a_j$. Esto nos dice que, si $p \in A[X]$ es el polinomio característico de la matriz $(b_{i,j})$, entonces $p(b) = 0$. Pero p es mónico, así que b es entero sobre A. Como A es íntegramente cerrado, vemos que $b \in A$. □

22. Lema. *Sea A un anillo nötheriano y sea I un ideal no nulo propio en A. Entonces I contiene un producto no nulo de ideales primos.*

Demostración. Si el resultado es falso, existe un ideal I en A no nulo y maximal con respecto a la propiedad de no contener productos no nulos de ideales primos. Por supuesto, I no puede ser primo, así que existen $a, b \in A \setminus I$ tales que $ab \in I$.

Es claro que $I \subsetneq I + Aa$ y $I \subsetneq I + Ab$. Además, $I \subset (I + Aa)(I + Ab) = I + Aab \subset I$, así que $(I + Aa)(I + Ab) = I$.

Pero entonces, si fuese $I + Aa = A$, sería $I = (I + Aa)(I + Ab) = I + AB$, lo que es absurdo. Luego $I + Aa \subsetneq A$ y, similarmente, $I + Ab \subsetneq A$. La elección de I implica, entonces, que existen ideales primos $P_1, \dots, P_n$ y $Q_1, \dots, Q_n$ tales que $I + Aa \supset P_1 \cdots P_n \neq 0$ y $I + Ab \supset Q_1 \cdots Q_m \neq 0$. Esto es imposible, porque en ese caso

$$I = (I + Ra)(I + Rb) \supset P_1 \cdots P_n Q_1 \cdots Q_n \neq 0.$$

□

23. Lema. *Sea A un dominio nötheriano en el que todo ideal primo es maximal e I un ideal propio no nulo de A. Sea F el cuerpo de fracciones de A. Entonces existe $c \in F \setminus A$ tal que $cI \subset R$.*

Demostración. Sea $a \in I \setminus 0$. El lema anterior implica que existen primos $P_1, \dots, P_n$ tales que $Aa \supset P_1 \cdots P_n \neq 0$. Supongamos que n es el mínimo elemento de $\mathbb{N}$ con esta propiedad. Si P es un ideal maximal de A tal que $P \supset I$, es $P \supset P_1 \cdots P_n$. Podemos suponer entonces, sin pérdida de generalidad, que $P_1 \subset P$. La hipótesis implica que de hecho $P_1 = P$.

Si $n = 1$, entonces $P = I = Aa$ es maximal, así que $a^{-1} \in F \setminus A$ es tal que $a^{-1}I \subset R$.

Si $n > 1$, la elección de n implica que $P_2 \cdots P_n \not\subset Aa$, de manera que existe $b \in P_2 \cdots P_n \setminus Aa$. Pongamos $c = b/a$. Entonces $c \in F \setminus A$ y

$$cI \subset cP_1 = a^{-1}bP_1 \subset a^{-1}P_1 \cdots P_n \subset a^{-1}Aa = R.$$

□

24. Teorema. *Un dominio de integridad A es un dominio de Dedekind sii*

(i) *todo ideal primo no nulo es maximal;*
(ii) *A es íntegramente cerrado en su cuerpo de fracciones; y*
(iii) *A es nötheriano.*

Demostración. Para ver la necesidad, a esta altura alcanza con verificar la segunda condición. Sea entonces F el cuerpo de fracciones de A y $a \in F$ un elemento entero sobre A, de manera que existe un polinomio mónico $p = X^n + a_1X^{n-1} + \cdots + a_n \in A[X]$ tal que $p(a) = 0$.

Sea $M = \sum_{i=0}^{n-1} Aa^i$. Claramente se trata de un submódulo de F estable por la multiplicación por a. Si $a = \frac{p}{q}$ con $p, q \in A$, entonces $q^{n-1}M \subset A$ y vemos que $M \in \mathsf{Id}(A)$. Como $aM = M$, multiplicando por M^{-1} vemos que $aA \subset A$. En particular, $a \in A$.

Veamos ahora la suficiencia de las condiciones. Sea $I \in \mathsf{Id}(A)$ y pongamos $J = \{a \in A : aJ \subset A\}$.

Si $K = \{a \in A : aIJ \subset A\}$, entonces $A \supset K(IJ) = (KJ)I$. Luego $KJ \subset J$. Usando **21**, vemos que $K \subset A$. Por otro lado, si $IJ \subsetneq A$, **23** nos dice que existe $c \in F \setminus A$ tal que $cIJ \subset A$. Esto es imposible. □

Referencias

[1] J. Rosenberg, *Algebraic K-theory and its applications*, Graduate Texts in Mathematics, vol. 147, Springer-Verlag, New York, 1994. MR **1282290 (95e:**19001) ↑1

Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón I, Buenos Aires (1428) Argentina.
E-mail address: mariano@dm.uba.ar