DOMINIOS DE DEDEKIND

MARIANO SUÁREZ-ALVAREZ

Índice

1. Dominios de Dedekind

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

1.2. 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.

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

1.4. Un sub-A-módulo $I \subset A$ que es finitamente generado es un ideal fraccionario. En efecto, si $\{\frac{a_i}{b_i}\}_{i=1}^n$ es un conjunto finito de generadores no nulos, entonces $b = \prod_{i=1}^n \in A$ es tal que $bI \subset A$.

1.5. 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.

1.6. Lema. *Sean I, $I' \in \mathsf{Id}(A)$. Entonces $\mathsf{hom}_A(I, A) \cong \{a \in F : aI \subset A\}$ y $\mathsf{hom}_A(I, I') \cong \{a \in F : aI \subset I'\}$.*

Demostración. Escribamos $J = \{a \in F : aI \subset A\}$.

Sea $x_0 \in I \setminus 0$. Si $y \in I$, entonces $f(x_0)y = f(x_0 y) = x_0 f(y)$, de manera que $f(y) = yf(x_0)/x_0$. Vemos así que $\lambda_f = f(x_0)/x_0 \in J$ y que $f(y) = \lambda_f y$ si $y \in I$. La aplicación $\phi : f \in \mathsf{hom}_A(I, A) \mapsto \lambda_f \in J$ es claramente un morfismo de grupos inyectivo. Pero si $\lambda \in J$, $f_\lambda : y \in I \mapsto \lambda x \in A$ es un elemento de $\mathsf{hom}_A(I, A)$ tal que $\phi(f_\lambda) = \lambda$. Luego ϕ es un isomorfismo. Esto prueba la primera afirmación. La segunda es completamente similar. □

1.7. 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 $\mathsf{Id}(A)$.

1.8. Decimos que A es un dominio de Dedekind si $\mathsf{Id}(A)$ es un grupo. Explícitamente, esta condición dice que cada ideal fraccionario $I \in \mathsf{Id}(A)$ es inversible, esto es, existe $I^{-1} \in \mathsf{Id}(A)$ tal que $II^{-1} = A$.

1.9. Si suponemos que $I \in \mathsf{Id}(A)$ es inversible y ponemos $J = \{a \in F : aI \subset R\}$, entonces es $I^{-1} \subset J$ y $R = II^{-1} \subset IJ \subset R$, de manera que $IJ = R$. Usando esto, vemos que

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

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

Fecha: 11 de junio, 2007; compilado: 14 de mayo de 2015.

1.11. 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 $\phi(I) = [x]$. □

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

1.13. El uso de ideales fraccionarios es, en cierta forma, un recurso técnico conveniente para estudiar las clases de isomorfismo de ideales enteros:

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 $C(A)$. □

1.14. 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. □ □

1.15. 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. □

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

1.17. Como todo ideal de A es proyectivo, un teorema de I. Kaplansky [1] implica que todo submódulo de un A-módulo proyectivo es proyectivo. Necesitamos para nuestros propósitos solamente el siguiente caso particular:

Teorema. *Sea* A *un dominio de Dedekind y* $n \in \mathbb{N}$*. Si* M *es un submódulo de* A^n*, entonces* M *es isomorfo a una suma directa de ideales de* A*. En particular, todo* A*-módulo proyectivo finitamente generado es suma directa de ideales.*

Demostración. Basta mostrar, haciendo inducción sobre n, que

> Si $M \subset A^n$ es un submódulo, 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 submódulo. Sea además $\pi : A^n \to A$ la última proyección. Si $M \subset \ker \pi$, entonces M es un submódulo 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 submódulo 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. □

1.18. 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, …, 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, …, P_n en A tales que $aI = P_1 \cdots P_n$. Además, existen ideales primos no nulos Q_1, …, 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. □

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

Sea $i \in \{1, \ldots, r\}$. 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 $i \in \{1, \ldots, r\}$. Como $a \in I$, aI^{-1} es un ideal entero. Sea $aI^{-1} + J = Q_1 \ldots Q_s$ la factorización como producto de ideales primos de $aI^{-1} + J$. Si $Q_1 = P_i$ para algún $i \in \{1, \ldots, r\}$, 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 $i \in \{1, \ldots, r\}$ 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, $aI^{-1} + J = A$. □

1.20. Las dos afirmaciones de este lema son válidas en un dominio de ideales principales. De hecho, usándolas podemos ver que un dominio de Dedekind no está demasiado lejos de ese caso:

Corolario. *Sea A un dominio de Dedekind. Entonces todo ideal fraccionario de A puede ser generado por dos elementos. Más precisamente, si $I \in \mathsf{Id}(A)$ y $a \in I \setminus 0$, existe $b \in I$ tal que $I = Aa + Ab$.*

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 $I = Aa + Ab$. □

1.21. Este corolario nos permite ver fácilmente que un dominio de Dedekind es 'minimal' con respecto a la propiedad de poseer ideales no principales:

Corolario. *Sea A un dominio de Dedekind y $\mathfrak{a}$ un ideal propio no nulo de A. Entonces todo ideal de $A/\mathfrak{a}$ es principal.*

Demostración. Todo ideal de $A/\mathfrak{a}$ es de la forma $\mathfrak{b}/\mathfrak{a}$ para algún ideal $\mathfrak{b}$ de A tal que $\mathfrak{b} \supset \mathfrak{a}$. Además, $\mathfrak{b}/\mathfrak{a}$ es propio no nulo sii $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq A$.

El corolario **1.20** implica que existen elementos $a_1, a_2 \in \mathfrak{a}$ tales que $\mathfrak{a} = (a_1, a_2)$. Como $\mathfrak{a} \neq 0$, podemos suponer, sin pérdida de generalidad, que $a_1 \neq 0$. Como $a_1 \in \mathfrak{b}$, el mismo corolario nos dice que existe $b \in \mathfrak{b}$ tal que $\mathfrak{b} = (a_1, b)$. Pero entonces $\mathfrak{b}/\mathfrak{a}$ está generado por la clase de b módulo $\mathfrak{a}$. □

2. Módulos, I

2.1. Si R es un dominio de integridad y M es un R-módulo, el *submódulo de torsión $t(M)$ de M* es

$$t(M) = \{m \in M : \text{existe } r \in R \text{ tal que } rm = 0\}.$$

Es fácil ver que se trata, en efecto, de un submódulo. Decimos además que M *es libre de torsión* si $t(M) = 0$.

2.2. Lema. *Si R es un dominio de integridad y M es un R-módulo, $t(M/t(M)) = 0$.*

Demostración. Es claro que si $m \in M$ es tal que existe $r \in R$ con $rm \in t(M)$, entonces $m \in t(M)$. Esta afirmación es equivalente a la del lema. □

2.3. Sea R es un dominio de integridad y M un R-módulo. Decimos que un submódulo $N \subset M$ un *puro en M* si $rN = N \cap rM$ para todo $r \in R$.

2.4. La noción de pureza está íntimamente relacionada con la de torsión:

Proposición. *Sea R un dominio de integridad y M un R-módulo.*

(a) Si M es libre de torsión y $N \subset M$ es un submódulo puro en M, entonces M/N es libre de torsión.
(b) Si $N \subset M$ es un submódulo es tal que $t(M/N) = 0$, entonces N es puro en M. En particular, $t(M)$ es puro en M.

Demostración. (a) Esto sigue inmediatamente de la definición.

(b) Sea $N \subset M$ un submódulo tal que $t(M/N) = 0$, esto es, tal que si $m \in M$ es tal que existe $r \in R$ con $rm \in N$, entonces $m \in N$. Esto implica, inmediatamente, que $rM \cap N \subset rN$. Como la inclusión recíproca es siempre válida, esto prueba la primera afirmación. La segunda sigue de ella, teniendo en cuenta **2.2**. □

2.5. Proposición. *Sea R un dominio de integridad y M un R-módulo.*

(a) Todo sumando directo de M es puro en M.
(b) Si $N \subset M$ es un submódulo puro en M y $P \subset N$ es un submódulo puro en N, entonces P es un submódulo puro en M.
(c) Si $\{N_i\}_{i\in I}$ es una familia de submódulos puros en M, entonces $\bigcap_{i\in I} N_i$ es puro en M.
(d) Si $X \subset M$ es un subconjunto arbitrario, existe un menor submódulo $N \subset M$ puro en M tal que $X \subset N$.

Demostración. Dejamos esto como un sencillo ejercicio para el lector. □

2.6. Proposición. *Sea R un dominio de integridad y M un R-módulo finitamente generado, sin torsión y tal que $\mathsf{rk}_R M = 1$. Entonces existe un ideal fraccionario $I \in \mathsf{Id}(R)$ tal que $M \cong I$.*

Demostración. Sea F el cuerpo de fracciones de R, $m_0 \in M \setminus 0$ e

$$I = \{\tfrac{a}{b} \in F : a \in R,\ b \in R \setminus 0,\ am_0 \in bM\}.$$

Definimos una aplicación $\phi : M \to I$ de la siguiente manera. En primer lugar, ponemos $\phi(0) = 0$. Sea ahora $m \in M \setminus 0$. Como $\mathsf{rk}_R M = 1$, existen a, $b \in R$ tales que $am_0 = bm$ y $(a, b) \neq (0, 0)$. Como además M es libre de torsión, resulta que $ab \neq 0$. Podemos poner, entonces, $\phi(m) = a/b$.

Esto está bien definido, si a', $b' \in R$ son tales que también es $a'm_0 = b'm$, entonces $ab'm_0 = bb'm = ba'm_0$ y, como $m_0 \neq 0$, tenemos que $ab' = ba'$, esto es, $a/b = a'/b'$.

La aplicación ϕ es un morfismo de R-módulos:

- Sean $m \in M \setminus 0$ y $r \in R \setminus 0$. Si a, $b \in R$ son tales que $am_0 = bm$ y $ab \neq 0$, de manera que $\phi(m) = a/b$, entonces $arm_0 = brm$. La definición de ϕ implica entonces que $\phi(rm) = ar/b = r\phi(m)$.
- Sean m, $m' \in M \setminus 0$ y sean a, b, a', $b' \in R$ tales que $am_0 = bm$, $a'm_0 = b'm'$, $ab \neq 0$ y $a'b' \neq 0$, de manera que $\phi(m) = a/b$ y $\phi(m') = a'/b$.

  Si $m + m' = 0$, entonces $-am_0 = bm'$ y $\phi(m') = -a/b = -\phi(m)$, así que $\phi(m + m') = 0 = \phi(m) + \phi(m')$. Si por otro lado $m + m' \neq 0$, entonces como

$ab'm_0 = bb'm$ y $ba'm_0 = bb'm'$, es $(ab' + ba')m_0 = bb'(m + m')$ y

$$\phi(m + m') = (ab' + ba')/(bb') = \phi(m) + \phi(m').$$

Es claro que $\ker \phi = 0$. Por otro lado, la elección de I implica que ϕ es sobreyectiva, así que ϕ es un isomofismo de R-modulos. Como M es finitamente generado, I es es un submodulo de F finitamente generado y concluimos que $I \in \mathsf{Id}(A)$. □

2.7. Teorema. *Sea A un dominio de Dedekind y sea M un A-módulo finitamente generado. Entonces $t(M)$ es un sumando directo de M. Si M es libre de torsión, entonces es proyectivo.*

Demostración. Sea M un A-módulo finitemente generado libre de torsión. Mostremos que es proyectivo haciendo inducción sobre $\mathsf{rk}_A M$.

Si $\mathsf{rk}_A M = 1$, la proposición **2.6** nos dice que M es isomorfo a un ideal fraccionario y **1.15** implica entonces que es proyectivo.

Supongamos entonces que $\mathsf{rk}_A M > 1$ y sea $m \in M \setminus 0$. La proposición **2.5** nos dice que existe un menor submódulo $N \subset M$ tal que N es puro en M y $m \in M$. Sea $\pi : M \to M/Am$ la proyección canónica y $N' = \pi^{-1}(t(M/Am))$.

Como N es puro en M, $(M/Am)/(N/Am) \cong M/N$ es libre de torsión y entonces $N/Am \supset t(M/Am)$. Esto nos dice que $N \supset N'$. Por otro lado, evidentemente $Am \subset N'$ y

$$t(M/N') \cong t\Big(\frac{M/Am}{N'/Am}\Big) = t\Big(\frac{M/Am}{t(M/Am)}\Big) = 0,$$

así que N' es puro y la elección de N implica que $N \subset N'$. Vemos así que, de hecho, $N = N'$.

Si $N = M$, debe ser entonces $t(M/Am) = M/Am$ y, en consecuencia, es $\mathsf{rk}_A M = 1$, contradiciendo nuestra hipótesis. Entonces $N \subsetneq M$ y, por lo tanto, $0 < \mathsf{rk}_A N < \mathsf{rk}_A M$. En particular, es $\mathsf{rk}_A M/N < \mathsf{rk}_A M$. La hipótesis inductiva implica que N y M/N son proyectivos. Como entonces la sucesión exacta

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

se parte, $M \cong N \oplus M/N$ y concluimos que M es proyectivo, como queríamos. Esto prueba la segunda afirmación del teorema.

Sea ahora M un A-módulo finitamente generado arbitrario. Como hay una sucesión exacta

$$0 \longrightarrow t(M) \longrightarrow M \longrightarrow M/t(M) \longrightarrow 0$$

El cociente $M/t(M)$ es libre de torsión y finitamente generado, así que por lo ya hecho se trata de un módulo proyectivo. La sucesión exacta se parte entonces y vemos que $t(M)$ es un sumando directo de M □

2.8. Lema. *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 **1.19** muestra que existe $a_2 \in I_2$ tal que $a1I_1^{-1} + a_2 I_2^{-1} = A$. Sean $b_1 \in I_1^{-1}$ y $b_2 \in I_2^{-1}$ tales que $1 = a_1 b_1 + a_2 b_2$. 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

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

de manera que se trata de un isomorfismo. □

2.9. Proposición. *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 $M \cong A^{k-1} \oplus I$. La clase de isomorfismo de I depende únicamente de M.*

Demostración. Sea M un A-módulo proyectivo finitamente generado de rango k. Usando **1.17** vemos que existen ideales $I_1, \dots, I_l$ tales que $M \cong I_1 \oplus \cdots \oplus I_l$. En particular, $k = \sum_{i=1}^{l} \operatorname{rk}_A I$. Pero $\operatorname{rk}_A I = \dim_F I \otimes_A F$ y $I \otimes_A F$ es un sub-F-espacio vectorial no nulo de $A \otimes_A F \cong F$, así que $\operatorname{rk}_A I = 1$. Esto nos dice que $l = k$. Usando ahora varias veces **2.8**, vemos que $M \cong A^{k-1} \oplus I_1 \cdots I_k$. Podemos toman, entonces $I = I_1 \cdots I_k$.

Para ver la última afirmación, supongamos que I e I' son ideales de A tales que $A^{k-1} \oplus I \cong A^{k-1} \oplus I'$ y mostremos que $I \cong I'$. En vista de **1.6**, si $f : A^{k-1} \oplus I \to A^{k-1} \oplus I'$ es un isomorfismo, existe una matriz $M \in \mathsf{M}_k(F)$ inversible tal que f es la multiplicación a izquierda por M. En particular, f^{-1} es la multiplicación por M^{-1}. Sea $d = \det M$.

Ahora bien, si $x \in I$ y X es la matriz diagonal con coeficientes diagonales $1, \dots, 1, x$, entonces $MX : A^n \to A^{k-1} \oplus I'$, así que $\det MX \in I'$. Como además es $\det MX = xd$, vemos que $dI \subset I'$. Razonando de manera análoga con M^{-1}, concluimos que $dI = I'$ y, en definitiva, que $I \cong I'$. □

3. Módulos, II

3.1. Si A es un dominio de Dedekind, el grupo de clases de ideales $C(A)$ refleja — de alguna manera — la estructura multiplicativa de los ideales de A. En esta sección queremos mostrar que también provee información sobre los A-módulos. Necesitaremos antes algunas consideraciones de carácter general.

3.2. El siguiente lema generaliza la construcción usual de $\mathbb{Z}$ a partir de $\mathbb{N}_0$:

Lema. (Grothendieck) *Sea S un semigrupo abeliano. Existe un par $(G(S), \iota)$, en el que $G(S)$ es un grupo abeliano e $\iota : S \to G(S)$ un morfismo de semigrupos, tal que*

> *para cada morfismo de semigrupos $f : S \to H$ con valores en un grupo abeliano H, existe un único morfismo de grupos $\bar{f} : G(S) \to H$ tal que $\bar{f}\iota = f$.* (1)

El grupo $G(S)$ está generado por la imagen de ι y, de hecho, si $g \in G(S)$, existen $s, t \in S$ tales que $g = \iota(s) - \iota(t)$. Más aún, si $s, t \in S$, entonces $\iota(s) = \iota(t)$ sii existe $u \in S$ tal que $s + u = t + u$.

Demostración. Sea $X = S \times S$ y sea $\sim$ la relación sobre X tal que

$$(s, s') \sim (t, t') \iff \exists u \in S,\ s + t' + u = t + s' + u$$

Pongamos $G(S) = X/\sim$. Si $s, t \in S$, notemos $[s, t]$ a la clase de (s, t) en $G(S)$ y definamos $\iota : s \in S \mapsto [s, 0] \in G(S)$.

Es fácil ver que la operación

$$[s, s'] \cdot [t, t'] = [s + t, s' + t']$$

hace de $G(S)$ un grupo abeliano. El elemento neutro es la clase $[0, 0]$ y si $s, t \in S$, es $-[s, t] = [t, s]$. Claramente, además, ι resulta un morfismo de semigrupos con respecto a esta operación.

Es claro que el par $(G(S), \iota)$ satisface las condiciones del final del enunciado, así que tenemos que mostrar solamente que tambien satisface a (1). Sea entonces $f : S \to H$ un morfismo de semigrupos con valores en un grupo abeliano H. Definimos $\bar{f} : G(S) \to H$ poniendo $\bar{f}([s, t]) = f(s) - f(t)$. La definición de $G(S)$ y de ι implican inmediatamente que $\bar{f}$ es un morfismo de grupos y que $\bar{f}\iota = f$.

Finalmente, como $\operatorname{im}\iota$ genera a $G(S)$ como grupo, $\bar{f}$ es está unívocamente determinado. □

3.3. Hay varias otras formas de construir el par $(G(S), \iota)$ del lema, pero todas dan esencialmente el mismo resultado:

Lema. *Sea S un semigrupo abeliano y sean (G, ι) y (G', ι') dos pares que satisfacen la condición* (1). *Entonces existe un único isomorfismo $h : G' \to G$ tal que $\iota h = \iota'$.*

Demostración. Dejamos esto como un ejercicio para el lector. □

3.4. Por ejemplo, si $\mathbb{N}_0$ es el semigrupo aditivo de los enteros no negativos, entonces el par $(\mathbb{Z}, i)$, en el que $i : \mathbb{N}_0 \hookrightarrow \mathbb{Z}$ es la inclusión, tiene la propiedad (1). En particular, $G(\mathbb{N}_0) \cong \mathbb{Z}$.

3.5. Sea R un anillo arbitrario y sea $\mathsf{proj}(R)$ el conjunto de clases de isomorfismo de R-módulos (izquierdos) proyectivos finitamente generados. Si P es un R-módulo proyectivo, escribimos $[P]$ a su clase de isomorfismo.

El conjunto $\mathsf{proj}(R)$ es un semigrupo abeliano con respecto a la operación $+$ inducida por la suma directa. Explícitamente, si $[P]$, $[Q] \in \mathsf{proj}(R)$, ponemos $[P] + [Q] = [P \oplus Q]$; es claro que esto es, en efecto, una operación en $\mathsf{proj}(R)$ que resulta asociativa y conmutativa y que tiene a la clase $[0]$ del módulo nulo como elemento neutro.

Si R' es otro anillo y $f : R \to R'$ es un morfismo de anillos, entonces la función

$$\mathsf{proj}(f) : [P] \in \mathsf{proj}(R) \mapsto [R' \otimes_R P] \in \mathsf{proj}(R')$$

está bien definida y es un morfismo de semigrupos. Es fácil ver que obtenemos así un functor $\mathsf{proj} : \mathsf{Rng} \to \frac{1}{2}\mathsf{Ab}$ de la categoría de los anillos a la de los semigrupos abelianos.

3.6. Notemos $K_0(R)$ al grupo abeliano $G(\mathsf{proj}(R))$ construido a partir del semigrupo $\mathsf{proj}(R)$ como en el lema **3.2**. Si P es un R-módulo proyectivo finitamente generado, escribiremos $[\![P]\!]$ a la imagen de $[P] \in \mathsf{proj}(R)$ en $K_0(R)$ bajo el morfismo $\mathsf{proj}(R) \to K_0(R)$.

Por otro lado, si R' es otro anillo y $f : R \to R'$ es un morfismo de anillos, notemos $K_0(f) : K_0(R) \to K_0(R')$ al morfismo inducido sobre $K_0(R) = G(\mathsf{proj}(R))$ por la composición

$$\mathsf{proj}(R) \xrightarrow{\mathsf{proj}(f)} \mathsf{proj}(R') \longrightarrow G(\mathsf{proj}(R')) = K_0(R')$$

Es fácil ver $K_0 : \mathsf{Rng} \to \mathsf{Ab}$ es un functor de la categoría de la categoría de los anillos a la de los grupos abelianos.

3.7. El teorema de estructura de módulos finitamente generados sobre un dominio de ideales principales R nos permite determinar fácilmente a $K_0(R)$:

Proposición. *Sea R un dominio de ideales principales. Entonces hay un isomorfismo de grupos abelianos $K_0(R) \cong G(\mathbb{N}_0) \cong \mathbb{Z}$ y, bajo este isomorfismo, a la clase $[\![R]\!] \in K_0(R)$ del R-módulo libre de rango uno corresponde $1 \in \mathbb{Z}$.*

Demostración. Como R es un dominio de ideales principales, todo R-módulo proyectivo finitamente generado es libre. Esto nos dice que $\mathsf{proj}(R) = \{[R^n] : n \in \mathbb{N}_0\}$. Más aún, es fácil ver que la aplicación $[R^n] \in \mathsf{proj}(R) \mapsto n \in \mathbb{N}_0$ es un isomorfismo de semigrupos. Luego $K_0(R) = G(\mathsf{proj}(R)) \cong G(\mathbb{N}_0) \cong \mathbb{Z}$. □

3.8. En particular, esta proposición nos dice que $K_0(\mathbb{Z})$ es un grupo abeliano libre generado por la clase $[\![\mathbb{Z}]\!]$ del $\mathbb{Z}$-módulo libre de rango uno. Desde ahora consideraremos este isomorfismo como una identificación.

3.9. Si R es un anillo cualquiera, existe exactamente un morfismo de anillos $\varepsilon : \mathbb{Z} \to R$ que induce un morfismo de grupos $K_0(\varepsilon) : \mathbb{Z} = K_0(\mathbb{Z}) \to K_0(R)$. Notamos $\tilde{K}_0(R) = \operatorname{coker} K_0(\varepsilon)$.

3.10. Proposición. *Sea R un anillo conmutativo. Supongamos que se trata de un dominio de integridad. Entonces existe un morfismo de grupos $r : K_0(R) \to \mathbb{Z}$ tal que $r \circ K_0(\varepsilon) = \mathsf{id}_{\mathbb{Z}}$. En particular, $K_0(R) \cong \mathbb{Z} \oplus \tilde{K}_0(R)$.*

Demostración. Sea F el cuerpo de fracciones de R y sea $r : \operatorname{proj}(R) \to \mathbb{Z}$ tal que si P es un R-módulo proyectivo finitamente generado, es $r([P]) = \dim_F P \otimes_R F$. Esto está bien definido y es, de hecho, un morfismo de semigrupos. Usando **3.2**, vemos que r induce un morfismo de grupos $K_0(R) \to \mathbb{Z}$, que notamos también r. Un cálculo directo muestra que $r(K_0(\varepsilon)(1)) = 1$, así que $r \circ K_0(\varepsilon) = \mathsf{id}_{\mathbb{Z}}$. □

3.11. En las condiciones de **3.10**, el subgrupo $\tilde{K}_0(R)$ puede identificarse con $\ker r$ y todos sus elementos son de la forma $[\![P]\!] - [\![P]\!]'$ de $K_0(R)$ con P y P' dos R-módulos proyectivos finitamente generados del mismo rango. En efecto, si $[\![P_1]\!], \dots, [\![P_l]\!] \in K_0(R)$ y $n_1, \dots, n_l \in \mathbb{Z}$ son tales que $u = \sum_{i=1}^{l} n_i [\![P_i]\!] \in \tilde{K}_0(R)$, entonces

$$u = \Big[\!\!\Big[\bigoplus_{\substack{1 \le i \le l \\ n_i > 0}} P_i^{n_i} \Big]\!\!\Big] - \Big[\!\!\Big[\bigoplus_{\substack{1 \le i \le l \\ n_i < 0}} P_i^{n_i} \Big]\!\!\Big].$$

Como $r(u) = 0$, las dos sumas directas que aparecen en esta expresión tienen el mismo rango.

3.12. Teorema. *Sea A un dominio de Dedekind. Hay un isomorfismo $\tilde{K}_0(A) \cong C(A)$.*

Demostración. Si P y P' son A-módulos proyectivos finitamente generados del mismo rango k, entonces existen ideales I e I' de A tales que $P \cong A^{k-1} \oplus I$ y $P' \cong A^{k-1} \oplus I'$. Definimos $\phi : \tilde{K}_0(A) \to C(A)$ poniendo $\phi([\![P]\!] - [\![P]\!]') = II'^{-1}$. Esto tiene sentido porque todo elemento de $\tilde{K}_0(A)$ es de la forma $[\![P]\!] - [\![P]\!]'$ pero tenemos que mostrar que está bien definido.

Sean entonces Q y Q' otros dos A-módulos proyectivos finitamente generados del mismo rango l y J y J' ideales tales que $Q \cong A^{l-1} \oplus J$ y $Q' \cong A^{l-1} \oplus J'$. Supongamos que $[\![P]\!] - [\![P']\!] = [\![Q]\!] - [\![Q']\!]$. Existe entonces un A-módulo proyectivo finitamente generado R tal que $P \oplus Q' \oplus R \cong P' \oplus Q' \oplus R$. Si K es un ideal de A tal que $R \cong A^s \oplus K$, entonces tenemos que

$$\begin{aligned} A^{k+l+s-2} \oplus IJ'K &\cong A^{k-1} \oplus I \oplus A^{l-1} \oplus J' \oplus A^s \oplus K \\ &\cong A^{k-1} \oplus I' \oplus A^{l-1} \oplus J \oplus A^s \oplus K \\ &\cong A^{k+l+s-2} \oplus I'JK, \end{aligned}$$

así que $IJ'K \cong I'JK$. Multiplicando por $I'^{-1}J'^{-1}K^{-1}$, vemos que $II'^{-1} \cong JJ'^{-1}$. Esto muestra que nuestra aplicación ϕ está bien definida, como queríamos.

Para ver que ϕ es un isomorfismo, damos un morfismo inverso. Definamos $\psi : C(A) \to \tilde{K}_0(A)$ de manera que si $I \in \mathsf{Id}(A)$, entonces $\psi([I]) = [\![I]\!] - [\![A]\!]$. Claramente si I es principal es $[\![I]\!] = [\![A]\!]$, así que esto está bien definido. Que ψ y ϕ son inversos sigue de un cálculo directo, que omitimos. □

3.13. Además del isomofismo del teorema, hay un isomorfismo

$$[\![P]\!] \in K_0(A) \mapsto (k, [I]) \in \mathbb{Z} \oplus C(A)$$

si $P \cong A^{k-1} \oplus I$ con $I \in \mathsf{Id}(A)$. Dejamos la verificación de esto al lector.

4. La caracterización de Noether

4.1. 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 $b \in A$. □

4.2. 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

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

4.3. 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 **4.2** 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

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

4.4. 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 **4.1**, vemos que $K \subset A$. Por otro lado, si $IJ \subsetneq A$, **4.3** nos dice que existe $c \in F \setminus A$ tal que $cIJ \subset A$. Esto es imposible. □

Referencias

[1] I. Kaplansky, *Modules over Dedekind rings and valuation rings*, Trans. Amer. Math. Soc. **72** (1952), 327–340. MR0046349 (13,719e) ↑2

[2] J. Rosenberg, *Algebraic K-theory and its applications*, Graduate Texts in Mathematics, vol. 147, Springer-Verlag, New York, 1994. MR1282290 (95e:19001) ↑

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