Algunas caracterizaciones de los DIP's

Facultad de Ciencias UNAM

Introducción

Hace dos secciones introducimos a los DIP's y vimos que gozan de un montón de propiedades interesantes. Por eso, en esta sección presentamos tres caracterizaciones de los DIP's.

Proposición 1

Supongamos que R es un dominio entero. Si todo ideal primo en R es principal, entonces R es un DIP.

Demostración. Supongamos que todo ideal primo en R es principal y procedamos por contradicción, es decir, también supongamos que

$$\mathfrak{U} := \{I \subset R \mid I \text{ es un ideal no principal de } R\} \neq \emptyset.$$

Usando el Lema de Zorn y el hecho de que $\bigcup_{I \in \mathcal{C}} I$ es un ideal cuando $\mathcal{C}$ es una cadena de ideales (respecto a la inclusión)[1], concluimos que $\mathfrak{U}$ tiene un elemento maximal I.

Ahora bien, como $I \in \mathfrak{U}$ y todo ideal primo en R es principal, entonces I no es primo. Es decir, existen $a, b \in R$ tales que $ab \in I$, $a \notin I$, y $b \notin I$.

[1] Esto es fácil de verificar pero recuerda que también lo vimos en la sección 1.11.

Sean

$$I_a := (I \cup \{a\}), \;\; I_b := (I \cup \{b\}), \;\; J := \{r \in R \mid rI_a \subset I\}$$

Veamos que

1. I_a es principal.
2. J es principal.
3. $I_a J$ es principal.
4. $I_a J = I$.

Claramente, el inciso (4) contradice el hecho de que I no es principal y por lo tanto, si probamos esto, ya acabamos.

Demostración de 1,2,3,4

1. Como $a \notin I$, entonces $I \subsetneq I_a$ y por lo tanto, como I es maximal en $\mathfrak{U}$, entonces $I_a \notin \mathfrak{U}$. En particular, I_a es principal, digamos $I_a = (\alpha)$.
2. Por un razonamiento análogo al del inciso anterior, basta demostrar que $I_b \subset J$. Para esto, supongamos que $x \in I_b$. Entonces por definición de I_b existen $i \in I$, $r, s \in R$ tales que $x = r_i + sb$. Para ver que $x = r_i + sb \in J$ necesitamos ver que $(r_i + sb)I_a \subset I$.

Por eso, sea $y \in I_a$. Por definición de I_a, existen $i' \in I$, $r', s' \in R$ tales que $y = r'i' + s'a$. Luego,

$$(r_i + sb)y = (r_i + sb)(r'i' + s'a) = rir'i' + ris'a + sbr'i' + sbs'a$$

Como I es ideal, es claro que los primeros tres sumandos pertenecen a I; el cuarto sumando pertenece porque $ab \in I$, $sbs'a = (ss')(ab)$, e I es ideal. Por lo tanto, $I_b \subset J$ y J es un ideal principal.

3. Esto es consecuencia inmediata de los dos incisos anteriores.
4. La inclusión $I_a J \subset I$ es consecuencia inmediata de la definición de J. Para la inclusión conversa, supongamos que $x \in I$, entonces como $I \subset I_a = (\alpha)$, existe $k \in R$ tal que $x = k\alpha$. Veamos que $k \in J$, es decir, veamos que $kI_a \subset I$. Sea $y \in kI_a$, entonces $y = k(ri + sa)$ para algunas $i \in I$, $r, s \in R$. Por otro lado, como $a \in I_a = (\alpha)$, entonces existe $l \in R$ tal que $a = l\alpha$. Por lo tanto,

$$y = kri + ksa = kri + ksl\alpha = kri + sl(k\alpha) = kri + slx \in I$$

donde la pertenencia se cumple porque I es ideal y $i, x \in I$.

$\square$

Dominio de Bezout

Definición

Supongamos que R es un dominio entero. Decimos que R es un **dominio de Bezout** si todo ideal generado por 2 elementos es principal. En otras palabras, R es un dominio de Bezout si para toda $a, b \in R$ existe $d \in R$ tal que $(a, b) = (d)$.

DIP $\iff$ DFU y Bezout

Proposición 2

Supongamos que R es un dominio entero. Entonces R es un DIP si y solo si R es DFU y de Bezout.

Demostración.
$\implies$) Obviamente todo DIP es un dominio de Bezout y en la sección anterior demostramos que DIP $\implies$ DFU.
$\impliedby$) Supongamos que R es DFU y de Bezout. Si $x \in R \setminus \{0\}$ es no invertible y $x = q_1 \cdots q_m$ es una factorización en primos de x, entonces (por la unicidad de la factorización) podemos definir

$$N(x) \coloneqq m = \text{el numero de primos en la factorización de } x$$

Ahora bien, para ver que R es DIP, supongamos que $I \neq 0$ es un ideal no trivial de R. Entonces $I \neq R$ y por lo tanto todo elemento de I es no invertible. Luego, por el axioma del buen orden podemos encontrar $a \in I$ tal que $N(a) \leq N(x)$ para toda $x \in I$.

Veamos que $I = (a)$. Como $a \in I$, la inclusión "$\supset$" es inmediata. Para ver "$\subset$", supongamos que $b \in I$. Como R es de Bezout, existe $d \in R$ tal que $(a, b) = (d)$. En particular, $d|a$ y por lo tanto, si

$$a = p_1^{k_1} \cdots p_n^{k_n}$$

es una factorización en primos[2] de a con $p_i \neq p_j$ para $i \neq j$, entonces (por la proposición 1.20.2.)

$$d = up_1^{l_1} \cdots p_n^{l_n} \tag{1}$$

con $u \in R$ invertible y $l_i \leq k_i$ para toda $i \in \{1, \dots, n\}$. Ahora bien, como $d \in (d) = (a, b) \subset^3 I$, entonces por la minimalidad de a tenemos que

$$k_1 + \cdots + k_n = N(a) \leq N(d) = l_1 + \cdots + l_n \tag{2}$$

De donde $l_i = k_i$ para toda $i \in \{1, \dots, n\}$.

---

[2] La cual existe porque $a \in I$ implica que a no es invertible (de lo contrario, tendríamos $I = R$).

[3] $a, b \in I$.

En efecto, si $l_j \neq k_j$ para alguna $j \in \{1, \ldots, n\}$, entonces (como $l_i \leq k_i$ para toda $i \in \{1, \ldots, n\}$) tendríamos $l_j < k_j$ y por lo tanto (sumando las desigualdades $l_i \leq k_i$ y $l_j < k_j$)

$$l_1 + \cdots + l_n < k_1 + \cdots + k_n$$

contradiciendo (2).

Juntado esto con (1) obtenemos que $d = ua$ y por lo tanto (como u es invertible) $(d) = (a)$. Pero entonces, $b \in (a, b) = (d) = (a)$. Como b era un elemento arbitrario de I, entonces $I \subset (a)$ y por lo tanto $I = (a)$. Finalmente, como I era un ideal arbitrario de R, entonces R es un DIP.

$\square$

Norma de Dedekind-Hasse

Acabamos esta sección dando una caracterización de los DIP's que usaremos para demostrar que

$$\text{Dominio euclidiano} \not\Leftarrow \text{DIP}$$

Para esto, necesitamos la siguiente definición.

Definición

Supongamos que R es un anillo conmutativo y que N es una norma en R. Decimos que N es una **norma de Dedekind-Hasse** si N es positiva[4] y se cumple la siguiente condición

$$\forall a, b \in R \left(a \notin (b) \implies \exists x \in (a, b) \setminus \{0\} \left(N(x) < N(b) \right) \right). \tag{3}$$

[4] Es decir, $N(x) > 0$ para toda $x \neq 0$.

DIP $\iff$ existe una norma de Dedekind-Hasse

Proposición 3

Supongamos que R es un dominio entero. Entonces, R es un DIP si y solo si R tiene una norma de Dedekind-Hasse.

Demostración.

$\Longleftarrow$) Supongamos que R tiene una norma N de Dedekind-Hasse y que $I \neq 0$ es un ideal en R. Por el axioma del buen orden, podemos encontrar $b \in I$ tal que $N(b) \leq N(x)$ para toda $x \in I$. Veamos que $I = (b)$. Por supuesto, basta probar "$\subset$". Para esto, supongamos que $a \in I$. Para ver que $a \in (b)$, supongamos lo contrario, es decir, que $a \notin (b)$. El hecho de que N sea de Dedekind-Hasse implica que existe $x \in (a, b) \setminus \{0\}$ tal que $N(x) < N(b)$. Sin embargo, como $a, b \in I$, entonces $(a, b) \subset I$ y por lo tanto, la existencia de x contradice nuestra elección de b.

$\Longrightarrow$) Supongamos que R es un DIP. Entonces R también es un DFU y por lo tanto (por la unicidad de las factorizaciones) podemos definir

$$N(x) := \begin{cases} 0 & \text{si } x = 0 \\ 1 & \text{si } x \text{ es invertible} \\ 2^n & \text{si } x = p_1 \cdots p_n \text{ es una factorización en primos de } x \end{cases}$$

Claramente $N(x) \geq 0$ para toda $x \in R$ y es fácil verificar que $N(xy) = N(x)N(y)$ para toda $x, y \in R$.

Veamos que N es una norma de Dedekind-Hasse. Supongamos que $a, b \in R$ son tales que $a \notin (b)$. Como R es DIP, $(a, b) = (x)$ para alguna $x \in R$. Entonces $x \notin (b)$ porque de lo contrario, $(x) \subset (b)$ y como $a \in (a, b) = (x)$, tendríamos $a \in (b)$.

Por otro lado, como $b \in (a, b) = (x)$, entonces existe $k \in R$ tal que $kx = b$. Además, k no es invertible porque de lo contrario, tendríamos $x \in (b)$. Finalmente, notemos que

$$N(x) < N(x)N(k) = N(xk) = N(b)$$

donde la desigualdad se cumple porque k no es invertible y por la definición de N. Por lo tanto N satisface la condición (3) y N es de Dedekind-Hasse.

$\square$

Una aplicación de esta caracterización es que $\mathcal{O}(-19) = \mathbb{Z}[(1 + \sqrt{-19})/2]$ es un DIP. Se puede demostrar que N_{-19} es una norma de Dedekind-Hasse. Sin embargo, omitiremos esta demostración porque es larga, tediosa, y usa técnicas que no volveremos a usar. Al lector interesado, lo referimos a la pagina 282 del libro Dummit y Foote.