Dominios de ideales principales

Facultad de Ciencias UNAM

Introducción

En la sección anterior vimos que todos los ideales de un dominio euclidiano son principales. En esta sección estudiamos a los anillos que tienen esta propiedad. En particular, todos las propiedades que gocen estos anillos, también las gozan los dominios euclidianos.

Dominios de ideales principales

Definición

Supongamos que R es un dominio entero. Decimos que R es un **dominio de ideales principales** (abreviado **DIP**) si todo ideal en R es principal.

Observación

Por lo mencionado en la introducción, con esta terminología tenemos que

$$\text{Dominio euclidiano} \implies \text{DIP}.$$

Sin embargo, pronto veremos que la implicación conversa no es cierta.

En la siguiente proposición enunciamos las propiedades básicas de los máximos comunes divisores en los DIP's. Esta proposición es idéntica[1] a el corolario 1.17.2. De hecho, es fácil verificar que la demostración de este corolario sigue sirviendo[2].

[1] Si cambiamos "dominio euclidiano" por "DIP".

[2] Solo ocupamos la existencia de una d tal que $(d) = (a, b)$. Recordemos que el algoritmo de la división dice que r_{n-1} cumple lo deseado.

El máximo común divisor en un DIP

Proposición 1

Supongamos que R es un DIP y $a, b \in R$ con $b \neq 0$. Entonces

1. a y b tienen un máximo común divisor d (la $d \in R$ tal que $(a, b) = (d)$ que existe porque R es DIP).
2. En un DIP *si* se vale la equivalencia

$$d' \text{ es un máximo común divisor de } a \text{ y } b \iff (d') = (a, b).$$

3. Si d' es un máximo común divisor de a y b, entonces d' puede ser escrito como R-combinación lineal de a y b. Específicamente, existen $x, y \in R$ tales que

$$d = ax + by.$$

El mínimo común múltiplo en un DIP

Corolario 2

Supongamos que R es un DIP y $a, b \in R \setminus \{0\}$

1. a y b tienen un mínimo común múltiplo en R.
2. Si d es un mcd de a y b, entonces $\frac{ab}{d}$ es un mcm de a y b.

Demostración.

1. Considera el ideal $(a) \cap (b)$. Como R es DIP, entonces existe $e \in R$ tal que $(a) \cap (b) = (e)$. Por la caracterización en términos de ideales de los mcm's, tenemos que e es un mínimo común múltiplo de R.
2. Para empezar, las igualdades $\frac{ab}{d} = a\frac{b}{d}$ y $\frac{ab}{d} = b\frac{a}{d}$ implican que $\frac{ad}{b}$ es múltiplo de a y b respectivamente. Para ver que es el mínimo común, supongamos que e es un múltiplo común de a y b. Queremos ver que $\frac{ab}{d} | e$ o equivalentemente, $ab | de$.

Para ver esto, recordemos que
(i) Como R es un DIP y d es máximo común divisor de a y b, entonces podemos escribir

$$d = ax + by$$

para algunas $x, y \in R$.

(ii) Como e es múltiplo común de a y b, entonces $e = az$ y $e = bw$ para algunas $z, w \in R$.

Por lo tanto,

$$de = (ax + by)e = axe + bye = ax(bw) + by(az) = ab(xw + yz)$$

Es decir, $ab|de$.

□

Una curiosidad de la divisibilidad en los DIP's

Proposición 3

Supongamos que R es un DIP, que $a, b \in R \setminus \{0\}$, y que $c \in R$. Si $a|bc$, entonces $\frac{a}{d}|c$ donde d es un máximo común divisor de a y b. En particular, si R tiene 1 y a, b son primos relativos, entonces $a|bc$ implica $a|c$.

Demostración. Supongamos que $a|bc$, es decir, existe $k \in R$ tal que $ak = bc$. Como R es DIP, podemos escribir a cualquier máximo común divisor de a y b como R-combinación lineal de a y b. Por lo tanto, podemos escribir

$$d = xa + yb = x\left(d\frac{a}{d}\right) + y\left(d\frac{b}{d}\right) = d\left(x\frac{a}{d} + y\frac{b}{d}\right)$$

para algunas $x, y \in R$.

Ahora bien, como R es un dominio euclidiano, en particular es un dominio entero; por lo tanto[3], la ecuación anterior implica

$$1 = x\frac{a}{d} + y\frac{b}{d}$$

Multiplicando por c obtenemos la primera de las siguientes igualdades (para justificar las siguientes recuerda que $ak = bc$ y recuerda que en la sección 1.15 justificamos las igualdades $c\frac{b}{d} = \frac{bc}{d}$ y $\frac{ak}{d} = k\frac{a}{d}$).

$$\begin{aligned} c = cx\frac{a}{d} + cy\frac{b}{d} = cx\frac{a}{d} + y\frac{bc}{d} = cx\frac{a}{d} + y\frac{ak}{d} &= cx\frac{a}{d} + ky\frac{a}{d} \\ &= \frac{a}{d}(cx + ky) \end{aligned}$$

□

[3]Recordemos que en un dominio euclidiano podemos cancelar factores no nulos.

Un DIP que no es un dominio euclidiano

Corolario 4

Dominio euclidiano $\not\Leftarrow$ DIP

Primero recuerda que en la sección anterior demostramos que

$$\mathcal{O}(-19) = \mathbb{Z}[(1+\sqrt{-19})/2]$$

no es un dominio euclidiano.

En la sección 1.21 demostraremos una caracterización de los DIP's que nos permitirá ver que $\mathcal{O}(-19)$ es un DIP. Sin embargo, hasta ahí llegaremos porque la demostración de que $\mathcal{O}(-19)$ satisface la caracterización, es muy tediosa.

En un DIP, primo $\iff$ irreducible

Proposición 5

Supongamos que R es un DIP. Si $p \in R$, entonces,

$$p \text{ es primo} \iff p \text{ es irreducible.}$$

Demostración. Antes que nada, recuerda que en un dominio entero, primo $\implies$ irreducible (c.f. proposición 1.16.3) y por lo tanto, basta demostrar (que en un DIP) irreducible $\implies$ primo.

Supongamos que p es irreducible y veamos que (p) es maximal.

De esta manera, tendremos que (en particular) (p) es un ideal primo[4] y por lo tanto, p es primo.

Para ver que (p) es maximal, supongamos que I es un ideal en R tal que $(p) \subsetneq I \subset R$. Como R es un DIP, existe $a \in I$ tal que $I = (a)$ y por lo tanto, tenemos

$$p \in (p) \subsetneq I = (a).$$

En particular, también existe $b \in R$ tal que $p = ab$. Como p es irreducible, la igualdad anterior implica que a es invertible o b es invertible. Si b es invertible, entonces $a = pb^{-1} \in (p)$ y por lo tanto, $(a) \subset (p)$. Contradiciendo $(p) \subsetneq (a)$. Por lo tanto, debe ser a invertible, y en este caso tenemos $I = (a) = R$. Es decir, el único ideal de R que contiene propiamente a (p) es R mismo. $\square$

[4]Recuerda que en un anillo conmutativo con 1, ideal maximal $\implies$ ideal primo (c.f. proposición 1.12.2).

En un DIP, ideal primo $\iff$ ideal maximal

Proposición 6

Supongamos que R es un DIP. Si I es un ideal de R, entonces

$$I \text{ es primo en } R \iff I \text{ es maximal en } R.$$

Demostración. De nuevo, recordemos que en la proposición 1.12.2 vimos que en un anillo conmutativo con 1, ideal maximal $\implies$ ideal primo. Por lo tanto, basta probar la implicación conversa.

Supongamos que I es un ideal primo no trivial de R. Para ver que es maximal, supongamos que J es un ideal de R tal que $I \subsetneq J$ y veamos que $J = R$. Como R es un DIP, entonces existen $p, q \in R$ tales que $I = (p)$ y $J = (q)$. Por lo tanto, tenemos

$$(p) = I \subsetneq J = (q)$$

o equivalentemente, $qx = p$ para alguna $x \in R$. Como $I = (p)$ es primo y $qx = p \in (p)$, entonces $q \in (p)$ o $x \in (p)$. En caso de que $q \in (p)$, entonces $(q) \subset (p)$ y por lo tanto, $(p) = (q)$, contradiciendo $(p) \subsetneq (q)$.

Por lo tanto, debemos tener $x \in (p)$. Entonces existe $y \in R$ tal que $x = py$. Usando esto y que $qx = p$ obtenemos

$$p = qx = q(py) = p(qy)$$

lo cual implica[5] que $qy = 1$. Pero entonces, $1 = qy \in (q)$, o equivalentemente $J = (q) = R$. □

[5] De nuevo, recordemos que en dominios enteros podemos cancelar factores no nulos.

Todo cociente de un DIP por un ideal primo es un campo

Corolario 7

Supongamos que R es un dominio euclidiano. Si I es un ideal primo de R, entonces R/I es un campo (y en particular, es un DIP)[6].

Demostración. Supongamos que I es un ideal primo en R. Por la proposición anterior, I es maximal. Luego, por la caracterización de ideales maximales en términos de cocientes, R/I es un campo.

[6] Recordemos que todo campo es trivialmente un dominio euclidiano pero también es fácil ver directamente que es un DIP: los únicos ideales en un campo son $0 = (0)$ y $R = (1)$.

El cociente de un DIP por un ideal principal

Proposición 8

Supongamos que R es un DIP y que $a \in R \setminus \{0\}$. Entonces todos los ideales de $R/(a)$ son de la forma $(b)/(a)$ donde $b|a$.

Demostración. Por el cuarto teorema de isomorfismos, todo ideal de $R/(a)$ es de la forma $I/(a)$ donde I es un ideal de R que contiene a (a). Además, como R es un DIP, todo ideal es principal y por lo tanto, para cada I existe $b \in R$ tal que $I = (b)$. Luego $(a) \subset I = (b)$, y por lo tanto $b|a$. En resumen, todo ideal de $R/(a)$ es de la forma $I/(a) = (b)/(a)$ donde $b|a$. $\square$

Proposición 9

Supongamos que R es un anillo conmutativo con 1. Si el anillo de polinomios $R[x]$ es un DIP, entonces R es un campo.

Demostración.

$$
\begin{aligned}
R[x] \text{ es un DIP} &\implies R[x] \text{ es un dominio entero} \\
&\iff R \text{ es un dominio entero} \\
&\iff R[x]/(x) \text{ es un dominio entero} && (\text{pues } R[x]/(x) \cong R) \\
&\iff (x) \text{ es un ideal primo en } R[x] \\
& && (\text{por la caracterización de ideales primos}) \\
&\iff (x) \text{ es un ideal maximal en } R[x] \\
& && (\text{pues en un DIP, primo} \iff \text{maximal}) \\
&\iff R[x]/(x) \text{ es un campo} && (\text{por la caracterización de ideales maximales}) \\
&\iff R \text{ es un campo} && (\text{pues } R[x]/(x) \cong R)
\end{aligned}
$$

□