Ejemplos y propiedades de dominios euclididanos

Facultad de Ciencias UNAM

Introducción

En esta sección continuamos nuestro estudio de dominios euclidianos.

Dominios euclidianos y campos

- Supongamos que F es un campo y N es cualquier norma en F. Veamos que F es un dominio euclidiano. Sean $a, b \in F$ y $b \neq 0$. Definimos $q := ab^{-1}$ y $r = 0$. De esta manera,

$$a = bq + r$$

  y por lo tanto, F es un dominio euclidiano.

- Si F es un campo, entonces $F[x]$ es un dominio euclidiano con la norma N dada por $N(p(x)) = \deg p(x)$. El algoritmo de la división en $F[x]$ es consecuencia de la famosa "división larga de polinomios" (la cual tal vez conoces en $\mathbb{R}[x]$). De hecho, para que un anillo de polinomios $R[x]$ sea un dominio euclidiano, es *necesario* que R sea un campo pues la "división larga de polinomios" depende de que podamos dividir por elementos no nulos.

  En este momento omitimos las demostraciones de cada una de estas afirmaciones pero el lector interesado ya tiene las herramientas para adelantarse a la sección 1.24 y leer las demostraciones.

Los enteros cuadráticos

Supongamos que $D \in \mathbb{Z}$ es tal que $k^2 \nmid D$ para toda $k \in \mathbb{Z}_{\geq 1}$. Como los enteros cuadráticos $\mathcal{O}(D)$ son un subanillo de $\mathbb{C}$, entonces son un dominio entero. Sin embargo, en general, $\mathcal{O}(D)$ no es un dominio euclidiano con la norma N_D (o con cualquier otra norma). Por ejemplo, pronto veremos que $\mathcal{O}(-5) = \mathbb{Z}[\sqrt{-5}]$ y $\mathcal{O}(-19) = \mathbb{Z}[(1+\sqrt{-19})/2]$ *no* son dominios euclidianos respecto a *cualquier* norma. En contraste, ahorra veremos, que los enteros Gaussianos $\mathcal{O}(-1) = \mathbb{Z}[i]$ *si* son un dominio euclidiano con la norma N_{-1}. De hecho, la demostración que daremos se puede modificar para demostrar que $\mathcal{O}(D)$ también es un dominio euclidiano en los casos $D = -2, -3, -7, -11$.

Los enteros Gaussianos son un dominio euclidiano

Supongamos que $\alpha = a + bi, \beta = c + di \in \mathbb{Z}[i]$ con $\beta \neq 0$. Antes que nada, recordemos que en el campo $\mathbb{Q}(i) \subset \mathbb{C}$ tenemos que

$$\frac{\alpha}{\beta} = r + si$$

donde

$$r := \frac{ac + bd}{c^2 + d^2} \quad \text{y} \quad s := \frac{bc - ad}{c^2 + d^2}$$

Ahora si, veamos que $\mathbb{Z}[i]$ es un dominio euclidiano respecto a N demostrando que

$$\alpha = (p + qi)\beta + \gamma \text{ para alguna } \gamma \in \mathbb{Z}[i] \text{ tal que } N(\gamma) < N(\beta),$$

donde p es el entero mas cercano a r y q es el entero mas cercano a s.[1] Por supuesto, empezamos definiendo $\gamma := \alpha - (p + qi)\beta$. De esta manera, es claro que $\alpha = (p + qi)\beta + \gamma$ y que $\gamma \in \mathbb{Z}[i]$.

[1] En particular, $|r - p| \leq \frac{1}{2}$ y $|s - q| \leq \frac{1}{2}$.

Para ver la desigualdad necesitamos un truquito:

$$\gamma = \alpha - (p+qi)\beta = \left(\frac{\alpha}{\beta} - (p+qi)\right)\beta = \\ \big((r+si) - (p+qi)\big)\,\beta = \big((r-p) + (s-q)i\big)\,\beta,$$

y por lo tanto,

$$\begin{aligned} N_{-1}(\gamma) &= \mathcal{N}_{-1}\left(\big((r-p)+(s-q)i\big)\,\beta\right) && (\text{pues } N_{-1} = \mathcal{N}_{-1}\restriction_{\mathcal{O}(-1)}) \\ &= \mathcal{N}_{-1}\big((r-p)+(s-q)i\big)\,\mathcal{N}_{-1}(\beta) && (\text{pues } \mathcal{N}_{-1} \text{ es multiplicativa}) \\ &= \left((r-p)^2 + (s-q)^2\right) N_{-1}(\beta) \\ & && (\text{evaluando en } \mathcal{N}_D \text{ y usando que } \beta \in \mathcal{O}(-1)) \\ &\leq \left(\frac{1}{4} + \frac{1}{4}\right) N_{-1}(\beta) && (\text{pues } |r-p| \leq \tfrac{1}{2} \text{ y } |s-q| \leq \tfrac{1}{2}) \\ &= \frac{1}{2} N_{-1}(\beta) < N_{-1}(\beta). \end{aligned}$$

Por lo tanto, $\mathbb{Z}[i]$ es un dominio euclidiano respecto a N_{-1}.

Todo ideal en un dominio euclidiano es principal

Proposición 1

Supongamos que R es un dominio euclidiano con la norma N. Si $I \neq 0$ es un ideal en R, entonces $I = (d)$ donde d es cualquier elemento no cero de I con norma mínima.

Demostración. Supongamos que d es cualquier elemento no cero de I con norma mínima. Es decir, $N(d) \leq N(x)$ para toda $x \in I \setminus \{0\}$. Cabe aclarar que este elemento existe por el axioma del buen orden de $\mathbb{Z}_{\geq 0}$ aplicado a $\{N(x) \mid x \in I \setminus \{0\}\} \subset \mathbb{Z}_{\geq 0}$.

Ahora bien, como $d \in I$, entonces $(d) \subset I$. Para ver la inclusión conversa, supongamos que $a \in I$. Como R es dominio euclidiano, entonces $a = dq + r$ para algunas $q, r \in R$ tales que $N(r) < N(d)$. Luego, como $r = a - dq \in^2 I$, $N(r) < N(d)$, y $N(d) \leq N(x)$ para toda $x \in I \setminus \{0\}$, entonces debe ser $r = 0$. Por lo tanto, $a = dq \in (d)$ y $I \subset (d)$. □

[2] Pues $a, d \in I$ y I es ideal de R.

Observación

A primera vista, podría parecer que la proposición anterior vuelve obsoleto a el algoritmo de la división. Al fin y al cabo, el algoritmo de la división demuestra que cualquier ideal de la forma (a, b) es principal[3] y la proposición anterior demuestra que *cualquier* ideal es principal.

La diferencia esta en la "calidad" del generador. Por ejemplo, en $\mathbb{Z}$ puede ser mas "fácil" calcular el algoritmo de la división "a pata", para encontrar r_{n-1} que encontrar una $d \in (a, b) \setminus \{0\}$ tal que $N(d) \leq N(x)$ para toda $x \in (a, b) \setminus \{0\}$ (recordemos que esto es equivalente a encontrar una $\mathbb{Z}$-combinación lineal a y b tal que su valor absoluto sea menor o igual al valor absoluto de cualquier otra $\mathbb{Z}$-combinación lineal de a y b). Cabe aclarar que "fácil" no necesariamente significa mas rápido, pero si conocemos los valores q_i y r_i, el algoritmo de la división siempre nos permite calcular *explícitamente* un máximo común divisor.

[3] Recordemos que demostramos $(a, b) = (r_{n-1})$ porque $(x, y) = (d)$ implica que d es máximo común divisor de x y y.

Cualquier cociente en los enteros Gaussianos es finito

Proposición 2

$\mathbb{Z}[i]/I$ es finito para todo ideal I de $\mathbb{Z}[i]$.

Demostración. Supongamos que I es un ideal de $\mathbb{Z}[i]$. Hacemos dos observaciones:

- Como $\mathbb{Z}[i]$ es un dominio euclidiano, entonces (por la proposición anterior) I es principal, es decir, existe $\alpha \in \mathbb{Z}[i]$ tal que $I = (\alpha)$.
- Para toda $\beta \in \mathbb{Z}[i]$, existe a lo mas una cantidad finita de elementos en $\mathbb{Z}[i]$ con norma menor o igual a la norma de β. En otras palabras, para toda $\beta \in \mathbb{Z}[i]$, el conjunto

$$\{x \in \mathbb{Z}[i] \mid N_{-1}(x) < N_{-1}(\beta)\} = \{z + wi \mid z^2 + w^2 < N_{-1}(\beta)\}$$

es finito.

Usando esto, es fácil ver que para demostrar que $\mathbb{Z}[i]/I$ es finito, basta demostrar que para todo $a \in \mathbb{Z}[i]$ existe $r \in \mathbb{Z}[i]$ tal que $N_{-1}(r) < N_{-1}(\alpha)$ y $a + I = r + I$. En efecto, esto implicaría que tenemos un conjunto de representantes contenido en

$$\{x \in \mathbb{Z}[i] \mid N_{-1}(x) < N_{-1}(\alpha)\},$$

el cual es un conjunto finito.

Por lo tanto, supongamos que $a \in \mathbb{Z}[i]$. Como $\mathbb{Z}[i]$ es un domino euclidiano, entonces existen $q, r \in \mathbb{Z}[i]$ tales que

$$a = q\alpha + r \quad \text{y} \quad N_{-1}(r) < N_{-1}(\alpha)$$

De donde $a - r = q\alpha \in (\alpha) = I$ o equivalentemente, $a + I = r + I$. Como $N_{-1}(r) < N_{-1}(\alpha)$, obtenemos lo deseado. $\square$

Observación

En la demostración de la proposición anterior, la única propiedad especifica a $\mathbb{Z}[i]$ que ocupamos fue la segunda observacion. Por lo tanto, podemos generalizar la proposición anterior de la siguiente manera (le dejamos la verificación al lector).

Proposición 3

Supongamos que R es un dominio euclidiano con la norma N. Si para toda $\alpha \in R$ el conjunto

$$\{x \in R \mid N(x) < N(\alpha)\}$$

es finito, entonces R/I es finito para todo ideal I de R.

Ejemplos de dominios enteros no euclidianos

- Recordemos que el anillo de polinomios $\mathbb{Z}[x]$ es un dominio entero[4] y que el ideal $(2, x)$ de $\mathbb{Z}[x]$ no es principal[5]. Por lo tanto, la proposición anterior implica que $\mathbb{Z}[x]$ es un dominio entero no euclidiano.
- El anillo de enteros cuadráticos $\mathbb{Z}[\sqrt{-5}]$ es un dominio entero que no es euclidiano: Veamos que el ideal $I = (3, 2 + \sqrt{-5})$ de $\mathbb{Z}[\sqrt{-5}]$ no es principal.

  Supongamos lo contrario, es decir, existen $a, b \in \mathbb{Z}$ tales que $I = (a + b\sqrt{-5})$. En particular, existen $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ tales que

$$3 = \alpha(a + b\sqrt{-5}) \tag{1}$$

$$2 + \sqrt{-5} = \beta(a + b\sqrt{-5}) \tag{2}$$

[4] c.f. sección 1.4
[5] c.f. sección 1.9

Por otro lado, recordemos que la norma N_{-5} en $\mathbb{Z}[\sqrt{-5}]$ esta dada por $N_{-5}(x + y\sqrt{-5}) = x^2 + y^2 5$. Solo usaremos a N_{-5} para demostrar que I no es principal, lo cual, por la proposición anterior, implica que $\mathbb{Z}[\sqrt{-5}]$ no es euclidiano.

Cabe aclarar que las únicas propiedades que ocuparemos de N_{-5} es (i) que N_{-5} es una función de $\mathbb{Z}[\sqrt{-5}]$ a $\mathbb{Z}$ y (ii) que N_{-5} es multiplicativa. La razón por la que hacemos este comentario es para que no haya ninguna confusión del tipo "solo demostramos que $\mathbb{Z}[\sqrt{-5}]$ no es un dominio euclidiano con la norma N_{-5}".

Con esto en mente, notemos que la ecuación (1) implica que

$$\begin{aligned} 9 = N_{-5}(3) = N_{-5}\left(\alpha(a + b\sqrt{-5})\right) &= N_{-5}(\alpha)N_{-5}(a + b\sqrt{-5}) \\ &= N_{-5}(\alpha)(a^2 + b^2 5) \end{aligned}$$

Como $N_{-5}(\alpha)$ y $a^2 + b^2 5$ son enteros mayores o iguales a 0, entonces la ecuación anterior implica que $a^2 + b^2 5 \in \{1, 3, 9\}$.

Caso 1. $a^2 + b^2 5 = 9$.
Entonces $\alpha = \pm 1$ y por (1), $\pm 3 = a + b\sqrt{-5}$. Juntando esto con (2) obtenemos $2 + \sqrt{-5} = \pm 3\beta$ lo cual es obviamente imposible[6].

Caso 2. $a^2 + b^2 5 = 3$.
Es imposible porque no hay $a, b \in \mathbb{Z}$ tales que $a^2 + b^2 5 = 3$.

Caso 3. $a^2 + b^2 5 = 1$.
Antes que nada, veamos que en este caso, $a + b\sqrt{-5} = \pm 1$. Debería de ser claro que para esto, basta ver que $b = 0$. Por eso, supongamos que $b \neq 0$. Entonces (como $b \in \mathbb{Z}$) $b^2 \geq 1$ y por lo tanto, $1 = a^2 + b^2 5 \geq b^2 5 \geq 5$, una contradicción.

Por lo tanto, tenemos $1 = a + b\sqrt{-5} \in (a + b\sqrt{-5}) = I = (3, 2 + \sqrt{-5})$, o equivalentemente, $I = \mathbb{Z}[\sqrt{-5}]$. En particular, existen $\gamma, \delta \in \mathbb{Z}[\sqrt{-5}]$ tales que $1 = 3\gamma + (2 + \sqrt{-5})\delta$.

[6] Recordemos que $x + y\sqrt{-5} = z + w\sqrt{-5}$ si y solo si $x = z$ y $y = w$.

Multiplicando por $2-\sqrt{-5}$ obtenemos

$$2-\sqrt{-5}=(2-\sqrt{-5})(3\gamma+(2+\sqrt{-5})\delta)=3\gamma(2-\sqrt{-5})+9\delta$$

De donde, 3 divide a $2-\sqrt{-5}$ en $\mathbb{Z}[\sqrt{-5}]$. Lo cual es obviamente imposible[7].

Por lo tanto, I no es un ideal principal en $\mathbb{Z}[\sqrt{-5}]$ y por la proposición anterior, $\mathbb{Z}[\sqrt{-5}]$ no es un dominio euclidiano.

[7] De nuevo, recordemos que $x+y\sqrt{-5}=z+w\sqrt{-5}$ si y solo si $x=z$ y $y=w$.

Divisores universales

Acabamos esta sección con un criterio que a veces se puede ocupar para demostrar que un dominio entero *no* es un dominio euclidiano.

Definición

Supongamos que R es un dominio euclidiano y denotemos por $\tilde{R}$ al conjunto que consiste de los elementos invertibles en R y el 0, es decir $\tilde{R} := R^\times \cup \{0\}$. Decimos que un elemento $u \in R \setminus \tilde{R}$ es un *divisor universal* en R si para cada $x \in R$ existe una $z \in \tilde{R}$ tal que $u|(x - z)$. En otras palabras, para cada $x \in R$ podemos escribir

$$x = qu + z$$

donde $q, z \in R$ y z es invertible o 0.

Dominios euclidianos y divisores universales

Proposición 4

Supongamos que R es un dominio entero que *no* es un campo. Si R es un dominio euclidiano, entonces R tiene divisores universales.

Demostración. Supongamos que R es un dominio euclidiano con la norma N y que R no es campo. Como R no es campo, entonces $R \setminus \tilde{R}$ es no vació. Además, por el axioma del buen orden, podemos escoger $u \in R \setminus \tilde{R}$ tal que $N(u) \leq N(a)$ para toda $a \in R \setminus \tilde{R}$. Ahora bien, supongamos que $x \in R$. Como R es dominio euclidiano, podemos escribir

$$x = qu + z$$

con $q, z \in R$ y $N(z) < N(u)$. Como u es tal que $N(u) \leq N(a)$ para toda $a \in R \setminus \tilde{R}$, entonces la desigualdad $N(z) < N(u)$ implica que $z \in \tilde{R}$. En resumen, cualquier elemento en $R \setminus \tilde{R}$ con norma mínima es un divisor universal de R. $\square$

Otro dominio entero no euclidiano

Veamos que $\mathcal{O}(-19) =^{8} \mathbb{Z}[(1+\sqrt{-19})/2]$ no es un dominio euclidiano.

Como $\mathcal{O}(-19)$ es un dominio entero que no es campo, por la proposición anterior, basta demostrar que $\mathcal{O}(-19)$ no tiene divisores universales. Cabe recalcar que en la siguiente sección veremos que todos los ideales de $\mathcal{O}(-19)$ son principales. Por eso, no podemos ocupar la proposición 3 para demostrar que $\mathcal{O}(-19)$ no es dominio euclidiano.

Antes de empezar, recordemos que la norma N_{-19} en $\mathcal{O}(-19)$ esta dada por $N_{-19}(a+b(1+\sqrt{-19})/2) := a^2+ab+5b^2$. Mas aun, notemos que si $a, b \in \mathbb{Z}$ y $b \neq 0$, entonces

$$N_{-19}(a+b(1+\sqrt{-19})/2) = a^2+ab+5b^2 = (a+b/2)^2+b^2 19/4 \geq 5.$$

Usando esto, es fácil verificar que los valores mas chicos que puede tomar N_{-19} son cuando $b=0$ y $a=\pm 1, \pm 2$. En cuyo caso, N_{-19} toma los valores 1 y 4 respectivamente.

[8] Pues $-19 \equiv 1 \mod 4$.

Por otro lado, recordemos que en la proposición 1.14.7 demostramos que $\alpha \in \mathcal{O}(-19)$ es invertible si y solo si $N_{-19}(\alpha) = \pm 1$. Usando la definición de N_{-19}, es fácil verificar que esto implica que los únicos elementos invertibles en $\mathcal{O}(-19)$ son ± 1. Por lo tanto, $\widetilde{\mathcal{O}(-19)} = \{0, \pm 1\}$.

Ahora bien, para ver que $\mathcal{O}(-19)$ no tiene divisores universales, supongamos lo contrario. Específicamente, supongamos que $u \in \mathcal{O}(-19)$ es un divisor universal. Entonces (como $2 \in \mathcal{O}(-19)$) existe $q \in R$ y $z \in \widetilde{\mathcal{O}(-19)}$ tal que $u|(2 - z)$. Usando que $\widetilde{\mathcal{O}(-19)} = \{0, \pm 1\}$, obtenemos que $u|(2 - 0)$ o $u|(2 \pm 1)$. Pero como $u \in \mathcal{O}(-19) \setminus \widetilde{\mathcal{O}(-19)}$, entonces $u \nmid 1$ y por lo tanto, tenemos que $u|2$ o $u|3$. Por lo tanto[9], $u \in \{\pm 2, \pm 3\}$. Sin embargo, es fácil verificar que si $x = (1 + \sqrt{-19})/2$, entonces x o $x \pm 1$ no son divisibles por ± 2 o ± 3 (en $\mathcal{O}(-19)$), contradiciendo la suposición de que u es un divisor universal.

[9] Veamos que los únicos divisores de 2 en $\mathcal{O}(-19)$ son $\{\pm 1, \pm 2\}$. Supongamos que $2 = \alpha\beta$ con $\alpha, \beta \in \mathcal{O}(-19)$. Entonces $4 = N_{-19}(2) = N_{-19}(\alpha\beta) = N_{-19}(\alpha)N_{-19}(\beta)$. Usando esto y el hecho de que los valores mas chicos que puede tomar N_{-19} son 1 y 4 (en ± 1 y ± 2 respectivamente), obtenemos lo deseado. Análogamente, los únicos divisores de 3 en $\mathcal{O}(-19)$ son $\{\pm 1, \pm 3\}$.

Comentario

Cabe recalcar que de la misma manera en la que podemos modificar la demostración de que $\mathbb{Z}[i]$ es un dominio euclidiano a los casos $D = -2, -3, -7. - 11$; también podemos modificar la demostración anterior a los casos $D = -43, -67, -163$.

Una curiosidad de la divisibilidad en dominios euclidianos

Proposición 5

Supongamos que R es un dominio euclidiano. Si R tiene 1 y $\alpha \in R$ es tal que $N(\alpha) = \text{mín}\{N(x) \mid x \in R \setminus \{0\}\}$, entonces α es invertible. En particular, todo elemento no nulo con norma 0 es invertible.

Demostración. Supongamos que $\alpha \in R$ es tal que $N(\alpha) = \text{mín}\{N(x) \mid x \in R \setminus \{0\}\}$. Como R es dominio euclidiano y $1 \in R$, existen $q, r \in R$ tales que

$$1 = q\alpha + r \text{ y } N(r) < N(\alpha)$$

La desigualdad y la elección de α implican que $r = 0$. Por lo tanto, $1 = q\alpha$ y α es invertible.