Dominios de factorización única

Facultad de Ciencias UNAM

Introducción

Hace dos secciones generalizamos el algoritmo de la división en $\mathbb{Z}$. En esta sección, generalizamos el teorema fundamental de la aritmética. Por si no lo recuerdas, este dice que

> *Todo entero puede ser escrito como un producto de primos (no necesariamente distintos).*

En efecto, supongamos que $n \in \mathbb{Z}$. Veamos que n puede ser escrito como un producto de primos (no necesariamente distintos). Si n no es primo, entonces por definición, existen $n_1, n_2 \in \mathbb{Z} \setminus \{\pm 1\}$ tales que $n = n_1 n_2$. Mas aun, esta igualdad implica[1] que $|n_1|, |n_2| < |n|$. Si n_1 y n_2 son primos, ya acabamos. De lo contrario, n_1 o n_2 puede ser factorizado en dos enteros con valor absoluto estrictamente menor al de n_1 o al de n_2 respectivamente. Como no existen sucesiones infinitas estrictamente decrecientes en $\mathbb{Z}_{\geq 0}$, este proceso debe eventualmente terminar. En otras palabras, eventualmente debemos poder escribir a n como un producto de primos.

[1] El valor absoluto del producto de dos enteros siempre es mas grande que el valor absoluto de cada uno de los factores.

De hecho, sabemos que esta factorización es *única* en el siguiente sentido: dos factorizaciones en primos positivos de un entero positivo $n \in \mathbb{Z}_{\geq 0}$ solo difieren en el orden de los factores. Esta restricción a primos y enteros positivos se hace para no considerar las factorizaciones $(3)(5)$ y $(-3)(-5)$ como distintas.

Dominios de factorización única

Definición

Supongamos que R es un dominio entero. Decimos que R es un **dominio de factorización única** (abreviado **DFU**) si para todo $r \in R \setminus \{0\}$ que no es invertible se satisfacen las siguientes dos condiciones:

1. r se puede escribir como un producto de elementos irreducibles (no necesariamente distintos) en R. Específicamente, existen $p_1, \ldots, p_n \in R$ irreducibles tales que $r = p_1 \cdots p_n$.
2. La factorización en (i) es única salvo asociados. Específicamente si $p_1, \ldots, p_n$ y $q_1, \ldots, q_m$ son elementos irreducibles en R tales que

$$p_1 \cdots p_n = r = q_1 \cdots q_m$$

entonces, $m = n$ y podemos reordenar los índices de manera que p_i sea asociado a q_i para toda $i \in \{1, \ldots, n = m\}$.

Ejemplos básicos

- Como un campo no tiene elementos no invertibles, todo campo es trivialmente un DFU.
- El subanillo de los enteros Gaussianos $\mathbb{Z}[2i] = \{a + b2i \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ es un dominio entero pero no es un DFU. En efecto,

$$4 = 2 \cdot 2 \quad \text{y} \quad 4 = (2i)(-2i)$$

son dos factorizaciones en irreducibles distintas de 4 pues 2 y $2i$ son irreducibles[2] no asociados[3] en $\mathbb{Z}[2i]$.

[2] Esto es consecuencia inmediata de la multiplicidad de la norma N_{-1}.

[3] Esto es consecuencia de (i) que los elementos invertibles en $\mathbb{Z}[i]$ son exactamente aquellos con norma ± 1 (c.f. proposición 1.14.7), es decir solo $\pm 1, \pm i \in \mathbb{Z}[i]$ y (ii) que $\pm i \notin \mathbb{Z}[2i]$.

Cabe recalcar que 2 y $2i$ *si* son asociados en $\mathbb{Z}[i]$ pues $(2)(i) = 2i$ y i es invertible en $\mathbb{Z}[i]$. Por lo tanto, hay que tener cuidado con donde estamos considerando a los elementos cuando estemos pensando en una factorización en irreducibles.

- El anillo de enteros cuadráticos $\mathbb{Z}[\sqrt{-5}]$ también es un dominio entero que no es un DFU. En efecto,

$$6 = 2 \cdot 3 \quad \text{y} \quad 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

son dos factorizaciones en irreducibles[4] distintas[5].

[4] Esto se puede verificar usando (i) la multiplicidad de la norma N_{-5} y (ii) el hecho de que $N_{-5}(a + b\sqrt{-5}) \geq 5$ si $b \neq 0$.

[5] Esto de nuevo es consecuencia inmediata de que (i) los elementos invertibles en $\mathbb{Z}[\sqrt{-5}]$ son exactamente aquellos con norma ± 1 (c.f. proposición 1.14.7), es decir, solo $\pm 1 \in \mathbb{Z}[\sqrt{-5}]$.

En un DFU, primo $\iff$ irreducible

Proposición 1

Supongamos que R es un DFU y $p \in R$. Entonces p es primo si y solo si p es irreducible.

Demostración. Como en un dominio entero, primo $\implies$ irreducible, basta probar la implicación "$\impliedby$". Para esto, supongamos que $r \in R$ es irreducible y que $a, b \in R$ son tales que $r|ab$. Queremos ver que $r|a$ o $r|b$.

Primero consideremos el caso en que alguno de los dos a o b es invertible. Supongamos sin perdida de generalidad que a es invertible. Entonces podemos multiplicar $r|ab$ por a^{-1} para obtener $a^{-1}r|b$. Juntando esto con $r|a^{-1}r$, obtenemos $r|b$.

Por lo tanto, supongamos que a y b no son invertibles. Como R es un DFU, existen $p_1, \ldots, p_n$ y $q_1, \ldots, q_m$ elementos irreducibles en R tales que

$$a = p_1 \cdots p_n \quad \text{y} \quad b = q_1 \cdots q_m.$$

Usando esto y el hecho de que $r|ab$, obtenemos que

$$rk = ab = (p_1 \cdots p_n)(q_1 \cdots q_m) \quad \text{para alguna } k \in R$$

Entonces, por la unicidad de la factorización, la igualdad anterior implica que existe p_i o q_j que es asociado a r. Sin perdida de generalidad, supongamos que r y p_1 son asociados. Es decir, existe $u \in R$ invertible tal que $p_1 = ru$. Pero entonces

$$a = p_1 p_2 \cdots p_n = (ru)p_2 \cdots p_n = r(up_2 \cdots p_n)$$

En particular, $r|a$. Cabe recalcar que en caso de suponer que r y q_1 son asociados, hubiéramos obtenido que $r|b$. □

Gracias a esta proposición, de ahora en adelante, cuando estemos en un DFU, ocupamos las palabras “primo” e “irreducible” indistintamente.

Divisores en un DFU

Proposición 2

Supongamos que R es un DFU y que $r \in R \setminus \{0\}$ no es invertible. Si

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

es una factorización en primos de r tal que $k_i \in \mathbb{Z}_{\geq 1}$ para toda $i \in \{1, \ldots, n\}$ y $p_i \neq p_j$ si $i \neq j$, entonces todo divisor de a es de la forma

$$u p_1^{l_1} \cdots p_n^{l_n}$$

donde $u \in R$ es invertible y $l_i \leq k_i$ para toda $i \in \{1, \ldots, n\}$.

Demostración. Supongamos que d es cualquier divisor de a.

En caso de que d sea invertible, entonces $l_i = 0$ y $u = d$ cumplen lo deseado.

En caso de que d no sea invertible, entonces existe una factorización en primos de d, digamos

$$d' = q_1 \cdots q_t$$

Como $d|a$, entonces existe $r \in R$ tal que

$$(q_1 \cdots q_t)\, r = dr = a = p_1^{k_1} \cdots p_n^{k_n}$$

Por unicidad de la factorización, esto implica que cada q_i es asociado de algún p_j. En particular, podremos escribir

$$d = u p_1^{l_1} \cdots p_n^{l_n}$$

con $l_i \leq k_i$ y $u \in R$ invertible. $\square$

Una factorización de dos elementos

Lema 3

Supongamos que R es un DFU y $a, b \in R \setminus \{0\}$. Entonces, existen $p_1, p_2 \ldots, p_n \in R$ irreducibles no asociados dos a dos[6] y u, v invertibles tales que

$$a = up_1^{k_1} p_2^{k_2} \cdots p_n^{k_n} \quad \text{y} \quad b = vp_1^{l_1} p_2^{l_2} \cdots p_n^{l_n} \tag{1}$$

donde $k_i, l_i \in \mathbb{Z}_{\geq 0}$ para toda $i \in \{1, \ldots, n\}$.

Decimos que estas factorizaciones son **una factorización de a y b con notación** (n, p, k, l).

La demostración es sencilla, pero muy tediosa y por eso se la dejamos al lector.

[6] Es decir, si $i \neq j$, entonces p_i y p_j no son asociados.

El máximo común divisor en un DFU

Proposición 4

Supongamos que R es un DFU. Si $a, b \in R \setminus \{0\}$ y tenemos una factorización de a y b con notación (n, p, k, l), entonces

1. Todo divisor común de a y b es de la forma

$$up_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$$

donde $u \in R$ es invertible y $m_i \leq \text{mín}\{k_i, l_i\}$ para toda $i \in \{1, \ldots, n\}$.

2. El elemento

$$p_1^{\text{mín}\{k_1,l_1\}} p_2^{\text{mín}\{k_2,l_2\}} \cdots p_n^{\text{mín}\{k_n,l_n\}}$$

es un máximo común divisor de a y b.

1. Supongamos que d' es cualquier divisor común de a y b. Como $d'|a$, la proposición 2 implica que

$$d = up_1^{m_1} \cdots p_n^{m_n} \tag{2}$$

con $m_i \leq k_i$ y $u \in R$ invertible. Luego, como también $d'|b$, entonces existe $s \in R$ tal que

$$\left(up_1^{m_1} \cdots p_n^{m_n}\right) s = d's = b = p_1^{l_1} \cdots p_n^{l_n}$$

y por lo tanto, debemos tener $m_i \leq l_i$. Como ya sabíamos $m_i \leq k_i$, esto implica que $m_i \leq \text{mín}\{k_i, l_i\}$ y (2) cumple lo deseado.

2. Es consecuencia inmediata del inciso anterior.

□

El mínimo común múltiplo en un DFU

Proposición 5

Supongamos que R es un DFU. Si $a, b \in R \setminus \{0\}$ y tenemos una factorización de a y b con notación (n, p, k, l), entonces el elemento

$$p_1^{\text{máx}\{k_1,l_1\}} p_2^{\text{máx}\{k_2,l_2\}} \cdots p_n^{\text{máx}\{k_n,l_n\}}$$

es un mínimo común múltiplo de a y b.

Demostración. Recordemos que si $a, b \in R \setminus \{0\}$ y d es un mcd de a y b, entonces $\frac{ab}{d}$ es un mcm de a y b. Usando esto y la proposición anterior, obtenemos lo deseado. □

En un DIP no existen cadenas infinitas estrictamente ascendentes de ideales

Lema 6

Supongamos que R es un DIP y que $\{I_k\}_{k\in\mathbb{Z}_{\geq 0}}$ es una familia de ideales en R. Si $I_1 \subset I_2 \subset \cdots \subset R$, entonces existe $n \in \mathbb{Z}_{\geq 0}$ tal que $I_k = I_n$ para toda $k \geq n$.

Demostración. Supongamos que $\{I_k\}_{k\in\mathbb{Z}_{\geq 0}}$ es una familia de ideales en R tales que $I_1 \subset I_2 \subset \cdots \subset R$. Es fácil verificar que

$$I := \bigcup_{k\in\mathbb{Z}_{\geq 0}} I_k$$

es un ideal en R (de hecho ya habíamos visto esto en la sección 1.11).

Como R es un DIP, existe $a \in R$ tal que $I = (a)$. En particular, por definición de I, existe $n \in \mathbb{Z}_{\geq 0}$ tal que $a \in I_n$. Pero entonces para toda $k \geq n$ tenemos que $(a) \subset I_n \subset I_k \subset I = (a)$ y por lo tanto, $(a) = I_n = I_k$ para toda $k \geq n$. $\square$

DIP $\implies$ DFU

Proposición 7

Supongamos que R es un dominio entero. Si R es un DIP, entonces R es un DFU.

Demostración. Supongamos que R es un DIP y que $r \in R \setminus \{0\}$ no es invertible.

Existencia:
La demostración de la existencia de una factorización en irreducibles es completamente análoga a la demostración de la existencia de una factorización en primos en $\mathbb{Z}$. Específicamente, si $r \in R \setminus \{0\}$ es no invertible y no irreducible[7], entonces aplicamos la definición de "no irreducible" (al elemento y luego a sus factores y luego a los factores de los factores...) hasta que tengamos puros irreducibles en la factorización.

[7] Si r es irreducible, no hay nada que demostrar.

Sin embargo, hay que tener cuidado: en $\mathbb{Z}$ podíamos garantizar que este proceso eventualmente terminaba porque cada vez que factorizabamos, obteníamos dos enteros con valor absoluto mas chico al del entero que acabamos de factorizar. De esta manera, si este proceso continuara indefinidamente, obtendríamos una sucesión infinita estrictamente decreciente en $\mathbb{Z}_{\geq 0}$, lo cual es imposible.

Afortunadamente, hay una forma muy sencilla de resolver esta dificultad en el caso general: Supongamos que $r = r_1 r_2$ es la igualdad que es consecuencia de aplicar la definición de "no irreducible" a r. En vez de enfocarnos en valores absolutos, y en desigualdades de la forma $|r_1| < |r|$, nos enfocamos en divisibilidad y en inclusiones de la forma $(r) \subsetneq^{8} (r_1)$. Con este enfoque, concluimos que si el proceso de factorización continuara indefinidamente, obtendríamos una cadena infinita estrictamente ascendente de ideales en R, lo cual (por el lema anterior) es imposible en un DIP.

[8] La inclusión existe porque $r_1 | r$ y es propia porque $r_1 \notin (r)$ (de lo contrario, es fácil verificar (usando $r = r_1 r_2$) que esto implicaría que r_2 es invertible, contradiciendo la elección de r_2.

Unicidad:
Supongamos que $r \in R \setminus \{0\}$ es no invertible y que

$$p_1 p_2 \cdots p_n = r = q_1 q_2 \cdots q_m$$

son dos factorizaciones en irreducibles de r. En particular, $p_1 | q_1 q_2 \cdots q_m$ lo cual implica[9] que $p_1 | q_j$ para alguna $j \in \{1, \ldots, m\}$. Sin perdida de generalidad, supongamos que $j = 1$, es decir, que $p_1 | q_1$. Por lo tanto, $p_1 u = q_1$ para alguna $u \in R$ invertible[10]. Entonces,

$$p_1 p_2 \cdots p_n = (p_1 u) q_2 \cdots q_m = p_1 \left(u q_2 \cdots q_m\right)$$

y por lo tanto, como en un dominio entero podemos cancelar factores no nulos,

$$p_2 p_3 \cdots p_n = u q_2 q_3 \cdots q_m$$

[9] Recuerda que en un DIP, irreducible $\iff$ primo.

[10] Como q_1 es irreducible y $q_1 = p_1 u$, entonces p_1 es invertible o u es invertible. Pero p_1 no es invertible porque es irreducible.

Luego, si definimos $q_2' := uq_2$, entonces es fácil verificar que q_2' es irreducible y claramente

$$p_2 p_3 \cdots p_n = q_2' q_3 \cdots q_m$$

Usando este argumento e inducción sobre n, obtenemos lo deseado.

Cabe recalcar que el paso base $n = 1$ requiere un poco de cuidado: supongamos que $m \in \mathbb{Z}_{\geq 1}$ y $p, q_1, \ldots, q_m \in R$ son irreducibles tales que

$$p = q_1 q_2 \cdots q_m = q_1 (q_2 \cdots q_m)$$

Como p es irreducible, entonces la igualdad anterior implica que q_1 es invertible o que $q_2 \cdots q_m$ es invertible. Como q_1 no es invertible (es irreducible), entonces $q_2 \cdots q_m$ es invertible y por lo tanto $p = q_1 u$ con $u \in R$ invertible. $\square$

Terminamos esta sección con un resultado bastante trivial pero que escribimos para referenciarlo en el futuro.

Los isomorfismos preservan factorizaciones en irreducibles

Proposición 8

Supongamos que R, R' son DFU's y que $\phi : R \to R'$ es un isomorfismo. Si $r \in R \setminus \{0\}$ no es invertible y

$$r = p_1 \cdots p_n$$

es una factorización en irreducibles de r en R, entonces

$$\phi(r) = \phi(p_1) \cdots \phi(p_n)$$

es una factorización en irreducibles de $\phi(r)$ en R'.

Demostración. Esto es consecuencia inmediata de que los isomorfismos preservan irreducibilidad (c.f. proposición 1.16.5) □