Anillos de polinomios y DFU's (parte uno)

Facultad de Ciencias UNAM

Introducción

El objetivo de las siguientes dos secciones es demostrar que

$$R \text{ es un DFU } \iff R[x] \text{ es un DFU.} \tag{1}$$

La implicación "$\Longrightarrow$" requiere bastante trabajo y *varios* lemas. En contraste, la implicación "$\Longleftarrow$" es sencilla y de hecho invitamos al lector a intentarla en este momento teniendo en cuenta que en general,

$$R \text{ es un DFU y } S \text{ es un subanillo de } R \not\Longrightarrow S \text{ es un DFU.}$$

De hecho, supongamos que ya sabemos (1) y veamos que si F es un campo, entonces existe un subanillo $\mathcal{S}$ de $F[x]$ que *no* es un DFU: Considera

$$\mathcal{S} := \left\{ a_n x^n + \cdots + a_1 x + a_0 \in F[x] \mid n \in \mathbb{Z}_{\geq 0},\ a_i \in F,\ a_1 = 0 \right\}$$

y veamos (por contradicción) que x^2 y x^3 son elementos irreducibles en $\mathcal{S}$.

Supongamos que x^2 es reducible en $\mathcal{S}$, entonces por definición existen $p(x), q(x) \in \mathcal{S}$ tales que $x^2 = p(x)q(x)$. Por otro lado, como x es irreducible en $F[x]$ (en la sección anterior vimos que el polinomio x es irreducible en $R[x]$ si R es un dominio entero)[1] y tenemos la factorización $x^2 = x \cdot x$, entonces la unicidad de la factorización en $F[x]$ implica que

$$p(x) = ux \quad \text{y} \quad q(x) = vx$$

para algunas $u, v \in R$ invertibles. Sin embargo, $ux \notin \mathcal{S}$ y $vx \notin \mathcal{S}$, contradiciendo $p(x), q(x) \in \mathcal{S}$ y por lo tanto, x^2 es irreducible en $\mathcal{S}$. Usando esto, es fácil ver (de manera análoga) que x^3 es irreducible en $\mathcal{S}$.

Usando esto, obtenemos que

$$x^6 = (x^3)(x^3) \quad \text{y} \quad x^6 = (x^2)(x^2)(x^2)$$

son dos factorizaciones en irreducibles en $\mathcal{S}$ con longitudes distintas y en particular, sin un reacomodo como el de la definición de unicidad. Por lo tanto, $\mathcal{S}$ no es un DFU.

[1] c.f. proposición 1.24.5.

Un lema para otro lema

Lema 1

Supongamos que R es un anillo conmutativo, que F es su campo de fracciones, y que $p(x) \in F[x]$. Si $A(x), B(x) \in F[x]$ son tales que $p(x) = A(x)B(x)$, entonces existen $a'(x), b'(x) \in R[x]$ y $d \in R$ tales que $dp(x) = a'(x)b'(x)$.

Demostración. Supongamos que $n, m \in \mathbb{Z}_{\geq 0}$ y $a_i, \alpha_i, b_j, \beta_j \in R$ son tales que

$$A(x) = \sum_{i=0}^{n} \frac{a_i}{\alpha_i} x^i \quad \text{y} \quad B(x) = \sum_{j=0}^{m} \frac{b_j}{\beta_j} x^j$$

Define

$$d_A \coloneqq \alpha_1 \alpha_2 \cdots \alpha_n \quad \text{y} \quad d_B \coloneqq \beta_1 \beta_2 \cdots \beta_m$$

Veamos que

$$d \coloneqq d_A \cdot d_B, \quad a'(x) \coloneqq d_A A(x), \quad b'(x) \coloneqq d_B B(x)$$

cumplen lo deseado. Antes de ver que $dp(x) = a'(x)b'(x)$, veamos que $a'(x), b'(x) \in R[x]$. Por definición,

$$\begin{aligned} a'(x) = d_A A(x) &= (\alpha_1 \alpha_2 \cdots \alpha_n) \left(\sum_{i=0}^{n} \frac{a_i}{\alpha_i} x^i \right) \\ &= \sum_{i=0}^{n} (\alpha_1 \cdots \alpha_{i-1} \alpha_{i+1} \cdots \alpha_n) a_i x^i \in R[x] \end{aligned}$$

Análogamente, $b'(x) \in R[x]$. Ahora si, veamos la igualdad

$$dp(x) = dA(x)B(x) = (d_A d_B)A(x)B(x) = \big(d_A A(x)\big)\big(d_B B(x)\big) = a'(x)b'(x)$$

□

El lema de Gauss

Lema 2

Supongamos que R es un DFU, que F es su campo de fracciones, y que $p(x) \in R[x]$.

Si $A(x), B(x) \in F[x]$ son tales que $p(x) = A(x)B(x)$, entonces existen $a(x), b(x) \in R[x]$ tales que $p(x) = a(x)b(x)$ con $a(x) = rA(x)$ y $b(x) = sB(x)$ donde $r, s \in F$.

En particular, si $p(x) \in R[x]$ es reducible en $F[x]$, entonces también es reducible en $R[x]$.

Demostración. Supongamos que $A(x), B(x) \in F[x]$ son tales que $p(x) = A(x)B(x)$. Por el lema anterior, existen $d_A, d_B, d \in R$ y $a'(x), b'(x)$ tales que

$$d = d_A \cdot d_B,\ a'(x) = d_A A(x),\ b'(x) = d_B B(x),\ dp(x) = a'(x)b'(x) \qquad (2)$$

En caso de que d sea invertible, es fácil verificar que $a(x) := d^{-1}a'(x)$ y $b(x) := b'(x)$ cumplen lo deseado.

En caso de que d no sea invertible, como estamos en un DFU, existe una factorización en irreducibles de d, digamos

$$d = p_1 p_2 \cdots p_n$$

Como en un DFU, irreducible $\iff$ primo, entonces p_i es primo para toda i. En particular, (p_1) = el ideal generado por p_1 en R, es un ideal primo en R y por lo tanto (por la caracterización de ideales primos), $R/(p_1)$ es un dominio entero. Usando la el hecho de que "S dominio entero $\iff$ $S[y]$ dominio entero" y el isomorfismo

$$R[x]/(p_1)[x] \cong (R/(p_1))[x]$$

obtenemos que $R[x]/(p_1)[x]$ es un dominio entero. Si para cada $q(x) \in R[x]$ denotamos $\overline{q(x)} := q(x) + (p_1)[x]$, entonces (2) implica que

$$\overline{0} = \overline{p_1 \left(p_2 \cdots p_n p(x)\right)} = \overline{dp(x)} = \overline{a'(x)b'(x)} = \overline{a'(x)}\,\overline{b'(x)}$$

donde la primera igualdad se cumple porque $p_1 \left(p_2 \cdots p_n p(x)\right) \in (p_1)[x]$.

Como $R[x]/(p_1)[x]$ es un dominio entero, entonces la igualdad anterior implica que $\overline{a'(x)} = \overline{0}$ o $\overline{b'(x)} = \overline{0}$. Sin perdida de generalidad, supongamos que $\overline{a'(x)} = \overline{0}$. Esto es equivalente a que $a'(x) \in (p_1)[x]$ y esto es equivalente a que los coeficientes de $a'(x)$ pertenezcan a (p_1), finalmente, esto es equivalente a que los coeficientes de $a'(x)$ sean R-múltiplos de p_1. Por eso, podemos escribir

$$a'(x) = p_1 a''(x)$$

para algún $a''(x) \in R[x]$. Sustituyendo esto en (2) obtenemos

$$p_1 \left(p_2 \cdots p_n p(x)\right) = (p_1 \cdots p_n)\, p(x) = dp(x) = a'(x)b'(x) = p_1 a''(x)b'(x)$$

Como R es un dominio entero y $p_1 \neq 0$, esto implica que

$$p_2 \cdots p_n p(x) = a''(x)b'(x)$$

Considerando esta igualdad en el cociente $R[x]/(p_2)[x]$, encontraremos[2] $a'''(x)$ o $b'(x)$ en $R[x]$ tal que

$$a''(x) = p_2 a'''(x) \quad \text{y} \quad p_3 \cdots p_n p(x) = a'''(x) b'(x)$$

o

$$b'(x) = p_2 b''(x) \quad \text{y} \quad p_3 \cdots p_n p(x) = a''(x) b''(x).$$

Procediendo de esta manera (hasta cancelar todas las p_i) es fácil ver que eventualmente obtendremos lo deseado. Para ser precisos, supongamos sin perdida de generalidad que existe $k \leq n$ tal que

$$\begin{aligned} a'(x) = p_1 a''(x), \;\; a''(x) = p_2 a'''(x), \; \ldots \, , a^{(k-1)}(x) = p_k a^{(k)}(x) \\ b'(x) = p_{k+1} b''(x), \;\; b''(x) = p_{k+2} b'''(x), \; \ldots \, , b^{(n-k)}(x) = p_n b^{((n-k)+1)}(x) \end{aligned} \quad (3)$$

Donde $a^{(3)} := a'''$, $a^{(4)} := a''''$, $\ldots$ y análogamente para las b's.

[2] De exactamente la misma manera en la que encontramos a $a'(x)$.

Naturalmente, definimos

$$a(x) \coloneqq a^{(k)}(x) \quad \text{y} \quad b(x) \coloneqq b^{((n-k)+1)}(x)$$

y por lo tanto, usando (3)

$$a(x) = \frac{1}{p_k} a^{(k-1)}(x) = \frac{1}{p_k}\left(\frac{1}{p_{k-1}} a^{(k-2)}\right) = \cdots = \frac{1}{p_k}\frac{1}{p_{k-1}} \cdots \frac{1}{p_2}\frac{1}{p_1} a'(x)$$

Finalmente, usando esta igualdad y la definición de $a'(x)$ (c.f. (2)), obtenemos

$$a(x) = \frac{1}{p_k p_{k-1} \cdots p_2 p_1} d_A A(x)$$

De manera análoga,

$$b(x) = \frac{1}{p_n p_{n-1} \cdots p_{k+2} p_{k+1}} d_B B(x)$$

Por lo tanto,

$$\begin{aligned} a(x)b(x) &= \left(\frac{1}{p_k p_{k-1}\cdots p_2 p_1} d_A A(x)\right)\left(\frac{1}{p_n p_{n-1}\cdots p_{k+2} p_{k+1}} d_B B(x)\right) \\ &= \frac{1}{p_1 p_2 \cdots p_n} d_A d_B A(x)B(x) \\ &= \frac{1}{p_1 p_2 \cdots p_n} d A(x)B(x) \\ &= \frac{1}{p_1 p_2 \cdots p_n} (p_1 p_2 \cdots p_n) A(x)B(x) \\ &= A(x)B(x) = p(x) \end{aligned}$$

y los elementos de F

$$r := \frac{d_A}{p_k p_{k-1}\cdots p_2 p_1} \quad \text{y} \quad s := \frac{d_B}{p_n p_{n-1}\cdots p_{k+2} p_{k+1}}$$

cumplen lo deseado. □

Observación

A pesar de que $a(x)$ es un F-múltiplo de $A(x)$, en general no vamos a poder garantizar que $a(x)$ sea un R-múltiplo de $A(x)$. En efecto, sea $R = \mathbb{Z}$, y por lo tanto, $F = \mathbb{Q}$

$$p(x) := x^2, \quad A(x) := 2x, \quad B(x) := \frac{1}{2}x$$

Entonces

$$p(x) = x^2 = (2x)\left(\frac{1}{2}x\right) = A(x)B(x)$$

Queremos ver que no existen $a(x), b(x) \in \mathbb{Z}[x]$ tales que $a(x)$ es un $\mathbb{Z}$-múltiplo de $A(x)$, $b(x)$ es un $\mathbb{Z}$-múltiplo de $B(x)$, y $p(x) = a(x)b(x)$. Por eso, supongamos lo contrario, es decir, supongamos la existencia de semejantes $a(x), b(x) \in \mathbb{Z}[x]$.

Entonces existen $n, m \in \mathbb{Z}[x]$ tales que $a(x) = nA(x)$ y $b(x) = mB(x)$. Pero entonces

$$A(x)B(x) = p(x) = nA(x)mB(x)$$

Como $\mathbb{Q}[x]$ es dominio entero, entonces la ecuación anterior implica $nm = 1$ y por lo tanto $n, m = \pm 1$. Sin embargo, esto implicaría
$\pm\frac{1}{2}x = \pm B(x) = mB(x) = b(x) \in \mathbb{Z}[x]$. Una contradicción.

De hecho, podemos generalizar este argumento:

El producto de dos polinomios mónicos sobre el campo de fracciones

Corolario 3

Supongamos que R es un DFU, que F es su campo de fracciones, y que $A(x), B(x) \in F[x]$ son mónicos. Si $A(x)B(x) \in R[x]$, entonces $A(x), B(x) \in R[x]$.

En otras palabras, si el producto de dos polinomios mónicos sobre F es un polinomio sobre R, entonces los coeficientes de estos polinomios mónicos son elementos de R.

Demostración. Definimos $p(x) := A(x)B(x) \in R[x]$. Por el lema de Gauss, existen $a(x), b(x) \in R[x]$ y $r, s \in F$ tales que $a(x) = rA(x)$, $b(x) = sB(x)$, y $p(x) = a(x)b(x)$.

Veamos que $r \in R$. De lo contrario, $r \in F \setminus R$ y como $A(x)$ es mónico, entonces la igualdad $a(x) = rA(x)$ implicaría $a(x) \in F[x] \setminus R[x]$ (pues el coeficiente delantero de $rA(x)$ es $r \in F \setminus R$). Análogamente, $s \in R$.

Por otro lado, las hipótesis implican

$$A(x)B(x) = p(x) = a(x)b(x) = rA(x)sB(x)$$

y como $F[x]$ es un dominio entero, entonces $rs = 1$.

Por lo tanto,

$$\begin{aligned} A(x) &= srA(x) && (\text{pues } rs = 1) \\ &= sa(x) && (\text{pues } a(x) = rA(x)) \\ &\in R[x] && (\text{pues } s \in R \text{ y } a(x) \in R[x]) \end{aligned}$$

Análogamente, $B(x) \in R[x]$. $\square$

Condiciones suficientes para que un anillo no sea DFU

Si jugamos un poquito con la formulación del enunciado del corolario anterior obtenemos

Corolario 4

Supongamos que R es un dominio entero[3], que F es su campo de fracciones. Si existen $A(x), B(x) \in F[x]$ mónicos tales que $A(x)B(x) \in R[x]$ pero $A(x) \in F[x] \setminus R[x]$, entonces R no es un DFU.

Una aplicación inmediata de esta reformulación es: $\mathbb{Z}[2\sqrt{2}]$ no es un DFU:

Denotemos $R = \mathbb{Z}[2\sqrt{2}]$. Usando que el campo de fracciones de un anillo es el campo mas chico que lo contiene, es fácil verificar que

$$F = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

[3]No estamos pidiendo que R sea un DFU

Además, $\sqrt{2} \notin R$ porque de lo contrario, existirían $a, b \in \mathbb{Z}$ tales que $a + b2\sqrt{2} = \sqrt{2}$ y por lo tanto tendríamos

$$\sqrt{2}(1 - b2) = \sqrt{2} - b2\sqrt{2} = a \in \mathbb{Z}.$$

Pero esto solo sucede si $1 - b2 = 0$ o equivalentemente, si $b = \frac{1}{2}$.
Contradiciendo $b \in \mathbb{Z}$.

Por lo tanto, si $A(x) = B(x) = x + \sqrt{2} \in F[x]$, entonces
$A(x) = B(x) \in F[x] \setminus R[x]$ y

$$\begin{aligned} A(x)B(x) = (x + \sqrt{2})(x + \sqrt{2}) &= x^2 + \sqrt{2}x + \sqrt{2}x + \sqrt{2}\sqrt{2} \\ &= x^2 + 2\sqrt{2}x + 4 \in R[x] \end{aligned}$$

Es decir, $A(x) = B(x) = x + \sqrt{2}$ satisfacen las condiciones del corolario y por lo tanto, $R = \mathbb{Z}[2\sqrt{2}]$ no es un DFU.