Anillos de polinomios y DFU's (parte dos)

Facultad de Ciencias UNAM

Introducción

En esta sección por fin demostramos que

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

Para empezar, introducimos una definición que va a estar muy presente en el resto de nuestro estudio de anillos de polinomios.

Polinomios primitivos

Definición

Supongamos que R es un anillo conmutativo y que $p(x) \in R[x]$. Si los coeficientes de $p(x)$ son primos relativos (es decir, el 1 es mcd de los coeficientes de $p(x)$), decimos que $p(x)$ es **primitivo**.

En particular, todo polinomio mónico es primitivo.

Condiciones suficientes para que $p(x) \in R[x]$ irreducible en $R[x] \iff p(x) \in R[x]$ irreducible en $F[x]$.

Proposición 1

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

1. Si $p(x)$ es primitivo, entonces

$$p(x) \text{ es irreducible en } R[x] \iff p(x) \text{ es irreducible en } F[x].$$

2. Si $p(x)$ no es primitivo, entonces

$$p(x) \text{ es irreducible en } R[x] \not\Longleftarrow p(x) \text{ es irreducible en } F[x].$$

Demostración.

1. Supongamos que $p(x)$ es primitivo.

   $\Longrightarrow$) Recordemos que una consecuencia inmediata del lema de Gauss es que si $p(x) \in R[x]$ es reducible en $F[x]$, entonces también es reducible en $R[x]$.

   $\Longleftarrow$) Supongamos que $p(x) \in R[x]$ es reducible en $R[x]$. Es decir, existen $a(x), b(x) \in F[x]$ tales que $p(x) = a(x)b(x)$, $a(x)$ no es invertible, y $b(x)$ tampoco.
   Usando esto, veamos que $a(x)$ y $b(x)$ no son constantes. Obviamente no son constantes invertibles y por lo tanto, basta probar que no son constantes no invertibles. En caso de que lo fueran, tendríamos $p(x) = a(x)b(x) = c \in^1 R \setminus \{1\}$, contradiciendo que $p(x)$ es primitivo.

[1] Pues si $c = 1$ entonces $a(x)$ y $b(x)$ serian invertibles.

En resumen, $a(x)$ y $b(x)$ son polinomios no constantes y por lo tanto, la misma factorización $p(x) = a(x)b(x)$ demuestra que $p(x)$ es reducible en $F[x]$ (recordemos que para un dominio entero D, los elementos invertibles de $D[x]$ son los polinomios constantes con valor un elemento invertible en D).

2. Sea $R = \mathbb{Z}$ y por lo tanto $F = \mathbb{Q}$. El polinomio $7x$ es reducible en $\mathbb{Z}[x]$ porque $7x = 7 \cdot x$ y 7 no es invertible en $\mathbb{Z}[x]$. Sin embargo, $7x$ es irreducible en $\mathbb{Q}[x]$ porque (i) el polinomio x es irreducible en en $\mathbb{Q}[x]$ (c.f. proposición 1.24.5), (ii) el polinomio 7 es invertible en $\mathbb{Q}[x]$, y (iii) el producto de un irreducible con un invertible es irreducible es el producto de un elemento irreducible (c.f. proposición 1.16.4).

□

La necesidad de que R sea DFU en la proposición anterior

Proposición 2

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

1. Si R es un DFU, entonces

$$p(x) \text{ es irreducible en } R[x] \implies p(x) \text{ es irreducible en } F[x].$$

2. Si R es un dominio entero arbitrario, entonces

$$p(x) \text{ es irreducible en } R[x] \not\implies p(x) \text{ es irreducible en } F[x].$$

Demostración.

1. Esto es consecuencia inmediata de que (i) todo polinomio mónico es primitivo (pues el 1 es uno de esos coeficientes) y (ii) el inciso (1) del corolario anterior.
2. Sea $R = \mathbb{Z}[2i]$ y $p(x) = x^2 + 1$. Si F es el campo de fracciones de R, entonces (por construcción) F es el campo mas chico que contiene a $\mathbb{Z}[2i]$. Usando esto es fácil verificar que

$$F \cong \left\{ a + ib \mid a, b \in \mathbb{Q} \right\}.$$

Como F es campo, $F[x]$ es DFU y por lo tanto la factorización en irreducibles[2]

$$x^2 + 1 = (x + i)(x - i)$$

es única salvo asociados.

[2] En la siguiente diapositiva demostramos que $(x + i)$ y $(x - i)$ son irreducibles en $F[x]$.

Como (i) los elementos invertibles de $F[x]$ son precisamente los elementos de F y (ii) para toda $u \in F$ tendremos que $u(x+i), u(x-i) \notin^3 R[x]$, entonces $p(x)$ es irreducible en $R[x]$.

Ahora si, veamos que $(x+i)$ es irreducible en $F[x]$, la demostración de que $(x-i)$ es irreducible en $F[x]$ es análoga.
Supongamos que $a(x), b(x) \in F[x]$ son tales que $x+i = a(x)b(x)$. Como $\deg(x+i) = 1$, podemos suponer (sin perdida de generalidad) que $\deg a(x) = 1$ y $\deg b(x) = 0$. Entonces $a(x) = a_1 x + a_0$ y $b(x) = b_0$ para algunas $a_1, a_0, b_0 \in F$. Pero entonces

$$x^2 + 1 = a(x)b(x) = (a_1 x + a_0)b_0 = b_0 a_1 x + b_0 a_0$$

Lo cual implica $b_0 a_1 = 1$ y en particular, $b_0 = b(x)$ es invertible.

[3] De lo contrario, como $ux + ui = u(x+i)$, y por lo tanto tendríamos $u \in R$ y $ui \in R$ lo cual es imposible por definición de R.

El lema de Gauss generalizado

Lema 3

Supongamos que R es un DFU, que $n \in \mathbb{Z}_{\geq 2}$, y que $p(x) \in R[x]$.
Si $A_1(x), \ldots, A_n(x) \in F[x]$ son tales que

$$p(x) = A_1(x) \cdots A_n(x),$$

entonces existen $a_1(x), \ldots, a_n(x) \in R[x]$ y $r_1, \ldots, r_n \in F$ tales que

$$p(x) = a_1(x) \cdots a_n(x) \quad \text{y} \quad a_i(x) = r_i A_i(x) \text{ para toda } i \in \{1, \ldots, n\}$$

La demostración es una inducción de rutina y por eso se la dejamos al lector.

Si los polinomios primitivos se factorizan en irreducibles salvo asociados, entonces $R[x]$ es un DFU

Lema 4

Supongamos que R es un DFU y que F es su campo de fracciones.

Si para todo $p(x) \in R[x]$ tal que
(i) $\deg p(x) \geq 1$ y
(ii) $p(x)$ es primitivo
existe una única factorización en irreducibles (salvo asociados),
entonces $R[x]$ es un DFU.

En otras palabras, para ver que $R[x]$ es un DFU, basta demostrar la existencia y unicidad de las factorizaciones de los polinomios primitivos no constantes.

Demostración. Supongamos la existencia y unicidad de las factorizaciones de los polinomios primitivos no constantes.

Primero notemos que la existencia y unicidad de las factorizaciones de los polinomios constantes no invertibles es consecuencia inmediata del hecho de que R es un DFU y de que los elementos invertibles en $R[x]$ son precisamente los elementos invertibles en R.

Resta probar la existencia y unicidad de las factorizaciones de los polinomios no constantes[4]. Por eso, supongamos que $p(x) \in R[x]$ es tal que $\deg p(x) \geq 1$.

Notemos que si $d \in R$ es un máximo común divisor de los coeficientes de $p(x)$, entonces $\frac{1}{d}p(x) \in R[x]$ (cabe recalcar que esto sucedería con cualquier divisor común de los coeficientes de $p(x)$, no solo con el mcd).

Por otro lado, recordemos que en la proposición 1.15.9 vimos que

$$\operatorname{mcd}\left\{\frac{a}{\operatorname{mcd}\{a,b\}}, \frac{b}{\operatorname{mcd}\{a,b\}}\right\} = 1$$

Usando (una generalización de) esto, obtenemos que los coeficientes de $\frac{1}{d}p(x)$ son primos relativos y por lo tanto $\frac{1}{d}p(x) \in R[x]$ es primitivo.

[4]No hace falta mencionar que son "no invertibles" pues no existen polinomios no constantes y no invertibles.

Usando la hipótesis en el polinomio primitivo $\frac{1}{d}p(x) \in R[x]$, obtenemos una factorización

$$\frac{1}{d}p(x) = q_1(x) \cdots q_n(x) \tag{1}$$

que es única salvo asociados.
Por otro lado, como $d \in R$ y ya sabemos de la existencia y unicidad de las factorizaciones de los polinomios constantes, entonces también tenemos una factorización

$$d = d_1 \cdots d_m \tag{2}$$

que también es única salvo asociados.
Finalmente, es claro que

$$p(x) = (d_1 \cdots d_m)(q_1(x) \cdots q_n(x))$$

es la factorización buscada (la unicidad es consecuencia de la unicidad de las factorizaciones en (1) y (2)). □

Los factores de un polinomio primitivo son primitivos

Lema 5

Supongamos que F es un campo y $p(x) \in F[x]$. Si $p(x) \in R[x]$ es primitivo y $a_1(x), \ldots, a_n(x) \in R[x]$ son tales que

$$p(x) = a_1(x) \cdots a_n(x),$$

entonces $a_i(x)$ es primitivo para toda $i \in \{1, \ldots, n\}$.

Demostracion. Supongamos que

$$a_i(x) = a^i_{n_i} x^{n_i} + a^i_{n_i - 1} x^{n_i - 1} + \cdots + a^i_1 x + a^1_0$$

y que $d \in R$ es R-divisor común de todas las a^i_j con $j \in \{1, \ldots, n_i\}$. De esta manera, es fácil ver que el polinomio constante $d \in R[x]$ es $R[x]$-divisor de $a_i(x)$. Como $a_i(x)$ es $R[x]$-divisor común de $p(x)$, lo anterior implica que $d \in R[x]$ es $R[x]$-divisor común de $p(x)$. Entonces existe $k(x) \in R[x]$ tal que $dk(x) = p(x)$ y por lo tanto, $\deg k(x) = \deg p(x) = n$.

En particular, si

$$k(x) = k_n x^n + k_{n-1} x^{n-1} + \cdots + k_1 x + k_0 \quad \text{y}$$
$$p(x) = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_1 x + p_0$$

entonces la igualdad $dk(x) = p(x)$ implica que $dk_i = p_i$ para toda $i \in \{1, \ldots, n\}$. En particular, d es R-divisor común de los coeficientes de $p(x)$ y por lo tanto, (como $p(x)$ es primitivo) entonces $d|1$.

En resumen, acabamos de demostrar que todo divisor común de $a_1^i, \ldots, a_{n_i}^i$ divide al 1. Por lo tanto, el 1 es máximo común divisor de los coeficientes de $a_i(x)$ y $p(x)$ es primitivo. $\square$

R es un DFU $\iff$ $R[x]$ es un DFU

Proposición 6

Supongamos que R es un domino entero. Entonces R es un DFU si y solo si $R[x]$ es un DFU.

Demostración.
$\Longleftarrow$) Supongamos que $R[x]$ es un DFU y que $p \in R$ no es invertible.

Existencia de la factorización.
Como $p \in R$, $R \subset R[x]$, y $R[x]$ es DFU, entonces existe una factorización en irreducibles de $R[x]$ para p. Es decir, existen $p_1(x), \ldots, p_n(x) \in R[x]$ irreducibles en $R[x]$ tales que

$$p = p_1(x) \cdots p_n(x) \tag{3}$$

Usando que $\deg p = 0$ y que $\deg\big(p(x)q(x)\big) = \deg p(x) + \deg q(x)$, es fácil ver que la ecuación anterior implica que $p_i(x)$ es constante para toda i.

Es decir, podemos escribir $p_i(x) = p_i \in R$. Además, cada p_i también es irreducible en R porque $R \subset R[x]$. Por lo tanto, para ver que (3) es la factorización buscada, solo resta probar su unicidad.

Unicidad de la factorización.
Es consecuencia inmediata de la unicidad de la factorización en $R[x]$ y del hecho de que los elementos invertibles en $R[x]$ son precisamente los elementos invertibles en R.

$\Longrightarrow$) Naturalmente, haremos uso del primer inciso del lema anterior y por eso, suponemos que $p(x)$ es primitivo y que $n := \deg p(x) \geq 1$.

Existencia de la factorización.
Como $p(x)$ no es invertible[5] y $F[x]$ es un dominio de factorización única, entonces existen $A_1(x), \ldots, A_m(x) \in F[x]$ irreducibles tales que

$$p(x) = A_1(x) \cdots A_m(x).$$

Luego, por el lema de Gauss generalizado, existen $a_1(x), \ldots, a_m(x) \in R[x]$ y $r_1, \ldots, r_m \in F$ tales que

$$p(x) = a_1(x) \cdots a_m(x) \quad \text{y} \quad a_i(x) = r_i A_i(x) \text{ para toda } i \in \{1, \ldots, m\} \tag{4}$$

Como r_i es invertible[6] y $A_i(x)$ es irreducible en $F[x]$, entonces la igualdad $a_i(x) = r_i A_i(x)$ implica[7] que $a_i(x) \in R[x]$ es irreducible en $F[x]$.

Usando
(i) que $a_i(x) \in R[x]$ es irreducible en $F[x]$,
(ii) la proposición "Condiciones suficientes para que $q(x) \in R[x]$ irreducible en $R[x] \iff q(x) \in R[x]$ irreducible en $F[x]$", y
(iii) el inciso 2 del lema anterior,
obtenemos que $a_i(x)$ es irreducible en $R[x]$.

Por lo tanto, para ver que la primera igualdad en (4) es la factorización buscada, solo resta probar su unicidad.

[6] Pues F es campo y $r_i \in F \setminus \{0\}$.
[7] Recuerda que si u es invertible y v es irreducible, entonces uv es irreducible.

Unicidad de la factorización
Supongamos que $q_1(x), \ldots, q_r(x), q'_1, \ldots, q'_s(x) \in R[x]$ son irreducibles en $R[x]$ y que

$$p(x) = q_1(x) \cdots q_r(x) \quad \text{y} \quad p(x) = q'_1(x) \cdots q'_s(x) \tag{5}$$

Como $p(x)$ es primitivo, el inciso 2 del lema anterior implica $q_i(x)$ y $q'_j(x)$ también son primitivos para toda i y toda j. Usando esto y la proposición "Condiciones suficientes para que $q(x) \in R[x]$ irreducible en $R[x] \iff$ $q(x) \in R[x]$ irreducible en $F[x]$" obtenemos que $q_1(x), \ldots, q_r(x), q'_1, \ldots, q'_s(x) \in R[x]$ son irreducibles en $F[x]$. Usando (i) esto, (ii) la igualdad (5), y (iii) que $F[x]$ es un DFU, obtenemos que $r = s$, y que (después de reordenar los índices) $q_i(x) = \frac{a}{b} q'_i(x)$ para algunos $a, b \in R$. Equivalentemente, $bq_i(x) = aq'_i(x)$.

Ahora bien, (como $q_i(x)$ y $q_i'(x)$ son primitivos) es fácil verificar que b es un mcd de los coeficientes de $bq_i(x)$ y que a es un mcd de los coeficientes de $aq_i'(x)$. Pero como $bq_i(x) = aq_i'(x)$, estos coeficientes son precisamente los mismos elementos. En particular, existen elementos en R para los cuales b y a son mcd. Como el mcd es único salvo asociados, entonces existe $u \in R$ invertible tal que $b = ua$. Sustituyendo esto en $bq_i(x) = aq_i'(x)$ y cancelando a, obtenemos $uq_i(x) = q_i'(x)$. Es decir, $q_i(x)$ y $q_i'(x)$ son $R[x]$-asociados y por lo tanto, las factorizaciones en irreducibles en $R[x]$ son únicas salvo asociados.

□

Una consecuencia inmediata de este resultado es que $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$ son DFU's.
Otra consecuencia inmediata de este resultado y de la igualdad $R[x_1, \ldots, x_n] = \big(R[x_1, \ldots, x_{n-1}]\big)\,[x_n]$ es la siguiente proposición.

R es un DFU $\iff$ $R[x_1, \ldots, x_n]$ es un DFU

Proposición 7

Supongamos que R es un dominio entero. Entonces R es un DFU si y solo si $R[x_1, \ldots, x_n]$ es un DFU.

Demostración. Procedamos por inducción sobre n. El paso base es la proposición anterior. Para el paso inductivo, supongamos que

$$R \text{ es un DFU} \iff R[x_1, \ldots, x_{n-1}] \text{ es un DFU.} \tag{6}$$

Por otro lado, la proposición anterior y la igualdad $R[x_1, \ldots, x_n] = \big(R[x_1, \ldots, x_{n-1}]\big)[x_n]$ implican que

$$R[x_1, \ldots, x_{n-1}] \text{ es un DFU} \iff R[x_1, \ldots, x_n] \text{ es un DFU.} \tag{7}$$

Juntando (6) y (7) obtenemos lo deseado. □

En particular, $\mathbb{Z}[x_1, \ldots, x_n]$ y $\mathbb{Q}[x_1, \ldots, x_n]$ son DFU's.