El algoritmo de la división para polinomios con coeficientes en un campo

Facultad de Ciencias UNAM

Introducción

En esta sección demostramos que $F[x]$ es un dominio euclidiano con la norma dada por $N(p(x)) = \deg p(x)$ si $p(x) \neq 0$ y $N(0) =^1 0$ si F es un campo. También veremos que este hecho combinado con la importancia del concepto de grado de un polinomio nos da mas información acerca de $F[x]$.

[1] Recuerda que por definición $\deg 0 = -1$ y por lo tanto, $N(0) = \deg 0 = -1 < 0$ no definiría una norma.

El algoritmo de la división en $F[x]$

Proposición 1

Supongamos que F es un campo. Si $a(x), b(x) \in F[x]$ con $b(x) \neq 0$, entonces existen $q(x), r(x) \in F[x]$ únicos tales que

$$a(x) = q(x)b(x) + r(x) \text{ con } r(x) = 0 \text{ o } \deg r(x) < \deg b(x).$$

En particular, $F[x]$ es un dominio euclidiano con la norma N dada por $N(p(x)) = \deg p(x)$ si $p(x) \neq 0$ y $N(0) = 0$.

Demostración.

Existencia.
En caso de que $a(x) = 0$, obviamente $q(x) := 0$ y $r(x) := 0$ cumplen lo deseado. Por lo tanto, supongamos que $a(x) \neq 0$. Veamos la existencia de $q(x)$ y $r(x)$ usando inducción (fuerte) sobre $\deg a(x)$.

Paso base. Supongamos que $\deg a(x) = 0$.
Si $\deg b(x) = 0$, entonces $a(x)$ y $b(x)$ son polinomios constantes y por lo tanto existen $\alpha, \beta \in R$ tales que $a(x) = \alpha$ y $b(x) = \beta$. Es fácil verificar que $q(x) \coloneqq \frac{\alpha}{\beta}$ y $r(x) \coloneqq 0$ cumplen lo deseado (cabe recalcar que $\frac{\alpha}{\beta}$ existe porque F es campo).
Si $\deg b(x) > 0$, entonces $q(x) \coloneqq 0$ y $r(x) \coloneqq a(x)$ cumplen lo deseado, pues por el caso en el que estamos, $\deg r(x) = \deg a(x) = 0 < \deg b(x)$.

Paso inductivo. Sea $n \in \mathbb{Z}_{>1}$ fija y supongamos que para toda $a'(x), b'(x) \in F[x]$ con $\deg a'(x) < n$ y $b'(x) \neq 0$, existen $q'(x), r'(x)$ únicos tales que

$$a'(x) = q'(x)b'(x) + r'(x) \text{ con } r(x) = 0 \text{ o } \deg r(x) < \deg b(x).$$

Ahora bien, sean $a(x), b(x) \in F[x]$ con $\deg a(x) \geq 1$ y $b(x) \neq 0$, veamos que existen $q(x), r(x)$ únicos tales que

$$a(x) = q(x)b(x) + r(x) \text{ con } r(x) = 0 \text{ o } \deg r(x) < \deg b(x).$$

Para esto, denotemos

$$\deg a(x) = n \quad \text{y} \quad a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$
$$\deg b(x) = m \quad \text{y} \quad b(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

Si $\deg a(x) < \deg b(x)$, entonces $q(x) := 0$ y $r(x) := a(x)$ cumplen lo deseado, pues por el caso en el que estamos, $\deg r(x) = \deg a(x) < \deg b(x)$.
Si $\deg a(x) \geq \deg b(x)$, definimos

$$a'(x) := a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$$

Usando que el termino delantero de $a(x)$ y de $\frac{a_n}{b_m} x^{n-m} b(x)$ es el mismo $(a_n x^n)$, obtenemos que $\deg a'(x) < n$.

Por lo tanto, podemos aplicar la hipótesis de inducción a $a'(x)$ y $b'(x) := b(x)$ para obtener $q'(x), r'(x) \in F[x]$ únicos tales que

$$a(x) - \frac{a_n}{b_m} x^{n-m} b(x) = a'(x) = q'(x)b'(x) + r'(x) = q'(x)b(x) + r'(x) \qquad (1)$$

Veamos que

$$q(x) := q'(x) + \frac{a_n}{b_m} x^{n-m} \quad \text{y} \quad r(x) := r'(x) \qquad (2)$$

cumplen lo deseado:

$$
\begin{aligned}
q(x)b(x) + r(x) &= \left(q'(x) + \frac{a_n}{b_m}x^{n-m}\right) b(x) + r'(x) && \text{(sustituyendo (2))} \\
&= q'(x)b(x) + \frac{a_n}{b_m}x^{n-m}b(x) + r'(x) && \text{(distribuyendo)} \\
&= q'(x)b(x) + r'(x) + \frac{a_n}{b_m}x^{n-m}b(x) && \text{(conmutando)} \\
&= a(x) - \frac{a_n}{b_m}x^{n-m}b(x) + \frac{a_n}{b_m}x^{n-m}b(x) = a(x) \\
& && \text{(sustituyendo (1))}
\end{aligned}
$$

y

$$\deg r(x) = \deg r'(x) < \deg b'(x) = \deg b(x)$$

por la forma en la que pedimos r, r', y b'.
Fin de la demostración de la existencia.

Unicidad.
Supongamos que $a(x), b(x) \in F[x]$ con $b(x) \neq 0$. Si
$q(x), r(x), q_1(x), r_1(x) \in F[x]$ son tales que

$$a(x) = q(x)b(x) + r(x) \text{ con } r(x) = 0 \text{ o } \deg r(x) < \deg b(x) \quad \text{y}$$
$$a(x) = q_1(x)b(x) + r_1(x) \text{ con } r_1(x) = 0 \text{ o } \deg r_1(x) < \deg b(x),$$

entonces

$$r(x) = a(x) - q(x)b(x) \quad \text{y} \quad r_1(x) = a(x) - q_1(x)b(x), \tag{3}$$

entonces

$$\deg \big(a(x) - q(x)b(x)\big) = \deg r(x) < \deg b(x) \quad \text{y}$$
$$\deg \big(a(x) - q_1(x)b(x)\big) = \deg r_1(x) < \deg b(x),$$

entonces

$$\begin{aligned}
\deg b(x) + \deg\big(q(x) - q_1(x)\big) &= \\
\deg\Big(b(x)\big(q(x) - q_1(x)\big)\Big) &= \\
\deg\big(b(x)q(x) - b(x)q_1(x)\big) &= \\
\deg\Big(\big(a(x) - q(x)b(x)\big) - \big(a(x) - q_1(x)b(x)\big)\Big) &\leq \\
\text{máx}\Big\{\deg\big(a(x) - q(x)b(x)\big), \deg\big(a(x) - q_1(x)b(x)\big)\Big\} &= \\
\text{máx}\big\{\deg r(x), \deg r_1(x)\big\} &< \\
\deg b(x)
\end{aligned}$$

entonces

$$\deg\big(q(x) - q_1(x)\big) < 0$$

y por lo tanto, $q(x) - q_1(x) = 0$, o equivalentemente, $q(x) = q_1(x)$. Finalmente, sustituyendo esto en (3), obtenemos $r(x) = r_1(x)$.
Fin de la demostración de la unicidad.

□

Un corolario obvio pero importante del algoritmo de la división en $F[x]$

Proposición 2

Supongamos que F es un campo. Entonces,

- $F[x]$ es un DE.
- $F[x]$ es un DIP.
- $F[x]$ es un DFU.

Demostración. Es consecuencia inmediata de que

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

□

Observación

En la proposición 1.19.9. demostramos que si $F[x]$ es un DIP, entonces F es un campo. Juntando esto con el corolario anterior obtenemos las siguientes equivalencias.

$$F \text{ es un campo} \iff F[x] \text{ es un DIP} \iff F[x] \text{ es un DE}$$

Una consecuencia inmediata de esta equivalencia es la siguiente:

- $\mathbb{Z}[x]$ no es un DIP (pues $\mathbb{Z}$ no es un campo)[2].
- $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong \mathbb{Z}/p\mathbb{Z}[x] = \mathbb{Z}_p[x]$ es un DIP si $p \in \mathbb{Z}_{\geq 1}$ es primo (pues $\mathbb{Z}_p$ es un campo).

En particular, acabamos de demostrar que sacarle cociente a un no DIP puede producir un DIP. En otras palabras,

$$R/I \text{ es un DIP} \not\Longrightarrow R \text{ es un DIP.}$$

[2]Recordemos que ya sabíamos esto pues habíamos demostrado que el ideal $(2, x)$ de $\mathbb{Z}[x]$ no es principal.

Una consecuencia interesante de la unicidad del cociente y residuo del algoritmo de la división en $F[x]$.

Corolario 3

Supongamos que F, E son campos tales que $F \subset E$. Si $a(x), b(x) \in F[x]$ con $b(x) \neq 0$, entonces

$$b(x) \text{ divide a } a(x) \text{ en } F[x] \iff b(x) \text{ divide a } a(x) \text{ en } E[x].$$

Demostración.

$\Longrightarrow$) Es consecuencia inmediata de que $F \subset E$.

$\Longleftarrow$) Supongamos que $b(x)$ divide a $a(x)$ en $E[x]$. Entonces existe $k(x) \in E[x]$ tal que $k(x)b(x) = a(x)$. Por otro lado, sean $q(x), r(x) \in F[x]$ los polinomios inducidos por el algoritmo de la división en $F[x]$ aplicado a $a(x)$ y $b(x)$. Entonces

$$q(x)b(x) + r(x) = a(x) = k(x)b(x)$$

Pero entonces, la unicidad del cociente y residuo en $E[x]$ implica que $q(x) = k(x)$ y $r(x) = 0$. En particular, $q(x) \in F[x]$ y por lo tanto, $b(x)$ divide a $a(x)$ en $F[x]$.

$\square$

Comentario

Recuerda que si R es un anillo con unidad y $a, b \in R$, entonces $d \in R$ es un máximo común divisor de a y b en R si

- d es divisor común (en R) de a y b, es decir existen $r, s \in R$ tales que $dr = a$ y $ds = b$.
- Todo divisor común (en R) de a y b divide a d.

Por ejemplo, si F es un campo, y $f(x), g(x) \in F[x]$, entonces $p(x) \in F[x]$ es máximo divisor común de $f(x)$ y $g(x)$ en $F[x]$ si

- Existen $a(x), b(x) \in F[x]$ tales que $p(x)a(x) = f(x)$ y $p(x)b(x) = g(x)$.
- Si $q(x) \in F[x]$ tal que $q(x)$ divide a $f(x)$ y $g(x)$ en $F[x]$, entonces $q(x)$ divide a $p(x)$ en $F[x]$.

Notemos que aquí hicimos énfasis en el hecho de que la propiedad "ser divisor" depende en el anillo en donde estamos considerando a los elementos. En el siguiente corolario veremos que en el caso de anillos de polinomios, este cuidado no es necesario.

El máximo común divisor de dos polinomios

Corolario 4

Supongamos que F, E son campos tales que $F \subset E$. Si $f(x), g(x) \in F[x]$, entonces el máximo común divisor de $f(x)$ y $g(x)$ en $F[x]$ coincide con el máximo común divisor de $f(x)$ y $g(x)$ en $E[x]$. En otras palabras, para todo $p(x) \in F[x]$

$$p(x) \text{ es mcd de } f(x) \text{ y } f(x) \text{ en } F[x] \iff p(x) \text{ es mcd de } f(x) \text{ y } f(x) \text{ en } E[x].$$

Demostración. Esto es inmediato por la definición de máximo común divisor y porque el corolario anterior implica que

$$q(x) \text{ es divisor común de } f(x) \text{ y } g(x) \text{ en } F[x] \iff q(x) \text{ es divisor común de } f(x) \text{ y } g(x) \text{ en } E[x].$$

□

Comentario

Como estamos estudiando divisibilidad en anillos de polinomios y

$$b(x) \text{ divide a } a(x) \text{ en } F[x] \iff a(x) \in \big(b(x)\big)\,,$$

es natural interesarse en entender un poquito mejor los ideales de la forma $\big(p(x)\big)$. En lo que sigue, hacemos precisamente esto. Como es de esperarse, el algoritmo de la division en $F[x]$ jugara un papel muy importante.

El cociente de $F[x]$ por un ideal principal

Proposición 5

Supongamos que F es un campo. Si $p(x) \in F[x]$, entonces los siguientes incisos son equivalentes:

1. $p(x)$ es irreducible[3] en $F[x]$
2. $F[x]/(p(x))$ es un dominio entero
3. $F[x]/(p(x))$ es un campo

En particular, como $R[x]/(x) \cong R$, el polinomio $p(x) = x$ es irreducible cuando R es un dominio entero.

[3] Después veremos la importancia de los polinomios irreducibles y por lo tanto, la utilidad de esta equivalencia.

Demostración.

La equivalencia

$$p(x) \text{ es irreducible en } F[x] \iff F[x]/(p(x)) \text{ es un dominio entero}$$

es consecuencia de que (i) $F[x]$ es un DIP (pues F es campo), (ii) el hecho de que en un DIP, "elemento primo $\iff$ elemento irreducible" (c.f. proposición 1.19.5), y (iii) la caracterización de ideales primos en términos del cociente.

La equivalencia

$$F[x]/(p(x)) \text{ es un dominio entero} \iff F[x]/(p(x)) \text{ es un campo}$$

es consecuencia de que (i) $F[x]$ es un DIP, (ii) el hecho de que en un DIP, "ideal primo $\iff$ ideal maximal" (c.f. proposición 1.19.6), (iii) la caracterización de ideales primos en términos del cociente, y (iv) la caracterización de ideales maximales en términos del cociente. □

Una descripción de $F[x]/(p(x))$ cortesía del algoritmo de la división en $F[x]$

Proposición 6

Supongamos que F es un campo. Si $p(x) \in F[x]$ y $\deg p(x) \geq 1$, entonces para toda $a(x) \in F[x]$, existe un único $b(x) \in F[x]$ tal que $a(x) = \overline{b(x)}$ y $\deg b(x) < \deg p(x)$. En particular,

$$F[x]/(p(x)) = \left\{ \overline{b(x)} \mid \deg b(x) < \deg p(x) \right\}.$$

Demostración. Supongamos que $a(x) \in^4 F[x] \setminus \{0\}$. Como $\deg p(x) \geq 1$, en particular $p(x) \neq 0$ y por lo tanto, por el algoritmo de la división en $F[x]$, existen $q(x), r(x) \in F[x]$ únicos tales que

$$a(x) = q(x)p(x) + r(x) \text{ con } r(x) = 0 \text{ o } \deg r(x) < \deg p(x) \tag{4}$$

En caso de que $r(x) = 0$, entonces $p(x)|a(x)$ y por lo tanto, $\overline{a(x)} = \overline{p(x)} = \overline{0}$. Como $\deg 0 = -1 < 1 \leq \deg p(x)$, entonces $b(x) := 0$ cumple lo deseado.

En caso de que $\deg r(x) < \deg p(x)$, entonces restamos $r(x)$ en ambos lados de (4) para obtener

$$a(x) - r(x) = q(x)p(x).$$

En particular, $p(x)|a(x) - r(x)$ o equivalentemente $\overline{a(x)} = \overline{r(x)}$. Por lo tanto, $b(x) := r(x)$ cumple lo deseado. □

[4] El caso $a(x) = 0$ es trivial porque $\deg 0 = -1 < 1 \leq \deg p(x)$.

La cardinalidad de $F[x]/(p(x))$ cuando F es finito

Proposición 7

Supongamos que F es un campo y que $p(x) \in F[x]$. Si F es finito y $\deg p(x) \geq 1$, entonces

$$|F[x]/(p(x))| = |F|^{\deg p(x)}.$$

Demostración. Denotemos $n := \deg p(x)$. Como todo polinomio de grado $< n$ es de la forma

$$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0, \tag{5}$$

entonces por un argumento de combinatoria básica, hay exactamente $|F|^n = |F|^{\deg p(x)}$ polinomios de grado $< n = \deg p(x)$. En efecto, todo polinomio de la forma (5) lo podemos identificar con la n-ada

$$(a_{n-1}, a_{n-2}, \ldots, a_1, a_0). \tag{6}$$

Como hay $|F|$ opciones para cada coordenada, entonces hay exactamente $|F|^n = |F|^{\deg p(x)}$ n-adas de la forma (6) o equivalentemente hay exactamente $|F|^n = |F|^{\deg p(x)}$ polinomios de grado $< n = \deg p(x)$. En otras palabras,

$$\left| \left\{ \overline{b(x)} \mid \deg p(x) < \deg p(x) \right\} \right| = |F|^{\deg p(x)}.$$

Usando los incisos 2.i. y 2.ii. obtenemos lo deseado. $\square$