Polinomios en varias variables

Facultad de Ciencias UNAM

Introducción

En esta sección introducimos y estudiamos a los anillos de polinomios en varias variables. Veremos que hay dos formas distintas de ver a este anillo y (en esta y las siguientes secciones) también veremos que gozan de muchas de las propiedades que gozan los polinomios de una sola variable.

Polinomios en varias variables

Supongamos que R es un anillo y que $x_1, \ldots, x_n$ son variables indeterminadas. Un **polinomio en** $x_1, \ldots, x_n$ **con coeficientes en** R es una suma finita de elementos de la forma

$$ax_1^{d_1} \cdots x_n^{d_n} \tag{1}$$

donde $a \in R$ y $d_i \in \mathbb{Z}_{\geq 0}$ para toda $i \in \{1, \ldots, n\}$.

Por ejemplo,

$$xy^2 + y^2 + x^2y + 3y + x + 3$$

es un polinomio en x, y con coeficientes en $\mathbb{Z}$.

A el conjunto de todos los polinomios en $x_1, \ldots, x_n$ con coeficientes en R lo denotamos por $R[x_1, \ldots, x_n]$ y lo llamamos el **anillo de polinomios en** $x_1, \ldots, x_n$ **sobre** R.

Siguiendo la notación usual para polinomios de una sola variable, denotamos a los elementos de $R[x_1, \ldots, x_n]$ por símbolos como "$p(x_1, \ldots, x_n)$" o "$a(x_1, \ldots, x_n)$".

Supongamos que $a \in R$ y $d_1, \ldots, d_n \in \mathbb{Z}_{\geq 0}$. Definimos **el grado de** $ax_1^{d_1} \cdots x_n^{d_n}$ como $d_1 + \cdots d_n$ y escribimos

$$\deg ax_1^{d_1} \cdots x_n^{d_n} = d_1 + \cdots d_n$$

Supongamos que $p(x_1, \ldots, x_n) = \sum_{i=0}^{n} a_i x_1^{d_1^i} \cdots x_n^{d_n^i} \in R[x_1, \ldots, x_n]$.

- Para cada $i \in \{1, \ldots, n\}$, decimos que $ax_1^{d_1} \cdots x_n^{d_n}$ es un **termino de** $p(x_1, \ldots, x_n)$. Por ejemplo, si

  $$p(x, y, z) = 2x^3y + 3y^2z^2 + 3xz + 5$$

  entonces $2x^3y$, $3y^2z^2$, $3xz$ y 5 son términos de $p(x, y, z)$.
- El **grado de** $p(x_1, \ldots, x_n)$ es el mayor de los grados de sus términos. En otras palabras,

$$\deg \left(\sum_{i=0}^{n} a_i x_1^{d_1^i} \cdots x_n^{d_n^i} \right) = \max_{i=0}^{n} \left\{ d_1^i + \cdots + d_n^i \right\}$$

Las operaciones que hacen que $R[x_1, \ldots, x_n]$ sea un anillo son las siguientes: en ambos casos, las definimos primero para términos de la forma (1) y luego las extendemos sobre todo $R[x_1, \ldots, x_n]$ de la unica forma posible.

Supongamos que $a, b \in R$ y que $d_1, \ldots, d_n, e_1, \ldots, e_n \in \mathbb{Z}_{\geq 0}$.

La suma:
Si $d_i = e_i$ para toda $i \in \{1, \ldots, n\}$ definimos

$$\left(ax_1^{d_1} \cdots x_n^{d_n}\right) + \left(bx_1^{e_1} \cdots x_n^{e_n}\right) = (a+b)x_1^{d_1} \cdots x_n^{d_n}$$

En otro caso, simplemente definimos

$$\left(ax_1^{d_1} \cdots x_n^{d_n}\right) + \left(bx_1^{e_1} \cdots x_n^{e_n}\right) = ax_1^{d_1} \cdots x_n^{d_n} + bx_1^{e_1} \cdots x_n^{e_n}$$

recordemos que los elementos de $R[x_1, \ldots, x_n]$ son sumas finitas de elementos como los de (1) y por lo tanto, el lado derecho de la igualdad anterior tiene sentido.

La multiplicación:

$$\left(ax_1^{d_1}\cdots x_n^{d_n}\right)\cdot\left(bx_1^{e_1}\cdots x_n^{e_n}\right)=(ab)x_1^{d_1+e_1}\cdots x_n^{d_n+e_n}$$

Por ejemplo, consideremos los siguientes elementos de $\mathbb{Z}[x,y]$

$$p(x)=2x^3+xy-y^2 \quad \text{y} \quad q(x,y)=-3xy+2y^2+x^2y^3.$$

Entonces

$$\begin{aligned} p(x)+q(x) &= 2x^3-2xy+y^2+x^2y^3 \quad \text{y} \\ p(x)\cdot q(x) &= -6x^4y+4x^3y^2+2x^5y^3-3x^2y^2+ \\ &\qquad 5xy^3+x^3y^4-2y^4-x^2y^5. \end{aligned}$$

Otra manera de ver a $R[x_1, \ldots, x_n]$

Proposición 1

Supongamos que R es un anillo y que $x_1, \ldots, x_n$ son variables indeterminadas. Para toda $i \in \{1, \ldots, n\}$ tenemos

$$R[x_1, \ldots, x_n] \cong \left(R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]\right)[x_i].$$

Sea $\varphi : R[x_1, \ldots, x_n] \to \left(R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]\right)[x_i]$ tal que

$$\sum_{i=0}^{n} a_i x_1^{d_1^i} \cdots x_n^{d_n^i} \mapsto \sum_{i=0}^{n} \left(a_i x_1^{d_1^i} \cdots x_{i-1}^{d_{i-1}} x_{i+1}^{d_{i+1}} \cdots x_n^{d_n^i} \right) x_i^{d_i}$$

para toda $a \in R$ y toda $d_1, \ldots, d_n \in \mathbb{Z}_{\geq 0}$. Por ejemplo, si $R[x_1, \ldots, x_n] = \mathbb{Z}[x, y]$, entonces

$$xy^2 + y^2 + x^2y + 3y + x + 3 \mapsto (x+1)y^2 + (x^2+3)y + (x+3)$$

Es fácil verificar que φ es un isomorfismo. $\square$

Observación

- La naturalidad del isomorfismo anterior implica que podemos ver a los elementos de $R[x_1, \ldots, x_n]$ como polinomios en x_n con coeficientes en $R[x_1, \ldots, x_{n-1}]$. Por eso, hacemos la siguiente convención

$$R[x_1, \ldots, x_n] = \left(R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]\right)[x_i].$$

- $\mathbb{Q}[x, y]$ *no* es un DIP:

  Esto es consecuencia de que
  - $\mathbb{Q}[x, y] = \left(\mathbb{Q}[x]\right)[y]$,
  - $\mathbb{Q}[x]$ no es campo[1], y
  - La proposición que dice "$R[z]$ es un PID $\implies$ R es un campo" (c.f. proposición 1.19.9).

[1] Todo polinomio de grado ≥ 1 no es invertible.

El ideal $(x_1, \ldots, x_n)$ de $R[x_1, \ldots, x_n]$

Proposición 2

Supongamos que R es un anillo conmutativo y que $n \in \mathbb{Z}_{\geq 1}$. Entonces

1. $(x_1, \ldots, x_n) = \{\text{los polinomios con constante} = 0\}$.
2. $R[x_1, \ldots, x_n]/(x_1, \ldots, x_n) \cong R$.

Demostración.

1. $\subset$) Primero notemos que $\{\text{los polinomios con constante} = 0\}$ es un ideal. Luego, como $x_1, \ldots, x_n \in \{\text{los polinomios con constante} = 0\}$, entonces $(x_1, \ldots, x_n) \subset \{\text{los polinomios con constante} = 0\}$.
   $\supset$) Primero notemos que todos los monomios con grado mayor o igual a 1 pertenecen a $(x_1, \ldots, x_n)$. En efecto, supongamos que $ax_1^{d_1} \cdots x_n^{d_n}$ tiene grado mayor o igual a 1. Entonces existe i tal que $d_i \geq 1$ y por la siguiente igualdad tiene sentido.

$$ax_1^{d_1} \cdots x_n^{d_n} = \left(ax_1^{d_1} \cdots x_i^{d_i - 1} \cdots x_n^{d_n}\right) x_i \in (x_i) \subset (x_1, \ldots, x_n)$$

Demostración.

2. Sea $\varphi : R[x_1, \ldots, x_n] \to R$ tal que

$$p(x_1, \ldots, x_n) \mapsto p(0, \ldots, 0) = \text{el termino constante de } p(x_1, \ldots, x_n)$$

Es fácil verificar que φ es un homomorfismo suprayectivo y que

$$\ker \varphi = \{\text{los polinomios con constante} = 0\} = (x_1, \ldots, x_n)$$

donde la segunda igualdad es por el inciso anterior. Por lo tanto,

$$R[x_1, \ldots, x_n]/(x_1, \ldots, x_n) = R[x_1, \ldots, x_n]/\ker \varphi \cong \operatorname{im} \varphi = R.$$

□

Un isomorfismo útil

Proposición 3

Supongamos que R es un anillo conmutativo y que $n \in \mathbb{Z}_{\geq 1}$. Considera el anillo $R[x_1, \ldots, x_n]$. Entonces para toda $i \in \{1, \ldots, n\}$

1. $(x_i) = \left\{ \sum_{j=0}^{n} a_j x_1^{d_1^j} \cdots x_n^{d_n^j} \mid d_i^j \geq 1 \text{ para toda } j \right\}$.
2. $R[x_1, \ldots, x_n]/(x_i) \cong R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$.

1. Veamos que para toda $i \in \{1, \ldots, n\}$

$$(x_i) = \left\{ \sum_{j=0}^{n} a_j x_1^{d_1^j} \cdots x_n^{d_n^j} \mid d_i^j \geq 1 \text{ para toda } j \right\}.$$

$\subset$) Supongamos que $p(x_1, \ldots, x_n) \in (x_i)$. Por definición, existen $b_1, \ldots, b_m \in R$ y $d_1^k, \ldots, d_n^k \in \mathbb{Z}_{\geq 0}$ (para cada $k \in \{1, \ldots, m\}$) tales que

$$\begin{aligned} p(x_1, \ldots, x_n) &= \left(\sum_{k=0}^{m} b_k x_1^{e_1^k} \cdots x_n^{e_n^k} \right) x_i \\ &= \sum_{k=0}^{m} b_k x_1^{e_1^k} \cdots x_{i-1}^{e_{i-1}^k} x_i^{e_i^k+1} x_{i+1}^{e_{i+1}^k} \cdots x_n^{e_n^k} \end{aligned}$$

Como $e_i^k + 1 \geq 1$, la igualdad anterior implica lo deseado.

$\supset$) Es consecuencia inmediata de que $d_i^j \geq 1$ para toda j: a cualquier elemento de $\left\{ \sum_{j=0}^{n} a_j x_1^{d_1^j} \cdots x_n^{d_n^j} \mid d_i^j \geq 1 \text{ para toda } j \right\}$ le podremos factorizar el polinomio x_i.

2. Veamos que $R[x,y]/(x) \cong R[y]$. La idea para el caso general es la misma.

   Sea $\phi : R[x,y] \to R[y]$ tal que $\phi(p(x))$ es el polinomio en $R[y]$ que se obtiene a partir de omitir los términos de $p(x)$ que *no* son de la forma ay^k. Por ejemplo, si $R = \mathbb{Z}$

$$\phi\left(y^3 + xy^2 + 2xy + 5y^2 + 3x + 2\right) = y^3 + 5y^2.$$

   Es fácil verificar que φ es un homomorfismo de anillos suprayectivo.

   Veamos que $\ker \phi = (x)$.

   Supongamos que $p(x,y) \in \ker \phi$. Por definición de φ, esto es si y solo si $p(x,y)$ no contiene ningún termino de la forma ay^k. Pero esto es si y solo si $p(x,y)$ es una suma finita de términos de la forma $ax^d y^e$ con $a \in R$, $e \in \mathbb{Z}_{\geq 0}$, y $d \in \mathbb{Z}_{\geq 1}$. Luego, usando el inciso anterior obtenemos lo deseado.

   Finalmente, por el primer teorema de isomorfismos,

$$R[x,y]/(x) = R[x,y]/\ker \phi \cong \operatorname{im} \phi = R[y].$$

□

Observación

- Otra forma (tal vez mas elegante) de demostrar el inciso (2) de la proposición anterior es la siguiente:

$$\begin{aligned} R[x_1,\ldots,x_n]/(x_i) &= \Big(\big(R[x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n\big)\,[x_i]\Big)\,/(x_i) \\ &\cong R[x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n]. \end{aligned}$$

(c.f. proposición 1.9.3)

- Si R es un dominio entero, entonces (x,y) es un ideal primo en $R[x,y]$: Esto es consecuencia de (i) la caracterización de ideales primos y (ii) el isomorfismo $R[x,y]/(x,y) \cong R$.
- Si R es un campo, entonces (x,y) es un ideal maximal en $R[x,y]$: Esto es consecuencia de (i) la caracterización de ideales maximales y (ii) el isomorfismo $R[x,y]/(x,y) \cong R$.

Mas ideales primos y maximales en anillos de polinomios de varias variables

Veamos que

1. $\mathbb{Z}[x,y]/(2,x,y) \cong \mathbb{Z}_2$. En particular, como $\mathbb{Z}_2$ es un campo, entonces (por la caracterización de ideales maximales) $(2,x,y)$ es un ideal maximal en $\mathbb{Z}[x,y]$.
2. $\mathbb{Q}[x,y]/(x) \cong \mathbb{Q}[y]$. En particular, como $\mathbb{Q}[y]$ es un dominio entero (pues $\mathbb{Q}$ es dominio entero), entonces (por la caracterización de ideales primos) (x) es un ideal primo en $\mathbb{Q}[x,y]$.

Demostración.

1. Sea $\varphi : \mathbb{Z}[x,y] \to \mathbb{Z}_2$ tal que

$$p(x,y) \mapsto \big[p(0,0)\big]_2 = \text{la clase de equiv. mod 2 del termino constante de } p(x,y)$$

Es fácil verificar que φ es un homomorfismo de anillos suprayectivo.

Veamos que $\ker \varphi = (2, x, y)$.
Como $\ker \varphi$ es un ideal y claramente $2, x, y \in \ker \varphi$, entonces $(2, x, y) \subset \ker \varphi$. Conversamente, supongamos que $p(x) \in \ker \varphi$. Por la definición de φ, debería de ser claro que esto es equivalente a que el termino constante de $p(x)$ sea par. Por lo tanto, basta probar que todo polinomio con termino constante par pertenece a $(2, x, y)$. Pero esto es consecuencia de que si $p(x)$ tiene tiene termino constante par, es decir $p(0)$ es par, entonces

$$p(x) = \underbrace{p(x) - p(0)}_{\in (x,y)} + \underbrace{p(0)}_{\in (2)} \in (x, y) + (2) = (2, x, y)$$

donde $p(x) - p(0) \in (x, y)$ porque
$(x, y) = \{\text{los polinomios con constante} = 0\}$. Finalmente, por el primer teorema de isomorfismos,

$$\mathbb{Z}[x, y]/(2, x, y) = \mathbb{Z}[x, y]/\ker \varphi \cong \operatorname{im} \varphi = \mathbb{Z}_2.$$

Notación

Por el resto de la sección (cuando sea conveniente) denotamos $X = x_1, \ldots, x_n$. Por ejemplo, en vez de escribir $p(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ simplemente escribimos $p(X) \in R[X]$.

Propiedades básicas del grado de polinomios de varias variables

Proposición 4

Supongamos que R es un dominio.
Si $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$, entonces

$$\deg\big(p(X) + \deg q(X)\big) \leq \text{máx}\{\deg p(X), \deg q(X)\}$$
$$\deg\big(p(X) \cdot q(X)\big) = \deg p(X) + \deg q(X)$$

La demostración es análoga a la demostración de las respectivas igualdades de polinomios de una sola variable, pero es mas tediosa de escribir. Por eso, se la dejamos al lector.

Los anillos de polinomios de varias variables en un anillo conmutativo con 1 no son DIP's

Proposición 5

Supongamos que R es un dominio entero con 1. Entonces para toda $n \in \mathbb{Z}_{\geq 2}$, $R[x_1, \ldots, x_n]$ no es un DIP.

Demostración. Dividimos la demostración en dos casos:

- *Caso 1.* R es un campo.
  En particular, R es un dominio entero y por lo tanto, la igualdad $\deg\big(p(X)q(X)\big) = \deg p(X) + \deg q(X)$ es cierta en $R[X]$. Para ver que R no es DIP, veamos que (x_1, x_2) no es principal. Procedamos por contradicción. Es decir, supongamos que existe $a(X) \in R[x_1, \ldots, x_n]$ tal que $(x_1, x_2) = (a(X))$.

En particular, existen $k(X), l(X) \in R[x_1, \ldots, x_n]$ tales que

$$x_1 = k(X)a(X) \quad \text{y} \quad x_2 = l(X)a(X).$$

Por lo tanto,

$$\begin{aligned} 1 = \deg(x_1) &= \deg\big(k(X)a(X)\big) \\ &= \deg k(X) + \deg a(X) \end{aligned}$$

Pero entonces, tenemos dos subcasos:

Caso 1.1. $\deg k(X) = 1$ y $\deg a(X) = 0$.
La segunda ecuación implica que $a(X) = r$ para alguna $r \in R$, sin embargo esto es imposible porque entonces

$$(x_1, x_2) = (a(X)) = (r) = (1) = R$$

donde la tercera igualdad se cumple porque R es campo. Esta igualdad contradice el hecho de que $(x_1, x_2) \subsetneq R[x_1, \ldots, x_n]$.

Caso 1.2. $\deg k(X) = 0$ y $\deg a(X) = 1$.
La primera ecuación implica que

$$k(X) = r \text{ para alguna } r \in R.$$

Sustituyendo esto en $x_1 = k(X)a(X)$ obtenemos

$$x_1 = ra(X)$$

y por lo tanto, como R es un campo,

$$a(X) = r^{-1}x_1.$$

En particular, $\deg a(X) = 1$.

Usando esto, la ecuación $l(X)a(X) = x_2$ implicaría que $\deg l(X) = 0$.
Pero entonces existiría $r' \in R$ tal que

$$r'r^{-1}x_1 = l(X)a(X) = x_2$$

Lo cual obviamente es imposible.

- *Caso 2.* R no es un campo.
  Como en este caso queremos demostrar que

$$R \text{ no es un campo } \implies R[x_1, \ldots, x_n] \text{ no es un DIP}$$

  podemos demostrar que

$$R[x_1, \ldots, x_n] \text{ es un DIP } \implies R \text{ es un campo.} \tag{2}$$

  Recuerda que en la proposición 1.19.9 demostramos que

$$R[x] \text{ es un DIP } \implies R \text{ es un campo.} \tag{3}$$

  En lo que sigue, veremos que la demostración de (2) es esencialmente igual a la demostración de (3).

$$
\begin{aligned}
R[x_1,\ldots,x_n] \text{ es un DIP} &\implies R[x_1,\ldots,x_n] \text{ es un dominio entero} \\
&\iff R \text{ es un dominio entero} \\
&\iff R[x_1,\ldots,x_n]/(x_1,\ldots,x_n) \text{ es un dominio entero} \\
&\qquad\qquad (\text{pues } R[x_1,\ldots,x_n]/(x_1,\ldots,x_n) \cong R) \\
&\iff (x_1,\ldots,x_n) \text{ es un ideal primo en } R[x_1,\ldots,x_n] \\
&\qquad\qquad (\text{por la caracterización de ideales primos}) \\
&\iff (x_1,\ldots,x_n) \text{ es un ideal maximal en } R[x_1,\ldots,x_n] \\
&\qquad\qquad (\text{pues en un DIP, primo} \iff \text{maximal}) \\
&\iff R[x_1,\ldots,x_n]/(x_1,\ldots,x_n) \text{ es un campo} \\
&\qquad\qquad (\text{por la caracterización de ideales maximales}) \\
&\iff R \text{ es un campo} \quad (\text{pues } R[x_1,\ldots,x_n]/(x_1,\ldots,x_n) \cong R)
\end{aligned}
$$

Por lo tanto, (2) es cierto.

En resumen, vimos que si R es un anillo conmutativo con 1, entonces

1. R campo $\implies$ $R[x_1,\ldots,x_n]$ no es un DIP.
2. R no campo $\implies$ $R[x_1,\ldots,x_n]$ no es un DIP.

$\therefore$ R anillo conmutativo con 1 $\implies$ $R[x_1,\ldots,x_n]$ no es un DIP. $\square$