Propiedades básicas de anillos de polinomios

Facultad de Ciencias UNAM

Introducción

En el resto del capitulo 1 estudiaremos a los anillos de polinomios. Por eso, en esta sección recordamos lo que ya sabemos de ellos y también los empezamos a estudiar mas a fondo.

Un recordatorio amistoso

Supongamos que R es un anillo y que x es una variable indeterminada. Una suma formal

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \tag{1}$$

con $n \in \mathbb{Z}_{\geq 0}$ y $a_i \in R$ es un **polinomio en x con coeficientes en R**. A el conjunto de todos los polinomios en x con coeficientes en R lo denotamos por $R[x]$ y lo llamamos **el anillo de polinomios en x sobre R**. Específicamente,

$$R[x] := \left\{ a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid n \in \mathbb{Z}_{\geq 0} \text{ y } a_i \in R \right\}$$

Por brevedad, normalmente denotamos a los elementos de $R[x]$ por símbolos como "$p(x)$" o "$a(x)$". Hay que tener cuidado de no confundir esta notación con la notación usual de evaluar una función en un valor. De hecho, pronto veremos que si R no es conmutativo, no es formalmente correcto pensar en los polinomios sobre R como funciones de R en R.

Supongamos que $p(x) := a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$.

- Si $a_i = 0$ para toda $i > 0$, decimos que $p(x)$ es un **polinomio constante**. En este caso tendremos $p(x) = a_0$ con $a_0 \in R$. Por eso hay una inclusión natural $R \hookrightarrow R[x]$ y de hecho identificamos a R con el conjunto de polinomios constantes. De esta manera, hacemos la natural convención de que $R \subset R[x]$.
- Si $a_n \neq 0$, decimos que $p(x)$ tiene **grado** n y escribimos $\deg p(x) = n$. Mas aun, decimos que $a_n x^n$ es su **termino delantero** y que a_n es su **coeficiente delantero**. Si $a_n = 1$, decimos que $p(x)$ es **mónico**.
- Si $a_i = 0$ para toda i, decimos que $p(x)$ es el **polinomio cero**, y escribimos $p(x) = 0$. También, definimos $\deg 0 = -1$.

Cabe recalcar que el grado de todo polinomio constante no cero es 1, pero el grado del polinomio cero es -1.

Las operaciones que hacen que $R[x]$ sea un anillo son las siguientes

La suma se hace componente a componente:

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i := \sum_{i=0}^{n} (a_i + b_i) x^i$$

Cabe recalcar que aquí, a_n o b_n puede ser cero y por lo tanto, la igualdad anterior define la suma entre polinomios de cualesquiera grados.

La multiplicación se define por pasos: Primero, definimos la multiplicación para polinomios con exactamente un solo coeficiente distinto de 0 de la siguiente manera: $(ax^i)(bx^j) := (ab)x^{i+j}$. Luego, extendemos esta definición a todos los polinomios usando las leyes distributivas. De esta manera obtenemos:

$$\sum_{i=0}^{n} a_i x^i \times \sum_{i=0}^{n} b_i x^i := \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k$$

Un detalle con los polinomios sobre anillos no conmutativos

Una consecuencia importante de la definición

$$(ax^i)(bx^j) := (ab)x^{i+j} \tag{2}$$

es el siguiente: si R no es conmutativo, entonces no es formalmente correcto pensar en los polinomios sobre R como funciones de R en R.

El (sutil) detalle es que si R no es conmutativo, $a, b \in R$, y definimos

$$f(y) := ay^i \quad \text{y} \quad g(y) := by^j,$$

entonces la no conmutatividad de R implica que *podemos*[1] tener

$$f(y)g(y) = (ay^i)(by^j) \neq (ab)y^{i+j},$$

en contraste con (2).

[1] Si $a, b \in R$ son tales que conmutan con cualquier otro elemento de R, entonces la siguiente igualdad no es cierta.

Veamos un ejemplo especifico de este detalle: Sea $\mathbb{H}$ el anillo de cuaterniones y considera los siguientes elementos de $\mathbb{H}[x]$

$$p(x) = (x+i)(x-i) \quad \text{y} \quad q(x) = x^2 + 1$$

Por la forma en la que definimos la multiplicación en $\mathbb{H}[x]$,

$$\begin{aligned} p(x) = (x+i)(x-i) &= (x)(x) + (x)(-i) + (i)(x) + (i)(-i) \\ &= x^2 - ix + ix - i^2 \\ &= x^2 + 1 = q(x) \end{aligned}$$

Sin embargo, si definimos a las funciones $f, g \in \mathbb{H}^{\mathbb{H}}$ por

$$f(y) = (y+i)(y-i) \quad \text{y} \quad g(y) = y^2 + 1$$

entonces

$$f(y) = (y+i)(y-i) = y^2 - yi + iy + 1 \neq y^2 + 1 = g(y)$$

pues en general, $-xi + ix \neq 0$ (recuerda que $\mathbb{H}$ no es conmutativo).

En palabras, acabamos de ver que hay expresiones que son iguales como polinomios pero no son iguales como funciones. El problema obviamente nace de que por la definición de multiplicación en polinomios, $(x)(a) = ax$, pero como funciones esto solo es cierto cuando el anillo es conmutativo (o a esta en el centro de R). Esta discusión nos lleva a hacer la siguiente observacion:

Si R no es conmutativo y definimos el subanillo de R^R por

$$\text{Poli}(R) := \left\{ f \in R^R \mid f(y) = \sum_{i=0}^{n} a_i y^i \text{ para algunas } a_i \in R \text{ y } n \in \mathbb{Z}_{\geq 0} \right\}$$

entonces, la función $\mathfrak{F} : \text{Poli}(R) \to R[x]$ dada por $\mathfrak{F}(f) := \sum_{i=0}^{n} a_i x^i$ si $f(y) = \sum_{i=0}^{n} a_i y^i$, entonces $\mathfrak{F}$ no es necesariamente un isomorfismo.

En nuestro caso particular, $\mathfrak{F}$ no es inyectiva: si $f, g \in \mathbb{H}^{\mathbb{H}}$ y $p(x), q(x) \in \mathbb{H}[x]$ significan lo mismo que en las diapositivas anteriores, entonces $f \neq g$ pero $\mathfrak{F}(f) = p \neq q = \mathfrak{F}(g)$.

Claramente, en anillos conmutativos no tenemos este detalle y por lo tanto, en anillos conmutativos, si podemos pensar en los polinomios como funciones.

Una ventaja de esta perspectiva es que ya sabemos un montón de cosas acerca de funciones. Por ejemplo, sabemos como *componer* funciones y por lo tanto, también sabemos como componer polinomios sobre anillos conmutativos:

Supongamos que R es un anillo conmutativo y que $p(x), q(x) \in R[x]$ son tales que

$$p(x) = \sum_{i=0}^{n} a_i x^i \quad \text{y} \quad q(x) = \sum_{j=0}^{m} b_j x^j$$

con $a_n \neq 0$ y $b_m \neq 0$.

Entonces

$$p \circ q(x) = p(q(x)) = \sum_{i=0}^{n} a_i (q(x))^i = \sum_{i=0}^{n} \left\{ a_i \left(\sum_{j=0}^{m} b_j x^j \right)^i \right\}$$

$$= \sum_{i=0}^{n} \left\{ a_i \underbrace{\left(\sum_{j=0}^{m} b_j x^j \right) \cdots \left(\sum_{j=0}^{m} b_j x^j \right)}_{i-\text{veces}} \right\}.$$

Notemos que los últimos dos términos de estas igualdades esta bien definido en cualquier anillo de polinomios (solo es una suma de productos de polinomios). Por lo tanto, hacemos la siguiente definición.

Composición de polinomios

Supongamos que R es un anillo y que $p(x), q(x) \in R[x]$ son tales que

$$p(x) = \sum_{i=0}^{n} a_i x^i \quad \text{y} \quad q(x) = \sum_{j=0}^{m} b_j x^j$$

con $a_n \neq 0$ y $b_m \neq 0$. Definimos la **composición de** $p(x)$ **con** $q(x)$ por

$$p(q(x)) := \sum_{i=0}^{n} \left\{ a_i \left(\sum_{j=0}^{m} b_j x^j \right)^i \right\} = \sum_{i=0}^{n} \left\{ a_i \underbrace{\left(\sum_{j=0}^{m} b_j x^j \right) \cdots \left(\sum_{j=0}^{m} b_j x^j \right)}_{i-\text{veces}} \right\}.$$

El homomorfismo inducido en anillos de polinomios

Supongamos que $\phi : R \to R'$ es un homomorfismo de anillos. El **homomorfismo inducido por ϕ en los anillos de polinomios** es

$$\Phi : R[x] \to R'[x]$$
$$a_n x^n + \cdots + a_1 x + a_0 \mapsto \phi(a_n)x^n + \cdots + \phi(a_1)x + \phi(a_0).$$

En palabras, Φ le aplica ϕ a los coeficientes de un polinomio sobre R para obtener un polinomio sobre R'.

Es fácil verificar que Φ de verdad es un homomorfismo y que cuando ϕ es inyectivo (suprayectivo) entonces Φ también es inyectivo (suprayectivo).

Propiedades básicas (y ya conocidas) de polinomios

Proposición 1

Supongamos que R es un anillo.

1. $R[x]$ es conmutativo si y solo si R es conmutativo.
2. $R[x]$ tiene unidad si y solo si R tiene unidad.
3. Si R es un dominio, entonces
   1) Para toda $p(x), q(x) \in R[x]$

$$\deg\big(p(x)+q(x)\big) \leq \text{máx}\big\{\deg p(x), \deg q(x)\big\} \tag{3}$$

$$\deg\big(p(x)\cdot q(x)\big) = \deg p(x) + \deg q(x) \tag{4}$$

$$\deg\big(p(q(x))\big) = \deg p(x)\cdot \deg q(x) \tag{5}$$

   2) $p(x) \in R[x]$ es invertible en $R[x]$ si y solo si $p(x) = u$ para alguna $u \in R$ invertible.
4. $R[x]$ es un dominio si y solo si R es un dominio.
5. $R[x]$ es un dominio entero si y solo si R es un dominio entero.

Comentario

La demostración de los primeros dos incisos es trivial y para ver una demostración de los últimos dos incisos, checa la proposición 1.5.9.

Ahora, procedemos a estudiar $R[x]$ a través de sus ideales.

El anillo de polinomios de un cociente

Proposición 2

Supongamos que R es un anillo conmutativo y que I es un ideal de R. Entonces el ideal generado por I en $R[x]$ es el conjunto de polinomios en x con coeficientes en I, es decir, $(I) = I[x]$ y

$$R[x]/I[x] \cong (R/I)[x].$$

En particular, si I es un ideal primo en R, entonces $(I) = I[x]$ es un ideal primo en $R[x]$.

Demostración. Primero veamos que $(I) = I[x]$. La inclusión $(I) \subset I[x]$ es consecuencia inmediata de que $I[x]$ es ideal de $R[x]$ y de que $I \subset I[x]$. Para ver que $(I) \supset I[x]$, primero notemos que todo elemento de $I[x]$ es una suma de polinomios de la forma ax^n con $a \in I$ y $n \in \mathbb{Z}_{\geq 0}$. Pero como I es ideal, entonces para toda $a \in I$ y toda $n \in \mathbb{Z}_{\geq 0}$, $x^n \cdot a = ax^n \in I$. Para concluir, basta recordar que (I) es cerrado bajo suma.

Ahora bien, sea $\varphi : R[x] \to (R/I)[x]$ tal que

$$\sum_{i=0}^{n} a_i x^i \overset{\varphi}{\mapsto} \sum_{i=0}^{n} \overline{a_i} x^i$$

donde $\overline{a} := a + I \in R/I$. Usando las definiciones de las operaciones en R/I y $R[x]$ es fácil verificar que φ es un homomorfismo suprayectivo y que $\ker \varphi = I[x]$. Por lo tanto, por el primer teorema de isomorfismos,

$$(R/I)[x] \cong R[x]/\ker \varphi = R[x]/I[x].$$

Finamente, supongamos que I es un ideal primo de R y veamos que $I[x]$ es un ideal primo de $R[x]$. Para esto, recordemos la caracterización de ideales primos en términos del cociente (c.f. proposición 1.12.1):

Si S es un anillo conmutativo y J es un ideal en S, entonces S es un ideal primo en S si y solo si S/J es un dominio entero.

Usando esto y el isomorfismo anterior, tenemos que

$$\begin{aligned} I \text{ es un ideal primo en } R &\iff R/I \text{ es un dominio entero} \\ &\implies (R/I)[x] \text{ es un dominio entero} \\ &\iff R[x]/I[x] \text{ es un dominio entero} \\ &\iff I[x] \text{ es un ideal primo de } R[x] \end{aligned}$$

□

Una aplicación de la proposición anterior

Supongamos que $n \in \mathbb{Z}_{\geq 1}$. Por la proposición anterior,

$$\mathbb{Z}[x]/n\mathbb{Z}[x] \cong (\mathbb{Z}/n\mathbb{Z})[x] = \mathbb{Z}_n[x]$$

En particular, si $p \in \mathbb{Z}_{\geq 1}$ es primo, entonces $p\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$ y por lo tanto, la proposición anterior implica que $p\mathbb{Z}[x]$ (el subanillo de $\mathbb{Z}[x]$ con coeficientes divisibles por p), es un ideal primo de $\mathbb{Z}[x]$.

Observación

A pesar de la fortaleza de el resultado anterior, esto no representa toda la historia de los ideales de anillos de polinomios. Esto es porque no todo ideal de $R[x]$ es de la forma $I[x]$.

En efecto, no existe ningún ideal propio I de R tal que $(x) = I[x]$. De lo contrario, como

$$I[x] = \{\text{polinomios en } x \text{ con coeficientes en } I\}$$

la pertenencia $1x = x \in (x) = I[x]$ implicaría que $1 \in I$, contradiciendo que I es propio.

Otra observación

En la ultima oración de la proposición anterior no podemos cambiar "primo" por "maximal". Específicamente, tenemos que

$$I \text{ es un ideal maximal en } R \not\Longrightarrow I[x] \text{ es un ideal maximal en } R[x].$$

- *Intuitivamente*, esta diferencia sucede porque en la demostración de "I primo $\Longrightarrow$ $I[x]$ primo" usamos la caracterización de ideales primos en términos de cocientes y la siguiente implicación (cierta para cualquier anillo conmutativo S)

  $$S \text{ es un dominio entero} \Longrightarrow S[x] \text{ es un dominio entero.}$$

  A pesar de que también tenemos una caracterización de ideales maximales en términos de cocientes[2], también tenemos que

  $$S \text{ es un campo} \not\Longrightarrow S[x] \text{ es un campo.}$$

[2] Si S es un anillo conmutativo con 1 y J es un ideal en S, entonces J es maximal en S si y solo si S/J es un campo.

- *Formalmente*, considera el siguiente contraejemplo: Sea $R = \mathbb{Z}$ e $I = 2\mathbb{Z}$. Ya sabemos que $2\mathbb{Z}$ es maximal en $\mathbb{Z}$, pero $2\mathbb{Z}[x]$ *no* es maximal en $\mathbb{Z}[x]$ pues $2\mathbb{Z}[x] \subsetneq^{3} (2, x) \subsetneq^{4} \mathbb{Z}[x]$.

A pesar de todo esto, de hecho *si* podemos decir algo afirmativo de los ideales maximales y los anillos de polinomios, pero antes necesitaremos los siguientes lemas (cabe recalcar que el primero ya los habíamos visto (en la sección 1.9) pero de cualquier manera, volvemos a presentar la demostración).

[3] Claramente todo polinomio con coeficientes pares pertenece a $(2, x)$ pero $x \notin 2\mathbb{Z}[x]$.
[4] En la sección 1.9 demostramos que $(2, x)$ es un ideal propio de $\mathbb{Z}[x]$.

El ideal (x) de $R[x]$

Lema 3

Supongamos que R es un anillo conmutativo. Entonces

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

Demostración.

1. $\subset$) Es fácil verificar que $\{\text{los polinomios con constante} = 0\}$ es un ideal de $R[x]$ y como $x \in \{\text{los polinomios con constante} = 0\}$, entonces $(x) \subset \{\text{los polinomios con constante} = 0\}$.

   $\supset$) Supongamos que $p(x)$ tiene constante $= 0$. Es decir, $p(x) =^5 \sum_{i=1}^{n} a_i x^i$ para algunas $a_i \in R$ y $n \in \mathbb{Z}_{\geq 1}$. Entonces

$$p(x) = \sum_{i=1}^{n} a_i x^i = \left(\sum_{i=1} a_i x^{i-1} \right) x \in (x).$$

[5] Este polinomio tiene termino constante $= 0$ porque estamos empezando la suma en $i = 1$.

2. Supongamos que $\varphi : R[x] \to R$ es tal que

$$p(x) \mapsto p(0) = \text{el termino constante de } p(x)$$

Entonces φ es un homomorfismo suprayectivo y

$$\ker \varphi = \{\text{los polinomios con constante} = 0\} = (x)$$

donde la ultima igualdad se cumple por el inciso anterior. Finalmente, por el primer teorema de isomorfismos

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

□

Ideales de la forma $(A \cup \{x\})$

Lema 4

Supongamos que R es un anillo conmutativo. Entonces

1. $(R \cup \{x\}) = R[x]$.
2. Si J es un ideal en $R[x]$, entonces

$$J_{\text{cte}} := \{\text{los polinomios constantes en } J\}.$$

es un ideal de R y $J \subset (J_{\text{cte}} \cup \{x\})$.

Demostración.

1. Supongamos que $\sum_{i=0}^{n} a_i x^i \in R[x]$. Por el inciso anterior tenemos

$$\sum_{i=0}^{n} a_i x^i = \underbrace{\sum_{i=1}^{n} a_i x^i}_{\in (x)} + \underbrace{a_0}_{\in R} \in (x) + (R) = (R \cup \{x\}).$$

2. La verificación de que J_{cte} es un ideal de R es muy sencilla y por eso se la dejamos al lector. Para ver la inclusión, supongamos que $\sum_{i=0}^{n} a_i x^i \in J$. Por el inciso anterior tenemos

$$\sum_{i=0}^{n} a_i x^i = \underbrace{\sum_{i=1}^{n} a_i x^i}_{\in (x)} + \underbrace{a_0}_{\in J_{\text{cte}}} \in (x) + (J_{\text{cte}}) = (J_{\text{cte}} \cup \{x\}).$$

□

I maximal $\Longrightarrow$ $(I \cup \{x\})$ maximal

Proposición 5

Supongamos que R es un anillo conmutativo y que I es un ideal de R. Si I es maximal en R, entonces $(I \cup \{x\})$ es maximal en $R[x]$.

Demostración. Supongamos que $(I \cup \{x\})$ no es maximal. Es decir, existe J ideal en $R[x]$ tal que $(I \cup \{x\}) \subsetneqq J \subsetneqq R[x]$. Notemos que la primera inclusión implica que

$$J = J_{\text{cte}}. \tag{6}$$

En efecto, la inclusión "$\subset$" es consecuencia del lema y la inclusión "$\supset$" es consecuencia de que $x \in (I \cup \{x\}) \subset J$.

Ahora, veamos que I no es maximal demostrando que $I \subsetneqq J_{\text{cte}} \subsetneqq R$.

$J_{\text{cte}} \subsetneqq R$: De lo contrario, $J_{\text{cte}} = R$. Usando esto, la ecuación (6), y el lema, obtenemos que

$$J = (J_{\text{cte}} \cup \{x\}) = (R \cup \{x\}) = R[x],$$

contradiciendo $J \subsetneqq R$.

$I \subsetneqq J_{\text{cte}}$: De lo contrario, $I = J_{\text{cte}}$. Usando esto y la ecuación (6) obtenemos que

$$(I \cup \{x\}) = (J_{\text{cte}} \cup \{x\}) = J,$$

contradiciendo $(I \cup \{x\}) \subsetneqq J$.