UNA CONSTRUCCION DEL ANILLO DE POLINOMIOS R$[X]$

Francisco González Maján
Catedrático de Matemáticas del
I.B."José Mª Parra",de Alcira(Valencia)

INTRODUCCION

De todos es conocido que el concepto de polinomio no es nuevo para los alumnos de Bachillerato. Sin embargo,es notoria en ellos una cierta tendencia a identificar la indeterminada con un número-menos veces con una letra-al que llaman "desconocido","incógnita","letra X",etc.

Estos hechos,y el deseo de acostumbrar al alumnado a la abstracción, aprovechando temas que,bien o no,ha estudiado ya,han sido los motivos fundamentales que nos han llevado a elaborar el trabajo que aquí exponemos.

A lo largo de todo este estudio,la letra X representará únicamente un símbolo,sin ningún significado especial,ni matemático ni alfabético.

MONOMIOS PRIMITIVOS

Llamaremos *monomio primitivo* a cualquier aplicación

$$f : \{X\} \longrightarrow \mathrm{N}$$

Si la aplicación es

$$\begin{aligned} f : \{X\} &\longrightarrow \mathrm{N} \\ X &\longrightarrow n \end{aligned}$$

,la designaremos por X^n y la llamaremos *monomio primitivo de grado n*. Los monomios primitivos de grados 0 y 1 son las aplicaciones

$$X^0 : \{X\} \longrightarrow N \qquad\qquad X^1 : \{X\} \longrightarrow N$$
$$X \longrightarrow 0 \qquad y \qquad X \longrightarrow 1$$

Designaremos por M_p al conjunto de monomios primitivos, es decir,

$$M_p = \{ X^0 , X^1 , X^2 , \ldots , X^n \}$$

Por medio de la suma en N se puede definir en M_p una operación, a la que llamaremos *producto de monomios primitivos*, así :

Dados dos monomios primitivos X^n y X^m, su produco $X^n . X^m$, es la aplición

$$X^n . X^m : \{X\} \longrightarrow N$$
$$X \longrightarrow n+m$$

, es decir, por definición es

$$X^n . X^m = X^{n+m}$$

Son de demostración inmediata las propiedades de asociatividad, existencia de elemento neutro (el monomio primitivo X^0) y conmutatividad. En consecuencia, (M_p , .) es un *semigrupo unitario y conmutativo.*

MONOMIOS

Consideremos el producto cartesiano R x M_p, y definamos en él la siguiente relación

$$(r , X^n) \equiv (s , X^m) \Longleftrightarrow \begin{cases} r = s \text{ y } n = m \\ \text{ó} \\ r = s = 0 \end{cases}$$

Es inmediato comprobar que se trata de una relación de equivalencia y que, para $r \neq 0$, el único par equivalente a (r, X^n) es él mismo; mientras que todos los pares de la forma $(0, X^n)$ son equivalentes, o sea,

$$(0, X^0) \equiv (0, X^1) \equiv (0, X^2) \equiv \ldots \qquad (1)$$

A toda clase de equivalencia la llamaremos *monomio*. Si es $r \neq 0$, el monomio (r, X^n) se llama *monomio de grado n y coeficiente* r. El monomio constituido por los elementos (1) es el *monomio cero* y de él diremos que no tiene grado. Finalmente, designaremos por M(R) al conjunto de monomios.

Producto de monomios

El producto de números reales y el producto de monomios primitivos permiten definir en M(R) la siguiente operación,que llamaremos *producto de monomios* :

$$(r , X^n) . (s , X^m) = (r.s , X^{n+m})$$

Es claro que el producto de monomios es otro monomio,y que éste es el monomio cero,si y sólo si alguno de los monomios factores lo es.

Asimismo,es evidente que el producto de dos monomios no nulos tiene por grado la suma de los grados de los factores.

El producto de monomios cumple las siguientes propiedades :

.. Asociativa.-Es consecuencia de la asociatividad del producto en R y del producto de monomios primitivos.

.. Conmutativa.-Porque,tanto el producto de números reales como el de monomios primiticos son conmutativos.

.. Existe un elemento neutro,el monomio $(1,X^0)$.

.. Los únicos monomios que admiten inversos son los de grado cero. El inverso de (r,X^0) es $(1/r,X^0)$.

Según esto,(M(R) , .) es un *semigrupo abeliano y unitario.*

INMERSION DE R EN M(R)

Cada número real se puede identificar con un monomio. Concretamente, "el número real r lo consideraremos idéntico al monomio (r,X^0)". Esta identificación la hacemos porque respeta el producto;de un modo más preciso,porque la aplicación

$$\begin{aligned} i : R &\longrightarrow M(R) \\ r &\longrightarrow (r,X^0) \end{aligned}$$

es inyectiva y cumple la igualdad

$$i(r.s) = i(r).i(s)$$

Veamos la demostración:

De la condición $r \neq s$,resulta $(r,X^0) \neq (s,X^0)$, luego la aplicación es inyectiva.

Además,se tiene $i(r.s) = (r.s , X^0) = (r,X^0) . (s,X^0) = i(r).i(s)$, y, por tanto, se trata de un morfismo.

Debido a esta identificación, indicaremos los monomios de grado cero escribiendo sólo sus coeficientes, es decir, notaremos r en vez de (r, X^0). En particular, el elemento neutro del producto de monomios es 1.

INMERSION DE M_p EN M(R)

Cada monomio primitivo se puede identificar con un monomio. Concretamente, "identicaremos el monomio primitivo X^n con el monomio $(1, X^n)$". Como antes, hacemos esta identificación porque respeta las operaciones, esto es, porque la aplicación

$$i' : M_p \longrightarrow M(R)$$
$$X^n \longrightarrow (1, X^n)$$ es inyectiva y verifica que

$$i'(X^n . X^m) = i'(X^n) . i'(X^m)$$

En virtud de esta identificación, designaremos a los monomios de la forma $(1, X^n)$, a excepción de $(1, X^0)$, escribiendo simplemente X^n. En el caso de $(1, X^0)$, como ya dijimos, notaremos 1. Escribiremos también X, en lugar de X^1.

RESUMEN RELATIVO A NOTACIONES

Aparte de las notaciones anteriores, cualquier monomio de la forma (r, X^n), se indicará suprimiendo el paréntesis y la coma; así : rX^n. (Ver NOTA, al final de este trabajo). En resumen, con estas notaciones resulta:

.. Los monomios de grado cero son los números reales.

.. Los de grado $n \neq 0$ son las expresiones de la forma rX^n, con $r \neq 0$.

.. El monomio cero, que designaremos por 0, puede ser representado por cualquier expresión de la forma $0X^n$.

.. La regla de multiplicación es $rX^n . sX^m = (rs) X^{n+m}$

POLINOMIOS

Llamaremos *polinomio* a una colección finita de monomios de distinto grado definida con la siguiente condición : *Dos de dichas colecciones* *son iguales si tienen los mismos monomios ,o si el único monomio que está en una de ellas y no en la otra es el monomio cero.*

Al monomio cero lo llamaremos también *polinomio nulo.*

Por definición,el grado de un polinomio no nulo es el mayor de los grados de los monomios que contiene.

Continuaremos llamando monomios a los polinomios que contengan un solo monomio.Suele llamarse "binomio" al polinomio formado por sólo dos monomios no nulos;"trinomio",al que sólo contiene tres y,"cuatrinomio", al de cuatro términos no nulos solamente.

Ejemplos :

. Son polinomios los conjuntos $p(X) = \{ 3X^4 , 6X^7 , -2 \}$ y $q(X) = \{ 7\sqrt{2}\ X^9 \}$. El primero de ellos es un trinomio y el segundo un monomio

. Consideramos que no es un polinomio la colección $\{ 3X^2 , 5X^2 , X \}$, porque contiene monomios de igual grado.

. Se consideran iguales los polinomios siguientes :

$$p(X) = \{ X^3 , 0X^2 , 0X , 1 \} \quad \text{y}$$
$$q(X) = \{ X^3 , 1 \}$$

Sea ahora $p(X)$ un polinomio de grado n. Diremos que $p(X)$ está expresado en forma *canónica* si sus monomios aparecen ordenados en orden decreciente de grados. Por ejemplo,$\{ 3X^3 , X^2 , 0X , -7 \}$ está expresado en forma canónica,y no lo está el $\{ 3X^2 , X^3 , -2 \}$.

Es obvio que todo polinomio puede ser expresado en forma canónica, por lo que,en definitiva,podemos considerar que un polinomio de grado n no es otra cosa que una colección de monomios de la forma

$$p(X) = \{ a_n X^n , a_{n-1} X^{n-1} , \ldots.., a_1 X , a_0 \} ,$$

en donde se supone que $a_n \neq 0$, pero puede que algún otro nº a_i sea nulo.

Los números a_n , a_{n-1} , ...,a_1 , a_0 que aparecen en la forma antedicha,se llaman *coeficientes* del polinomio $p(X)$;concretamente,de a_i se dice que es el coeficiente del monomio de grado i.

SUMA DE POLINOMIOS

Dados dos polinomios

$$p(X) = \{ a_n X^n , \ldots , a_1 X , a_0 \} \quad y$$

$$q(X) = \{ b_{n+h} X^{n+h} , \ldots , b_1 X , b_0 \} ,$$

se llama *suma* de $p(X)$ y $q(X)$ al polinomio definido por

$$p(X) + q(X) = \{ b_{n+h} X^{n+h} , \ldots , (a_n+b_n) X^n , \ldots , (a_1+b_1) X , a_0+b_0 \}$$

Las propiedades de la suma en R permiten demostrar, de manera obvia, que la suma así definida es asociativa, conmutativa, que el polinomio nulo es elemento neutro y cada polinomio tiene un opuesto. Así pues, el conjunto de los polinomios es un *grupo aditivo abeliano.*

Obsérvese que, dado el polinomio

$$p(X) = \{a_n X^n , \ldots , a_1 X , a_0\} \text{ , se cumple que}$$

$$p(X) = \{a_n X^n\} + \ldots + \{a_1 X\} + \{a_0\}$$,es decir, que *todo polinomio coincide con la suma de los monomios que contiene.* Debido a este hecho, en lo sucesivo expresaremos los polinomios como sumas de monomios.

PRODUCTO DE POLINOMIOS

Producto de un monomio por un polinomio

Dado un monomio, $p(X) = aX^n$, y un polinomio, $q(X) = b_h X^h + \ldots + b_1 X + b_0$, llamaremos *producto* de $p(X)$ por $q(X)$ al polinomio siguiente :

$$p(X) \cdot q(X) = (ab_h) X^{h+n} + \ldots + (ab_1) X^{n+1} + (ab_0) X^n$$

Proposición.— Dados el monomio aX^n y los polinomios $q(X)$ y $r(X)$, se verifica que

$$aX^n \cdot \left[q(X) + r(X)\right] = aX^n \cdot q(X) + aX^n \cdot r(X).$$

Demostración.-Si b_i y c_i son, respectivamente, los coeficientes de los términos de grado i en $q(X)$ y $r(X)$, entonces, el coeficiente de grado $n+i$ en el primer miembro de la igualdad anterior es $a(b_i+c_i)$ y en el segundo es ab_i+ac_i. Por consiguiente, la distributividad de . respecto a + en R asegura la validez de dicha igualdad.

Producto de dos polinomios arbitrarios

Dados dos polinomios

$$p(X) = a_n X^n + \dots + a_1 X + a_0 \quad \text{y}$$
$$q(X) = b_h X^h + \dots + b_1 X + b_0$$

definimos su *producto* mediante la siguiente fórmula

$$p(X) \,.\, q(X) = a_n X^n . q(X) + \dots + a_1 X . q(X) + a_0 . q(X)$$

Obsérvese que es inmediato que $p(X) \,.\, q(X)$ es la suma de todos los monomios que se pueden formar multiplicando un monomio de $p(X)$ por otro de $q(X)$, es decir, el polinomio $p(X).q(X)$ es la suma de todos los monomios de la forma $a_i X^i \,.\, b_j X^j$, siendo $0 \leqslant i \leqslant n$ y $0 \leqslant j \leqslant h$. Ejemplo:

$$(5X^2 + 2X) \,.\, (3X^3 + X^2 + 2) =$$
$$= 5X^2 \,.\, (3X^3 + X^2 + 2) + 2X \,.\, (3X^3 + X^2 + 2) =$$
$$= (15X^5 + 5X^4 + 10X^2) + (6X^4 + 2X^3 + 4X) =$$
$$= 15X^5 + 11X^4 + 2X^3 + 10X^2 + 4X$$

El producto de polinomios verifica las siguientes propiedades:

..Conmutativa.-Su demostración es trivial a partir de la observación hecha anteriormente(el producto es la suma de todos .....),puesto que el producto de monomios es conmutativo y la suma de polinomios también.

..Distributiva.-Vamos a demostrar que

$$p(X).\left[q(X) + r(X)\right] = p(X).q(X) + p(X).r(X)$$

Supongamos que $p(X) = a_n X^n + \dots + a_1 X + a_0$. Entonces,por definición de producto de polinomios,y teniendo en cuenta la proposición vista y la conmutatividad de la suma,podemos escribir :

$$\begin{aligned} p(X).\left[q(X) + r(X)\right] &= a_n X^n.\left[q(X) + r(X)\right] + \dots + a_1 X.\left[q(X) + r(X)\right] + \\ &\quad + a_0.\left[q(X) + r(X)\right] = a_n X^n.q(X) + a_n X^n.r(X) + \\ &\quad + \dots + a_1 X.q(X) + a_1 X.r(X) + a_0.q(X) + a_0.r(X) = \\ &= \Big(a_n X^n.q(X) + \dots + a_1 X.q(X) + a_0.q(X)\Big) + \\ &\quad + \Big(a_n X^n.r(X) + \dots + a_1 X.r(X) + a_0.r(X)\Big) = \end{aligned}$$

$$= p(X) \,.\, q(X) + p(X) \,.\, r(X).$$

..Asociativa: $p.(q.r) = (p.q).r$,siendo p,q,r polinomios arbitrarios.

En efecto,aplicando la propiedad distributiva resulta que $p.(q.r)$ es la suma de todos los monomios de la forma $m.(m'.m'')$,siendo m un monomio de p; m',uno de q y m'',uno de r. Es,pues,evidente la propiedad asociativa,por ser asociativo el producto de monomios y conmutativa la suma.

..El monomio 1 es elemento neutro multiplicativo.

ESTRUCTURA DEL CONJUNTO DE LOS POLINOMIOS

De todo lo anterior se deduce que el conjunto de polinomios es, respecto a las operaciones suma y producto, un *ANILLO CONMUTATIVO*. Se trata del anillo $R[X]$ de los polinomios con coeficientes reales.

Nota

Una explicación de la notación rX^n puede darse a través del concepto de *aplicación monomia*. Una aplicación $f: R \longrightarrow R$, se llama monomia, si existe una constante r y un número natural n, tales que $f(\alpha) = r.\alpha^n$, para todo número real α. Es fácil probar que la aplicación que asigna al monomio (r, X^n) la aplicación monomia $r.\alpha^n$ es una biyección que conserva el producto; de ahí la notación rX^n para designar al monomio (r, X^n).