El anillo de polinomios

Definición 1. *Sea A un anillo conmutativo con 1. Un polinomio en x con coeficientes en A es una expresión del tipo*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 x^0$$

donde $n \in \mathbb{N}$ y $a_i \in A$ para todo $i = 0, ..., n$

Al conjunto de polinomios en x con coeficientes en A lo denotamos $A[x]$ y usaremos $f(x), g(x)$ para denotar a sus elementos.
Al polinomio

$$0x^n + 0x^{n-1} + \cdots + 0x + 0x^0$$

lo llamaremos el polinomio cero (sin importar el valor de n) y lo denotamos por 0.
A un polinomio de la forma

$$a_n x^n$$

se le llama monomio.
Con el fin de mostrar las operaciones y propiedades entre polinomios, introducimos las expresiones

$$p(x) = \sum_{i=0}^{\infty} a_i x^i$$

en donde casi todos los coeficientes son cero, lo que significa que para algún $n \in \mathbb{N}$, $a_j = 0$ para $j > n$, esto es, solamente para un número finito de valores de i se tiene $a_i \neq 0$.

Definición 2. *Dos polinomios $\sum_{i=0}^{\infty} a_i x^i$ y $\sum_{i=0}^{\infty} b_i x^i$ serán iguales si $a_i = b_i$ para toda $i = 1, 2, ...$*

Operaciones en $A[x]$

Definición 3. *Sean $f(x) = \sum_{i=0}^{\infty} a_i x^i$ y $g(x) = \sum_{i=0}^{\infty} b_i x^i$ polinomios en $A[x]$. La suma de $f(x)$ y $g(x)$ es el polinomio, denotado como $f(x) + g(x)$, dado por*

$$f(x) + g(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

Evidentemente $f(x) + g(x) \in A[x]$, ya que como para alguna $n \in \mathbb{N}$, $a_j = 0$ para $j > n$ y para alguna $m \in \mathbb{N}$, $b_k = 0$ para $k > m$, se tiene entonces que $a_j + b_j = 0$ para toda $j > \text{máx}\{n, m\}$. Además recurde que A es un anillo y por lo tanto $a_i + b_i \in A$ para toda $j = 1, 2, ...$

Teorema 1. *Sea A un anillo conmutativo y $f(x), g(x)$ y $h(x)$ polinomios en $A[x]$. Entonces*

1. $(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$
2. $f(x) + g(x) = g(x) + f(x)$

3. $f(x) + 0 = f(x)$
4. *Existe* $t(x) \in A[x]$ *tal que* $f(x) + t(x) = 0$

Demostración. Sean $f(x) = \sum_{i=0}^{\infty} a_i x^i$, $g(x) = \sum_{i=0}^{\infty} b_i x^i$ y $h(x) = \sum_{i=0}^{\infty} c_i x^i$ tenemos que

1. en este caso

$$\begin{aligned}(f(x) + g(x)) + h(x) &= \left(\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i\right) + \sum_{i=0}^{\infty} c_i x^i \\ &= \sum_{i=0}^{\infty} (a_i + b_i) x^i + \sum_{i=0}^{\infty} c_i x^i \\ &= \sum_{i=0}^{\infty} ((a_i + b_i) + c_i) x^i \\ &= \sum_{i=0}^{\infty} (a_i + (b_i + c_i)) x^i \\ &= \sum_{i=0}^{\infty} a_i x^i + \left(\sum_{i=0}^{\infty} b_i x^i + \sum_{i=0}^{\infty} c_i x^i\right) \\ &= f(x) + (g(x) + h(x))\end{aligned}$$

2. En este caso

$$\begin{aligned}f(x) + g(x) &= \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i \\ &= \sum_{i=0}^{\infty} (a_i + b_i) x^i \\ &= \sum_{i=0}^{\infty} (b_i + a_i) x^i \\ &= \sum_{i=0}^{\infty} b_i x^i + \sum_{i=0}^{\infty} a_i x^i \\ &= g(x) + f(x)\end{aligned}$$

3. En este caso

$$f(x) + 0 = \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} 0 x^i = \sum_{i=0}^{\infty} (a_i + 0) x^i = \sum_{i=0}^{\infty} a_i x^i = f(x)$$

4. En este caso sea $t(x) = \sum_{i=0}^{\infty} (-a_i) x^i$. Entonces

$$f(x) + t(x) = \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} (-a_i) x^i = \sum_{i=0}^{\infty} (a_i - a_i) x^i = \sum_{i=0}^{\infty} 0 x^i = 0$$

□

Definición 4. *Sean* $f(x)=\sum_{i=0}^{\infty}a_ix^i$ *y* $g(x)=\sum_{i=0}^{\infty}b_ix^i$ *polinomios en* $A[x]$*. el producto de* $f(x)$ *y* $g(x)$ *es el polinomio, denotado como* $f(x)g(x)$*, dado por*

$$f(x)g(x)=\sum_{i=0}^{\infty}c_ix^i,\quad \textit{donde } c_i=\sum_{j+k=i}a_jb_k$$

para toda $i=0,1,2,...$

Para mostrar que la definición del producto esta bien dada, basta observar que si n y m son tales que $a_j=0$ para $j>n$ y $b_k=0$ para $k>m$, entonces $c_i=\sum_{j+k=i}a_jb_k=0$ para toda $i>n+m$. debido a que $i=j+k>n+m$ implica $j>n$ o $k>m$ (si $j\leq n$ y $k\leq m$, entonces $j+k\leq n+m$ que no es el caso) y esto a su vez implica, en cualquiera de los casos, que $a_jb_k=0$. Por último es claro que $c_i=\sum_{j+k=i}a_jb_k\in A$.

Teorema 2. *Sea* A *un anillo conmutativo y* $f(x),g(x)$ *y* $h(x)$ *polinomios en* $A[x]$*. Entonces*

1. $(f(x)g(x))h(x)=f(x)(g(x)h(x))$
2. $f(x)g(x)=g(x)f(x)$
3. $f(x)1=f(x)$
4. $f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x)$

Demostración. Sean $f(x)=\sum_{i=0}^{\infty}a_ix^i$, $g(x)=\sum_{i=0}^{\infty}b_ix^i$ y $h(x)=\sum_{i=0}^{\infty}d_ix^i$ tenemos que

1. En este caso

$$\begin{aligned}
[f(x)g(x)]h(x)&=\left[\sum_{i=0}^{\infty}c_ix^i\right]\left(\sum_{i=0}^{\infty}d_ix^i\right)\quad \textit{donde}\quad c_i=\sum_{j'+k'=i}a_{j'}b_{k'}\\
&=\sum_{i=0}^{\infty}e_ix^i\quad \textit{donde}\quad e_i=\sum_{j+k=i}c_jd_k\\
&=\sum_{i=0}^{\infty}\left(\sum_{j+k=i}c_jd_k\right)x^i\\
&=\sum_{i=0}^{\infty}\left(\sum_{j+k=i}\left(\sum_{j'+k'=j}a_{j'}b_{k'}\right)d_k\right)x^i\\
&=\sum_{i=0}^{\infty}\left(\sum_{j+k=i}\left(\sum_{j'+k'=j}a_{j'}b_{k'}d_k\right)\right)x^i
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{\infty} \left(\sum_{j+k=i} \left(\sum_{j'+k'=k} a_j b_{j'} d_{k'} \right) \right) x^i \\
&= \sum_{i=0}^{\infty} \left(\sum_{j+k=i} a_j \left(\sum_{j'+k'=k} b_{j'} d_{k'} \right) \right) x^i \\
&= \sum_{i=0}^{\infty} \left(\sum_{j+k=i} a_j k_k \right) x^i \quad donde \quad k_k = \sum_{j'+k'=k} b_{j'} d_{k'} \\
&= \sum_{i=0}^{\infty} \ell_i x^i \quad donde \quad \ell_i = \sum_{j+k=i} a_j k_k \\
&= \left(\sum_{i=0}^{\infty} a_i x^i \right) \left[\sum_{i=0}^{\infty} k_i x^i \right] \quad donde \quad k_i = \sum_{j'+k'=i} b_{j'} d_{k'} \\
&= f(x)[g(x)h(x)]
\end{aligned}
$$

2. Sean

$$f(x)g(x) = \sum_{i=0}^{\infty} d_i x^i \quad donde \quad d_i = \sum_{j+k=i} a_j b_k$$

$$g(x)f(x) = \sum_{i=0}^{\infty} e_i x^i \quad donde \quad e_i = \sum_{j+k=i} b_j a_k$$

debemos demostrar que $d_i = e_i$ para toda $i = 1, 2, ...$

$$d_i = \sum_{j+k=i} a_j b_k = \sum_{k+j=i} b_k a_j = e_i$$

3. En este caso

$$1 = \sum_{i=0}^{\infty} d_i x^i, \quad donde\ d_0 = 1\ y\ d_k = 0\ \forall\ k > 0$$

por tanto

$$f(x)1 = \sum_{i=0}^{\infty} e_i x^i \quad donde \quad e_i = \sum_{j+k=i} a_j d_k$$

Considerando el valor de d_k obtenemos

$$e_i = \sum_{j+k=i} a_j d_k = \sum_{j+0=i} a_j 1 = \sum_{j=i} a_j = a_i$$

y por lo tanto $f(x)1 = f(x)$

4. Sean $f(x)(g(x)+h(x)) = \left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty}(b_i+d_i)x^i\right) = \sum_{i=0}^{\infty} d_i x^i$ donde

$$d_i = \sum_{j+k=i} a_j(b_k+c_k), \quad f(x)g(x) = \sum_{i=0}^{\infty} u_i x^i, \ \textit{donde}\ u_i = \sum_{j+k=i} a_j b_k$$

y

$$f(x)h(x) = \sum_{i=0}^{\infty} e_i x^i, \ \textit{donde}\ e_i = \sum_{j+k=i} a_j c_k$$

Debemos demostrar que $d_i = u_i + e_i$ para toda $i = 0, 1, 2, 3, ...$

$$d_i = \sum_{j+k=i} a_j(b_k+c_k) = \sum_{j+k=i}(a_j b_k + a_j c_k) = \sum_{j+k=i} a_j b_k + \sum_{j+k=i} a_j c_k = u_i + e_i$$

□

Teorema 3. *Si A es un anillo conmutativo, entonces $A[x]$ es un anillo conmutativo*

Teorema 4. *Si A es un dominio entero, entonces $A[x]$ es un dominio entero.*

Demostración. Sea $f(x) = \sum_{i=0}^{\infty} a_i x^i$ y $g(x) = \sum_{i=0}^{\infty} b_i x^i$ ambos distintos de 0. Debemos demostrar que $f(x)g(x) \neq 0$. Como $f(x)$ y $g(x)$ son distintos de 0, entonces existen $n, m \in \mathbb{N}$ tales que $a_n \neq 0$ y $a_k = 0$ para toda $k > n$ y $b_m \neq 0$ y $b_j = 0$ para toda $j > m$. Sea

$$f(x)g(x) = \sum_{i=0}^{\infty} c_i x^i, \quad \textit{donde} \quad c_i = \sum_{j+k=i} a_k b_j$$

Mostraremos que

$$c_{m+n} = \sum_{j+k=i} a_k b_j \neq 0$$

Existen dos posibilidades para k y j que son $(k > n \ o \ j > m)$ o $(k \leq n \ o \ j \leq m)$. En el primer caso se tendrá que $a_k = 0$ o $b_j = 0$ y por lo tanto $a_k b_j = 0$ y en el segundo caso forzosamente $k = n$ y $j = m$, ya que si no es así, $k + j < n + m$ y por lo tanto $a_k b_j$ no aparece como sumando en c_{m+n}. Concluimos entonces que

$$c_{m+n} = \sum_{j+k=n+m} a_k b_j = a_n b_m \neq 0$$

puesto que $a_n \neq 0$ y $b_m \neq 0$ y A es un dominio entero. Luego $f(x)g(x) \neq 0$ □

Uno de los conceptos importantes en el anillo de polinomios es el grado de un polinomio, y será mediante este concepto que podremos adaptar al anillo de polinomios resultados de los enteros como lo es el Algoritmo de la división.

Definición 5. *Sea A un anillo y $fx = \sum_{i=0}^{\infty} a_i x^i$ un polinomio distinto de 0 en $A[x]$. Al elemento $a_n \neq 0$ de A tal que $a_k = 0$ para toda $k > n$ lo llamaremos el coeficiente principal de $f(x)$ y en este caso decimos que el grado de $f(x)$ es n y lo denotamos por $\partial f(x) = n$ y cuando el coeficiente principal es 1 diremos que el polinomio es mónico.*

Teorema 5. *Sea A un dominio y sean $f(x)$ y $g(x)$ polinomios distintos de 0 en $A[x]$.*

1. *Si $f(x) + g(x) \neq 0$, entonces $\partial(f(x) + g(x)) \leq \text{máx}\{\partial f(x), \partial g(x)\}$.*
2. *Si $\partial f(x) \neq \partial g(x)$, entonces $\partial(f(x) + g(x)) = \text{máx}\{\partial f(x), \partial g(x)\}$.*
3. *$\partial(f(x)g(x)) = \partial f(x) + \partial g(x)$*

Demostración. Sea $f(x) = \sum_{i=0}^{\infty} a_i x^i$ y $g(x) = \sum_{i=0}^{\infty} b_i x^i$ con $a_n \neq 0$, $a_k = 0$ para toda $k > n$ y $b_m \neq 0$, $b_j = 0$ para toda $j > m$. Esto es $\partial f(x) = n$ y $\partial g(x) = m$.

1. Supongamos que $n \geq m$.
$$f(x) + g(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$
donde $a_k + b_k = 0$ para todo $k > n$ y por lo tanto
$$\partial(f(x) + g(x)) \leq n = \text{máx}\{\partial f(x), \partial g(x)\}$$

2. Supongamos $n > m$. Como en (1), $a_k + b_k = 0$ para toda $k > n$.
Debido a que $b_n = 0$, entonces $a_n + b_n = a_n \neq 0$ y por lo tanto
$$\partial(f(x) + g(x)) = n = \text{máx}\{\partial f(x), \partial g(x)\}$$

3. En el caso del producto $f(x)g(x)$
$$f(x)g(x) = \sum_{i=0}^{\infty} c_i x^i$$
se tiene que $c_{n+m} = a_n b_m \neq 0$ y $c_i = 0$ para toda $i > n + m$ y por lo tanto
$$\partial(f(x)g(x)) = n + m = \partial f(x) + \partial g(x)$$

□

Corolario 1. *Si A es un dominio entero, entonces los polinomios en $A[x]$ que son invertibles son los elementos de A que lo son. En el caso particular cuando A es campo, estos elementos son $A - \{0\}$*

Demostración. Si $f(x) \in A[x]$ es invertible, existe $g(x) \in A[x]$ tal que $f(x)g(x) = 1$ y por tanto $\partial f(x) + \partial g(x) = 0$ y por lo tanto $\partial f(x) = 0$, es decir, $f(x)$ es un elemento de A. Si A es campo los elementos invertibles de $A[x]$ son los elementos de $A - \{0\}$ □

Los polinomios de grado cero en $A[x]$ son justamente los elementos de $A - \{0\}$ y los llamamos polinomios constantes.